

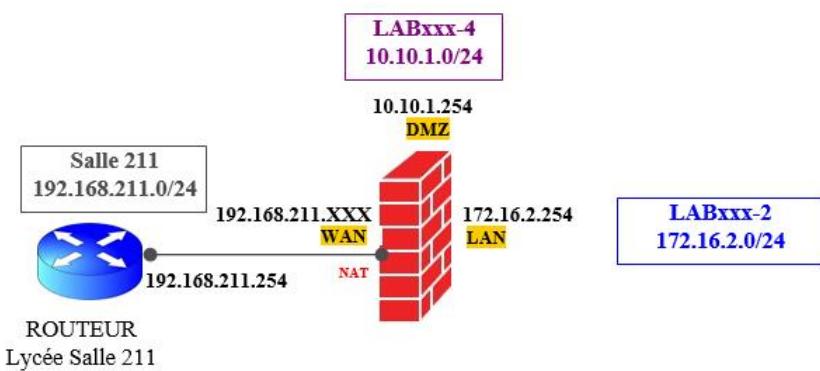
Documentation projet MDL



Table des matières

Schéma du réseau.....	3
Mission 1 : Installation du routeur-pare-feu PfSense	3
Mission 2 C: création des utilisateurs avec leur dossier personnel de base ; configuration d'autorisations spécifiques à certains dossiers	6
Création des groupes utilisateurs « Ligue Football » et « Ligue Basket ».....	9
Inventaire du matériel avec GLPI/fusionInventory	13
Installation du SGBD mySQL	16
Installation et exécution de l'agent FusionInventory sous Windows	23
Importation des utilisateurs avec l'annuaire Idap.....	24
Configuration du serveur OpenVPN sur le routeur-parefeu PfSense	29
Mission 6 : Cluster PfSense :	46
Bureau à distance	57

Schéma du réseau



Mission 1 : Installation du routeur-pare-feu PfSense

Le but de cette mission est d'installer et configurer le routeur PfSense.

Celui-ci aura trois interfaces : WAN, LAN, et DMZ.

L'interface DMZ ne sera pas utilisée ici, mais on la configurera en vue d'une éventuelle installation d'une DMZ ultérieurement.

- On commence par créer une machine PfSense avec le modèle suivant :



- Vérifier que la machine virtuelle PfSense dispose de 3 cartes réseau (si ce n'est pas le cas, mettre hors-tension la machine et ajouter les cartes nécessaires). On va maintenant ajouter 3 cartes réseaux supplémentaires :

WAN : vmx0
LAN : vmx1
OPT1 : vmx2
OPT2 : vmx3

- Pour cela il faut se rendre dans « modifier les paramètres », « matériel virtuel » puis ajouter les 4 cartes réseaux (fonctions « ajouter un périphérique ») :

> Adaptateur réseau 1	LAB-SISR-02-2	<input checked="" type="checkbox"/> Connecté
> Adaptateur réseau 2	LAB-SISR-02-3	<input checked="" type="checkbox"/> Connecté
> Adaptateur réseau 3	LAB-SISR-02-4	<input checked="" type="checkbox"/> Connecté
> Adaptateur réseau 4	SALLE - 211	<input checked="" type="checkbox"/> Connecté

- On peut maintenant assigner les interfaces du Pfsense (fonction 1 : *Assign Interfaces* sur l'écran d'interface texte du Pfsense) :

WAN :

```
Enter the WAN interface name or 'a' for auto-detection
(vmx0 vmx1 vmx2 vmx3 vmx4 or a): vmx0
```

LAN :

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vmx1 vmx2 vmx3 vmx4 a or nothing if finished): vmx1
```

OPT1 :

```
Optional interface 1 description found: OPT1
Enter the Optional 1 interface name or 'a' for auto-detection
(vmx2 vmx3 vmx4 a or nothing if finished): vmx2
```

OPT2 :

```
Optional interface 2 description found: OPT2
Enter the Optional 2 interface name or 'a' for auto-detection
(vmx3 vmx4 a or nothing if finished): vmx3
```

- Attribuer des adresses IP aux interfaces du Pfsense (fonction 2 : *Set Interface(s) IP address* sur l'écran d'interface texte du Pfsense) (ne pas oublier de spécifier la passerelle nécessaire pour chaque interface).
Attention : ne pas configurer de DHCP (sur aucune interface)

WAN :

```
1 - WAN (vmx0 - static)
2 - LAN (vmx1 - static)
3 - OPT1 (vmx2 - static)
4 - OPT2 (vmx3)
```

```
Enter the number of the interface you wish to configure: 1
```

```
Configure IPv4 address WAN interface via DHCP? (y/n) n
```

```
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.211.220
```

LAN :

```
Available interfaces:
```

```
1 - WAN (vmx0 - static)
2 - LAN (vmx1 - static)
3 - OPT1 (vmx2 - static)
4 - OPT2 (vmx3)
```

```
Enter the number of the interface you wish to configure: 2
```

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.2.254
```

OPT1 :

```
Enter an option: 2
```

```
Available interfaces:
```

```
1 - WAN (vmx0 - static)
2 - LAN (vmx1 - static)
3 - OPT1 (vmx2 - static)
4 - OPT2 (vmx3)
```

```
Enter the number of the interface you wish to configure: 3
```

```
Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 10.10.1.254
```

NB : OPT2 sera configuré plus tard

- On va maintenant attribuer l'étiquette réseau adéquate à chaque interface réseau selon l'adresse MAC de la carte, on peut utiliser la fonction 8 « shell » de Pfsense :
- Par exemple pour vmx0 qui correspond à l'interface WAN on peut taper la commande dans le shell : « ifconfig vmx0 » et puis voir l'adresse MAC :

```
[2.5.1-RELEASE][root@pfSense.home.arpa]# ifconfig vmx0
vmx0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=e000bb<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCS
        UM,RXCSUM_IPV6,TXCSUM_IPV6>
        ether 00:50:56:90:f1:08
        inet6 fe80::250:56ff:fe90:f108%vmx0 prefixlen 64 scopeid 0x1
        inet 192.168.211.220 netmask 0xffffffff broadcast 192.168.211.255
        media: Ethernet autoselect
        status: active
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
[2.5.1-RELEASE][root@pfSense.home.arpa]#
```

- On peut maintenant vérifier les correspondances entre les adresses MAC dans les paramètres des adaptateurs réseaux de PfSense, l'adaptateur réseau 4 correspond à l'adresse MAC de l'interface WAN, on peut donc lui mettre SALLE-211 :

Adaptateur réseau 4		SALLE - 211	<input checked="" type="checkbox"/> Connecté
Statut	<input checked="" type="checkbox"/> Connecter lors de la mise sous tension		
Type d'adaptateur	VMXNET 3		
DirectPath I/O	<input checked="" type="checkbox"/> Activer		
Adresse MAC	00:50:56:90:f1:08	Automatique	

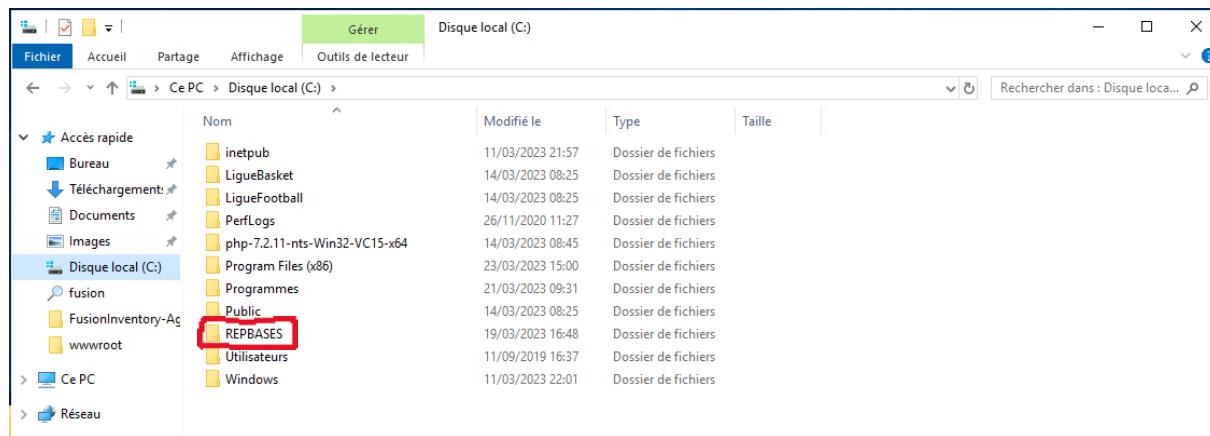
- On peut maintenant reproduire l'opération pour l'interfaces LAN et OPT1 :

```
[2.5.1-RELEASE][root@pfSense.home.arpa]# ifconfig vmx1
vmx1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=e000bb<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCS
        UM,RXCSUM_IPV6,TXCSUM_IPV6>
        ether 00:50:56:90:19:c1
        inet6 fe80::250:56ff:fe90:19c1%vmx1 prefixlen 64 scopeid 0x2
        inet 172.16.2.254 netmask 0xffffffff broadcast 172.16.2.255
        media: Ethernet autoselect
        status: active
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
[2.5.1-RELEASE][root@pfSense.home.arpa]#
```

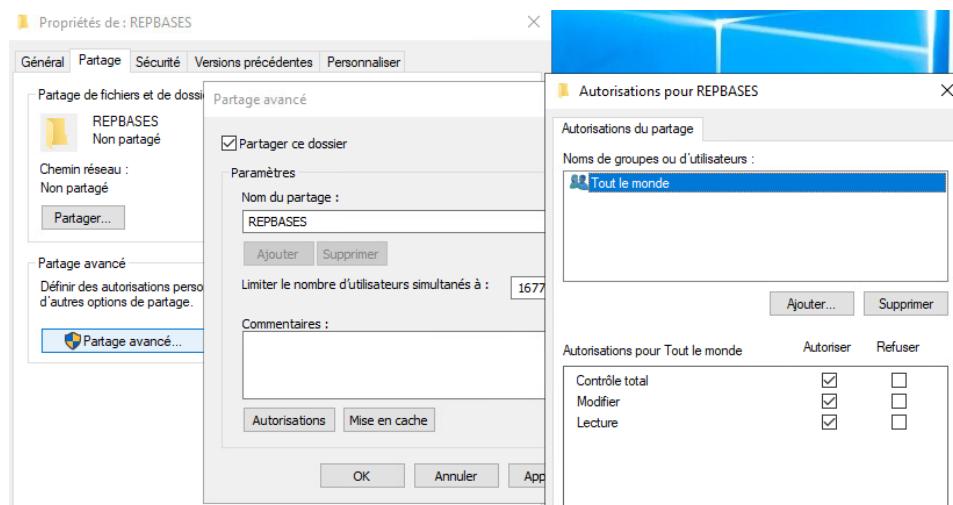
Adaptateur réseau 1		LAB-SISR-02-2	<input checked="" type="checkbox"/> Connecté
Statut	<input checked="" type="checkbox"/> Connecter lors de la mise sous tension		
Type d'adaptateur	VMXNET 3		
DirectPath I/O	<input checked="" type="checkbox"/> Activer		
Adresse MAC	00:50:56:90:19:c1	Automatique	

Mission 2 C: création des utilisateurs avec leur dossier personnel de base ; configuration d'autorisations spécifiques à certains dossiers

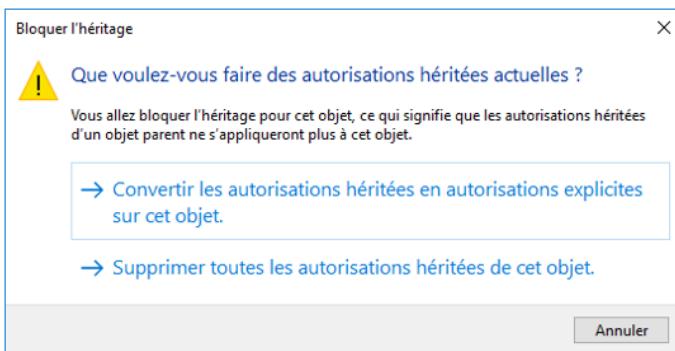
- Sur le serveur de domaine on va créer le dossier REPBASES à la racine et configurer ses autorisations de partage et ses autorisations de sécurité NTFS
- Le dossier REPBASES contiendra les dossiers personnels de base des tous les utilisateurs du domaine MDL.local



- Après avoir créé le dossier REPBASES sur le serveur de domaine on va tout d'abord le partager en allant dans « autorisation » et en mettant « contrôle total » à tout le monde.

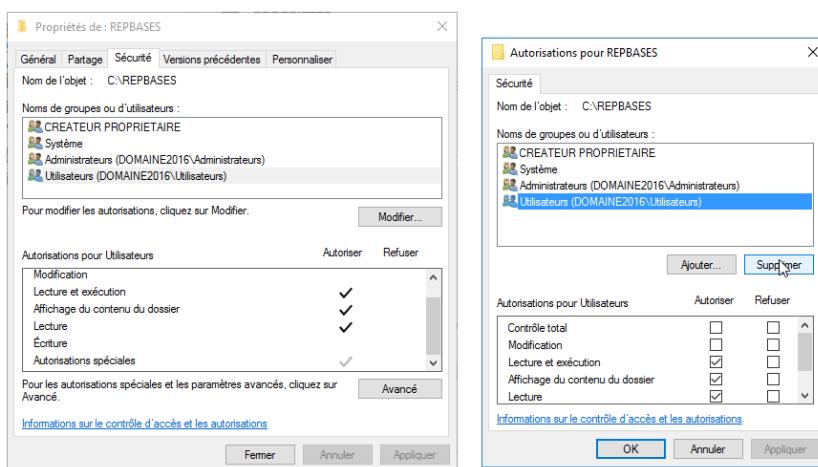


- On va maintenant désactiver l'héritage, pour ce faire on va aller dans « sécurité » puis dans « avancé » et ensuite on va cliquer sur le bouton « désactivé l'héritage » **Désactiver l'héritage** puis cliquer ensuite sur le lien « convertir les autorisations explicites sur cet objet ».



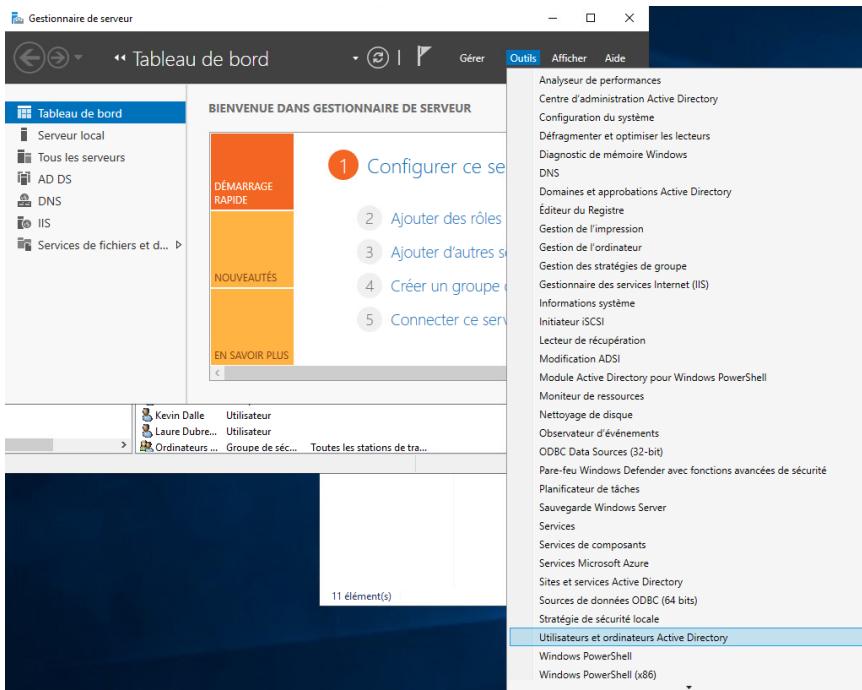
- On va ensuite supprimer toutes les autorisations accordées à « Utilisateurs » (du domaine) :

- Cliquer sur le bouton « Modifier »
- Sélectionner « Utilisateurs » (du domaine)
- Cliquer sur le bouton « supprimer »



- Le dossier REPBASES, Utilisateurs (du domaine) n'a plus aucun droits, cependant CREATEUR PROPRIETAIRE, Système et Administrateur conservent le contrôle total.
- Les dossiers personnels de base des utilisateurs, qui seront des sous-dossiers de REPBASES vont hériter automatiquement de ces autorisations du dossier parent REPBASES.

- On va maintenant créer les utilisateurs sur le serveur de domaine grâce à la fonctionnalité ADDS ajouté précédemment, pour cela on va se rendre dans le « Gestionnaire de serveur », cliquer ensuite sur « outil » et dans « Utilisateur et ordinateur active directory »



- On va ensuite se rendre dans le dossier « Users » et cliquer sur l’icône « créer un nouvel utilisateur dans le conteneur actuel »

Nom	Type	Description
Administrat...	Utilisateur	Compte d'utilisateur d'a...
Administrat...	Groupe de séc...	Les membres de ce grou...
Administrat...	Groupe de séc...	Les membres de ce grou...
Administrat...	Groupe de séc...	Administrateurs désigné...
Administrat...	Groupe de séc...	Administrateurs désigné...
Admins du ...	Groupe de séc...	Administrateurs désigné...
Clément Ogi...	Utilisateur	

- Dans la fenêtre qui s’ouvre on va pouvoir entrer les informations de l’utilisateur, voici la liste des utilisateurs à créer dans le domaine MDL.local :

Nom et prénom	Nom d'ouverture de session	Nom du dossier personnel	Mot de passe
Clément Ogier	cogier	cogier	Windows2019
Laure Dubreuil	ldubreuil	ldubreuil	Windows2019
Sylvie Pommier	spommier	spommier	Windows2019
Kevin Dalle	kdalle	kdalle	Windows2019

- Les informations à entrer sont comme ceci :

- Dans la fenêtre suivant on va entrer un mot de passe, il faut sélectionner la case « Le mot de passe n'expire jamais »

Faire la même chose pour tous les autres utilisateurs du domaine !

Création des groupes utilisateurs « Ligue Football » et « Ligue Basket »

- On commence par créer les 2 dossiers « ligue football » et « ligue basket », on va y gérer les droits NTFS différents dessus.

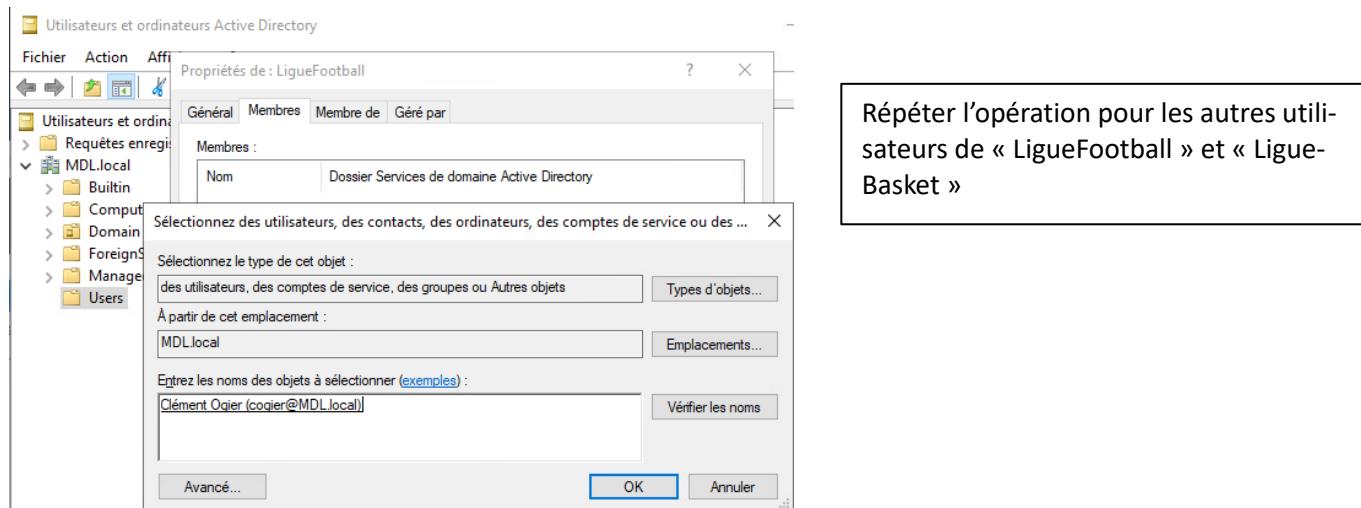
LigueBasket	14/03/2023 08:25	Dossier de fichiers
LigueFootball	14/03/2023 08:25	Dossier de fichiers

- On va maintenant affecter les utilisateurs dans les bon groupe :

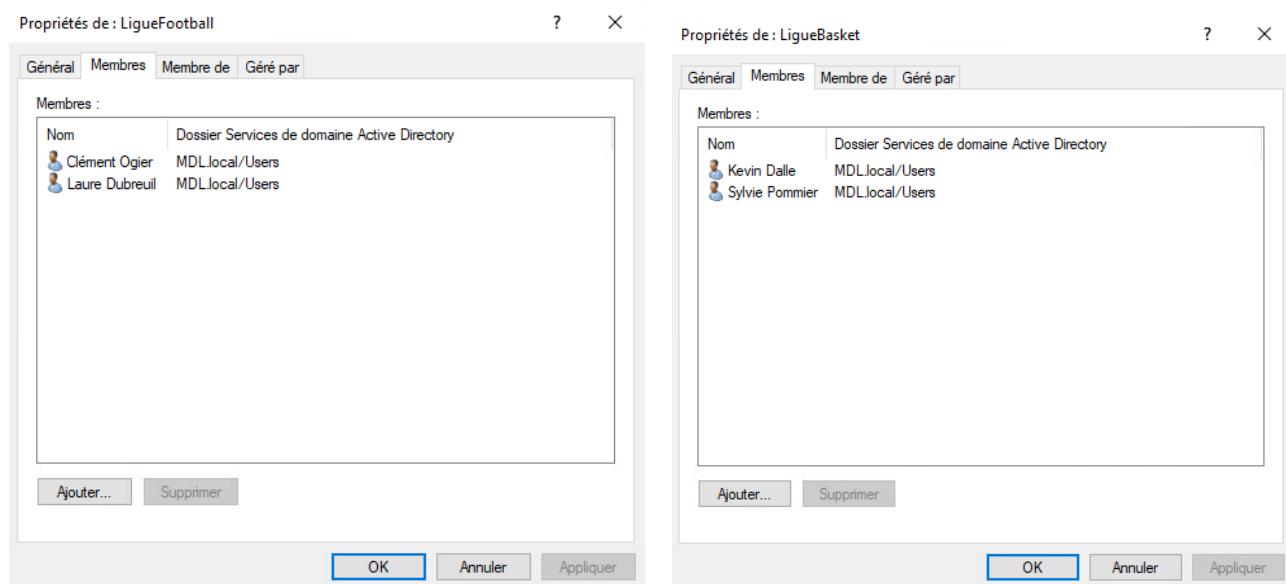
Nom de groupe	Membres du groupe
LigueFootball	Clément Ogier Laure Dubreuil
LigueBasket	Sylvie Pommier Kevin Dalle

- Pour cela on va se rendre dans le Gestionnaire de serveur dans « outils » et « utilisateur et ordinateur active directory », on va maintenant créer les groupes utilisateurs « LigueFootball » et « LigueBasket » en cliquant sur l'icône « créer un nouveau groupe dans le conteneur actuelle »
- On créer maintenant ces groupes comme ceci, en mettant bien l'étendu du groupe en « domaine local » :

- On va maintenant affecter les utilisateurs au groupe que l'on vient de créer, pour cela il faut se rendre dans les propriétés du groupe puis dans « membres » et les ajouter. Pour ajouter un utilisateur il faut mettre le début de son nom puis cliquer sur « vérifier les noms » :



- Un fois les utilisateurs ajoutés sur les deux groupes cliquer sur « appliquer » :



- Après avoir associer les utilisateurs aux groupes il va falloir configurer les droits NTFS des différents dossiers créés précédemment, pour cela on va retourner dans le dossier racine C : puis d'abord partager ces deux fichiers. Pour cela on va se rendre dans les Propriétés du fichiers, dans l'onglet « partage », « partage avancé », cocher la case « partager ce dossier » puis dans « autorisations » on met « contrôle totale » à tout le monde, cliquer sur « appliquer » et « ok ». Répéter la même opération pour le dossier LigueFootball :

The screenshot shows two windows side-by-side. On the left, the 'Autorisations du partage' (Sharing and Security) dialog for the 'LigueBasket' folder. It lists 'Noms de groupes ou d'utilisateurs : Tout le monde' and has buttons for 'Ajouter...' and 'Supprimer'. On the right, the 'Partage de fichiers et de dossiers en réseau' (File and folder sharing) dialog for the 'LigueBasket' folder. It shows the share name 'LigueBasket' with 'Partagé' checked (highlighted with a red box), and the network path '\\SERVEUR1\LigueBasket'.

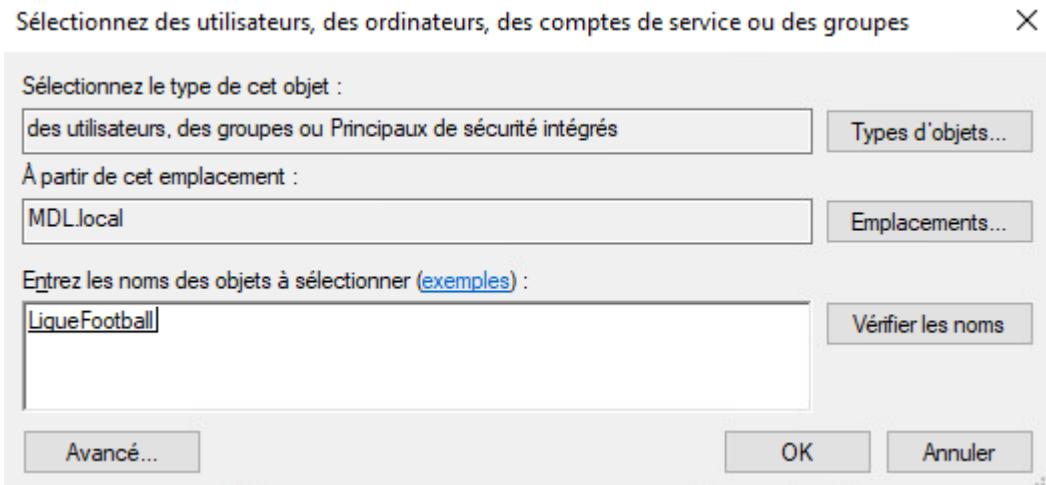
Autorisations pour Tout le monde	Autoriser	Refuser
Contrôle total	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modifier	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lecture	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- Maintenant que les dossiers sont partagés, on va désactiver l'héritage des 2 dossiers dans « propriétés », « sécurité » et « avancés » ; cliquer sur « désactiver l'héritage » puis sur « convertir les autorisations en autorisations explicites puis appliquer (faire la même chose pour l'autre dossier) :

The screenshot shows the 'Paramètres de sécurité avancés pour LigueFootball' dialog box. It displays basic security information like owner and group, and a table of explicit permissions for the 'LigueFootball' folder. The 'Activer l'héritage' button is highlighted in blue. At the bottom, there's a checkbox for replacing child object permissions with inheritable ones, and standard OK, Cancel, and Apply buttons.

Type	Principal	Accès	Hérité de	S'applique à
Auto...	Système	Contrôle total	Aucun	Ce dossier, les sous-dossiers et...
Auto...	Administrateurs (MDL\Administrateurs)	Contrôle total	Aucun	Ce dossier, les sous-dossiers et...
Auto...	Utilisateurs (MDL\Utilisateurs)	Lecture et exécution	Aucun	Ce dossier, les sous-dossiers et...
Auto...	Utilisateurs (MDL\Utilisateurs)	Spéciale	Aucun	Ce dossier et les sous-dossiers
Auto...	CREATEUR PROPRIETAIRE	Contrôle total	Aucun	Les sous-dossiers et les fichiers...

- On va maintenant ajouter les groupes « LigueFootball » au dossier « football » et « LigueBasket » au dossier « Basket » pour que seul les utilisateurs de bons groupe puissent avoir les bons droits dessus, pour cela on va aller dans propriétés et l'onglet « sécurité », puis sur le bouton ajouter afin de mettre le groupe « LigueFootball ». Faire la même chose pour l'autre dossier :



- Pour le dossier football, il faut que les utilisateurs puissent accéder au dossier mais ne peuvent pas créer, supprimer ou modifier des fichiers et dossiers sauf l'utilisateur « Clément Ogier », pour cela on met uniquement le droit « lecture et exécution » au groupe « LigueFootball » et on ajoute l'utilisateur Clément Ogier pour lui donner le droit « Modification ».

The screenshot shows two side-by-side Windows file permission configuration windows. Both have a header with user/group names and a "Modifier..." button. The left window is for "LigueFootball (MDL\LigueFootball)" and the right is for "Clément Ogier (cogier@MDL.local)". Both show a list of permissions: Contrôle total, Modification, Lecture et exécution, Affichage du contenu du dossier, Lecture, and Écriture. Under "LigueFootball", the "Modification" and "Écriture" checkboxes are checked under "Autoriser". Under "Clément Ogier", all checkboxes are checked under "Autoriser".

- Pour le dossier Basket, c'est la même chose mais ici c'est l'utilisateur Kevin Dalle qui doit avoir le droit de modification.

Inventaire du matériel avec GLPI/fusionInventory

Installation de l'infrastructure logicielle : IIS, Mysql, PHP, et GLPI

Préparer et effectuer l'installation de GLPI sur le serveur membre SERVEUR1 MDL avec les contraintes suivantes :

- Installation de GLPI sous un serveur web Microsoft IIS (sur SERVEUR2) ;
- Utilisation imposée du SGBD Mysql (sur SERVEUR2) ; Nom de la base de donnée GLPI à créer sous Mysql : *glpi* ;
- Installation imposée de PHP Manager (processeur PHP utilisant Fast CGI pour Windows) (sur SERVEUR2) ;

Déploiement du plugin FusionInventory sur chaque poste pour la remontée automatique des données vers GLPI

- Tout d'abord il faut installer le rôle Serveur Web IIS avec les rôle CGI

→ On va maintenant installer PHP 7 :

- Copier la dernière version (Non-Thread Safe (NTS)) du dossier PHP 7 fourni (*php-7.2.11-nts-Win32-VC15-x64*) dans le dossier *C:\Program Files* (en Français Programmes) ;
- Renommer le fichier *php.ini-development* en ***php.ini*** ;
- Ajouter le chemin du dossier *C:\Program Files\php-7.2.11-nts-Win32-VC15-x64* à la variable d'environnement *Path*

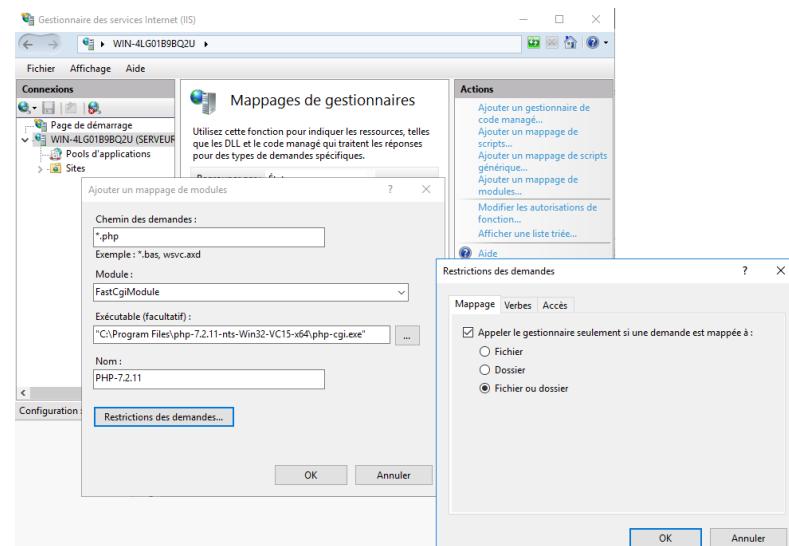
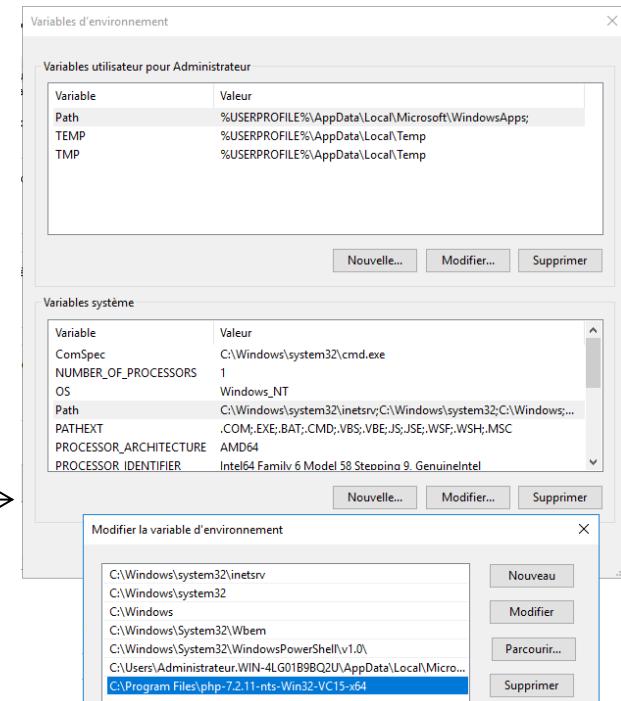
(Panneau de configuration / Système et sécurité, Système, lien Paramètres système avancés ; dans la fenêtre qui s'ouvre, sélectionner l'onglet Avancé, puis le bouton Variables d'environnement ; dans Variables système, sélectionner la ligne Path, puis cliquer sur le bouton Modifier ; cliquer sur le bouton Nouveau pour ajouter le chemin *C:\Program Files\php-7.2.11-nts-Win32-VC15-x64* à la variable Path) →

- Dans le Gestionnaire IIS, configurer PHP comme suit : cliquer sur le nom du serveur, puis double-cliquer sur l'icône *Mappages de gestionnaires* ; dans le panneau Action, cliquer sur le lien *Ajouter un mappage de module* :

Chemin demandes : *.php
 Module : *FastCgiModule*
 Exécutable : taper le chemin d'accès complet à *Php-cgi.exe* :
C:\Program Files\php-7.2.11-nts-Win32-VC15-x64\php-cgi.exe
 Nom : entrer un nom pour le mappage : *php-7.2.11*

cliquer ensuite sur le bouton *Restrictions des demandes* et cocher *Fichier ou dossier*.

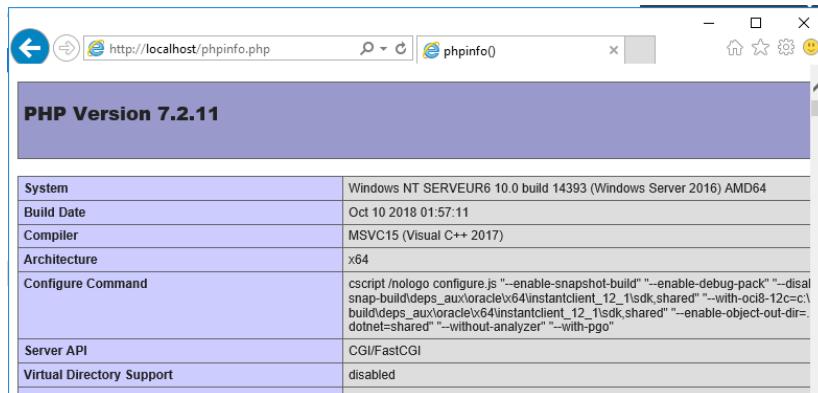
Ainsi, tous les fichiers d'extension .php seront envoyés au module *FastCGIModule* pour y être exécutés par le programme *php-cgi.exe*.



- Installer le package redistribuable Microsoft Visual C++ *vc_redist.x64-2015.exe* (c'est bien la version 2015 pour systèmes 64 bits qui est nécessaire ici) ;
- Pour vérifier l'installation de PHP, créer le fichier suivant avec le bloc-notes :

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

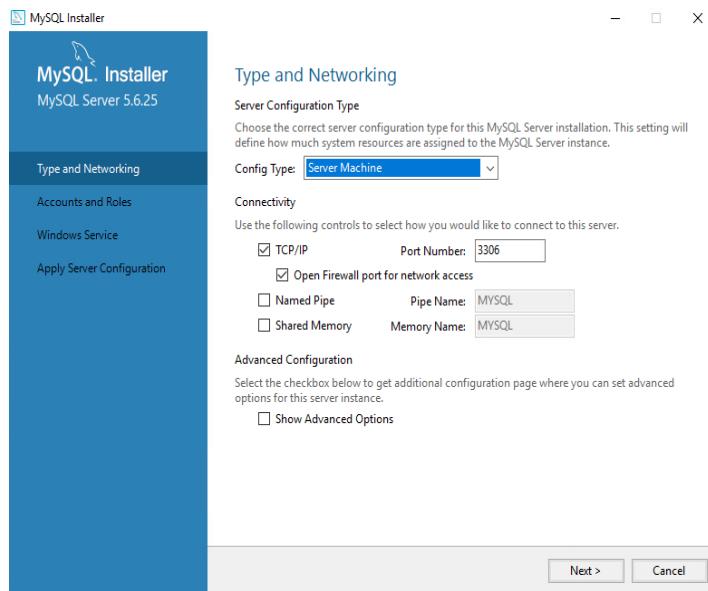
enregistrer ce fichier dans **C:\inetpub\wwwroot\phpinfo.php**
 puis ouvrir le navigateur et entrer l'URL suivante : *http://localhost/phpinfo.php* :
 une page Web bien formatée doit s'afficher et présenter les paramètres PHP actuels :



PHP Version 7.2.11	
System	Windows NT SERVEUR6 10.0 build 14393 (Windows Server 2016) AMD64
Build Date	Oct 10 2018 01:57:11
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-snap-builddeps_aux\oracle\x64\instantclient_12_1\ sdk\shared" "--with-oci8-12c=c:\builddeps_aux\oracle\x64\instantclient_12_1\ sdk\shared" "--enable-object-out-dir=dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled

- Installer *PHPManager* version 1.5, qui fonctionne bien avec IIS version 10, avec le .msi fourni.
- Redémarrer le serveur (indispensable pour que le programme PHP Manager apparaisse dans la liste des fonctionnalités de IIS).
- Lancer PHP Manager, puis enregistrer PHP dans IIS (*Enregistrer une nouvelle version de PHP*), puis vérifier que PHP est bien fonctionnel (*Vérifier phpinfo()*) ; si cette dernière vérification ne fonctionne pas, c'est sans doute que la version installée du package redistribuable Microsoft Visual C++ *n'est pas la bonne* !

Installation du SGBD MySQL



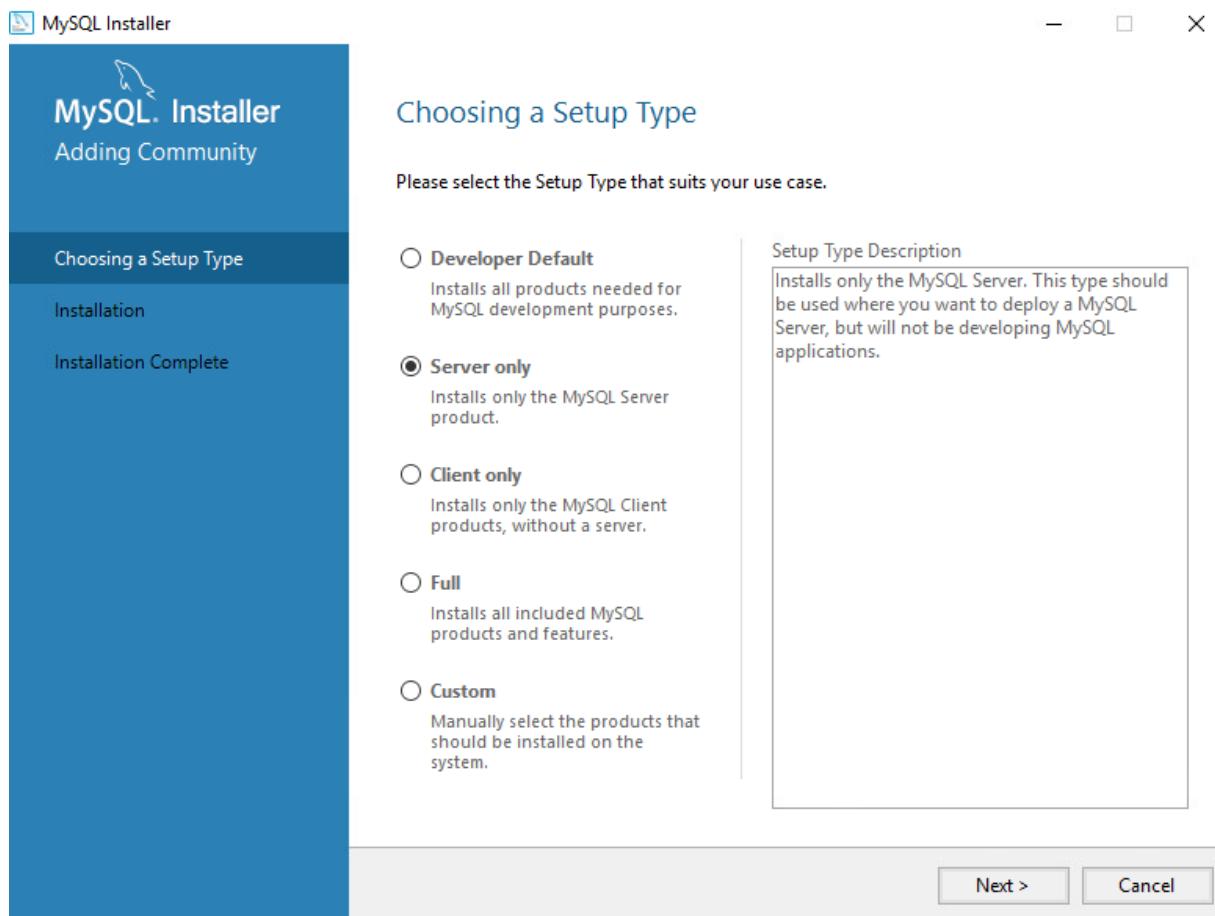
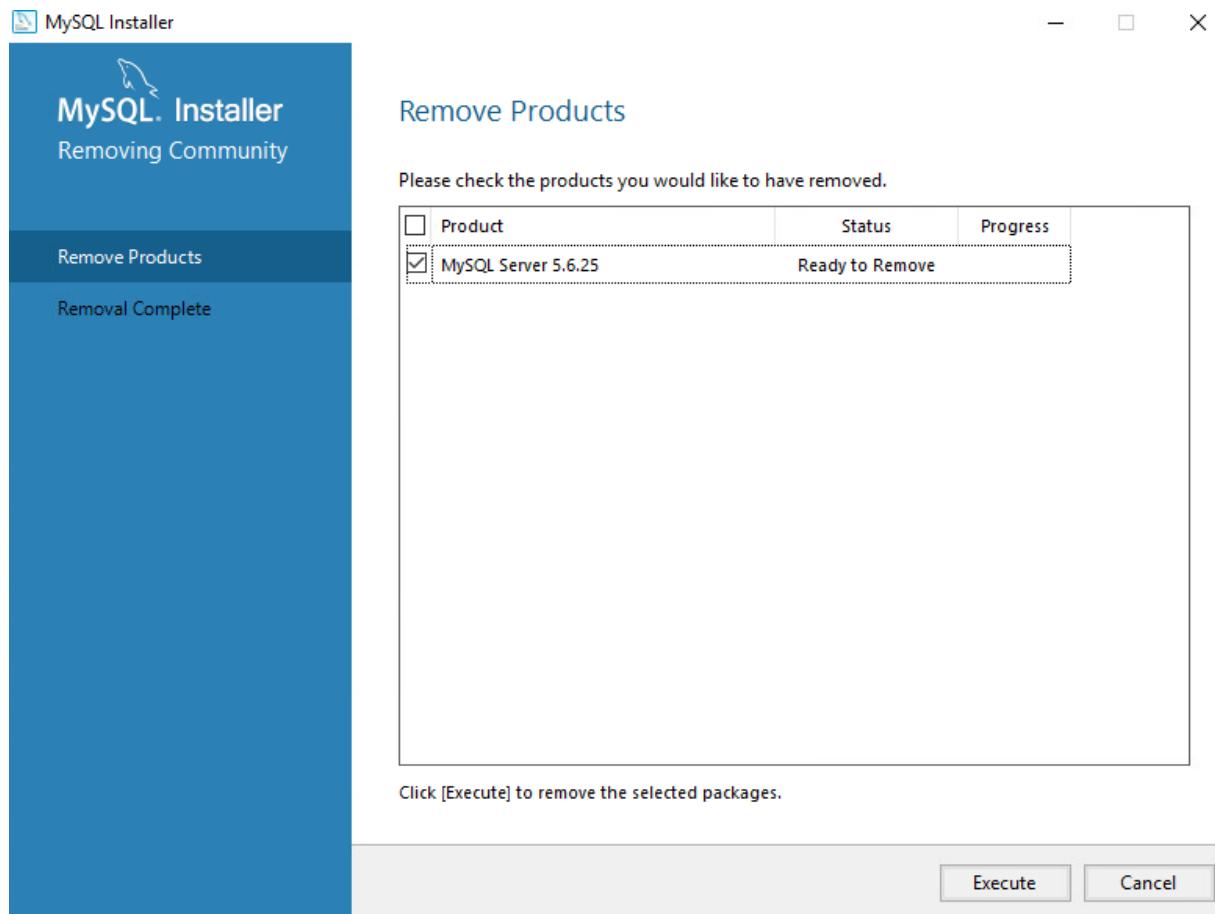
Accounts and Roles

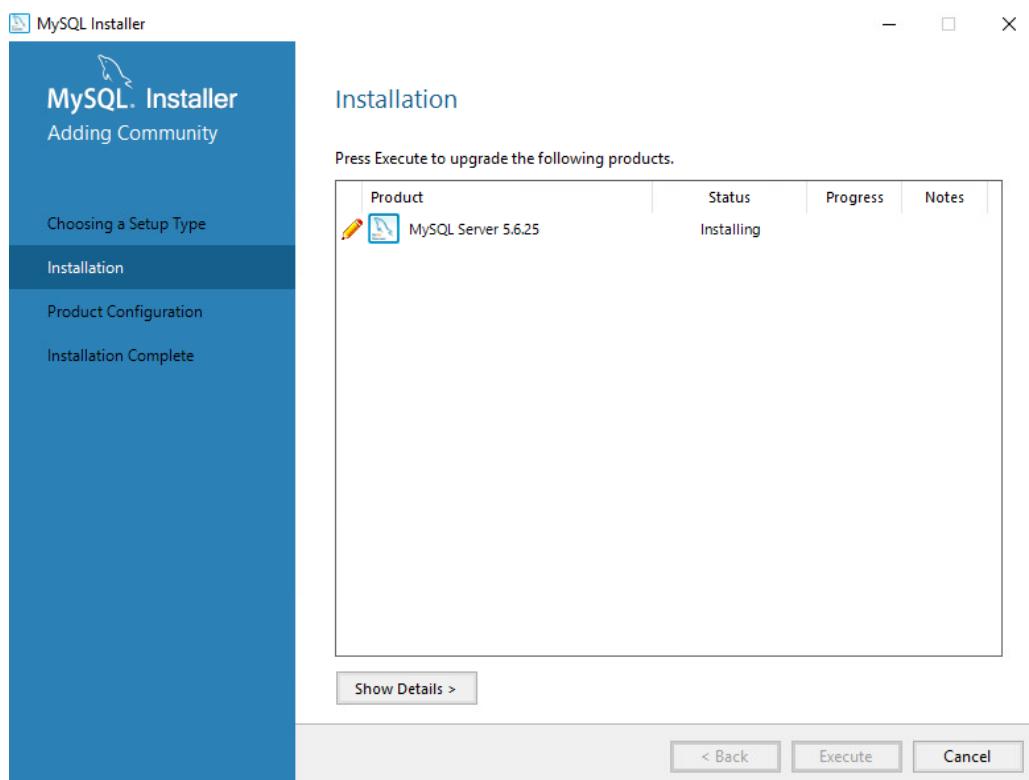
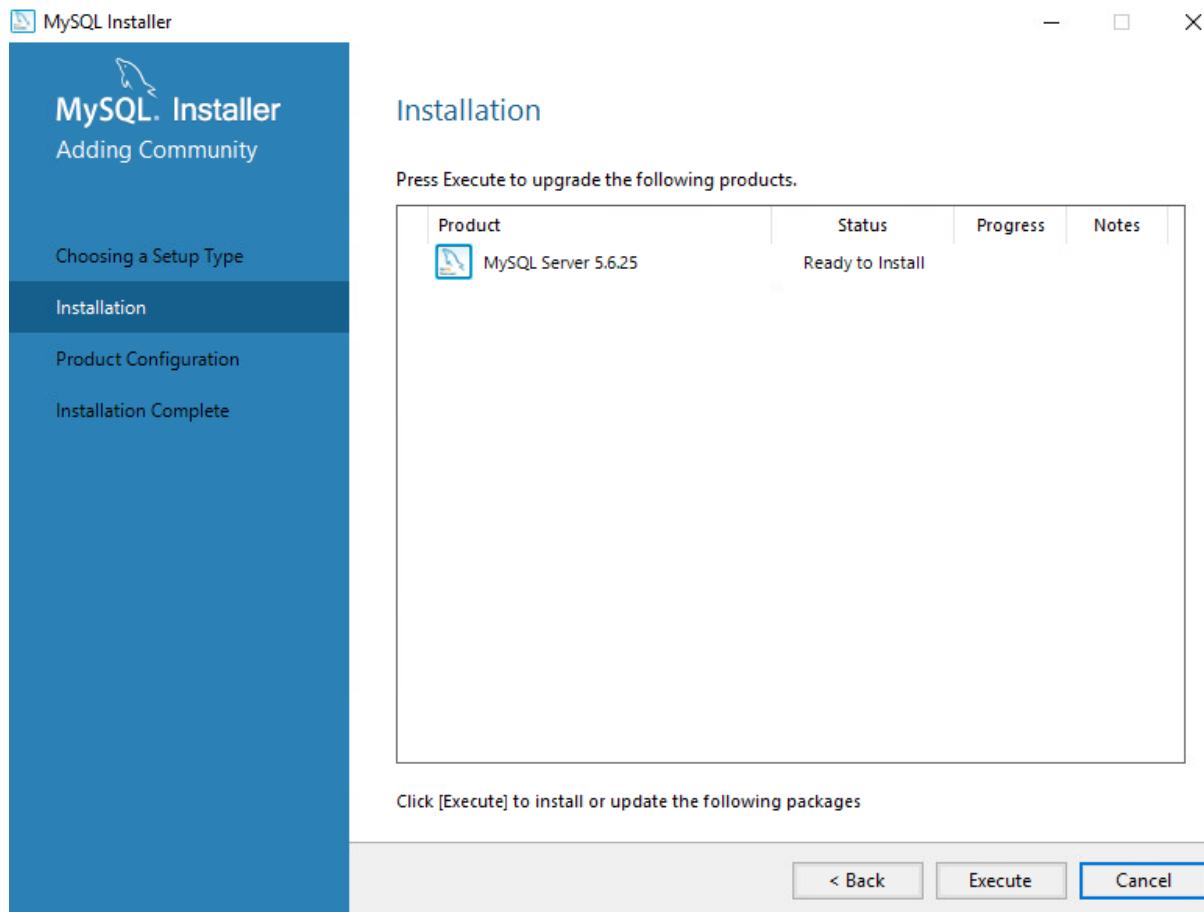
Root Account Password

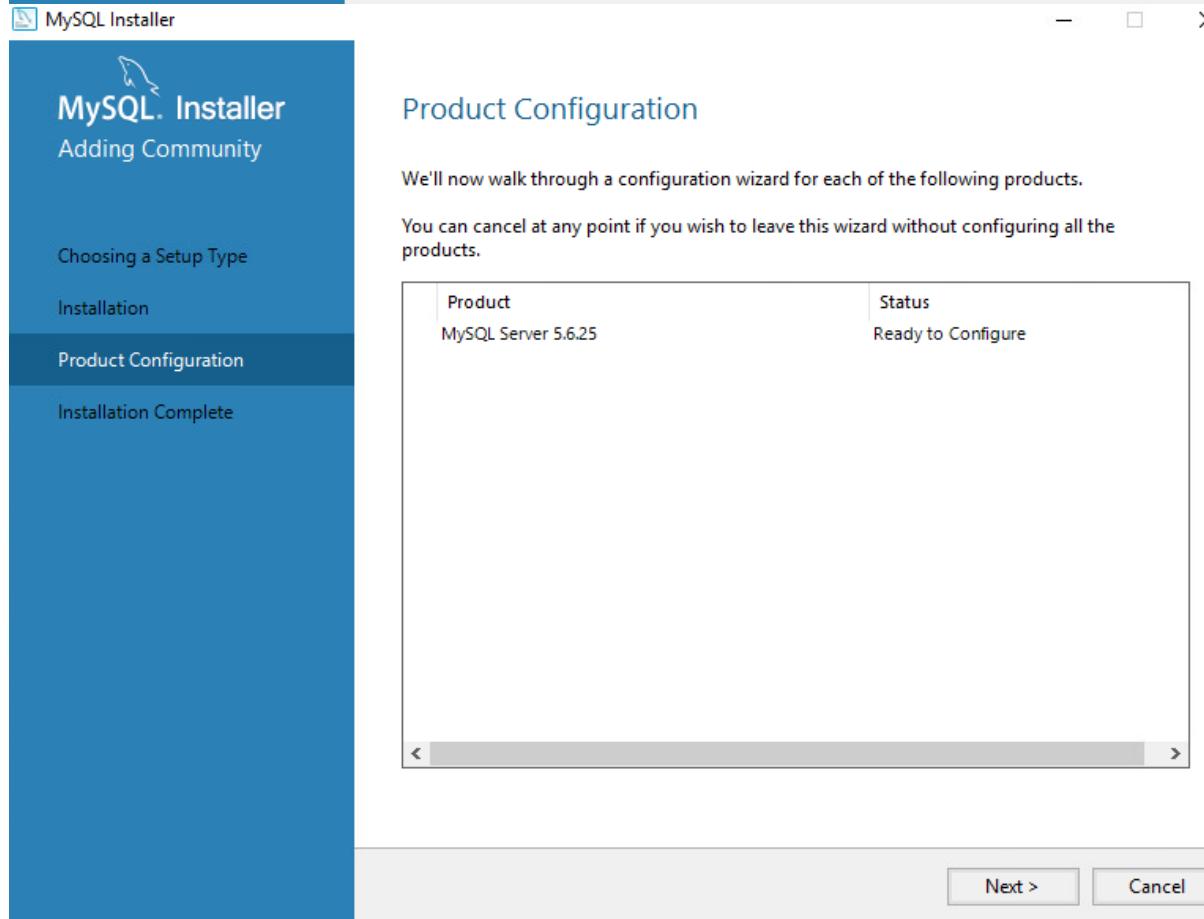
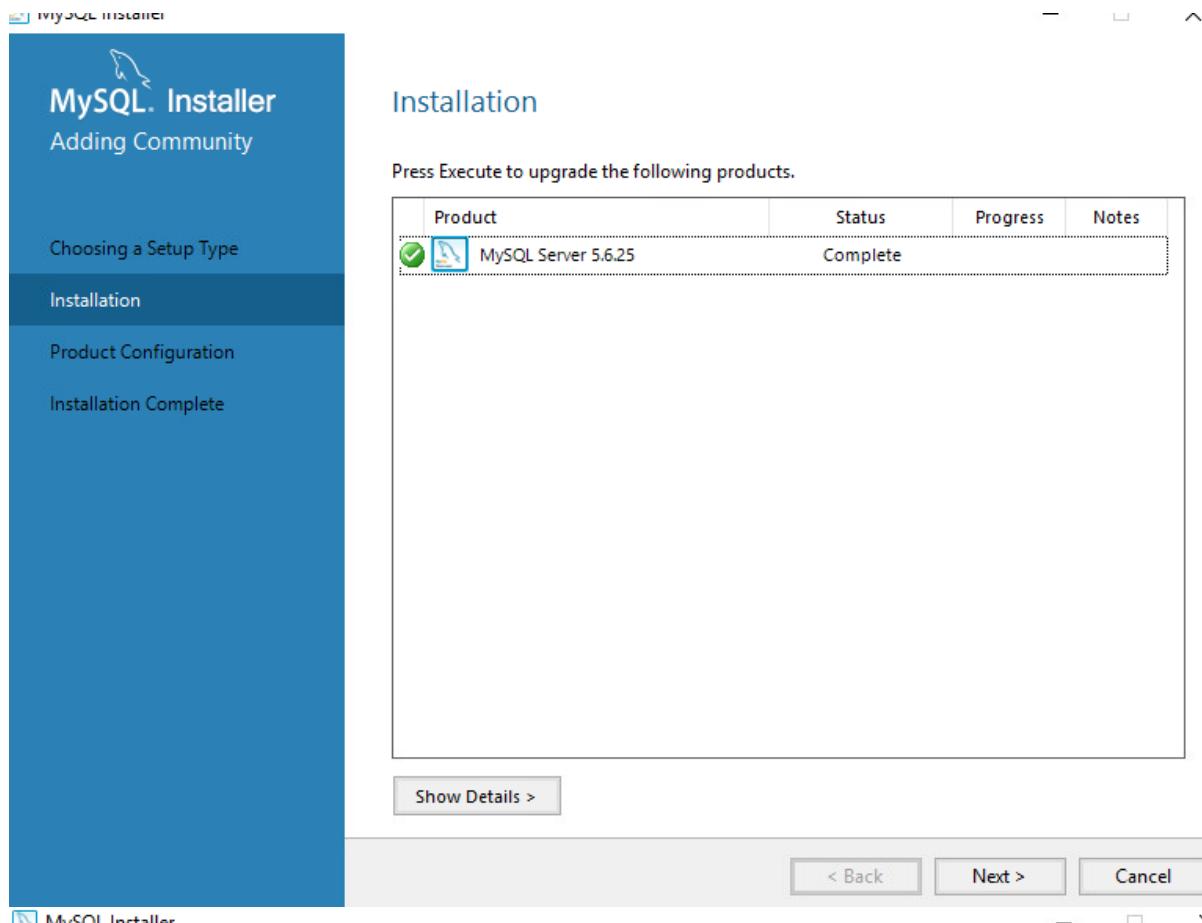
Enter the password for the root account. Please remember to store this password in a secure place.

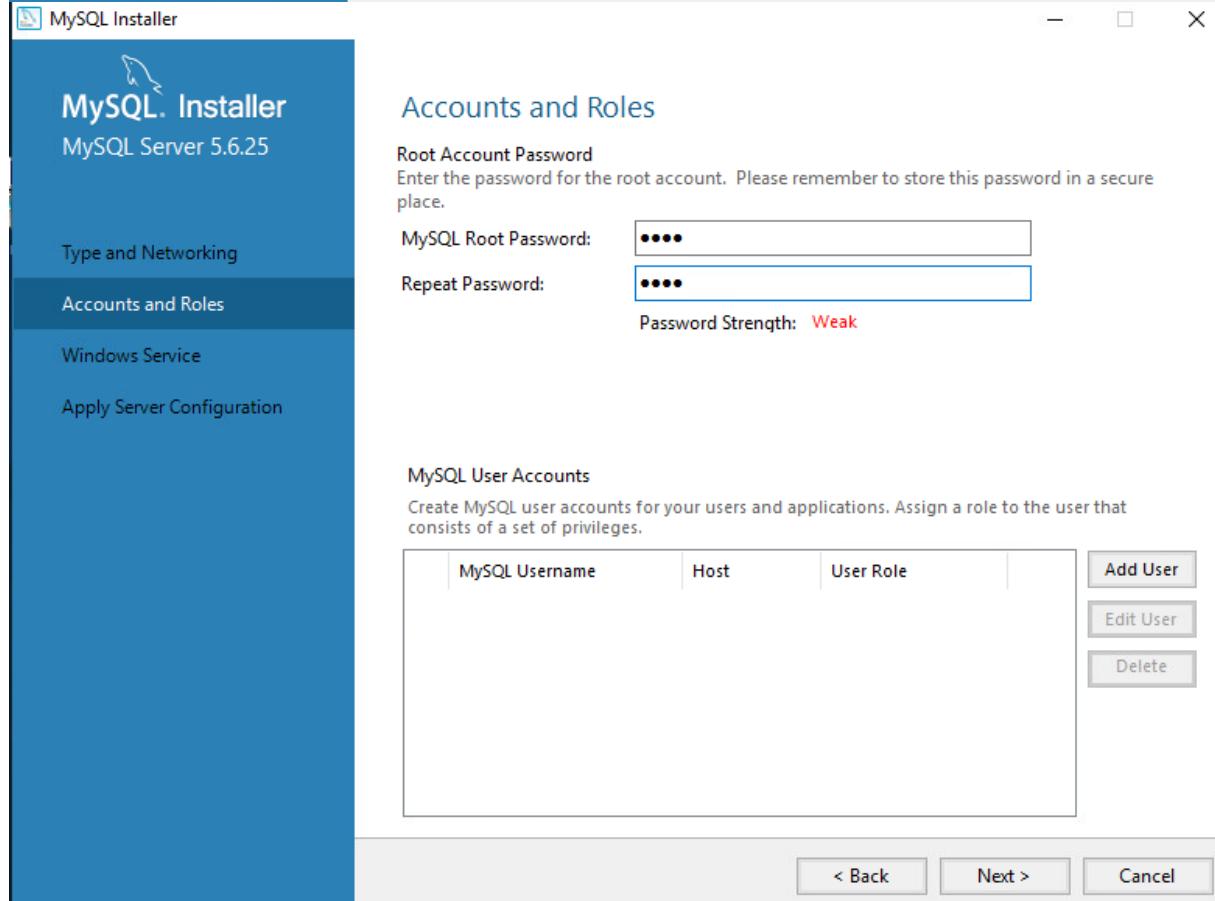
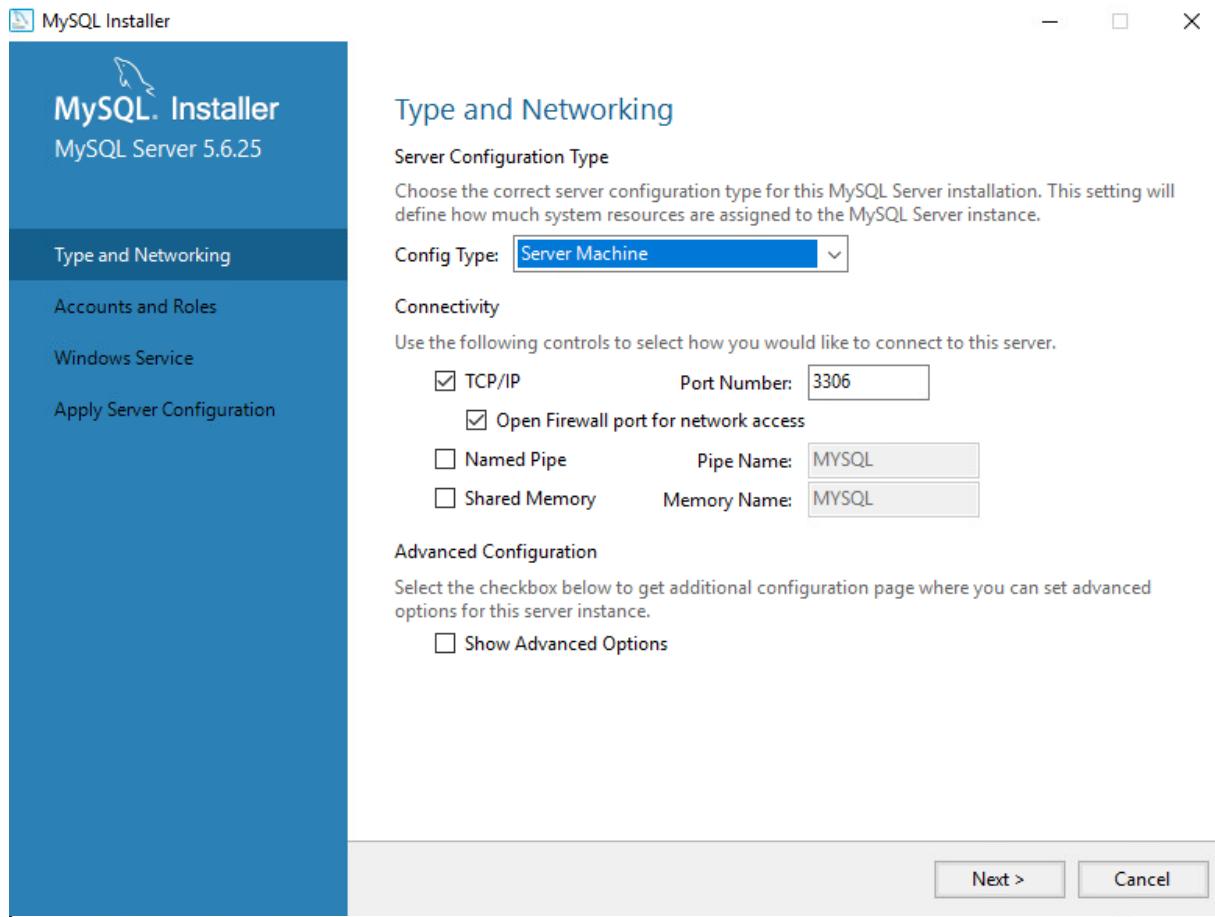
Current Root Password:

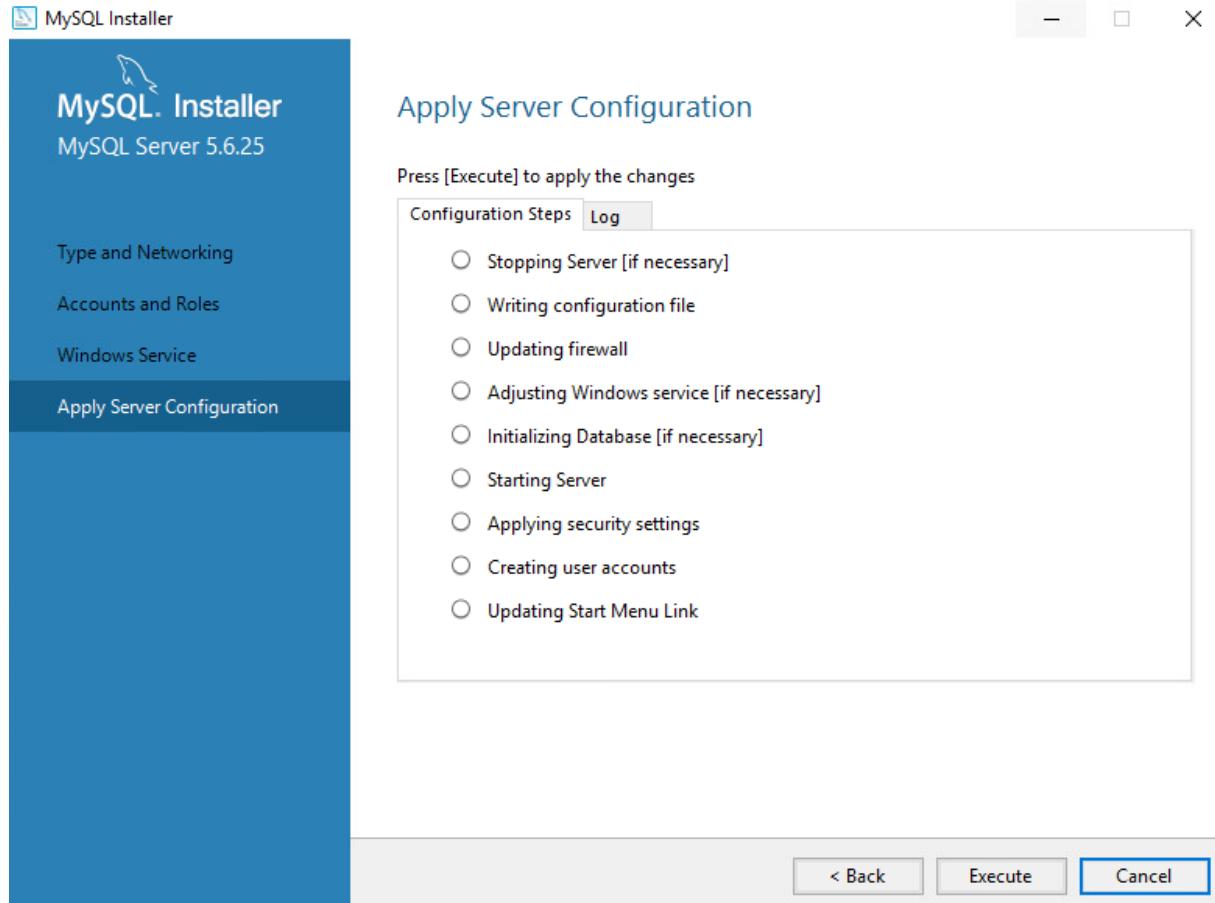
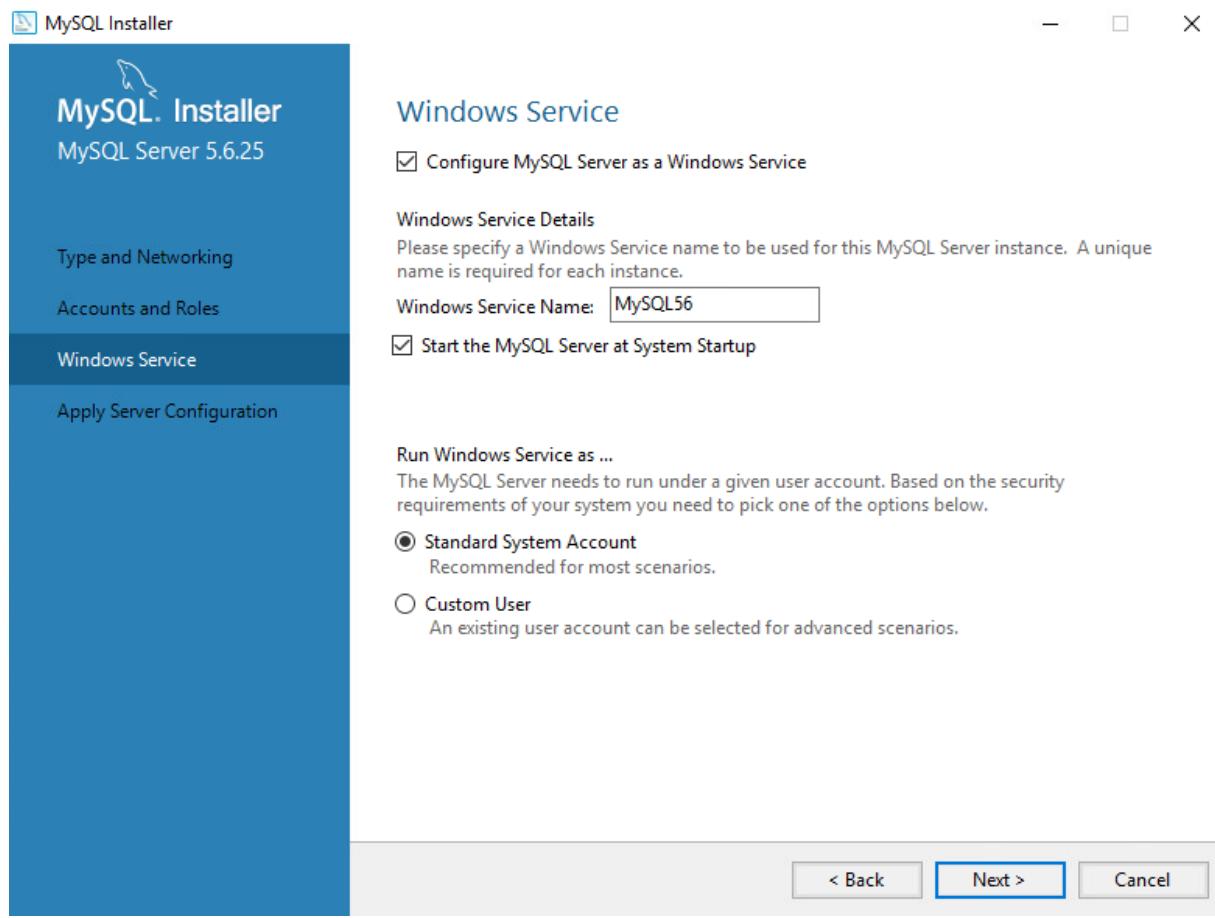
Check

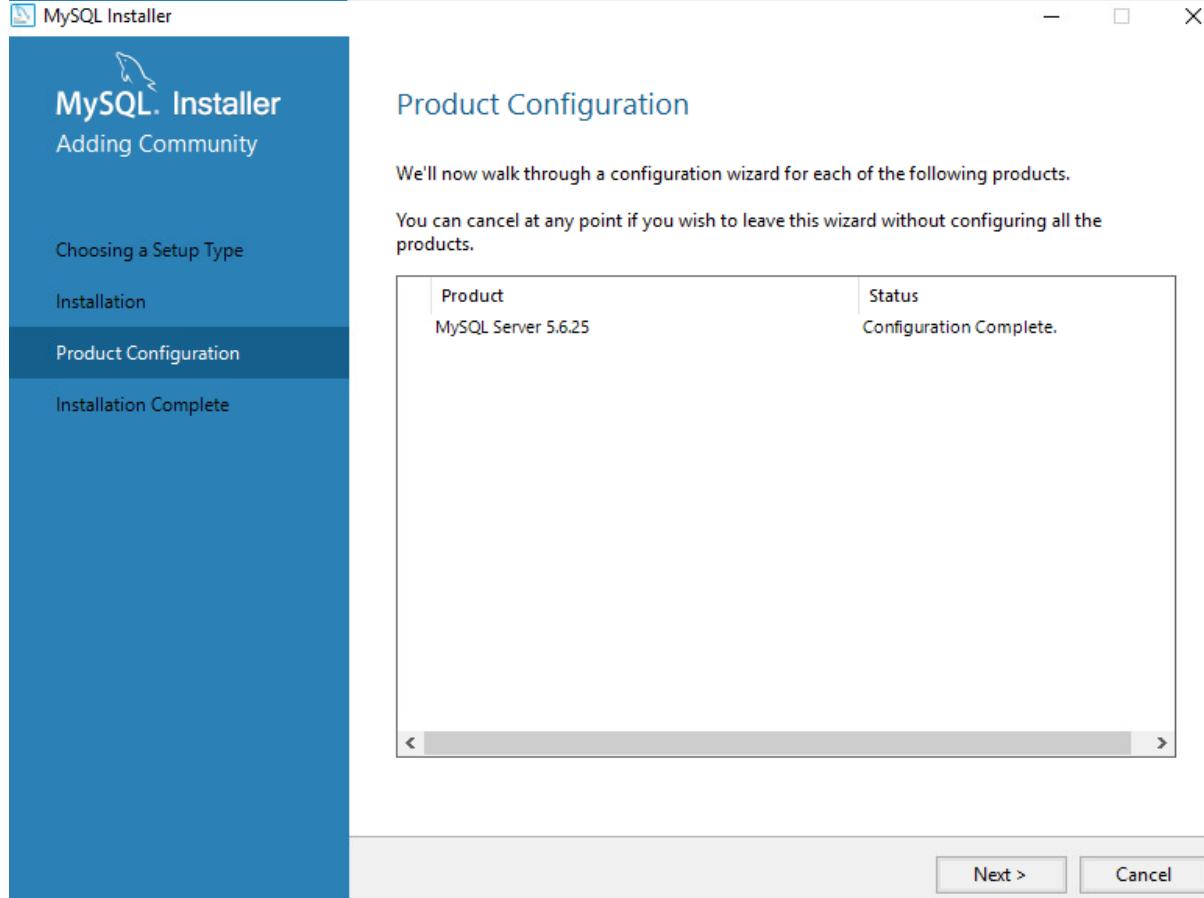
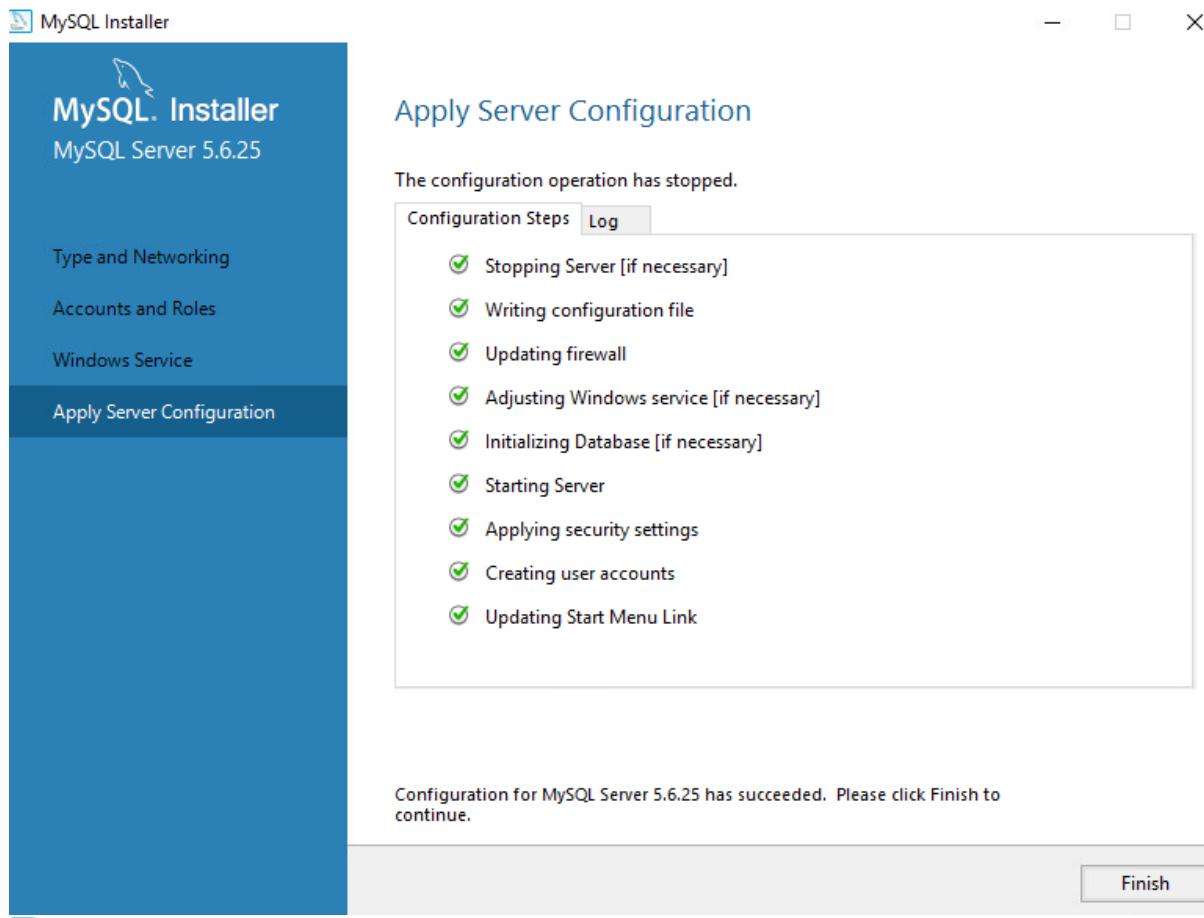












Dans PHP Manager, activer les extensions suivantes (utilisées par GLPI) :
- **php_fileinfo.dll**
- **php_ldap.dll**

- ***php_imap.dll***

- ***php_mysqli.dll***

(utiliser le lien *Activer ou désactiver une extension*, puis cliquer sur l'extension à activer, et enfin cliquer sur le lien *Activer* ; on peut aussi ouvrir directement le fichier *php.ini*, et supprimer le commentaire ; devant l'extension voulue).

Installer GLPI :

1. copier le dossier *glpi* dans *inetpub\wwwroot*
2. Dans l'explorateur Windows, attribuer l'autorisation *Modification* à *Utilisateurs* pour le dossier *C:\inetpub\wwwroot\glpi*
3. sous IIS, si besoin, créer le site web sous le nom *glpi* avec le nom d'hôte *www.glpi.fr*

Pour la première connexion à GLPI, suivre les indications de l'[Annexe 1](#)

Installer le plugin FusionInventory :

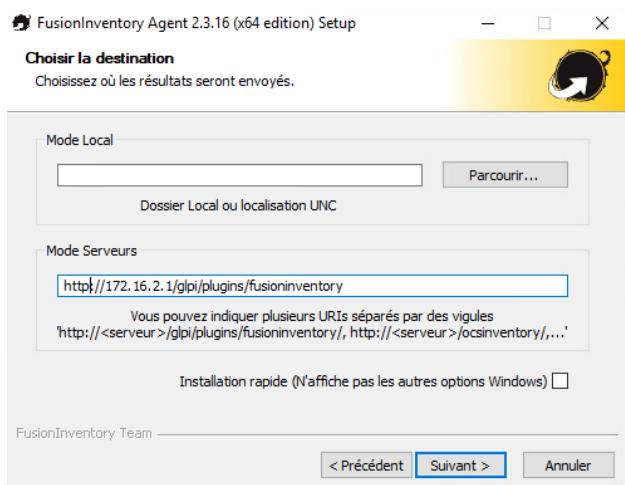
1. copier le dossier *fusionInventory* dans *inetpub\wwwroot\glpi\plugins*
2. Dans GLPI, sélectionner la commande *Configuration / Plugins* ; dans la ligne du plugin FusionInventory, cliquer sur le lien *Installer*, puis ensuite sur le lien *Activer* ;
3. Toujours dans GLPI, sélectionner la commande *Administration / Entités*, puis cliquer sur le lien *Root entity, puis sur le lien Fusioninventory* : saisir l'URL d'accès au service :
http://192.168.3.2/glpi/plugins/fusioninventory/

Déployer l'agent FusionInventory Windows (en tant que service Windows) **sur chaque poste Windows du réseau** (installer manuellement et configurer l'agent FusionInventory Windows sur chaque poste Windows).

Installation et exécution de l'agent FusionInventory sous Windows

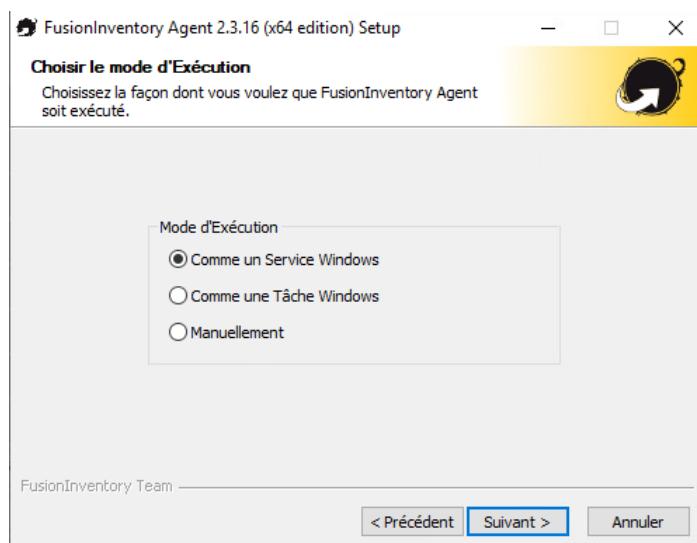
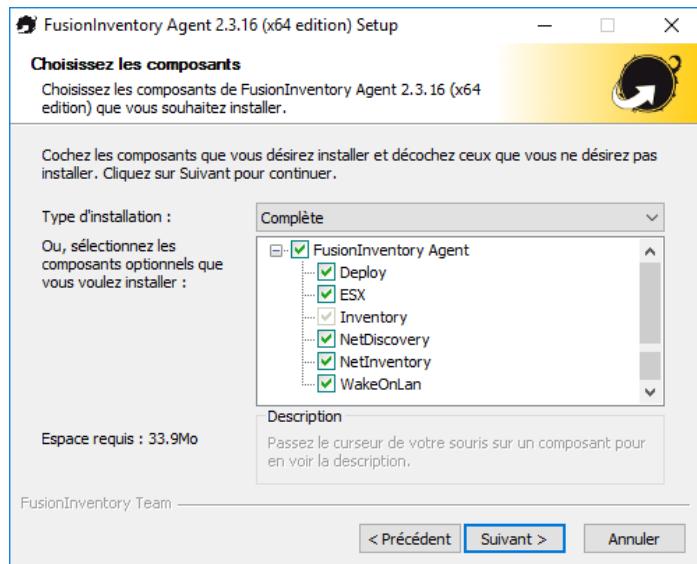
Installation manuelle de l'agent

(toujours choisir le type d'installation **Complète**) :



Installation manuelle de l'agent

(toujours choisir le type d'installation **Complète**) :



- Le plugin doit être installé sur chaque poste !

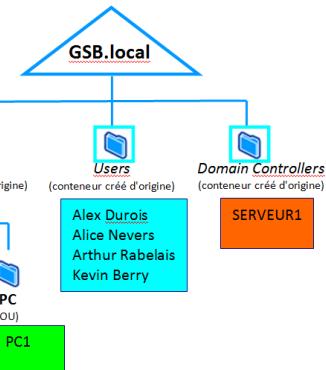
Importation des utilisateurs avec l'annuaire ldap

Au lieu de créer les utilisateurs un par un dans GLPI, nous allons importer ceux déjà créés dans l'Active Directory du domaine Windows 2016 (Active Directory est en effet un annuaire LDAP).

- Dans le fichier *php.ini*, penser à supprimer le commentaire ; devant *extension=php_ldap.dll* (le module LDAP pour PHP sera ainsi installé) ; de même, penser à supprimer le commentaire ; devant *extension=php_imap.dll* (le protocole de messagerie IMAP sera ainsi installé).

- b. Dans GLPI, configurer le serveur LDAP à atteindre (*Configuration / Authentification* puis *Annuaires LDAP*) (ajouter un nouvel annuaire en cliquant sur le bouton “+” situé dans la barre de menu) :

Nom (du serveur LDAP) :	<i>SERVEUR1</i>
Serveur par défaut :	<i>Oui</i>
Actif :	<i>Oui</i>
Serveur (adresse IP) :	<i>192.168.3.1</i>
Port :	<i>389</i>
Filtre de connexion :	<i>(&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))</i>
Basedn :	<i>CN=Users,DC=GSB,DC=local</i>
DN du compte :	<i>CN=Administrateur,CN=Users,DC=GSB,DC=local</i>
Mot de passe du compte :	<i>Windows2016</i>
Champ de l'identifiant :	<i>samaccountname</i>



Remarques :

- le *filtre de connexion* pour Windows est toujours celui donné ci-dessus.
- *Basedn* est le chemin du conteneur (ou éventuellement de l'OU) dans lequel sont stockés les utilisateurs de l'Active Directory.
- *DN du compte* est le nom du compte Active Directory qui permettra de se connecter à l'AD (ici, l'administrateur).

Annuaire LDAP - ID 1		
Nom	SERVEUR1	Dernière modification 2015-06-25 17:22
Serveur par défaut	Oui	Actif Oui
Serveur	192.168.3.1	Port (par défaut 389) 389
Filtre de connexion	<i>(&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))</i>	
BaseDN	<i>CN=Users,DC=GSB,DC=local</i>	
DN du compte (pour les connexions non anonymes)	<i>CN=Administrateur,CN=Users,DC=GSB,DC=local</i>	
Mot de passe du compte (pour les connexions non anonymes)	<input type="password"/>	<input type="checkbox"/> Effacer Champ de l'identifiant <i>samaccountname</i>
Commentaires	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>	
Sauvegarder		
Supprimer		

- c. Sauvegarder la configuration de ce serveur LDAP (bouton *Sauvegarder*), et tester la connexion à ce serveur (bouton *Tester*).

- d. Importer les utilisateurs de ce serveur LDAP (*Administration / Utilisateurs* puis bouton *Liaison annuaire LDAP* puis lien *Importation de nouveaux utilisateurs* puis bouton *Rechercher* ; cocher tous les utilisateurs puis dans *Actions*, sélectionner *Importer* ; valider avec *Envoyer*) :

Identifiant	Courriel
kberry	2013-07-21 14:26
arabelais	2013-07-21 23:50
anevers	2013-08-19 18:46
adurois	2013-07-21 15:40

Identifiant	Dernière mise à jour dans l'annuaire LDAP
	2013-07-21 14:26
	2013-07-21 23:50
	2013-08-19 18:46
	2013-07-21 15:40

- e. Vérifier que les utilisateurs ont bien été importés (*Administration / Utilisateurs*) :

Identifiant	Nom de famille	Adresses de messagerie	Téléphone	Lieu	Actif
adurois	Durois				Oui
anevers	Never				Oui
arabelais	Rabelais				Oui
glpi					Oui
kberry	Berry				Oui
normal					Oui
Plugin_FusionInventory					Oui
post-only					Oui
tech					Oui

Installation d'un VPN :

- a. Depuis le poste SERVEUR1 par exemple, se connecter à l'interface LAN du routeur-parefeu PfSense pour le configurer, avec le navigateur Mozilla Firefox.
- b. Sélectionner la commande PfSense System Cert Manager, puis dans l'onglet CAs, créer une nouvelle autorité de certification et son certificat d'autorité de certification, en cliquant sur Add, de nom **CA_Acces_VPN**, avec une clé RSA de 2048 bits, l'algorithme de hashage **sha256**, et en choisissant la méthode *Create an internal Certificate Authority* (**attention : veiller à toujours mettre le même nom pour les champs Descriptive Name et Common Name**) :

The screenshot shows the 'Create / Edit CA' configuration page. The 'Descriptive name' field is set to 'CA_Acces_VPN'. The 'Method' dropdown is set to 'Create an internal Certificate Authority'. Under 'Internal Certificate Authority', the 'Key type' is 'RSA', 'Key Length' is '2048', and the 'Digest Algorithm' is 'sha256'. The 'Lifetime (days)' is set to '3650'. The 'Common Name' is also 'CA_Acces_VPN'. Below these fields, optional subject components are listed: 'Country Code' (FR), 'State or Province' (test), 'City' (test), 'Organization' (test), and 'Organizational Unit' (e.g. My Department Name (optional)). A blue 'Save' button is at the bottom.

- c. Toujours dans la commande *System Cert Manager*, mais dans l'onglet *Certificates*, créer un nouveau certificat, le certificat SSL du serveur Pfsense OpenVPN (dont la clé publique permettra de chiffrer le trafic entre client et serveur VPN), de nom *Certificat_Acces_VPN*, de type **Server Certificate**, et en choisissant la méthode *Create an internal Certificate* ; sélectionner l'autorité de certification créée précédemment *CA_Acces_VPN* qui va signer ce certificat (**attention : veiller à toujours mettre le même nom pour les champs Descriptive Name et Common Name**) :

Configuration du serveur OpenVPN sur le routeur-parefeu PfSense

 **Rappel préalable :** le serveur OpenVPN sera accessible de l'extérieur via son interface WAN ; on devra pouvoir accéder à ce serveur à partir d'un poste de la salle R211 (qui a donc une adresse privée).

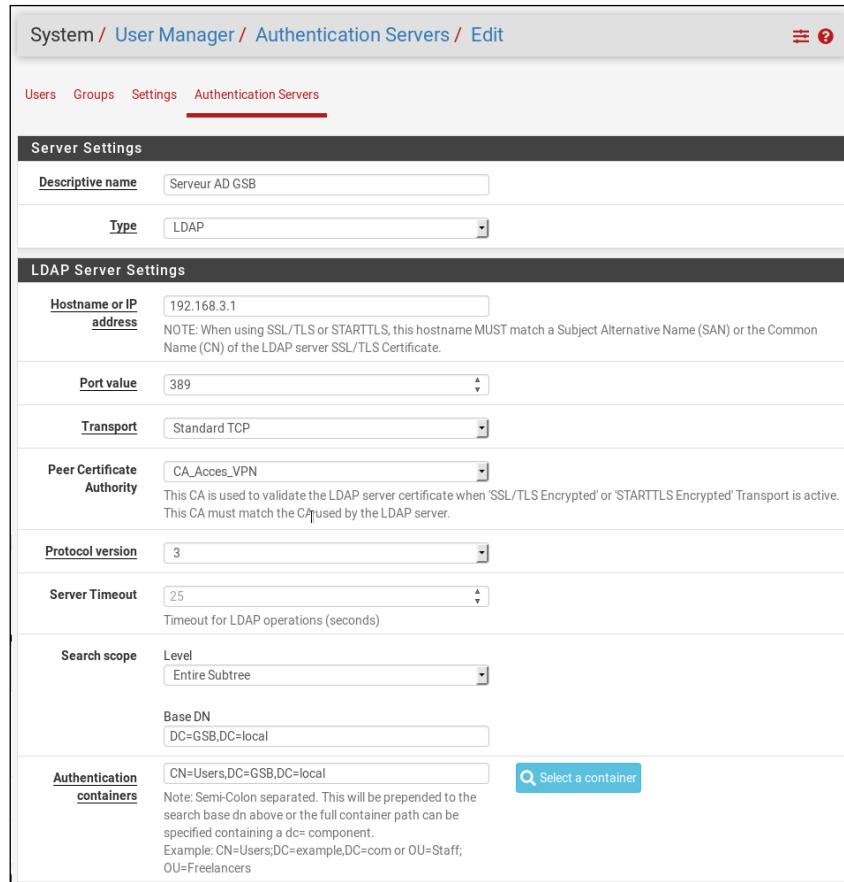
Il faut donc bien penser à rendre accessible le Pfsense depuis un poste ayant une adresse IP privée en vérifiant que la case *Block private networks* **de l'interface WAN** est décochée.

- Sur le poste SERVEUR1, créer l'utilisateur suivant dans l'Active Directory du domaine GSB (décocher la case «*L'utilisateur doit changer le mot de passe ...*» et cocher la case «*Le mot de passe n'expire jamais*») :

Nom	Nom d'ouverture de session	Mot de passe
User_VPN_LDAP	User_VPN_LDAP	Windows2019

Cet utilisateur *User_VPN_LDAP* permettra au firewall de s'authentifier sur l'Active Directory.

- Configurer l'authentification depuis l'Active Directory, avec la commande *System User Manager*, dans l'onglet *Authentication Servers*, pour créer un nouveau serveur d'authentification de nom *Serveur AD GSB*, de type *LDAP*, et de modèle initial *OpenLDAP*, qui sera le serveur de domaine *GSB.local* :



System / User Manager / Authentication Servers / Edit

Users Groups Settings Authentication Servers

Server Settings

Descriptive name: Serveur AD GSB

Type: LDAP

LDAP Server Settings

Hostname or IP address: 192.168.3.1
NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.

Port value: 389

Transport: Standard TCP

Peer Certificate Authority: CA_Acces_VPN
This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.

Protocol version: 3

Server Timeout: 25
Timeout for LDAP operations (seconds)

Search scope: Level
Entire Subtree

Base DN: DC=GSB,DC=local

Authentication containers: CN=Users,DC=GSB,DC=local
Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component.
Example: CN=Users;DC=example,DC=com or OU=Staff; OU=Freelancers

(suite de la figure : page suivante)

System / User Manager / Authentication Servers / Edit

Users Groups Settings Authentication Servers

Server Settings

Descriptive name Serveur AD GSB

Type LDAP

LDAP Server Settings

Hostname or IP address 192.168.3.1

NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.

Port value 389

Transport Standard TCP

Peer Certificate Authority CA_Acces_VPN

This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.

Protocol version 3

Server Timeout 25

Timeout for LDAP operations (seconds)

Search scope Level
Entire Subtree

Base DN DC=GSB,DC=local

Select a container

Authentication containers CN=Users,DC=GSB,DC=local

Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component.

Example: CN=Users;DC=example,DC=com or OU=Staff, OU=Freelancers

Extended query Enable extended query

Bind anonymous Use anonymous binds to resolve distinguished names

Bind credentials CN=User_VPN_LDAP,CN=Users,DC=GSB,DC=local

Initial Template OpenLDAP

User naming attribute samAccountName

Group naming attribute cn

Group member attribute member

RFC 2307 Groups LDAP Server uses RFC 2307 style group membership

RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).

Group Object Class posixGroup

Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

Shell Authentication Group DN

If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login.

Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com

UTF8 Encode UTF8 encode LDAP parameters before sending them to the server.

Required to support international characters, but may not be supported by every LDAP server.

Username Alterations Do not strip away parts of the username after the @ symbol
e.g. user@host becomes user when unchecked.

Allow unauthenticated bind Allow unauthenticated bind

Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.

Save

- c. Valider et tester le serveur d'authentification, avec la commande System User Manager, dans l'onglet Settings :

Authentication Server : *Serveur AD GSB*

The screenshot shows the pfSense User Manager settings page. The navigation bar at the top includes links for System, User Manager, and Settings. The Settings tab is selected. Below the tabs, there are several configuration sections:

- Session timeout:** A dropdown menu set to "Serveur AD GSB". A note below it states: "Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire sessions. NOTE: This is a security risk!"
- Authentication Server:** A dropdown menu also set to "Serveur AD GSB".
- Shell Authentication:** A checkbox labeled "Use Authentication Server for Shell Authentication" is checked. A note below it says: "If RADIUS or LDAP server is selected it is used for console and SSH authentication. Otherwise, the Local Database is used. To allow logins with RADIUS credentials, equivalent local users with the expected privileges must be created first. To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP server configuration page."
- Auth Refresh Time:** A dropdown menu set to "30". A note below it states: "Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hour). Shorter times result in more frequent queries to authentication servers."

At the bottom of the page are two buttons: "Save" and "Save & Test".

En cliquant sur *Save & Test*, on devrait constater le succès complet du test :

The screenshot shows the results of an LDAP connection test. It displays three rows of status information:

Attempting connection to	192.168.3.1	OK
Attempting bind to	192.168.3.1	OK
Attempting to fetch Organizational Units from	192.168.3.1	OK

Below the test results, a section titled "Organization units found" shows the result: "CN=Users,DC=GSB,DC=local".

- d. Configurer une nouvelle connexion VPN, de type *Remote Access (User Auth)* avec la commande VPN OpenVPN, dans l'onglet Wizards :

Type of Server :	<i>LDAP</i>
LDAP Servers :	<i>Serveur AD GSB</i>
Certificate Authority :	<i>CA_Access_VPN</i>
Certificate :	<i>Certificat_Acces_VPN</i>
Description :	<i>Serveur VPN avec authentification LDAP GSB</i>
Local Port :	<i>1195</i>

Wizard / OpenVPN Remote Access Server Setup / Server Setup

Step 9 of 11

Server Setup

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Interface	WAN	The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol	UDP on IPv4 only	Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.
Local Port	1195	Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.
Description	Serveur VPN avec authentification LDAP GSB	A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

Cryptographic Settings	
TLS Authentication	<input checked="" type="checkbox"/> Enable authentication of TLS packets.
Generate TLS Key	<input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key.
TLS Shared Key	<input type="text"/> Paste in a shared TLS key if one has already been generated.
DH Parameters Length	2048 bit
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.	
Data Encryption Negotiation	<input checked="" type="checkbox"/> Enable negotiation of Data Encryption Algorithms between client and server. The best practice is keep this setting enabled.
Data Encryption Algorithms	AES-256-GCM AES-128-GCM CHACHA20-POLY1305
List of algorithms clients can negotiate to encrypt traffic between endpoints. The best practice is to use the exact algorithms listed above, in that order. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips. Edit the server after finishing the wizard for additional choices.	
Fallback Data Encryption Algorithm	AES-256-CBC (256 bit key, 128 bit block)
The algorithm used to encrypt traffic between endpoints when data encryption negotiation is disabled or fails.	
Auth Digest Algorithm	SHA256 (256-bit)
The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.	
Hardware Crypto	No Hardware Crypto Acceleration
The hardware cryptographic accelerator to use for this VPN connection, if any.	

Tunnel Settings	
Tunnel Network	<input type="text" value="192.168.100.0/24"/>
<p>This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.</p>	
Redirect Gateway	<input type="checkbox"/>
<p>Force all client generated traffic through the tunnel.</p>	
Local Network	<input type="text" value="192.168.3.0/24"/>
<p>This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</p>	
Concurrent Connections	<input type="text"/>
<p>Specify the maximum number of clients allowed to concurrently connect to this server.</p>	
Allow Compression	<input type="button" value="Refuse any non-stub compression (Most secure)"/>
<p>Allow compression to be used with this VPN instance, which is potentially insecure.</p>	
Compression	<input type="button" value="Disable Compression [Omit Preference]"/>
<p>Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.</p>	
Type-of-Service	<input type="checkbox"/>
<p>Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.</p>	
Inter-Client Communication	<input type="checkbox"/>
<p>Allow communication between clients connected to this server.</p>	
Duplicate Connections	<input type="checkbox"/>
<p>Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.</p>	

Client Settings

Dynamic IP	<input checked="" type="checkbox"/>	Allow connected clients to retain their connections if their IP address changes.
Topology	Subnet -- One IP address per client in a common subnet <input type="button" value="▼"/>	
Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".		
DNS Default Domain	GSB.local	
Provide a default domain name to clients.		
DNS Server 1	192.168.3.1	
DNS server IP to provide to connecting clients.		
DNS Server 2		
DNS server IP to provide to connecting clients.		
NTP Server		
Network Time Protocol server to provide to connecting clients.		
NetBIOS Options	<input type="checkbox"/>	Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
NetBIOS Node Type	none <input type="button" value="▼"/>	
Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).		
NetBIOS Scope ID		
A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.		
WINS Server 1		
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.		
WINS Server 2		
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.		

Firewall Rule Configuration

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule	<input checked="" type="checkbox"/>	Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.
----------------------	-------------------------------------	--

Traffic from clients through VPN

OpenVPN rule	<input checked="" type="checkbox"/>	Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.
---------------------	-------------------------------------	---

Le fait d'avoir coché les cases *Firewall Rule* et *OpenVPN rule* a automatiquement ajouté des règles de filtrage.

- a. Vérifier avec la commande *Firewall Rules* que ces règles ont bien été créées.
- b. Vérifier avec la commande *Diagnostics Authentication*, que l'utilisateur *anevers* est authentifié par *Serveur AD GSB* :

Diagnostics / Authentication

User *anevers* authenticated successfully. This user is a member of groups:

Authentication Test

<u>Authentication Server</u>	<input type="text" value="Serveur AD GSB"/> <input type="button" value="▼"/>
Select the authentication server to test against.	
<u>Username</u>	<input type="text" value="anevers"/>
<u>Password</u>	<input type="password" value="••••••••••••"/>
<input type="button" value="🔧 Test"/>	

Les règles de filtrage qui ont été créées par l'assistant sont les suivantes :

- sur l'interface **OpenVPN** (crée pour la connexion VPN) :

Rules (Drag to Change Order)											Actions
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	IPv4	*	*	*	*	*	none		OpenVPN Serveur VPN avec authentificat wizard	  
											 Add  Add  Delete  Save 

- sur l'interface **WAN** :

Rules (Drag to Change Order)											Actions
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	IPv4 UDP	*	*	WAN address	1195	*	none		OpenVPN Serveur VPN avec authentificat wizard	  

Remarque :

Dans les paramètres cryptographiques, vous avez vu qu'une clé TLS supplémentaire est générée pour renforcer la sécurité d'une connexion OpenVPN en exigeant que les deux parties disposent d'une clé commune avant qu'un pair puisse effectuer un handshake TLS.

Cette clé symétrique n'est utilisée que pour signer les paquets du canal de contrôle avec une signature HMAC pour l'authentification lors de l'établissement du tunnel.

Elle n'a aucun effet sur les données du tunnel.

Attention !

Dans certaines versions de Pfsense, il y a un bug qui ne permet pas d'utiliser plusieurs connexions VPN simultanément.

Si une connexion VPN a déjà été configurée dans un autre TP (dans le TP 28, une connexion VPN utilisant le serveur d'authentification local Pfsense sur le port 1194 a été configurée), il faut la désactiver.

Si tel est le cas :

- e. Sélectionner la commande VPN OpenVPN Servers, puis modifier la connexion VPN utilisant le serveur d'authentification local Pfsense sur le port 1194 ; cocher la case *Désactivée* :

The screenshot shows two parts of the Pfsense configuration interface:

Left Panel (List View):

VPN / OpenVPN / Serveurs

Serveurs Clients Ré-écritures spécifiques au client Assistants Client Export Shared Key Export

Serveurs OpenVPN

Interface	Protocole / Port	Réseau tunnel	Chiffrement	Description	Actions
WAN	UDP / 1194	192.168.100.0/24	Crypto: AES-256-CBC/SHA256 D-H Params: 2048 bits	Serveur VPN local (tun)	
WAN	UDP / 1195	192.168.100.0/24	Crypto: AES-256-CBC/SHA256 D-H Params: 2048 bits	Serveur VPN avec aut LDAP GSB (tun)	

Right Panel (Edit View):

VPN / OpenVPN / Serveurs / Modifier

Serveurs Clients Ré-écritures spécifiques au client Assistants Client

Informations Générales

Désactivé Désactiver ce serveur
Définissez cette option pour désactiver ce serveur sans le supprimer.

Mode serveur Accès à distance (SSL/TLS + Authentification utilisateur)

Backend pour l'authentification Serveur AD GSB
Base de données locale

Seule la connexion VPN que l'on veut utiliser (ici celle utilisant le serveur d'authentification LDAP SERVEUR1 sur le port 1195) doit être active.

Nous allons configurer le PfSense pour qu'il accède à Internet, de façon à pouvoir installer un nouveau package qui nous permettra d'exporter vers les ordinateurs clients le fichier de configuration et le certificat-client.

- Sélectionner la commande System General Setup, afin de configurer l'adresse du DNS :

DNS Server : 192.168.216.74

Cliquer sur *Save* pour enregistrer la configuration. **Redémarrer** ensuite le PfSense.

The screenshot shows the 'DNS Server Settings' page. On the left, there's a section for 'DNS Servers' with a text input field containing '192.168.216.74'. To the right of the input field is a 'DNS Hostname' label with a corresponding empty input field. Below these fields is a detailed description of what the DNS servers are used for: they are used for DNS resolution by the system, and also for DHCP service, DNS Forwarder and DNS Resolver when DNS Query Forwarding is enabled. At the bottom left is a 'Add DNS Server' button, and at the bottom center is a green 'Add DNS Server' button with a plus sign.

Le package *OpenVPN Client Export Utility* permet d'exporter facilement la configuration qui devra être installée sur l'ordinateur client. Nous allons donc déjà installer ce package sur le PfSense serveur :

- Installer le package *OpenVPN Client Export Utility* :

Sélectionner la commande System Packages, puis cliquer sur l'onglet *Available Packages*.

Sur la ligne *OpenVPN Client Export Utility*, cliquer sur le signe + pour ajouter le package.

Après l'installation, cliquer sur l'onglet *Installed Packages* pour vérifier que le module a bien été installé.

- Sélectionner la commande VPN OpenVPN, dans l'onglet Client Export, pour le type d'utilisateur *Authentication Only (No Cert)*, afin de vérifier la présence de l'archive (contenant les trois fichiers de configuration), ou mieux encore, de l'exécutable *Windows Installer*, qui est à exporter sur les machines clientes (attention : sélectionner le bon serveur dans la zone *Remote Access Server*) :

OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards Client Export Shared Key Export

OpenVPN Server

Remote Access Server Serveur VPN avec authentificat UDP4:1195

OpenVPN Clients

User	Certificate Name	Export
Authentication Only (No Cert)	none	<ul style="list-style-type: none">- Inline Configurations: Most Clients AndroidOpenVPN Connect (iOS/Android)- Bundled Configurations: Archive Config File Only- Current Windows Installer (2.5.2-lx01): 64-bit 32-bit- Legacy Windows Installers (2.4.11-lx01): 10/2016/2019 7/8/8.1/2012r2- Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config

- d. Cliquer sur le lien *64-bits* dans la rubrique *Current Windows Installer* pour exporter un fichier exécutable qui installera automatiquement les fichiers de configuration, ou sur le lien *Archive* pour exporter les trois fichiers de configuration eux-mêmes ; il faut les enregistrer dans un endroit accessible aux postes clients (sur le serveur 192.168.216.74 par exemple, ou sur une clé USB).

Remarque : Le fichier .ovpn contient la configuration à installer sur chaque poste client OpenVPN. Le fichier .key contient la clé TLS supplémentaire. Le fichier .crt contient le certificat de l'autorité de certification CA_Access_VPN.

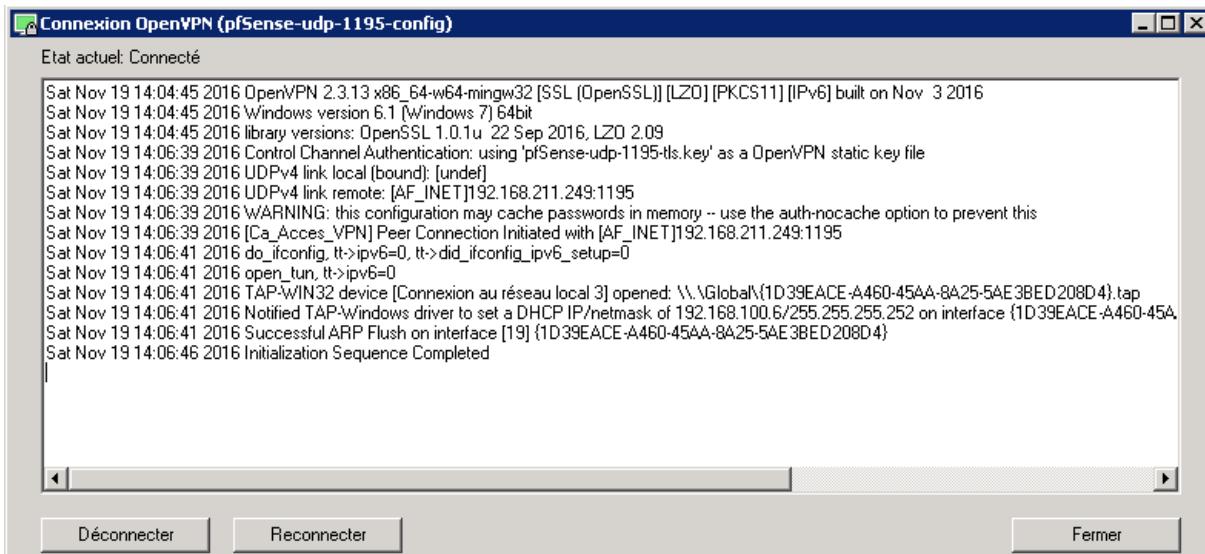
Nom	Modifié le	Type	Taille
pfSense-udp-1195.ovpn	19/11/2016 13:41	Fichier OVPN	1 Ko
pfSense-udp-1195-ca.crt	19/11/2016 13:41	Certificat de sécurité	2 Ko
pfSense-udp-1195-tls.key	19/11/2016 13:41	Fichier KEY	1 Ko

- a. Sur le poste client, télécharger le client OpenVPN depuis le site suivant (onglet *Community*, *Windows Installer 64 bits*) :

<http://openvpn.net/index.php/open-source/downloads.html>

- b. Installer ce logiciel client sur le poste (installer aussi le logiciel *TAP-Windows Provider V9 Cartes réseau*).
- c. Recopier le fichier d'installation exécutable dans le dossier C:\Programmes\OpenVPN\Config (si la copie directe ne fonctionne pas, on pourra copier le fichier d'abord dans le dossier Documents du PC local, puis du dossier Documents vers C:\Programmes\OpenVPN\Config) puis exécuter ce fichier qui installera automatiquement les 3 fichiers de configuration dans le dossier.
- d. Cliquer-droit sur l'icône de l'application OpenVPN GUI et sélectionner la commande *Régler les problèmes de compatibilité*, puis le bouton *Essayer les paramètres recommandés* ; lancer ainsi l'application.
- e. L'application OpenVPN GUI devra ensuite toujours être lancée en mode administrateur.
- f. Se connecter avec l'utilisateur *anevers* et le mot de passe *Windows2019* :



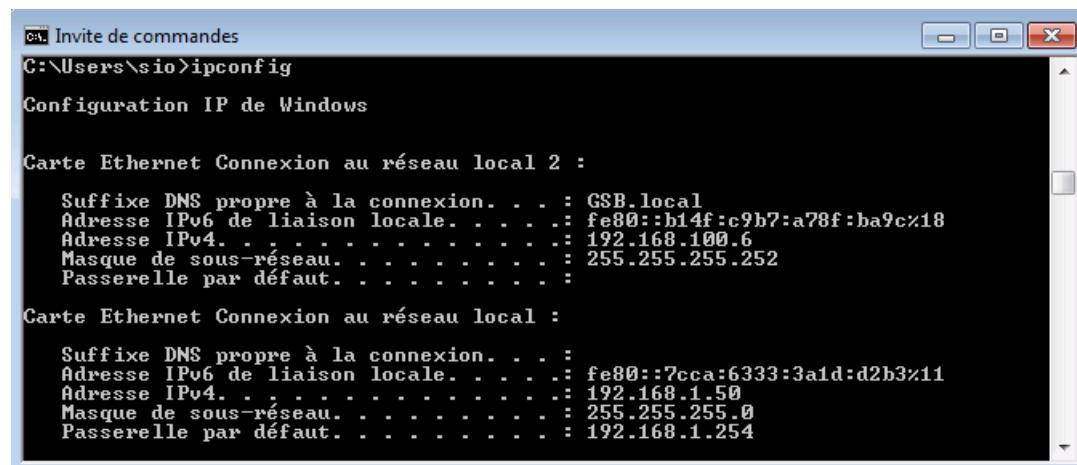


Pour info, le fichier de configuration du client OpenVPN,
de nom *pfSense-udp-1195-config.ovpn*
doit avoir le contenu suivant :

The screenshot shows a Windows Notepad window titled "pfSense-udp-1195-config - Bloc-notes". The content of the file is as follows:

```
dev tun
persist-tun
persist-key
cipher AES-256-CBC
auth SHA256
tls-client
client
resolv-retry infinite
remote 192.168.211.249 1195 udp
lport 0
auth-user-pass
ca pfSense-udp-1195-ca.crt
tls-auth pfSense-udp-1195-tls.key 1
ns-cert-type server
```

g. Vérifier que le poste client a bien deux connexions en cours :



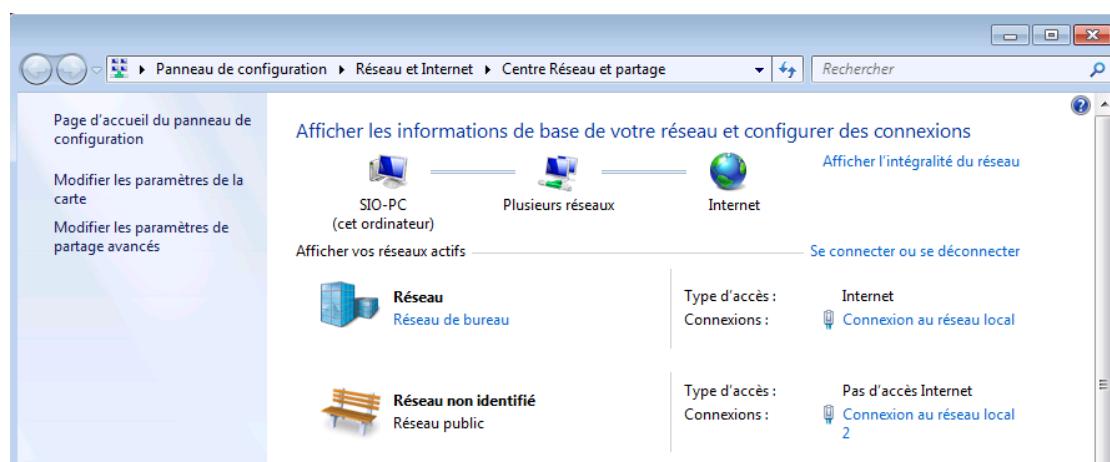
```
C:\ Invité de commandes
C:\Users\sio>ipconfig
Configuration IP de Windows

Carte Ethernet Connexion au réseau local 2 :

Suffrage DNS propre à la connexion . . . . . : GSB.local
Adresse IPv6 de liaison locale . . . . . : fe80::b14f:c9b7:a78f:ba9c%18
Adresse IPv4 . . . . . : 192.168.100.6
Masque de sous-réseau . . . . . : 255.255.255.252
Passerelle par défaut . . . . . :

Carte Ethernet Connexion au réseau local :

Suffrage DNS propre à la connexion . . . . . :
Adresse IPv6 de liaison locale . . . . . : fe80::7cca:6333:3aid:d2b3%11
Adresse IPv4 . . . . . : 192.168.1.50
Masque de sous-réseau . . . . . : 255.255.255.0
Passerelle par défaut . . . . . : 192.168.1.254
```



```
C:\ Invite de commandes
C:\Users\sio>ipconfig /all
Configuration IP de Windows

    Nom de l'hôte . . . . . : sio-PC
    Suffixe DNS principal . . . . . : GSB.local
    Type de noeud . . . . . : Hybride
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non
    Liste de recherche du suffixe DNS . . . . . : GSB.local

Carte Ethernet Connexion au réseau local 2 :

    Suffixe DNS propre à la connexion . . . . . : GSB.local
    Description . . . . . : TAP-Windows Adapter V9
    Adresse physique . . . . . : 00-FF-74-03-5A-EB
    DHCP activé . . . . . : Oui
    Configuration automatique activée . . . . . : Oui
    Adresse IPv6 de liaison locale . . . . . : fe80::b14f:c9b7:a78f:ba9c%18<préféré
    >
        Adresse IPv4 . . . . . : 192.168.100.6<préféré>
        Masque de sous-réseau . . . . . : 255.255.255.252
        Bail obtenu . . . . . : lundi 29 juin 2015 07:49:29
        Bail expirant . . . . . : mardi 28 juin 2016 07:49:28
        Passerelle par défaut . . . . . :
        Serveur DHCP . . . . . : 192.168.100.5
        IAID DHCPv6 . . . . . : 302055284
        DUID de client DHCPv6 . . . . . : 00-01-00-01-19-D5-E4-30-00-50-56-8B-29
-EC
    Serveurs DNS . . . . . : 192.168.3.1
    NetBIOS sur Tcpip . . . . . : Activé

Carte Ethernet Connexion au réseau local 1 :

    Suffixe DNS propre à la connexion . . . . . : Connexion réseau Intel(R) PRO/1000 MT
    Description . . . . . : Connexion réseau Intel(R) PRO/1000 MT
    Adresse physique . . . . . : 00-50-56-8B-7E-86
    DHCP activé . . . . . : Non
    Configuration automatique activée . . . . . : Oui
    Adresse IPv6 de liaison locale . . . . . : fe80::7cca:6333:3aid:d2b3%11<préféré
    >
        Adresse IPv4 . . . . . : 192.168.1.50<préféré>
        Masque de sous-réseau . . . . . : 255.255.255.0
        Passerelle par défaut . . . . . : 192.168.1.254
        IAID DHCPv6 . . . . . : 234901590
        DUID de client DHCPv6 . . . . . : 00-01-00-01-19-D5-E4-30-00-50-56-8B-29
-EC
    Serveurs DNS . . . . . : 192.168.216.74
    NetBIOS sur Tcpip . . . . . : Activé
```

- h. Vérifier sur le serveur OpenVPN avec la commande Diagnostic OpenVPN, les connexions des clients en cours :

Status: OpenVPN



Serveur VPN avec aut LDAP GSB UDP:1195 Client connections					
Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received
anevers	192.168.1.50:56769	192.168.100.6	Sat Nov 19 12:59:28 2016	6 KB	6 KB
Running					
Serveur VPN avec aut LDAP GSB UDP:1195 Routing Table					
Common Name	Real Address	Target Network	Last Used		
anevers	192.168.1.50:56769	192.168.100.6	Sat Nov 19 13:00:02 2016		
An IP address followed by C indicates a host currently connected through the VPN.					

- i. Vérifier que le serveur OpenVPN lui-même a bien aussi une connexion ovpns1 d'adresse 192.168.100.1 :

Aucune route n'a été rajoutée pour ce réseau 192.168.100.0 dans le routeur puisqu'il s'agit d'une adresse "fictive".

pfSense.localdomain - Diagnostics: Execute command - Windows Internet Explorer

http://192.168.2.253/exec.php

Execute Shell command

```
$ ifconfig
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:8b:7e:76
        inet 192.168.1.253 netmask 0xffffffff broadcast 192.168.1.255
        inet6 fe80::250:56ff:fe8b:7e76%em0 prefixlen 64 scopeid 0x1
        nd6 options=1<PERFORMNUD>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
em1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:8b:7e:77
        inet6 fe80::250:56ff:fe8b:7e77%em1 prefixlen 64 scopeid 0x2
        inet 192.168.2.253 netmask 0xffffffff broadcast 192.168.2.255
        nd6 options=1<PERFORMNUD>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
plip0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> metric 0 mtu 1500
enc0: flags=0<> metric 0 mtu 1536
pflog0: flags=100<PROMISC> metric 0 mtu 33144
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=3<RXCSUM,TXCSUM>
        inet 127.0.0.1 netmask 0xffffffff
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
pfsync0: flags=0<> metric 0 mtu 1460
        syncpeers: 224.0.0.240 maxupd: 128 syncok: 1
ovpns1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu 1500
        options=80000<LINKSTATE>
        inet6 fe80::250:56ff:fe8b:7e76%ovpns1 prefixlen 64 scopeid 0x8
        inet 192.168.100.1 --> 192.168.100.2 netmask 0xffffffff
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
Opened by PID 89609
```

Mission 6 : Cluster PfSense :

Doc mission 6

- Faire une sauvegarde du PfSense unique (pfSense backup)



- Dupliquer le pfSense existant (qui devient pfSense secondaire)

Projet MDL (Examen)

pfSense backup

Pfsense MDL Maître

pfSense secondaire

- Pour être efficace, il faut pouvoir travailler avec les 2 PfSense à l'écran simultanément

- On va maintenant changer les adresses IP des deux pfSenses :

PfSense maître :

LAN : 172.16.2.252
WAN : 192.168.211.220
OPT1 : 10.10.1.252
OPT2 : 192.168.60.1/30

PfSense secondaire :

LAN : 172.16.2.253
WAN : 192.168.211.221
OPT1 : 10.10.1.253
OPT2 : 192.168.60.2/30

- On va maintenant se rendre sur les 2 interfaces graphiques de pfSense dans firewall et ip virtuals

pfSense.home.arpa - Firewall: [V](#) [X](#) +

172.16.2.252/firewall_virtual_ip_edit.php

Type	<input type="radio"/> IP Alias	<input checked="" type="radio"/> CARP	<input type="radio"/> Proxy	<input type="radio"/> Other
Interface	LAN			
Address type	Single address			
Address(es)	172.16.2.254		/	24
The mask must be the network's subnet mask. It does not specify a CIDR range.				
Virtual IP	*****		*****	
Password	Enter the VHID group password.		Confirm	
VHID Group	2			
Enter the VHID group that the machines will share.				
Advertising frequency	1	0	Base Skew	
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.				
Description	A description may be entered here for administrative reference (not parsed).			

pfSense.home.arp - Firewall: Virtual IP

172.16.2.253/firewall_virtual_ip_edit.php

Edit Virtual IP

Type: CARP IP Alias Proxy ARP Other

Interface: LAN

Address type: Single address

Address(es): 172.16.2.254 / 24
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP:
Password: Enter the VHID group password. Confirm

VHID Group: 2
Enter the VHID group that the machines will share.

Advertising frequency: 1 (Base) 100 (Skew)
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description: A description may be entered here for administrative reference (not parsed).

Save

Pour le wan

pfSense.home.arpa - Firewall: V X +

172.16.2.253/firewall_virtual_ip_edit.php

Edit Virtual IP

Type CARP IP Alias Proxy ARP Other

Interface **WAN**

Address type **Single address**

Address(es) **192.168.211.150 / 24**
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP *********

Password **Enter the VHID group password.** Confirm

VHID Group **1**
Enter the VHID group that the machines will share.

Advertising frequency **1** Base **100** Skew
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description
A description may be entered here for administrative reference (not parsed).

Save

i

Activer Windows
Accédez aux paramètres pour activer Windows.

The screenshot shows the 'Edit Virtual IP' configuration page in a web browser. The 'Type' section has 'CARP' selected. The 'Interface' is 'WAN'. The 'Address type' is 'Single address' with the address '192.168.211.150 / 24'. Below it, a note says 'The mask must be the network's subnet mask. It does not specify a CIDR range.' The 'Virtual IP' field contains '*****'. There are two password fields: 'Password' (containing 'Enter the VHID group password.') and 'Confirm'. The 'VHID Group' dropdown is set to '1'. A note below it says 'Enter the VHID group that the machines will share.' Under 'Advertising frequency', there are two dropdowns: 'Base' set to '1' and 'Skew' set to '100'. A note below says 'The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.' The 'Description' field is empty. At the bottom, there is a blue 'Save' button and a small information icon. To the right of the 'Save' button, there is a link to 'Activer Windows' with the sub-instruction 'Accédez aux paramètres pour activer Windows.'

pfSense.home.arpa - Firewall: [V](#) X +

Edit Virtual IP

Type IP Alias CARP Proxy ARP Other

Interface **WAN**

Address type **Single address**

Address(es) **192.168.211.150 / 24**
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP *********

Password **Enter the VHID group password.** Confirm

VHID Group **1**
Enter the VHID group that the machines will share.

Advertising frequency **1** Base **0** Skew
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description
A description may be entered here for administrative reference (not parsed).

Save

i

This screenshot shows the 'Edit Virtual IP' configuration page for pfSense. The 'CARP' type is selected. The interface is set to 'WAN'. The address is '192.168.211.150' with a subnet mask of '24'. A note states that the mask must be the network's subnet mask. The virtual IP is masked out as '*****'. The VHID group is set to '1'. The advertising frequency is '1' for 'Base' and '0' for 'Skew'. A description field is empty. A 'Save' button is at the bottom.

Pour opt1

pfSense.home.arpa - Firewall: Virtual IP

172.16.2.252/firewall_virtual_ip_edit.php

Edit Virtual IP

Type: CARP IP Alias Proxy ARP Other

Interface: OPT1

Address type: Single address

Address(es): 10.10.1.254 / 24
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP:
Password: Enter the VHID group password. Confirm

VHID Group: 3
Enter the VHID group that the machines will share.

Advertising frequency: 1 Base 0 Skew
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description: A description may be entered here for administrative reference (not parsed).

 Save

pfSense.home.arpa - Firewall: V X +

172.16.2.253/firewall_virtual_ip_edit.php

Edit Virtual IP

Type	<input type="radio"/> IP Alias	<input checked="" type="radio"/> CARP	<input type="radio"/> Proxy ARP	<input type="radio"/> Other
Interface	OPT1			
Address type	Single address			
Address(es)	10.10.1.254 / 24			
The mask must be the network's subnet mask. It does not specify a CIDR range.				
Virtual IP	*****		*****	
Password	Enter the VHID group password. Confirm			
VHID Group	3			
Enter the VHID group that the machines will share.				
Advertising frequency	1 Base	100 Skew	The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.	
Description				
A description may be entered here for administrative reference (not parsed).				
<input type="button" value="Save"/> Activer Windows Accédez aux paramètres pour activer Windows.				

On doit donc se retrouver avec ces adresses IP virtuelles :

Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
172.16.2.254/24 (vhid: 2)	LAN	CARP		
192.168.211.150/24 (vhid: 1)	WAN	CARP		
10.10.1.254/24 (vhid: 3)	OPT1	CARP		

- On va maintenant effectuer la synchronisation entre les Pfsenses

State Synchronization Settings (pfsync)

Synchronize states	<input checked="" type="checkbox"/> pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
---------------------------	---

Synchronize Interface	OPT2
	If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.
pfsync Synchronize Peer IP	192.168.60.2

pfsync Synchronize Peer IP	192.168.60.2
	Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP	192.168.60.2
	Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

Remote System Username	<input type="text" value="admin"/>	Enter the webConfigurator username of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and username option on backup cluster members!
Remote System Password	<input type="password" value="*****"/>	<input type="password" value="*****"/> Confirm Enter the webConfigurator password of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and password option on backup cluster members!
Synchronize admin	<input type="checkbox"/> synchronize admin accounts and autoupdate sync password. By default, the admin account does not synchronize, and each node may have a different admin password. This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.	
Select options to sync	<input checked="" type="checkbox"/> User manager users and groups <input checked="" type="checkbox"/> Authentication servers (e.g. LDAP, RADIUS) <input checked="" type="checkbox"/> Certificate Authorities, Certificates, and Certificate Revocation Lists <input checked="" type="checkbox"/> Firewall rules <input checked="" type="checkbox"/> Firewall schedules <input checked="" type="checkbox"/> Firewall aliases <input checked="" type="checkbox"/> NAT configuration <input checked="" type="checkbox"/> IPsec configuration <input checked="" type="checkbox"/> OpenVPN configuration (Implies CA/Cert/CRL Sync) <input checked="" type="checkbox"/> DHCP Server settings <input checked="" type="checkbox"/> WoL Server settings <input checked="" type="checkbox"/> Static Route configuration <input checked="" type="checkbox"/> Virtual IPs	

Pour pfsnese secondaire

State Synchronization Settings (pfsync)

Synchronize states	<input checked="" type="checkbox"/> pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
---------------------------	---

Synchronize Interface	WAN
	If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.

pfsync Synchronize Peer IP	192.168.60.1
	Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP	192.168.60.1
	Enter the IP address of the firewall to which the selected configuration sections should be

as this system - make sure the remote system's port and protocol are set accordingly!
Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username	<input type="text" value="admin"/>	Enter the webConfigurator username of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and username option on backup cluster members!	
Remote System Password	<input type="password" value="*****"/>	<input type="password" value="*****"/>	Confirm Enter the webConfigurator password of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and password option on backup cluster members!
Synchronize admin	<input type="checkbox"/> synchronize admin accounts and autoupdate sync password. By default, the admin account does not synchronize, and each node may have a different admin password. This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.		
Select options to sync	<input checked="" type="checkbox"/> User manager users and groups <input checked="" type="checkbox"/> Authentication servers (e.g. LDAP, RADIUS) <input checked="" type="checkbox"/> Certificate Authorities, Certificates, and Certificate Revocation Lists <input checked="" type="checkbox"/> Firewall rules <input checked="" type="checkbox"/> Firewall schedules <input checked="" type="checkbox"/> Firewall aliases <input checked="" type="checkbox"/> NAT configuration <input checked="" type="checkbox"/> IPsec configuration <input checked="" type="checkbox"/> OpenVPN configuration (Implies CA/Cert/CRL Sync) Activer Windows Accédez aux paramètres pour activer Window <input checked="" type="checkbox"/> DHCP Server settings <input checked="" type="checkbox"/> WoL Server settings		

- On va maintenant créer une règle de filtrage sur l'interface OPT2 car par défaut tout est interdit, on a juste à aller dans firewall et rules et ajouter une règle pour l'interface OPT2 (pfsynch), dès que la règle est créée on a juste à save car les paramètre par défaut autorise tout.

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP	*	*	*	*	*	none			 

- On peut voir que maintenant on a accès à pfSense avec l'adresse IP virtuelle 192.168.211.150

Bureau à distance

Configuration d'un serveur hôte de session bureau à distance sur SERVEUR1

Attention : pour toutes les manipulations suivantes, il faut avoir ouvert une session Administrateur du domaine (GSB) sur le serveur concerné (SERVEUR1) (et non Administrateur local du poste) !

- a. Ouvrir le Gestionnaire de serveur (s'il n'est pas déjà ouvert) en cliquant sur le bouton  de la barre des tâches actives.
- b. Dans ce tableau de bord, sélectionner Gérer, puis le lien Ajouter des rôles et fonctionnalités.
- c. Dans la fenêtre *Assistant Ajout des rôles*, choisir le type d'installation *Installation des services Bureau à distance*, puis le type de déploiement *Démarrage rapide* et le scénario de déploiement *Déploiement de bureaux basés sur une session*.
- d. Choisir le serveur SERVEUR1 parmi le pool de serveurs sur lequel seront installés les services.
- e. Cocher la case *Redémarrer automatiquement le serveur de destination si nécessaire* puis cliquer sur *Déployer*.
- f. Laisser l'installation se faire et la machine redémarrer.

Remarque :

Si le message d'erreur suivant apparaît : *La communication à distance Powershell ne permet pas la connexion avec le serveur (Unable to connect to the server by using Windows PowerShell remoting)*, il faut lancer les deux commandes suivantes sous PowerShell en tant qu'Administrateur pour activer la gestion à distance et déployer RDS :

```
Get-service WinRM  
Enable-PSRemoting
```

puis redémarrer la machine si nécessaire.

Voir aussi : <https://hichamkadiri.wordpress.com/2015/03/15/how-to-fix-unable-to-connect-to-the-server-by-using-windows-powershell-remoting-rds-sur-microsoft-azure/>
<https://blog.adsl2meg.fr/administration-a-distance-dun-serveur-windows-server-2012-par-le-gestionnaire-de-serveur/>

Chaque utilisateur ou périphérique informatique qui se connecte à un serveur hôte de session Bureau à distance doit obtenir une licence d'accès client aux services Bureau à distance auprès d'un serveur de licences des services Bureau à distance (obligatoire depuis Windows 2008 R2).

Sur le serveur hôte de session bureau à distance, il faut donc spécifier le serveur de licences qui sera utilisé : ce sera le même SERVEUR1 dans notre cas

- g. Dans le Gestionnaire de serveur, sélectionner Gérer, puis le lien Ajouter des rôles et fonctionnalités.

Après avoir installé les rôles, il faut maintenant effectuer la configuration proprement dite des services Bureau à distance.

- n. Dans le Gestionnaire de serveur, sélectionner Services Bureau à distance.

Avec Windows Server, nous pouvons diffuser des applications qui peuvent être utilisées par des machines clientes. C'est le système «RemoteApp». Cette solution est incluse au service de Bureau à distance et permet de faire tourner des applications lourdes sur le serveur depuis des ordinateurs clients.

Les applications tournent sur le serveur et le client reçoit en réalité un «stream» de l'application. Ceci permet d'économiser de l'argent dans une entreprise en achetant un gros serveur et des clients légers pour les employés.

Les services Bureau à distance sont configurés au travers des collections. Une collection permet de déclarer des applications "Remote App" pour un serveur, et de définir les utilisateurs qui pourront les exécuter.

Une collection est déjà créée par défaut : *QuickSessionCollection* ; elle permet de déclarer les 3 applications Calculatrice, Paint, et WordPad comme applications RemoteApp exécutables sur SERVEUR1 et accessibles à tous les utilisateurs du domaine.

Nous allons soit créer une nouvelle collection, soit modifier la collection existante *QuickSessionCollection* pour permettre de déclarer l'application *Cisco Packet Tracer* comme application RemoteApp exécutable sur SERVEUR1 et accessible à tous les utilisateurs du domaine.

- o. Installer Packet Tracer sur le serveur SERVEUR1 (et non sur la station !).
- p. Dans le Gestionnaire de serveur de SERVEUR1, sélectionner Services Bureau à distance, puis depuis la vue *Collections*, cliquer sur le lien *QuickSessionCollection* pour modifier cette collection existante :
- le serveur hôte sur lequel doit s'exécuter l'application est SERVEUR1 (rubrique *Serveurs hôtes*)
 - les utilisateurs autorisés à exécuter cette application sont GSB\Utilisateurs du domaine (rubrique *Propriétés*)
 - l'application Cisco Packet Tracer doit être ajoutée à la liste *Programmes RemoteApp* (cliquer sur le bouton *TÂCHES* de la zone *PROGRAMMES REMOTEAPP*, puis sélectionner *Publier des programmes RemoteApp* ; dans la liste des programmes, sélectionner *Cisco Packet Tracer* puis cliquer sur *Publier*) :

Gestionnaire de serveur ▶ Services Bureau à distance ▶ Collections ▶ QuickSessionCollection

PROPRIÉTÉS
Propriétés de la collection

Type de collection	Session
Ressources	Programmes RemoteApp
Groupe d'utilisateurs	GSB\Utilisateurs du domaine

PROGRAMMES REMOTEAPP
Dernière actualisation le 08/12/2017 12:38:18 | Programmes RemoteApp publiés | 3 au total

Nom du programme RemoteApp	Alias	Visible dans l'Accès Web des services Bureau à distance
Calculatrice	Calculatrice	Oui
Paint	Paint	Oui
WordPad	WordPad	Oui
Cisco Packet Tracer	Packet Tr	Oui

SERVEURS HÔTES
Dernière actualisation le 08/12/2017 12:38:18 | Tous les serveurs | 1 au total

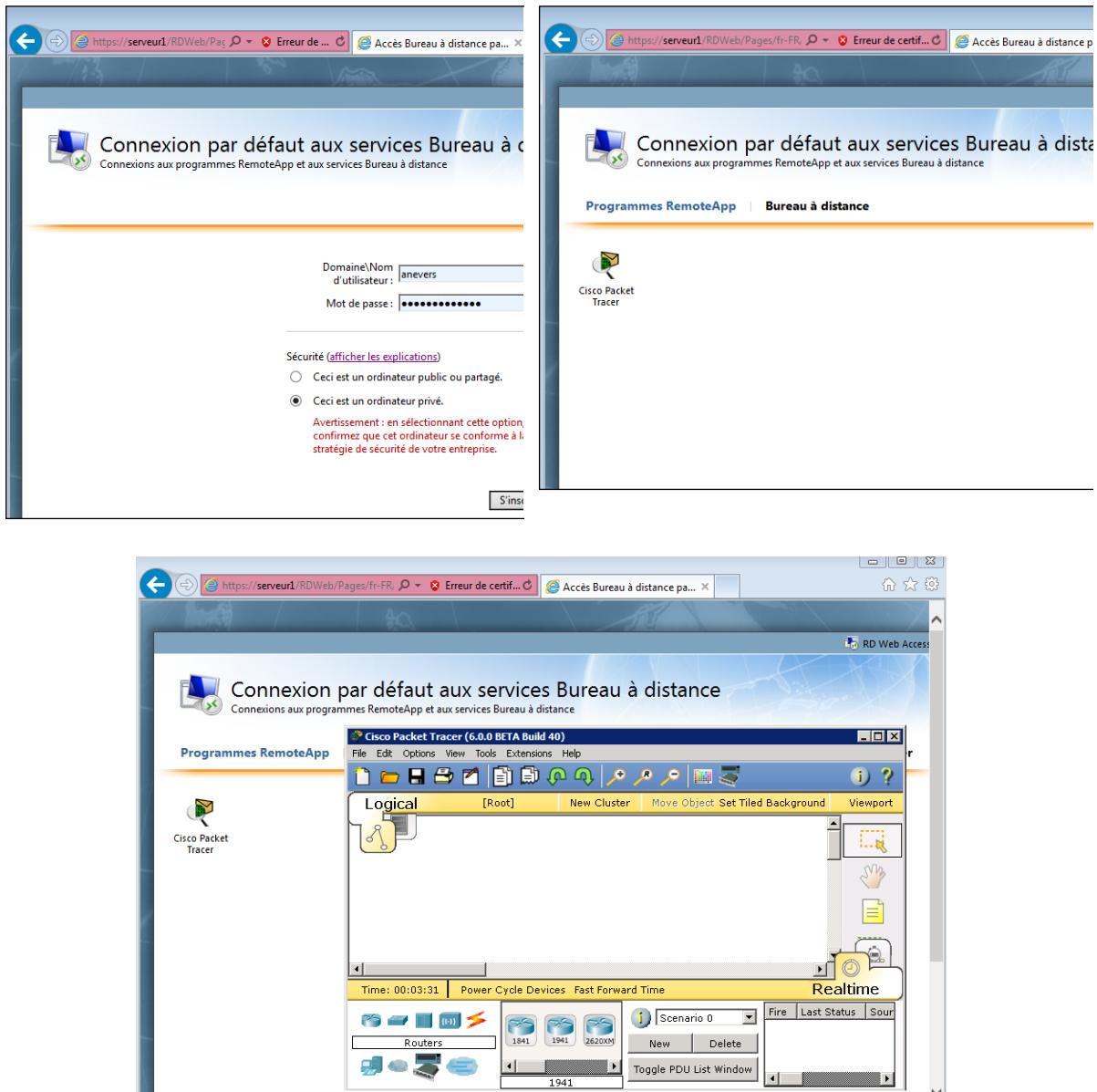
Nom du serveur	Type	Bureaux virtuels	Autoriser les nouvelles collections
SERVEUR1	Hôte de session Bureau à distance	N/A	Vrai

Ouverture d'une application RemoteApp (à distance) depuis PC1

Le service de rôle *Accès Bureau à distance par le Web*, installé sur SERVEUR1, permet aux utilisateurs d'accéder aux programmes RemoteApp et aux services Bureau à distance via un navigateur Web. En effet, depuis Windows 2012, tous les utilisateurs désirant exécuter des applications RemoteApp doivent passer par le navigateur de leur poste, et se connecter au serveur hébergeant le service Broker (SERVEUR1) qui héberge aussi le service Accès Web.

Nous allons maintenant tester l'*Accès Bureau à distance par le Web* :

- a. Démarrer la machine PC1 et ouvrir une session Windows avec l'utilisateur *anevers* et le mot de passe *Windows2016*
- a. Avec le navigateur Internet, ouvrir la page <https://SERVEUR1/rdweb> ou <https://SERVEUR1.GSB.local/rdweb> ; après s'être authentifié (*GSB\anevers / Windows2016*), dans la liste des programmes RemoteApp proposés, cliquer sur Packet Tracer : le programme se lance dans une nouvelle fenêtre !



On peut surveiller les connexions bureau à distance ouvertes sur le serveur SERVEUR1 :

- b. Sur SERVEUR1, vérifier les connexions bureau à distance ouvertes: dans le Gestionnaire de serveur de SERVEUR1, sélectionner Services Bureau à distance, puis cliquer sur le nom de la collection à surveiller (exemple : *QuickSessionCollection*) : on constate que *anevers* a bien une session active en cours.

The screenshot shows the 'Services Bureau à distance' management console. On the left, a navigation pane lists 'Vue d'ensemble', 'Serveurs', and 'Collections'. The 'Collections' section is selected, and 'QuickSessionCollection' is highlighted. The main area is divided into three sections:

- PROPRIÉTÉS**: Shows the collection type (Session), resources (Programmes RemoteApp), and user groups (GSB\Utilisateurs du domaine).
- CONNEXIONS**: Displays a table of active sessions. The table includes columns for 'Nom de domaine complet du serveur', 'Utilisateur', 'État de la session', and 'Heure d'ouverture de session'. Three sessions are listed:

Nom de domaine complet du serveur	Utilisateur	État de la session	Heure d'ouverture de session
SERVEUR1.GSB.local	GSB\Administrateur	Actif	08/12/2017 12:34:43
SERVEUR1.GSB.local	GSB\anevers	Déconnecté	08/12/2017 15:51:12
SERVEUR1.GSB.local	GSB\anevers	Actif	08/12/2017 15:56:08
- PROGRAMMES REMOTEAPP**: Shows a list of remote application programs: Calculatrice, Paint, WordPad, and Cisco Packet Tracer. Each program has an 'Alias' column indicating if it has a local alias.

