23/05/2020

Projet UF

Gestion d'un Intranet

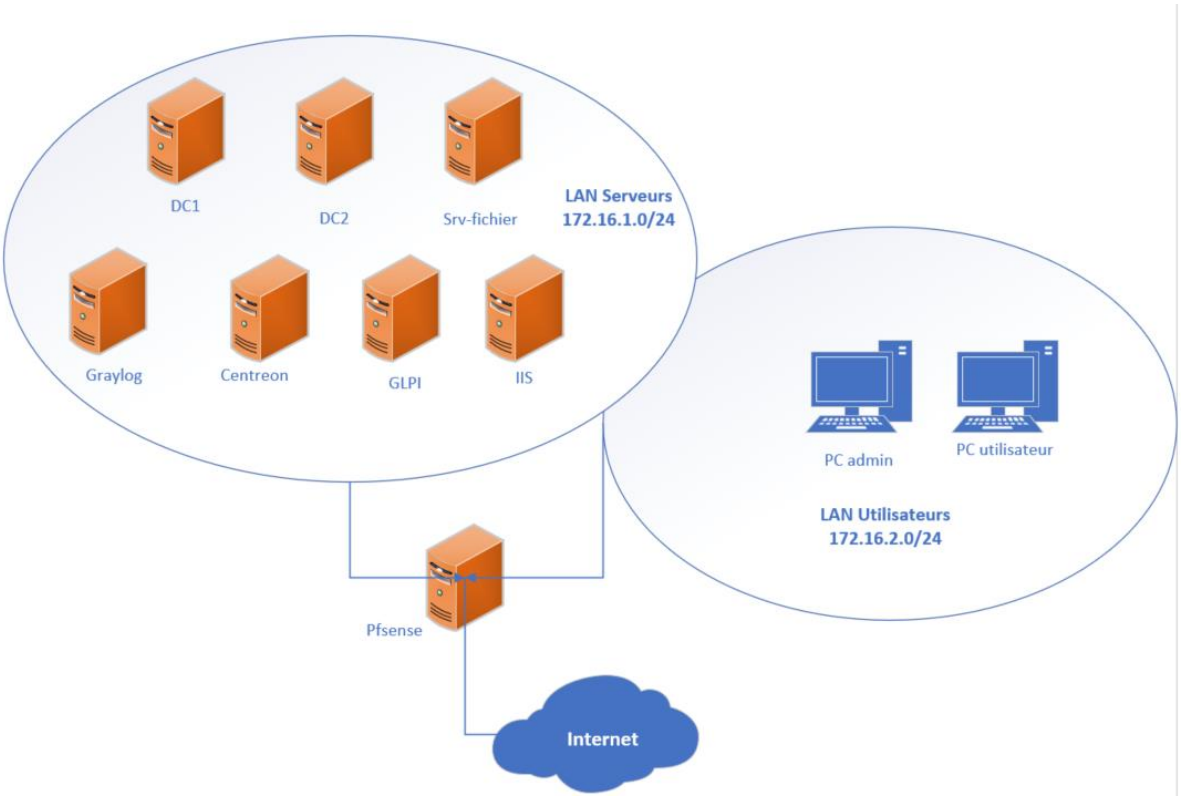
Louis LE SAUX, Ludovic SACHOT
YNOV CAMPUS

Table des matières

Contexte

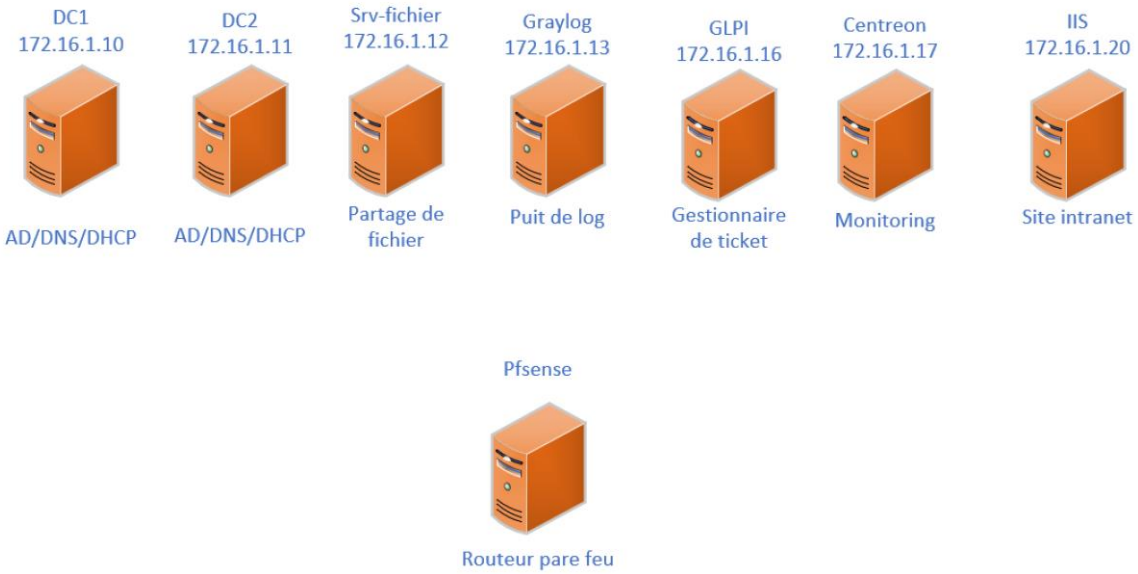
L'objectif de notre projet était de mettre en place une gestion simplifiée de l'ensemble de services IT d'une entreprise. Nous avons donc mis en place différents services telle qu'un contrôleur de domaine (AD/DNS/DHCP). Nous avons également ajouté une deuxième machine virtuelle portant les mêmes rôles pour pouvoir ajouter de la redondance. Nous avons également mis en place un serveur de fichier pour que les utilisateurs du domaine puissent stocker leurs données. Nous avons également ajouté des machines virtuelles pour pouvoir centraliser les logs et monitorer notre infrastructure. Un serveur web (IIS) a aussi été mis en place pour que les utilisateurs puissent accéder à l'Intranet. Cette intranet permet aux utilisateurs du domaine d'accéder à leur messagerie (Gmail), à au gestionnaire de ticket (GLPI) mais aussi à leur agenda.

Schéma de l'infrastructure par zone :



Nous avons mis en place un Pfsense pour avoir 2 réseau distant. Un réseau pour les utilisateurs et un réseau pour les serveurs. Les noms de ces derniers y sont retranscrits et appartiennent au domaine « uf_infra_B.local ».

Service(s) par serveur :



Adressage IP :

LAN Serveur

Hotes	Adresse IP	Passerelle
DC1	172.16.1.10	172.16.1.1
DC2	172.16.1.11	172.16.1.1
srv-fichier	172.16.1.12	172.16.1.1
Graylog	172.16.1.13	172.16.1.1
glpi	172.16.1.16	172.16.1.1
centreon	172.16.1.17	172.16.1.1
IIS	172.16.1.20	172.16.1.1

Pfsense

Interface	LAN segment
192.168.1.19	WAN
172.16.1.1	LAN Serveurs
172.16.2.1	LAN User

LAN User

Hote	Adresse IP	Passerelle
PC admin	172.16.2.10	172.16.2.1
PC user	172.16.2.100	172.16.2.1

Détail des bonnes pratiques :

- Les utilisateurs de l'entreprise doivent changer leur mot de passe tous les mois.
- Forme du mot de passe : caractère spéciaux, chiffre, lettre majuscule obligatoire).
- Sauvegarde régulière vers google drive.
- Seuls les administrateurs ont le rôle d'admin du domaine.
- Les utilisateurs n'ont pas le droit de circuler sur les sites pouvant nuire à leur travail (Réseaux sociaux, site pornographique, etc…).
- Configuration d'une redondance pour le contrôleur de domaine.
- Réseaux sécurisés.
- Les mises à jour sont effectuées régulièrement.

Mise en place des contrôleurs de domaine :

Nous avons commencé par ajouter les rôles AD/DNS/DHCP sur les deux serveurs. Nous avons ensuite créé notre nom de domaine (uf_infra_B.local). Après avoir créé notre domaine sur le premier contrôleur de domaine, nous avons ajouté le second à celui-ci. Nous l'avons ensuite promu en tant que contrôleur de domaine à un domaine existant.

Adressage IP des serveurs :

Nom = DC1.uf_infra_B.local

@IP = 172.16.1.10/24

Passerelle = 172.16.1.1

DNS primaire : lui-même

DNS secondaire : DC2 (172.16.1.11)

Nom = DC2.uf_infra_B.local

@IP = 172.16.1.11/24

Passerelle = 172.16.1.1

DNS Primaire = Lui-même

DNS secondaire = DC1 (172.16.1.10)

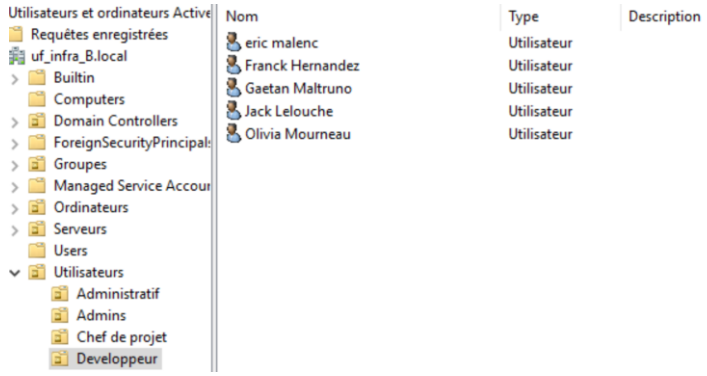
1) Active directory

Nous avons ensuite configuré l'Active Directory en ajoutant 13 utilisateurs séparé en plusieurs service (groupe).

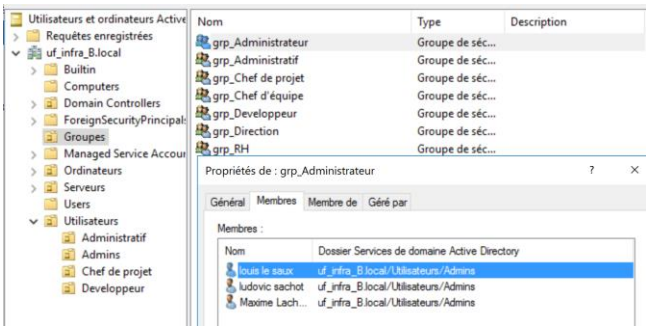
Administrateurs	Développeurs	Equipe administrative	Chef de projet
Louis Le Saux	Gaetan Maltruno	Marc Henry	Carles Dariot
Ludovic Sachot	Eric Malenc	Marie Darienzo	Jessica Pontier
Maxime Lacharge	Franck Hernandez	Segolène Namache	
	Jack Lelouche		
	Olivia Mourneau		

Chef d'équipe	Direction	RH
Maxime Lacharge	Marc Henry	Segolène Namache
Gaetan Maltruno	Marie Darienzo	

Les différents utilisateurs ont été créés dans l'AD et placé dans des OU spécifiques.

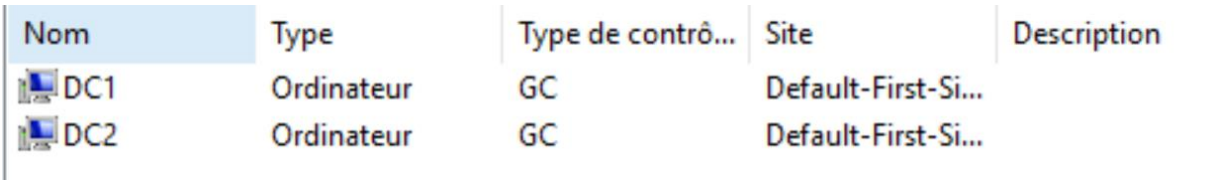


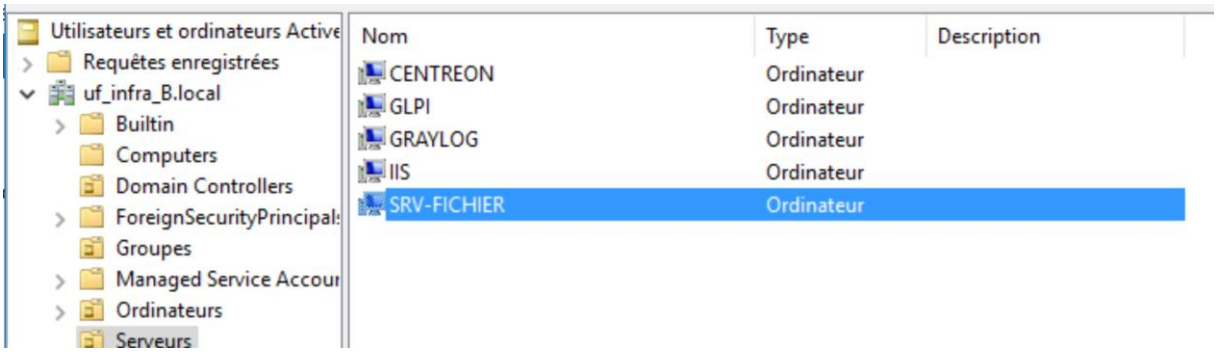
Ils ont également été ajoutés à leur groupe respectif (nous verrons que les groupes sont importants pour le serveur de fichiers).



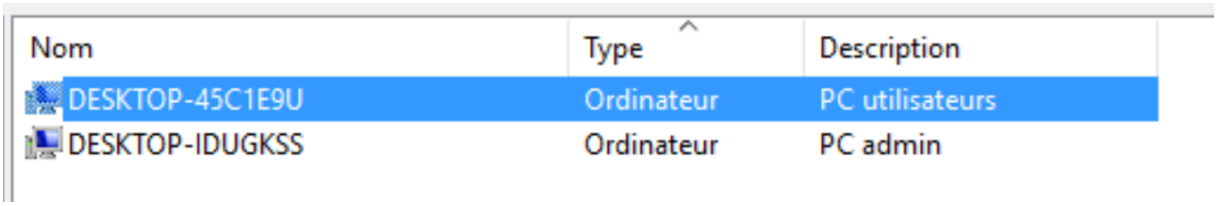
Les administrateurs ont été ajoutés au groupe « admins du domaine ».

Les différents serveurs installés ont tous été ajoutés au domaine :





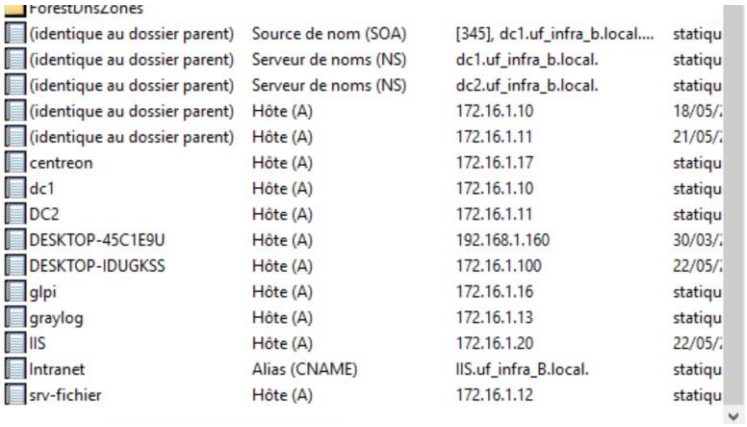
Ainsi que les postes de travail :



Nom	Type	Description
DESKTOP-45C1E9U	Ordinateur	PC utilisateurs
DESKTOP-IDUGKSS	Ordinateur	PC admin

2) DNS

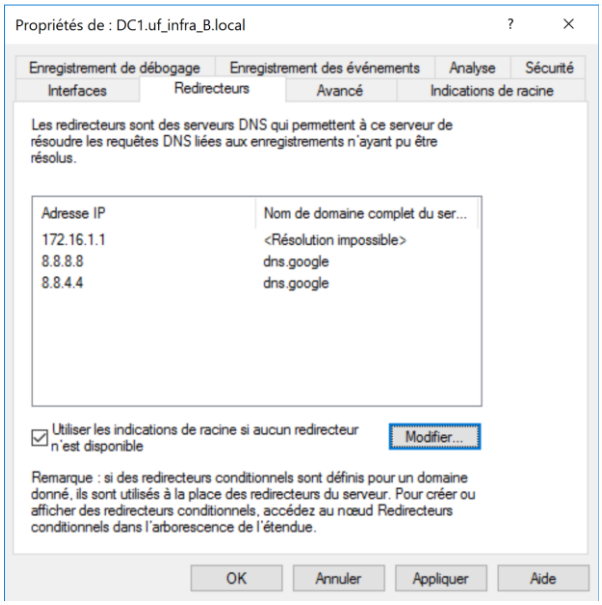
Dans le gestionnaire DNS, nous avons ajouté tous les hôtes avec leur adresse IP dans les zones de recherche directes.



ForestDnsZones			
(identique au dossier parent)	Source de nom (SOA)	[345], dc1.uf_infra_b.local....	statiqu
(identique au dossier parent)	Serveur de noms (NS)	dc1.uf_infra_b.local.	statiqu
(identique au dossier parent)	Serveur de noms (NS)	dc2.uf_infra_b.local.	statiqu
(identique au dossier parent)	Hôte (A)	172.16.1.10	18/05/.
(identique au dossier parent)	Hôte (A)	172.16.1.11	21/05/.
centreon	Hôte (A)	172.16.1.17	statiqu
dc1	Hôte (A)	172.16.1.10	statiqu
DC2	Hôte (A)	172.16.1.11	statiqu
DESKTOP-45C1E9U	Hôte (A)	192.168.1.160	30/03/.
DESKTOP-IDUGKSS	Hôte (A)	172.16.1.100	22/05/.
glpi	Hôte (A)	172.16.1.16	statiqu
graylog	Hôte (A)	172.16.1.13	statiqu
IIS	Hôte (A)	172.16.1.20	22/05/.
Intranet	Alias (CNAME)	IIS.uf_infra_B.local.	statiqu
srv-fichier	Hôte (A)	172.16.1.12	statiqu

Nous avons également ajouté un alias pour le serveur IIS pour qu'il soit joignable via le nom « Intranet ». Cela sera utile lorsque l'on mettra en place l'intranet.

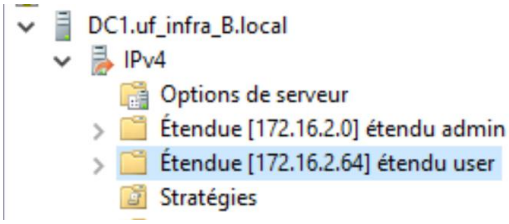
Nous avons également ajouté des redirecteurs au cas où les contrôleurs de domaine n'arrivent pas à résoudre des requêtes DNS.



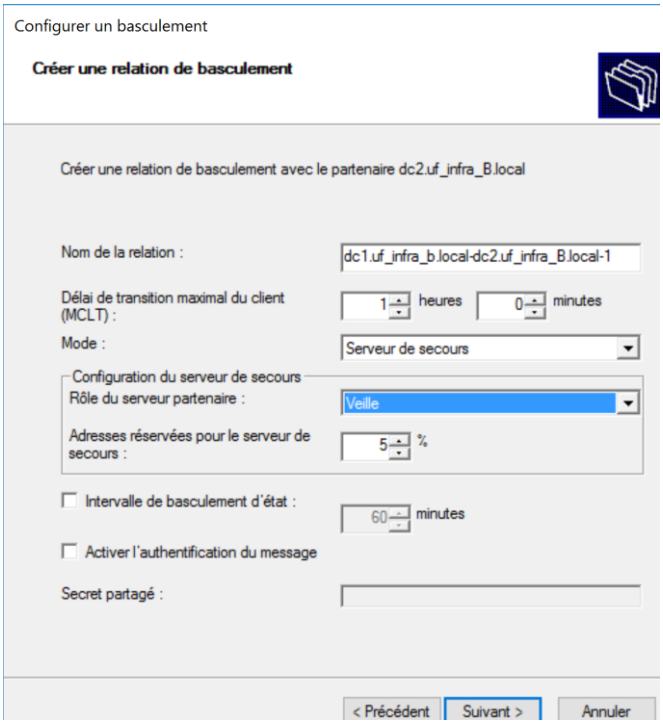
3) DHCP

Nous avons mis en place 2 étendus pour notre infrastructure.

La première est réservée aux PC des administrateurs. La seconde est réservée aux utilisateurs de l'entreprise.



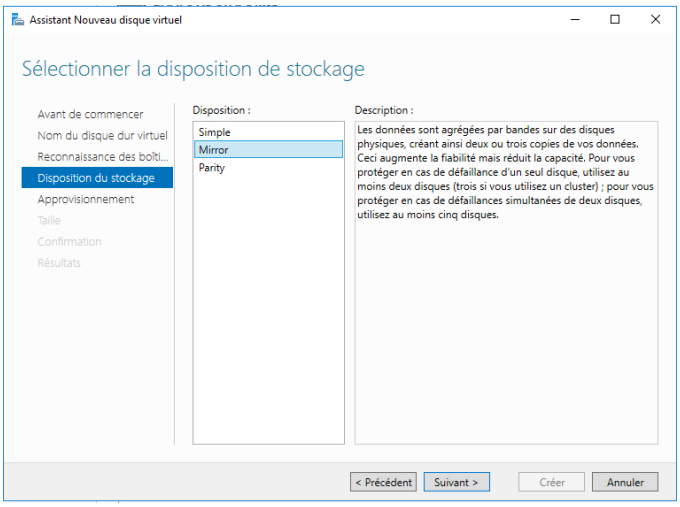
Nous avons également prévu un basculement entre les deux contrôleurs de domaine. Il a été décidé que le 1er contrôleur de domaine (DC1) serait le serveur DHCP principale. Le DC2 sera donc le serveur de secours. Nous avons choisi de mettre cela en place pour pallier à une éventuelle panne du DC1. Le second contrôleur de domaine délivrera les adresses aux différents PC.



Serveur de fichier :

Nous avons donc mis un serveur de fichier pour que les utilisateurs de l'entreprise puissent stocker leur document dans des dossiers partagés.

Pour cela, nous avons choisi d'utiliser deux disques pour pouvoir faire du miroir sur ces deux disques. Dans ce cas, les données seront écrites sur les deux disques en simultanément.

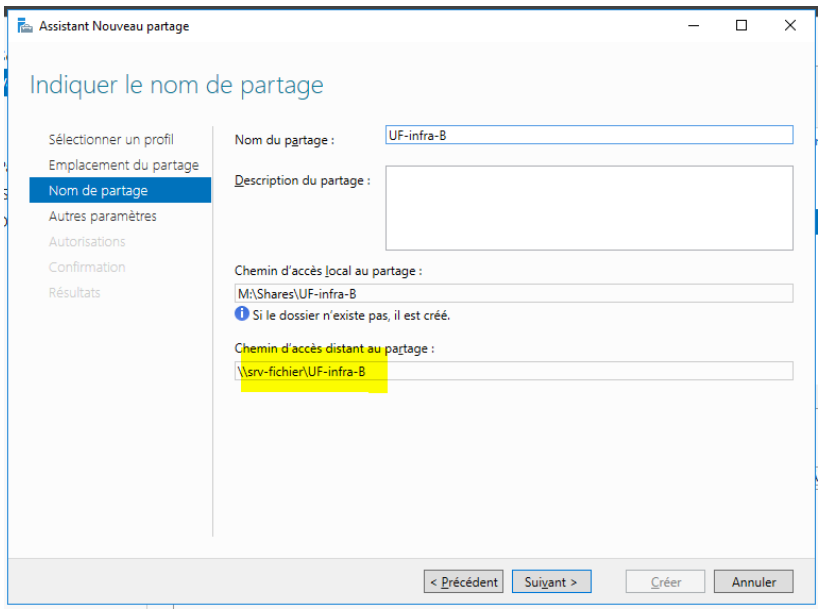


Nous avons également choisi d'utiliser un approvisionnement fixe permettant ainsi d'utiliser la totalité de l'espace disque.

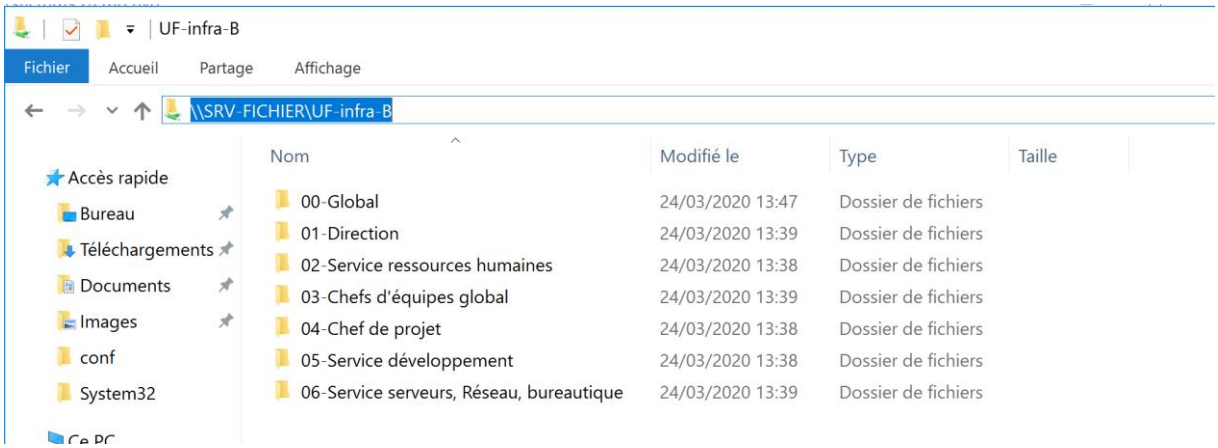
Nous avons, dans un premier temps, créé le volume « M » avec le disque virtuel créé précédemment.

Dans un second temps, nous avons créé notre dossier partagé avec un partage SMB simple (pas besoin de gestionnaire de quotas ou autres car nous sommes une petite entreprise).

Pour pouvoir accéder au partage depuis un poste utilisateur, il faudra noter le chemin suivant dans l'explorateur de fichier \\srv-fichier\uf-infra-B (srv-fichier étant le nom du serveur et uf-infra-B le nom du dossier partagé).



Test avec le compte l.lesaux (admins du domaine) :



Les comptes Admins du domaine ont accès à tous les dossiers en contrôle total pour que ceux-ci puissent répondre aux demandes utilisateurs (demande d'accès, etc…).

Les accès au dossier sont gérés uniquement par des groupes (groupe AD créé précédemment).

Cela permet donc de faciliter l'administration du serveur de fichiers.

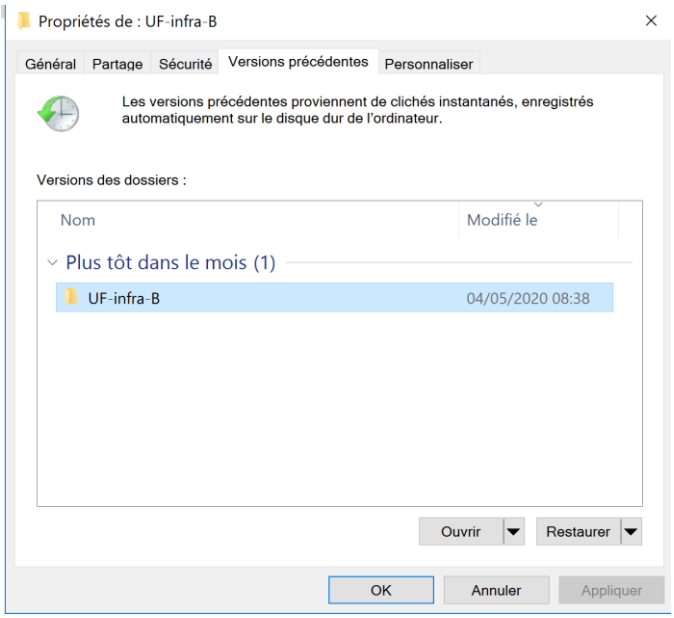
00-Global	01-Direction	02-Service Ressources humaines
Utilisateurs du domaine	grp_Direction	grp_RH

03-Chefs d'équipe global	04-Chef de projet	05-Service développement
grp_Chef d'équipe	grp_Chef de projet	grp_développeur

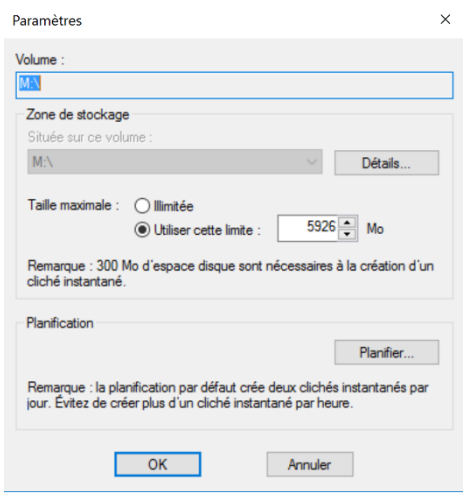
06-Service serveurs, Réseau, Bureautique
Admins du domaine

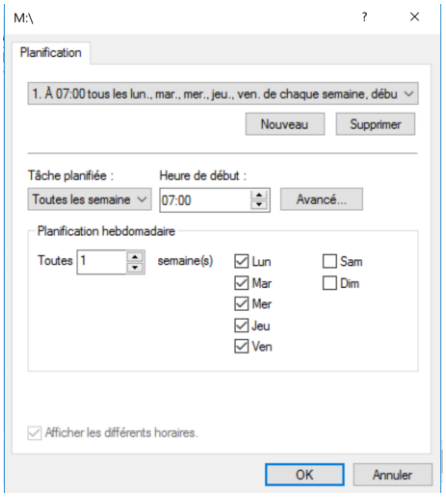
Cette gestion par groupe permet aux administrateurs de gérer plus efficacement les accès dossiers. L'intérêt de cette méthode parait limité dans le cadre d'une petite entreprise mais devient intéressante sur des plus grandes entreprises

Nous avons également mis en place les versions précédentes sur ce dossier. Cela est utile dans le cas où un utilisateur supprime malencontreusement un dossier ou un fichier.



Pour cela, nous avons mis en place les clichés instantanées sur le disque M (disque partagé).





Ces clichés instantanés sont planifiés tous les jours ouvré de la semaine à partir de 7h avant que les utilisateurs commencent à travailler. Dans le cas d'une grande entreprise, il est préférable d'effectuer cela pendant la nuit pour éviter tous ralentissement car l'opération risque d'être longue si le nombre de dossiers et fichiers est très grand.

Puit de log (Graylog) :

Nous avons décidé de mettre en place un puit de logs pour pouvoir récolter tous les logs systèmes de tous les serveurs de notre infrastructure. Nous avons donc décider de mettre en place un Graylog.

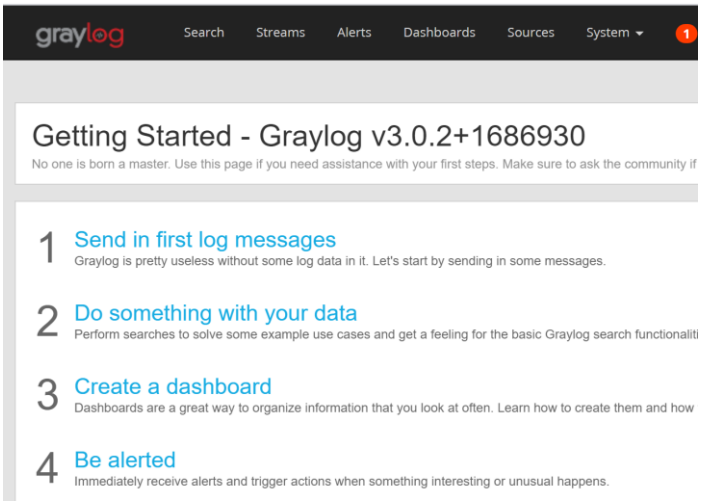
Source d'installation :

https://www.itzgeek.com/how-tos/linux/centos-how-tos/how-to-install-graylog-on-centos-7-rhel-7.html

Graylog a besoin de certains prérequis avant de commencer l'installation :

- Installation de java car Graylog et Elasticsearch sont tous les deux basés sur ce langage.
- Elasticsearch : Graylog utilise Elasticsearch pour stocker les **messages du journal** et propose également une fonction de recherche.
- MongoDB : Graylog utilise MongoDB comme base de données pour stocker des métadonnées (informations utilisateurs ou configuration de flux) et des configurations. (Stocker les données de CONFIGURATION et non pas les données de JOURNAL). MongoDB n'a pas un gros impact sur le système (pas nécessaire de le faire évoluer).

Après avoir installé le serveur Graylog, il nous est possible d'accéder à l'interface web (via l'adresse IP du serveur) nous permettant de configurer la centralisation des logs.



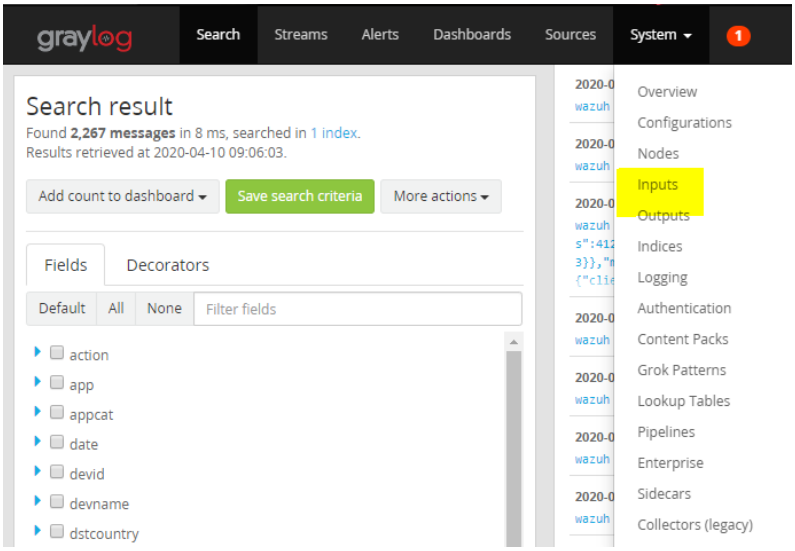
Pour pouvoir centraliser les logs des différents serveurs sur le graylog, nous avons dû ajouter des agents sur les différents serveurs. Bien sûr, la procédure est différente entre les serveurs Linux et Windows

Nous avons ajouté tous les serveurs pour pouvoir centraliser leur log dans une seule interface

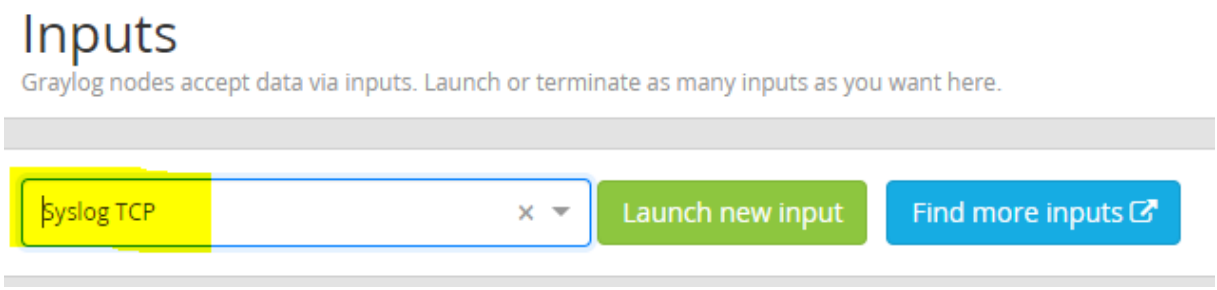
(DC1, DC2, srv-fichier, IIS, Graylog, GLPI, Centreon)

1) Linux

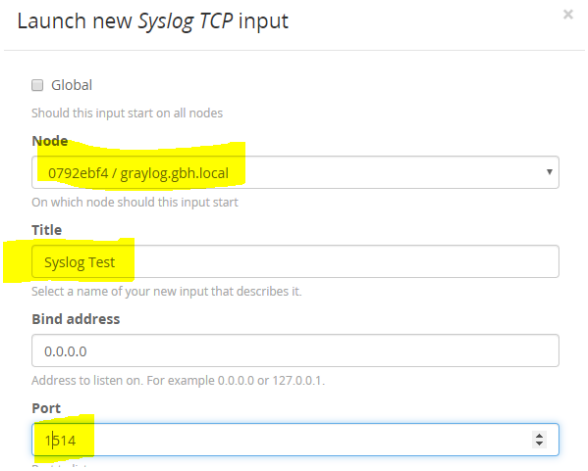
Pour commencer, sur l'interface web de Graylog, ajoutez une règle « inputs ».



Ensuite, ajoutez un input Syslog (TCP et UDP) puis cliquez sur « Launch new input »



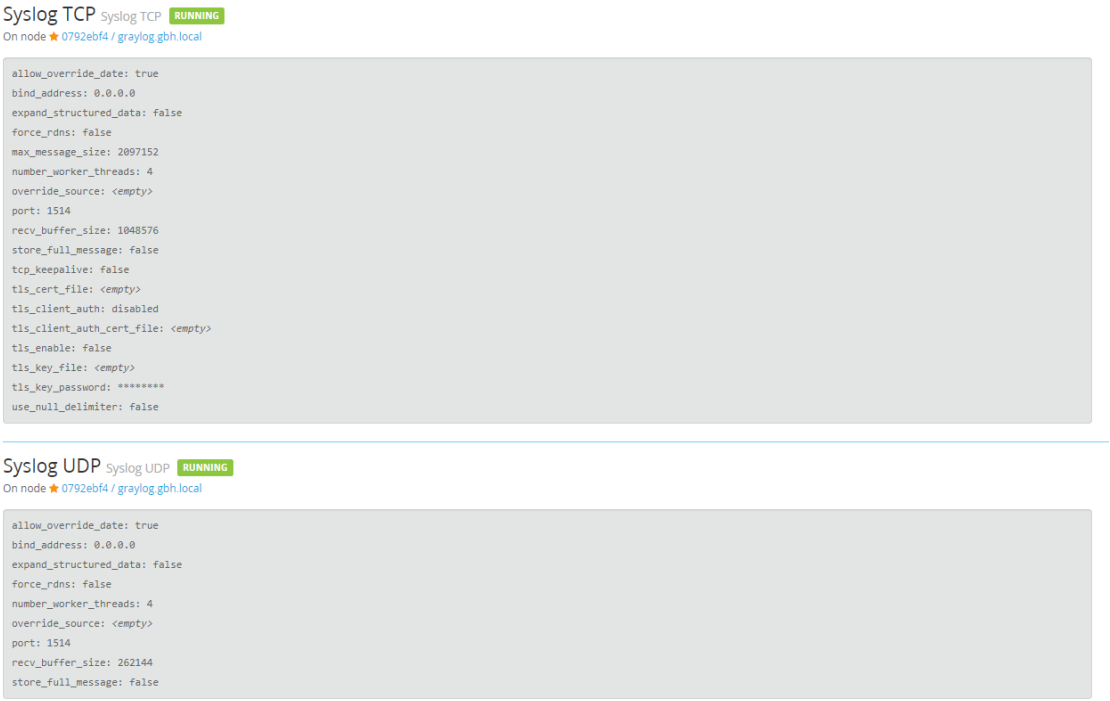
Ajoutez les config suivantes puis cliquez sur valider :



Node représente le serveur sur lequel nous voulons ajouter les logs (notre serveur).

Nous avons choisi le port 1514 car nous ne pouvons pas utiliser le port 514 comme préciser dans sur le site « itzgeek.com ».

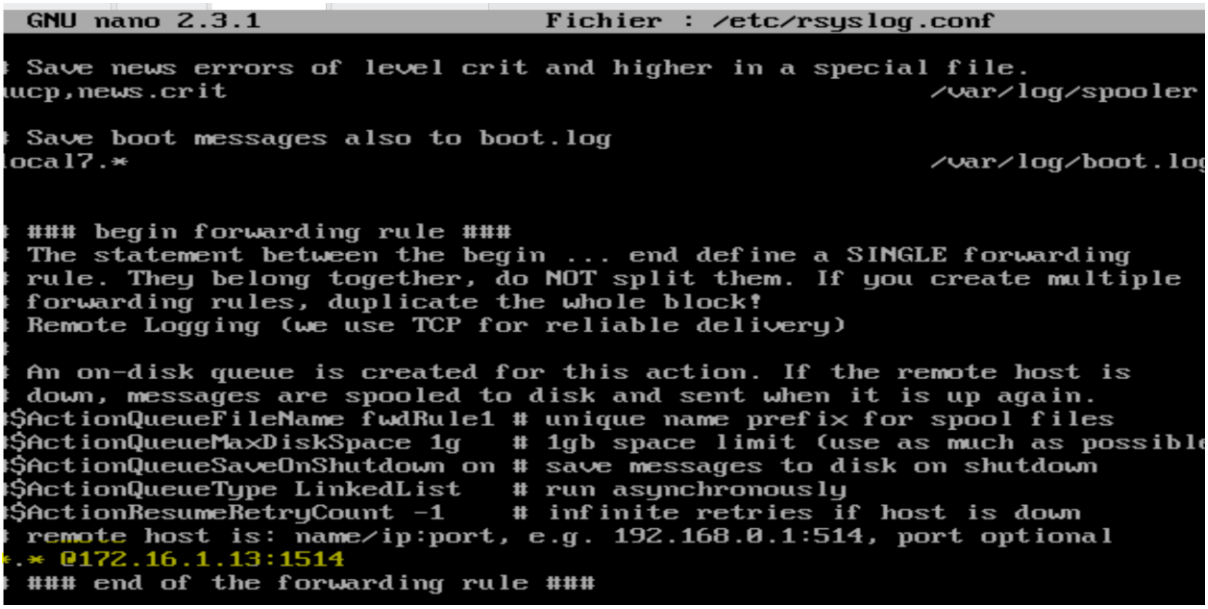
Après avoir configurer les deux « inputs » vous pouvez passer à l'étape suivante.



Ensuite, entrez dans le fichier de config */etc/rsyslog.conf*

Ajouter la ligne suivante à la fin du fichier de config (*.* @ « @ip du graylog » : « port utilisé ») puis enregistrer.

Cette ligne permet de répertorier « tous les logs » du serveur en question sur le serveur Graylog.



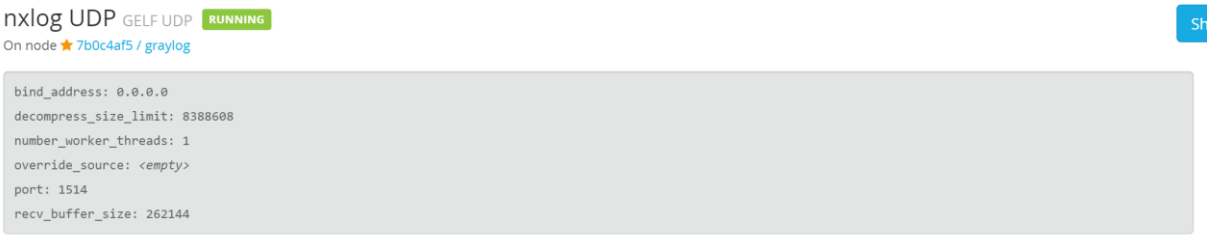
Redémarrer le service rsyslog *service rsyslog restart*

Ouvrir le port 9000, 514 et 1514 + les service http et https sur le serveur ayant besoin de l'agent.

Ouvrir le port 514 et 1514 sur le serveur graylog.

2) Windows

Sur l'interface web Graylog, nous avons ajouté l'entrée suivante :



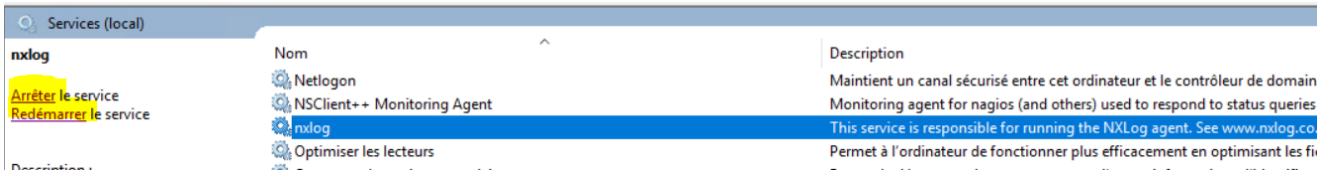
Sur les serveurs Windows sur lesquels nous voulons récupérer les logs, nous avons installé nxlog.

Ensuite, nous avons modifier le fichier nxlog.conf « C:\Program Files (x86)\nxlog\conf\nxlog.conf »

```
<Extension _syslog>
    Module      xm_syslog
    #Module     xm_gelf
</Extension>

<Input in>
    Module      im_msvistalog
</Input>

<Output out1>
    Module      om_tcp
    host        172.16.1.13
    Port        1514
    Exec        to_syslog_snare();
    #OutpuType  GELF
</Output>

<Output out2>
    Module      om_udp
    Host        172.16.1.13
    Port        1514
    Exec        to_syslog_snare();
    #OutputType GELF
</Output>

<Route 1>
        Path in=> out1, out2
```

Enregistrer le fichier modifié.

Windows+R → services.msc et rechercher nxlog. Cliquer sur démarrer



Le serveur remonte après sur le graylog.

Après avoir effectuée cette opération sur tous les serveurs, nous pouvons constater dans l'onglet « Search » que de tous les logs des serveurs remontes sur le graylog.

Logiciel de supervision (Centreon) :

Nous avons choisi d'installer Centreon pour pouvoir superviser l'ensemble de notre infrastructure. Nous n'avons pas eu le temps d'ajouter tous les connecteurs souhaités par manque de temps et car nous avons été confrontés à d'autres problèmes.

Nous pouvons donc accéder à Centreon via l'adresse IP du serveur (http://172.16.1.17/centreon).

Nous avons donc ajouté tous les serveurs de notre infrastructure.

Nom	Alias	Adresse IP / DNS	Collecteur
DC1		172.16.1.10	Central
DC2		172.16.1.11	Central
glpi		172.16.1.16	Central
graylog		172.16.1.13	Central
IIS		172.16.1.20	Central
srv-fichier		172.16.1.12	Central

Nous avons également regroupé ces hôtes en groupe.

Ensuite, nous avons ajouté le modèle PING pour savoir si les serveurs sont allumés ou non.

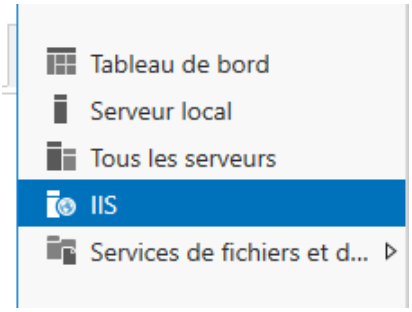
Groupe d'hôtes	Service	Planification	Modèle
Serveur_Linux	Ping Serveurs	5 min / 1 min	> Base-Ping-LAN > generic-active-service-custom > generic-active-service
Serveur_Windows	Ping Serveurs	5 min / 1 min	> Base-Ping-LAN > generic-active-service-custom > generic-active-service

Nous avons donc ajouté uniquement un test de la requête ping permettant de faire remonter les serveurs qui serait fonctionnel.

Mise en place de l'intranet (IIS) :

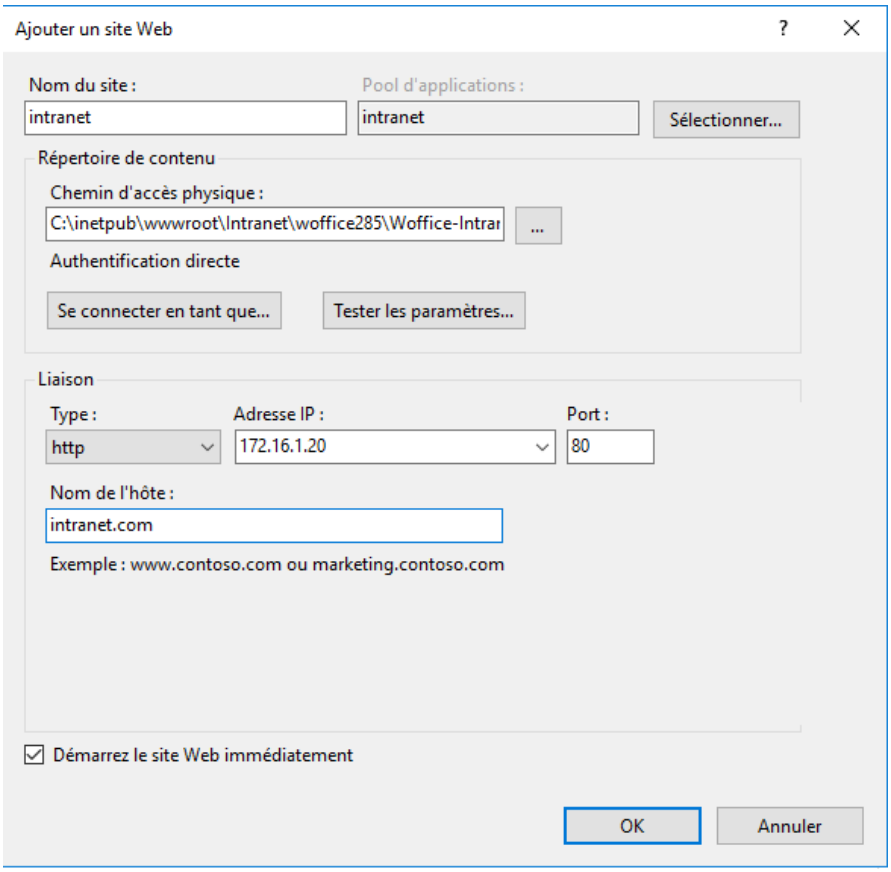
L'intranet de l'entreprise sera hébergé sur un serveur Web IIS. Nous avons décidé d'utiliser un Template Wordpress à cette adresse : https://www.vestathemes.com/ ; cette solution nous permet de gagner du temps tout en ayant un site opérationnel

Le rôle « IIS » devra être installé sur notre Windows Server 2016



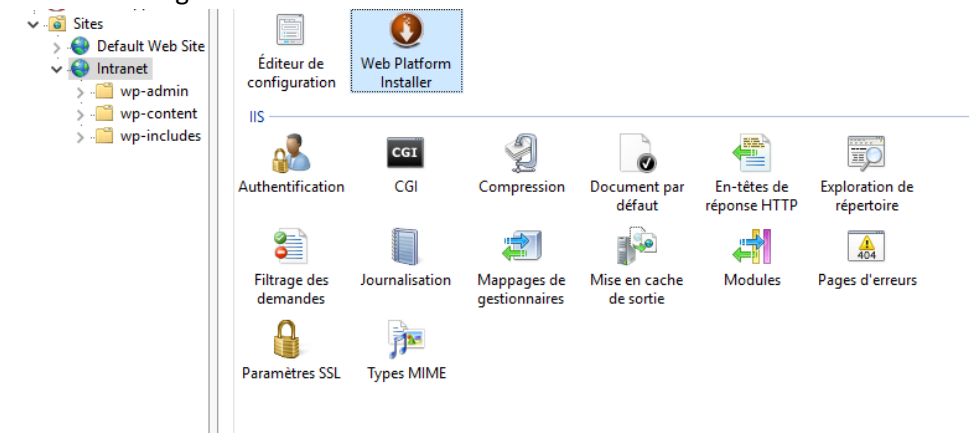
Nous pouvons désormais ajouter un site Web sur IIS :

- Nous le nommons « Intranet »
- Nous définissons son emplacement physique
- On renseigne son IP (ici nous prenons l'IP du serveur) ainsi que son port. Étant donné que notre intranet sera en http, nous choisissons le port 80

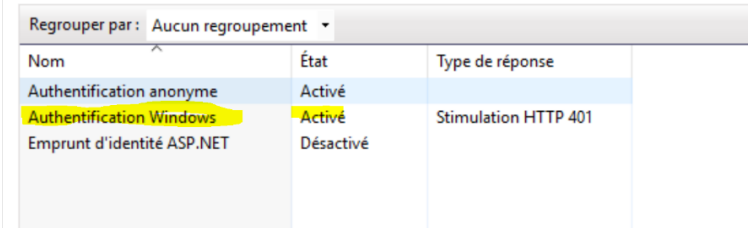


Ajout de l'alias « Intranet »

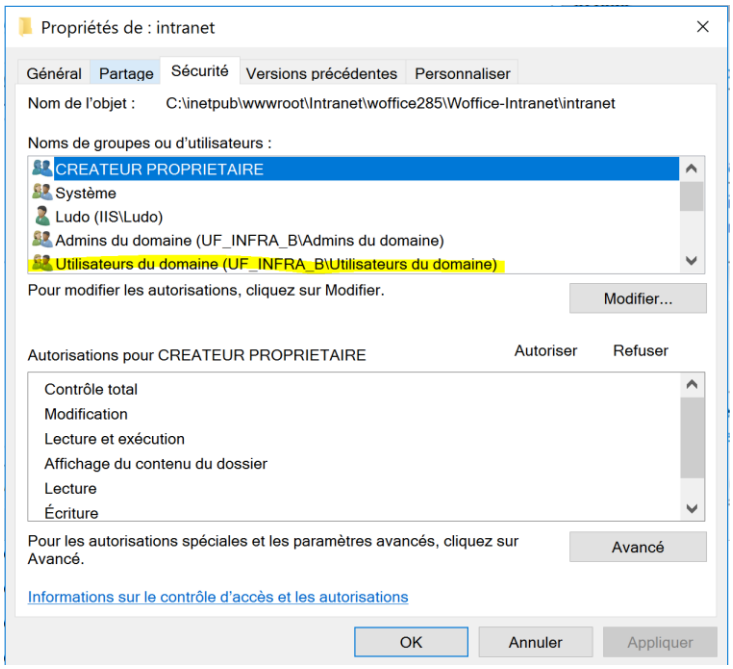
Le plugin Wordpress doit être installé. Pour cela nous allons utiliser le service « Web Platform Installer » intégré à IIS.



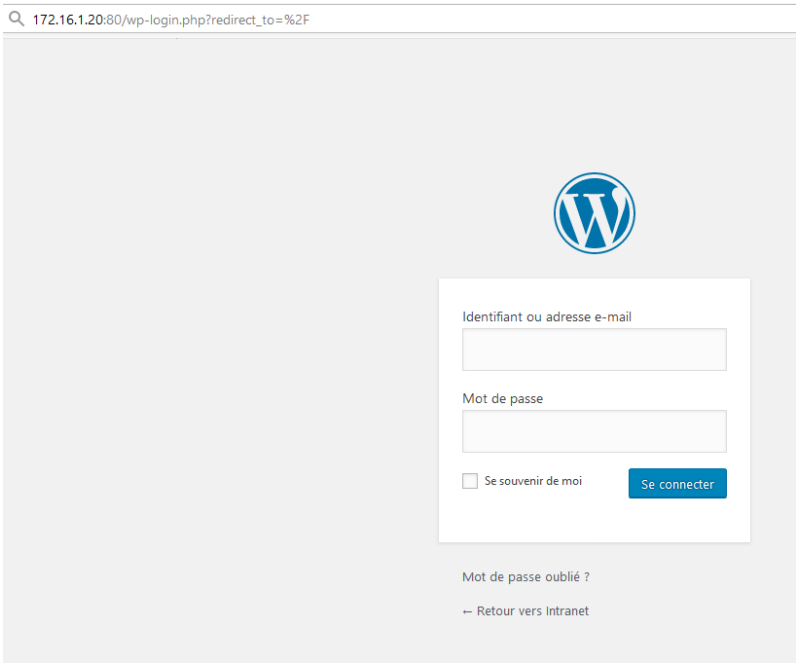
Gestion des authentifications : Nous avons ajouté l'authentification Windows afin que les clients puissent accéder au site grâce à leur compte du domaine



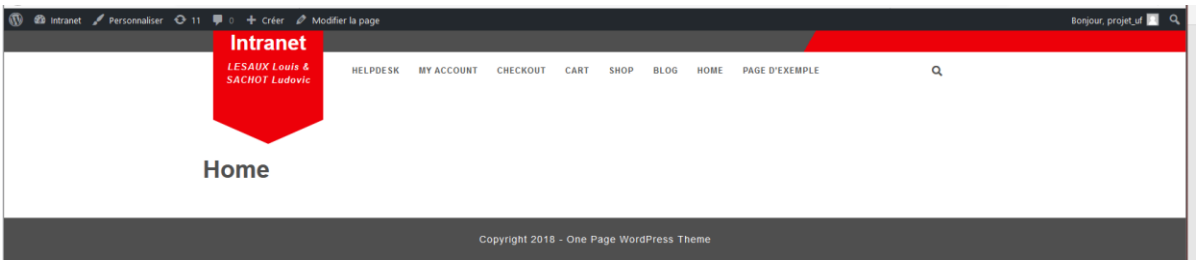
Gestion des droits : Permettre l'accès en lecture au dossier « Intranet » pour les utilisateurs du domaine afin de leur permettre de naviguer sur le site.



Il est désormais possible d'accéder à Wordpress depuis un navigateur

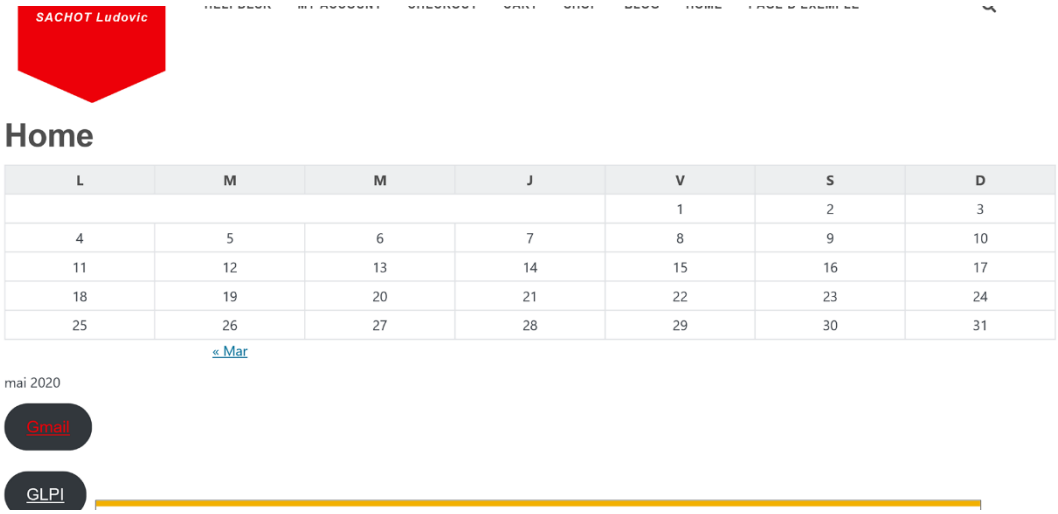


Nous atterrissons sur la page d'accueil de l'intranet



Nous avons implanté 2 boutons :

- Gmail : Permet aux collaborateurs d'accéder rapidement à leur boîte mail.
- GLPI : Permet d'accéder rapidement au service de ticketing de GLPI.


SACHOT Ludovic
Home
L M M J V S D
1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 31
« Mar
mai 2020
Gmail
GLPI

Gestionnaire de tickets (GLPI)

Le GLPI ou Helpdesk permet de centraliser l'ensemble du matériel informatique de l'entreprise de manière numérique. Il intègre notamment un service de « ticketing » qui permet de faciliter l'assistance informatique aux utilisateurs.

- GLPI tourne sur une VM Linux Debian 9
- Nous avons installé la version 9.3.3

GLPI à besoin d'un serveur Web pour être exploité. Nous avons décidé d'installer la pile LAMP :

- Linux → OS
- Apache → serveur Web -> version 2.4.25
- MariaDB → base de données -> version 10.1.44
- PHP → langage utilisé par GLPI -> version 7.0.33

Installation Apache

```
apt install apache2
```

Installation PHP

```
apt install php7.0 php7.0-curl php7.0-json php7.0-gmp php7.0-mbstring
php7.0-gd php7.0-mcrypt libapache2-mod-php7.0 php7.0-mysql php7.0-intl
php7.0-sqlite3 php7.0-xml php7.0-zip
```

Installation MariaDB & Configuration

```
apt install mariadb-server-10.1
```

Création de la database « GLPI ».

```
CREATE DATABASE glpi ;
```

```
+--------------------+
| Database           |
+--------------------+
| glpi               |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
```

Création de l'utilisateur « GLPI » et attribution des droits d'écriture/lecture

```
GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@'localhost' WITH GRANT OPTION;
```

```
+------+
| user |
+------+
| glpi |
| root |
+------+
```

On applique les modifications avec la commande `FLUSH PRIVILEGES;`

Configuration & Installation de GLPI

- Récupération de l'archive depuis GitHub.

```
wget https://github.com/glpi-project/glpi/releases/download/9.3.3/glpi-9.3.3.tgz
```

- Extraction de celle-ci

```
tar zxvf glpi-9.3.3.tgz
```

Afin que notre serveur Web puisse prendre en charge GLPI, nous devons déplacer son dossier dans `/var/www`, le répertoire prévu par Apache pour accueillir les services Web.

```
cp -r glpi /var/www/
```

Attribution des droits à « www-data », l'utilisateur qu'Apache utilise pour la gestion de ses services sur le dossier « GLPI »

```
chown -R www-data
```

Modification du fichier de conf Apache : Nous voulons que ce dernier voie notre site qui est situé dans `/var/www`. Par défaut Apache ne voit que les sites situés dans /`var/www/html`.

```
nano /etc/apache2/sites-available/000-default.conf
```

La ligne `DocumentRoot /var/www/html` devient `DocumentRoot /var/www/`

Installation d'extensions complémentaires

Nous installons certaines extensions optionnelles au bon fonctionnement de GLPI, notamment l'extension « LDAP », qui permettra l'interrogation des services d'annuaire (ici le LDAP d'Active Directory)

```
apt-get install php7.0-ldap php7.0-xmlrpc php7.0-imap php-apcu php-cas
```

Autorisation de la réécriture

```
a2enmod rewrite

nano /etc/apache2/sites-available/000-default.conf
```

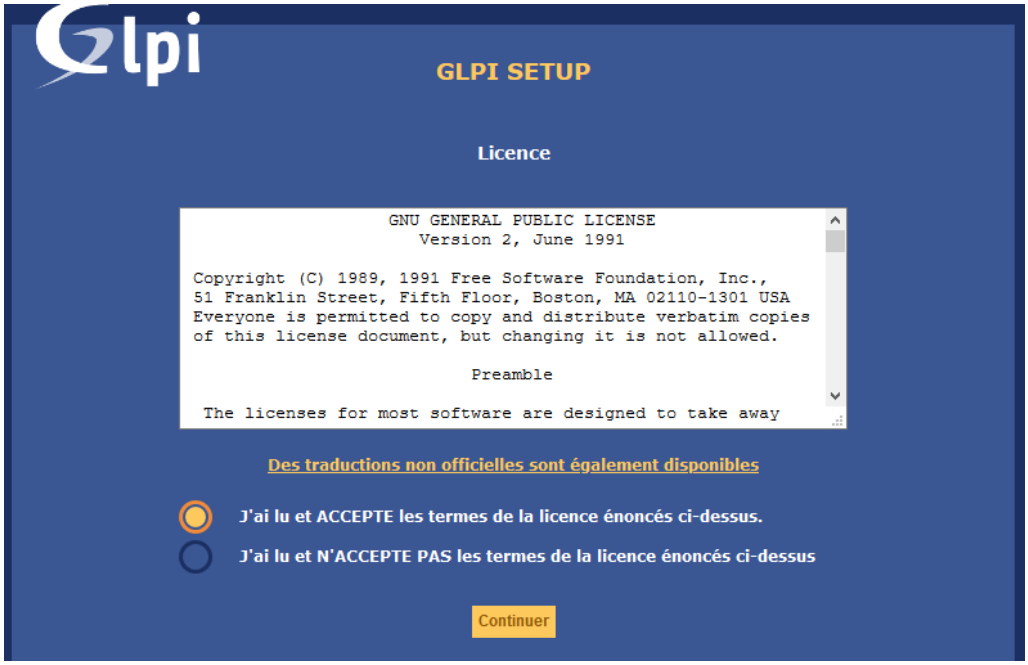
```
<Directory /var/www/glpi>
   Options Indexes FollowSymLinks
   AllowOverride All
   Require all granted
</Directory>
```

- Nous redémarrons Apache afin d'appliquer les changements

```
systemctl restart apache2
```

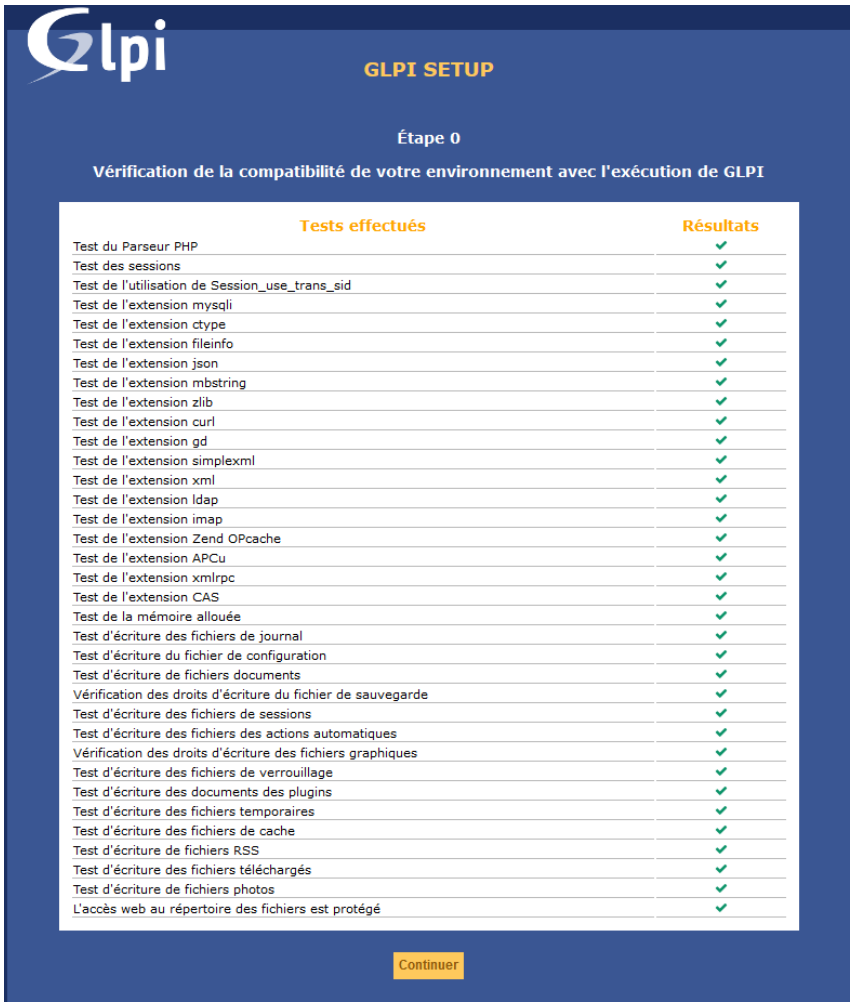
Nous pouvons désormais accéder à l'interface Web de la configuration de GLPI via un navigateur

Acceptation des termes de la licence



Nous voulons installer GLPI. Nous cliquons donc sur « Installer »

L'ensemble des tests de notre environnement est positif. Nous pouvons continuer.



Nous spécifions :

- Où se trouve la base de données GLPI
- L'utilisateur associé à cette même base

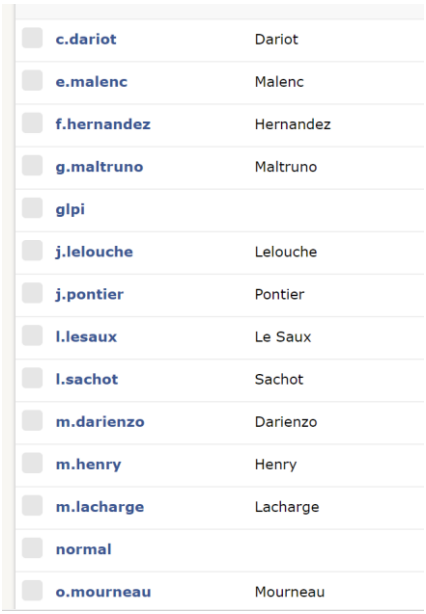
Sélection de la BDD « GLPI »

Initialisation de la BDD OK

Nous sommes renseignés des login précrées par GLPi ainsi que de leur utilité

Nous pouvons désormais nous connecter.

Après avoir ajouté le serveur GLPI au domaine (uf_infra_B.local), nous avons récupéré les utilisateurs de l'annuaire LDAP.



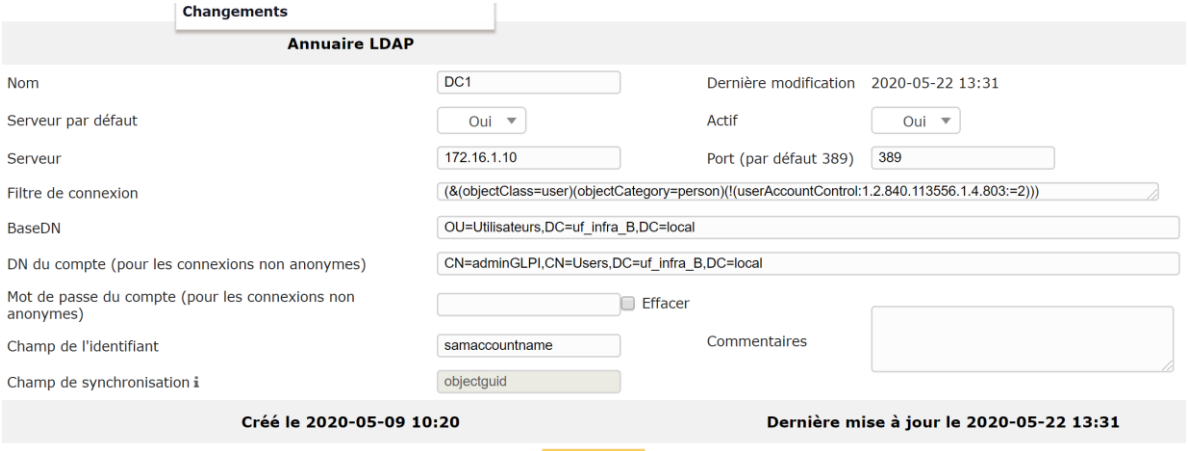
c.dariot	Dariot
e.malenc	Malenc
f.hernandez	Hernandez
g.maltruno	Maltruno
glpi	
j.lelouche	Lelouche
j.pontier	Pontier
l.lesaux	Le Saux
l.sachot	Sachot
m.darienzo	Darienzo
m.henry	Henry
m.lacharge	Lacharge
normal	
o.mourneau	Mourneau

Pour cela, grâce au compte administrateur du GLPI, nous sommes allés dans :

Configuration → authentification puis dans « annuaire LDAP ».

Ici, nous avons ajoutés l'adresse IP du DC1 puis nous avons référencé l'endroits où se situe tous les comptes utilisateurs de l'AD (OU=Utilisateurs,DC=uf_infra_B,DC=local).

Nous avons également créé un compte administrateur pour GLPI sur l'AD (adminGLPI).



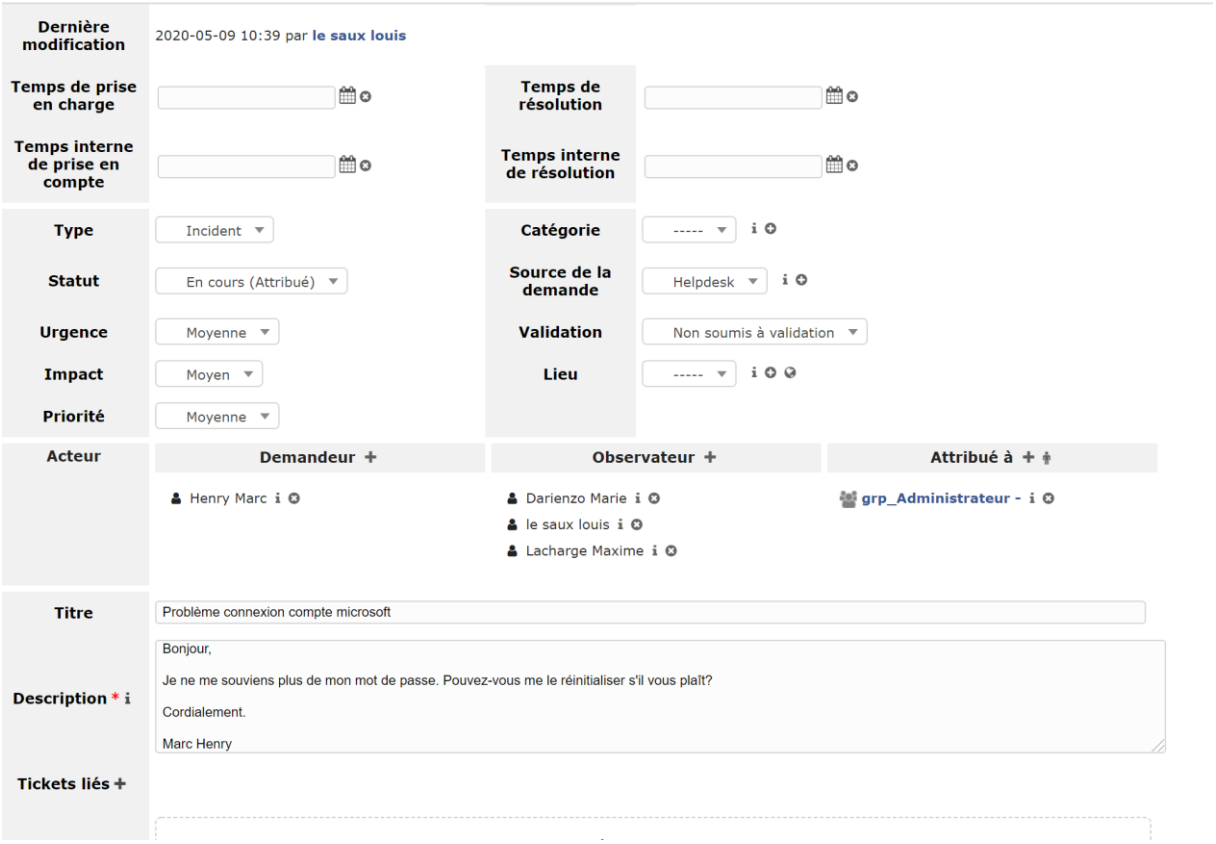
Changements

Annuaire LDAP

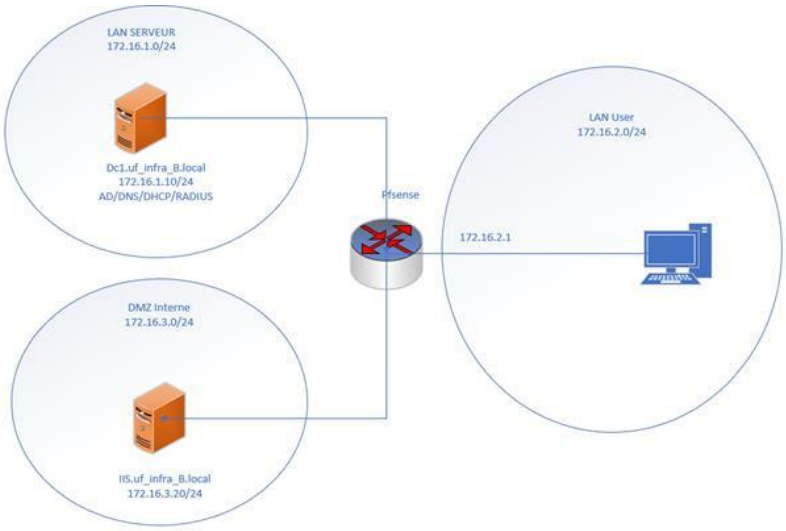
Nom	DC1	Dernière modification	2020-05-22 13:31
Serveur par défaut	Oui	Actif	Oui
Serveur	172.16.1.10	Port (par défaut 389)	389
Filtre de connexion	(&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))		
BaseDN	OU=Utilisateurs,DC=uf_infra_B,DC=local		
DN du compte (pour les connexions non anonymes)	CN=adminGLPI,CN=Users,DC=uf_infra_B,DC=local		
Mot de passe du compte (pour les connexions non anonymes)	Effacer		
Champ de l'identifiant	samaccountname	Commentaires	
Champ de synchronisation	objectguid		

Créé le 2020-05-09 10:20 **Dernière mise à jour le 2020-05-22 13:31**

Après avoir tester si les comptes était bien remonté, nous avons créé une simulation de ticket envoyé par le directeur à l'équipe serveur pour « un oubli de mot de passe ».



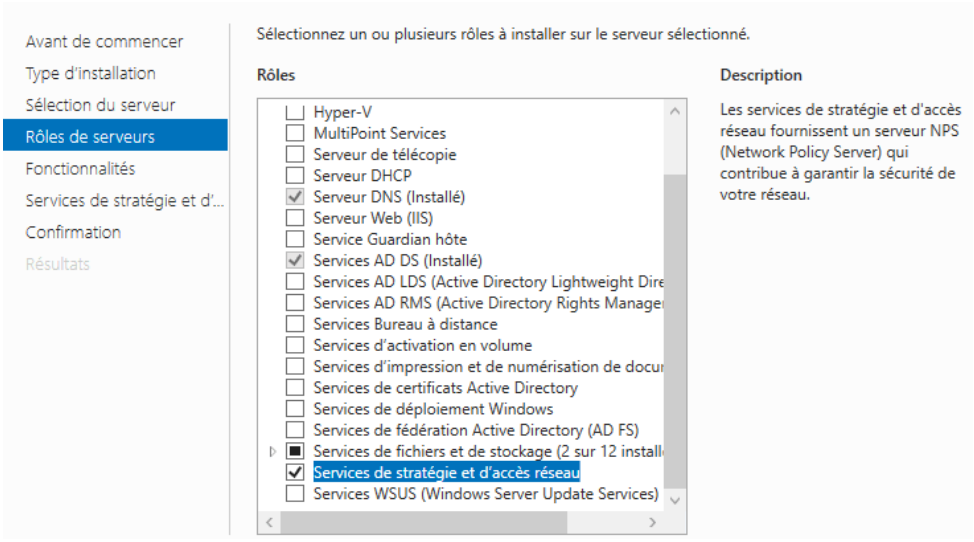
Portail captif



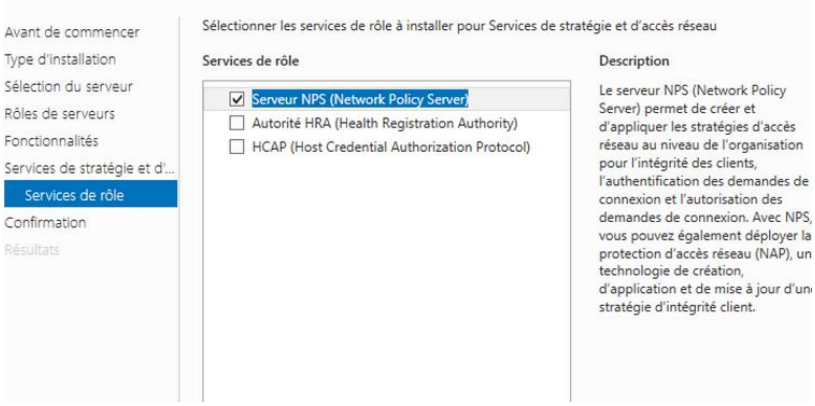
Afin de permettre un accès à certaines applications depuis l'extérieur du réseau de l'entreprise depuis n'importe quel appareil, connecté au domaine ou non, il est possible de mettre en place un portail captif hébergé sur le routeur Pfsense

Cette partie n'a pas été réalisée par manque de temps et de moyens. Sa mise en place sera tout de même expliquée. Les captures d'écrans qui vont suivre proviennent d'Internet

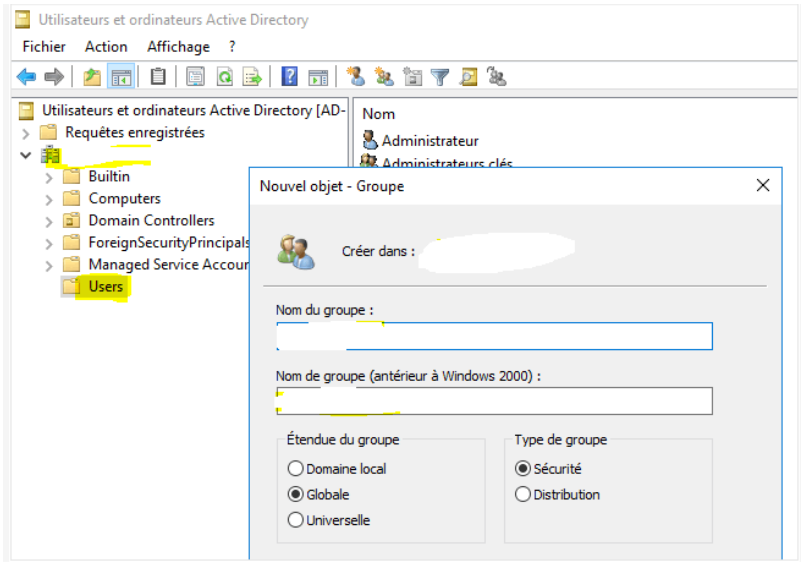
- Installation du service de stratégies et d'accès réseau



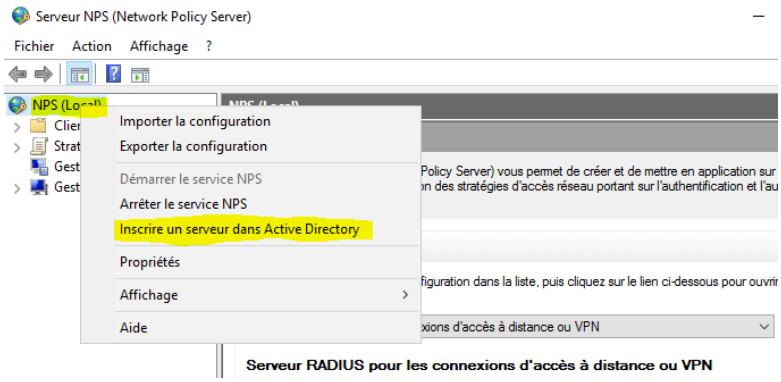
- Installation du rôle NPS

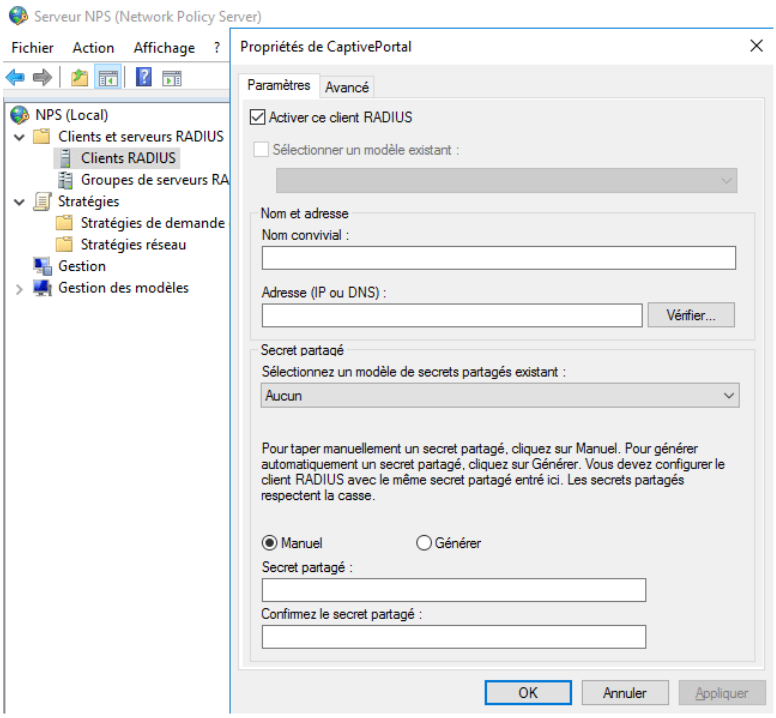


- Création d'un groupe de sécurité « portail captif » rassemblant tous les utilisateurs ayant le droit de se connecter au portail captif

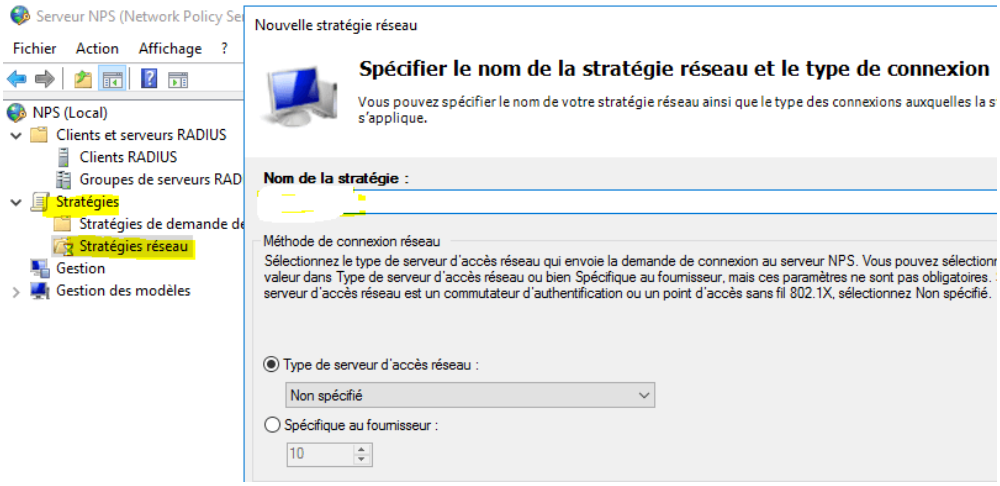


- Création d'un nouveau client RADIUS : le renseignement d'un secret partagé permet de chiffrer les transactions entres les clients et le serveur RADIUS. Il est donc à retenir

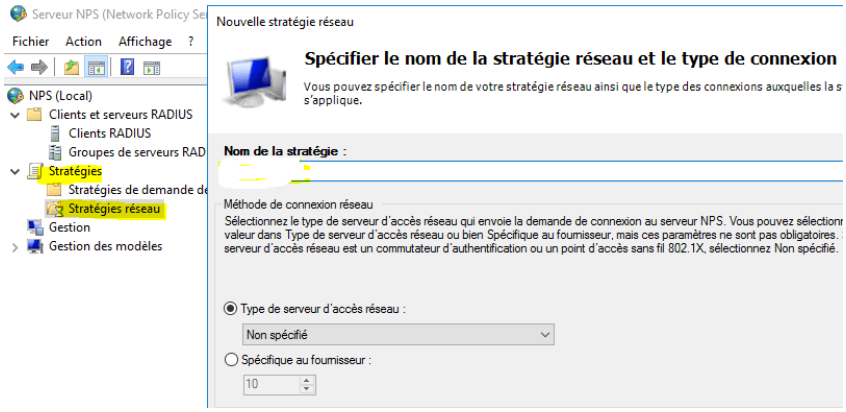




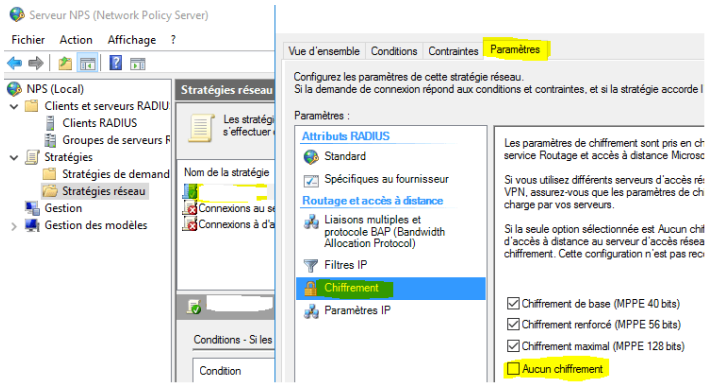
Configuration d'une stratégie réseau. Elle gérera les droits d'accès et permettra d'autoriser l'accès au portail le groupe de sécurité « portail captif » crée précédemment.



Nous ajoutons le groupe « portail captif » crée précédemment afin d'autoriser les membres à communiquer avec RADIUS

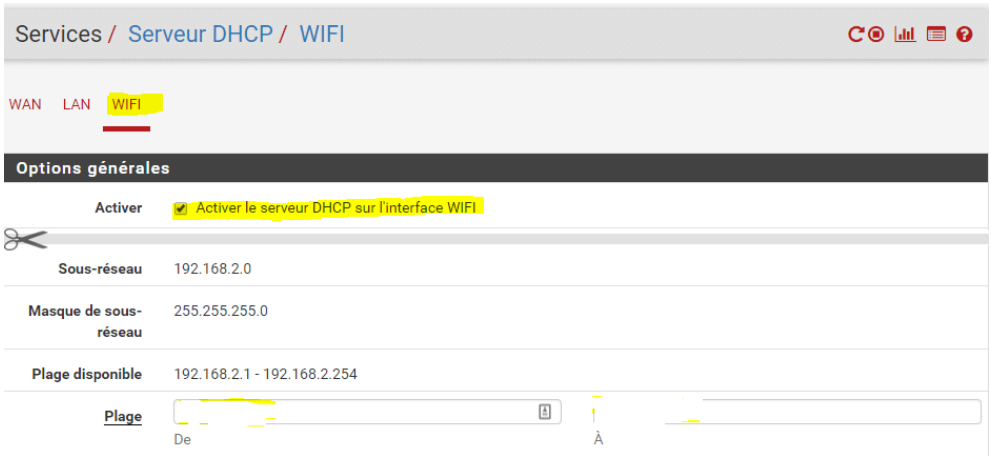


Afin de garantir un niveau de sécurité élevé, nous décochons la case « Aucun chiffrement »



Configuration Pfsense

- Activer le serveur DHCP sur l'interface WIFI



- Activation de la résolution DNS

Nous renseignons un nom descriptif, le type et le protocole d'authentification , le secret partagé, les ports d'écoute et l'IP sur serveur RADIUS.

Configuration du portail captif

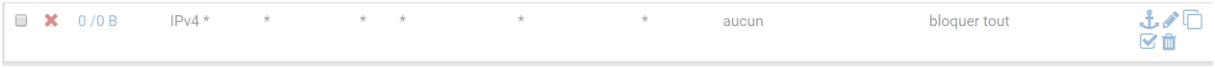
- ☑ **Activer le Portail Captif**
  - Interfaces : **WIFI**
  - ☑ **Activer la fenêtre de dialogue de fermeture de session**
  - Après authentification Redirection URL : *https://google.fr*
- Allez dans la partie **Authentification**
  - Méthode d'authentification : **Use an Authentication backend**
  - Serveur d'authentification : **CaptivePortal**
  - ☑ **Réauthentifier les utilisateurs connectés chaque minute**
- Allez dans la partie Comptabilité
  - ☑ **Send RADIUS accounting packets.**

Routeur/Firewall (Pfsense) :

Pour notre infrastructure, nous avons mis en place 2 réseau LAN différents. Le « LAN serveurs » (172.16.1.0/24) dédié à tous les serveurs installés précédemment et le « LAN user » dédié au poste de travail des utilisateurs de notre infrastructure. Il y a également une interface « WAN » dédié à la sortie vers Internet.

Règles pare-feu :

Tout d'abord, pour le LAN Users, nous avons ajouté une règle qui bloque tout le trafic. Cette règle sera positionnée en dernière position permettant de bloquer tous ce que nous n'avons pas ouvert.



Nous avons ensuite ouvert les ports 53, 389, 445, 139, 1025, 1026, 3268, 88, 137 et 138. L'ouverture de ces ports est obligatoire pour que les postes de travail des utilisateurs puissent communiquer dans le domaine.

Nous avons également ouvert les ports 80 et 443 pour que les utilisateurs puissent accéder à Internet.

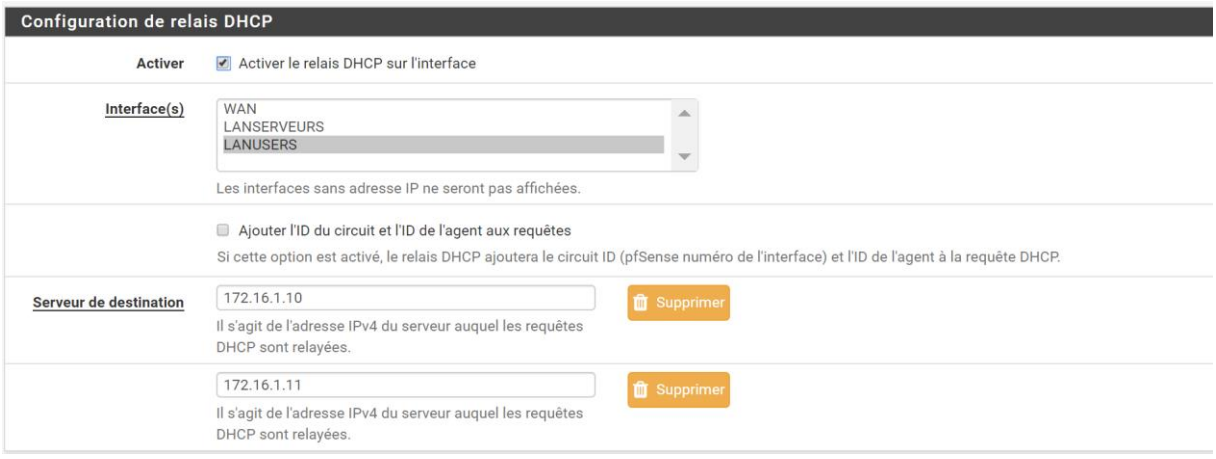
Les ports 67 (serveur DHCP) et 68 (client DHCP) ont également été ouvert pour que les clients puissent récupérer leur adresse IP auprès du serveur DHCP (DC1.uf_infra_B.local).

Nous avons également ouvert le protocole ICMP pour pouvoir effectuer des tests.

	États	Protocole	Source	Port	Destination	Port	Passerelle	d'attente	Ordonnancement	Description	Actions
	✔ 0 /0 B	IPv4 TCP/UDP	LANUSERS net	*	LANSERVEURS net	67 - 68	*	aucun		DHCP	
	✔ 0 /57.62 MiB	IPv4 TCP/UDP	LANUSERS net	*	*	443 (HTTPS)	*	aucun			
	✔ 0 /105.11 MiB	IPv4 TCP/UDP	LANUSERS net	*	*	80 (HTTP)	*	aucun			
	✔ 0 /0 B	IPv4 UDP	LANUSERS net	*	LANSERVEURS net	138 (NetBIOS-DGM)	*	aucun			
	✔ 0 /0 B	IPv4 UDP	LANUSERS net	*	LANSERVEURS net	137 (NetBIOS-NS)	*	aucun			
	✔ 0 /0 B	IPv4 TCP/UDP	LANUSERS net	*	LANSERVEURS net	88	*	aucun		kerberos	
	✔ 0 /0 B	IPv4 TCP	LANUSERS net	*	LANSERVEURS net	3268	*	aucun		LDAP Global Catalogue	
	✔ 0 /0 B	IPv4 TCP	LANUSERS net	*	LANSERVEURS net	1025 - 1026	*	aucun		RPC	
	✔ 0 /0 B	IPv4 TCP	LANUSERS net	*	LANSERVEURS net	139 (NetBIOS-SSN)	*	aucun			
	✔ 0 /20 KiB	IPv4 TCP	LANUSERS net	*	LANSERVEURS net	445 (MS DS)	*	aucun			
	✔ 0 /0 B	IPv4 TCP	LANUSERS net	*	LANSERVEURS net	389 (LDAP)	*	aucun			
	✔ 0 /1 KiB	IPv4 TCP/UDP	LANUSERS net	*	LANSERVEURS net	53 (DNS)	*	aucun			
	✔ 0 /0 B	IPv6 ICMP any	LANUSERS net	*	*	*	*	aucun			
	✔ 0 /5 KiB	IPv4 ICMP any	LANUSERS net	*	*	*	*	aucun		autoriser lan user vers tout le monde	
	✖ 0 /0 B	IPv4 *	*	*	*	*	*	aucun		bloquer tout	

Relai DHCP :

Nous avons également configuré le relai DHCP sur le PFsense pour que le LAN User puisse récupérer des adresses IP auprès du serveur DHCP.



Mise en place des Blacklists :

Nous avons décidé, comme tout bon administrateur, de bloquer certains site web pour que les utilisateurs se concentre uniquement sur leur travail.

Nous avons donc récupéré une liste existante faites par l'université de Toulouse 1 Capitole :

http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz.

Nous avons donc commencé par télécharger les paquets « Squid ».

Paquets installés

	Nom	Catégorie	Version	Description	Actions
✔	Lightsquid	www	3.0.6_6	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. Dépendances du paquet: lighttpd-1.4.54 lightsquid-1.8_5	
✔	squid	www	0.4.44_25	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Dépendances du paquet: squidclamav-7.1 squid_radius_auth-1.10 squid-4.10 c-icap-modules-0.5.4	
✔	squidGuard	www	1.16.18_5	High performance web proxy URL filter. Dépendances du paquet: squidguard-1.4_15	

Ensuite, nous allons activer les blacklists sur le Pfsense et ajouter l'URL de téléchargement.

Blacklist options

Blacklist ☑ Check this option to enable blacklist

Do NOT enable this on NanoBSD installs!

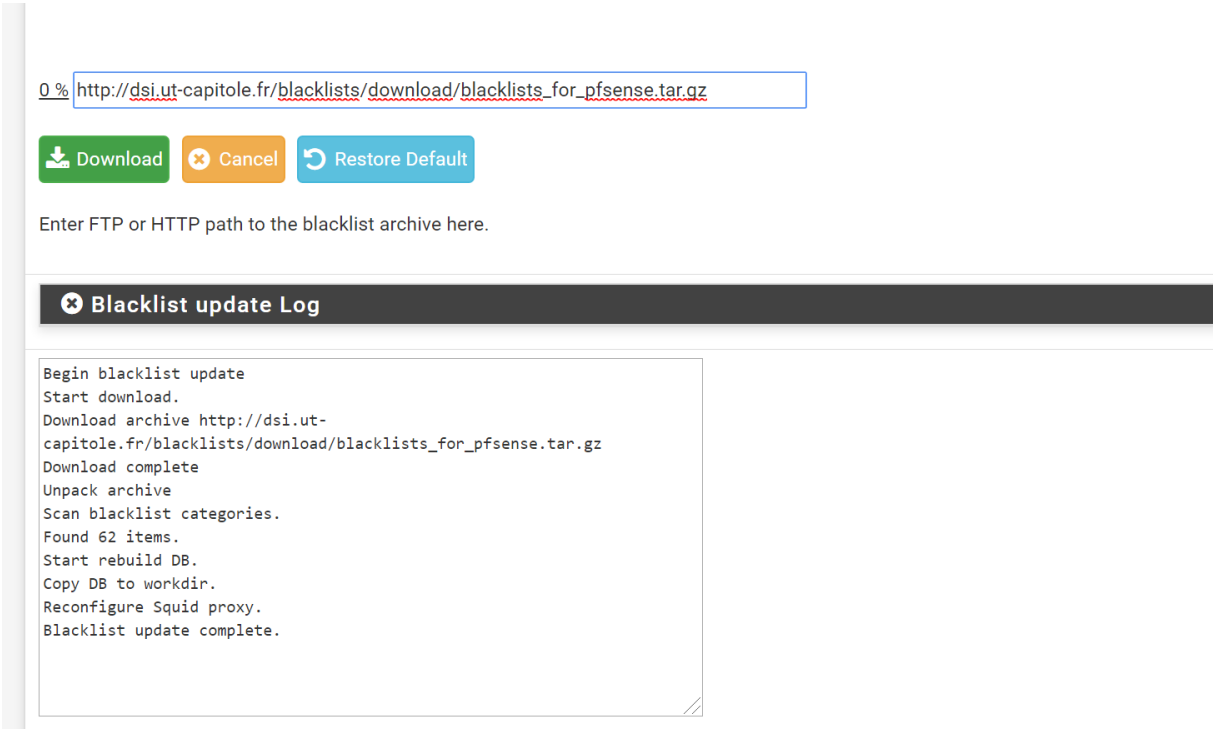
Blacklist proxy

Blacklist upload proxy - enter here, or leave blank.
Format: host:[port login:pass] . Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'

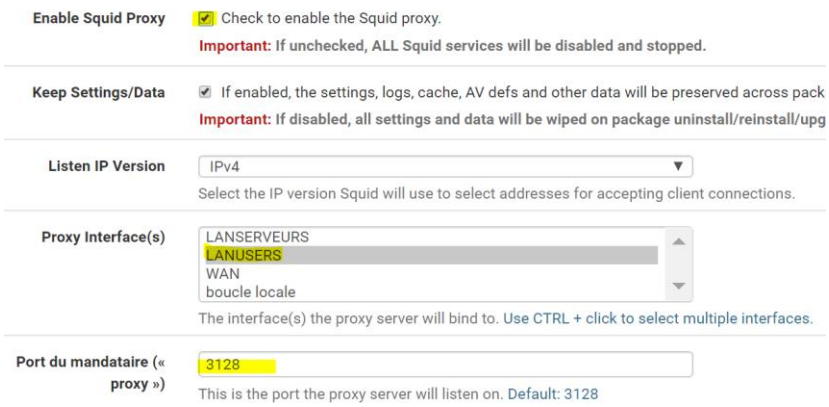
Blacklist URL http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.

Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or

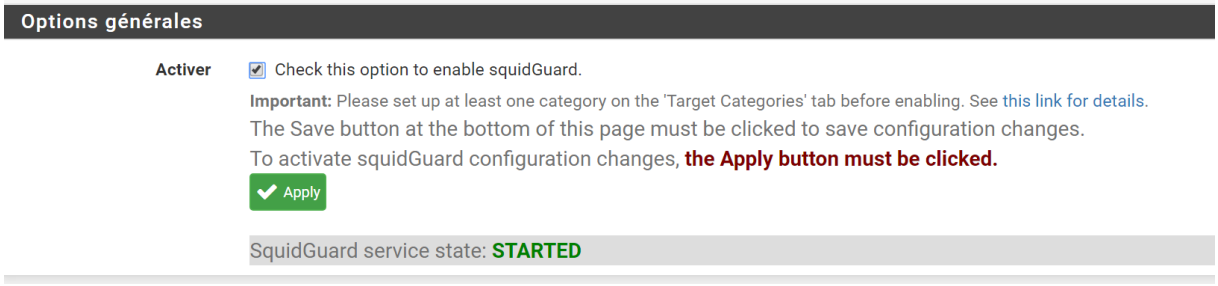
Ensuite, nous avons téléchargé la blacklist de Toulouse dans « SquidGuard Proxy Filter ».



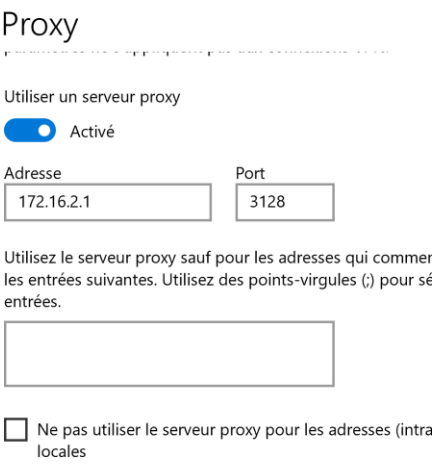
Après cela, dans le service « Squid Proxy Server », nous avons activer le serveur proxy en précisant qu'il sera actif sur l'interface du LAN user sur le port 3128.



Pour finir, nous sommes retournés dans l'onglet « SquidGuard Proxy Filter » et nous avons activer squidGuard.



Ensuite, sur la machine cliente, nous avons ajoutés un proxy (en ajoutant l'adresse de l'interface et le port utilisé).

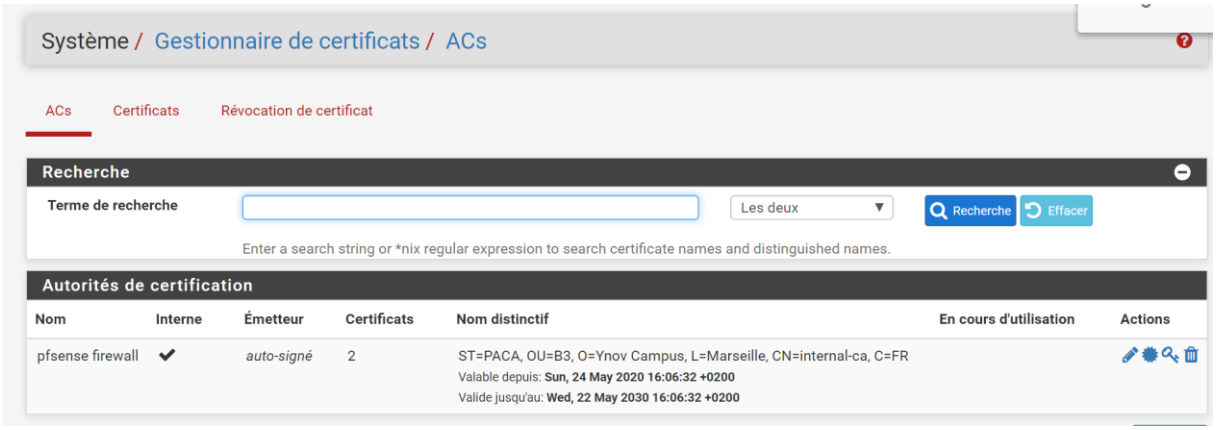


Nous avons choisi un site de la blacklist et nous voyons bien que celle-ci est fonctionnelle.

OpenVPN :

Il est possible avec Pfsense de mettre en place directement le VPN sur le routeur, ce qui nous évite d'avoir un serveur dédié à cette tâche.

Pour cela, nous allons commencer par créer notre autorité de certification.

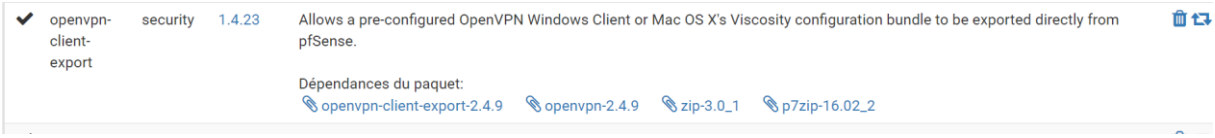


Ensuite, nous avons créé un certificat pour le serveur.

Nous avons également créé un utilisateur sur le Pfsense. A la fin, celui-ci pourra se connecter au réseau local via le VPN.

Ensuite, nous allons ajouter un certificat client VPN à cet utilisateur.

Après avoir créé les certificats, nous avons ajoutés les paquets OpenVPN-Client-Export sur le Pfsense.



(Nous n'avons pas eu le temps de terminer cette installation.) Nous avons donc uniquement créé les certificats pour nous connecter au VPN, mais nous n'avons pas mis en place le serveur VPN.

Sauvegarde des VM :

Il est très important dans une entreprise de sauvegarder les serveurs dans un réseau distant. Dans ce cas, si l'entreprise subit une attaque de grande ampleur, il est facile de remettre en place l'infrastructure en faisant remonter les sauvegardes. Pour cela, il est donc primordial que ces sauvegardes soit dans un réseau distant.

Dans notre cas, nous avons décidé de les intégré dans un dossier du one drive Ynov campus. Ce dossier est partagé entre les membres de l'équipe.