

# Projet sur la continuité de service et la qualité de service

## Table des matières

Projet sur la continuité de service et la qualité de service .....	1
Objectifs : .....	3
Prérequis : .....	3
Introduction à l'infogérance : .....	4
Expressions de besoins : .....	5
Les différents outils à notre disposition : .....	6
➤ ITOP : Service de Management .....	6
➤ POM/Nagios : Outil de Supervision .....	6
➤ La CMDB .....	6
➤ Description ITSM .....	7
➤ Witbe .....	7
➤ Osianoo : outils de gestion des taches : .....	8
➤ Les différentes documentations mis en place : .....	8
Les différents outils pour la sécurité : .....	8
➤ Outil de gestion des mots de passes : .....	8
➤ Outil de gestion des traces : .....	9
➤ WAB la suite logicielle de Wallix : .....	10
➤ Outil de journalisation : .....	10
➤ LE VPN : .....	12
Éléments appris durant les visites afin d'en apprendre plus sur leur métier : .....	12
Compréhension de la coexistence de l'ensemble des outils utilisé dans le DMS : .....	13
Récapitulatif de l'entretien avec la service réseau : .....	14
Compte rendu des entretiens : .....	15
Résolution des expressions de besoins : .....	16
Solution de documentation et d'indexation : .....	16
Solution de gestion d'IP : .....	17
Installation des IPAMs sur une VM Debian .....	18
Installation de PHPIPAM : .....	23
Installation de TeemIP : .....	30

## Objectifs :

Dans ce projet, nous allons faire en sorte que la continuité de service et la qualité de service se fassent à travers les différentes couches et les différents pôles de services. Afin de permettre à la couche Réseaux d'être plus industrialisé.

## Prérequis :

- Afin de comprendre au mieux le projet et l'environnement de la société voici quelques définitions :
  - **Proxy :**
    - Un proxy est un programme **servant d'intermédiaire** pour accéder à un autre réseau, généralement internet. Par extension, on appelle aussi « proxy » un matériel comme un serveur mis en place pour **assurer le fonctionnement** de tels services.
  - **Pare-feu(Firewall) :**
    - Logiciel et ou matériel permettant de **faire respecter la politique de sécurité** du réseau, permettant **d'autoriser sur le réseau informatiques les types de communications** choisit.
  - **Le LoadBalancer (Répartiteur de charge) :**
    - Ensemble de techniques permettant de **distribuer une charge de travail entre différents ordinateurs d'un groupe.**
      - Permet de répondre à une **charge trop importante d'un service** en la répartissant sur plusieurs serveurs et de **réduire l'indisponibilité potentielle de ce service** que pourrait provoquer la panne logicielle ou matérielle d'un unique serveur.
  - **SNMP :**
    - **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.
    - Concrètement, dans le cadre d'un réseau, SNMP est utilisé :
      - pour administrer les équipements ;
      - pour surveiller le comportement des équipements.

- **NAT :**
  - On dit qu'un routeur fait du *Network Address Translation* (NAT) (« traduction d'adresse réseau ») lorsqu'il fait **correspondre les adresses IP internes non uniques** et souvent non routables d'un **intranet à un ensemble d'adresses externes uniques et routables**. Ce mécanisme permet notamment de faire **correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé**, et pallie ainsi l'épuisement des adresses IPv4.

## Introduction à l'infogérance :

L'**infogérance** est l'externalisation de tout ou partie de la gestion et de l'exploitation du Système d'Information à un prestataire informatique tiers.

Schéma de la DMS (l'ensemble des services de la société) : infogérance infrastructure et les applications

Application	Application : Gérer les applications, BDD (oracle, SQLServeur), Java, TOMCAT,
Présentation	frontal : apache/iis
Session	OS : Windows, Linux, Aix
Transport	Virtualisation : VMware, HyperV etc.
Network	Réseau → Réseau, sécurité, firewall, proxy ; switch, routeur.
Donnée physique : câble/wifi	Physique → Datacenter

**Les couches du dessous ont besoin des couches du dessus pour fonctionner. Ainsi cela permet de faire comprendre que pour améliorer un service**

**DMS** : Organisation en centre de services :

- plusieurs personnes qui travaillent pour plusieurs clients.
- 24h/24 & 7j/7
- Niveaux de services + pénalités assorties → **qualité de service**

Travail dans des services pour les utilisateurs finaux → l'Informatique est le crash nécessaire pour cette finalité.

**Les deux éléments essentiels** : **Continuité de service & qualité de service.**

Dans l'entreprise ECONOCOM il y a une organisation en pôle de compétence :

Windows / Linux + Unix / BDD / réseau / ordonnancement.

La question qu'on va maintenant se poser.

**Comment on arrive à faire de la continuité de service et de la qualité de service à travers les différentes couches, les différents pôles de services.**

## **Expressions de besoins :**

***Il faut déjà savoir quel type de continuité on veut (l'importance)***

### **Continuité de services :**

- L'analyse des risques (humaine/naturelle)
- Maintenance (bonne procédures, niveau de compétence suffisant des équipes)
- Un bon partage des rôles → Tickets / astreintes / Historisation & traçabilité d'une action.
  - Roulement / planning
- Documentations adéquates.

### **Qualité :**

- Mesure préventives
  - Sauvegarde et restauration de données.

- Planning des actions à mener en cas de crise.
  - Conservation et archivage de données.
  - Mirroring
  - Etc.
- Documentations adéquates.

### **Efficiences économiques :**

- La sur-qualité est une efficacité économique.

## **Les différents outils à notre disposition :**

- **ITOP : Service de Management** (gestion des demandes, incidents, changements, problèmes, CMDB)

ITOP est l'outil de gestion des tickets utilisé pour les prestations d'infogérance CDS. Le client peut accéder à l'outil au travers d'un portail lui permettant de consulter et d'interagir sur les tickets mais également de saisir des demandes ou changements.

- **POM/Nagios : Outil de Supervision**

L'application Nagios permet de visualiser les alertes en cours, le contenu de la supervision et les graphiques générés à partir des données collectées.)

Dans le contexte d'hébergement de données, la finalité de la solution prévue est d'assurer la surveillance des serveurs, processus, applications et réseaux et la remontée des alertes au moyen de l'environnement POM/Nagios mutualisé du CDS (centre de services), dont les agents seront mis en œuvre sur les serveurs du client et sur l'infrastructure mutualisée.^

Deux modules complémentaires permettent de représenter les informations des outils précédents :

- Pour délivrer les différents compte rendus et tableaux de bord, le Centre de Services utilise Talend, un ETL open source rapide et puissant.

Talend Open data Studio va rechercher dans ITOP (ou autre outil ITSM), les données pour les stocker dans une base infocentre.

- Le Centre de Services utilise BIRT Open Source (Business Intelligence and Reporting Tools) pour mettre en forme les reportings à partir des données infocentre.

- **La CMDB** sert de référentiel du parc pour la prestation. Elle est en partie alimentée par les outils de supervision et sert de référentiel pour les tickets. Cela permet de **garantir une cohérence entre les différents outils.**

➤ **Description ITSM** (gestion des services informatiques) :

Dans le cadre de **client multiservice** et notamment pour des **services de helpdesk** (service chargé de répondre aux demandes d'assistance émanant des utilisateurs), la DMS s'appuie sur l'outil ITSM de BMC dans sa gestion des incidents.

L'environnement complet ITSM est hébergé **sur l'infrastructure Cloud Computing Econocom** sous forme de **machine virtuelle HyperV**.

Cette infrastructure est gérée par différents services d'Econocom :

- **APPLICATION ITSM : SERVICE SMC**
- **INFRASTRUCTURE CLOUD : SERVICE INFEENY**
- **MACHINE VIRTUEL (OS ET SERVICES) : SERVICE CDS**
- **OUTILS DE SUPERVISION : WITBE.**

➤ **Witbe** est une **solution de monitoring** (supervision d'un parc) de la Qualité et Disponibilité des Services IT. Les solutions Witbe couvrent l'ensemble des applications et les services :

Sites et applications Web	Applications métiers
Messageries	SVI et Centres de contact
Téléphonie et ToIP – Vidéo et IPTV	Transactions monétiques
Infrastructures, etc.	

Pour cette application, **la supervision est effectuée par l'intermédiaire d'équipement appelé « Robot »**. Ces robots simulent des transactions à fréquence régulière et **s'assurent du bon fonctionnement des services et applications critiques : disponibilité, performance et intégrité**.

Cette application permet plusieurs fonctionnalités tels que :

- Création de script sur-mesure pour chaque application Client.
- Les Robots permettent certains résultats tels que des analyses, du stockage, production de rapports et des alertes.

- Gestions des alertes et analyse des dysfonctionnements.
- Détails des disponibilités des applications.

### ➤ Osianoo : outils de gestion des taches :

**Outil d'ordonnancement des tâches** de contrôle et d'exploitation du Centre De Services et de pilotage du transfert de consignes. Cet outil est principalement utilisé aujourd'hui pour la **gestion des tâches récurrentes** (planification, affichage sur les écrans des pilotes, **gestion de la prise en charge de la tâche...**).

### ➤ Les différentes documentations mis en place :

- **Le wiki :**
  - Portail accessible via l'url « <http://wiki.ogs.oed/> » depuis le réseau OGS.
    - Regroupe la documentation, les processus et les procédures du CDS et des clients.
- **Filer :**
  - Accessible depuis l'adresse:\\13.168.20.16\data\
    - Serveur ou sont stockés les documents de travail ne relevant pas du wiki.

## Les différents outils pour la sécurité :

### ➤ Outil de gestion des mots de passes :

- L'outil **PasswordManager** est disponible pour l'ensemble de la DMS. Cet outil permet de **stocker l'ensemble des mots de passes** nécessaires aux prestations de **manière sécurisé** et permet de **centralisé** tout en **contrôlant l'accès à ces informations**.
- Ces fonctionnalités :
  - L'accès à l'outil se fait par une interface WEB



- Les mots de passes sont stockés chiffrés en base de données. Le chiffrement est réalisé avec une clé AES-256(algorithmes de cryptage aujourd'hui le plus fréquemment utilisé et le plus sécuritaire)
- Possibilité de stocker des mots de passes individuels. Ces mots de passes peuvent être chiffrés par la même clés que les mots de passes partagés ou par une clé privée.

### ➤ Outil de gestion des traces :

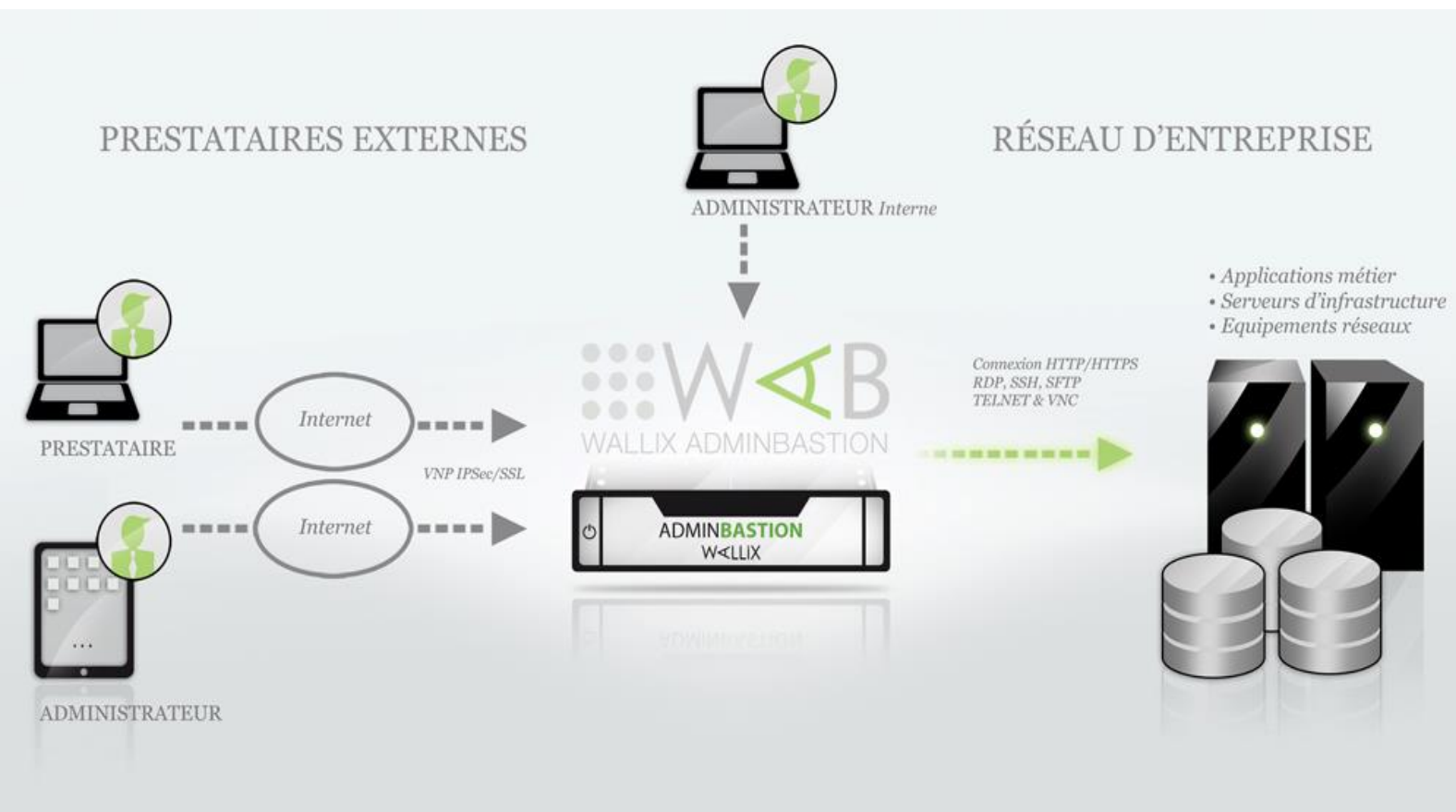
Afin de garantir **l'historisation d'évènements ou d'action** sur les différents composants du système d'information, l'agence CDS utilise l'outil **WALLIX ADMINBASTION**.

#### Les objectifs de l'outil Wallix Adminstion :

- Identification de la connexion (serveur, firewall, BDD)
- Identification de l'action effectuée sur les équipements serveurs ou applicatifs

La traçabilité :

- La durée de rétention
- La conservation des logs
- Et les habilitations à l'accès à ces informations.



### ➤ WAB la suite logicielle de Wallix :

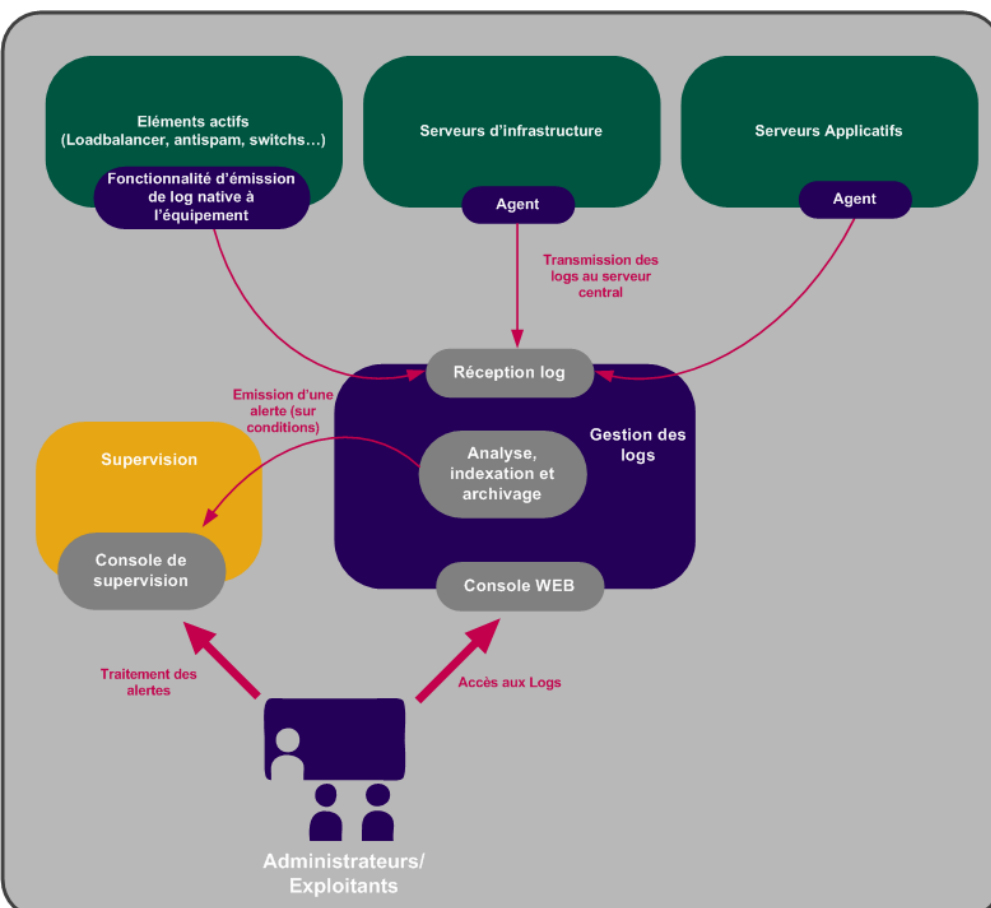
L'outil WAB s'appuie sur **les mécanismes d'authentification de l'Active Directory**. C'est sur la base des fichiers de « log » qu'Econocom **analyse les événements douteux et fournit un reporting**.

Certaines fonctionnalités de WAB :

- Tracer les connexions réussies ou non et actions menées par les administrateurs
- D'avoir des **statistiques sur le nombre et la répartition des connexions**.
- De mettre en place des **contrôles d'accès**.
- De **signaler des alertes en temps réel**.
- De **gérer les autorisations d'accès aux différents équipements**.

WAB est hébergé sur les **Datacenter**, il se positionne en intermédiaire entre **le réseau des administrateurs et les zones dédiés à l'hébergement** des équipements du client ou l'interconnexion réseau menant à son infrastructure.

### ➤ Outil de journalisation :



#### Le fonctionnement de l'outil :

On comprend grâce à ce schéma que l'outil de journalisation récupère les logs des serveurs, des éléments actifs et de la console web des administrateurs. Une fois récupérés, les logs sont analysés, indexés et archivés.

Afin d'émettre une alerte à la supervision, lorsque le cas est nécessaire.

- **La collecte de logs sur l'infrastructure du client :**

- Fait grâce à l'Open source **XLOG** qui est une solution de gestion de **log haute performance et multiplateforme**.
  - Cette solution inclut des **agents** permettant de **rediriger les logs vers une plateforme centralisée**.
  - La collecte des logs se base sur 2 principes :
    - Les agents pour les serveurs ont plusieurs rôles :
      - **Collecter les logs** (depuis les journaux d'événements Windows, les logs systèmes Unix ou des fichiers de logs).
      - La **standardisation du format** des logs.
      - La **transmission des logs vers les serveurs centraux**.
    - Les logs des différents Appliance (switch, anti-spam, LoadBalancer...) seront transmis directement aux serveurs de logs.  
**La standardisation des logs se fera au niveau de ces serveurs.**

- **La centralisation des logs :**

- L'objectif de centraliser les logs sont :
  - **Recevoir les logs transmis** par les différents équipements.
  - **Archiver les logs**.
  - **Stocker en indexant** une partie afin de **faciliter leur exploitation**.

- **Concernant les logs :**

- Stockés en BDD afin de permettre une indexation.
- Purge des logs, afin de garantir une performance élevée de la console.
- Les logs sont compressés et stockés pendant une durée de 6 mois sur les serveurs.
- La solution de gestion des logs est intégrée aux outils de supervision afin de faciliter l'exploitation des logs.
- Un système d'alarmes peut être installé afin de superviser sur des critères prédéfinis ou sur une répétition d'événements.

- **Consultation des informations :**

- Une application web est utilisé afin d'exploiter plus facilement les logs.
- Grace au système d'indexation, la recherche par combinaisons de mot clés ou des plages de temps données sont possible.

- Les logs non indexés initialement peuvent également être réinjectés dans la BDD si nécessaire pour effectuer une analyse post incident

### ➤ LE VPN :

Le client VPN utilisé « VPN Cisco AnyConnect Secure Mobility Client » est disponible depuis la page web : <https://webvpn-cts.osiatis.com/>

- VPN **signifie réseau privé virtuel**. C'est un système permettant de **créer un lien direct** entre des ordinateurs distants. Les ordinateurs connectés au VPN sont ainsi **sur le même réseau local** (virtuel), ce qui permet de passer outre d'éventuelles restrictions sur le réseau (comme des pare-feux ou des proxys).
- On utilise notamment ce terme dans le travail à distance (astreinte ou le télétravail), or ici il est utilisé afin d'accéder au serveur qui sont sous forme de VM.
- Une autorisation d'accès a été mise en place ainsi qu'une ouverture des flux selon le groupe AD (Dynamic Access Policies).
- Des algorithmes de chiffrement sont activés sur le firewall :

#### Active Algorithms

3DES-SHA1
AES128-SHA1
DES-SHA1
AES256-SHA1
RC4-SHA1

## Éléments appris durant les visites afin d'en apprendre plus sur leur métier :

- ✓ Réglage de flux : Certaines demandent sont de pouvoir accéder à des adresses/réseaux. Cependant des sécurités ont été installées sur le réseau. En effet des firewalls sont en place et protège des paquets venant de l'extérieur. Il faut donc pour cela régler les firewalls et de laisser passer les flux que l'on veut. Ainsi on ouvre dans le sens de la connexion de la source jusqu'à la destination.

*Les flux aux niveaux des firewalls : Un seul sens est nécessaire et non les deux, il faut faire la dissociation entre l'adresse de source et de destination.*

- Pour faire les changements sur les firewalls, le service dispose de documents avec l'ensemble des structures, et un outil CISCO ASDM.

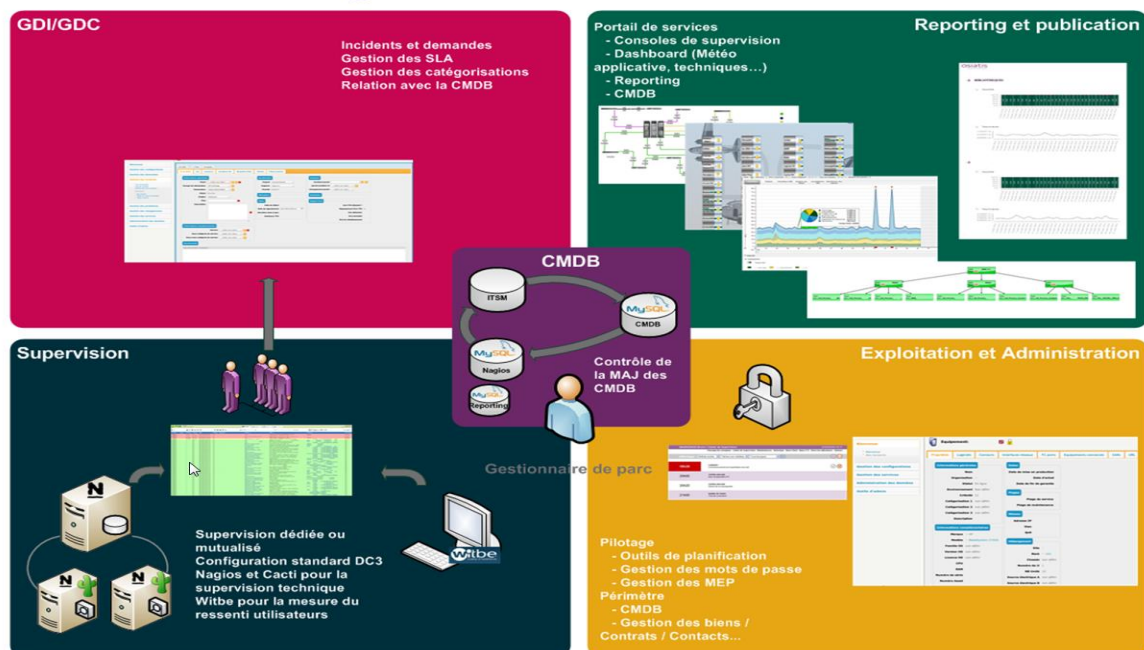
✓

## Compréhension de la coexistence de l'ensemble des outils utilisé dans le DMS :

Avant de passer l'entretien avec tous les membres de la couche réseau, il faut **comprendre comment marche l'ensemble de tous les logiciels** utilisé par le DMS.

Il ne faut pas oublier que les **futurs outils** que l'on souhaite mettre en œuvre doivent **coexister dans un écosystème global**.

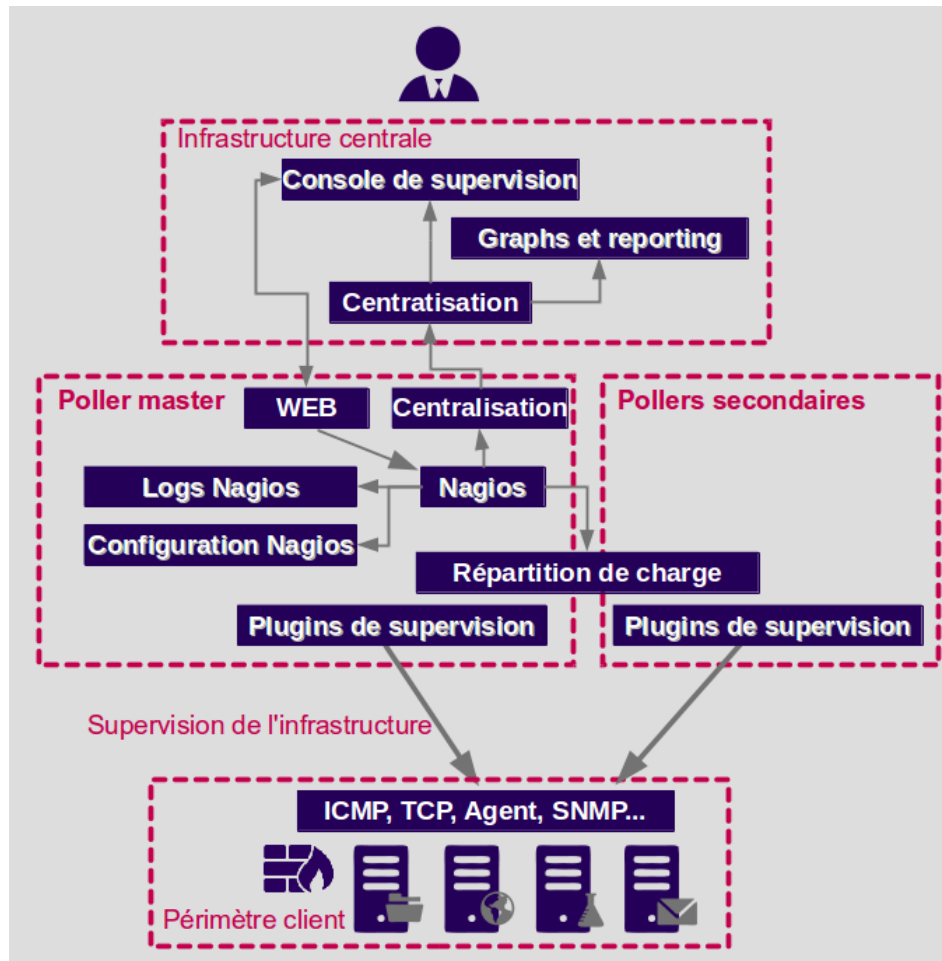
### Architecture générale



L'ensemble des outils sont implémenté sur un site, c'est une suite de logiciels et certains outils interagissent avec d'autres. On se connecte sur POM et cela permet d'être connecté à l'ensemble des outils.

Tout commence avec l'application POM/Nagios (supervision). Ces outils permettent une **gestion des demandes et des incidents éventuelles**. La **Base de données** est reliée aux outils de supervisions **afin d'assurer une cohérence des données**. ITOP, l'outil de management, permet de **gérer grâce à un système de tickets et de faire une gestion de ces demandes/incidents**. Le client peut aussi se connecter sur cet outil, **le permettant d'interagir avec le ticket ou de faire de**

demandes. Des statistiques en forme de **Dashboard** sont possibles grâce aux services de **Reporting** et publication.



## Récapitulatif de l'entretien avec la service réseau :

On va maintenant passer à une réunion collective afin de prévenir les membres du service réseau de ma prochaine utilité et les choses qu'on va leur demander aux entretiens.

Le but de mon intervention est la suivante :

**Il faut Réorganiser l'équipe réseau sur un point de vue humain mais aussi sur des méthodes de travail et d'outillage.**

Les questions posées seront les suivantes :

- Qu'elle est votre métier ? Que faites-vous ?
- De quoi avez-vous besoin pour faire votre métier concrètement ?
- Qu'est-ce qu'il manque véritablement ?
- Combien de temps ce type de chose/procédure/demande vous prend ?

- Cb de fois par jour arrive-t-il ?

Le but des entretiens individuel et d'avoir une idée personnel de leur problème et de leur perte de temps. Afin **de recueillir toutes informations pouvant participer à l'amélioration du service**. Il ne faut pas perdre de vue qu'on recherche **un point de vue industriel**, quelque chose qui vont vraiment leur servir et quelque chose qui est un **véritable poids** pour eux, les éventuelles mises en places seront bien entendu dans un but lucratif afin que l'entreprise gagne de l'argent et non en perdre ( lorsque l'employer ne peut pas régler le problème ou met beaucoup trop de temps par rapport à ce que ça devrait être).

Ainsi avec les multiples « plaintes » recueillies. Le but sera de **les classer afin d'avoir les plus importants et de pouvoir les traiter** et donc de **résoudre leur problèmes et leur perte de temps**.

### Compte rendu des entretiens :

L'entretien a apporté plusieurs poids qui subsistent dans la société :

- ❖ L'outil « POM » offre un moyen de décrire les équipements ou ils se situent...
  - Malheureusement il n'est pas renseigné et les descriptions sont incomplètes
- ❖ Manque de documentation au niveau des ports.
  - données manquantes ou partielles pour le référencement des ports (annuaire pour les flux).
- ❖ Gestion des IP, IP wifi ou réseaux des serveurs
  - Manque d'informations sur les IP, trop de documents sur le sujet, aucun complet.
    - Une IPAM ressemblant la totalité des réseaux serait une solution.
- ❖ Mettre en place une GED (gestion électronique de documents)
  - Cela permettrait d'avoir un gain de temps et une augmentation de l'efficacité et une suite de protocole, plutôt que de déranger les gens pour avoir les bonnes procédures.
- ❖ Gestion Humain : Trombinoscope
  - Lorsque quelqu'un arrive c'est dur de savoir le nom des gens et lorsqu'on est amené à demander de l'aide les collègues disent va voir tel ou tel personne.
- ❖ Gestion des clients :
  - Si le professionnel pour une raison ou une autre n'est plus dans la société et la DMS se retrouve à devoir gérer un client qui n'a jamais été gérer par quelqu'un d'autre que la personne qui vient de partir.

- Une indexation et une augmentation de documents pourrait permettre à un inconnu client de s'occuper correctement du client.
- ❖ Cartographie des interfaces :
  - Il existe un manque dans la description des interfaces et la description des équipements.
- ❖ Demandes de flux :
  - Les demandes de flux sont mal formulés/renseignés, un template permettant une demande complète serait nécessaire.
- ❖ Problème de tickets sur ITOP :
  - Les tickets devraient être renseignés le plus possible afin que chaque personne s'occupant des tickets devraient être explicite et bien tourné autour du problème.

## Résolution des expressions de besoins :

Afin de résoudre les problèmes, des réunions ont été mis en place permettant de faire un tableau « Expressions de besoins avec les poids du service réseaux ».

Ce tableau a permis de regrouper certains aspects qui leur posent problèmes.

Un regroupement a été fait et les grandes idées qui en ressortent sont les suivantes :

- Gestion de la documentation et d'indexation.
- Gestion D'IP.
- Le manque d'utilisation des outils fournis tels qu'ITOP et POM.

## Solution de documentation et d'indexation :

Pour ce problème, il existe deux choix :

- Mettre en place **un moteur de recherche** qui ne s'arrêterait pas seulement au titre du document mais qui permettrait de rentrer afin d'avoir une recherche approfondie.
- Créer un **Template / un modèle** qui servirait de **repère** à chaque création de dossier pour un nouveaux client.

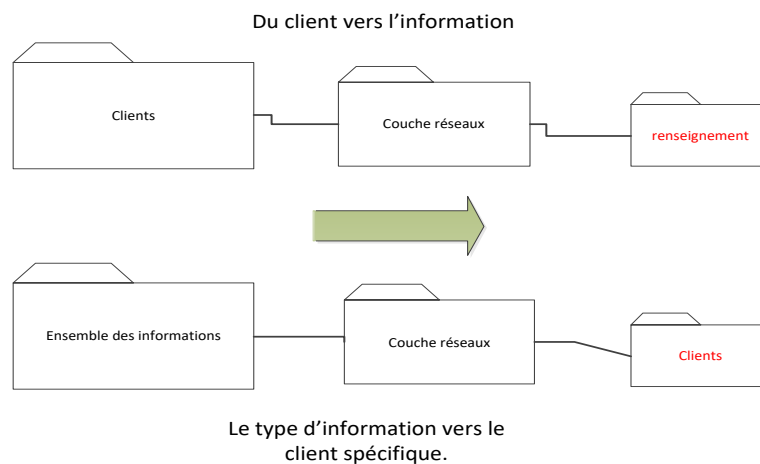


L'option qui a été choisie et celle du modèle. En effet un template modèle sera mieux en place et chaque nouveau dossier de client devra respecter la mise en forme. La première option n'est pas éliminée, elle reste en tant qu'option une fois que le template sera mis en place il est possible que le moteur de recherche en soit une suite.

Après avoir réfléchi il existe plusieurs façons d'annexer les documents.

En effet :

- soit les dossiers sont rangés par clients et après se déroule la grande liste de dossier
- Soit tous les dossiers principales sont déjà rangés par catégorie et se finissent par client.



- On choisira le fait que l'on démarre du client vers l'information souhaitée.

Le travail a été effectué et se nomme « **Template Indexation Réseau Securite** ».

- Mon **document Visio** permet de comprendre comment sont **liés les documents ensemble**. Le but de mon indexation a été de faire **qu'un seul document reseaux\_securite** afin que les personnes du service réseaux n'est **qu'un seul dossier à regarder** et **des raccourcis** ont été mis en place **afin de les rediriger vers les informations souhaitées**.

## Solution de gestion d'IP :

Nous allons commencer à chercher **les fonctionnalités voulues de l'IPAM** pour le service réseaux. Pour cela on va faire comme la résolution de l'indexation poser des réunions.

L'ensemble des fonctionnalités de l'IPAM qui est ressortis des réunions :

### Légende des expressions de besoins :

Rouge → Impératif

Bleu → Facultatif

- ✓ Gestion des plages, des multi clients (distinction des clients, granularité des droits)
- ✓ Gestion de VLAN ID
- ✓ Import d'information manuel (XLS ou autre)
- ✓ NAT : Vlan source / cible, équipements qu'il porte
- ✓ Gestion des plages / sous plage, filtrage des adresses macs, baux, exclusions ....
- ✓ Comment on inscrit un DNS ou reverse DNS ?
- ✓ Gestion de VIP
- ✓ Gestions des routes soit dans ITOP soit dans l'IPAM
- ✓ Gestion de champs pour L'IPhone (ex serveur TFTP)
- ✓ Module Serveur DNS (Pas de serveur DNS sur OGS)

### **Deux IPAM sont ressortis de ce tableau comparatif :**

- PHPipam
- TeemIP

La suite de ce document a pour but de tester complètement et en profondeur et de bien sûr travailler sur linux et installer et apprendre à gérer divers problèmes.

On va donc créer une seule VM ou on va installer les deux IPAMs choisit plus haut.

### **Installation des IPAMs sur une VM Debian**

Nous allons maintenant faire l'installation de ces deux IPAM sur une VM avec un OS Debian 8.3.0 x64 et tester jusqu'au bout les capacités de chacun et faire ressortir un seul IPAM afin qu'il soit intégré aux services.

ID et MDP :

root / Root1

letort / password123

On va commencer par **effectuer le partitionnement de la VM avec les différentes partitions et le /appli**

Tout d'abord penser à mettre un **deuxième disque** sur la VM.

Commencer l'installation de la VM, choisir un disque « SCSI1 », et créer une nouvelle table des partitions sur ce disque, faire pareil sur le deuxième disque « SCSI2 »

### **Configuration des volumes logiques (LVM) :**

Faire « configurer le gestionnaire de volumes logiques (LVM) » et appuyer sur oui

Ensuite il faut « Créer un groupe de volumes »

Il faut mettre un nom de groupe de volumes, on va mettre '**VG\_SYSTEM**' pour groupe de volume système.

On va le mettre sur le premier disque /dev/sda/free #1, appuyer sur oui,

Maintenant que le groupe de volume est créé on va faire des volumes logiques afin de répertorier /, /swap, /opt, /tmp, /var, /home, /root ... :

On va donc aller dans « Créer un volume logique », on va sélectionner VG\_SYSTEM.

Puis saisir un nom de volume, on va commencer par :

lv\_root et on va mettre comme taille du volume logique 5G, et on continue

lv\_tmp , 2G; lv\_var , 4G; lv\_home 1G; lv\_opt, 2G;

Pour finir on va créer le lv\_swap, et on va mettre autant de Giga que de ram qu'on a attribuée à la VM

On va ensuite cliquer sur terminer.

On va maintenant **assigner les LV au bon point de montage**, on va choisir le lv\_home,

Aller sur « utiliser comme : ne pas utiliser », choisir système de fichier journalisé ext4 pour tous les LV sauf pour le swap qui a son propre type de fichier « Espace d'échange 'swap' ».

### **Point de montage :**

Choisir le point de montage qui correspond au LV c'est à dire, on a choisi lv\_home on va prendre le point de montage /home.

Une fois tout configuré descendez la molette et cliquez sur « Terminer le partitionnement et appliquer les changements, faire appliquer les changements sur les disques.

On configurera en ligne de Commande sur le disque deux le / appli.

Installer ensuite normalement la VM, avec un miroir et GRUB, prendre le premier disque pour le installer le programme de démarrage

Penser à faire apt-get update/upgrade.

### **Mise en place de la partition /appli sur SCSI2**

Il faut d'abord dire que le disque deux /dev/sdb sera initialisé avec du LVM.

Pour cela :

```
root@Ipams:~# pvcreate /dev/sdb
```

Associer au disque physique 2 un volume groupe nommé VG\_DATA:

```
root@Ipams:~# vgcreate VG_DATA /dev/sdb
Physical volume "/dev/sdb" successfully created
Volume group "VG_DATA" successfully created
```

On doit obtenir cela :

```
root@Ipams:~# pvdisplay -C
PV          VG          Fmt  Attr PSize  PFree
/dev/sda1   VG_SYSTEM  lvm2 a--  20,00g  5,11g
/dev/sdb    VG_DATA    lvm2 a--  40,00g  40,00g
```

Une fois le groupe mis en place on peut faire un volume logique nommé lv\_applis dans le volume groupe DATA → VG\_DATA :

```
root@Ipams:~# lvcreate -L 20480M -n lv_applis VG_DATA
Logical volume "lv_applis" created
```

$1024M * 20G = 20480M$

Nous allons maintenant créer la couche système de fichier (Formater)

On va d'abord démonter la partition LVM, lv\_appli, puis le monter en ext4.

```
root@Ipams:~# umount /dev/VG_DATA/lv_applis
umount: /dev/VG_DATA/lv_applis : non monté
root@Ipams:~# mkfs.ext4 /dev/VG_DATA/lv_applis
mke2fs 1.42.12 (29-Aug-2014)
En train de créer un système de fichiers avec 5242880 4k blocs et 1310720 i-noeuds.
UUID de système de fichiers=f9cf5e94-d85c-4783-b476-635140d8e797
Superblocs de secours stockés sur les blocs :
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000

Allocation des tables de groupe : complété
Écriture des tables d'i-noeuds : complété
Création du journal (32768 blocs) : complété
Écriture des superblocs et de l'information de comptabilité du système de
fichiers : complété
```

On va maintenant aller dans le **fichier /etc/fstab**, ce fichier liste les partitions qui seront montées au démarrage ou à la connexion du périphérique, décrivant chacune les conditions de montage de chaque système de fichier.

On ajoute cette ligne au fichier :

```
/dev/mapper/VG_DATA-lv_applis /applis          ext4    defaults    0        2
```

On a dit dans cette ligne que le volume groupe était VG\_DATA, que le volume logique était lv\_applis et que notre /applis sera notre point de montage. Pour cela on doit créer le dossier /applis

```
root@Ipams:~# mkdir /applis
```

Et ensuite le monter :

```
root@Ipams:~# mount /applis
```

mount -a permet de monter tous les systèmes de fichiers disponible à monter.

La commande mount permet d'afficher les systèmes de fichiers déjà montés :

```
root@Ipams:~# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,relatime,size=10240k,nr_inodes=255118,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,relatime,size=411728k,mode=755)
/dev/mapper/VG_SYSTEM-lv_root on / type ext4 (rw,relatime,errors=remount-ro,data=ordered)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/lib/systemd/systemd-cgroups-agent,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=22,pgrp=1,timeout=300,minproto=5,maxproto=5,direct)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
/dev/mapper/VG_SYSTEM-lv_home on /home type ext4 (rw,relatime,data=ordered)
/dev/mapper/VG_SYSTEM-lv_var on /var type ext4 (rw,relatime,data=ordered)
/dev/mapper/VG_SYSTEM-lv_opt on /opt type ext4 (rw,relatime,data=ordered)
/dev/mapper/VG_SYSTEM-lv_tmp on /tmp type ext4 (rw,relatime,data=ordered)
rpc_pipefs on /run/rpc_pipefs type rpc_pipefs (rw,relatime)
/dev/mapper/VG_DATA-lv_applis on /applis type ext4 (rw,relatime,data=ordered)
```

**On voit a la dernière ligne que notre /applis a bien été monté !**

mount -a monte ce qui n'est pas monté.

**On peut maintenant commencer les installations/configurations.**

## **Configuration de l'interface Ethernet :**

Editez le fichier :

```
Fichier : /etc/network/interfaces
```

On va mettre l'interface eth0 **en statique**, une adresse IP donnée qui est **13.168.12.21**, un **masque en /24** et une **passerelle par défaut : 13.168.12.1**

**Remplacer le fichier :**

**Par :**

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#allow-hotplug eth0
#iface eth0 inet dhcp

auto eth0_
iface eth0 inet static
    address 13.168.12.21
    netmask 255.255.255.0
    gateway 13.168.12.1
```

On va redémarrer la carte réseaux eth0 :

```
root@Ipam:/home/appli# ifdown eth0
root@Ipam:/home/appli# ifup eth0
```

Et vérifier que la configuration a été acceptée :

```
root@Ipam:/home/appli# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:2e:2e:54
          inet adr:13.168.12.21  Bcast:13.168.12.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fe2e:2e54/64  Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11937 errors:0 dropped:1 overruns:0 frame:0
          TX packets:328 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:1703685 (1.6 MiB)  TX bytes:30732 (30.0 KiB)
```

### **Installation SSH :**

Nous allons ensuite se connecter à la VM avec putty pour être plus à l'aise.

Pour cela on va faire les commandes suivantes :

```
root@Ipam:/home/appli# apt-get install ssh_
```

**Pour activer la connexion distante SSH pour le compte root.** Editez le fichier :

```
Fichier : /etc/ssh/sshd_config
```

Remplacer:

```
# Authentication:
LoginGraceTime 120
PermitRootLogin without-password
StrictModes yes
```

PermitRootLogin without-password

Par:

PermitRootLogin yes

```
# Authentication:
LoginGraceTime 120
PermitRootLogin yes_
StrictModes yes
```

Ensuite, il ne reste plus qu'à redémarrer SSH :

```
root@Ipam:/home/appli# service ssh restart
```

## **Installation de PHPIPAM :**

Nous allons suivre le guide d'installation de PHPipam : <http://phpipam.net/documents/installation/>

*Avant de commencer à installer PHPipam, il faut Apache2, MySQL Server, et PHP version 5.3 minimum*

---

## **Installation d'apache2 :**

Avant de commencer on va effectuer un apt-get install /upgrade.

Nous allons maintenant installer apache2. Pour se faire tapez la commande suivante

**apt-get install apache2**

Si il demande d'insérer un disque c'est que Virtual box a enlevé le disque au début dans les configurations il faut alors retourner dans la configuration et lui remettre l'iso Debian 8.3.

Une fois installé, on tape l'IP de la machine sur le navigateur et on voit bien que notre apache marche.

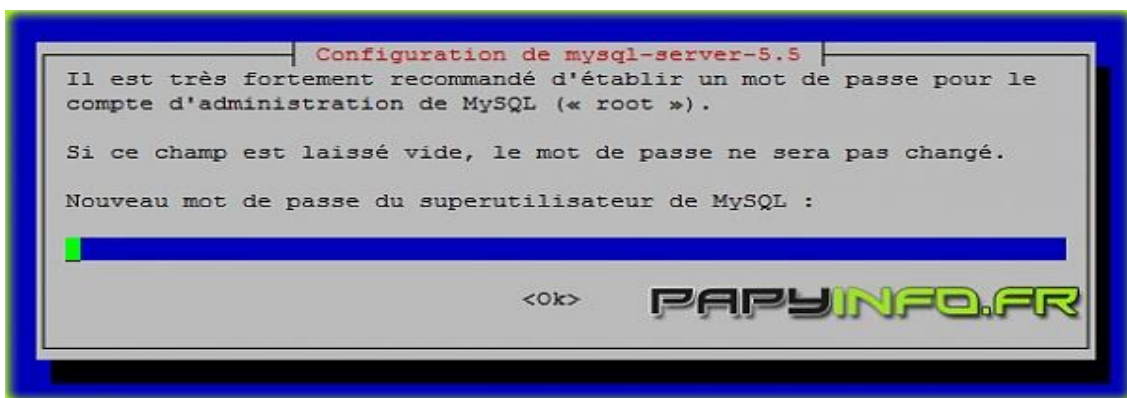
### Installation de mysql :

Nous allons maintenant installer MySQL

```
apt-get install mysql-server
```

À la question **souhaitez-vous continuer ? [O/n]** appuyez sur la lettre "o" puis validez.

Vous allez tomber sur la fenêtre suivante



Il vous faut rentrer un mot de passe pour votre compte administrateur de *mysql*. Une fois le mot de passe rentré appuyez sur la touche Entrée de votre clavier. Une confirmation vous sera demandée. Notez bien le mot de passe car il vous sera nécessaire sur phpmyadmin. L'installation se termine pour *mysql*.

### Installation de php versions 5.5 :

Pour l'installation de php5 il nous suffit de rentrer dans le shell la commande suivante :

```
apt-get install php5
```

On va maintenant vérifier que tout marche pour cela on va dans le chemin suivant :

```
cd /var/www/html/
```

Et on va créer un fichier php afin de valider l'installation du php5

```
Nano /var/www/html/php.php
```

```
<?Php  
phpinfo();  
?>
```



On va maintenant dans notre navigateur et on tape la ligne suivante :

« **Locahost/nomdufichier.php** » soit 13.168.12.21/index.php

Apache2, Mysql server et Php sont maintenant installé, cependant le phpipam a besoin de modules.

- pdo, pdo\_mysql : Adds support for mysql connections
- session : Adds persistent session support
- sockets : Adds sockets support
- openssl : Adds openSSL support
- gmp : Adds support for dev-libs/gmp (GNU MP library) -  
> to calculate IPv6 networks
- ldap : Adds LDAP support (Lightweight Directory  
Access Protocol – for AD also)
- crypt : Add support for password encryption
- SimpleXML: Support for SimpleXML (optional, for  
RIPE queries and if required for API)
- json: Enable JSON support
- gettext: Enables translation
- filter : Adds filtering support
- pcntl : Add support for process creation  
functions (optional, required for scanning)
- cli : Enable CLI (optional, required for scanning and  
status checks)

Pour voir les modules qu'on a : =====>

On remarque que les modules manquants sont :

- ❖ gmp : Adds support for dev-libs/gmp (GNU MP library) -  
> to calculate IPv6 networks
- ❖ ldap : Adds LDAP support (Lightweight Directory Access  
Protocol – for AD also)
- ❖ crypt : Add support for password encryption
- ❖ cli : Enable CLI (optional, required for scanning and  
status checks)

Pour chercher ces volumes manquants nous allons utiliser la commande :

```
root@Ipams:/var/www/html# php -m
[PHP Modules]
bcmath
bz2
calendar
Core
ctype
date
dba
dom
ereg
exif
fileinfo
filter
ftp
gettext
hash
iconv
json
libxml
mbstring
mhash
openssl
pcntl
pcre
PDO
Phar
posix
readline
Reflection
session
shmop
SimpleXML
soap
sockets
SPL
standard
sysvmsg
sysvsem
sysvshm
tokenizer
wddx
xml
xmlreader
xmlwriter
Zend OPcache
zip
zlib
```

apt-cache search

```
root@Ipams:/var/www/html# apt-cache search gmp | grep php
php5-gmp - GMP module for php5
```

Maintenant que nous avons trouvé le module nous allons l'installer et faire pareil pour les 3 autres modules manquants.

De même pour ldap :

```
root@Ipams:/var/www/html# apt-cache search gmp | grep php
php5-gmp - GMP module for php5
root@Ipams:/var/www/html# apt-get install php5-gmp

php5-ldap - module LDAP pour
root@Ipams:/var/www/html# apt-cache search ldap
php5-lasso      php5-ldap
root@Ipams:/var/www/html# apt-get install php5-ldap
```

De même pour crypt :

```
root@Ipams:/var/www/html# apt-cache search crypt | grep php
php-tcpdf - PHP class for generating PDF files on-the-fly
php5-mcrypt - module MCrypt pour PHP5
php-swiftmailer - Swiftmailer, free feature-rich PHP mailer
php-crypt-blowfish - Allows for quick two-way blowfish encryption without requiring the MCrypt PHP extension
php-crypt-gpg - PHP PEAR module for encrypting and decrypting with GnuPG

root@Ipams:/var/www/html# apt-get install php5-mcrypt php-horde-crypt
```

Et on finit par installer le module cli :

```
root@Ipams:/var/www/html# apt-cache search cli | grep php
php5-cli - interpréteur en ligne de commande pour le langage de script PHP5

root@Ipams:/var/www/html# apt-get install php5-cli
```

Téléchargement et installation de PHPipam :

On va se diriger dans le /appli

```
root@Ipams:/var/www/html# cd /applis/
```

Et on va télécharger le paquet de PHPipam :

```
root@Ipams:/applis# wget https://sourceforge.net/projects/phpipam/files/latest/download
```

On va renommer le paquet qu'on a téléchargé et on va le décompresser :

```
root@Ipams:/applis# mv download phpipam-1.2.1.tar
root@Ipams:/applis# ls -l
total 9252
drwx----- 2 root root 16384 juin 17 15:28 lost+found
-rw-r--r-- 1 root root 9457664 févr. 13 13:17 phpipam-1.2.1.tar
```

```
root@Ipams:/applis# tar -xvf phpipam-1.2.1.tar
```

Une fois décompressé le dossier apparaît :

```
root@Ipams:/applis# ls -l
total 9256
drwx----- 2 root root 16384 juin 17 15:28 lost+found
drwxr-xr-x 11 80 80 4096 févr. 13 13:15 phpipam
-rw-r--r-- 1 root root 9457664 févr. 13 13:17 phpipam-1.2.1.tar
```

Une fois cela fait, il faut renommer le fichier « config.dist.php » en « config.php ».

```
root@Ipams:/applis/phpipam# mv config.dist.php config.php
root@Ipams:/applis/phpipam# ls -l
total 64
drwxr-xr-x 4 80 80 4096 juin 17 17:55 api
drwxr-xr-x 14 80 80 4096 juin 17 17:55 app
-rwxr-xr-x 1 80 80 2902 févr. 9 17:23 config.php
drwxr-xr-x 3 80 80 4096 juin 17 17:55 css
drwxr-xr-x 3 80 80 4096 juin 17 17:55 db
drwxr-xr-x 11 80 80 4096 juin 17 17:55 functions
-rwxr-xr-x 1 80 80 10057 févr. 8 19:04 index.php
drwxr-xr-x 2 80 80 4096 juin 17 17:55 install
-rwxr-xr-x 1 80 80 110 janv. 28 17:34 INSTALL.txt
drwxr-xr-x 3 80 80 4096 juin 17 17:55 js
drwxr-xr-x 2 80 80 4096 juin 17 17:55 misc
-rwxr-xr-x 1 80 80 2455 janv. 28 17:34 README
-rwxr-xr-x 1 80 80 105 janv. 28 17:34 UPDATE
drwxr-xr-x 2 80 80 4096 juin 17 17:55 upgrade
```

On va maintenant configurer le fichier config.php

Il faut que les informations suivantes soit inscrite :

```
$db['host'] = "localhost";
$db['user'] = "phpipam";
$db['pass'] = "phpipamadmin";
$db['name'] = "phpipam";
```

Dans un deuxième temps il faut indiquer l'endroit où on a extrait le paquet PHPipam à cet endroit :

```
if(!defined('BASE'))
define('BASE', "/");
```

Je n'ai rien changé tout était déjà correctement écrit.

## Installation de la Database :

On va maintenant créer la database et on va mettre des droits :

```
root@Ipams:/applis/phpipam# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 43
Server version: 5.5.49-0+deb8u1 (Debian)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

```
mysql> create database phpipam;
Query OK, 1 row affected (0.01 sec)
```

```
mysql> GRANT ALL on phpipam.* to phpipam@localhost identified by 'phpipamadmin';
Query OK, 0 rows affected (0.00 sec)
```

On va ensuite importer le schéma SQL dans le dossier db qui se trouve dans PHPipam :

```
root@Ipams:/applis/phpipam# mysql -u root -p phpipam < db/SCHEMA.sql
Enter password:
```

Avec toujours en password : Root1

On va changer le nom de 000-default.conf et mettre le nom de phpipam.conf, et par la suite on va disabled le 000-default.conf

```

root@Ipams:/etc/apache2# locate 000-default
/etc/apache2/sites-available/000-default.conf
/etc/apache2/sites-enabled/000-default.conf
/var/lib/apache2/site/enabled_by_admin/000-default
root@Ipams:/etc/apache2# cd /etc/apache2/sites-available/
root@Ipams:/etc/apache2/sites-available# ls -l
total 12
-rw-r--r-- 1 root root 1332 oct. 24 2015 000-default.conf
-rw-r--r-- 1 root root 6437 oct. 24 2015 default-ssl.conf
root@Ipams:/etc/apache2/sites-available# cp 000-default.conf phpipam.conf
root@Ipams:/etc/apache2/sites-available# a2dissite 000-default.conf
Site 000-default disabled.
To activate the new configuration, you need to run:
    service apache2 reload
root@Ipams:/etc/apache2/sites-available# nano phpipam.conf █

```

Et dans le fichier phpipam.conf on ajoute une directive, et on place le chemin de notre fichier :

```

GNU nano 2.2.6          Fichier : /etc/apache2/sites-enabled/phpipam.conf
VirtualHost *:8080>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /applis/phpipam

# Available loglevels: trace8, ..., tracel, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn
<Directory /applis/phpipam>
    Options Indexes FollowSymLinks Multiviews
    AllowOverride all
    Require all granted
</Directory>

ErrorLog ${APACHE_LOG_DIR}/phpipam_error.log
CustomLog ${APACHE_LOG_DIR}/phpipam_access.log combined
# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

</VirtualHost>

```

On va aller dans le ports.conf pour rajouter le port 8080 :

```
GNU nano 2.2.6      Fichier : /etc/apache2/ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80
Listen 8080
<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>
```

Il faut enable le mod rewrite d'apache :

```
ln -s /etc/apache2/mods-available/rewrite.load /etc/apache2/mods-enabled/rewrite.load
```

On va ensuite mettre un lien symbolique au fichier phpipam.conf

```
root@Ipams:/etc/apache2/sites-available# a2ensite phpipam.conf
Enabling site phpipam.
To activate the new configuration, you need to run:
  service apache2 reload
```

Comme indiqué dans le message il faut reload Apache2 :

On peut ensuite se connecter au serveur sur le navigateur :

13.168.12.21/phpipam/install

Identifiant et mot de passe pour PHPipam une fois configuré :

Id: Admin MDP: P@ssw0rd

## Installation de TeemIP :

Assurez-vous d'avoir une instance correctement configuré d'Apache / PHP en cours d'exécution :

Lien de téléchargement de TeemIP 2.0.2 : <https://sourceforge.net/projects/teemip/files/latest/download>

On va se placer ici : /applis/

```
root@Ipams:~# cd /applis/
```

On va faire un wget <https://sourceforge.net/projects/teemip/files/latest/download>

```
root@Ipams:/applis# wget https://sourceforge.net/projects/teemip/files/latest/download
```

Ensuite on va renommer le fichier download par teemip-2.0.2.zip

```
root@Ipams:/applis# ls -l
total 4560
-rw-r--r--  1 root      root      4643365 mars   2  2015 download
drwx-----  2 www-data www-data   16384 juin  17 15:28 lost+found
drwxr-xr-x 11 www-data www-data   4096 juin  20 00:59 phpipam
```

Une fois cela fait on va décompresser le fichier teemip-2.0.2.zip :

```
root@Ipams:/applis# unzip teemip-2.0.2.zip -d teemip
```

On va maintenant créer un Virtual Host pour TeemIP, pour cela on prend le 000-default.conf d'apache, et on le copie et on donne pour nom au fichier teemip.conf

Dans ce fichier on va changer le port, le document Root et on va rajouter une balise directory :

```
<VirtualHost *:8081>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /applis/teemip/web

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

<Directory /applis/teemip>
    Options Indexes FollowSymLinks Multiviews
    AllowOverride all
    Require all granted
</Directory>

ErrorLog ${APACHE_LOG_DIR}/teemip_error.log
CustomLog ${APACHE_LOG_DIR}/teemip_access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

On va aussi devoir changer les droits du répertoire TeemIP qui est dans notre /applis/teemip, ils sont actuellement en root:root puisque le répertoire a été créé par moi-même en tant que root.

Pensez donc à mettre www-data :

```
chown -R www-data:www-data /applis/teemip/
```

```
drwxr-xr-x 3 www-data www-data 4096 juin 20 15:05 teemip
```

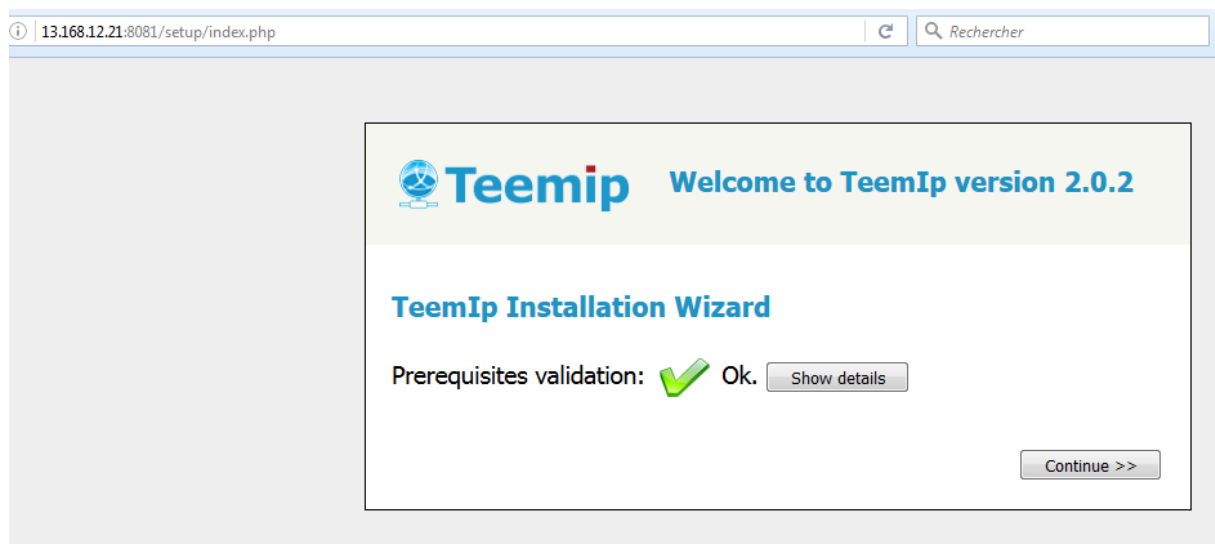
Une fois tout cela fait, on va pouvoir accéder à la configuration de TeemIP via le navigateur.

On peut donc mettre simplement :

**13.168.12.21 :8081**

On va tomber directement dessus car on **configuré** TeemIP sur le **port 8081** et on a **spécifié le chemin de TeemIP** comme ceci : **/applis/teemip/web**

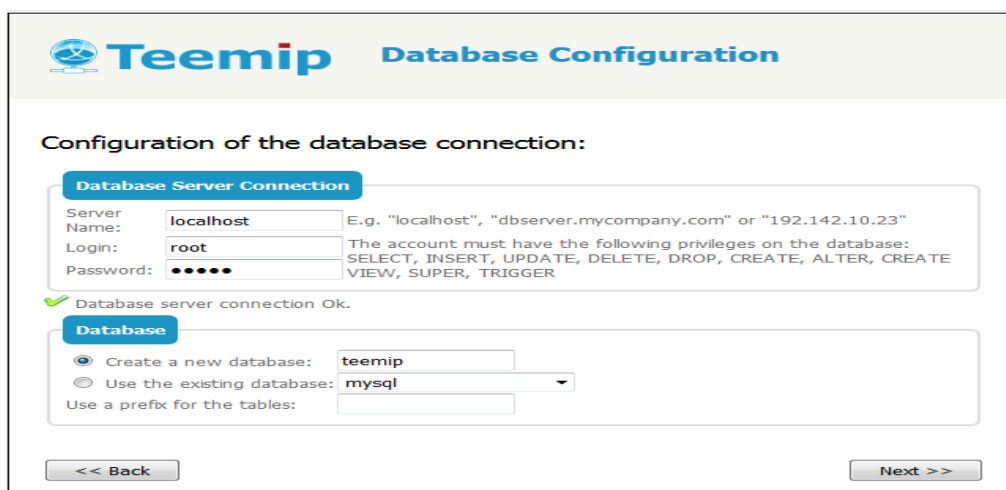
On arrive donc ici :



On nous dit que les **prérequis sont OK** et on va pouvoir passer à la suite.

Teemip nous demande ce qu'on veut faire on va choisir **installer un nouveau TeemIP**.

Il faut ensuite accepter **les termes de la licence**.

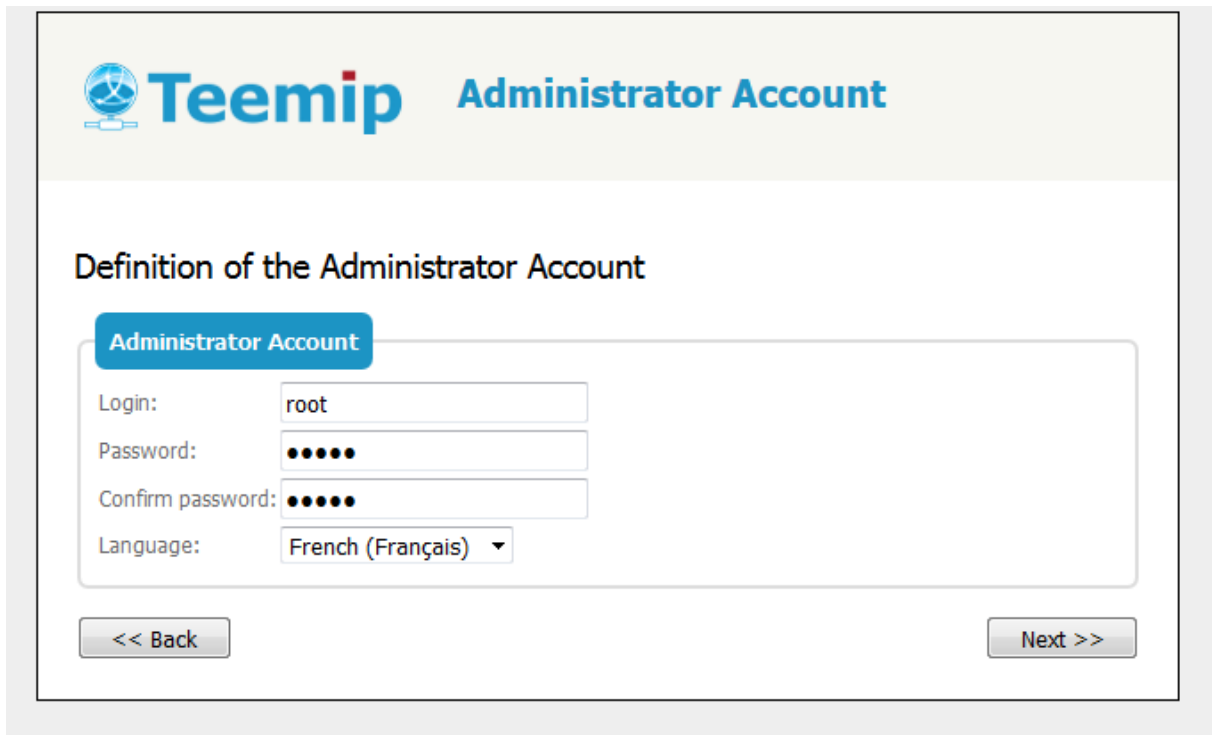




Voici la page de **configuration de teemip**.

On va ici définir le nom du serveur, j'ai ici mis localhost afin de pouvoir se connecter à teemip, a la maison comme au travail. On va de plus mettre l'identifiant et le mot de passe si on en a défini un de MySQL, et par la suite créer une nouvelle base de donnée avec bien sûr comme nom teemip.

On nous demande ensuite **d'administrer le compte de l'administrateur** :




The screenshot shows the 'Teemip Administrator Account' configuration page. The page title is 'Definition of the Administrator Account'. Below the title, there is a form with the following fields:

- Administrator Account** (Section header)
- Login:** root
- Password:** ●●●●
- Confirm password:** ●●●●
- Language:** French (Français) (dropdown menu)

At the bottom of the form, there are two buttons: '<< Back' on the left and 'Next >>' on the right.

On va ici mettre ID : root / MDP : Root1

On accède à une page afin de régler des **paramètres additionnel** :

 **Teemip** Miscellaneous Parameters


### Additional parameters


**Default Language**  
Default Language: French (Français) ▼

**Application URL**  
URL:   
Change the value above if the end-users will be accessing the application by another path due to a specific configuration of the web server.

**Sample Data**  
 I am installing a **demo or test** instance, populate the database with some demo data.  
 I am installing a **production** instance, create an empty database to start from.

On va choisir de faire une installation ‘production instance’ afin de mettre nos propres réseaux et de voir les étendues et les capacités et les defaults de teemip.

 **Teemip** Configuration Management options



The options below allow you to configure the type of elements that are to be managed inside TeemIp.

**Configuration Management Core**  
All the base objects that are mandatory in the TeemIp CMDB: Organizations, Locations, Teams, Persons, etc.

**End-User Devices**  
Manage devices related to end-users: PCs, Phones, Tablets, etc.

**Storage Devices**  
Manage storage devices such as NAS, SAN Switches, Tape Libraries and Tapes, etc.

**Virtualization**  
Manage Hypervisors, Virtual Machines and Farms.



## Decide whether you want to include a Helpdesk in TeemIP.



### Helpdesk

This option will enable the Helpdesk and the Portal modules.

Pour finir on arrive sur une page récapitulatif ou on peut installer ...

TeemIP est maintenant opérationnel, on va pouvoir cliquer sur enter TeemIP et faire nos test sur TeemIP et PHPipam afin de savoir quel IPAM est le mieux !

Notre but maintenant est de remplir ce tableau est d'avoir un gagnant entre les deux IPAM.

**Teemip Done**

**Manual operations required**

In order to complete the installation, the following manual operations are required:

- [Manual instructions for Tickets Management](#)

**Congratulations for installing TeemIp**

**Register now !**

**Get Professional Support**

**Get Professional Training**

**Enter Teemip**

IPAMs :	TeemIP	Phpipam
Discovery de l'infrastructure IP		Oui Si on veut de l'autodiscover automatiquement ( <a href="https://sourceforge.net/p/phpipam/bugs/280/">https://sourceforge.net/p/phpipam/bugs/280/</a> )
Gestion des plages, multi clients (distinction des clients)		Oui
Gestion des plages et sous plage		Oui
Granularité des droits		4 Choix de droits (na / ro / rw /rwa)
Gestion des VLAN ID		Oui
Import d'information manuel	oui	Oui
Nat : Vlan source /cible, l'équipement qu'il porte		Module Nat disponible ( <a href="https://github.com/phpipam/phpipam/blob/master/misc/Roadmap">https://github.com/phpipam/phpipam/blob/master/misc/Roadmap</a> )
Filtrage des adresses macs		Oui
Baux		
Exclusions		Oui grâce à un Tag « Exclus »
Gestion DNS / reverse DNS		Oui
Gestion de VIP (adresse IP Virtuelle)		
Gestion des routes		Champ customizable afin d'écrire des notes
Gestion de champs pour l'IPphone (Ex : Serveur http)	oui	Possibilité de rajouter un field dans les options et d'avoir une case de description. Qui est ensuite
Module Serveur DNS		Module DNS a Enable

