2021

Compte rendue globale

AYOUB BELBACHIR

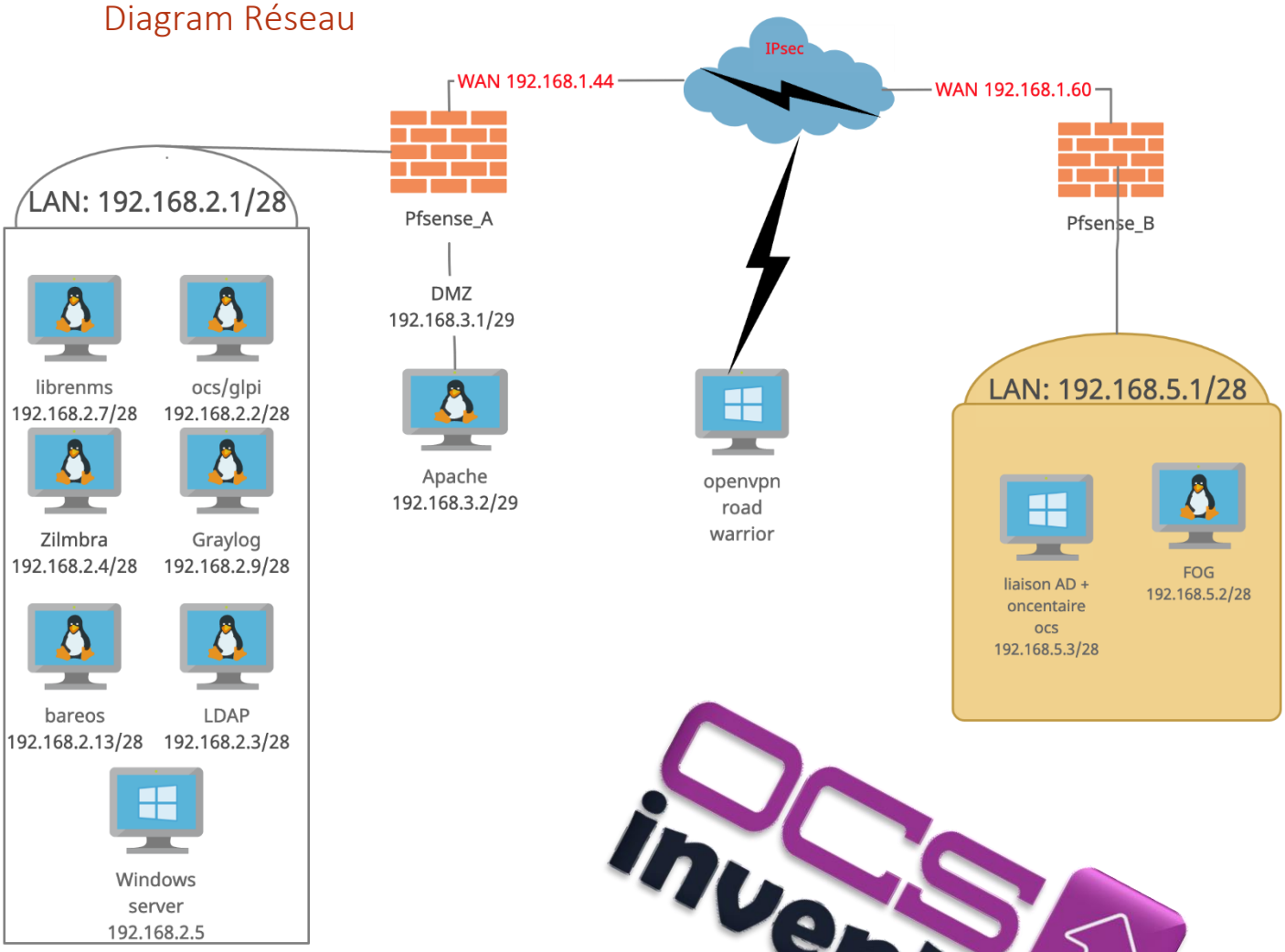
ITIC PARIS |BTS SIO SISR

Ayoub Belbachir

Sommaire

Ayoub Belbachir

Diagram Réseau



Ayoub Belbachir

Mise en Contexte

Pour notre projet de fin d'année Nous allons mettre en place un parc informatique avec plusieurs outils d'administration internet

Prérequis :

Un ordinateur performant (sous Windows de préférence) avec 200GO de place disponible, 16 Go de RAM ou plus, un processeur cadencer à 3,5 GHz ou plus.

L'ISO officielle de Pfsense (architecture amd64, on cherche à l'émuler pas à l'installer sur une Appliance netgate) ainsi que l'iso officielle de Windows 10 (x64 bits)

Virtual Box, ainsi que les VM suivante :

7 Ubuntu Server 20.04 LTS:

- 1 GHz processeur ou plus
- 15 Go d'espace libre sur le disque dur
- 1.5 Go de mémoire RAM

1 Ubuntu Server 18.04 LTS:

- 1 GHz processeur ou plus
- 10 Go d'espace libre sur le disque dur
  1.5 Go de mémoire RAM

2 Windows server (Active directory)

- Une RAM de 2 Go ou plus
- Un espace disque disponible de 40 Go
- 1,5 gigahertz (GHz) ou plus rapide
- Domain=samodigi.lan
- NetBIOS=samo

Ayoub Belbachir

Installation de pfsense et de Windows server

Mise en Contexte

Pfsense est un pare-feu (pare-feu) open source basée sur le système d'exploitation FreeBSD, Mise en place du firewall pour une protection optimale contre les malwares ou d'autres appareils qui partagent la même connexion et peuvent contaminer le réseau, nous permet de configurer l'accès réseaux, Windows server nous servira aussi à accéder au WebUI de pfsense

Tutoriel:

Dans VirtualBox Création du nouvel environnement ; attribution du nom "Pfsense", type "BSD[1]", Version [1]FreeBSD (64-bits). (Cette étape serre à renseigner à Virtual box le type de noyaux et l'architecture de notre OS, afin de crée un environnement fonctionnel à notre os)

Allouer de la mémoire vive à la machine virtuelle (1,5go selon vos préférences), création d'un disque dur virtuel (8go) en VDI (le VDI est le format natif de VirtualBox dans ce contexte nous n'avons pas besoin d'utiliser cette VM avec d'autres logiciel de verticalisation.)

Insertion de l'ISO de Pfsense ; aller dans configuration > Stockage > Pfsense > clique sur "vide " >  > "Choose a disk file "> puis sélectionner l'iso Pfsense télécharger précédemment.

Configurer une 2éme carte réseau ; aller dans configuration > Réseau > Adapter 2 > cocher la case "Activer l'interface réseau", mode d'accès réseau en réseau interne à nom écrive intnetlan, cliquer sur avancer mode de promiscuité en "Allow VMs" et configurer la premier carte réseau en mode d'accès réseau en réseau "NAT" (Cette étape nous permet de permettre au V.M de communiquer entre elle).

Configurer une 3éme carte réseau(opt1) : aller dans configuration > Réseau > Adapter 3 > cocher la case "Activer l'interface réseau", mode d'accès réseau en réseau interne à nom écrive intnetcaptif, cliquer sur avancer sélectionner un type d'interface diffèrent de celui d'adaptateur 2 si possible, mode de promiscuité en "Allow VMs"

Création d'un nouvel environnement ; attribution du nom "Windows Server" Virtual Box vas lui-même assigner automatiquement un type "Microsoft Windows" ainsi que la version "Windows 2016 (64-bit)" dans le cas contraire faite le vous-même Allouer de la mémoire vive à la machine virtuelle (3go selon vos préférences et votre matériel), création d'un disque dur virtuel (50go) en VDI. Configurer la 1e carte réseau en mode d'accès réseau en réseau interne et changer le nom en "intnetlan",

Lancer la V.M Pfsense, la navigation de l'installation se fait à l'aide des flèches du clavier, de la touche tabulation, d'espace pour cocher/décocher et entrer pour valider.

Accepter des droits d'auteur, sélectionner Install, sélectionner votre type de clavier, type de partition UFS (ce type de partition et propre à Unix sa particularité est qu'il crée plusieurs parties dont une pour grub (la partions boot d'amorçage). Ne redémarrer pas ouvrer Shell et taper la commande "Init 0" pour éteindre proprement votre machine, retiré ensuite l'iso (dans configuration > stockage) afin que votre machine ne s'amorce pas sur le CD indéfiniment.

[1] BSD=Berkeley Software Distribution (dérivé d'Unix)

Ayoub Belbachir

Lacer la V.M Windows 10 faite une installation personnaliser en sélection la partions cliquer sur nouveau et suivent une fois l'installation terminer retirer le cd.

Démarrer la V.M Windows 10, Lors du premier démarrage nous allons renseigner notre pays, notre type de clavier (qwerty pour moi), un nom d'utilisateur et nous connecter au wifi nous allons ensuite mettre ajours les driver pour une meilleur stabilité et optimisation de la machine. Une foi terminer la machine est prêt à l'utilisation. (Windows nous oblige à renseigner ou créé une adresse Outlook pour bypass il suffit de désactiver le wifi et de passer l'étape).

On sait que l'interface n°1 sera WAN celle qui est connectée au wifi. L'interface n°2 sera la LAN en réseau interne et qui l'administrateur de mon Pfsense Windows 10 ainsi que OPT1 pour la DMZ pour l'interface qui servira à accueillir notre site internet. Lacer la V.M Pfsense

Premier démarrage de la VM Pfsense, Paramétrage de la vlan laisser par défaut taper "n" pour la WAN taper " em0" pour le LAN taper "le0" et pour opt1 taper em2 ensuite taper "y" Pfsense va démarrer différent service dons le pare-feu un DNS et un service DHCP, paramétrage de l'adresse IP du LAN entré l'option "2" puis l'option "2"

Entrer l'adresse ip de votre choix (192.168.2.1) entrer ensuite le sous réseau qui lui correspond le CIDR (28) appuyer ensuite 2 fois sur entrer pour passer les étapes activer le DHCP, définir la plage d'adressage IP du DHCP (192.168.2.2 à 192.168.2.14), activer ensuite le protocole de configuration web

Paramétrage de l'adresse IP de opt1 entré l'option "2" puis l'option "3"

Entrer l'adresse ip de votre choix (192.168.4.1) entrer ensuite le sous réseau qui lui correspond le CIDR (29) appuyer ensuite 2 fois sur entrer pour passer les étapes activer le DHCP, définir la plage d'adressage IP du DHCP (192.168.3.2 à 192.168.3.4), activer ensuite le protocole de configuration web

Mode opératoire :

Rendez-vous sur votre V.M Windows server ouvrir le cmd taper les commandes suivantes ; "ipconfig /revise" puis" ipconfig /renew" Ouvre un navigateur (Firefox de préférence) entrer l'adresse ip que vous avez attribuer à votre Lan (192.168.2.1) connecter vous a l'interface web de Pfsense (utilisateur : admin, mot de passe : pfsense) saisir le DNS public de google 8.8.8.8 et 8.8.4.4, sélectionner le fuseau horaire (Europe paris), changer le mot de passe par défaut. Vérifier les maj. Ajouter le widget trafic graphe pour voir si pfsense détecte la fluctuation de donner entrant et sortant de notre V.M Windows, dans Dashboard appuyer sur l'Icon + et cliquer sur "trafic graphe".

Lancer un test de connexion sur Nperf on peut observer que la courbe de débit montant et descendent fluctue

Enfin ajouter un outil de gestion de disque de VM à Pfsense aller dans "System" > "Package Manager" > " Available Package" puis chercher "Open-VM-Tools" cliquer sur l'icône 

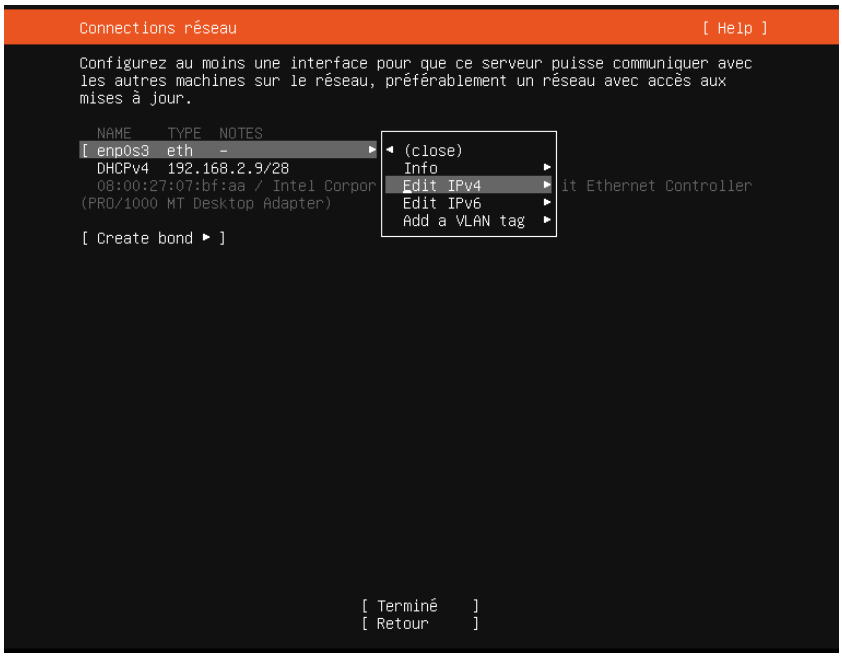
Nous allons renommer opt1 en DMZ interface>Opt1 renommer en DMZ

Dernière vérification sur le cmd de votre V.M pinger google.com pour vérifier notre connexion internet ; "ping goole.com"

Ayoub Belbachir

Ubuntu server adressage ip static

Lors de chaque installation de Ubuntu server nous allons paramétrer ladresse ip de la machine en statique



Ayoub Belbachir

Installation de ocs inventory

Mise en Contexte

OCS Inventory NG soit Open Computer and Software Inventory est une application permettant de réaliser un inventaire sur la configuration matérielle des machines du réseau, sur les logiciels qui y sont installés et de visualiser ces informations grâce à une interface web.

Tutoriel:

Télécharger les informations des packages source et mise à jour des paquets

- sudo apt-get update
- sudo apt-get upgrade

S'inscrire sur le site de ocs inventory

Télécharger le fichier tar.gz sur Ubuntu server

- Wget https://github.com/OCSInventory-NG/OCSInventory-ocsreports/releases/download/2.9/OCSNG_UNIX_SERVER-2.9.tar.gz

Décompresser avec la commande

- tar -xzf OCSNG_UNIX_SERVER-2.9.tar.gz
- cd OCSNG_UNIX_SERVER-2.9.tar.gz

Installation de maria dB pour crée une base de données et installation de apache2 pour le serveur web

- sudo apt install apache2 mariadb-client

Création d'une base de donner osc :

- sudo mysql -u root -p
- CREATE DATABASE ocs;

GRANT ALL PRIVILEGES ON ocs.* TO ocs_user IDENTIFIED BY "Notre mdp";
FLUSH PRIVILEGES;
Pour une configuration plus rapide nous allons renseigner les infos de la base de donner au fichier d'installation : sudo nano **setup.sh**
Ensuite Renseigner les infos correspondantes au ligne suivante selon notre base de donner

- DB_SERVER_HOST="localhost"
- DB_SERVER_PORT="3306"
- DB_SERVER_USER="ocs_user"
- DB_SERVER_PWD="strongpassword"

Lancée l'installation avec la commande

- sudo ./setup.sh

L'installation ne fonctionne pas il manque des modules

Installation des module perl manquante suivant ;

XML::Simple, Compress::Zli, DBD::mysql, DBI, Apache::DBI, Net::IP, SOAP::Lite

Création de lien symbolique avec la commande

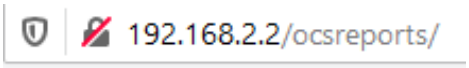
- sudo ln -s /etc/apache2/sites-enabled/ocsinventory-reports.conf /etc/apache2/sites-enabled/ocsreports.conf
- sudo ln -s /etc/apache2/sites-enabled/ocsinventory-reports.conf /etc/apache2/sites-enabled/ocsreports.conf”

Redémarrage de apache2 avec la commande

- /etc/init. d/apache2 restart

Mode opératoire :

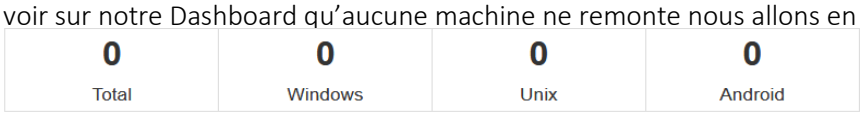
Ouvrir une page internet avec come url ”http ://adresse-ip-Ubuntu-serveur/ocsreports/ ”



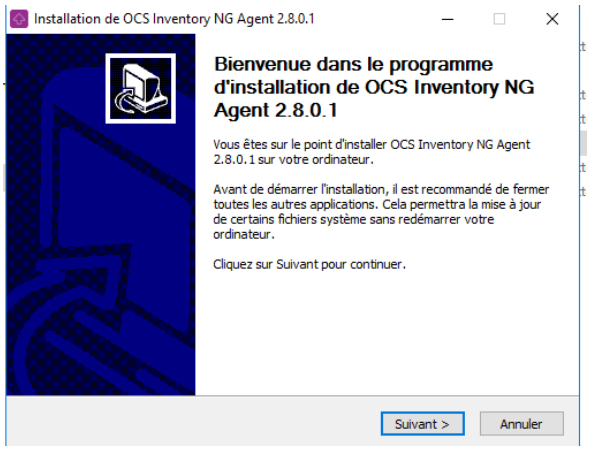
Renseigner ensuite les infos inscrites durant l’étape 7 si demander

Saisir comme login : admin et comme mot de passe : admin

Nous pouvons voir sur notre Dashboard qu’aucune machine ne remonte nous allons en ajouter une

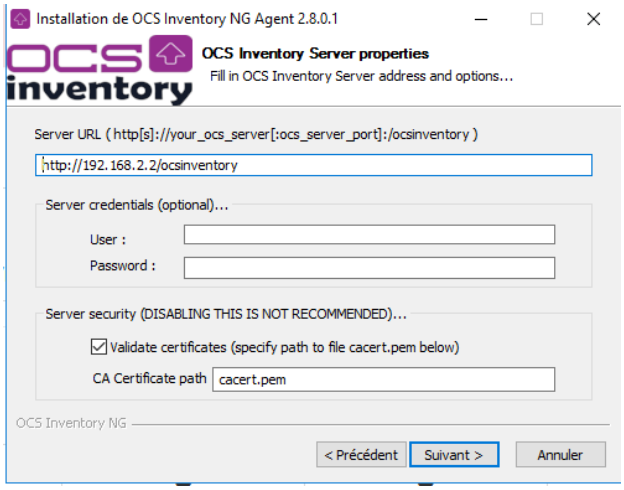


Pour se faire nous allons installer l’agent ocs inventory officiel sur notre Windows server



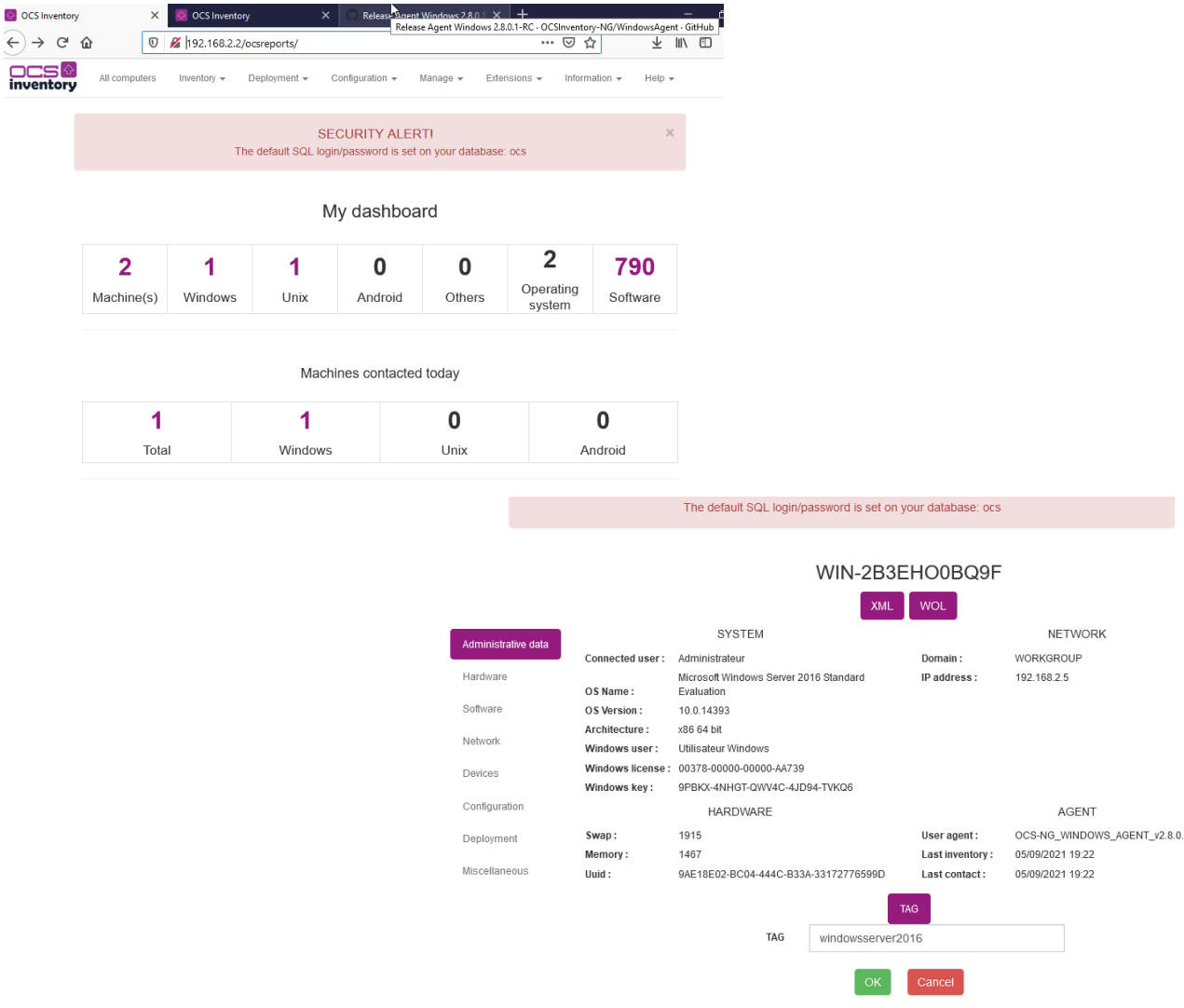
Cliquer 2 foi sur suivant puis à server url renseigner ”http ://adresse-ip-Ubuntu-serveur/ocsinventory”

Ayoub Belbachir



Cliquer 2 foi sur suivant puis cocher la premier et la seconde case, la première permet d'avoir les log la seconde remonter Windows server après l'installation vous pouvez aussi spécifier un tag ce qui permet de mieux reconnaitre ses machines

L'agents ocs à bien remonter les informations



Ayoub Belbachir

Mis en place de l'agent sur une VM Ubuntu Server

Pour cela tapez les commandes suivantes :

- ≥ sudo apt-get update
- ≥ sudo apt-get upgrade

Une fois la mise à jour terminé nous allons installer l'agent OCS Inventory Agent, pour cela taper ceci :

- ≥ sudo apt-get install ocsinventory-agent

Une fois le téléchargement et l'installation terminée, vous arriverez une fenêtre : choisissez la méthode HTTP puis presser « Entrer »

- ≥ sudo ocsinventory-agent

6	1	5	0	0	4	1856
Machine(s)	Windows	Unix	Android	Others	Operating system	Software

Machines contacted today

5	1	4	0
Total	Windows	Unix	Android

Statistics

Ayoub Belbachir

Installation de Glpi et liaison ocs

Mise en Contexte

GLPI est un logiciel libre de gestion des services informatiques et de gestion des services d'assistance GLPI est une application web qui aide les entreprises à gérer leur système d'information. Parmi ses caractéristiques, cette solution est capable de construire un inventaire de toutes les ressources de la société et de réaliser la gestion des tâches administratives et financières. Les fonctionnalités de cette solution aident les Administrateurs IT à créer une base de données regroupant des ressources techniques et de gestion, ainsi qu'un historique des actions de maintenance.

Tutoriel:

Nous pouvons installer l'outil GLPI sur la VM de OCS inventory

Creation d'une base de donner:

- sudo mysql -u root -p
- CREATE DATABASE glpi;
- CREATE USER 'glpiuser'@'localhost' IDENTIFIED BY '159898';
- GRANT ALL PRIVILEGES ON glpiuser.* TO 'glpi'@'%';
- FLUSH PRIVILEGES;
- quit;

Installation des dependences necessaire:

- sudo apt-get install apache2 php php-mysql libapache2-mod
- `sudo apt-get install php-json php-gd php-curl php-mbstring php-cas`
- `sudo apt-get install php-xml php-cli php-imap php-ldap php-xmlrpc php-apcu`

Activer le module a2enmod :

- sudo a2enmod rewrite
- sudo systemctl restart apache2

Télécharger et decompresser glpi dans le fichier temporaire de Ubuntu /tmp

- cd /tmp
- wget https://github.com/glpi-project/glpi/releases/download/9.5.5/glpi-9.5.5.tgz
- tar -zxvf glpi-9.5.5.tgz

Déplacez le dossier GLPI dans le répertoire racine d'Apache :

- sudo mv glpi /var/www/html/

Donnez à l'utilisateur www-data le contrôle total sur le répertoire GLPI et ses fichiers :

- sudo chown -R www-data /var/www/html/glpi

Créez un fichier de configuration Apache nommé glpi.conf et insérez le texte suivant :

- sudo nano /etc/apache2/conf-available/glpi.conf
- <Directory /var/www/html/glpi>
  AllowOverride All
  </Directory>
  <Directory /var/www/html/glpi/config>
  Options -Indexes
  </Directory>
  <Directory /var/www/html/glpi/files>
  Options -Indexes
  </Directory>

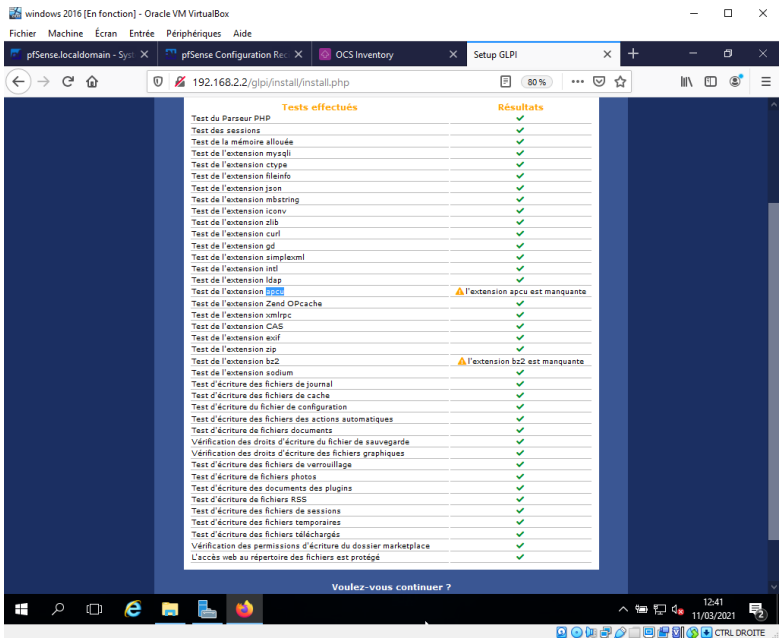
Activez la configuration et redémarrez le serveur Apache :

- sudo a2enconf glpi
- sudo systemctl reload apache2
- sudo service apache2 restart

Mode opératoire :

Ouvrir une page internet avec come url ”http ://adresse-ip-Ubuntu-serveur/glpi ”

Sélectionnez la langue, acceptez les termes de la licence, Cliquez sur le bouton Installer, vérifier le résultat de tous les tests, puis cliquez sur Continuer :



Renseignez les informations de connexion MySQL pour vous connectez à la base de données GLPI, sélectionnez la base de données glpi, créée dans une étape plus haut, une fois la base initialisée, cliquez sur Continuer, prenez note des identifiants par défaut, cliquez sur Utiliser GLPI, entrez le compte et mot de passe glpi/glpi

Sur la console Linux, supprimez le fichier d’installation de GLPI.

- sudo rm /var/www/html/glpi/install/install.php

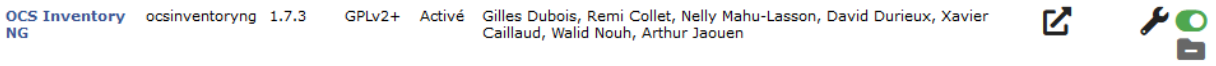
l ne me reste plus qu'à ajouter le plugin OCS Inventory dans GLPI, rendons nous dans le répertoire des plugins GLPI et télécharger le plugin

- cd /var/www/html/glpi/plugins
- sudo wget https://github.com/pluginsGLPI/ocsinventoryng/releases/download/1.7.3/glpi-ocsinventoryng-1.7.3.tar.gz

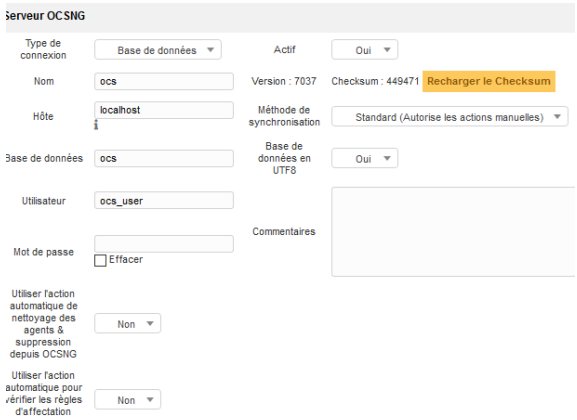
Décompresser le :

- tar -xzvf glpi-ocsinventoryng-1.7.3.tar.gz

Rendez-vous maintenant dans le menu Configuration> Plugin, Je clique sur Installer, puis activer.

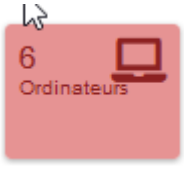


Ensuite, je vais dans le menu Outils > OCS Inventory NG et je clique sur la clé à molette je clique sur Serveurs OCSNG, Puis je clique sur le + et je renseigne les champs suivants :



Cliquez ensuite sur sauvegarder rendez-vous ensuite dans le menu Configuration puis cliquez sur OCS inventory NG dans l'onglet Outils, cliquez ensuite sur importation de nouveaux ordinateurs

Cliquez ensuite sur importer



Ayoub Belbachir

Installation de Graylog

Mise en Contexte

Graylog apporte des réponses aux questions de sécurité, d'application et d'infrastructure informatique de votre équipe en vous permettant de combiner, d'enrichir, de corréler, d'interroger et de visualiser toutes vos données de logs en un seul endroit.

Tutoriel:

Mise à jour des paquets, installation de dépendance nécessaire à Graylog et installation de pwgen (générateur de clé) :

- sudo apt update
- sudo apt install apt-transport-https pwgen
- sudo apt install openjdk-11-jre-headless

Importer la clé GPG du référentiel, exécutez la commande ci-dessous :

- wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add –

Ensuite, ajoutez le référentiel Elasticsearch au système :

- sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.list'

Maintenant, mettez à jour le référentiel et installez Elasticsearch :

- sudo apt update
- sudo apt install elasticsearch

Pour permettre au service de démarrer au démarrage, exécutez les commandes ci-dessous. :

- systemctl daemon-reload
- systemctl start elasticsearch.service
- systemctl enable elasticsearch.service

Modifiez le fichier de configuration Elasticsearch pour définir le nom du cluster pour Graylog :

- sudo nano /etc/elasticsearch/elasticsearch.yml

Modifier les paramètres ci-dessous.

- cluster.name: graylog
  network.host: 127.0.0.1
  action.auto_create_index: false

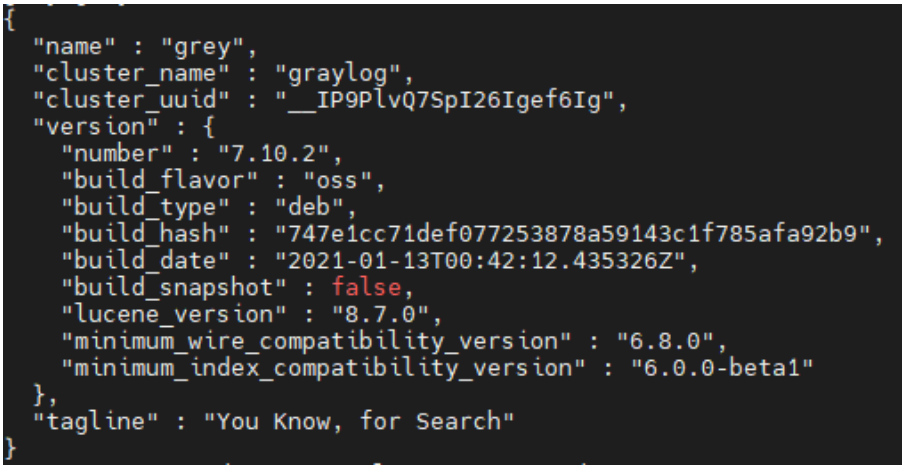
Enregistrez le fichier et quittez. Redémarrez maintenant le service comme indiqué ci-dessous :

- systemctl restart elasticsearch.service
- systemctl status elasticsearch.service

Pour vérifier qu'Elasticsearch est en cours d'exécution, exécutez la commande ci-dessous :

- curl -X GET "localhost:9200/"

nous avons le résultat suivant :



Mongodb est une base de données pour stocker la configuration du graylog. Vous pouvez l'installer avec apt repo comme indiqué ci-dessous :

- apt update
- apt install mongodb-server

Une fois que mongodb est installé, démarrez le service MongoDB et activez-le au démarrage :

- systemctl start mongodb
- systemctl enable mongodb
- systemctl status mongodb

Graylog n'est pas disponible dans le référentiel par défaut, vous devez télécharger et installer le référentiel, puis installer Graylog :

- wget https://packages.graylog2.org/repo/packages/graylog-4.0-repository_latest.deb
- sudo dpkg -i graylog-3.3-repository_latest.deb

Une fois le référentiel installé, mettez à jour le cache du référentiel et installez Graylog :

- apt update
- apt install graylog-server

Noter aussi l'adresse ip de Ubuntu :

- ip a

Une fois graylog installé, vous devez générer une clé secrète pour Graylog que vous allez copier (cette clé correspond au password_secret présent dans /etc/graylog/server/server.conf) :

- pwgen -N 1 -s 96

Maintenant, générez un mot de passe de hachage (sha256) pour l'utilisateur root (mot de passe administrateur graylog (cette clé correspond au root_password présent dans /etc/graylog/server/server.conf). Remplacez le 'mot_de_passe' par votre propre mot de passe administrateur :

- echo -n 'mot_de_passe' | sha256sum

Ensuite, modifiez le fichier server.conf :

sudo nano /etc/graylog/server/server.conf

Ajoutez-y les clés générer aux emplacements correspondants,

Et modifiez également la ligne http_bind_address et http_publish_uri pour accéder à l'interface Web. :

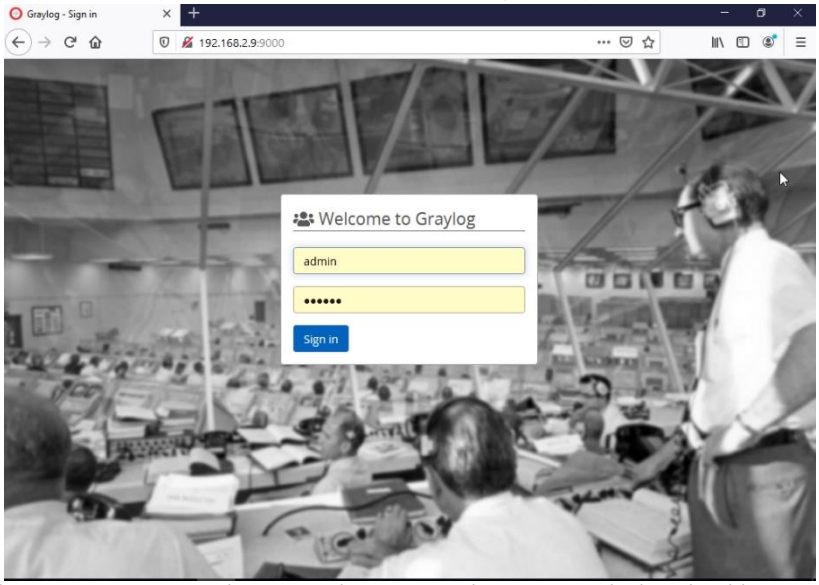
- http_bind_address = adress_ip:9000
  http_publish_uri = http://adresse_ip:9000/

Enregistrer le fichier et quitter. Maintenant, démarrez et activez le service Graylog pour le démarrage automatique au redémarrage.

- sudo systemctl daemon-reload
- sudo systemctl start graylog-server
- sudo systemctl enable graylog-server

Mode opératoire :

L'interface web graylog écoutera sur le port 9000 par défaut, ouvrez votre navigateur préféré et accédez à http: // adresse_ip: 9000



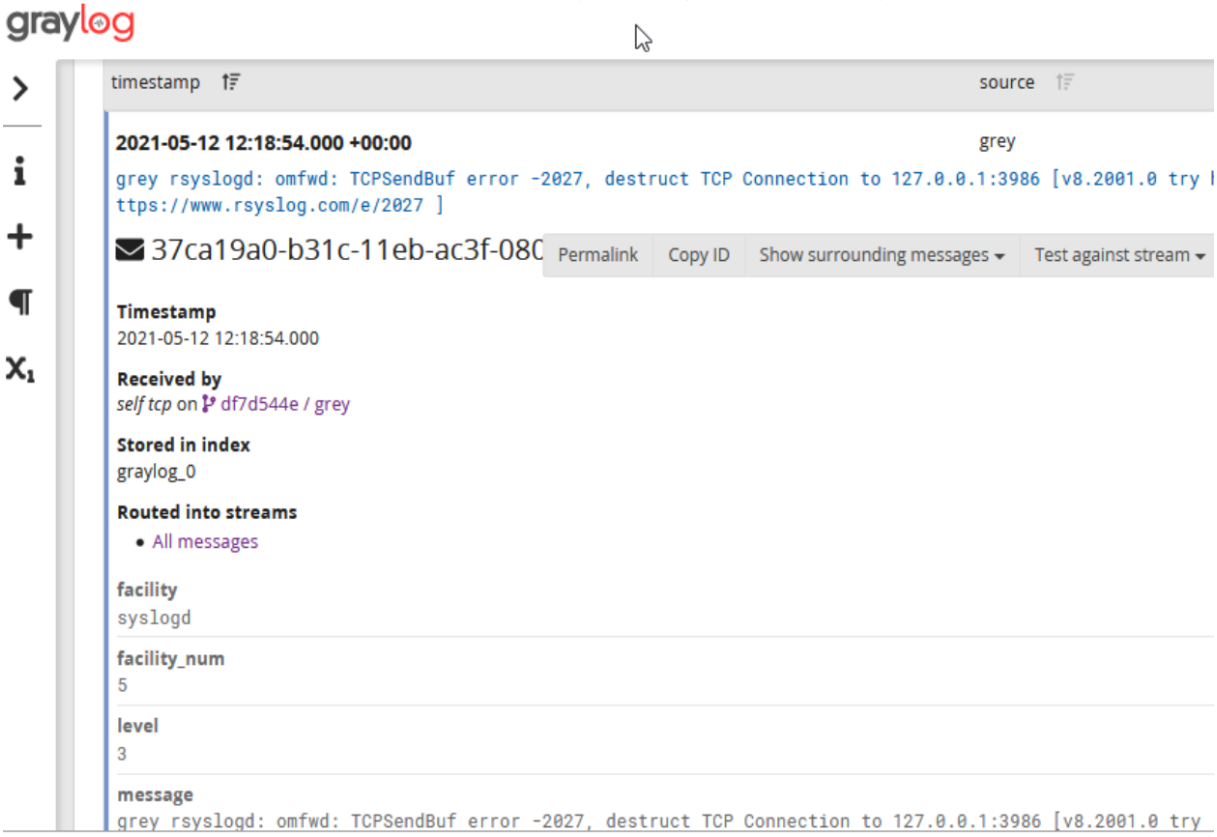
Le login et défaut est admin le mot de passe correspond au mot de passe utiliser pour générer la clé sha256sum
Nous allons mettre en place le self monitoring (autosurveillance) pour graylog
Dans le Webui rendez-vous dans system>inputs rechercher syslog tcp sélectionner le et cliquer sur launch new input
Lui attribuer un titre à bind adresse : 0.0.0.0 à port on peut sélectionner le port de notre choix, nous pouvons laisser les paramètres restants par default cliquer sur Save
Rendez-vous sur notre server graylog et modifier le fichier 90-graylog.conf :

- sudo nano /etc/rsyslog.d/90-graylog.conf

Ajoutez-y la ligne suivante :

- *.* @SERVER:5140;RSYSLOG_SyslogProtocol23Format

Sauvegarder les modifications, quitter et redémarré rsyslog :
sudo systemctl restart rsyslog
rendez-vous ensuite dans le Webui on constate que les logs son bien envoyer



Nous allons maintenant ajouter un agent nxlog sur notre Windows server de manière à ce que graylog reçoive les logs de Windows
Dans le Webui rendez-vous dans system>inputs rechercher GELF UDP sélectionner le et cliquer sur launch new input
Lui attribuer un titre, à bind adresse : 0.0.0.0 à port on peut sélectionner le port de notre choix, nous pouvons laisser les paramètres restants par default cliquer sur Save
Sur Windows server Télécharger l'agent nxlog et installer le
Rendez-vous dans le répertoire C:\Program Files (x86)\nxlog\conf
Est assigner la configuration suivante :

```
<Extension _gelf>
   Module     xm_gelf
</Extension>
<Extension _syslog>
   Module     xm_syslog
</Extension>
<Input win>
Module     im_msvistalog
</Input>
<Output graylog>
   Module     om_udp
   Host       adresse_ip_graylog
   Port       3519
   OutputType  GELF
</Output>
<Route graylog_routes
            Path win => graylog
</Route>
```

Ayoub Belbachir

Allez ensuite sur notre Windows server appuyer sur la touche "Windows" +R saisissez ensuite "services.msc" chercher le service nxlog et démarrer le.
Retourner sur le Webui, on peut voir que les logs de Windows son bien envoyer

All Messages

timestamp	source
2021-05-12 13:30:24.000 +00:00 Le service Microsoft Passport est entré dans l'état : en cou	WIN-2B3EHO0BQ9F
2021-05-12 13:30:24.000 +00:00 Fermeture de session d'un compte. Sujet : ID de sécurit	WIN-2B3EHO0BQ9F
2021-05-12 13:30:23.000 +00:00 L'ouverture de session d'un compte s'est correctement déroulée	WIN-2B3EHO0BQ9F

Ayoub Belbachir

Installation de librenms

Mise en Contexte

Librenms est un logiciel de surveillance de réseau basé sur PHP/MySQL/SNMP à découverte automatique qui inclut le support d'une large gamme de matériel réseau et de systèmes d'exploitation incluant Cisco, Linux, Juniper, Foundry, et bien d'autres.

Tutoriel:

Télécharger les informations des packages source et mise à jour des paquets

- sudo apt-get update
- sudo apt-get upgrade

Installer les modules et les dependence:

- sudo apt install -y curl composer fping git graphviz imagemagick mariadb-client mariadb-server mtr-tiny nginx-full nmap php7.3-cli php7.3-curl php7.3-fpm php7.3-gd php7.3-json php7.3-mbstring php7.3-mysql php7.3-snmp php7.3-xml php7.3-zip python-memcache python-mysqldb rrdtool snmp snmpd whois}

Modifier le fuseau horaire dans les fichiers suivant avec l'outil nano:

/etc/php/*/fpm/php.ini
/etc/php/*/cli/php.ini

```
date.timezone = Europe/Paris
```

redémarre php fpm: sudo systemctl restart php*-fpm.service

Ensuite on rentre dans le répertoire opt pour cloner le repository officiel

- cd /opt
- git clone https://github.com/librenms/librenms.git

Ensuite, créez un utilisateur qui gérera LibreNMS et ajoutez Nginx au groupe LibreNMS :

sudo useradd librenms -d /opt/librenms -M -r -s "$(which bash)"

Nous devrons modifier les autorisations de certains dossiers :

- sudo chown -R librenms:librenms /opt/librenms
- sudo setfacl -d -m g::rwx /opt/librenms/bootstrap/cache /opt/librenms/storage /opt/librenms/logs /opt/librenms/rrd
- sudo chmod -R ug=rwX /opt/librenms/bootstrap/cache /opt/librenms/storage /opt/librenms/logs /opt/librenms/rrd

Après cela, nous recevons un script PHP qui installera les dépendances du composeur. Pour exécuter cela, nous utiliserons la commande suivante. Pour exécuter ce script, nous devons passer à l'utilisateur Librenms :

- su - librenms
- cd / opt / librenms
- ./ scripts / composer_wrapper . php installation - no - dev
- Exit

Ensuite, nous devrons nous connecter à la console MariaDB et créer une base de données pour LibreNMS. Exécutez la commande suivante :

- mysql -u root -p
  CREATE DATABASE librenms CHARACTER SET utf8 COLLATE utf8_unicode_ci;
  CREATE USER 'librenms'@'localhost' IDENTIFIED BY mon_mot_de_passe';
  GRANT ALL PRIVILEGES ON librenms.* TO 'librenms'@'localhost';
  FLUSH PRIVILEGES;
  exit

Une fois cela fait, ouvrez le fichier de configuration MariaDB :

- sudo nano /etc/mysql/mariadb.conf.d/50-server.cnf

Ajoutez les lignes suivantes sous la section:[mysqld]

- innodb_file_per_table=1
  lower_case_table_names=0

Ensuite, sauvgarder le fichier modifier et redemarer le service mariadb :

- sudo systemctl restart mariadb

Puis définir un Vhost pour Nginx qui est à utiliser par LibreNMS:

- nano /etc/nginx/conf.d/librenms.conf

Ajoutez les lignes suivante :

```
server {
  listen      80;
  server_name librenms.idroot.us;
  root        /opt/librenms/html;
  index       index.php;

 charset utf-8;
 gzip on;
 gzip_types text/css
application/javascript text/javascript
application/x-javascript
image/svg+xml text/plain text/xsd
text/xsl text/xml image/x-icon;
 location / {
   try_files $uri $uri/
/index.php?$query_string;
  }
  location /api/v0 {
   try_files $uri $uri/
/api_v0.php?$query_string;
  }
  location ~ \.php {
   include fastcgi.conf;
   fastcgi_split_path_info
^(.+\.php)(/.+)$;
   fastcgi_pass
unix:/var/run/php/php7.4-fpm.sock;
  }
  location ~ /\.ht {
   deny all;
  }
 }
```

Sauvegarder le fichier modifier et redémarrer le service nging :

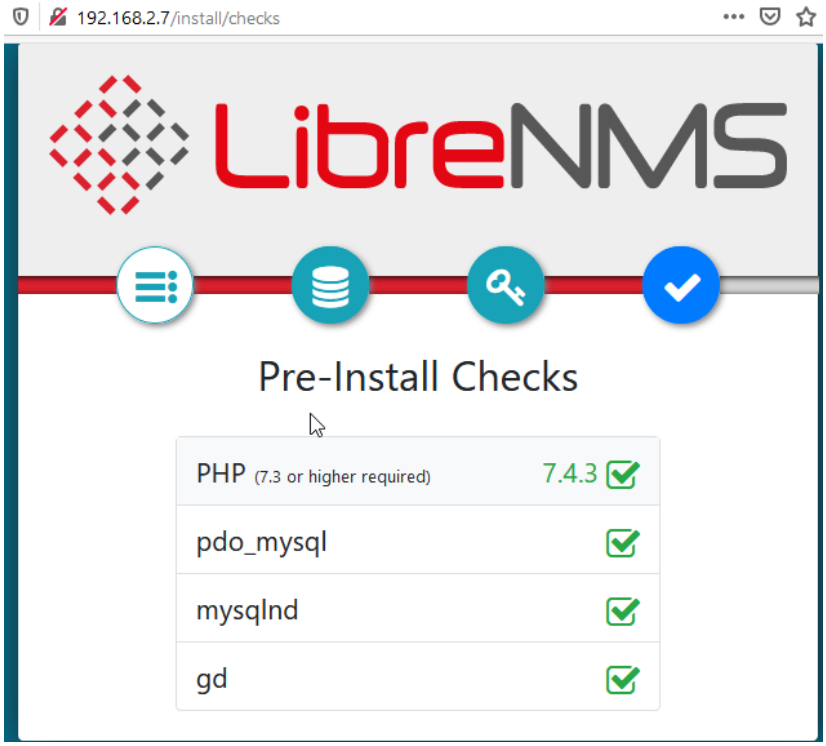
- sudo systemctl redémarrer nginx

Configurez le pare-feu :

- ufw allow 80/tcp
- ufw allow 443/tcp
- ufw reload

Mode opératoire :

Accéder au Webui (interface web graphique) de notre host librenms saisissez dans un navigateur l'adresse_ip_de_librenms/install.php
Si tous les modules son bien installer la page suivante s'affiche



cliquez sur l'icon en forme de base de donner résigner les informations saisies lors de la création de la base de donner cliquer ensuite sur Chek Credentiels puis sur Build Database
Pur déployer des agents sur Librenms il faut paramétrer pour chaque agent les Protocol SNMP (protocole simple de gestion de réseau) qui permet à l'agent de communiquer avec librenms.

Commençons par mètre un agent sur librenms lui-même

- sudo cp /opt/librenms/snmpd.conf.example /etc/snmp/snmpd.conf

Librenms on à juste copier l'exemple de configuration SNMP proposer dans le répertoire de librenms on va modifier le nom de communication par défaut qui est : RANDOMSTRINGGOESHERE
sudo nano /etc/snmp/snmpd.conf
Il est aussi conseiller de modifier la localisation du system : syslocation Paris
Ainsi que le contact du system : syscontact hostlibrenms

Ayoub Belbachir

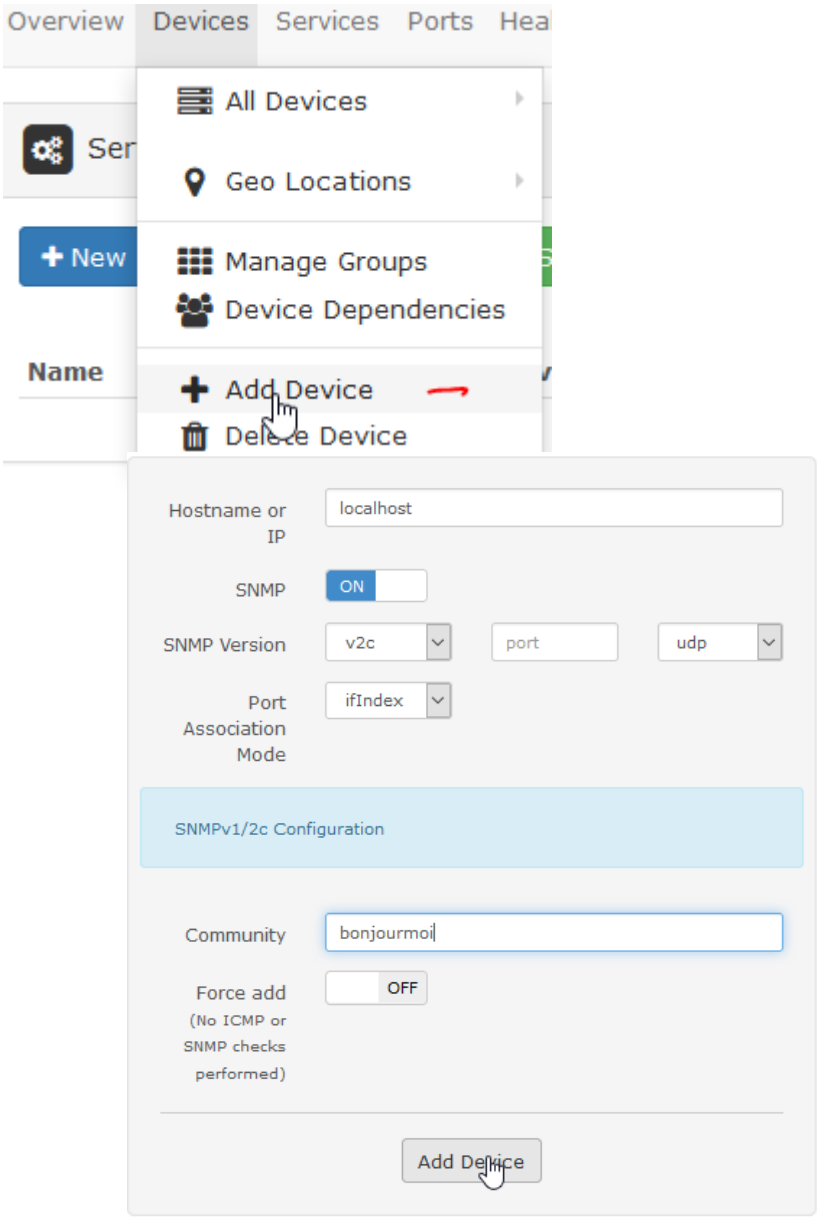
Pour mieux repérer notre machine, on va télécharger un script Shell pour aider à la détection de l'OS et redemarer SNMP :

sudo curl -o /usr/bin/distro https://raw.githubusercontent.com/librenms/librenms-agent/master/snmp/distro
sudo chmod +x /usr/bin/distro

sudo systemctl restart snmpd

Ensuite, nous allons ajouter librenms à la liste des machines :

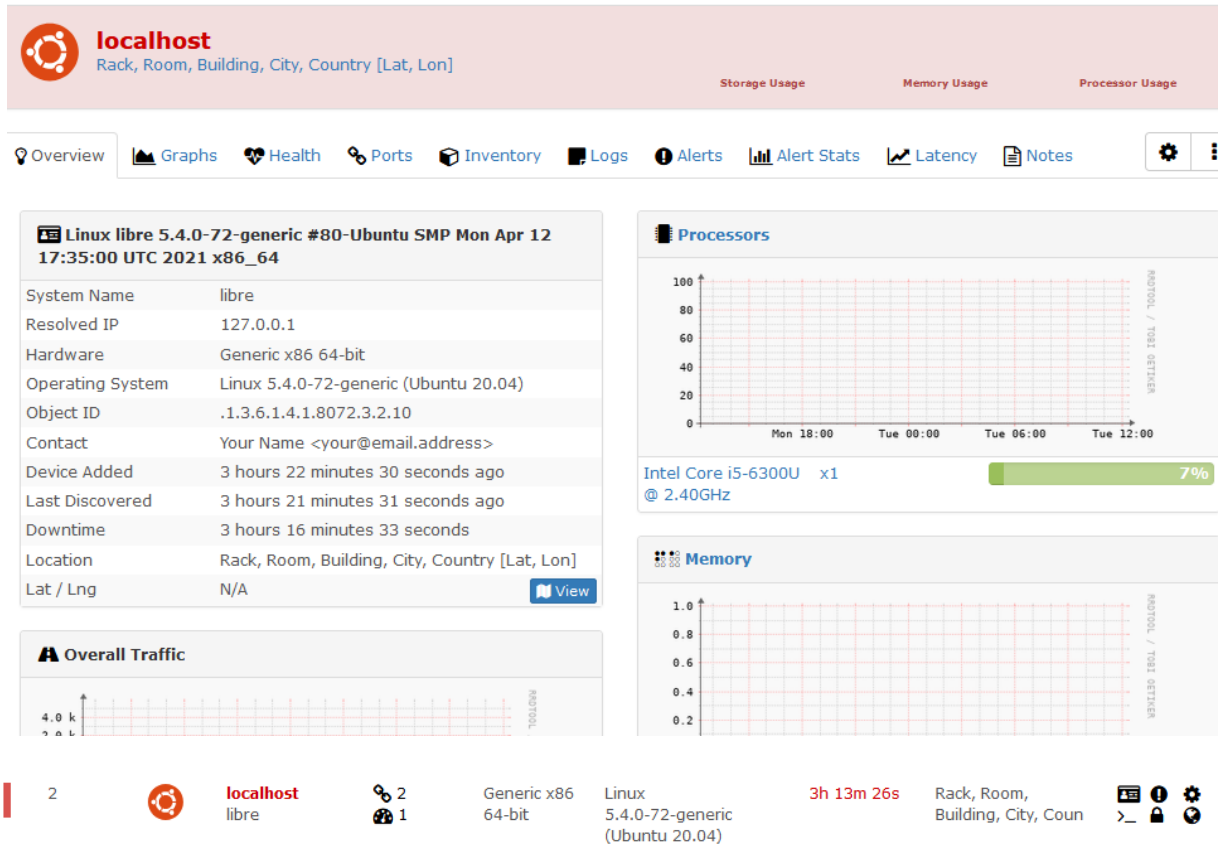
Ajouter un appareil



À Community inscrire le nom de communication (modifier lors de l'installation) de SNMP

Allez ensuite dans Devices > all Devices notre localhost

Ayoub Belbachir

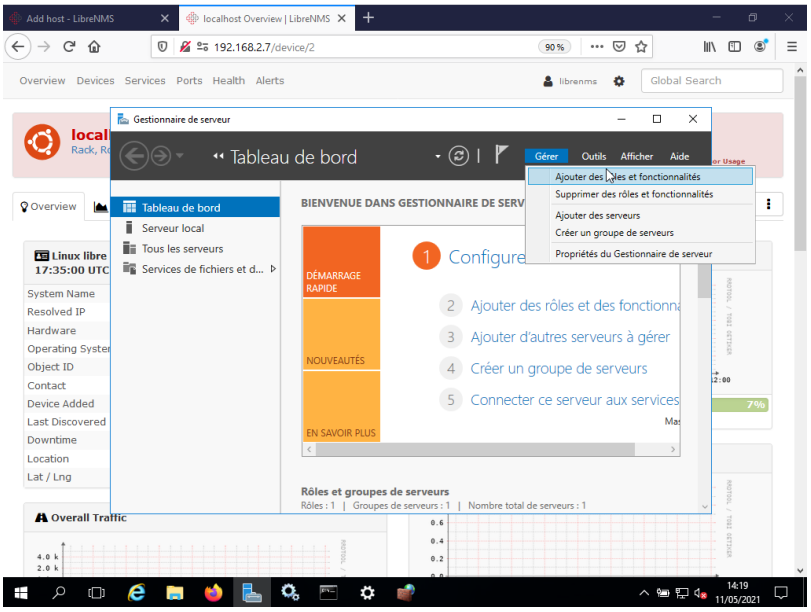


Notre appareil à était ajouter maintenant nous allons voir comment ajouter notre Windows server

Allez dans gestion du serveur cliquer sur gérer puis ajouter des rôles et des fonctionnalités

Aller dans fonctionnalité et la fonctionnalité SNMP, cliquer suivant puis installer

Retourner ensuite dans le gestionnaire de serveur, puis dans Pare-feu Windows

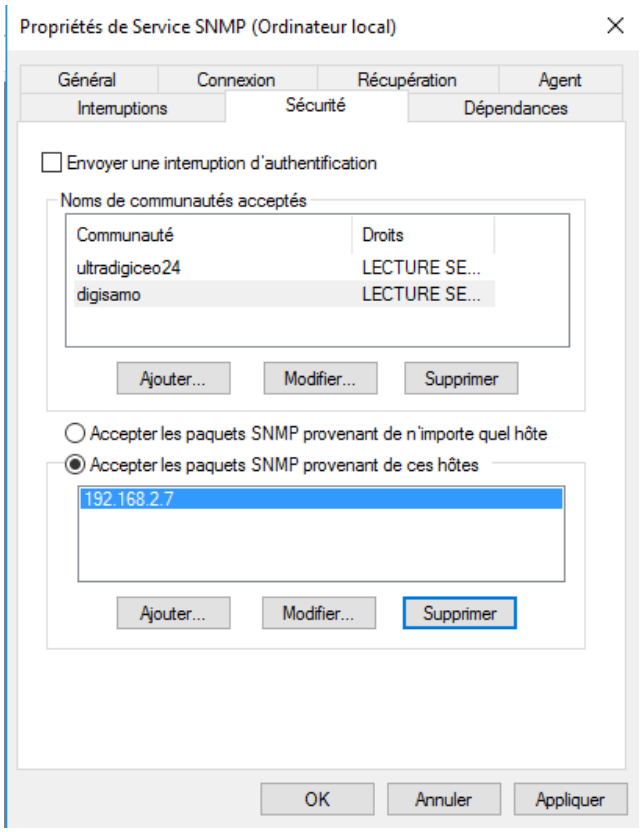


Ayoub Belbachir

Cliquer sur règle de trafic nous devons autoriser la réponse ping (ICMP) nous devons activer les règles contenantes suivante

Partage de fichiers et d'imprimantes (Demande d'écho ...	Partage de fichiers et d'impr...
Partage de fichiers et d'imprimantes (Demande d'écho ...	Partage de fichiers et d'impr...
Partage de fichiers et d'imprimantes (Demande d'écho ...	Partage de fichiers et d'impr...

Rendez-vous dans l'application Services cliquer sur « Service SNMP » aller dans agent puis renseigner le non de contact et l'emplacement de l'appareil cliquer ensuite sur sécurité ajouter un nom de communication en suite un hôte SNMP en ajoutent l'adresse ip de librenms



Rendez-vous sur le Webui de librenms ajouter un appareil dans host renseigner l'adresse IP de notre Windows server et le nom de communauté

4		192.168.2.5 win-2b3eho0bq9f	5	Intel x64	Microsoft Windows Server 2016 (NT 6.3) (Multiprocessor)	2h 41m 54s	digiland	
2		localhost libre	2 1	Generic x86 64-bit	Linux 5.4.0-72-generic (Ubuntu 20.04)	4h 7m 14s	Rack, Room, Building, City, Coun	

Notre Windows server à était ajouter et détecter par librenms.

Ayoub Belbachir

Installation de Zimbra

Mise en Contexte

Librenms est un logiciel de surveillance de réseau basé sur PHP/MySQL/SNMP à découverte automatique qui inclut le support d'une large gamme de matériel réseau et de systèmes d'exploitation incluant Cisco, Linux, Juniper, Foundry, et bien d'autres.

Tutoriel:

Mise à jour des paquets, installation de dépendance nécessaire à Graylog et installation de pwgen (générateur de clé) :

- sudo apt update
- sudo apt install -y build-essential net-tools curl git software-properties-common

attribution du nom host:

- sudo nano /etc/hosts

ajouter la ligne suivante

- 192.168.2.4 mail.mondomain92.com mail

Redémarre ubuntu puis telecharger Zimbra et decompresser le fichier

- wget https://files.zimbra.com/downloads/8.8.15_GA/zcs-8.8.15_GA_3869.UBUNTU18_64.20190918004220.tgz
- tar xvf zcs-8.8.15_GA_3869.UBUNTU18_64.20190918004220.tgz
- cd zcs*/

désactiver et arrêter l'outil system resolver

- sudo systemctl disable systemd-resolved ; systemctl stop systemd-resolved
- sudo rm /etc/resolv.conf ; echo "nameserver 8.8.8.8" > /etc/resolv.conf
- sudo apt update ; sudo apt-get install dnsmasq -y

ajouter les lignes suivante dans se fichier /etc/dnsmasq.conf :

- server=8.8.8.8
  listen-address=127.0.0.1
  domain=mondomain92.com
  mx-host=mondomain92.com, mail.mondomain92.com,0
  address=/mail.mondomain92.com/192.168.1.4

redémarre l'outil dnsmasq ajout de la clée et installation

- sudo systemctl restart dnsmasq ; systemctl status dnsmasq
- sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 9BE6ED79
- sudo apt update
- ./install.sh --platform-override

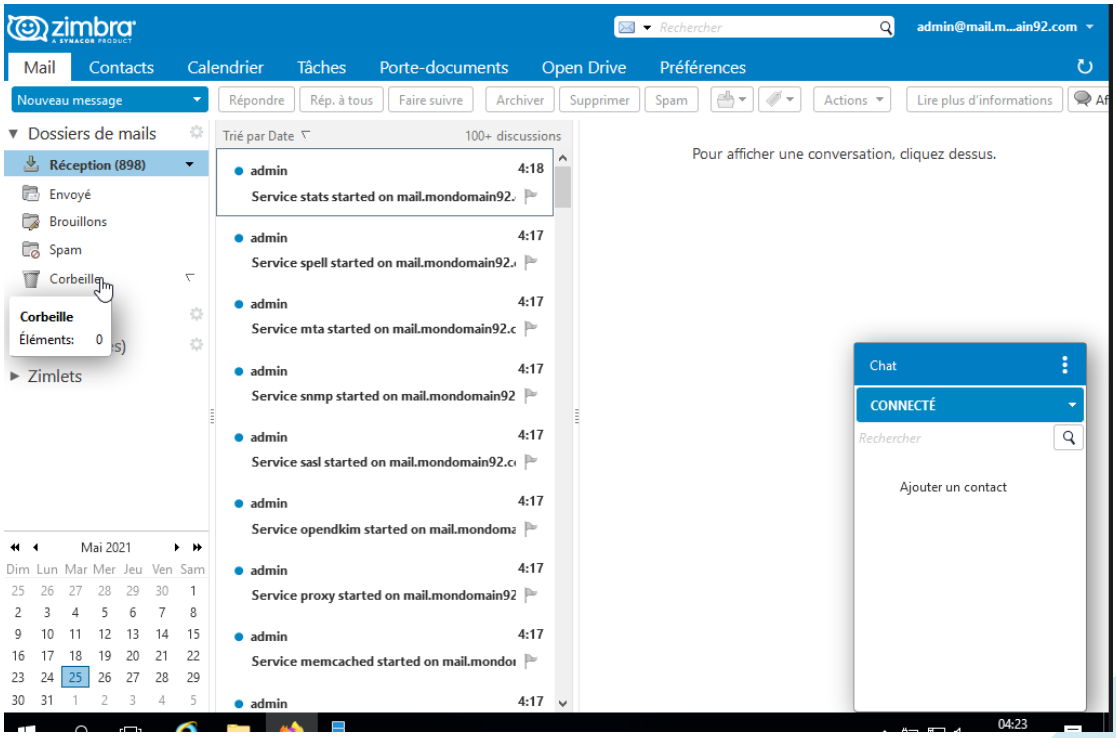
Suiver les etapes d'instalation par defaut
Modifier le mot de passe administrateur en tappant sur 6 puis 4
Sauvgarder les modification
Puis redémarre zmcontrol:

- su – zimbra
- zmcontrol restart

Ayoub Belbachir

Mode opératoire :

Rendez-vous sur le WebUI de Zimbra pour se faire aller sur un navigateur et tapper https://adresse_ip_de_ubuntu_server



Ayoub Belbachir

Installation de Zimbra

Mise en Contexte

Librenms est un logiciel de surveillance de réseau basé sur PHP/MySQL/SNMP à découverte automatique qui inclut le support d'une large gamme de matériel réseau et de systèmes d'exploitation incluant Cisco, Linux, Juniper, Foundry, et bien d'autres, notre bute et d'afficher notre page sur notre il se trouve que j'ai un repository GitHub avec une page internet

Tutoriel:

Commençons par mettre à jour l'index local des packages pour refléter tout nouveau changement en amont :

- sudo apt update

Ensuite, installez le package apache2

- sudo apt install apache2

ensuite nous allons cloner ma page internet qui se trouve mon GitHub :

- git clone https://github.com/digi-boy/comics.git

Supprimons l'index de base de apache

- sudo rm -rf /var/www/html/index.html

Copions note page web pour que apache l'affiche

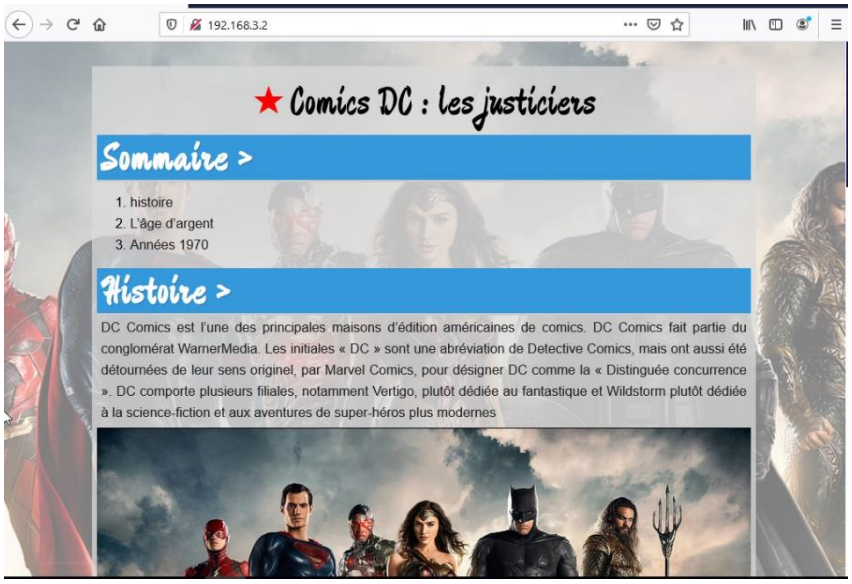
- cd comics
- sudo mv * /var/www/html/

Mode opératoire :

Sur notre navigateur dans le WebUI de Pfsense

- Firewall>Rules> opt1 add
- Action > pass
- Interface OPT1
- Protocol any source opt1 net cliquez sur Save,
- Cette règle nous permet de donner l'accès internet à DMZ

Pour nous render sur notre page web il suffit de et tapper https://adresse_ip_de_ubuntu_server



Ayoub Belbachir

Installation de Bareos

Mise en Contexte

Bareos est un programme de sauvegarde basé sur le modèle client-serveur, il va vous permettre de réaliser des sauvegardes sur votre système d'information par le réseau. En cas de perte de données, de mauvaise manipulation ou d'un ransomware vous aurez la possibilité de récupérer vos données.

Tutoriel:

Commençons par mettre à jour l'index local des packages pour refléter tout nouveau changement en amont :

- sudo apt update

Ensuite ajouter Bareos à l'index local des packages et installer le :

- sudo wget -O /etc/apt/sources.list.d/bareos.list https://download.bareos.org/bareos/release/20/xUbuntu_20.04/bareos.list
- sudo wget -q https://download.bareos.org/bareos/release/20/xUbuntu_20.04//Release.key -O- | sudo apt-key add -
- sudo apt-get update
- sudo apt-get install bareos bareos-database-postgresql

Suiver les étape d'installation simple

Nous allons lancer les scripts pour paramétrer la base de données:

- sudo /usr/lib/bareos/scripts/create_bareos_database
- sudo /usr/lib/bareos/scripts/make_bareos_tables
- sudo /usr/lib/bareos/scripts/grant_bareos_privileges

Lancez les commandes ci-dessous pour redémarrer/démarrer les services:

- sudo systemctl start bareos-dir
- sudo systemctl start bareos-fd
- sudo systemctl start bareos-sd
- sudo systemctl restart apache2

installer le webUI de Bareos

- sudo apt-get install bareos-webui -y
- systemctl reload apache2
- systemctl start bareos-dir
- systemctl start bareos-sd
- systemctl start bareos-fd

Tapez la commande suivante pour accéder à la console par terminal, même si vous avez choisi la seconde option vous devez utiliser cette commande pour ajouter un utilisateur sur l'interface webe et pour ajouter un utilisateur, personnalisez les champs « name » et « password » :

- bconsole
- configure add console name=admin password=admin profile=webui-admin

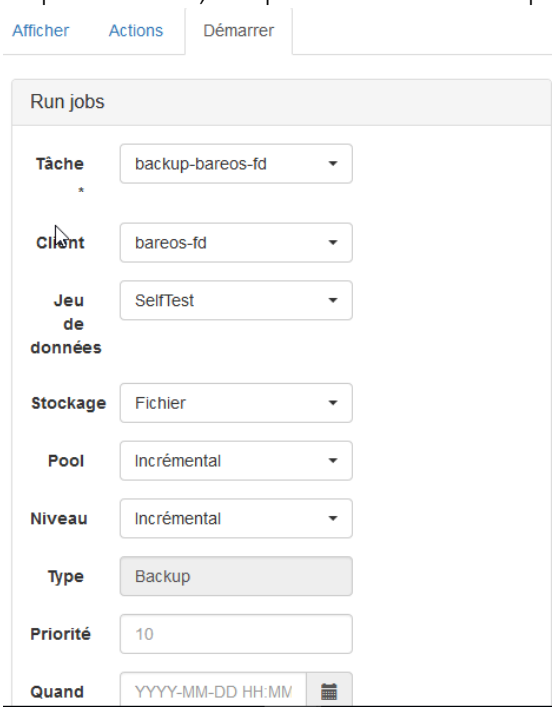
Ayoub Belbachir

Mode opératoire :

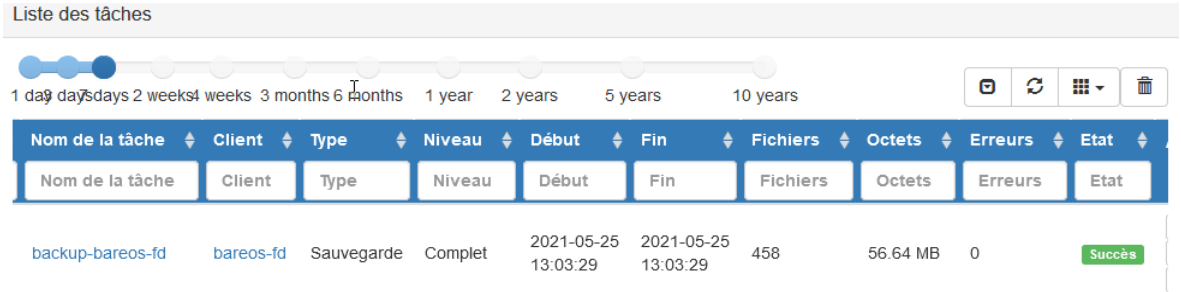
Pour accéder à l'interface web, ouvrez un navigateur et entrez l'adresse suivante :

```
http://IP_SERVEUR_Bareos/bareos-webui
```

Une fois connecté, rensez-vous dans l'onglet « Tâches » puis sur « Lancer ». Dans le champ job, sélectionnez « backup-bareos-fd », complétez les autres champs en fonction de vos préférences et lancez le job :



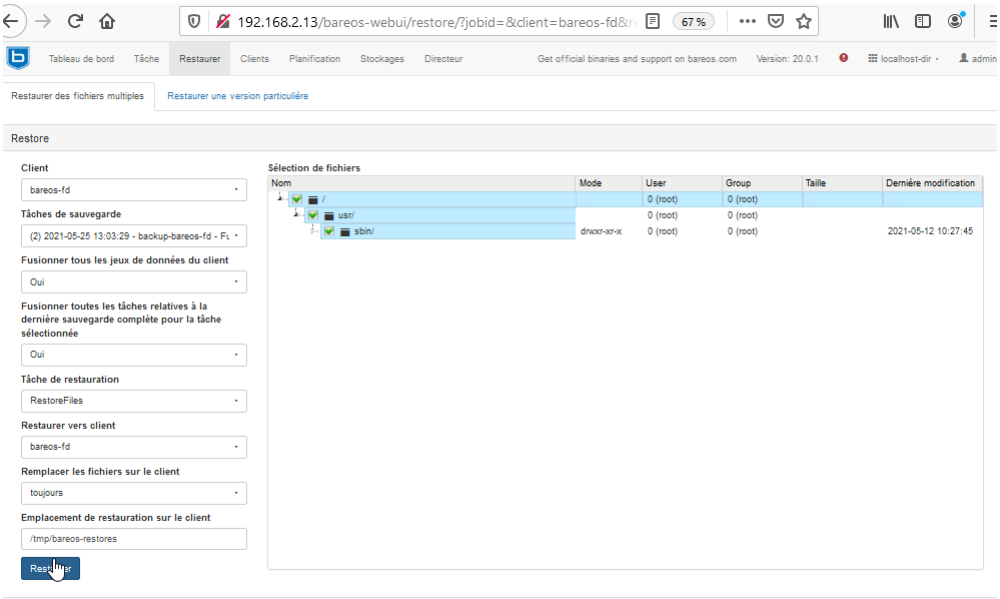
Enregistré en cliquant sur envoyer, patientez quelques minutes pour que le job se finisse:



La sauvegarde du serveur est terminée.

La restauration sera elle aussi très simple car pré-configurée. Dans le premier menu sélectionnez « Restaurer » et dans le champ « Client » sélectionnez le serveur puis cochez les fichiers que vous souhaitez restaurer:

Ayoub Belbachir



Instalation sur un client linux

Je vais réaliser cette partie sur un client Ubuntu. Installez le FD sur le client Linux:

- ≥ sudo apt-get install bareos-client

Sur le client, ouvrez le fichier suivant:

- ≥ sudo nano /etc/bareos/bareos-fd.conf

ajouter les lignes suivante en remplaçant name et password :

- Director {
  Name = <name>
  Password = <password>
  }

Retournez sur le serveur pour définir le job de sauvegarde pour le client Linux:

- ≥ Sudo nano /etc/bareos/bareos-dir.d/job/backup-bareos-fd.conf

Ajouter le texte suivant au fichier :

- Job {
  Name = "backup-linux-fd"
  Jobdefs = "Linux"
  Client = "client-linux-fd"
  }

Éditez ensuite le fichier ci-dessous:

- ≥ sudo nano /etc/bareos/bareos-dir.d/client/bareos-fd.conf

Ajoutez les lignes suivantes à ce fichier en adaptant le mot de passe, l'adresse et le nom du client par rapport à ce que vous avez renseigné :

```
Client {
 Name = client-linux-fd
 Address = 192.168.2.7
 Password = <password>
}
```

Ayoub Belbachir

Créez le job associé:

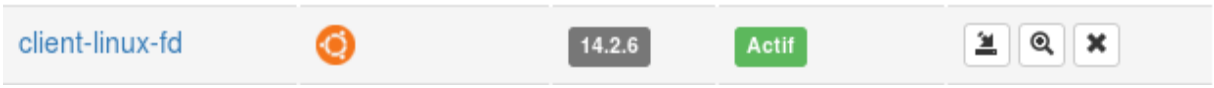
- `sudo nano /etc/bareos/bareos-dir.d/jobdefs/Linux.conf`

Ajoutez les lignes suivantes au fichier:

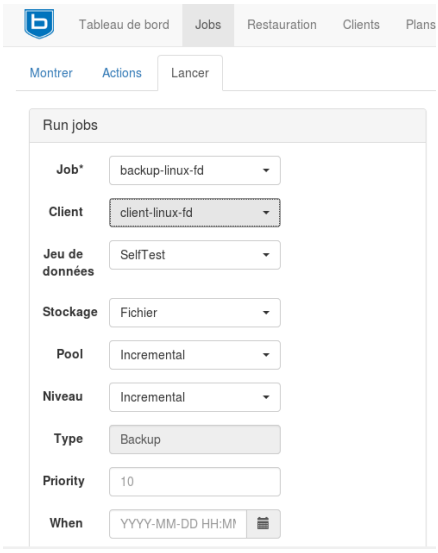
```
JobDefs {
Name = "Linux"
Type = Backup
Level = Incremental
Client = client-linux-fd
FileSet = "SelfTest" # selftest fileset $
Schedule = "WeeklyCycle"
Storage = File
Messages = Standard
Pool = Incremental
Priority = 10
Write Bootstrap =
"/var/lib/bareos/%c.bsr"
Full Backup Pool = Full # write Full
Backups into "Full" Poo$
Differential Backup Pool = Differential #
write Diff Backups into "Different$
Incremental Backup Pool = Incremental
# write Incr Backups into "Increment$
}
```

Redémarrez les services pour prendre en compte les modifications:

- sudo systemctl start bareos-dir
- sudo systemctl start bareos-fd
- sudo systemctl start bareos-sd



Allez dans le menu « Jobs » puis sur « Lancer ». Dans le champ « Job », sélectionnez le client correspondant à votre machine Linux et lancez-le:



La sauvegarde du client Linux est terminée.

Ayoub Belbachir

Configuration IPsec

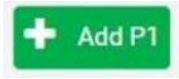
Mise en Contexte

Création un tunnel VPN IPsec site-to-site. Un VPN (Virtual Privat Network) Site-to-Site est un VPN qui permet de joindre deux réseaux de type LAN distant de manière à faire en sorte qu'ils puissent communiquer comme s'ils étaient sur le même réseaux et qu'un simple routeur les séparait. On peut trouver ce gendre de VPN entre des agences et le siège d'une entreprise par exemple. Les agences doivent pouvoir se connecter aux ressources du siège de manière transparente malgré leur distance. On établit alors un VPN au travers internet afin de joindre les deux réseaux mais également de sécuriser ces flux au travers un chiffrement.

Tutoriel:

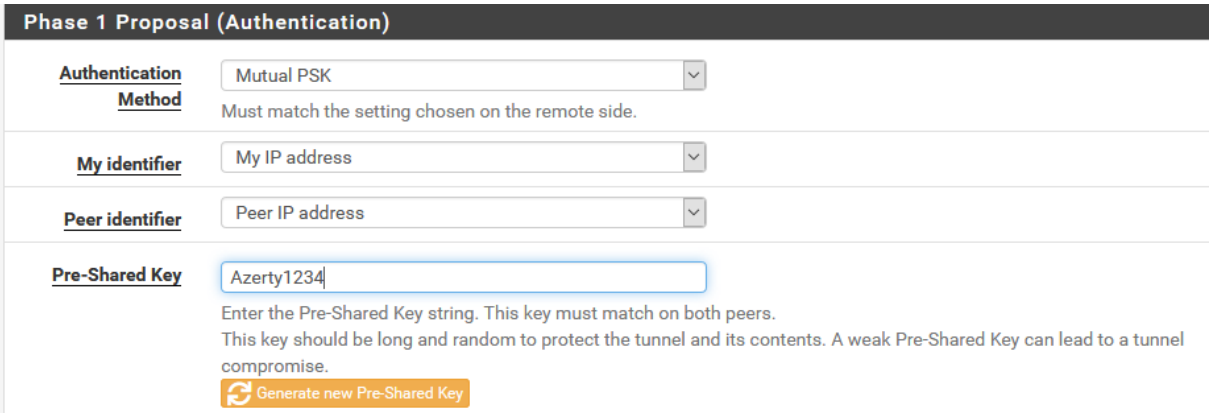
Configuration VPN IPsec : Pour la configuration de VPN en IPsec, il faut aller dans l'interface « graphique » dans l'onglet « VPN » -> IPsec.

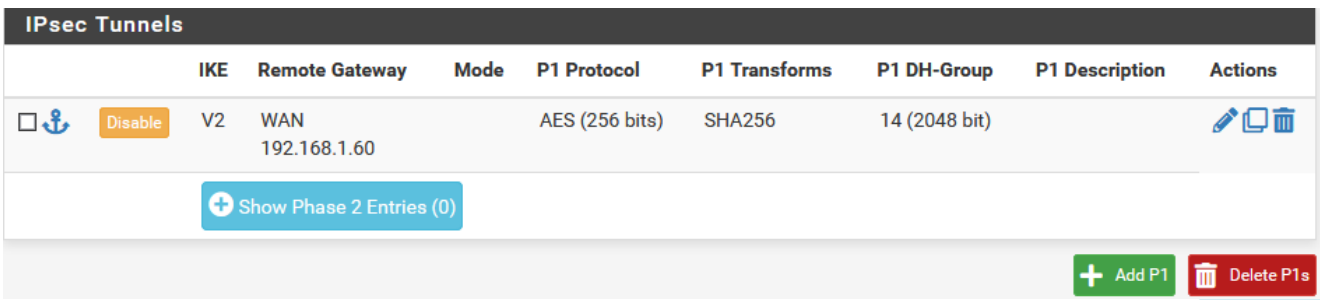
Puis en bas de la page sur la droite on cliquer sur le bouton vert sur lequel il y marquer Add P1



Ensuite, dans Remote Gateway, on rentre l'adresse du Wan du routeur auquel on veut se connecter

Dans la phase 1, « Proposal (Authentification) », saisir notre pre-Shared Key pour plus de sécurité il est préférable de générer une clé en cliquant sur « générale new pre-Shared Key » puis cliquer sur save



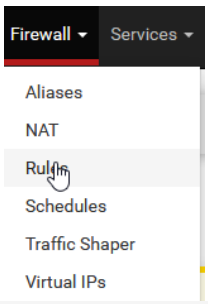


On clique sur « Show Phase 2 Entries(0)»,le nombre entre parenthésé correspond au nombre de phase configurer . Cliquez sur Add Phase 2 à présent.

Dans « Remote Network », il faut rentrer l'adresse IP du sous-réseau du LAN du routeur auquel on souhaite se connecter pour permettre la connexion entre les deux. Il faut faire une modification dans « Encryptions Algorithms », on décoche AES et AES128-GCM er on coche AES256-GCM

Dans l'interface « Advanced Configuration », on rentre l'adresse IP LAN du routeur sur lequel on souhaite se connecter et on sauvegarde tout ça en cliquant sur « Save ».

On peut à présent se servir du Widget IPsec. A ne pas oublier de créer une règle de pare-feu pour le IPsec ensuit configurer et accepter le trafic entre les routeurs. Pour cela se rendre dans Firewall >Rules/



Puis cliquer sur IPsec

Maintenant cliquer sur « Add » et créer la règle qui permettra d'accepter le trafic de données. Pour cela, utiliser les paramètres suivants :

Action : Pass
Diasbed : Ne pas cacher.
Interface: IPsec
Adress Family: IPv4
Protocol: Any.
Il n'y a pas besoin de modifications pour les paramètres restantes cliquer sur « Save » et sur « Apply Changes » pour que les modifications soient prises en compte

Mode opératoire :

Rendez-vous ensuite dans VPN > IPsec cliquer sue le « Related statuts » (L'icône en forme de graphique)

Puis cliquer sur « connecte VPN » la connexion se fait alors seulement si l'on a configuré de la même manier

Ayoub Belbachir

Configuration OpenVPN Road Warrior

Mise en Contexte

Dans le domaine des réseaux informatiques, une configuration de type « roadwarrior » signifie plusieurs choses :

- Un client mobile, constamment en mouvement
- Un client qui a besoin d'un accès internet
- Un client qui a besoin d'accéder aux ressources d'entreprise

C'est ce dernier point qui fait qu'on entend le mot « roadwarrior » presque exclusivement quand on parle de VPN. Le meilleur moyen pour un client nomade d'accéder aux données de l'entreprise, voir aux logiciels et autres ressources, c'est d'utiliser un VPN.

Tutoriel:

On va commencer tout d'abord par la création d'un certificat, cela permettra la sécurité de la connexion entre les deux tunnels. Tout d'abord, on crée l'autorité du certificat. Pour cela, on doit se rendre dans « Système > Cert. Manager > Cas » Puis remplir les cases suivantes : •Descriptive Name, « Ce qui est le nom de l'autorité du certificat »

•Method « ce qui est le type d'autorité »

•Common Name « ce que représente le nom généraliste »

Une fois les cases remplies, faire très attention de ne pas oublier de cliquer sur « Save », car si non toutes les modifications qu'on vient d'apporter au certificat, n'aurons quasiment servie a rien et ne seront pas prises en compte.

Pour la suite, il faut créer le certificat en lui-même. Pour cela on se rend dans « Système > Certificat Manager > Certificats est on va cliquer sur « add » pour créer ce contrat. Les cases à remplir dans cette page sont :

- Method >« Create an internal certificate »
- Certificate authority. > « Le nom »
- Comon name > « Lui attribuer un nom »

Pour la prochaine étape, dans « Certificat type », on sélectionne : Server Certificate

Cliquer sur « Save » pour que les modifications soient prises en compte.

On passe à la création d'un utilisateur. Pour le créer on va se rendre dans la surface « Système > Users Manager > add » Pour cette étape, il faut définir un nom pour l'utilisateur et lui attribuer un mot de passe. On coche la case : « Create a user certificate » on sélection le certificat qu'on a créé.

On va créer le tunnel, pour faire cela, on se rend dans : « VPN > OpenVPN » Après avoir créé le tunnel, on lui attribue une adresse IP et l'adresse de notre LAN

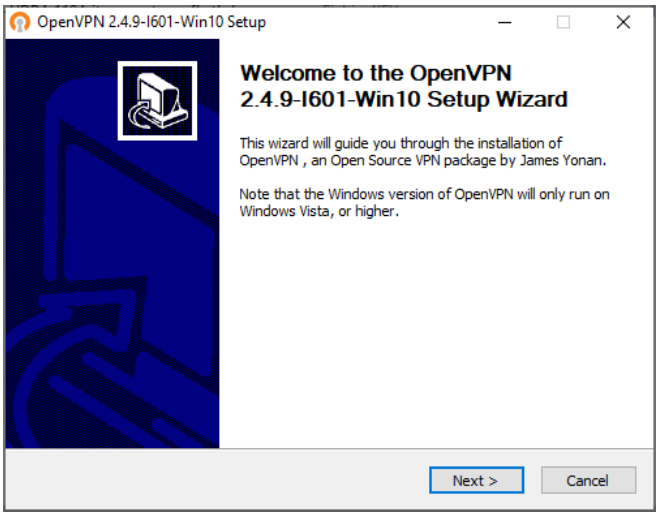
Server mode en Remote Access SSL/TLS+User

Device mode en tun – Layer 3 tunnels Mode

Ayoub Belbachir

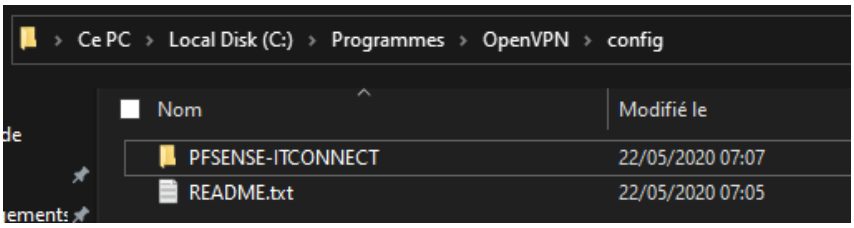
Mode opératoire :

Sur mon PC Windows 10, je commence par installer le client OpenVPN... Ce qui se fait très facilement, sans difficulté particulière ! ?



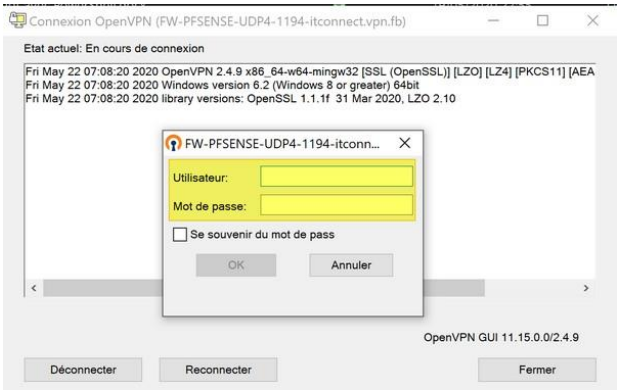
Dans le dossier "C:\Programmes\OpenVPN\Config" vous devez extraire le contenu de l'archive ZIP téléchargée depuis le Pfsense et qui contient la configuration. Vous pouvez créer un sous-dossier dans le dossier "config" si vous voulez.

Pour donner un nom plus simple à la connexion VPN, renommez le fichier. OVPN : son nom sera celui donné à la configuration.



Ensuite, sur l'icône OpenVPN effectuez un clic droit et cliquez sur "Connecter".

Vous devez fournir le nom d'utilisateur et le mot de passe, correspondant à un compte AD ou un compte local du pare-feu, en fonction de la configuration.



Lorsque le tunnel VPN est monté et actif, l'icône devient verte : 

Si l'on effectue un « ***ipconfig »*** sur le PC, nous pouvons voir que l'on a bien une adresse IP sur la plage 10.10.10.0, avec un sous-réseau en /30 pour l'isolation des clients.

Il ne reste plus qu'à établir une connexion sur vos serveurs, via RDP, Web, ou autre, selon vos besoins !

Configuration OpenVPN site à site.

On va d'abord ajouter un serveur VPN sur l'interface Pfsense, pour cela, on va dans :

VPN > OpenVPN > Servers > Add

Pour la prochaine étape, dans le Serveur mode, nous avons 5 possibilités.

La possibilité qu'on choisisse est la première, « Peer to Peer (SSL/TSL) ce qu'il nous permettra de monter un VPN site-à-site en utilisant une authentification par certificat ».

Protocol: « UDP on IPv4 Only »

Device mode : TUN (Frames IP)

Interface : L'interface sur laquelle le serveur va recevoir la connexion entrantes, WAN ou OPT1.

Local port : port d'écoute du serveur OpenVPN. La valeur par défaut est 1194.

A savoir que chaque serveur DNS possède son propre port d'écoutée il doit être attribue qu'a un seul serveur le port respectif (à bien vérifier cela).

Description : Nommer le serveur VPN. Le nom qu'on choisit apparaitra dans la liste de sélection de VPN.

SharedKey : « Automatically generate a shared key ».

Encryption Algorithm : AES 256 bits CBC.

La clé devra être le même sur les deux côtes, aussi bien côte client que cote serveur, si non la liaison ne se fera pas. La capacite minimale est de 128 bits.

Enable NCP : On laisse la case coche car elle permet d'activer le protocole NCP. Ceci va permettre que le client et le serveur négocient le protocole de chiffrement le plus approprié.

NCP Algorithms : Ce sont les algorithmes que nous souhaitons supporter du cote serveur.

Auth digest algorithm : La valeur reste par défaut. La valeur par défaut est : « SHA256 » Hardware : Pour cette étape il faut préciser si le serveur dispose d'un serveur cryptographique.

IPv4 Tunnel Network : C'est le réseau utilise pour le tunnel VPN. Pour la connexion d'un VPN site-a-site comme dans notre cas, un /30 serrait suffisante

IPv4 Remote Network(s) : Cette partie désigne les serveurs distants qui sont disponibles par le serveur.

Courrent Connexions : Il précise le nombre de clients disponibles possible en même temps sur le serveur. Dans le cas d'un VPN site-a-site, la casse devrait être à 1.

Compression : Décoche la case.

Custom option : Cette option permet d'attribuer des paramètres avancés à OpenVPN.

A ne pas oublier de tout sauvegarder en appuyant sur Save à la fin de tous les réglages qu'on vient de réaliser.

A présent, le la configuration OpenVPN est bien termine sur le cote serveur, on va maintenant fixer des règles de filtrage pour permettre l'accessibilité du serveur.

Pour accéder à l'interface qui vas nous permettre de faire la configuration, on va dans : « Firewall > Rules »

Interface : WAN.

Protocol : UDP. Source : Si l'adresse IP n'est pas connue avec l'option « any », alors on choisit l'option « Single host or alias ».

Destination : type « Single host or alias », adresse IP de destination.

Destination Port Range : Le port reste par défaut, 1194

A présent, la configuration du serveur est terminée. Il faut à présent autoriser ou filtrer les flux transits à travers de notre interface OpenVPN.

Pour cela, on va dans : Firewall > Rules > OpenVPN pour créer les règles.

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✔	0 /0 B	IPv4 *	192.168.1.0/24	*	192.168.2.0/24	*	*	none		LAN site A vers LAN site B

Exemple de la 2ème règle : Site B(Client) vers site A (serveur)

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✔	0 /0 B	IPv4 *	192.168.2.0/24	*	192.168.1.0/24	*	*	none		LAN site B vers LAN site A

Pour cela, aller dans VPN > OpenVPN > Clients > Add

Server Mode: Peer-to-Peer.

Protocol : C'est le même que celui qu'on a attribué du coté serveur

Device Mode : TUN

Interface : Il s'agit de l'interface WAN, c'est l'interface par la quelle OpenVPN vas joindre le serveur.

Local Port : Si on n'attribue rien à cette étape, le système lui attribuera une sélection aléatoire.

Server host or address : On met l'adresse IP publique du serveur, qui est notre site suivant.

Server port : On lui attribue le port d'écoute du OpenVPN distant, donc 1194.Desccription: Nommer le Tunnel VPN.

Auto generate/Share Key : Il faut décocher la case et faire une copie colle de la clé générée OpenVPN server. On peut même utiliser une clé physique pour faire le transfert d'une machine à une autre.

Encryption algorithm : AES-256-CBC.

NCP Algorithm : Cette étape reste exactement comme sur le côté serveur.

Auth digest algorithm : SHA256.

Hardware Crypto : A présent il faut préciser si notre serveur dispose d'un support cryptographique ou pas.

IPv4 Tunnel Network : On lui attribue le même réseau que celui du OpenVPN du cote serveur.

IPv4 Remote Networks(s) : On écrit le réseau du site distant en précisant le masque.

Compression : Cette étape doit être identique à la configuration du côté serveur. Et dernière étape, c'est d'autoriser les flux.

Ayoub Belbachir

Installation de FOG

Mise en Contexte

Free Open-source Ghost est une solution de clonage et de déploiement de systèmes d'exploitation et de logiciels sur des ordinateurs. Il s'installe à l'aide d'un script qui compile plusieurs paquets nécessaires à sa mise en place

Tutoriel:

Pour installer FOG, il faut télécharger un fichier .tar.gz de la dernière version sur le site du projet (http://fogproject.org/). La version installée dans ce tutoriel est la 1.5.9. Après extraction du .tar.gz (via la commande tar –xzf fichier.tar.gz), il faut lancer le script d'installation installfog.sh se trouvant dans le dossier targz-decompressé/bin :

- wget https://github.com/FOGProject/fogproject/archive/1.5.9.tar.gz
- tar -xzf fogproject-1.5.9.tar.gz
- cd fogproject-1.5.9
- sudo ./installfog.sh

Le script posera plusieurs questions concernant le paramétrage du serveur, répondre selon vos besoins. Au milieu de l'installation on doit renseigner le mot de passe de la base Mysql. On peut le laisser vide pour se simplifier la vie mais au niveau sécurité c'est moyen. On va donc positionner un mot de passe … Mais attention le mot de passe renseigné ne sera positionné que dans les fichiers de config de FOG. Il faut donc avant de continuer, ouvrir une autre fenêtre SSH pour positionner ce mot de passe sur la base MYSQL en elle-même.

1.1 Mode opératoire :

nous avons maintenant accès à l'interface WebUI de fog