



Ministère de l'Artisanat et de l'Economie
Sociale et Solidaire



ENSA

المدرسة الوطنية للعلوم التطبيقية بالجديدة
Ecole Nationale des Sciences Appliquées

ENSA
Tanger

المدرسة الوطنية للعلوم التطبيقية بطنجة
Ecole Nationale des Sciences Appliquées de Tanger

Du 4 Aout au 3 Septembre 2014

Réalisé par :

- IDRISSI Abdessamad
- OUDRISS Said

Encadré par :

- Mme LEHLALI Souad

**F MISE
SUPERV**

Sta

SOMMAIRE

| | |
|---|-----------|
| REMERCIEMENT | 3 |
| ACRONYMES & ABREVIATIONS..... | 4 |
| LISTE DES FIGURES | 5 |
| LISTE DES TABLEAUX | 6 |
| AVANT-PROPOS..... | 7 |
| RESUME | 10 |
| INTRODUCTION..... | 11 |
| CHAPITRE I. CADRE ET CONTEXTE DU STAGE..... | 12 |
| 1. Organisme d'accueil..... | 13 |
| a) Présentation générale du Ministère de l'Artisanat et de l'Economie Sociale et Solidaire (MAESS) :..... | 13 |
| b) Organisation du Ministère de l'Artisanat..... | 13 |
| c) Missions | 15 |
| 2. Contexte du stage : | 15 |
| a) Département d'accueil | 15 |
| b) Positionnement du thème | 15 |
| c) Cahier des charges..... | 16 |
| d) Contraintes | 16 |
| e) Méthodologie | 16 |
| CHAPITRE II. ETUDE ET CHOIX DE LA SOLUTION | 18 |
| 1. La Supervision..... | 19 |
| a) Qu'est-ce que la supervision : | 19 |
| b) Quoi superviser ? | 19 |
| c) Pourquoi superviser ? | 19 |
| d) Enjeux pour les DSI : | 19 |
| e) Comment superviser : | 19 |
| f) pourcentage d'indisponibilité | 20 |
| 2. Etude des solutions..... | 20 |
| a) Introduction | 20 |
| b) Critère de Sélection : | 21 |
| c) Analyse des produits..... | 21 |
| d) FAN..... | 21 |
| e) Nagios | 22 |
| f) Shinken | 22 |
| g) Eyes Of Network | 22 |
| h) Spiceworks..... | 23 |
| 3. Solution retenue..... | 23 |

| | |
|---|----|
| CHAPITRE III. PRESENTATION, INSTALLATION ET PARAMETRAGE DE LA SOLUTION..... | 25 |
| 1. Présentation de l'EON..... | 26 |
| 2. Présentation de la suite logicielle de l'EON | 26 |
| 3. Architecture adopté :..... | 27 |
| 4. Configuration du VMware :..... | 27 |
| 5. Installation de la solution | 28 |
| 6. Configuration de l'SNMP :..... | 32 |
| a) Installation du protocole SNMP sous linux | 32 |
| b) Installation et paramétrage du SNMP sous Windows | 33 |
| CHAPITRE IV. CONFIGURATION DES SERVEURS | 36 |
| 1. Configuration d'un serveur DHCP : | 37 |
| a) Configuration du serveur | 37 |
| b) Configuration des postes clientes :..... | 39 |
| 2. Installation et configuration d'un serveur DNS (Bind9) sur Ubuntu :..... | 39 |
| a) Pré-requis..... | 39 |
| b) Configuration de la carte réseau :..... | 39 |
| c) Installation et configuration de Bind9 : | 40 |
| d) Test de fonctionnement | 43 |
| 3. Configuration d'un serveur web | 44 |
| a) Configuration du serveur http (apache2) : | 44 |
| b) Sécurisation du serveur apache2 par SSL | 46 |
| CHAPITRE V. AJOUT DES SERVICES DE SUPERVISION A L'EON..... | 51 |
| 1. Connexion au serveur | 52 |
| 2. Scan du réseau..... | 52 |
| 3. Superviser un hôte :..... | 53 |
| 4. Ajout d'une commande de supervision (services)..... | 54 |
| 5. Superviser d'autres entités : | 55 |
| 6. Vue des équipements et des services | 55 |
| CONCLUSION..... | 58 |
| WEBOGRAPHIE..... | 59 |

REMERCIEMENT

Tout d'abord on tient à remercier très chaleureusement l'organisme ministère de l'Artisanat et de l'Economie Sociale et Solidaire au nom du Directeur de la Direction du Ressource et des Systèmes d'information et surtout la division des systèmes d'information qui nous ont offert cette opportunité d'effectuer notre stage au sein du ministère, chose qui nous mène qu'à bien croire à nos cadres supérieurs qui aident au développement et au progrès de notre cher pays à travers l'encadrement des jeunes compétences, les dirigeants du futur.

On tient aussi à remercier notre encadrante l'ingénieur Mme LEHLALI Souad, pour son accueil très chaleureux au sein de la DRSI, pour ses précieuses explications et pour avoir mettre à notre disposition tous les outils dont nous avons besoin pour le bon déroulement de notre stage.

Et sans oublier tout le corps de la division du système d'informations qui était tout le temps à notre disposition pour toute sorte d'information utile.

On aimerait aussi remercier la direction de l'Ecole National des Sciences Appliquées (ENSA) d'El-JADIDA et de TANGER et tous nos professeurs sans exception, lesquels faisaient de leur mieux pour qu'on ait une meilleure formation.

ACRONYMES & ABREVIATIONS

DHCP : Dynamic Host Configuration Protocol

DNS : Domaine Name Service

DRSI : Direction des Ressource et des Systèmes d'informations

ENSA : Ecole Nationale des Sciences Appliquées.

EON : EyesOfNetwork

FQDN : Fully Qualified Domain Name

GNU/GPL : GNU General Public License (en français la Licence publique générale GNU), une licence de logiciel libre provenant du projet GNU signifiant au sens large « Guaranteed Public for Life »

HTTP : HyperText Transfer Protocol

ITIL : Information Technology Infrastructure Library pour « Bibliothèque pour l'infrastructure des technologies de l'information » est un ensemble d'ouvrages recensant les bonnes pratiques « best practices » du management du système d'information.

LAMP : Linux Apache MySQL PHP

MAESS : Ministère de l'Artisanat et de l'Economie Sociale et Solidaire.

SLA : Service Level Agreement est un document qui définit la qualité de service requise entre un prestataire et un client

SNMP : Simple Network Management Protocol

SSL : Secure Sockets Layer, un protocole de sécurisation des échanges sur Internet

@IP : adresse IP

LISTE DES FIGURES

| | |
|---|----|
| Figure 1 : Organigramme générale du MAESS | 14 |
| Figure 2 : Organigramme de la DRSI du MAESS | 14 |
| Figure 3 : Architecture adoptée | 27 |
| Figure 4 : détails de paramétrage de la carte VMnet1 | 28 |
| Figure 5 : Configuration des paramètres réseaux de VMware | 28 |
| Figure 6 : page de démarrage de l'installation de l'EON | 29 |
| Figure 7 : suite de l'installation de l'EON | 30 |
| Figure 8 : paramétrage des périphériques réseau pour EON | 31 |
| Figure 9 : choix des services à installer | 31 |
| Figure 10 : ajout du SNMP pour Windows 7 et 8 | 33 |
| Figure 11 : ajout du SNMP pour Windows XP et Server | 34 |
| Figure 12 : configuration des propriétés du Service SNMP pour Windows | 35 |
| Figure 13 : Configuration du serveur DHCP sous Linux | 38 |
| Figure 14 : attribution d'une @IP fixe à une machine avec DHCP | 38 |
| Figure 15 : modification du fichier interfaces pour Linux | 39 |
| Figure 16 : paramétrage de l'interface du serveur DNS | 40 |
| Figure 17 : Configuration du fichier named.conf | 41 |
| Figure 18 : Configuration du fichier artisanat.com.zone | 41 |
| Figure 19 : modification du fichier artisanat.com.rev | 42 |
| Figure 20 : configuration du fichier resolv.conf | 43 |
| Figure 21 : test de fonctionnement du serveur DNS | 43 |
| Figure 22 : connexion au serveur http | 46 |
| Figure 23 : connexion au serveur EON par un navigateur web | 52 |
| Figure 24 : ajout d'un job pour le scan du réseau | 53 |
| Figure 25 : page d'information sur l'hôte ajouté | 54 |
| Figure 26 : Page de configuration d'un service | 54 |
| Figure 27 : ajout du service dhcp_status | 55 |
| Figure 28 : vue des équipements | 56 |
| Figure 29 : Vue de services | 57 |

LISTE DES TABLEAUX

| | |
|--|----|
| Tableau 1 : Rappel sur l'indisponibilité annuelle | 20 |
| Tableau 2 : Tableau comparatif des outils de supervision open source | 24 |
| Tableau 3 : informations sur les serveurs à installer | 37 |

AVANT-PROPOS

La formation des écoles des ingénieurs dans lesquels on suit nos études, se déroule en deux phases:

- un cycle préparatoire d'une durée de 2 années (ou quatre semestres) qui constitue le tronc commun
- un cycle ingénieur de 3ans (ou six semestres) dans de nombreux domaines de spécialités.

Durant ce cursus, l'accent est mis sur les enseignements scientifiques et techniques, les sciences humaines, la gestion et aussi sur la connaissance de l'entreprise. Les travaux pratiques prennent une part très importante dans la scolarité. La formation est complétée alors par des projets et des stages en entreprise.

La formation vise à préparer l'élève aux différentes filières des sciences de l'ingénieur à savoir Génie Informatique, Génie des Télécommunications et Réseaux, Génie Industriel, Génie Electrique, Génie Electronique et Informatique Industrielle.

Les lauréats de ces filières exercent dans les divers domaines liés à leur spécialité. Vue la formation polyvalente, ils peuvent s'orienter facilement en fonction des conjonctures économiques.

Le cycle préparatoire :

L'objectif du cycle préparatoire est de donner aux élèves une solide formation de base scientifique, technique, ainsi qu'en communication orale et écrite. A cela s'ajoute l'élaboration de mini-projets et stages. Le caractère généraliste de la formation du cycle préparatoire est indispensable pour donner, à tout ingénieur, les connaissances et les compétences qui lui permettent, quelle que soit sa spécialité, de se réorienter en cours de carrière. Le rôle de ce cycle est aussi d'aider l'élève à acquérir les méthodes et les techniques de travail qui lui seront indispensables pour la suite de ses études et dans sa carrière professionnelle.

Le cycle ingénieur :

L'objectif de ce cycle est de donner au futur ingénieur une solide formation dans le domaine de la spécialité choisie ainsi qu'en enseignement de langues, de communication orale et écrite, de connaissance de l'entreprise et aussi de préparer l'élève ingénieur à son futur métier par des stages et des projets.

Formation et organisation pédagogique

A l'instar du cycle préparatoire, la formation dans le cycle ingénieur est organisée au sein du département Cycle Ingénieur qui regroupe les filières de spécialités. L'organisation administrative de ce département est similaire à celle du département du cycle préparatoire. Le cursus est organisé sur trois années réparties en six semestres dans des filières de spécialité

A noter que d'autres spécialités peuvent être créées (par arrêté de l'autorité gouvernementale chargée de l'enseignement supérieur)

Le mode de gestion pédagogique est similaire à celui du cycle préparatoire.

La présence à toutes les formes d'enseignement est obligatoire. La formation est complétée par des stages en entreprise, établissement ou dans des laboratoires. Les stages préparent l'élève ingénieur à sa future profession par l'acquisition d'expériences pratiques. Il est donc capital qu'ils correspondent à une situation réelle de travail et qu'ils s'inscrivent à l'intérieur des activités normales de l'entreprise. Le nombre, la durée et l'emplacement de ces stages ainsi que le mode d'évaluation seront étudiés par les différents intervenants (direction, départements etc.). Le sixième semestre est consacré entièrement à un stage en entreprise ou dans des laboratoires de recherche dont le projet donne lieu à la rédaction d'un mémoire et à une soutenance devant un jury d'industriels et d'universitaires. Conditions d'accès :

Admission en première année :

L'accès en première année se fait par voie de concours ouvert, après présélection basée sur la moyenne générale du Bac, aux:

- Candidats inscrits à l'année terminale du baccalauréat de l'année en cours dans l'une des séries suivantes : sciences mathématiques ou sciences expérimentales ou sciences et technologies (nouveau système)
- Titulaires du Baccalauréat en sciences mathématiques ou sciences expérimentales ou sciences et technologies (nouveau système) ou en l'une des séries scientifiques ou techniques (ancien système) ou équivalent.

Admission en troisième année :

Élèves des classes préparatoires déclarés admissibles au Concours National Commun d'accès aux grandes écoles.

Candidats titulaires de l'un des diplômes suivants :

- Diplôme d'Études Universitaires Générales (D.E.U.G.)
- Diplôme d'Études Universitaires professionnelles (D.E.U.P.)
- Diplôme d'Études Universitaires des sciences et techniques (D.E.U.S.T.)

- Diplôme Universitaire de Technologie (D.U.T.)
- Licence

Admission en quatrième année :

Pour les titulaires d'une licence ou d'une maîtrise ou d'un diplôme reconnu équivalent selon les prérequis demandés.

Comme nous avons cité la formation est complétée par des stages en entreprise ou en établissement public ou privés ainsi que des laboratoires , et c'est dans ce cadre que nous avons intégré le Ministère de l'Artisanat et de l'Economie Sociale et Solidaire où nous allons travailler sur « L'ETUDE ET LA MISE EN ŒUVRE D'UNE SOLUTION DE SUPERVISION DU RESAUX ».

RESUME

La taille des réseaux ne cessant de grandir de jour en jour et l'importance de ceux-ci dans le monde de l'entreprise prenant une place prépondérante, le besoin de contrôler en temps réel leur qualité et leur état est rapidement devenu une priorité. C'est dans ce but qu'est apparu, il y a maintenant une vingtaine d'années, le concept de supervision de réseaux.

Nous présenterons dans ce document ce qu'est la supervision de réseaux ainsi qu'une implémentation sur une machine virtuelle.

Pour ce faire nous allons définir le concept et la notion de la supervision de réseaux. nous allons aussi faire une étude comparative sur les différentes solutions de supervision des réseaux, en vue de choisir la meilleure solution puis nous allons procéder à une étude approfondie de cette solution retenue. Enfin nous allons procéder à sa mise en œuvre en tenant compte d'une architecture bien déterminé.

INTRODUCTION

Les systèmes d'information sont tous différents par leur taille, leur nature, leur criticité. Ils ont cependant pour point commun d'être le théâtre d'incidents, à un moment ou à un autre. Un des rôles des administrateurs est justement de gérer cela. Ils doivent concevoir l'architecture du système d'information de telle manière qu'une panne ait un impact minimal sur le reste du système.

Les administrateurs ont un objectif clair : le maintien en production du système d'information. Cependant, tous les éléments ne sont pas logés à la même enseigne en ce qui concerne la criticité. Certaines parties sont vitales pour l'entreprise, comme les serveurs. Sans outil de supervision, il est quasi impossible pour un administrateur de garder en tête ces différents niveaux de criticité. L'outil de supervision peut ainsi aider à mettre des priorités sur les interventions des administrateurs et leur permettre de se concentrer sur l'essentiel.

C'est pourquoi les administrateurs réseaux et systèmes font appel à des logiciels de surveillance et de supervision de réseaux. Ces logiciels vérifient l'état du réseau ainsi que des machines connectées et permettent à l'administrateur d'avoir une vue d'ensemble en temps réel de l'ensemble du parc informatique sous sa responsabilité. Il peut être aussi informé (par email, par SMS) en cas de problème. Un tel système assure une gestion proactive du système et améliore la disponibilité effective des applications et des services opérant sur les serveurs. Mieux elle permet d'anticiper et de prévoir les éventuels besoins en termes d'équipements pour une gestion optimale du système d'information.

Conscient de cela, le MAESS dans sa volonté d'améliorer le fonctionnement de son réseau, veut se doter d'une solution de supervision Open Source qui surveille le taux d'occupation des disques, l'utilisation de la RAM, la charge des processeurs, les services web et de messagerie.

C'est ainsi que nous avons été sollicité pour l'étude et la mise en œuvre d'un outil de supervision de réseau.

Le présent rapport résume l'ensemble des actions que nous avons fait durant la mise en place de l'outil en ce qui concerne l'installation et la configuration

CHAPITRE I. CADRE ET CONTEXTE DU STAGE

Nous allons d'abord décrire l'environnement de travail dans lequel nous allons évoluer, ensuite nous présenterons le thème étudié, et la méthode de travail adoptée.

1. Organisme d'accueil

a) **Présentation générale du Ministère de l'Artisanat et de l'Economie Sociale et Solidaire (MAESS) :**

L'artisanat est un secteur primordial, qui se caractérise par un savoir-faire régional, spécifique et diversifié et qui recèle un énorme potentiel de croissance.

Il y a lieu d'abord de noter que le secteur de l'artisanat englobe aussi bien l'artisanat de production à fort contenu culturel que l'artisanat de service, d'une part, et d'autre part, que d'une manière générale, il existe une forte demande à travers le monde de l'art de vivre marocain, du patrimoine culturel artisanal, de la décoration d'intérieur et de la mode marocaine.

Aujourd'hui, la région Rabat Salé Zemmour Zaer compte 94.000 artisans dont 34.000 artisans d'art et 60.000 répartis entre les artisans de services et de production, soit 9% des emplois au niveau national. Compte tenu du taux d'urbanisation relativement élevé au niveau de la région, l'artisanat tire profit principalement du marché urbain avec un potentiel de plus en plus important, grâce notamment aux grands chantiers d'aménagement et d'urbanisation.

Les activités artisanales prédominantes sont celles liées au vêtement (tissage, confection traditionnelle, broderie, ..), au tapis, au travail du bois et à celui de la poterie.

Du a son importance et l'impact de ce secteur le Ministère de l'Artisanat est chargé d'élaborer les programmes de développement de ce dernier et d'en suivre la mise en œuvre ainsi que de réaliser toutes études se rapportant au domaine de l'artisanat et promouvoir les espaces de production et ses zones d'activités.

En effet, le Ministère permet de :

- promouvoir et organiser les activités relevant du secteur de l'artisanat et des métiers, en concertation avec les professionnels et les opérateurs concernés ;
- élaborer et mettre en œuvre des politiques de promotion commerciale des produits artisanaux et faciliter l'adaptation des entreprises de l'artisanat et des métiers aux exigences des marchés, des technologies et de la concurrence Internationale.
- œuvrer l'élaboration et la mise en œuvre des politiques et des programmes de promotion du secteur et de contrôle de la qualité de ses produits en mettant en place un système de normalisation et en agissant pour la généralisation de son adoption ;

b) **Organisation du Ministère de l'Artisanat.**

Le Ministère de l'Artisanat s'organise en plusieurs directions et divisions sous la direction du Ministre. Les figures de la page suivante (cf. figure 1, figure 2) représentent l'organigramme général du Ministère ainsi que l'organigramme de la Direction de Ressources et Systèmes d'Information (DRSI).



Figure 1 : Organigramme générale du MAESS

La Direction des Ressources et des Systèmes d'Information se divise en 4 divisions, comme le montre l'organigramme suivant :

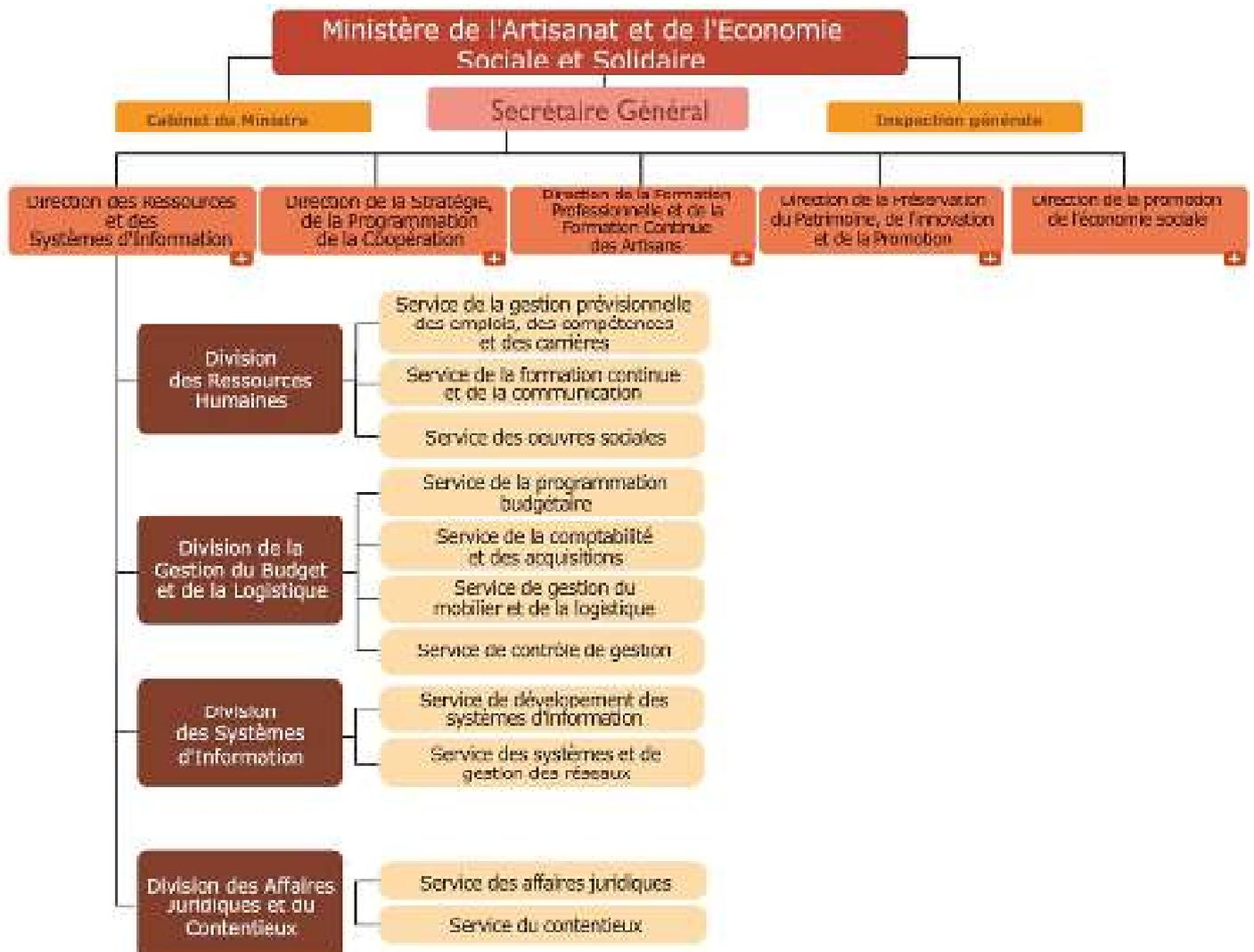


Figure 2 : Organigramme de la DRSI du MAESS

c) Missions

Le ministère d'artisanat a pour missions :

- Mise en œuvre de la stratégie de développement du secteur de l'artisanat.
- Animation économique des entreprises de l'artisanat.
- Réalisation de l'ensemble des études, recherches et statistiques concernant l'artisanat au niveau national et international.
- Elaboration et mise en œuvre des programmes de coopération susceptibles de contribuer au développement de l'artisanat.
- Suivi des activités des chambres de l'artisanat et leur fédération.
- Exercer la tutelle sur les établissements relevant de sa compétence.

La Direction des Ressource et des Système d'Informations a pour but :

- Préparer et exécuter le budget du Département ministériel de l'artisanat,
- gérer les ressources matérielles et le patrimoine mobilier et immobilier du Département ministériel de l'Artisanat,
- gérer les affaires du personnel et qualifier les ressources humaines,
- assurer le suivi du contentieux en matière des affaires du personnel et du patrimoine du Département de l'Artisanat
- Développer l'informatisation des services centraux du Département et assurer le suivi de sa mise en œuvre dans les services déconcentrés

2. Contexte du stage :

a) Département d'accueil

Nous avons été accueillis au Division du Systèmes d'information. Cette division a pour rôle de :

- Gérer le parc informatique
- Gérer la messagerie
- Configurer les machines
- Mettre à jour l'antivirus pour les postes utilisant les applications
- Administrer les systèmes
- installer les systèmes d'exploitation
- Gérer les disques
- Configurer et administrer les services réseaux
- Gérer le service d'annuaire
- Maintenir les équipements (les serveurs, postes de travail, imprimantes, onduleurs)

b) Positionnement du thème

La DRSI gère un parc informatique important. La tâche des administrateurs systèmes devenant de plus en plus complexe, il est impérieux pour l'équipe de gagner en temps et en efficacité grâce à un bon outil de supervision. L'enjeu du déploiement, de la configuration et de l'optimisation d'une solution de surveillance des équipements est de permettre aux administrateurs :

- D'être alertés en temps réel des dysfonctionnements des équipements et des services
- De pouvoir remonter facilement les alertes
- D'être proactifs aux problèmes
- D'améliorer la disponibilité effective des applications

vu le nombre important de logiciels de supervision, il paraît nécessaire de confronter une solution solide qui intègre plusieurs compléments et mettre en œuvre cette solution retenue. Ce qui justifie le thème :

« ETUDE ET MISE EN ŒUVRE D'UN OUTIL DE SUPERVISION DE RESAU »

c) Cahier des charges

L'objectif de la solution de supervision devra permettre de surveiller les équipements et services du réseau

Concernant les équipements et les services ce sont :

- Les serveurs DNS, DHCP et http.
- Le taux d'occupation des partitions
- Le taux d'utilisation des processeurs
- L'utilisation de la RAM
- etc.

d) Contraintes

La solution retenue devra être une licence Open Source, et n'inclus les équipements réseaux tels que les routeurs, les switches.

e) Méthodologie

Pour remplir cette mission nous allons procéder comme suit :

- Nous allons commencer par une collecte d'information générale sur le domaine de la supervision pour se familiariser avec ce concept.
- Ensuite nous allons faire une étude comparative des outils Open source existant en vue de choisir le plus optimale en tenant compte de l'évolution du réseau.
- Enfin nous allons mettre en œuvre cette solution, par son installation, sa configuration et son optimisation pour superviser tous les services configuré dans les machine (Serveur DHCP, DNS, http...).

CHAPITRE II. ETUDE ET CHOIX DE LA SOLUTION

Nous allons commencer par une présentation du concept de la supervision, puis une étude de quelques solutions open source existant dans le marché en vue de les évoluer et choisir la meilleure optimale que nous allons utiliser pour superviser notre réseau.

1. La Supervision

a) Qu'est-ce que la supervision :

Devenues incontournables depuis de nombreuses années, les solutions de supervision des systèmes d'information ont pour vocation d'apporter une vue d'ensemble sur le fonctionnement des systèmes d'information, de les auditer, d'en surveiller la disponibilité et la performance, et d'alerter les départements en charge de son exploitation.

La supervision est un ensemble de fonctions qui consiste à mettre en place des indicateurs d'état d'un système et d'un réseau.

Elle va donc nous permettre de :

- Vérifier l'état d'un hôte ou d'un service
- Remonter des alertes
- Détecter des comportements anormaux

b) Quoi superviser ?

Dans un premier temps nous nous concentrerons sur la supervision du système informatique. Ce dernier se compose en deux parties :

La supervision technique :

- Elle va consister à surveiller le réseau, l'infrastructure et les machines du système d'information

La supervision applicative :

- Elle va consister à surveiller les applications et les processus métiers.

c) Pourquoi superviser ?

Si quelque chose peut mal fonctionner, elle finira inévitablement par mal fonctionner un jour ou l'autre ». Partant de ce constat, nous avons fait le choix de la supervision pour nous permettre d'anticiper un éventuel dysfonctionnement et de vérifier rapidement l'état de santé et des performances de nos parcs informatiques.

d) Enjeux pour les DSI :

- Garantir la disponibilité et les niveaux de service (SLA) du système en cas de panne
- Prévenir en cas de problème
- Réduire les délais d'interventions

e) Comment superviser :

De nombreuses solutions sont disponibles.

Certaines sont spécialisées dans la supervision des composants du SI, d'autres sont plus globales. La différenciation s'effectue généralement sur le nombre de paramètres exploitables et leur finesse d'analyse. Cette précision ne doit pas pour autant rendre les tableaux de bord et les synthèses illisibles pour les administrateurs. Cependant elle doit alerter d'un fonctionnement normal ou anormal.

Le fonctionnement est simple, il se compose d'un superviseur qui va effectuer de l'acquisition de données de manière active ou passive.

Cette acquisition va se faire de façon automatique avec le protocole SNMP, qui est présent sur la majorité des équipements informatiques.

Nous pouvons en résumer le fonctionnement de la façon suivante :

Supervision = information + traitement

f) pourcentage d'indisponibilité

on rappelle que :

| Si disponible... | Indisponibilité annuelle |
|------------------|-----------------------------------|
| 90% | 876 heures |
| 95% | 438 heures |
| 99% | 87 heures, 36 minutes |
| 99.9% | 8 heures, 45 minutes, 36 secondes |
| 99.99% | 52 minutes, 33.6 secondes |
| 99.999% | 5 minutes, 15.36 secondes |
| 99.9999% | 31.68 secondes |

Tableau 1 : Rappel sur l'indisponibilité annuelle

2. Etude des solutions

a) Introduction

L'étude des solutions va suivre un certain cheminement logique.

Tout d'abord il faut définir des critères de sélection pour s'assurer que le produit remplit bien des fonctions attendues, importantes pour le projet.

Ensuite nous allons définir une liste de solution les plus utilisées par la communauté et qui ont fait leurs preuves.

Puis, nous testerons les produits et nous utiliserons un tableau de vote pondéré pour appliquer nos critères sur ces solutions.

Enfin, nous choisirons à l'aide du tableau la solution qui sera retenue pour les futurs déploiements.

b) Critère de Sélection :

Pour permettre de mieux calibrer la solution, les produits retenus, seront jugés selon les critères suivants :

- Licence du produit
- Plateforme d'installation
- Simplicité d'installation et d'utilisation
- Importance de la communauté
- Compatibilité
- Modularité du produit
- Génération de rapport
- Droit et profil d'utilisation
- Sauvegarde du produit
- Pertinence des alertes

c) Analyse des produits

Les produits ont été présélectionnés car ils font partis des solutions les plus utilisées par la communauté de supervision libre.

Ce sont ces mêmes produits qui seront soumis à un vote de pondération.

NB : La liste ne recensera pas l'ensemble des solutions existantes.

d) FAN

FAN pour Fully Automated Nagios est une distribution qui permet d'installer Nagios très rapidement avec les outils utilisés couramment pour Nagios.

Les avantages sont que l'installation est rapide et simple, il y a peu de configuration pour commencer et cette dernière est simple.

C'est une distribution parfaite pour ceux qui débute avec Nagios, mais elle présente aussi des inconvénients tels que la vieillesse des applications par rapports aux versions d'aujourd'hui, l'emplacement des fichiers de configurations et différent et peut donc compliquer la vie lors de la recherche de solution sur des problèmes de configuration.

Le plus gros inconvénient et pas des moindres est que la version de Nagios est patchée, sans une nouvelle version de FAN, il est impossible d'upgrader Nagios.

De plus le fait que tout soit préconfiguré ne nous permet pas de bien connaître le fonctionnement de notre serveur.

e) Nagios

Nagios est un programme libre sous licence GPL qui fonctionne sur linux et qui permet de surveiller le système et le réseau.

Il peut surveiller des hôtes, des services et des actifs réseaux.

Son rôle est d'alerter quand un élément supervisé à un problème.

C'est un programme modulaire qui se décompose en trois parties :

- Le moteur de l'application qui vient ordonnancer les tâches de supervision.
- L'interface web, qui permet d'avoir une vue d'ensemble du système d'information et des possibles anomalies.
- Les plugins, mini programmes que l'on peut compléter en fonction des besoins pour superviser chaque service ou ressource disponible sur l'ensemble des ordinateurs ou éléments réseaux du SI.

f) Shinken

Shinken est une version modifiée de Nagios par le célèbre (dans la communauté de la supervision) Jean GABES.

En effet il a réécrit totalement Nagios et a rajouté d'autre fonctionnalité, mais suite au refus des développeurs de Nagios d'en faire la branche principale du futur développement, le projet Shinken est devenu indépendant.

C'est un outil très puissant et qui évolue très rapidement (en date de la rédaction de ce document).

g) Eyes Of Network

Eyes Of Network (EON) est une distribution GNU/Linux dédiée à la supervision. Basée sur CentOS, elle rassemble et intègre tous les outils dont on peut avoir besoin pour superviser son réseau.

L'avantage majeur de la solution est que l'ensemble des services est réuni au sein d'une interface unique, l'idée sous-jacente étant de faciliter la mise en œuvre des processus ITIL.

Elle intègre tout ce qui est nécessaire pour la supervision (Nagios, Nagvis), la métrologie (Cacti, weathermap), la gestion d'un parc machine, Eonweb, pour l'interface Web, ou Backup manager, qui s'occupe de la sauvegarde des configurations et des données collectées.

Le tout est fourni sous licence GPL v2

Depuis la version 3.0, la solution intègre des nouveautés telles que Thruk 1.1.1 pour améliorer la composante supervision, mais aussi Shinken, qui est décidément de plus en plus présent.

h) Spiceworks

Spiceworks propose un outil destiné à simplifier le travail des administrateurs réseaux. L'application combine inventaire réseau, help desk, cartographie et surveillance. Spiceworks peut également vous mettre en relation des professionnels de l'informatique pour échanger des idées, résoudre des problèmes et décider de quelle nouvelle fonctionnalité vous pourriez avoir besoin. Enfin, le logiciel revêt une interface utilisateur d'une ergonomie à toute épreuve.

L'avantage principal est la simplicité et la rapidité d'installation mais aussi la possibilité d'intégrer l'application dans un Smartphone.

L'inconvénient majeur est le fait que la solution soit uniquement disponible pour Windows et que nous ne sommes pas maître des échanges entre le logiciel et la société qui le développe.

3. Solution retenue

Les produits seront jugés et classés en fonction des critères de sélection par une note (/10) pour chaque critère.

Le choix s'est arrêté sur la solution Eyes of Network car elle est mieux adaptée à notre demande.

Ce dernier a eu le meilleur score totale.

| Description | Coeff. | FAN | Nagios | Shinken | Eyes Of Network | Spiceworks | Remarques |
|---|--------|------------|------------|------------|-----------------|------------|---|
| Licence | | | | | | | |
| Disponible sous licence GPL | 1 | 10 | 10 | 10 | 10 | 10 | |
| Disponible facilement | 1 | 10 | 10 | 10 | 10 | 5 | Une inscription est obligatoire pour Spiceworks |
| Installation | | | | | | | |
| L'outil s'installe sous Linux | 1 | 10 | 10 | 10 | 10 | 0 | Spiceworks n'est disponible que sous Windows |
| Les données ne transitent pas en externe | 1 | 10 | 10 | 10 | 10 | 2 | Nous ne sommes pas maîtres des flux de données avec spiceworks |
| L'outil est simple à installer | 1 | 8 | 4 | 4 | 8 | 10 | Spiceworks reste le plus rapide à installer, ensuite nous avons EON et FAN. Nagios et shinken sont plus complexe à installer. |
| L'outil est compatible avec VMware | 1 | 10 | 10 | 10 | 10 | 10 | |
| Paramétrage | | | | | | | |
| L'outil est simple à paramétrer | 1 | 8 | 4 | 4 | 8 | 10 | Spiceworks est le plus simple |
| L'outil est modulable | 0,5 | 8 | 10 | 10 | 8 | 2 | Nagios et shinken sont plus modulable mais seulement pour un utilisateur confirmé |
| L'outil accepte l'ajout de plugins | 1 | 8 | 10 | 10 | 10 | 2 | L'utilisation de plugins demande un temps d'adaptation sur le produit |
| Fonctionnalités | | | | | | | |
| Envoi des mails d'alertes | 1 | 8 | 8 | 8 | 8 | 10 | bien définir les alertes mails avant de les activer |
| Peut fédérer d'autre installation | 0,5 | 6 | 6 | 6 | 6 | 6 | stratégie complexe à définir |
| Couplé à une base de connaissance | 0,5 | 6 | 8 | 8 | 10 | 10 | en natif sur EON et Spiceworks |
| L'outil est en français | 1 | 0 | 0 | 0 | 10 | 0 | seul EON est disponible en français nativement |
| Supervise des hôtes | 1 | 10 | 10 | 10 | 10 | 10 | |
| Supervise des actifs | 1 | 10 | 10 | 10 | 10 | 10 | |
| Supervise des services | 1 | 10 | 10 | 10 | 10 | 10 | |
| Fonctionne sur Smartphone | 0,4 | 5 | 5 | 5 | 5 | 10 | application gratuite seulement pour Spiceworks |
| Supervise les éléments définis dans le cahier des charges | 1 | 5 | 10 | 10 | 10 | 5 | Certains plugins ne peuvent pas être ajoutés |
| Génère des rapports | 1 | 8 | 8 | 8 | 10 | 2 | format des rapports |
| Gère plusieurs profils d'utilisateurs avec des restrictions de droits | 1 | 10 | 10 | 10 | 10 | 10 | |
| Peut être sauvegardé | 1 | 10 | 10 | 10 | 10 | 4 | |
| Total | | 157 | 158 | 158 | 178 | 123 | |

Tableau 2 : Tableau comparatif des outils de supervision open source

CHAPITRE III. PRESENTATION, INSTALLATION ET PARAMETRAGE DE LA SOLUTION

Dans ce chapitre on va présenter la solution retenue et la suite de ces compléments, puis on va détailler les étapes de son installation ainsi que son paramétrage.

1. Présentation de l'EON



Eyes Of Network (EON) est une solution open source qui répond à notre stratégie d'avoir un système d'exploitation libre contenant une suite de logiciels très utilisés dans la supervision libre.

Son installation est très rapide et c'est une solution facile à prendre en main.

Eyes of Network est une solution basée sur les processus ITIL, ainsi elle regroupe une série de logiciel permettant de faire de la gestion de la capacité et de la disponibilité.

Elle permet aussi de faire de la cartographie, de la métrologie et de générer des rapports, le tout centralisé dans une interface unique.

La liste des logiciels les plus populaires qu'elle contient est expliquée ci-dessous dans la partie architecture de EON.

2. Présentation de la suite logicielle de l'EON

La solution Eyes of Network fonctionne sur le système d'exploitation linux CentOS édité par la société Red Hat.

Sur ce système, les logiciels suivant sont installés :

- LAMP, pour Linux Apache MySQL PHP : est la suite de logiciels libres permettant de faire fonctionner notre interface graphique.
- Postfix : Postfix est un serveur de messagerie qui permet d'envoyer les mails d'alerte.
- Nagios : Nagios est l'application qui va nous permettre de surveiller les équipements de nos architectures réseau.
- Thruk : interface graphique amélioré de Nagios
- Nagvis : plugins permettant de visualiser des cartographies réseau
- Cacti : logiciel permettant de mesurer la performance des éléments supervisés
- Weathermap : plugin de Cacti permettant d'afficher une représentation graphique de l'état des liens réseaux.
- EONWEB : Eonweb est l'interface graphique de la solution qui centralise l'ensemble des outils.
- Lilac : Lilac est un outil qui permet de configurer Nagios plus simplement, cet outil intègre aussi la possibilité de scanner le réseau
- BackupManager : C'est le gestionnaire de sauvegarde de la solution.

3. Architecture adopté :

Pour réaliser notre travail on va utiliser la supervision de l'architecture suivant dans une machine virtuelle :

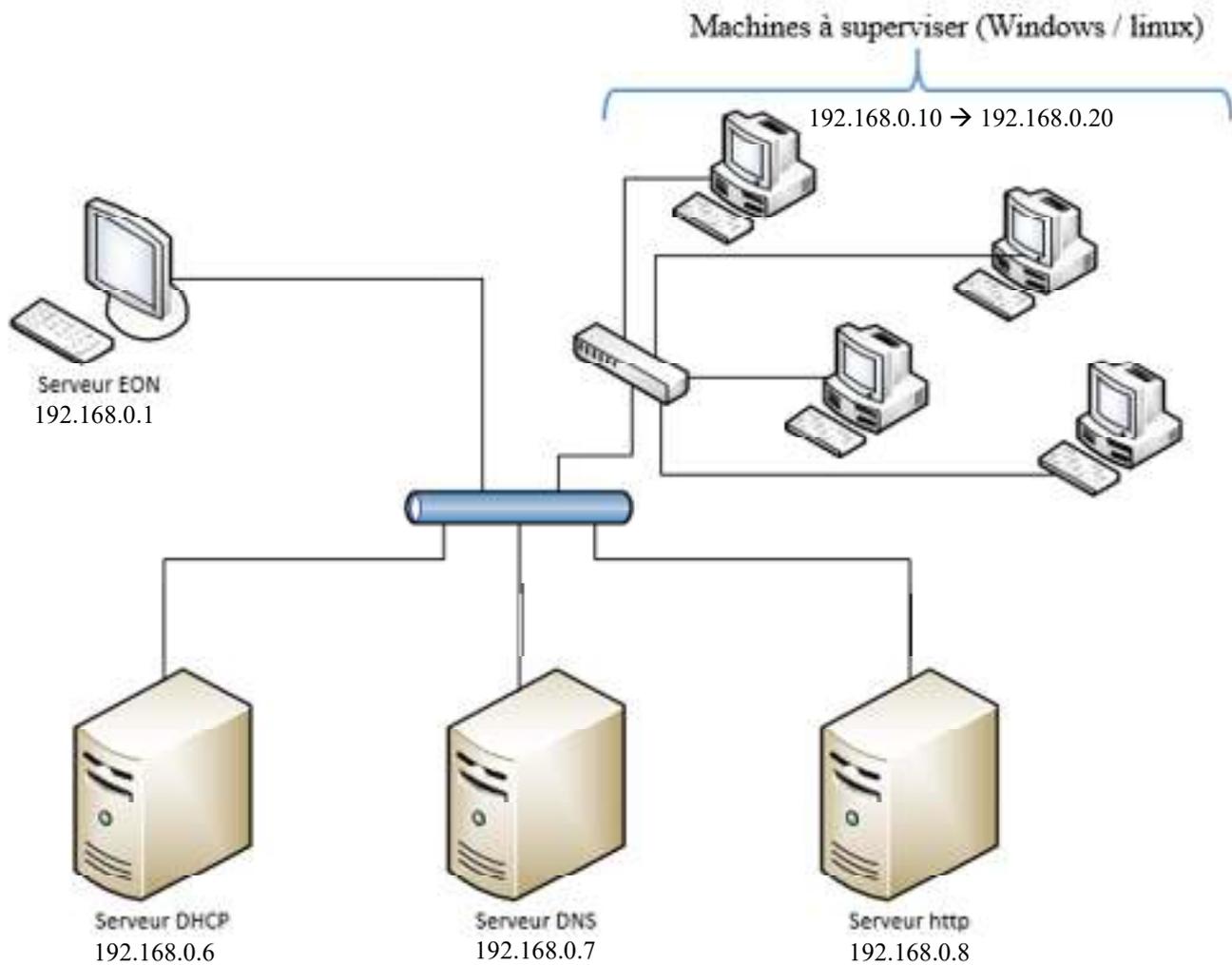


Figure 3 : Architecture adoptée

4. Configuration du VMware :

Notre projet nécessite d'avoir toutes les machine connecté au même réseau, c'est pour ça on doit choisir un réseau privé (le réseau utilisé dans notre cas et 192.168.0.0/24) et d'attribue des adresses appartenant a ce dernier pour toutes machine.

Dans notre System d'exploitation Windows on attribue 1 '@ IP 192.168.0.2 au VMware Virtual Ethenet Adapter Vmnet1

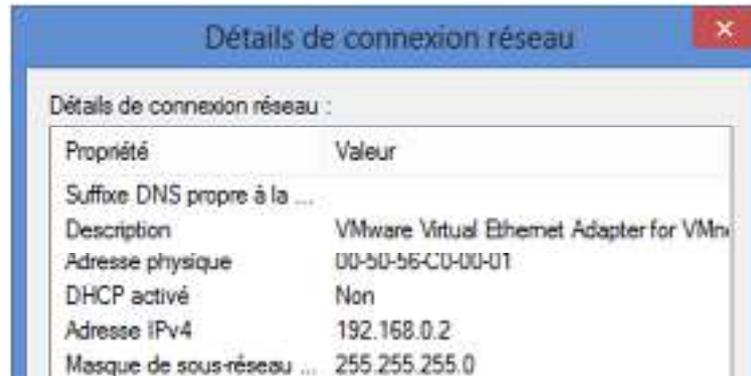


Figure 4 : détails de paramétrage de la carte VMnet1

Et pour chaque machine installé sur VMware (et même pour l'EON) on clique sur cette icône  à droite et en bas en choisit **settings** et puis on coche **Custom : Specific virtual network** en choisissant **VMnet1(Host-Only)** et puis on valide par OK.

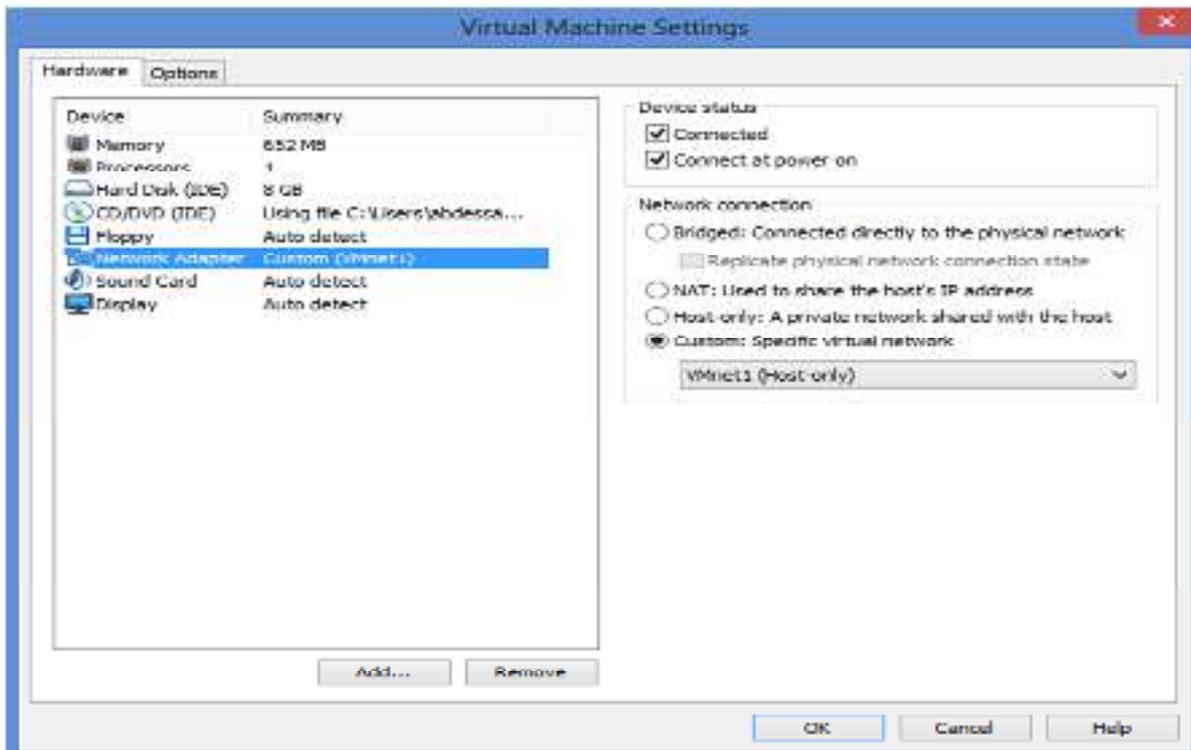


Figure 5 : Configuration des paramètres réseaux de VMware

Ce n'est pas encore terminé on attribue une adresse IP appartenant à ce réseau à l'interface de chaque machine installé sur le VMware en modifiant le fichier `/etc/network/interfaces` pour linux et en ajoutent l'`@IP` manuellement dans les propriétés réseau pour Windows.

5. Installation de la solution

Dans notre machien virtuelle VMware On choisit File/New/VirtualMachine

On choisit l'emplacement du fichier d'extension .iso téléchargé depuis le site officiel de l'EON puis suivant, pour le type du système d'exploitation on choisit autre et autre aussi pour la version, un clic sur suivant nous ramène à la fenêtre suivante :

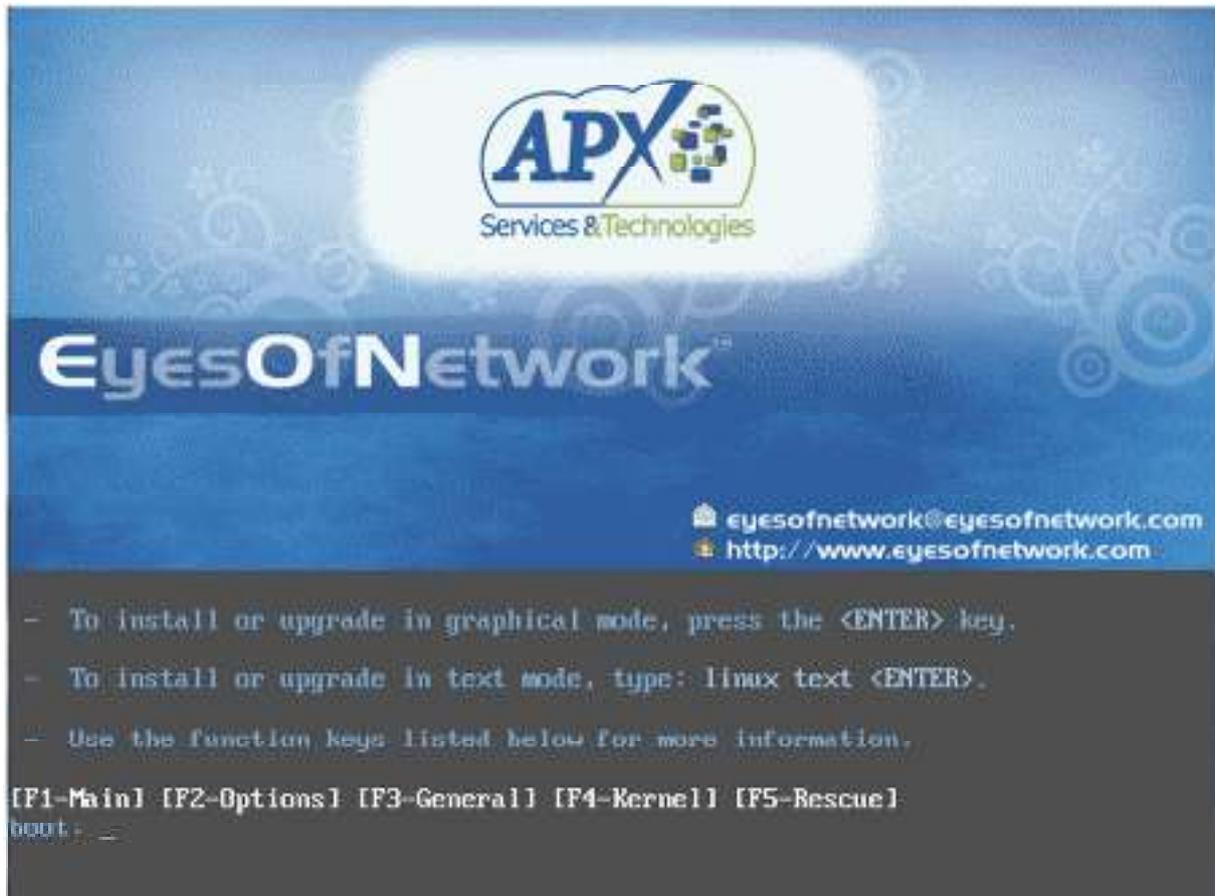


Figure 6 : page de démarrage de l'installation de l'EON

Puis on tape entrer, juste après on passe au choix du langage : on met « french » et pour le type du clavier on met « fr-latin1 ».

Et voilà la page suivant s'affiche :



Figure 7 : suite de l'installation de l'EON

On Clique sur Suivant, un message d'avertissement concernant le formatage du disque dur (virtuel), s'affiche on choisit oui.

Puis suivant, on trouve une demande de confirmation du partitionnement on choisit oui.

Nous avons maintenant la fenêtre de configuration réseau, qu'on doit configurer en entrant une adresse ip statique pour eth0, ainsi que le nom d'hôte (serveur EON), la passerelle et le DNS.



Figure 8 : paramétrage des périphériques réseau pour EON

On choisit la région Afrique/Casablanca et on coche horloge système en UTC et puis suivant.

Cette fois une fenêtre de choix du mot de passe pour l'utilisateur root s'ouvre, on tape un mot de passe et on clique sur Suivant.



Figure 9 : choix des services à installer

pour cette nouvelle fenêtre en coche tous les service pour les deux choix EON supervision et EON Production, puis suivant.

Maintenant, il faut attendre la fin de l'installation, et le temps restant est affiché sur l'écran.

Et enfin, à la fin de l'installation nous arrivons sur la page de démarrage du serveur EON qui nous renseigne l'IP de notre serveur pour pouvoir le joindre à l'aide d'un navigateur web.

6. Configuration de l'SNMP :

Avant de commencer la configuration de l'EON il faut ajouter le Protocole SNMP dans toutes les machines clients.

Simple Network Management Protocol (abrégé **SNMP**), en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

a) **Installation du protocole SNMP sous linux**

Nous allons installer les paquets SNMP : Snmp et snmpd Sous un système linux : ouvrir une console et taper la commande : `sudo apt-get install snmp snmpd`

Ensuite nous allons éditer le fichier `snmpd.conf` avec la commande :

- `Sudo nano /etc/snmp/snmpd.conf`

Et rentrer les paramètres suivant :

```
#com2sec paranoid default public  
#com2sec readonly default public  
com2sec readwrite default EyesOfNetwork
```

Ici on autorise en lecture et écriture la communauté EyesOfNetwork

Valider les changements (`ctrl+x`, `o`, `entrer`).

Nous allons aussi éditer le fichier `/etc/default/snmpd`

- `Sudo nano /etc/default/snmpd`

Chercher la ligne, et remplacez `127.0.0.1` par l'adresse IP de l'interface réseau utilisée pour communiquer avec le serveur de supervision (généralement l'IP de notre machine).

```
SNMPDOPTS='-Lsd -lf /dev/null -u snmp -l -smux -p /var/run/snmpd.pid 127.0.0.1'
```

Redémarrer le service SNMP

```
sudo /etc/init.d/snmpd restart
```

Pour tester SNMP sur le serveur linux, on rentre la commande :

- snmpwalk -v 2c -c EyesOfNetwork localhost

Pour tester que cela fonctionne du serveur de supervision, on rentre la commande :

- snmpwalk -v 2c -c EyesOfNetwork ip_du_poste_supervisé

b) Installation et paramétrage du SNMP sous Windows

Windows 7 et 8

Aller dans le panneau de configuration>programmes>Activer ou désactiver des fonctionnalités Windows, cocher ensuite la case correspondant au Protocole SNMP, puis cliquer sur ok.

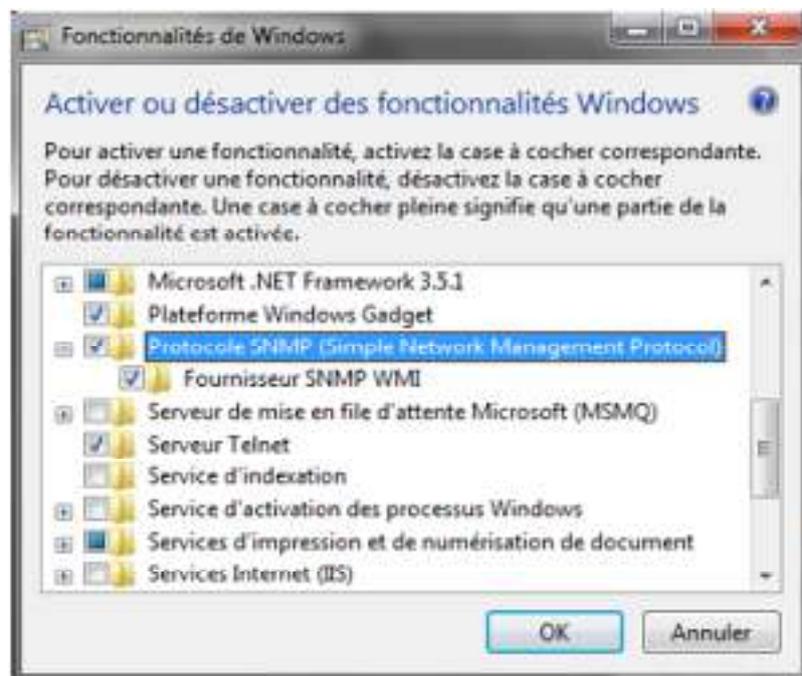


Figure 10 : ajout du SNMP pour Windows 7et 8

Windows XP et Windows server

Aller dans le panneau de configuration>ajout/suppression de programmes>Ajouter/Supprimer des composants Windows. L'Assistant Composants de Windows s'ouvre alors cliquer sur Outils de gestion et d'analyse, puis cliquer sur le bouton Détails.

Sélectionner ensuite le fournisseur SNMP WMI et le protocole SNMP.



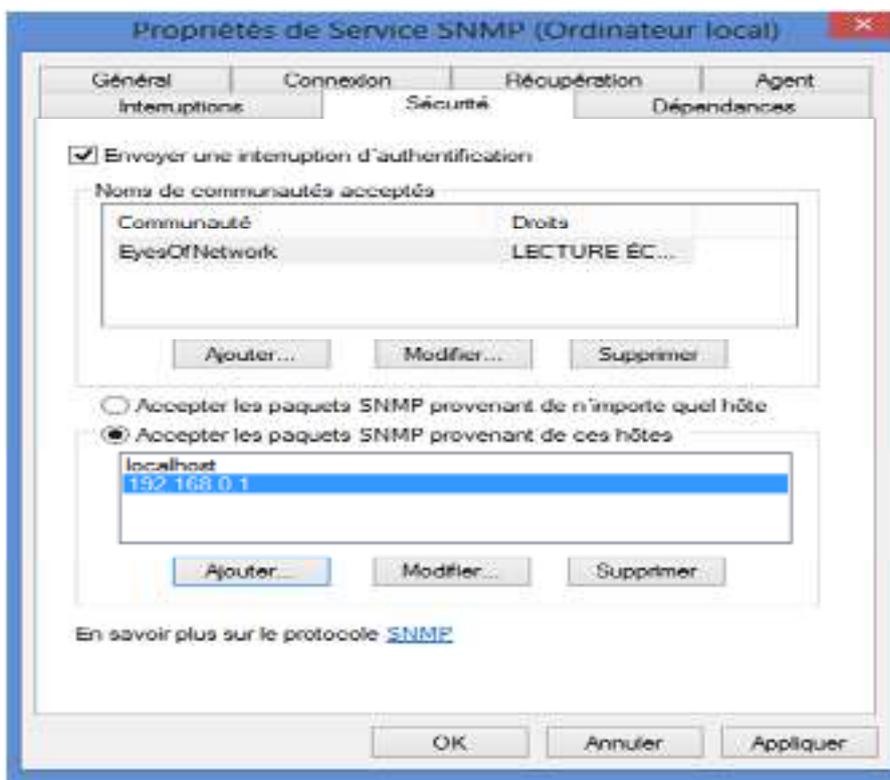
Figure 11 : ajout du SNMP pour Windows Xp et Server

Cliquer sur OK puis Suivant : Windows enregistre les nouveaux composants (le CD-Rom ou le fichier .iso d'installation vous sera éventuellement demandé). Cliquer sur Terminer. Le protocole SNMP est maintenant installé.

Ensuite le paramétrage reste le même sur toutes les plateformes Windows comme décrit ci-dessous. Dans Windows, ouvrir le panneau des services en lançant la commande **services.msc**.

Dans cette fenêtre ouverte, chercher le service SNMP et faire un clic droit/propriété pour accéder à la configuration. Aller dans l'onglet sécurité, ici l'on va renseigner la communauté que possède notre serveur de supervision et lui accorder les droits en lecture et écriture.

Nous allons renseigner l'IP de notre serveur de supervision, ici



supervision et droits en

aussi renseigner l'IP de notre serveur de supervision, ici

Figure 12 : configuration des propriétés du Service SNMP pour Windows

CHAPITRE IV. CONFIGURATION DES SERVEURS

Dans ce chapitre, nous allons citer les étapes de configuration des différents serveurs de façon détaillés et sous un système d'exploitation ubuntu 10.04 LTS à savoir : serveur DHCP, serveur DNS et un serveur http et la sécurisation de ce dernier en https.

NB : il faut installer les serveurs de façon séparé, chaque serveur sur une machine virtuelle, si la machine tombe en panne on perd un seul serveur, et 3 serveurs à la fois si ils sont sur la même machine, donc c'est mieux de les séparés.

Dans notre cas on va installer les serveurs selon les caractéristiques suivantes

| Serveur | Système d'Exploitation de la machine | @IP |
|------------|--------------------------------------|-------------|
| DHCP | Ubuntu 10.04 | 192.168.0.6 |
| DNS | Ubuntu 10.04 | 192.168.0.7 |
| http/https | Ubuntu 10.04 | 192.168.0.8 |

Tableau 3 : informations sur les serveurs à installer

1. Configuration d'un serveur DHCP :

a) Configuration du serveur

le serveur DHCP qui signifie **Dynamic Host Configuration Protocol**. Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau d'obtenir *dynamiquement* (c'est-à-dire sans intervention particulière) sa configuration (principalement, sa configuration réseau). Vous n'avez qu'à spécifier à l'ordinateur de se trouver une adresse IP tout seul par DHCP. Le but principal étant la simplification de l'administration d'un réseau.

Dans les lignes suivant on va bien détailler la configuration de ce serveur sous ubuntu 10.

Mais avant on va attribuer l'@IP 192.168.0.6 à notre serveur en modifiant le fichier /etc/network/interfaces.

Donc pour ce faire on va utiliser le paquet **dhcp3-server** en travaillant avec une console dans laquelle on est logué en root et connecté au internet.

Installation du paquet par la commande

- Apt-get install dhcp3-server

Puis on va modifier le fichier de configuration avec la commande :

- Nano /etc/dhcp3/dhcpd.conf

```

root@ubuntu: /etc/bind
File Edit View Terminal Help
GNU nano 2.2.2 File: /etc/dhcp3/dhcpd.conf Modified
#}

# A slightly different configuration for an internal subnet.
subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.10 192.168.0.20;
    option domain-name-servers 192.168.0.6;
    option domain-name "artisanat.com";
    option routers 192.168.0.1;
    option broadcast-address 192.168.0.255;
    default-lease-time 600;
    max-lease-time 7200;
}

```

Figure 13 : Configuration du serveur DHCP sous linux

On va modifier les lignes entre les accolades :

- La première ligne permet de définir la plage des adresses IP.
- La deuxième donne aux clients l'@IP du serveur DNS (on va détailler l'installation après)
- La ligne suivante donne aux clients le nom du serveur DNS.
- La ligne suivante donne l'adresse de la passerelle par défaut
- Les 2 dernières donnent le délai du bail en secondes. Il est préférable d'augmenter la valeur par défaut pour limiter le trafic sur le réseau.

Une fois la configuration terminée, il faut redémarrer le démon pour prendre en compte les modifications :

➤ /etc/init.d/dhcp3-server restart

On peut donner une adresse fixe pour une machine spécifique en modifiant la partie suivante du fichier dhcpd.conf :

```

#host fantasia {
# hardware ethernet 08:00:07:26:c0:a5;
# fixed-address fantasia.fugue.com;
#}

```

Figure 14 : attribution d'une @IP fixe à une machine avec DHCP

On enlève les # puis on entre l'@ mac du machine et l'@IP souhaité.

b) Configuration des postes clientes :

Pour les machines linux :

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
```

Modification du fichier /etc/network/interfaces comme suit :

Figure 15 : modification du fichier interfaces pour linux

Il ne faut pas oublier de redémarrer le service après la modification

Pour les machines Windows :

Pour la machine Windows c'est plus simple en coche juste « obtenir l'adresse IP automatiquement » dans les propriétés de notre carte.

2. Installation et configuration d'un serveur DNS (Bind9) sur Ubuntu :

a) Pré-requis

Pour installer ce service on doit disposer des choses suivant

- Disposer des droits d'administration sur le serveur : se connecté au terminale en mode root (commande : sudo su)
- Disposer d'un réseau local.
- Connaître les bases de TCP/IP.
- Éventuellement disposer d'une connexion à Internet configurée et activée : on doit juste changer les paramètre de réseau du VMware en cochant NAT à travers cette icône  à droite en bas de la fenêtre.

b) Configuration de la carte réseau :

Avant installer Bind9 il faut définir une adresse IP statique pour notre serveur.

Sous un système Ubuntu: on ouvre une console et on tape la commande :

```
root@ubuntu:~# nano /etc/network/interfaces
```

Ensuite on saisie les paramètres suivants :

```
GNU nano 2.2.2      File: /etc/network/interfaces
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.0.7
netmask 255.255.255.0
network 192.168.0.0
gateway 192.168.0.1
```

Figure 16 : paramétrage de l'interface du serveur DNS

Pour notre cas, on a choisis 192.168.0.7 comme une adresse IP statique associé à notre serveur.

Enfin, on valide les changements (ctrl+x, y, entrer) et on redémarre le service réseau :

```
root@ubuntu:~# /etc/init.d/networking restart
```

c) Installation et configuration de Bind9 :

Pour installer le paquet bind9 il suffit de taper la commande suivante dans une console sous Ubuntu :

```
root@ubuntu:/home/dnsserver# apt-get install bind9
```

D'abord, Dans le fichier **/etc/bind/named.conf.local** nous allons rajouter les informations suivantes :

```
GNU nano 2.2.2      File: named.conf.local

//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "artisanat.com" {
    type master;
    file "/etc/bind/artisanat.com.zone";
};

zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/artisanat.com.rev";
};

[ Read 18 lines ]
^G Get Help      ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text     ^C Cur Pos
^X Exit          ^J Justify     ^W Where Is    ^V Next Page    ^U UnCut Text  ^T To Spell
```

Figure 17 : Configuration du fichier named.conf.local

Ces informations vont créer le domaine artisanat.com, la zone est de type master (c'est-à-dire maitre).

Ensuite, on se place dans le répertoire /etc/bind :

```
root@ubuntu:/home/dnsserver# cd /etc/bind
root@ubuntu:/etc/bind#
```

Puis, on crée les deux fichiers artisanat.com.zone et artisanat.com.rev :

```
root@ubuntu:/etc/bind# touch artisanat.com.zone artisanat.com.rev
```

D'abord on commence par la configuration du fichier de la zone directe artisanat.com.zone :

```
root@ubuntu:/etc/bind# nano artisanat.com.zone
```

Ce fichier doit être rempli par les informations suivantes :

NB : dnsserver est le nom de notre serveur.

```

root@ubuntu: /etc/bind
File Edit View Terminal Help
GNU nano 2.2.2 File: artisanat.com.zone Modified
$TTL      604800
@         IN      SOA      dnsserver.artisanat.com. root.artisanat.com. (
                        42          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@         IN      NS       dnsserver.artisanat.com.
dnsserver IN      A         192.168.0.7
eon       IN      A         192.168.0.1

```

Figure 18 : Configuration du fichier artisanat.com.zone

Le « @ » spécifie la zone définie dans le fichier configuration

Ensuite « IN » précise qu'il s'agit d'une zone Internet, il s'agit « presque » de la valeur par défaut. Ensuite on précise le mot clé SOA suivi du FQDN du serveur qui héberge la zone (dnserver.artisanat.com.).

NB: Les « . » à la fin de dnserver.artisanat.com. et root.artisanat.com. sont obligatoires .

Ensuite il faut définir les éléments suivant :

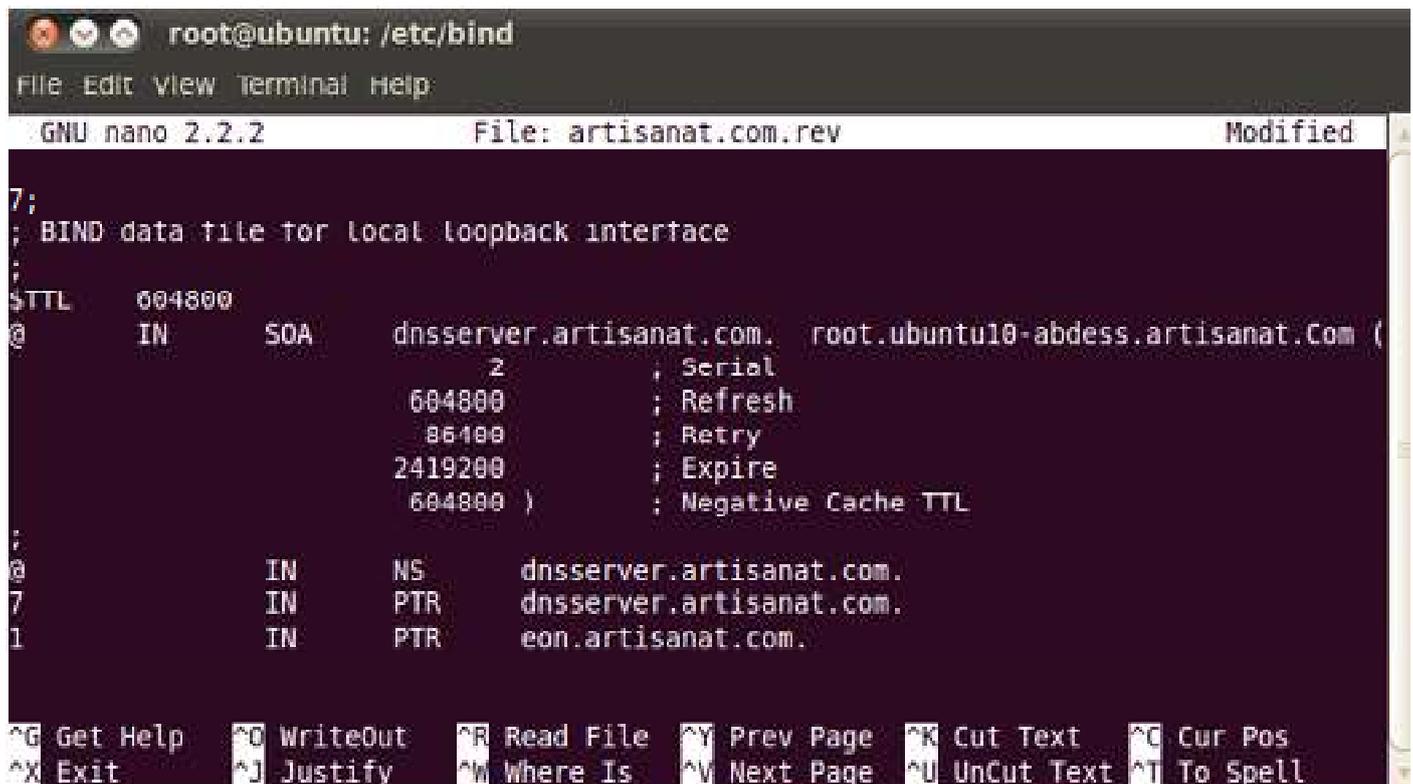
- Le numéro de série (serial), généralement la date du jour suivi d'un incrément : YYYYMMDDxx.
- Le temps de rafraichissement (refresh), ici 604800 seconds.
- Le temps entre deux essais (retry), ici 86400 secondes.
- Le temps d'expiration (expire) ici 2419200 secondes.
- La valeur TTL minimum (minimum TTL), ici, 604800 seconds.

Toutes les valeurs de temps sont précisées en secondes ... Je vous rassure, ce n'est pas obligatoire. Ensuite nous avons la définition des machines de notre réseau .Chaque ligne Précise : le nom du pc – le type de zone – le type d'enregistrement – l'adresse IP de la machine le type d'enregistrement A (A pour Alias) permet donc de pointer, par exemple, eon sur l'adresse IP 192.168.0.1).

Ensuite, on configure le fichier de la zone inversé artisanat.com.rev :

```
root@ubuntu:/etc/bind# nano artisanat.com.rev
```

Comme dans la partie précédente nous remplissons ce fichier par les informations suivantes :



```

7;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA     dnserver.artisanat.com.  root.ubuntu10-abdess.artisanat.Com (
;
; Serial
; Refresh
; Retry
; Expire
; Negative Cache TTL
;
@         IN      NS      dnserver.artisanat.com.
7         IN      PTR     dnserver.artisanat.com.
1         IN      PTR     eon.artisanat.com.

```

Figure 19 : modification du fichier artisanat.com.rev

On remarque que le fichier de la zone inversé ressemble presque à celui de la zone directe à l'exception de certain changement :

Les lignes commencent par un nombre, en fait ce nombre est la fin de l'adresse IP de la machine ... C'est en fait ce qu'il y a après : 192.168.0., notre serveur eyesofnetwork par exemple à l'adresse IP 192.168.0.1 alors on a mis 1 en face de son FQDN.

Le type d'enregistrement est PTR.

Puis, il faut éditer le fichier resolv.conf :

```
root@ubuntu:/etc/bind# nano /etc/resolv.conf
```

On renseigne le comme suit :

```

root@ubuntu:/etc/bind
File Edit View Terminal Help
GNU nano 2.2.2 File: /etc/resolv.conf Modified
nameserver 192.168.0.7
search artisanat.com
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

```

Figure 20 : configuration du fichier resolv.conf

Enfin, on redémarre le service Bind9 par /etc/init.d/bind9 restart

d) Test de fonctionnement

Pour tester le bon fonctionnement de notre configuration on utilise la commande nslookup : qui permet d'interroger un serveur de nom :

```

root@ubuntu:/etc/bind# nslookup
> 192.168.0.7
Server:          192.168.0.7
Address:         192.168.0.7#53

4.0.168.192.in-addr.arpa      name = dnserver.artisanat.com.
> eon.artisanat.com
Server:          192.168.0.7
Address:         192.168.0.7#53

Name:   eon.artisanat.com
Address: 192.168.0.1
>

```

Figure 21 : test de fonctionnement de serveur DNS

3. Configuration d'un serveur web

a) Configuration du serveur http (apache2) :

Mais avant on va attribuer l'@IP 192.168.0.6 à notre serveur en modifiant le fichier /etc/network/interfaces, puis nous allons installer le service apache avec la commande suivante :

➤ sudo apt-get install apache2

Maintenant, entrez votre mot de passe. Lorsque demandé, on entre «Y» pour oui. Une fois installé, on peut ouvrir le Navigateur Web et saisir l'adresse http: // localhost / dans la barre d'adresse pour tester, nous devrions être capable de voir une page affichant "ça marche!"

Maintenant, on va installer geany, Il suffit de taper:

➤ sudo apt-get install geany

Geany est une version simple d'un programme de création de site web. Sur votre bureau créez un dossier nommé monsite. Et dans le dossier on va créer un document vide appelé monsite.html. Faites un clic droit monsite.html et l'ouvrir dans Geany.

Nous allons créer un simple fichier HTML en ajoutant du code à l'aide de l'indice Geany. On tape le code suivant pour créer un site de démonstration :

```
<html>
<head>
  <nav>
    <hr size="8" width="800" noshade="noshade">
    <hr size="8" width="800" noshade="noshade">
    <h1><center>soyez les bienvenus dans l'espace <h1><i> mon site</i></h1></center></h1>
    <hr size="8" width="800" noshade="noshade">
    <hr size="8" width="1000" noshade="noshade">
  </nav>
</head>
<title>
  .: mo site :.
</title>
<body>
  <center>
    <h1>
      IDRISSI Abdessamad / OUDRISS SAID
    </h1>
  </center>
  <footer>
    <center>
      <hr size="8" width="1000" noshade="noshade">
      <h6>Copyright OUDRISS-IDRISSI Tous droits réservés</h6>
    </center>
  </footer>
</body>
</html>
```

Ensuite, on tape :

- cp-R de bureau /monsite/var/www/

Puis :

- chmod-R 777 /var/www/monsite/

et enfin:

- cd /etc/apache2/

Maintenant, on tape la commande ls et nous devrions être en mesure d'afficher un fichier appelé ports.conf. on ouvre ce dernier dans nano afin que nous puissions modifier ce fichier. Il suffit de taper nano ports.conf.

Maintenant, nous allons placer un signe # devant le

NameVirtualHost *: 80 de sorte que apache2 n'écouteront pas à cela et on clique sur CTRL + X, puis sur le bouton Y et ENTER pour sauvegarder les modifications. Maintenant, retournez au terminal et tapez la commande suivante pour aller dans le répertoire des sites-available.

- cd sites-available/

puis on modifie le fichier monsite avec la commande suivante:

- nano monsite

Cela va créer un fichier vide dans le répertoire des sites-available. Il sera vide de contenu maintenant tapez dans ces commandes les ligne suivant :

```
NameVirtualHost *:80
<VirtualHost *:80>
    ServerName monsite.com
    ServerAlias www.monsite.com
    DocumentRoot /var/www/monsite
</VirtualHost>
```

Puis on sauvegarde le fichier. Nous sommes presque compléter la mise en place du premier hôte virtuel. Maintenant, dans le terminal on tape la commande suivante afin que nous puissions modifier l'hosts dans le répertoire etc utilisant nano.

- nano /etc/hosts

Puis on ajoute une ligne comme suit :

```
192.168.0.8 artisanat.com ubuntu-http monsite.com www.monsite.com
```

Avec 192.16.0.8 et artisanat.com son respectivement l'@ IP du serveur http et le nom du domaine du serveur DNS.

NB : la modification de ce fichier hots ce fait au niveau de toutes les machines cliente Windows ou linux

Si on veut ajouter un second site, exemple : monsite2, la première ligne devrait ressembler à ceci:

```
192.168.0.8 artisanat.com ubuntu-http monsite.com www.monsite.com monsite2.com www.monsite2.com
```

On enregistre le fichier hosts. Maintenant, nous pouvons activer le site nous venons de créer en tapant dans le terminal:

```
> a2ensite monsite
```

Un message viendra dire pour exécuter 'reload /etc/init.d/apache2' pour activer le nouveau place. Donc, nous allons taper cette dernière commande dans le terminal.

Maintenant, nous pouvons aller dans notre navigateur et tapez www.monsite.com et il apparaîtra.



Figure 22 : connexion au serveur http

b) Sécurisation du serveur apache2 par SSL

b.1 Introduction

SSL est un protocole qui a été développé par la société Netscape.

Ce protocole permet à deux machines de communiquer de manière sécurisée. Les informations échangées entre les deux machines sont de ce fait inviolables.

Le protocole SSL se traduit par la combinaison de deux protocoles bien distincts (*Handshake* et *Record*) qui permettent la négociation entre les deux machines et le chiffrement des données échangées.

b.2 Les certificats

Un certificat permet de fournir diverses informations concernant l'identité de son détenteur (la personne qui publie les données). Ce certificat s'accompagne d'une **clé publique** qui est indispensable pour que la communication entre les machines soit chiffrée.

De même, afin de garantir l'authenticité du certificat, ce dernier est signé numériquement par le biais d'une **clé privée** provenant soit d'un organisme officiel (Société spécialisée dans la certification) soit par le détenteur du Certificat lui-même. Dans ce dernier cas, on parlera de certificat auto-signé.

Dans la plupart des cas, l'obtention d'un Certificat certifié par une autorité officielle ayant un prix assez élevé, les webmasters auront tendance à vouloir signer eux-mêmes leur certificat. Ce faisant, il est à noter que dans ce cas, le certificat ne sera pas reconnu par les navigateurs web comme étant certifié.

CA Cert permet d'obtenir des certificats gratuits. Il vous faudra néanmoins installer le certificat racine dans votre navigateur.

Dans les lignes suivantes on va bien détailler la procédure présentée explique la marche à suivre pour mettre en place un **Site Web sécurisé via protocole SSL en utilisant un Certificat auto-signé**.

Nous avons déjà mis en place un hôte virtuel basé sur le nom **monsite.com**, ce dernier étant accessible sur le **port 80** à l'adresse <http://monsite.com>

La création de notre premier serveur virtuel en utilisant apache2 est terminée. Pour créer un deuxième serveur virtuel suffit de suivre ces instructions de la même façon.

b.3 Activation du protocole SSL

Pour que le protocole SSL puisse fonctionner avec le Serveur HTTP Apache2, il faut activer le module **ssl** avec la commande :

➤ `sudo a2enmod ssl`

puis recharger la configuration d'Apache2 faites :

➤ `sudo service apache2 force-reload`

Ou si vous êtes sur une ancienne version

➤ `sudo /etc/init.d/apache2 force-reloadn d'Ubuntu :`

b.4 Création du certificat

On peut créer son certificat SSL auto signé en installant le paquet openssl. Il est aussi possible d'installer ca-certificates, mais ça ne semble pas utile dans le cas d'un certificat auto-signé.

On commence par

- `sudo openssl req -x509 -nodes -days 365 -newkey rsa:1024 -out /etc/apache2/server.crt -keyout /etc/apache2/server.key`

■ **Explications :**

- -x509 -nodes donne le type de certificat voulu
- -days 365 indique la durée de validité (en jours) de votre certificat
- -newkey rsa:1024 demande une clé RSA de 1024 bits - d'après la doc apache, il est déconseillé de créer une clé plus grosse pour des histoires de compatibilité
- -out /etc/apache2/server.crt est le chemin de votre certificat
- -keyout /etc/apache2/server.key est le chemin de la clé privée

Répondez alors aux questions posées :

■ **Country Name (2 letter code) :**

Entrez MA si vous êtes situé en Maroc et validez par la touche « Entrée »

■ **State or Province Name (full name) [Some-State]:**

Entrez MAROC et validez par la touche « Entrée »

■ **Locality Name (eg, city) []:**

Indiquez ici le nom de votre ville. (exemple : Rabat) et validez par la touche « Entrée »

■ **Organization Name (eg, company; recommended) []:**

Indiquez le nom de votre organisation, de votre société. (exemple : MAESS) et validez par la touche « Entrée ».

■ **Organizational Unit Name (eg, section) []:**

Indiquez ici le nom de la section de votre organisation, de votre société. Si vous n'en avez pas, mettez la même chose que pour la question précédente.

■ **Common Name (eg, YOUR name) []:**

Ici, il convient de faire particulièrement attention à ce que vous allez entrer. Vous devez indiquer le nom de domaine que vous désirez sécuriser. En ce qui nous concerne, il s'agit du domaine : monsite.com Nous indiquons donc monsite.com et nous validons par la touche « Entrée ».

■ **Email Address []:**

Ici, il s'agit d'indiquer l'adresse E-mail de l'administrateur.

Enfin, on empêche les curieux de lire notre clé privée :

- `sudo chmod o-rw /etc/apache2/server.key`

b.5 Configuration d'Apache2

Par défaut, Apache2 est configuré pour écouter sur le port 80. Il s'agit là de la configuration usuelle d'un Serveur Web. Cependant, le protocole SSL a besoin d'un port spécifique pour pouvoir fonctionner. Il s'agit du port 443.

Nous allons donc rajouter une directive de configuration nommée « Listen » qui permettra d'indiquer à Apache2 qu'il doit aussi écouter sur le port 443.

Pour ce faire, éditez le fichier `/etc/apache2/ports.conf` et rajoutez la ligne suivante : `Listen 443`

b.6 Création du fichier de configuration

Ayant déjà configuré notre hôte virtuel `nuxwin.com`, un fichier de configuration nommé `monsie` doit exister dans le répertoire `/etc/apache2/sites-available`.

Voir ci-dessous le contenu de ce fichier, Il s'agit ici du contenu minimal d'un virtualhost.

Et pour sécuriser cet Hôte Virtuel, nous allons donc devoir modifier ce fichier en y ajoutant un hôte virtuel accessible sur le port 443, ce dernier contenant des directives particulières qui sont les suivantes :

■ Directive `SSLEngine` :

Cette directive permet d'activer le moteur SSL au sein d'un hôte virtuel, Elle peut prendre deux arguments → `on/off`

■ Directive `SSLCertificateFile` :

Cette directive définit le certificat authentifiant le Serveur auprès des clients. L'argument est le chemin d'accès au certificat. En ce qui nous concerne, le certificat se trouve dans le répertoire `/etc/apache2/`

■ Directive `SSLCertificateKeyFile` :

Cette directive définit la clé privée du Serveur utilisée pour signer l'échange de clé entre le client et le serveur. Elle prend en argument le chemin d'accès à la clé (fichier). Dans notre cas, la clé se trouve dans le répertoire `/etc/apache2/`.

Par ailleurs, comme nous l'avons déjà fait pour notre hôte virtuel accessible sur le port 80, nous allons devoir rajouter une directive `NameVirtualHost` qui permettra que l'adresse nommée par le nom de notre hôte virtuel accessible sur le port 443 soit résolue correctement. Nous rajouterons donc cette directive (`NameVirtualHost *:443`) au début de notre fichier de configuration.

Enfin, afin que les clients puissent continuer d'accéder au site Web en tapant une url de type `http` et non `https`, nous allons modifier l'hôte virtuel accessible sur le port 80 en remplaçant la directive `DocumentRoot` par une directive de redirection.

Voici donc le contenu de notre fichier une fois modifié :

```
NameVirtualHost *:443
<VirtualHost *:80>
  ServerName monsite.com/
  Redirect / https://monsite.com/
</VirtualHost>
<VirtualHost *:443>
  ServerName monsite.com
  DocumentRoot /var/www/monsite.com
  SSLEngine on
  SSLCertificateFile /etc/apache2/server.crt
  SSLCertificateKeyFile /etc/apache2/server.key
</VirtualHost>
```

Relance du serveur HTTP Apache2

Afin que les modifications que nous venons d'effectuer soient prises en compte, nous devons demander au Serveur Http Apache2 de relire ses fichiers de configuration.

Pour ce faire, il suffit de taper la commande suivante dans un terminal :

➤ `sudo /etc/init.d/apache2 reload`

Normalement, si tout s'est bien passé, vous devriez désormais avoir accès à votre site Web de manière sécurisée.

Mais avant il faut ajouter le certificat créer dans les certificats du navigateur dans ses paramètre et voila notre serveur web est sécuriser.

CHAPITRE V. AJOUT DES SERVICES DE SUPERVISION A L'EON

Dans ce présent chapitre, nous allons expliquer les démarches à suivre pour ajouter les services : les hôtes, les serveurs DHCP,DNS etc ... au serveur EON, pour pouvoir superviser leur états.

1. Connexion au serveur

Une fois on a connecter toutes les machine du réseau on lance un navigateur puis on tape l'@ 192.168.0.1 du serveur DNS pour pouvoir se connecter au page web de configuration de l'EON (l'identifiant et le mot de passe par défaut sont **admin** et **admin**) :



Figure 23 : connexion au serveur EON par un navigateur web

2. Scan du réseau

Pour pouvoir scanner le réseau, il faut se connecter sur l'interface web d'EON.

Lilac va nous permettre de découvrir automatiquement le réseau car il s'appuie sur le logiciel Nmap qui est un scanner de port.

Dans **Administration** -> **Nagios** --> **configuration** ; cliquez sur « Tools » puis « Auto Discovery »

Ensuite dans la fenêtre suivante nous allons remplir les champs suivant :

Figure 24 : ajout d'un job pour le scan du réseau

- Job name : nom du travail
- Job description : description du travail
- Nmap binary location : emplacement de l'exécutable Nmap (laisser par défaut)
- Target spécification : adresse que l'on souhaite superviser,
- exemple : 192.168.0.x/32 ou 192.168.10.x-x/32

Cliquez ensuite sur « add target » puis sur « Begin auto-discovery job »

Le processus démarre, il faut maintenant attendre la fin du processus pour pouvoir exporter les hôtes dans Nagios.

3. Superviser un hôte :

Dans Administration/nagios/configuration , cliquez sur « Network » puis « add a new child host »

Remplissez ensuite les champs suivants :

- Host Name : Nom de l'hôte (ne doit pas contenir d'espace)
- Host Description : Description de l'hôte
- Address : adresse ip, nom d'hôte ou adresse internet

Cliquez sur « Add host » et la fenêtre suivante apparaît.



Figure 25 : page d' information sur l'hôte ajouté

Dans cette fenêtre, cliquez sur « Inheritance » pour choisir un template à associer à l'hôte exemple : printer, Windows, linux, etc... selon le type du hôte à superviser.

Une fois le Template sélectionné, cliquez sur « Add Template » Nagios recherchera alors les checks qui sont personnalisés pour le template en question.

Dans Lilac, cliquez ensuite sur « Tools » puis sur « Exporter » Et enfin sur « Restart » pour pouvoir charger la configuration de Lilac dans Nagios.

Ce redémarrage du Job « scan réseau » qu'on a créé se fait après les modifications pour pouvoir les charger vers nagios.

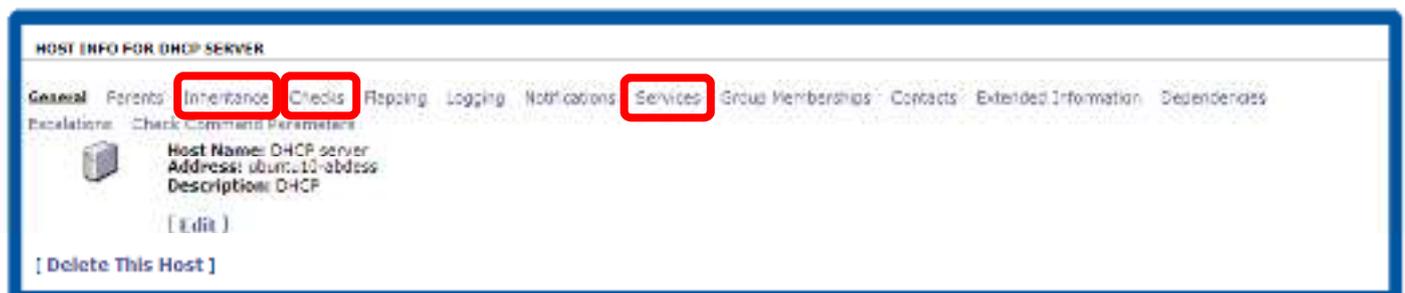
NB : on suit la même procédure pour ajouter toute les machines à superviser mais il ne faut pas oublier de redémarrer le job pour que nagios puisse prendre les modifications en considération.

4. Ajout d'une commande de supervision (services)

Pour des templates précise, EON ajoute par des défaut des services (ex : mémoire, partition, CPU ...), on peut ajouter d'autre selon notre besoin.

En ce qui nous concerne on va ajouter des services pour superviser l'états de nos serveur.

Après avoir ajouté trois hote només DHCP Server, DNS Server et HTTP Server, avec des templates :



Generic_Host on va ajouter un service pour chacune.

Figure 26 : Page de configutration d'un service

Dans cette page qui apparait juste après la création du hôte ou en cliquant sur Administration->Ngios ->configuration->network-> DHCP Server, on clique sur **services** puis **Create A New Service For This Host**

Puis on remplit ces deux champs

- **Service Description** : description du service à ajouter c'est obligatoire
- **Display Name: (Optional)** : c'est optionnel

Puis **add service**, mais on doit aussi choisir le template **Generic_Service** pour ce service en cliquant sur **inheritance** et en choisissant ce dernier. Maintenant le service est créé mais on doit ajouter la commande correspondante, et pour se faire il faut cliquer sur **Checks->editer**, puis cocher **Provide value** ensuite choisir **dhcp_status** et enfin valider par **update checks**

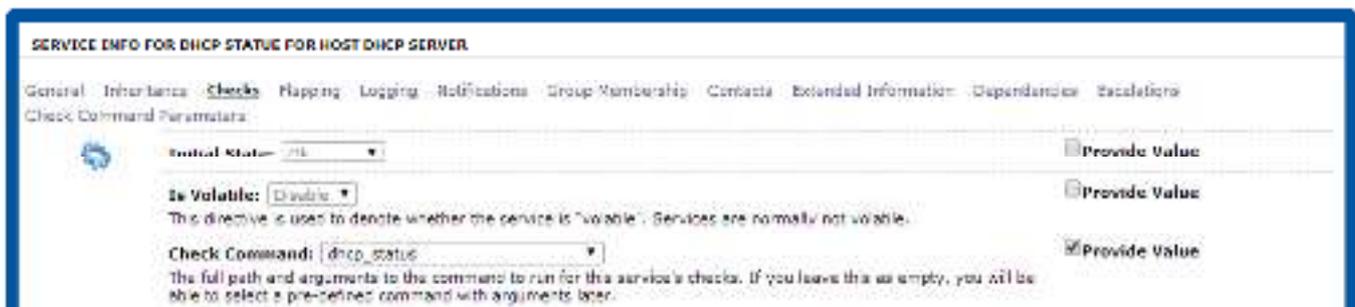


Figure 27 : ajout du service dhcp_status

On suit la même démarche pour les deux autres serveurs DNS Server et HTTP Server sauf que pour **check commande** on choisit respectivement **dns_status** et **http**.

5. Superviser d'autres entités :

Suivez la procédure nommée : « Superviser un hôte », puis choisissez le Template :

- Printer : pour une imprimante
- Generic_Host : pour les actifs (ex : Serveur DNS, DHCP ...)
- Cisco : pour un équipement cisco
- Etc

Pour notre cas on va utiliser juste Generic_Host pour la supervision des Serveurs DHCP, DNS et HTTP en créant un hôte mais en choisissant la template Generic_Host on va aussi ajouter une commande spécifique pour chaque serveur, la procédure bien détaillée et dans la partie suivante.

6. Vue des équipements et des services

On a bien configuré notre machine donc on doit passer à la visualisation des équipements et des services, et pour ce faire on clique sur **Disponibilité/événement->vue équipements**

Current Network Status
 Last Updated: Thu Aug 28 18:11:21 WEST 2014
 Updated every 90 seconds
 Thrift 1.34 - www.thrifting.com
 Logged in as admin

Host Status Totals

| Up | Down | Unreachable | Pending |
|---------------------|------|------------------|---------|
| 6 | 1 | 0 | 0 |
| All Problems | | All Types | |
| 1 | | 1 | |

Service Status Totals

| Ok | Warning | Unknown | Critical | Pending |
|---------------------|---------|------------------|----------|---------|
| 11 | 0 | 15 | 1 | 0 |
| All Problems | | All Types | | |
| 16 | | 21 | | |

- View Service Status Detail For All Host Groups
- View Status Overview For All Host Groups
- View Status Summary For All Host Groups
- View Status Grid For All Host Groups

Host Status Details For All Host Groups

select host with leftclick to send multiple commands. Select multiple with shift + mouse.
 select all + inspect all + all problems + all with down time.

| Host | Status | Last Check | Duration | Status Information |
|-------------|--------|------------|----------------|---|
| DNS server | UP | 18:09:42 | 04:0h 1m 12s | PING OK - Packet loss = 0%, RTA = 807.15 ms |
| W3 server | UP | 18:10:29 | 04:0h 1m 2s | PING OK - Packet loss = 0%, RTA = 14.05 ms |
| ftp Server | UP | 18:09:49 | 04:0h 1m 0s | PING OK - Packet loss = 0%, RTA = 3.38 ms |
| localhost | UP | 18:10:29 | 04:11h 47m 56s | PING OK - Packet loss = 0%, RTA = 3.05 ms |
| ubuntu-dns | DOWN | 18:11:01 | 04:11h 49m 32s | CRITICAL - Host Unreachable (ubuntu) |
| windows6 | UP | 18:10:59 | 04:11h 47m 56s | PING OK - Packet loss = 0%, RTA = 3.34 ms |
| ubuntu-dns2 | UP | 18:10:52 | 04:0h 1m 28s | PING OK - Packet loss = 0%, RTA = 1.13 ms |

Figure 28 : vue des équipements

On peut remarquer que l'EON nous affiche l'état de tous les équipements qu'on a ajouté (UP : pour ceux qui sont allumés et DOWN pour les autres qui sont inactifs), cette page a une durée d'actualisation automatique qui vaut 90 secondes mais ça reste modifiable.

En haut de cette page EON affiche aussi des petits tableaux statistiques pour les hôtes et les services en indiquant le nombre et le niveau de criticité de chacun.

Et pour visualiser les services on choisit **Disponibilité/événement->vue services**

| Host | Service | Status | Last Check | Duration | Attempt | Status Information |
|----------------|-------------|----------|------------|---------------|---------|---|
| DHCP server | dhcp status | OK | 18:43:31 | 0d 0h 22m 49s | 1/4 | OK: Received 1 DHCPREQUEST(s), 1 of 1 requested servers responded, max lease time = 600 sec. |
| DNS server | dns status | OK | 18:46:02 | 0d 0h 22m 49s | 1/4 | DNS OK: 1.093 seconds response time, 192.168.0.1 returns ubuntu 16-address artisanat.com |
| http Server | http | OK | 18:46:53 | 0d 0h 22m 49s | 1/4 | HTTP OK: HTTP/1.1 200 OK - 453 bytes in 0.004 second response time |
| localhost | memory | OK | 18:47:03 | 0d 0h 22m 49s | 1/4 | Ram: 78% Swap: 8% : OK |
| | rrvd | OK | 18:46:54 | 0d 0h 22m 49s | 1/4 | Uptime: 110431 Threads: 3 Questions: 127039 Slow queries: 0 Opens: 2742 Flush tables: 1 Open tables: 64 Queries per second avg: 1.150 |
| | partitions | OK | 18:46:05 | 0d 0h 22m 49s | 1/4 | All selected storages (<90%): OK |
| | processes | OK | 18:44:23 | 0d 0h 22m 49s | 1/4 | 1 process named ssh (> 3): |
| | processor | OK | 18:46:18 | 0d 0h 22m 49s | 1/4 | CPU used 8.0% (<80): OK |
| | ssh | OK | 18:46:19 | 0d 0h 22m 49s | 1/4 | SSH OK - OpenSSH_4.3 (protocol 2.0) |
| | system | OK | 18:46:10 | 0d 0h 22m 49s | 1/4 | System time OK - 08-25-2014, 18:46:18 |
| | uptime | OK | 18:46:41 | 0d 0h 22m 49s | 1/4 | OK: Systemuptime 1 day, 6:42:22.99 |
| Ubuntu-12.04 | memory | UNKNOWN | 18:46:07 | 0d 0h 21m 06s | 4/4 | ERROR: rrdtool: No response from remote host 'ubuntu'. |
| | partitions | UNKNOWN | 18:44:37 | 0d 0h 22m 49s | 4/4 | ERROR: General time-out (Alarm signal) |
| | processor | UNKNOWN | 18:44:33 | 0d 0h 22m 49s | 4/4 | ERROR: Description table: No response from remote host 'ubuntu'. |
| | system | UNKNOWN | 18:46:23 | 0d 0h 22m 49s | 4/4 | Timeout: No Response from ubuntu |
| | uptime | UNKNOWN | 18:46:59 | 0d 0h 22m 49s | 4/4 | |
| | users | OK | 18:46:01 | 0d 0h 21m 34s | 1/4 | Users OK - 1 users currently logged in |
| Windows8 | memory | WARNING | 18:46:38 | 0d 0h 22m 10s | 4/4 | Virtual Memory: 66%used(3600MB/5073MB) Physical Memory: 86%used(2404MB/2771MB) (>80%) WARNING |
| | partitions | WARNING | 18:44:31 | 0d 0h 22m 15s | 4/4 | C:\Local: SerialNumber e24c742: 94%used(10208MB/10730MB) (>90%) WARNING |
| | processor | OK | 18:44:32 | 0d 0h 22m 49s | 1/4 | 2 CPUs, average load 7.5% < 80% : OK |
| | system | CRITICAL | 18:44:55 | 0d 0h 21m 48s | 4/4 | CRITICAL - System time is off by 328227 sec (08-01-2014, 13:55:22) |
| | uptime | OK | 18:46:33 | 0d 0h 22m 49s | 1/4 | OK: Systemuptime 15:27:34.73 |
| Xp1-Abdessamad | memory | OK | 18:46:11 | 0d 0h 22m 28s | 1/4 | Physical Memory: 55%used(1108/2018) Virtual Memory: 11%used(111MB/1011MB) (<80%) : OK |
| | partitions | OK | 18:44:07 | 0d 0h 22m 49s | 1/4 | All selected storages (<90%): OK |
| | processor | OK | 18:45:37 | 0d 0h 22m 28s | 1/4 | 1 CPU, load 0.0% < 80% : OK |
| | system | CRITICAL | 18:46:17 | 0d 0h 22m 28s | 4/4 | CRITICAL - System time is off by 328223 sec (08-01-2014, 13:55:45) |
| | uptime | OK | 18:44:16 | 0d 0h 22m 49s | 1/4 | OK: Systemuptime 7 days, 3:37:41.25 |

Figure 29 : Vue de services

Commentaire :

on remarque que l'EON affiche l'états de criticité des différent service du machine

ex :

- pour la machine windows8, 80 % de la mémoire et 94 % de disque son utilisés ces informations permet au administrateur de mettre en place des actions correctif en vue d'éviter une panne.
- Tous les serveurs sont en bonne états

NB :

EON offre la possibilité d'ajouter d'autre service selon notre besoin, il suffit juste de les ajouter en suivant la partie 4. **Ajout d'une commande de supervision (services)** au-dessus.

Ex :

- Nombre d'adresse IP utilisé pour DHCP
- Nombre d'utilisateur connecté sur une machine
- etc

CONCLUSION

Quel que soit la qualité des dispositifs de sécurité ne peuvent pas protéger de façon optimale un réseau s'il n'est pas correctement supervisé.

En effet, la sécurité d'un système informatique ne se résume pas qu'au piratage. Elle correspond à un vaste domaine qui englobe beaucoup de notions.

Ainsi, la sécurité d'un réseau repose d'une part sur l'architecture et son adéquation aux besoins des composants qui le constituent, mais aussi sur l'administration et la supervision, continue et efficace de ces équipements.

La supervision des réseaux, doit prendre une part très importante au sein de l'administration d'un parc informatique, il aide à anticiper les pannes et réagir rapidement tout en donnant une meilleure disponibilité et une meilleure qualité de service.

La supervision vous permet aussi dans un temps différé d'avoir une vision synthétique de la vie de votre parc informatique car elle vous permettra par exemple de mieux calibrer vos lignes ou au contraire restreindre l'utilisation de celles-ci lorsqu'elles sont polluées.

La supervision c'est sans contestation le plus qui vous permettra de vous distinguer des autres. Aujourd'hui, ce n'est plus un luxe mais une nécessité dans cette guerre à la disponibilité et de la sécurité informatique.

Au terme de ce projet, on a eu la satisfaction de bien apprendre un outil géant de la supervision ainsi que sa configuration et son fonctionnement.

Mais plus que cette satisfaction, on a eu le plaisir de travailler dans un domaine passionnant qui est la Supervision des Réseaux informatiques.

En effet, ce stage nous a permis non seulement d'approfondir nos connaissances en Supervision des réseaux informatiques mais aussi d'acquérir une expérience extrêmement valorisante dans la mesure où il reflète parfaitement un domaine passionnant et intéressant.

On estime être heureux d'avoir pu effectuer ce travail, de développer la notion de travail en équipes, la méthode de conception d'un projet et la procédure pour atteindre le but fixé par notre encadrante, ainsi que la création des solutions face aux différents obstacles rencontrés tel que les contraintes de temps et la gestion de travail demandé dans le but de finaliser un projet correcte, conforme au cahier de charge est à la hauteur des attentes de notre encadrante Mme LEHLALI Souad qu'on tient à le remercier chaleureusement pour tous ces efforts fournis durant toutes les étapes de la réalisation de notre stage.

WEBOGRAPHIE

<http://www.eyesofnetwork.com/eonrepo/FR%20-%20Eon%20v4%20Installation.pdf>

<http://www.eyesofnetwork.com/eonrepo/FR%20-%20Eon%20v4%20Configuration.pdf>

<http://www.eyesofnetwork.com/eonrepo/FR%20-%20Eon%20v4%20Utilisation.pdf>

http://home.ite.sfcollege.edu/~daniel.m.eakins/media/LAMP_HOW_TO.pdf

<http://www.reseaucerta.org/sites/default/files/coteLaboGSBEon.pdf>

www.artesnet.gov.ma

www.wikipédia.com

www.commetcamarche.com

<http://doc.ubuntu-fr.org/>

www.youtube.com

www.slideshare.net