FICHE DE SUIVI

Table des matières

[Réseau 2](#_Toc7691165)

[PFSense 2](#_Toc7691166)

[Règles de pare-feu 2](#_Toc7691167)

[Redirection du flux http et HTTPS vers le serveur web 2](#_Toc7691168)

[Squid 3](#_Toc7691169)

[VLAN 5](#_Toc7691170)

[Contrôleur de domaine 5](#_Toc7691171)

[Configuration d’une adresse IP statique et d’un nom 5](#_Toc7691172)

[Exporter les utilisateurs dans un fichier. 6](#_Toc7691173)

[Configuration machine client et ajout au domaine 7](#_Toc7691174)

[Création des utilisateurs et OU par script 7](#_Toc7691175)

[Mise en place des GPO 9](#_Toc7691176)

[Contrôleur de domaine supplémentaire 14](#_Toc7691177)

[NAS 17](#_Toc7691178)

[Zabbix 20](#_Toc7691179)

[GLPI 23](#_Toc7691180)

## Réseau

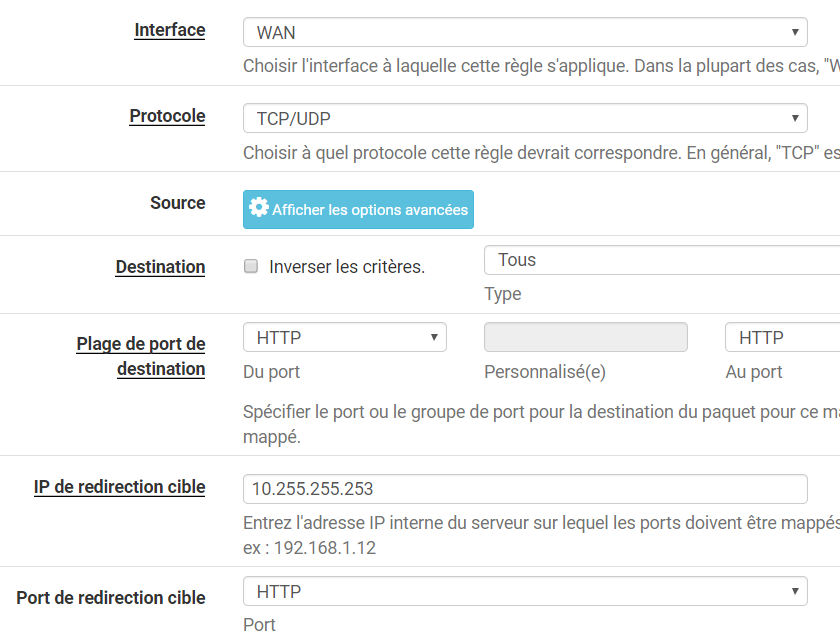
## PFSense

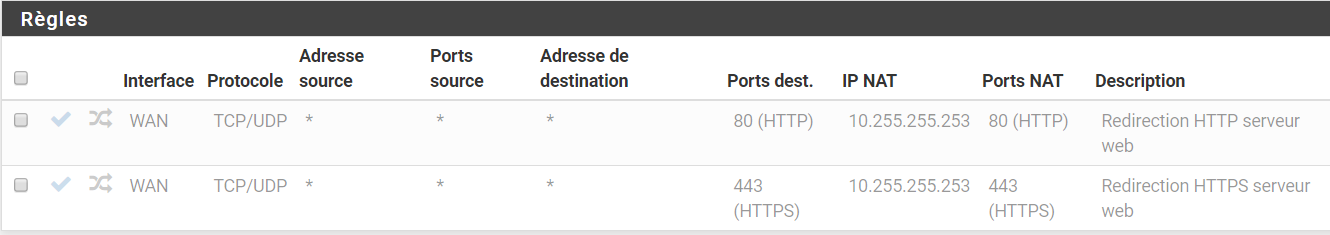
### Règles de pare-feu

On créera les règles de pare-feu suivantes :

* Autoriser @IP depuis le WAN pour connexion SSH port 22 qui sera redirigée vers les serveur Proxmox
* Autoriser depuis WAN vers DMZ (srv web) pour connexion http port 80
* Autoriser depuis WAN vers DMZ (srv web) pour connexion HTTPS port 443
* Autoriser depuis LAN vers DMZ pour connexion ICMP
* Autoriser depuis LAN vers DMZ pour connexion sur le port 10050
* Autoriser depuis DMZ vers @IP Zabbix LAN pour connexion sur le port 10051
* Autoriser depuis DMZ vers LAN pour connexion ICMP

### Redirection du flux http et HTTPS vers le serveur web

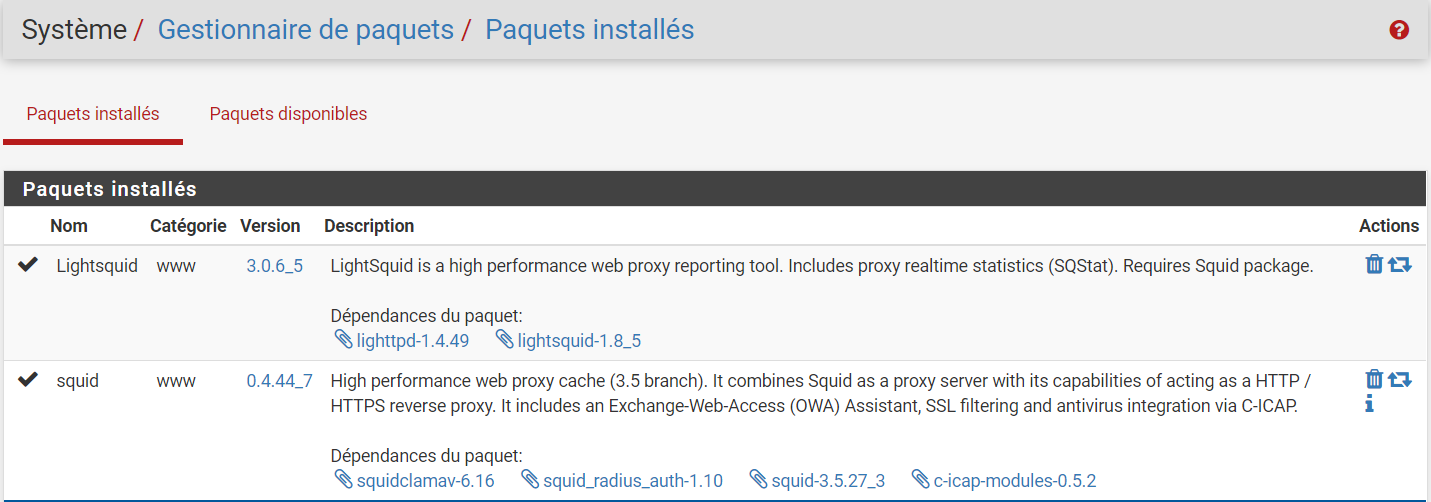
On souhaite faire en sorte que les flux http et HTTPS venant du WAN soient redirigés vers le serveur web présent dans la DMZ. Pour cela, on créera deux règles de NAT (Port fowarding), l’une pour l’http et l’autre pour l’HTTPS.



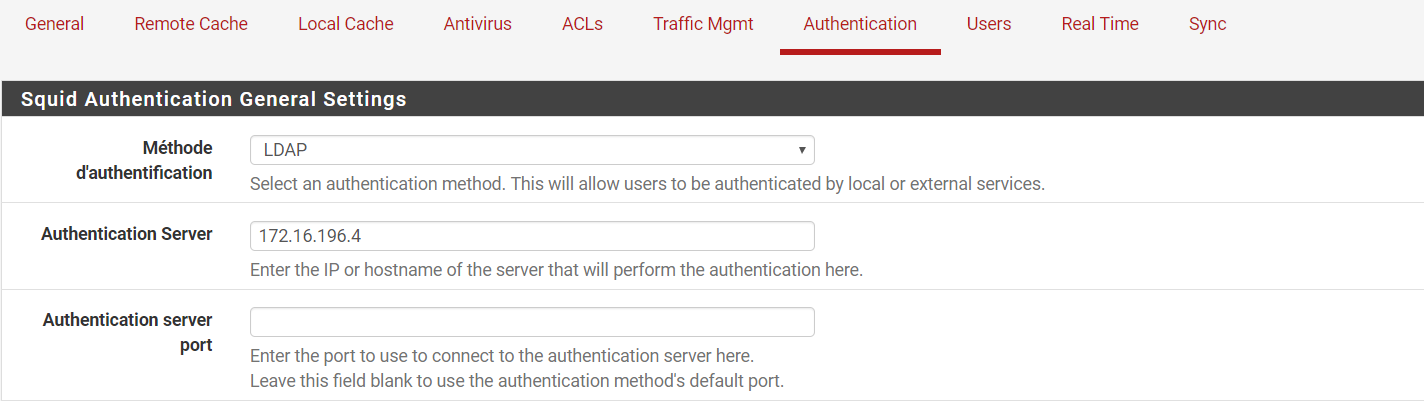
On verra ensuite que deux règles ont été créées dans **Pare-feu > Règles**, on les activera.

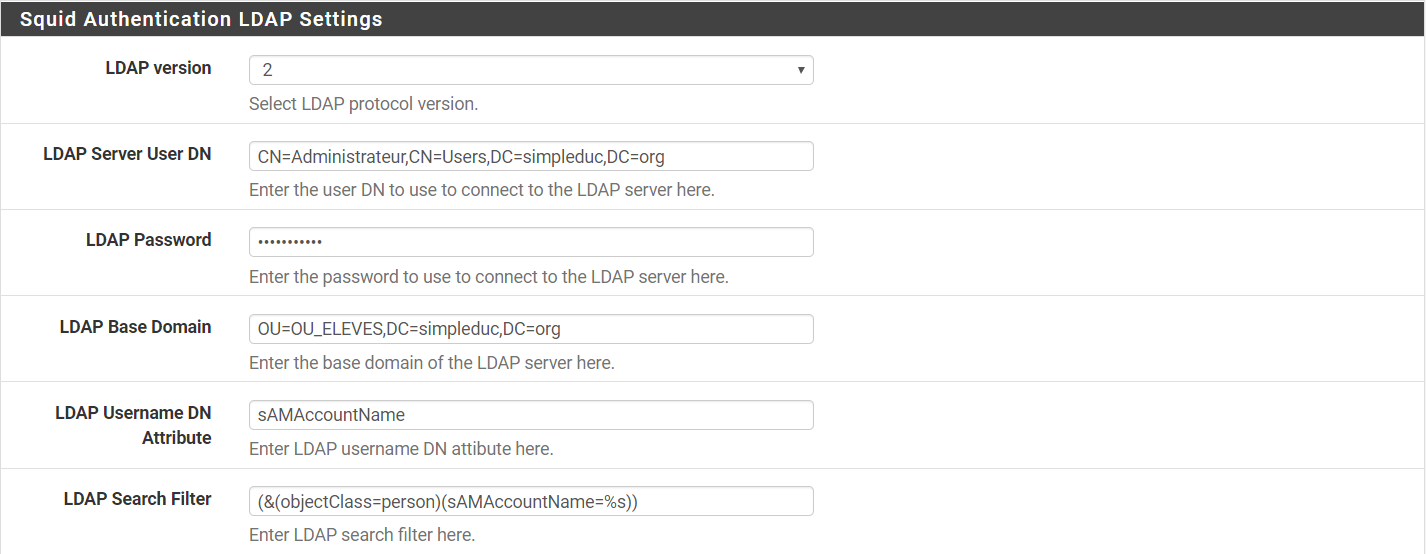
### Squid

On installe les paquets nécessaire à la mise en place de Squid et Lightsquid sur PFSense

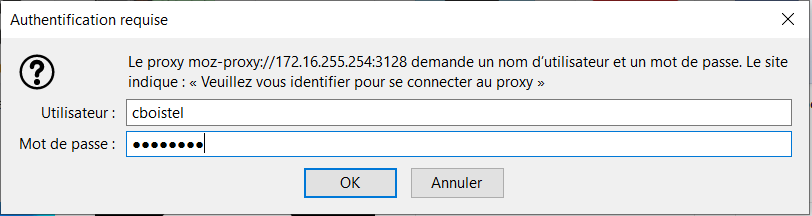


On configurera ensuite le proxy de façon qu’une identification soit requise pour se connecter à internet via le proxy. On configurera celle-ci pour qu’elle se fasse via le LDAP, on configurera donc de la façon suivant :



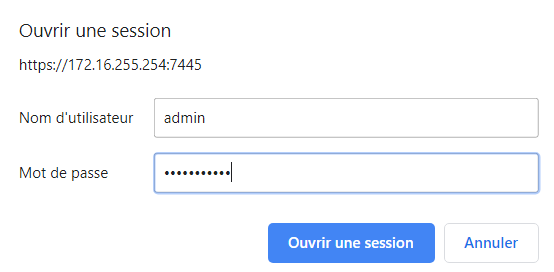


On peut voir qu’une identification est requise lorsque l’on rentre les paramètres du proxy dans notre navigateur.

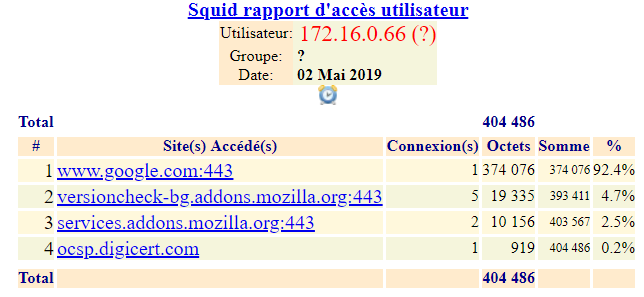


En entrant le login et mot de passe d’un compte présent dans l’OU OU\_ELEVES de l’active directory, on peut maintenant avoir accès à internet.

On veut également mettre en place un reporting des connexions faites via le proxy. Pour cela, on configurera Lightsquid dans **Etat > Squid Proxy Report**. On changera le mot de passe de connexion et on passera le langage pour français. On rafraichira la page et on pourra accéder aux rapports.



On se connecte avec les identifiants que l’on vient de définir. On a enfin accès aux rapports, ranger par date. Ici, on peut voir un screen de l’affichage par utilisateurs.



## Contrôleur de domaine

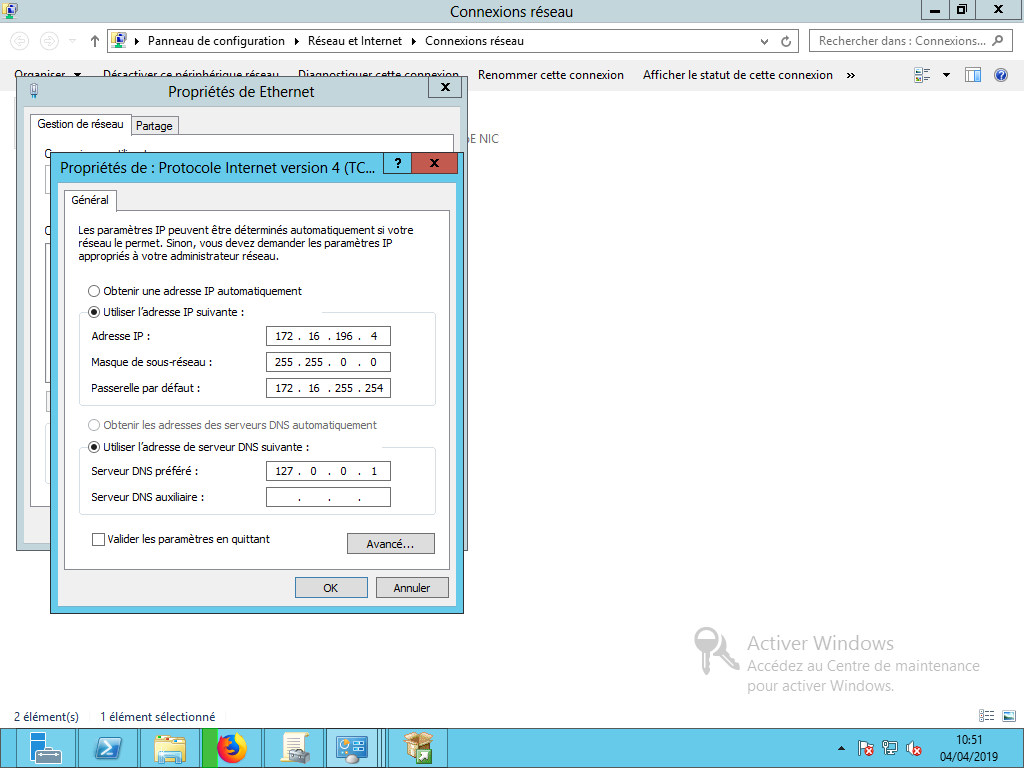
### Configuration d’une adresse IP statique et d’un nom

IP : 172.16.196.4

Masque : 255.255.0.0

Passerelle : 172.16.255.254 (IP coté LAN du routeur)

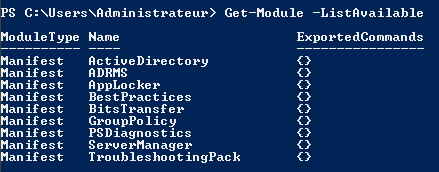
L’active directory est déjà mis en place avec un DNS.



On mettra localhost en DNS, puis on modifiera le nom de l’ordinateur pour DC-01. Il faut ensuite redémarrer la machine.

### Exporter les utilisateurs dans un fichier.

Dans power shell, on peut voir les modules disponible



On peut voir les commandes disponibles pour le module en question



On récupère les tous utilisateurs présent dans l’AD, puis on exporte dans le fichier présent dans C:\scripts

On délimite les utilisateurs avec des ; et on précise l’encodage.

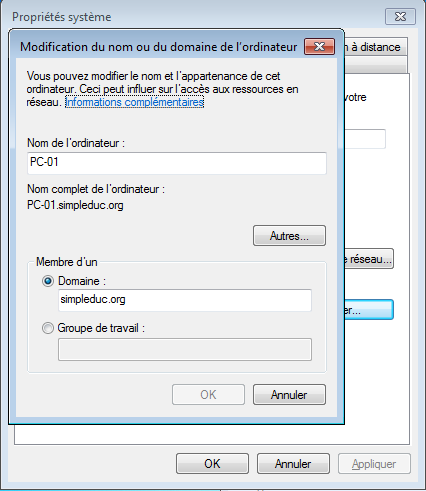


### Configuration machine client et ajout au domaine

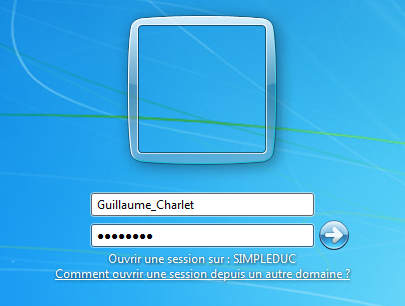
Machines virtuelles sous Virtual Box. Le système d’exploitation est **Windows 7 Professionnel.** Ces machines virtuelles sont soit déjà intégrées au domaine **simpleduc.org** soit hors domaine.

Adressage IP dynamique, adresses fournies par le DHCP installé et configuré sur le routeur PFSENSE.

Ajout du poste dans le domaine simpleduc.org

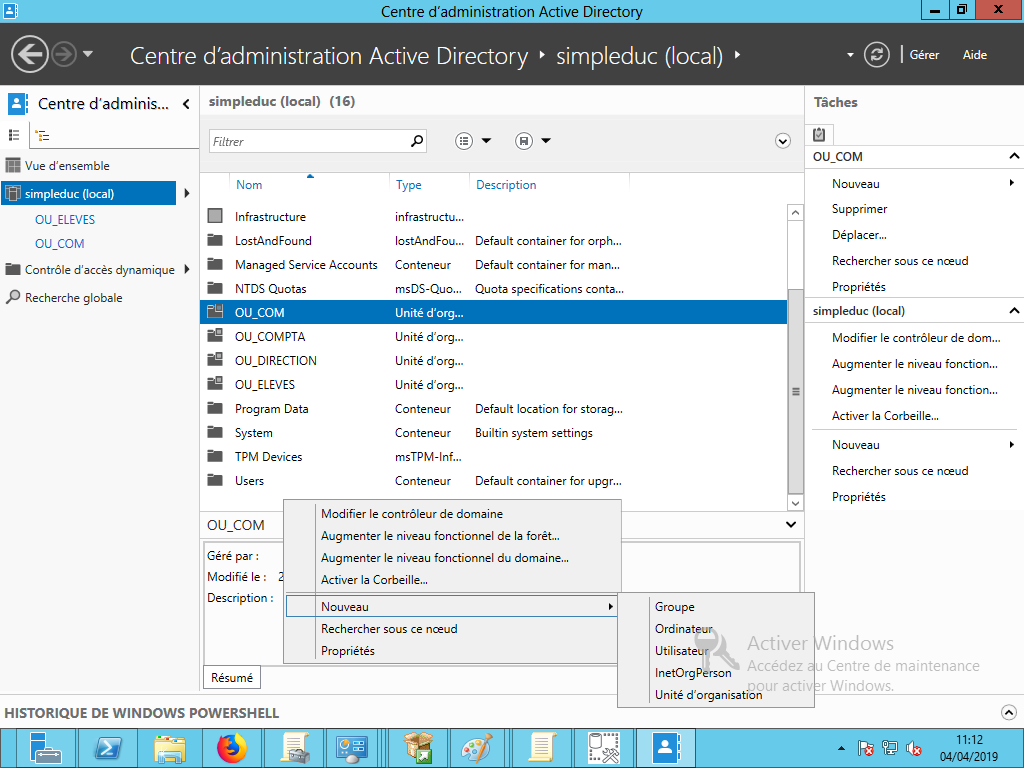


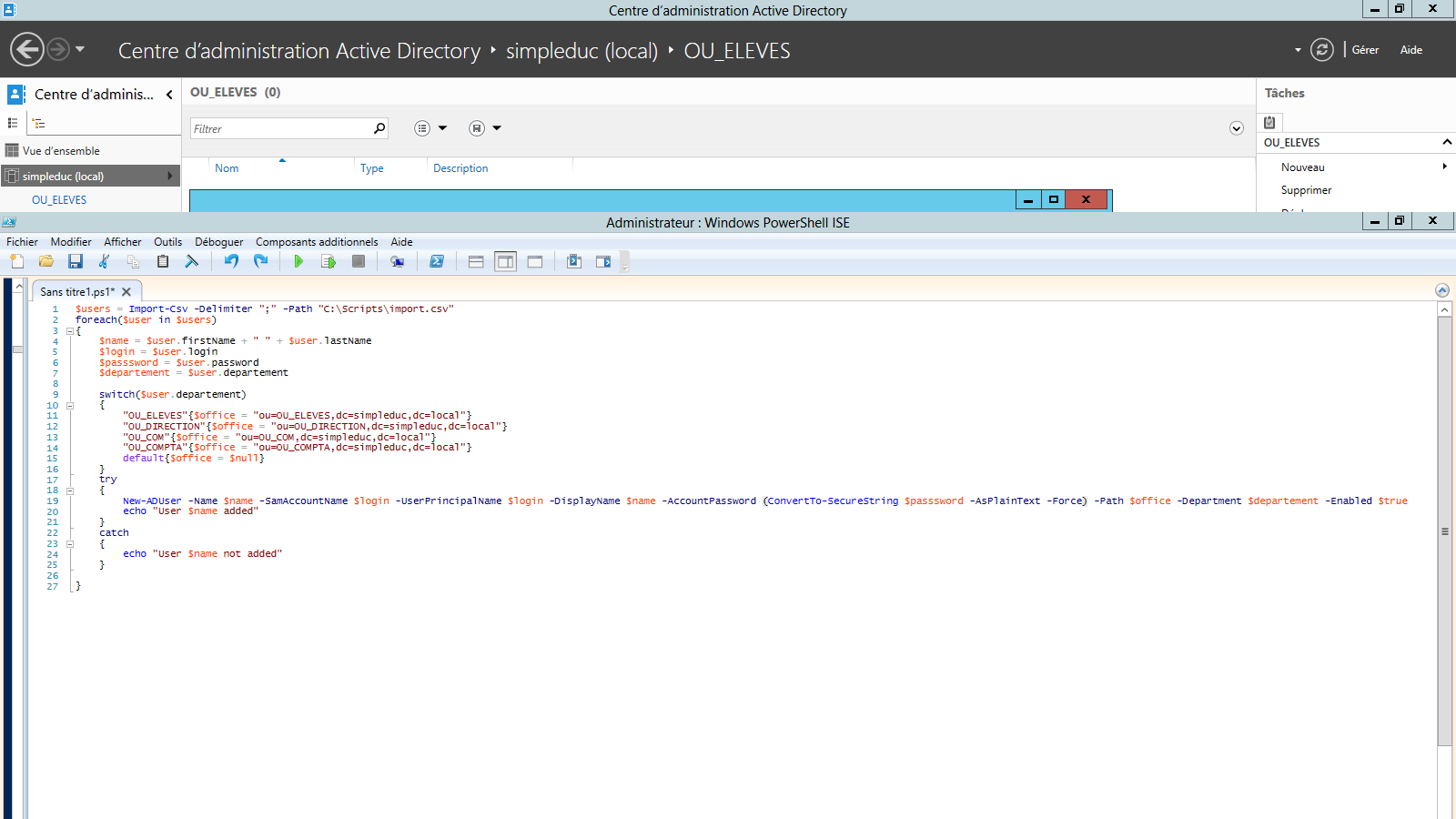
On redémarre le pc et on peut maintenant se connecter avec l’active directory.



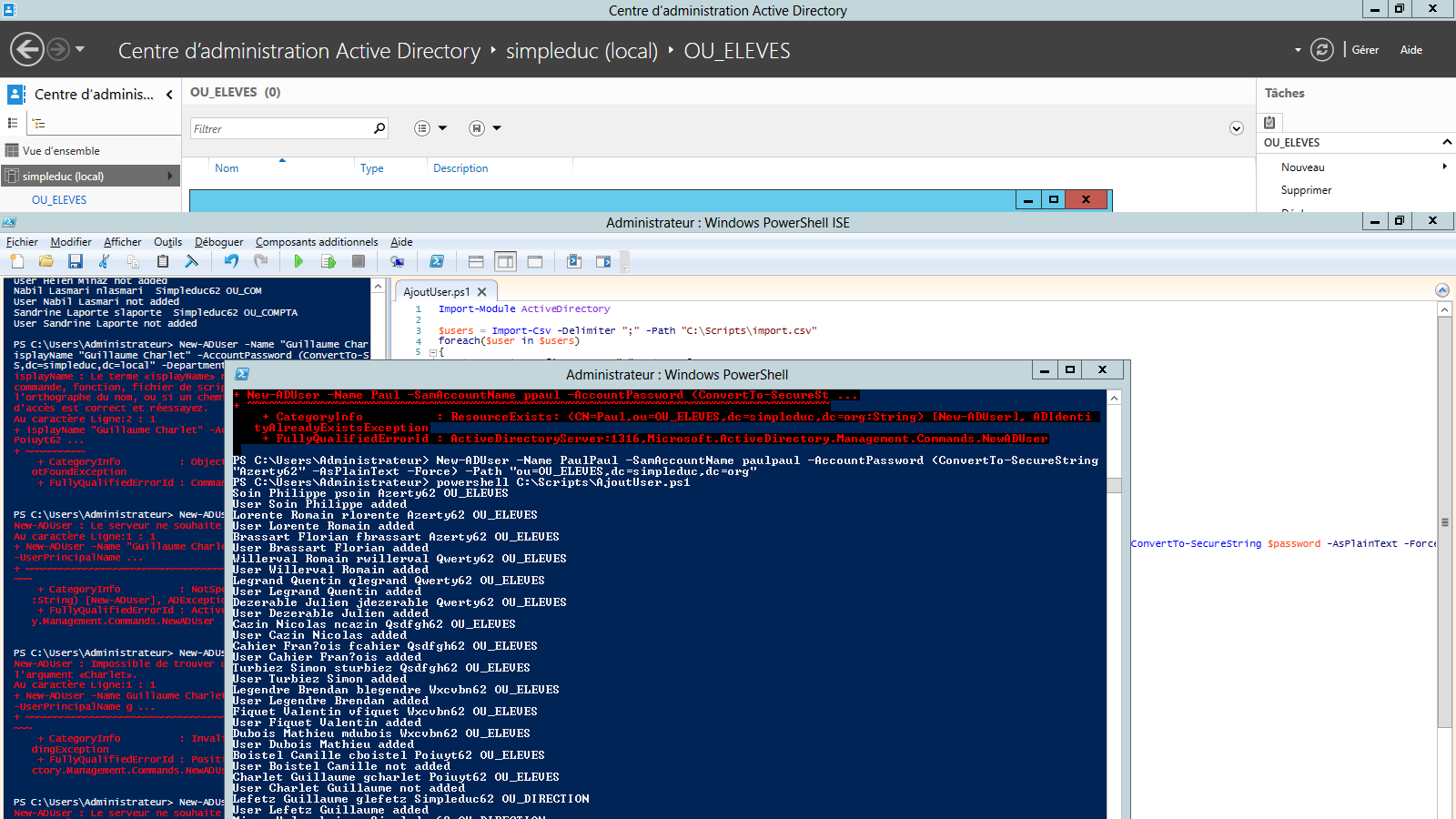
### Création des utilisateurs et OU par script

Création des OU OU\_ELEVES, OU\_COM, OU\_DIRECTION et OU\_COMPTA avec l’interface graphique :



Ensuite, on va créer un script pour pouvoir ajouter des utilisateurs saisis dans un fichier .csv.

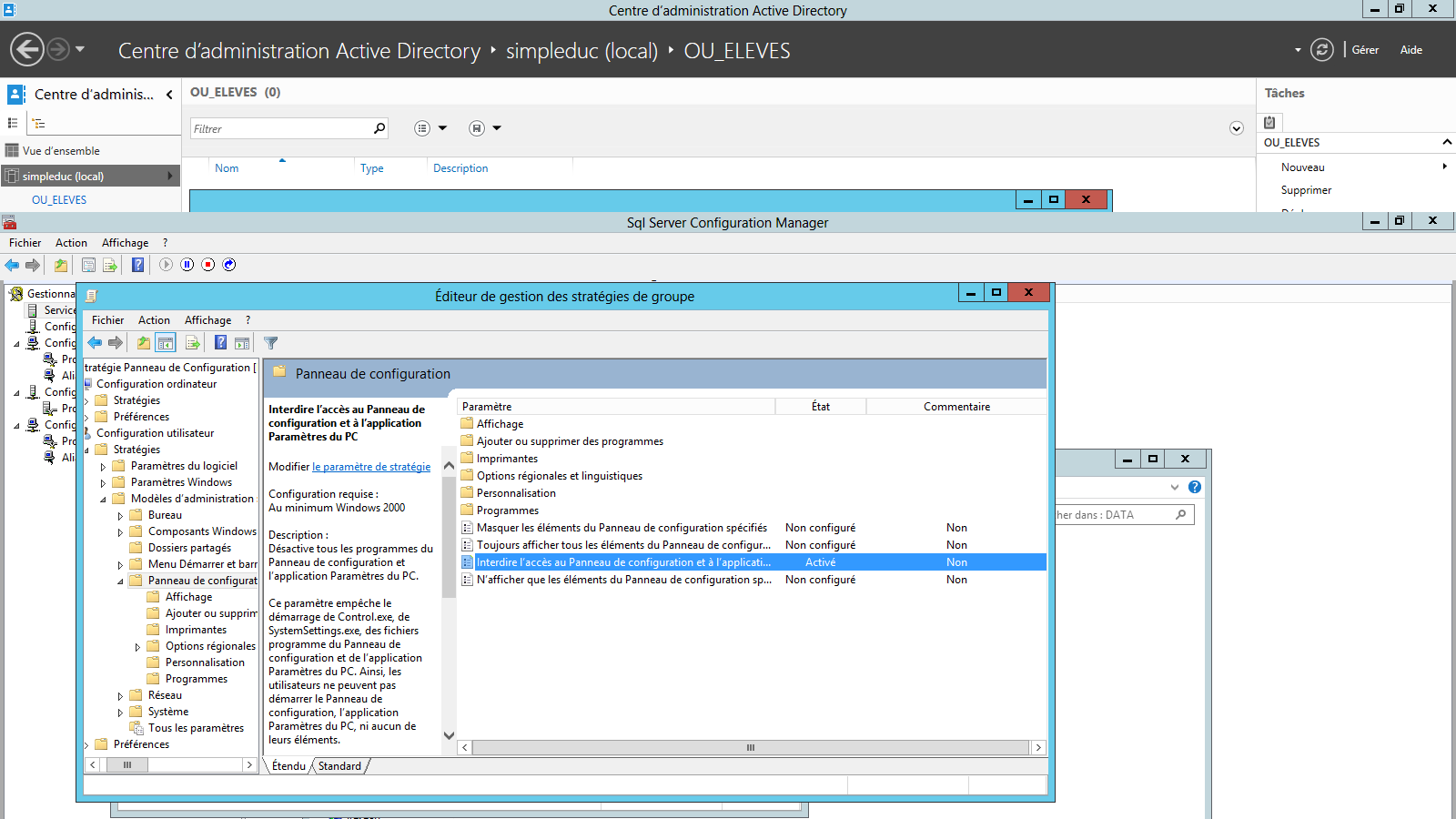
On lance le script dans un powershell, on voit que les utilisateurs sont bien ajouté, il est quand même nécessaire de vérifier également dans l’active directory.

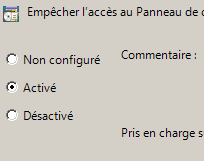


### Mise en place des GPO

#### Interdire l’accès au panneau de configuration pour les utilisateurs (sauf l’administrateur et l’OU INFO)

On crée une nouvelle GPO qu’on appellera Panneau de configuration. On le modifie et on active « Interdire l’accès au panneau de configuration »





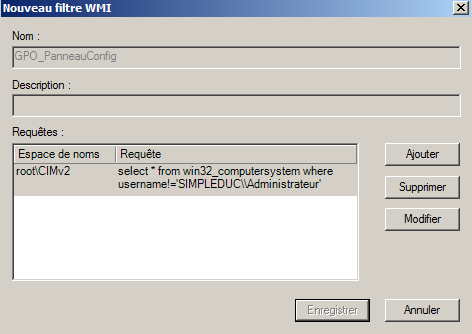
On accepte

Ensuite, on faire faire en sorte que l’administrateur puisse quand même y accéder.

On récupère le nom de l’administrateur dans le shell.

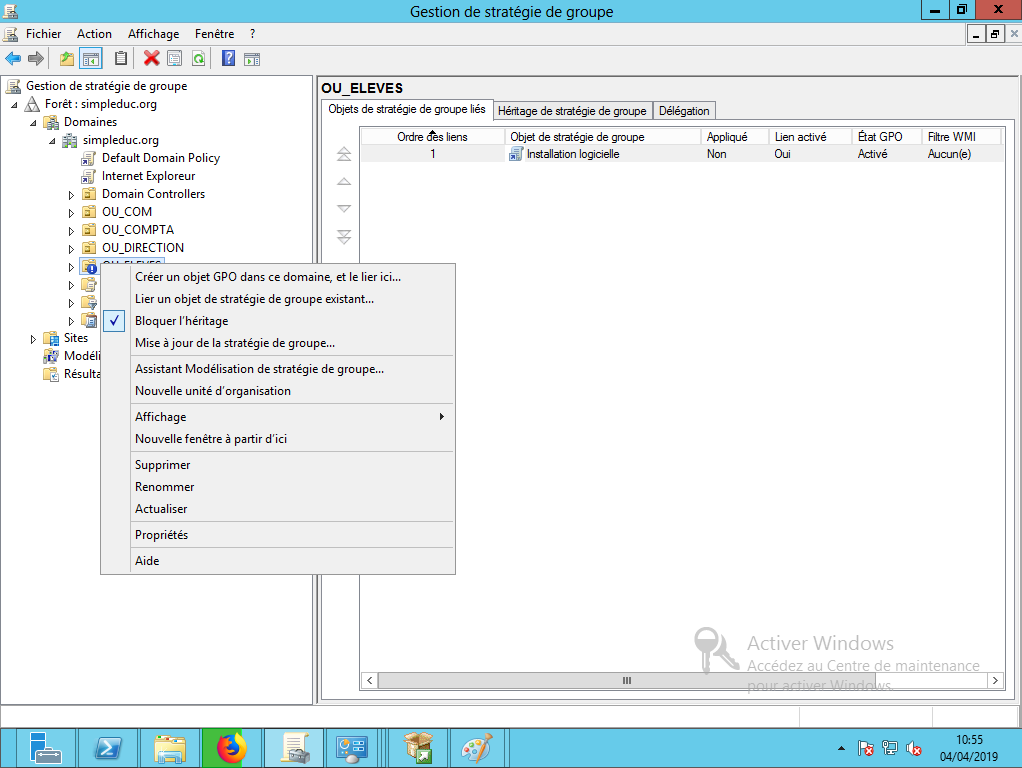


On crée un filtre WMI avec une requête : si l’utilisateur n’est pas l’admin, on appliquera la GPO.



On ajoute le filtre WMI que l’on vient de créer à la GPO « panneau de configuration » pour l’appliquer.

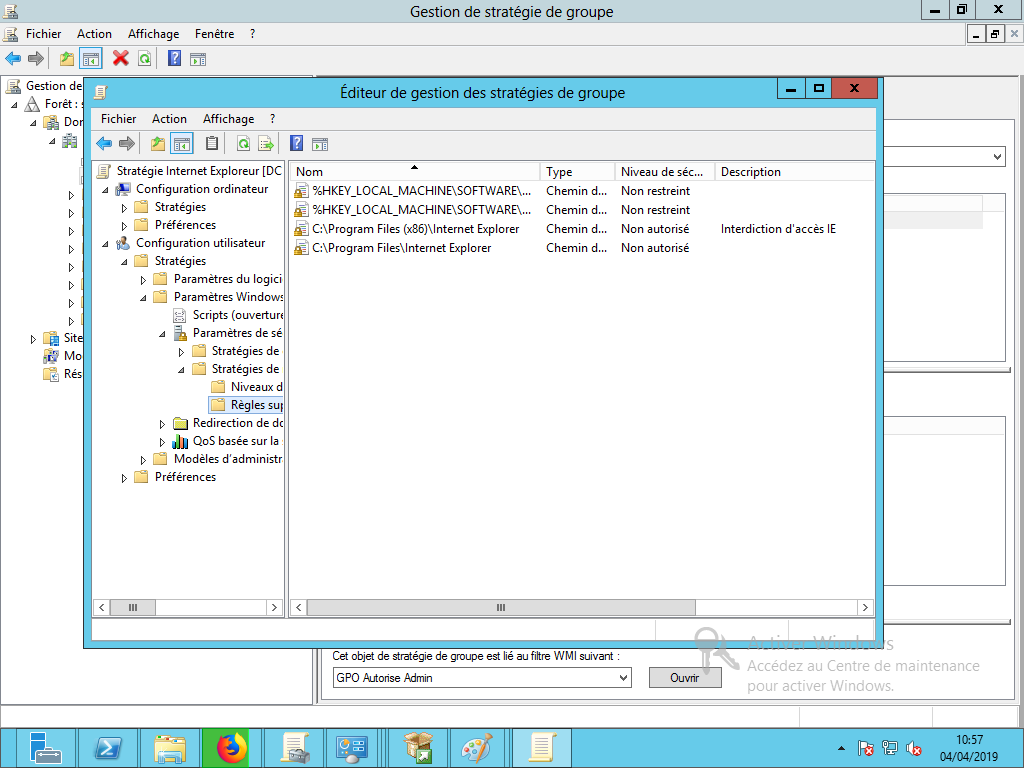
On bloque ensuite l’héritage des GPO pour l’OU INFO afin qu’elle ne soit pas affectée par la GPO panneau de configuration



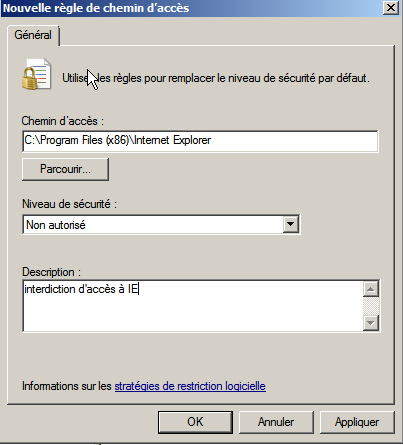
#### 

#### Interdiction pour tout le monde (sauf l’administrateur) d’utiliser Internet Explorer 32 et 64 bits.

On crée une règle qui bloque le chemin d’accès à internet explorer pour le domaine.



On fera de même dans l’OU INFO puisque l’héritage est désactivé.

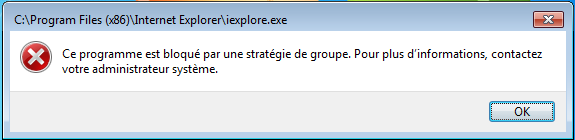


Et on ajoute le filtre WMI créé précédemment pour que l’admin puisse toujours l’utiliser.



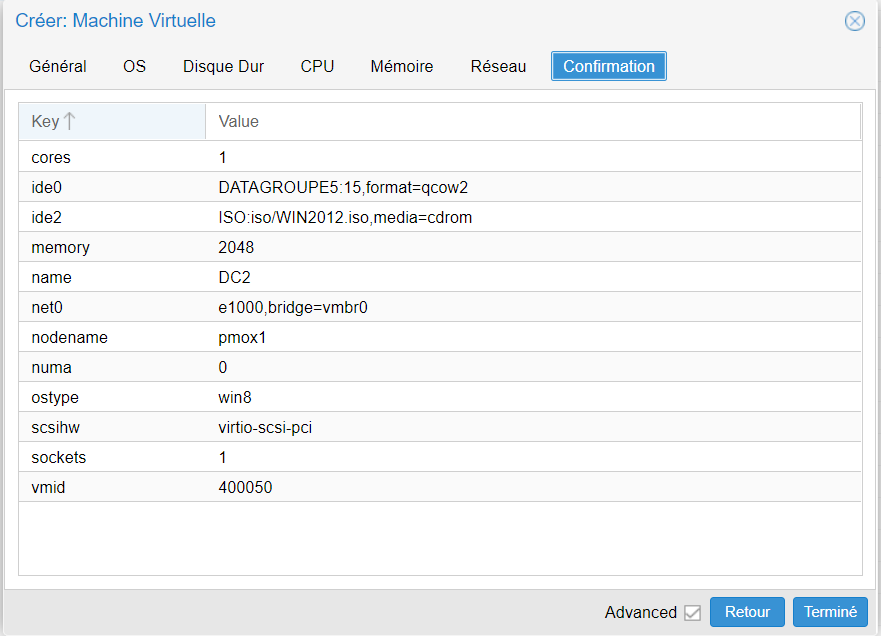
Penser à faire pour IE 64 bit et 32 bit.

Un message d’erreur s’affiche maintenant quand on essaie de lancer Internet Explorer depuis un autre compte que celui de l’administrateur

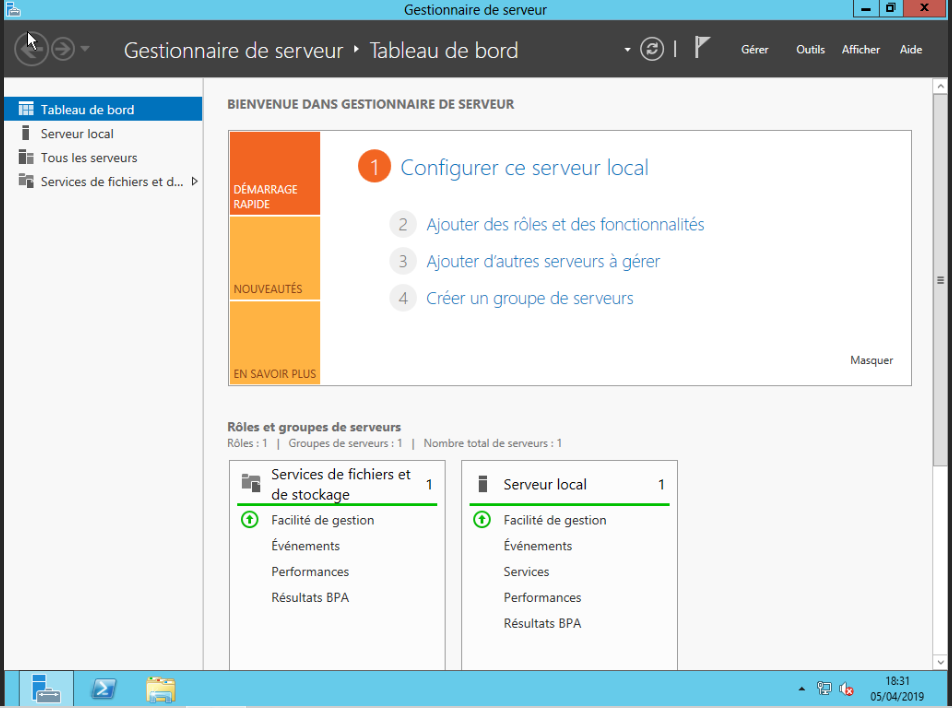


## Contrôleur de domaine supplémentaire

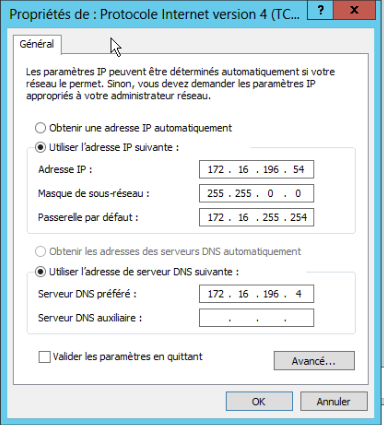
On crée une nouvelle VM sur Proxmox qui sera également un serveur Windows 2012.



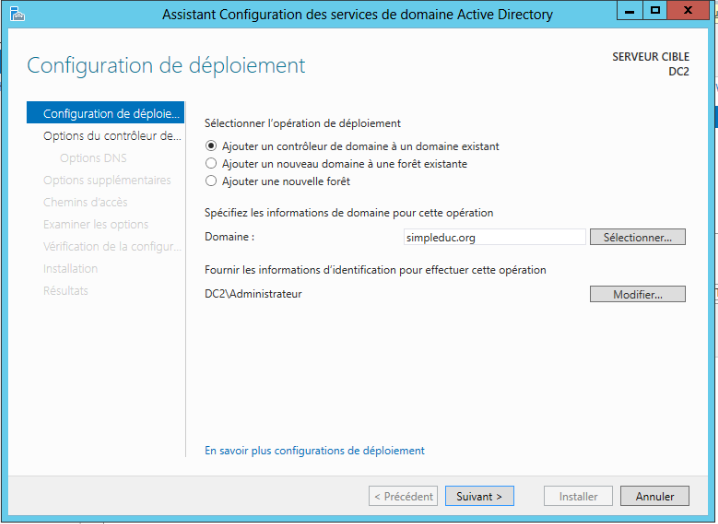
On aura également besoin de télécharger des pilotes virtuo-win pour pouvoir installer la machine, on rajoutera donc un CD/DVD avec l’ISO correspondant. Une fois l’installation terminée, on va pouvoir mettre en place le deuxième controleur.



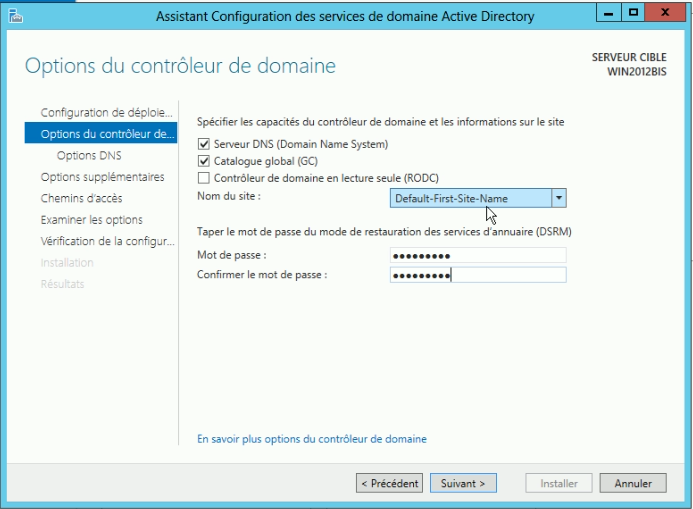
On lui met une IP statique ainsi que le masque, la passerelle et le DNS. On changera aussi le nom de l’ordinateur pour DC2



On installera le service AD sur le serveur, puis on le configurera pour être un nouveau contrôleur de domaine sur un domaine existant :

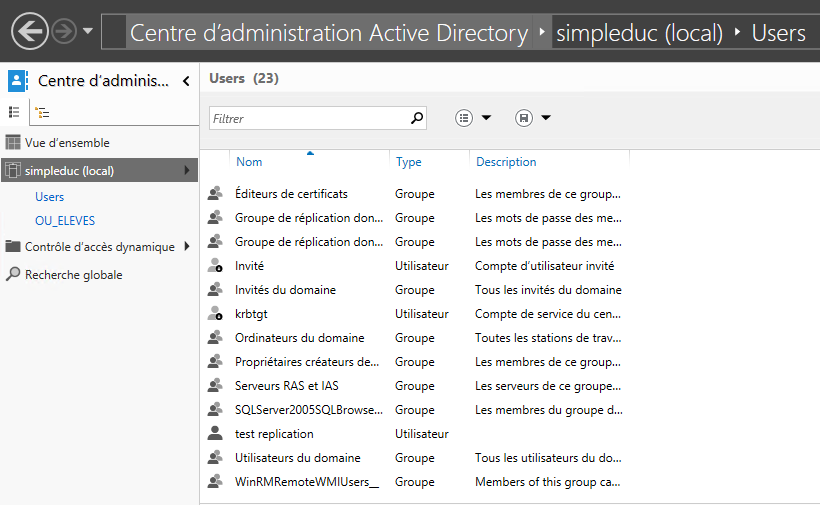


On ajoutera un mot de passe pour la restauration :



Dans l’onglet **Options supplémentaires**, on choisira DC1.simpleduc.org pour la réplication. On ne changera plus de paramètres et l’on installera le contrôleur de domaine.

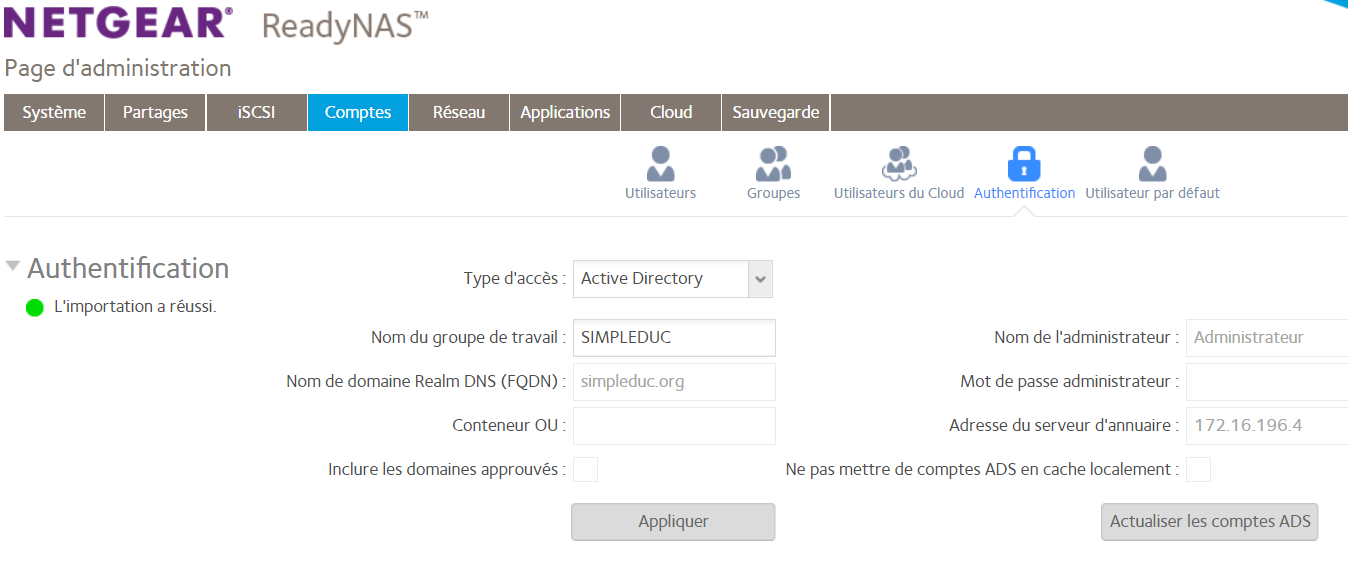
Maintenant que DC2 est installé et configuré en tant que contrôleur de domaine supplémentaire, on peut tester la réplication. Pour cela, on créera un utilisateur « test réplication » à partir de DC2, puis on vérifiera qu’il existe bien pour le DC1.



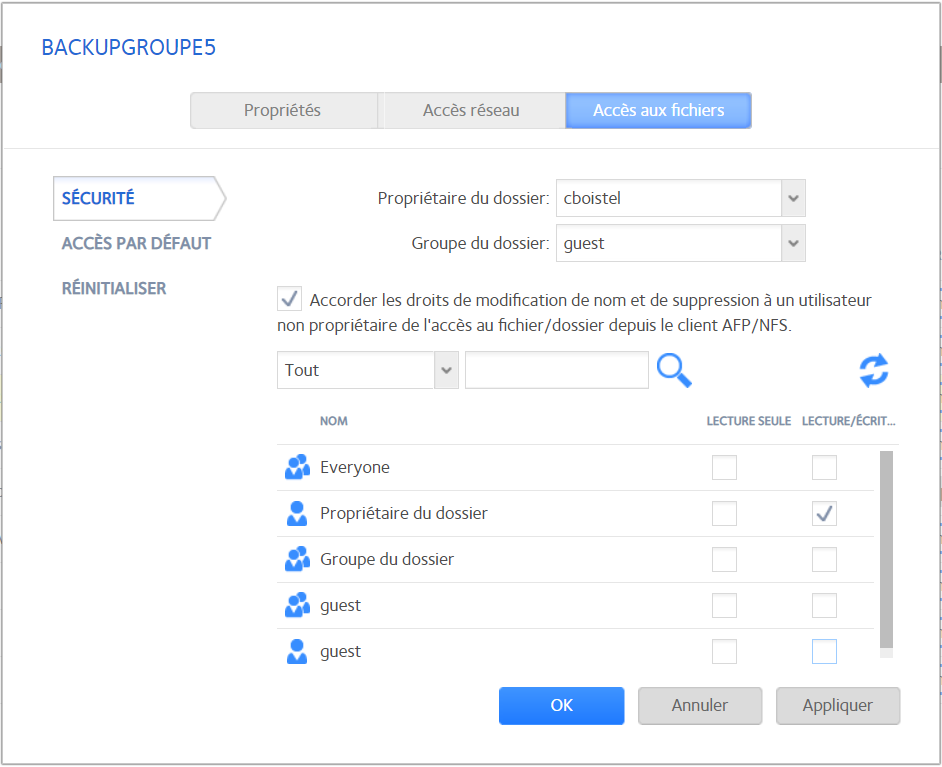
On peut voir sur DC1 que l’utilisateur à bien été créé.

## NAS

On veut pouvoir faire des snapshots des VM et qu’ils soient sauvegarder sur le NAS. Pour cela, on va d’abord vouloir mettre en place une identification LDAP sur celui-ci ; pour pouvoir ensuite gérer les partages de fichiers en fonction des utilisateurs.



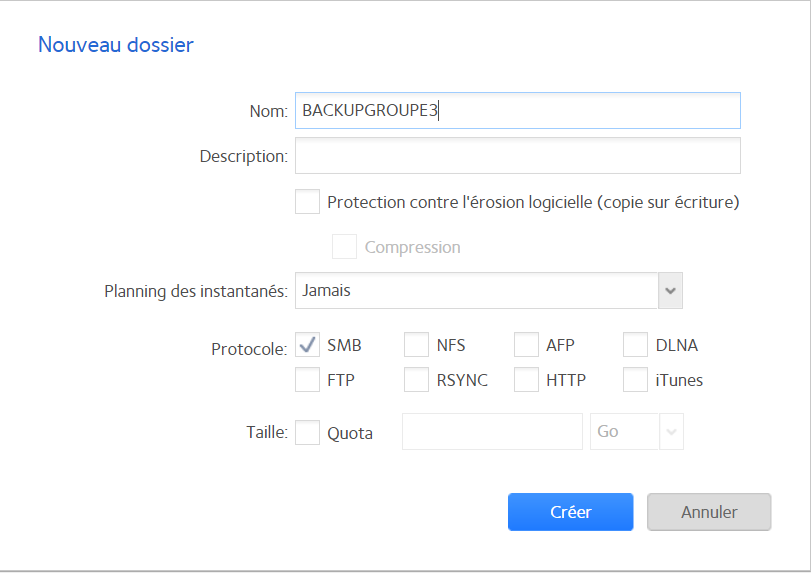
Une fois connecté, on actualise la page des utilisateurs pour voir si l’import à bien fonctionné. On va ensuite aller dans l’onglet **Partages** pour aller dans les paramètres du dossier correspondant. Dans l’accès réseau, on désactivera le NFS et on activera SMB. Dans l’accès au fichier, on modifiera les paramètres de la manière suivante afin d’être la seule à avoir accès à mes snapshots :



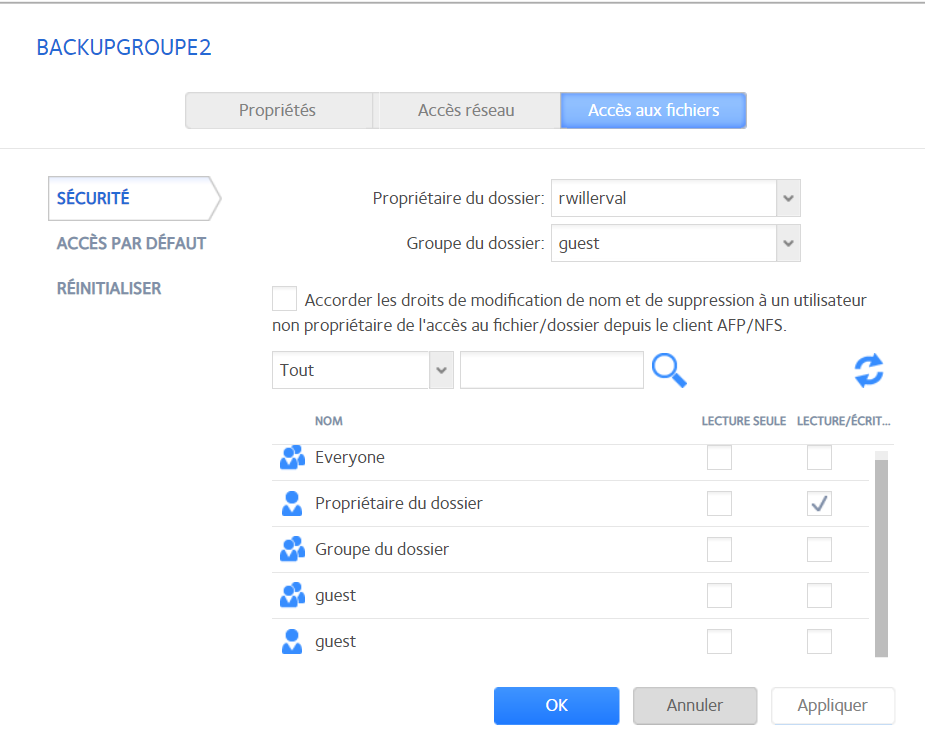
Création des storage Backup pour tous les fgroupes

Créer le partage correspondant sur le NAS

Partage > Nouveau dossier

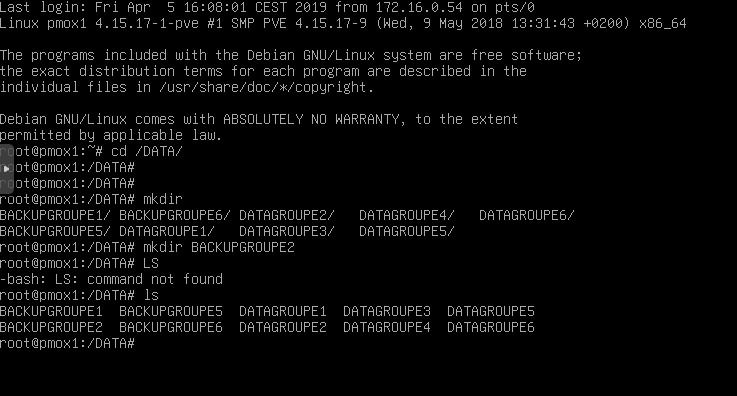


On mettra les mêmes paramètres que pour BACKUPGROUPE5



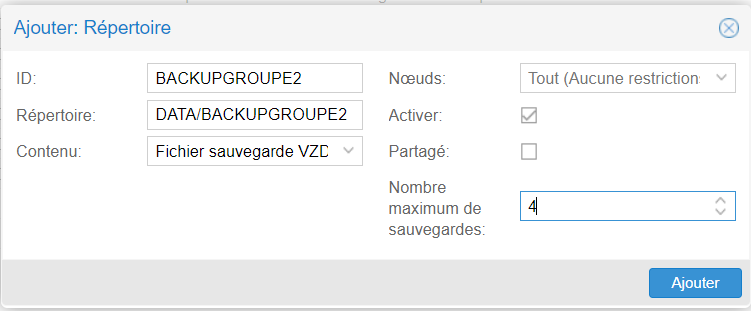
On se connecte en temps qu’admin au Proxmox et créer un directory sur le proxmox.

On se connectera à la console et on créera les répertoires des groupes dans le répertoire /DATA.

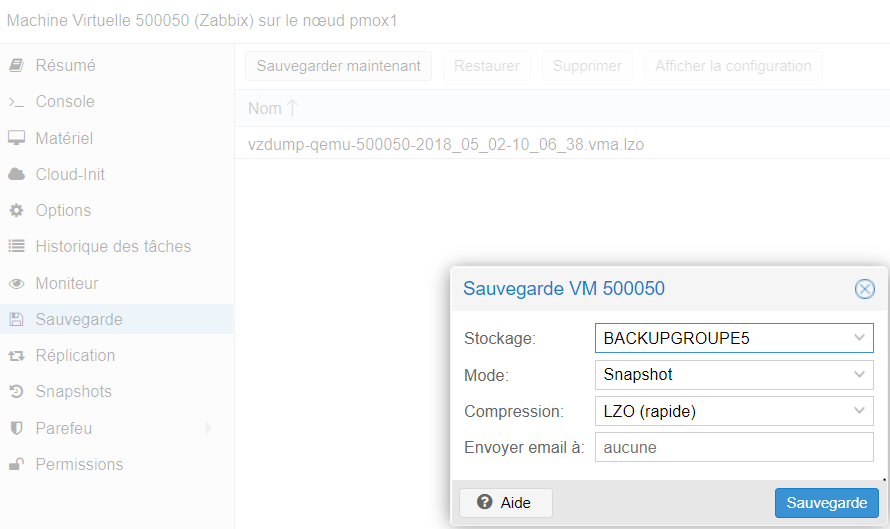




Sur Proxmox, on se connectera en tant qu’admin pour créer la zone de stockage BACKUPGROUPE2.

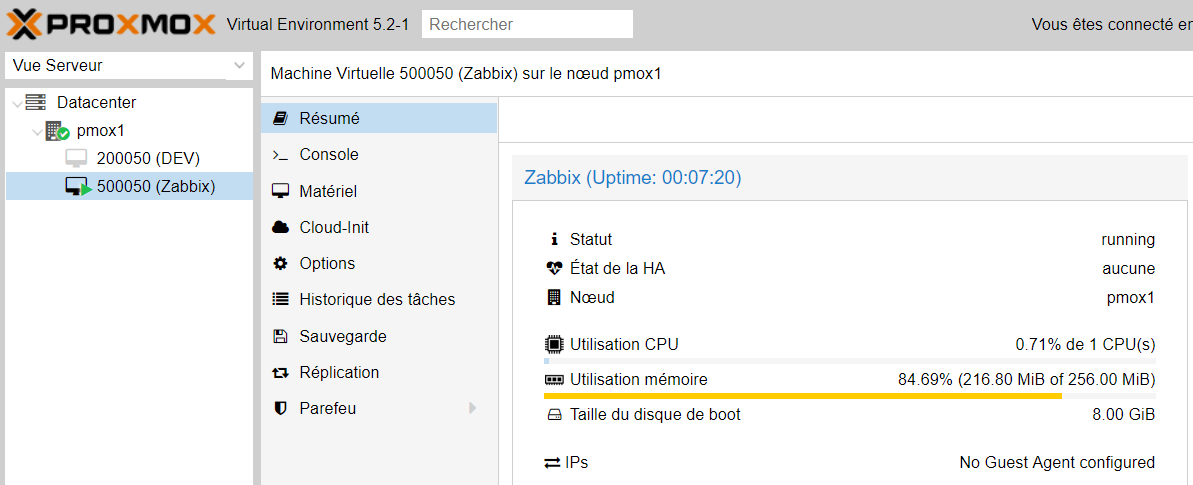


On peut maintenant prendre des snapshots.



## Zabbix

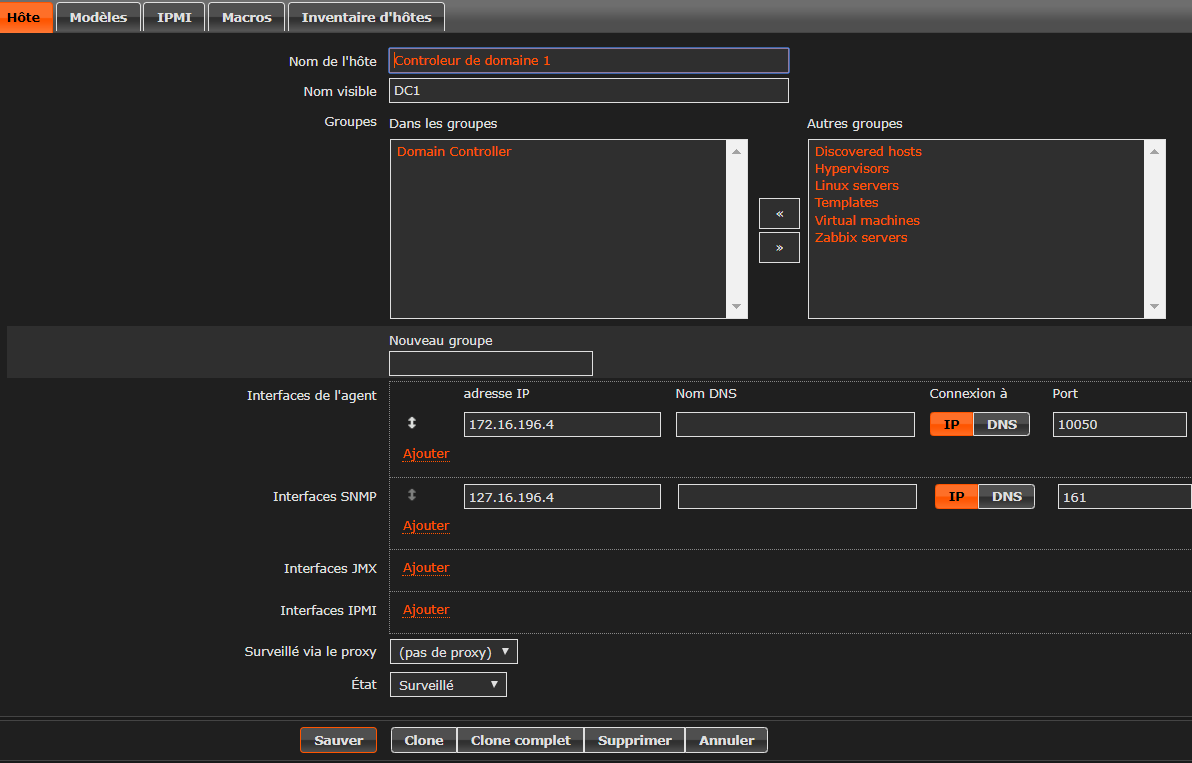
On peut accéder au serveur Zabbix depuis le serveur Proxmox. Celui-ci étant déjà mis en place sur le réseau, aucune installation n’est nécessaire, néanmoins, il va falloir reconfigurer certains paramètres, notamment le nom de la machine et le mot de passe root.



On passera sur l’onglet **Console** pour les prochaines modifications. On commence par prendre un snapshot avant de commencer, dans l’onglet **Sauvegarde > Sauvegarder maintenant**.

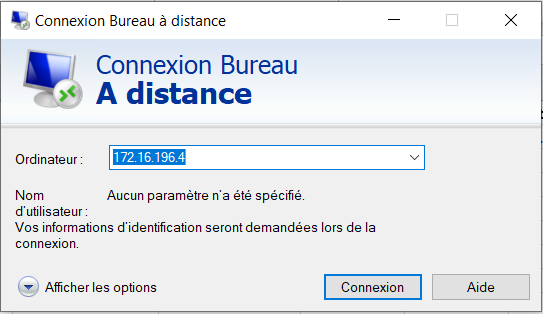
On lance la machine et on regarde quelle IP elle possède avant de vérifier dans /etc/network/interfaces s’il s’agit bien d’une IP statique.

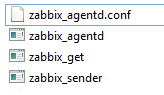
On voudra ensuite se connecter à l’interface web grâce à 172.16.196.55/zabbix. Une fois connecté à l’interface, on va pouvoir commencer à superviser le réseau, pour cela, on ajoutera un hôte pour le contrôleur de domaine :



### Contrôleur de domaine 1

Il va maintenant falloir installer le protocole SNMP sur le serveur DC1 pour pouvoir le superviser. On se connectera au contrôleur avec la connexion à distance Windows :



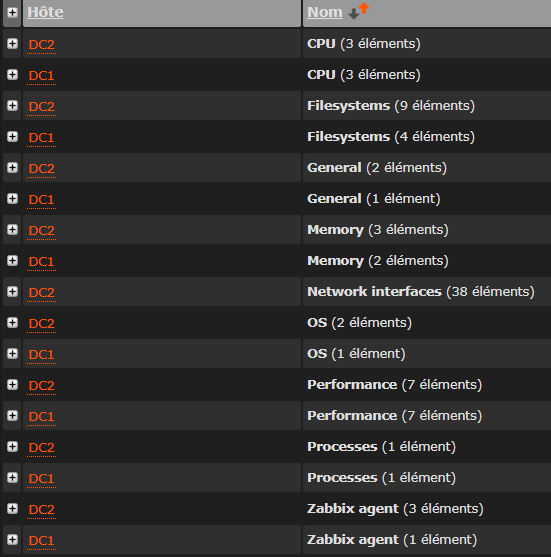
On veut superviser notre contrôleur de domaine via l’agent Zabbix. On téléchargera les fichiers de configuration de celui-ci et on conservera uniquement les fichiers suivants que l’on placera dans un dossier **C:\Zabbix**.

On modifiera ensuite **zabbix\_agentd.conf**, pour écrire uniquement les options Server et ServerActive en précisant l’IP de notre serveur Zabbix.

Une fois modifié, on ouvrira PowerShell et on lancera l’installation de l’agent.



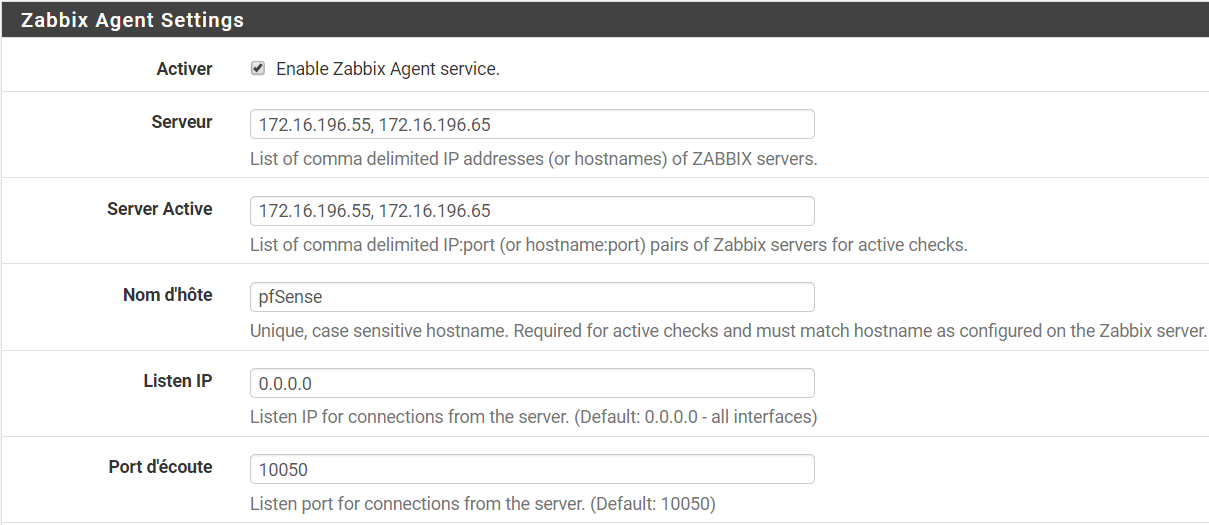
Il ne nous reste qu’à activer le service Zabbix Agent pour commencer à récupérer des informations. On fera la même manipulation sur le contrôleur de domaine supplémentaire :



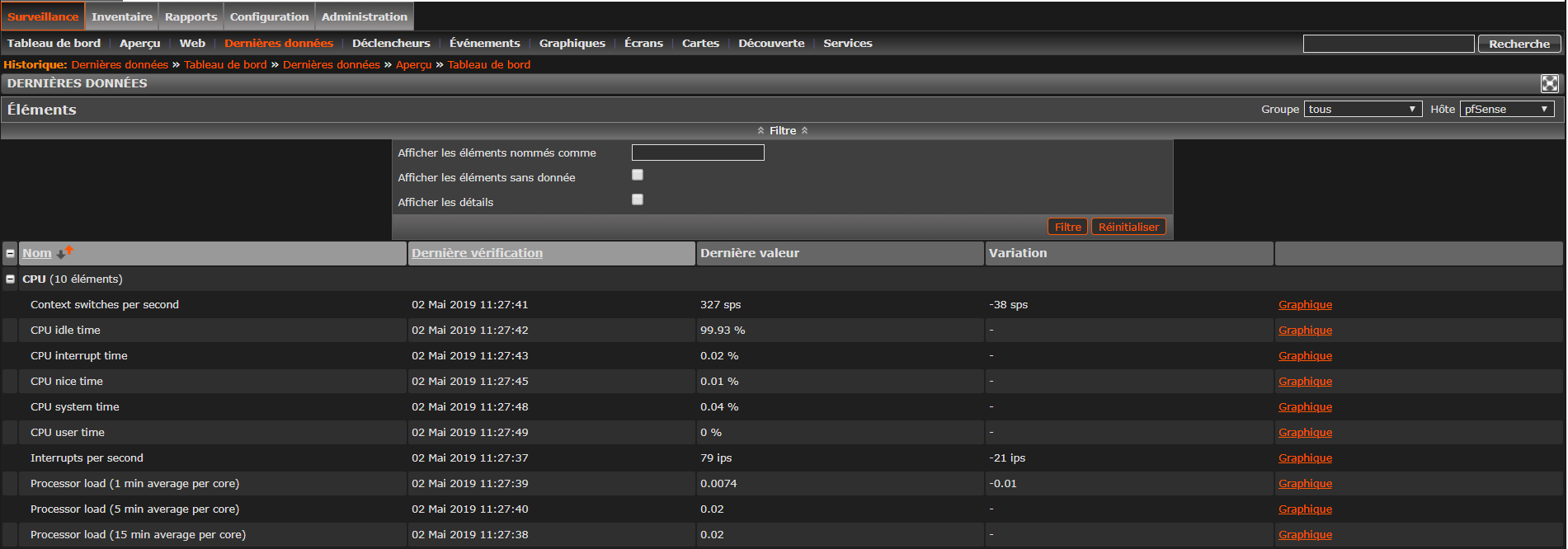
### PfSense

On veut ensuite superviser le serveur PFSense, on créera également l’hôte qui lui sera associé sur Zabbix. Ensuite on va télécharger le paquet zabbix-agent2.2 sur PFSense. On le configurera ensuite dans **Services > Agent Zabbix 2.2**.

On mettra les IP des serveurs Zabbix de Guillaume et moi, afin que nous puissions super



On peut voir que les informations collectées sur le serveur PfSense remontent :



### GLPI

On installe sur le serveur l’agent Zabbix.

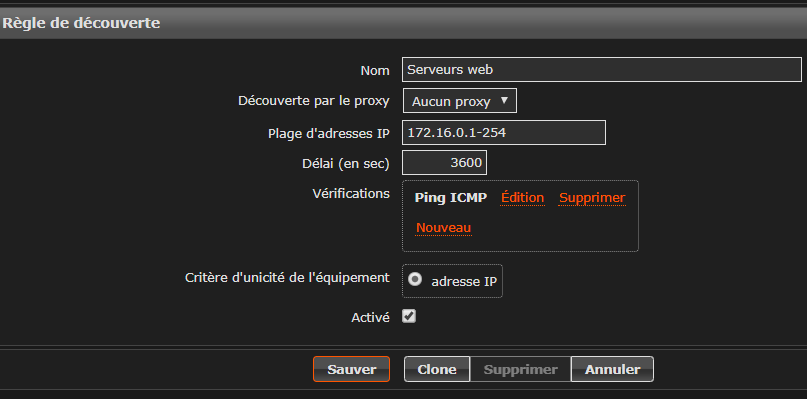


On devra ensuite modifier le fichier de configurations **/etc/zabbix/zabbix\_agentd.conf**. On donne l’IP de notre serveur Zabbix pour l’option **servers**. On doit ensuite redémarrer le service.



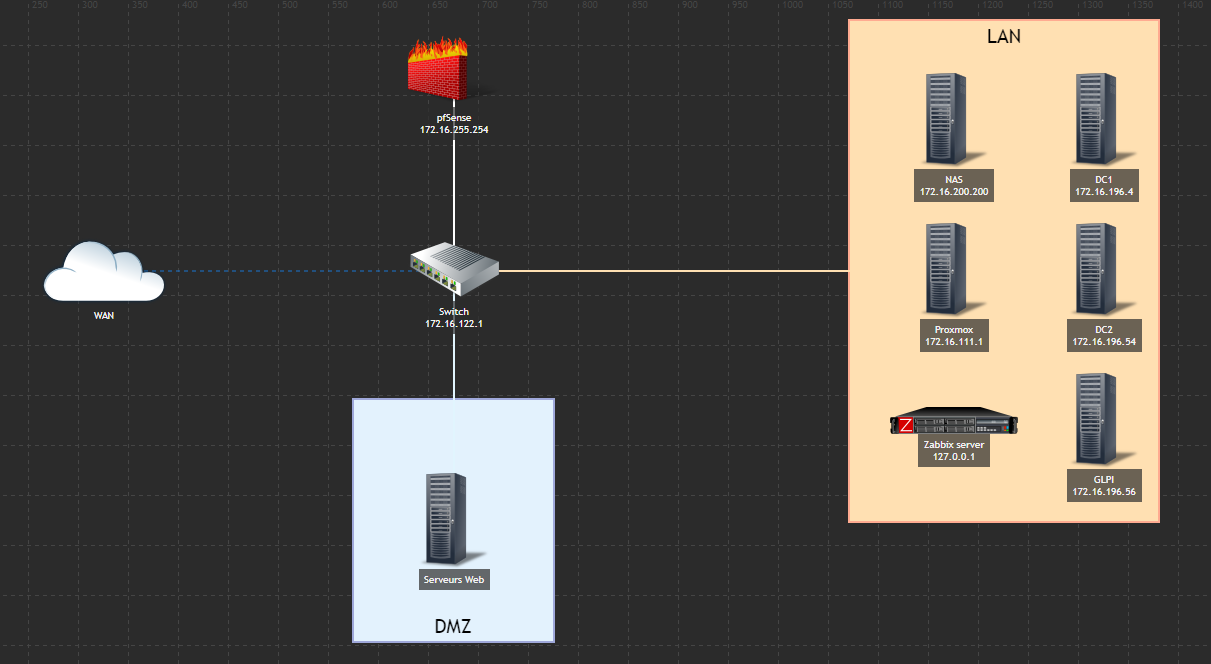
### Serveurs web

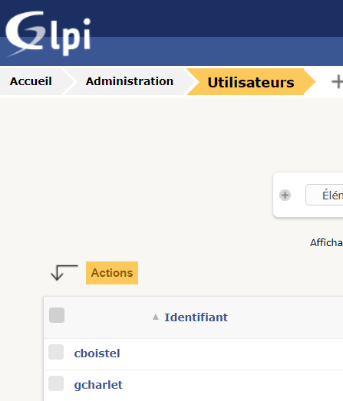
On voudra récupérer les informations sur les différents serveurs web présents sur la DMZ. Pour cela, on créera une règle de découverte pour récupérer les machines sur le réseau 172.16.0.0/24 via un ping.



### MAP

Création d’une map pour représenter les différents éléments de notre infrastructure :





## GLPI

Serveur GLPI déjà installé, on se connecte donc à l’interface web. On créera d’abord les utilisateurs cboistel et gcharlet, qui seront des administrateurs. On créera un groupe Admin Réseau dans lequel on placera les utilisateurs créé aux préalables.

On ajoutera ensuite les différents serveurs dans la liste des équipements. On configurera ces serveurs de façon à les placer dans la zone « baie BTS » et supervisée par le groupe Admin Réseau.

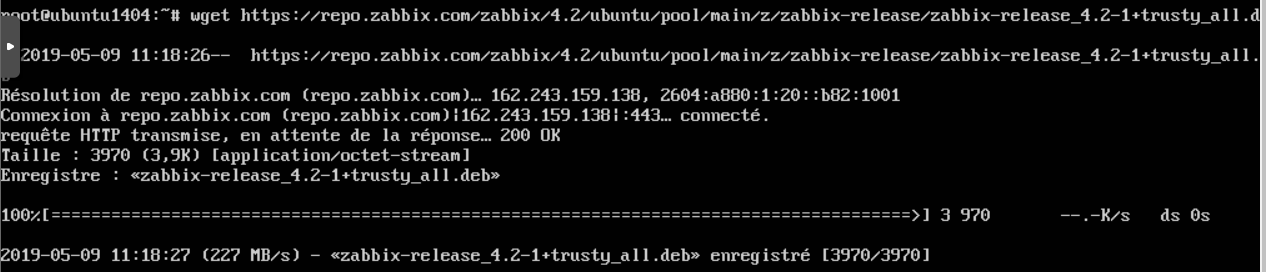


Problème : pas de retour du switch via le SNMP.

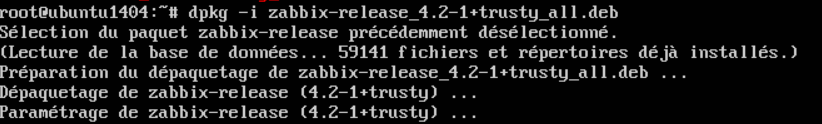
* Tentative de mise à jour de la version 2.2 à la version actuelle (4.2).

On doit d’abord prendre un snapshot de notre serveur zabbix, pour pouvoir restaurer l’ancienne version en cas de problème.

On stoppe d’abord le service zabbix-server. On supprime le fichier /etc/apt/sources.list.d/zabbix.list. On peut ensuite télécharger les fichiers avec wget.



Il faut ensuite l’installer.



On mettra ensuite les paquets à jour



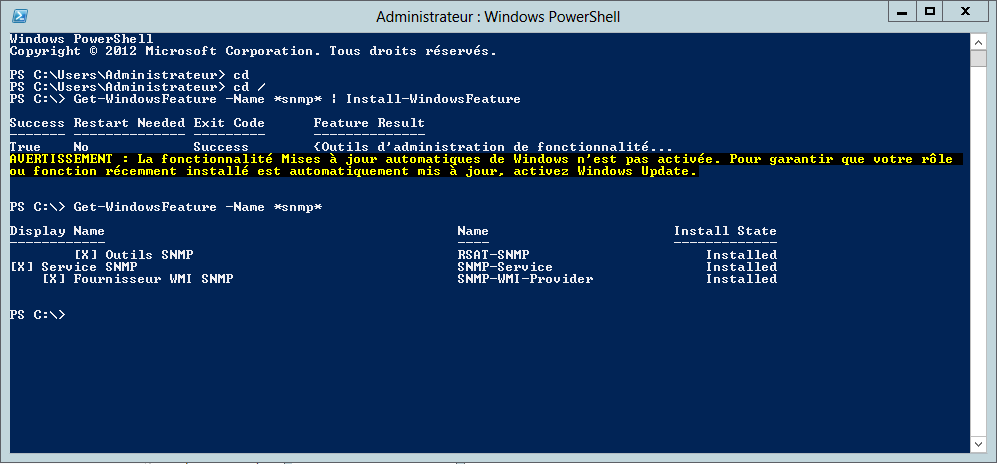
On valide pour toutes les options et on redémarre Zabbix-server.



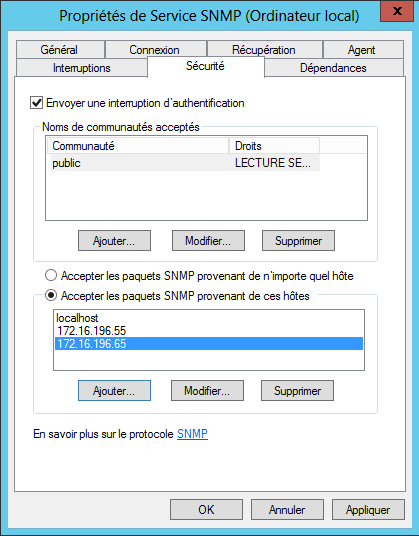
Problème avec la base de données, plus rapide de recommencer à 0…

SNMP enlevé

On va installer SNMP sur DC1 via PowerShell.



On configurera ensuite celui-ci via la console des services. On ira dans les propriétés du service SNMP et l’on ajoutera sa communauté dans l’onglet **Sécurité**, ainsi que les adresses de nos deux serveurs Zabbix.



On peut voir que différentes informations remontent :