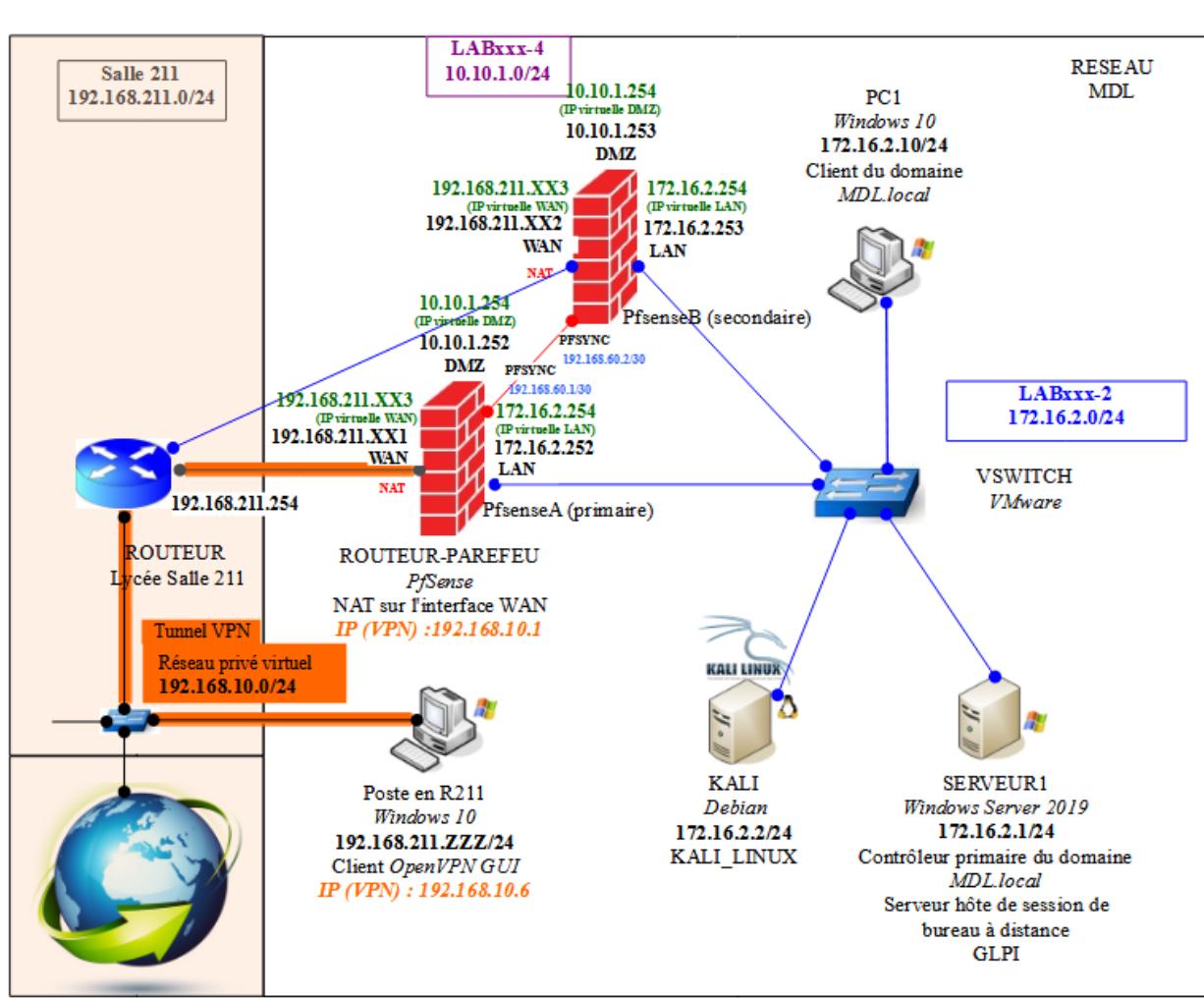


Projet MDL



TP 1 A - Installation d'un réseau Windows Server 2019

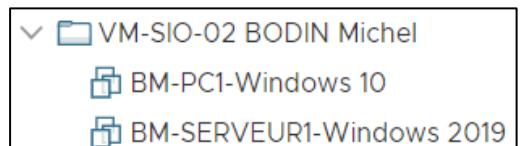
Création du contrôleur de domaine et connexion d'un poste au domaine

Objectifs

Le but de ce TP est l'installation complète d'un réseau client/serveur comprenant un serveur **Windows Server 2019**, et un poste de travail client **Windows 10** :

XX est un numéro de 01 à 25 attribué à chaque étudiant.

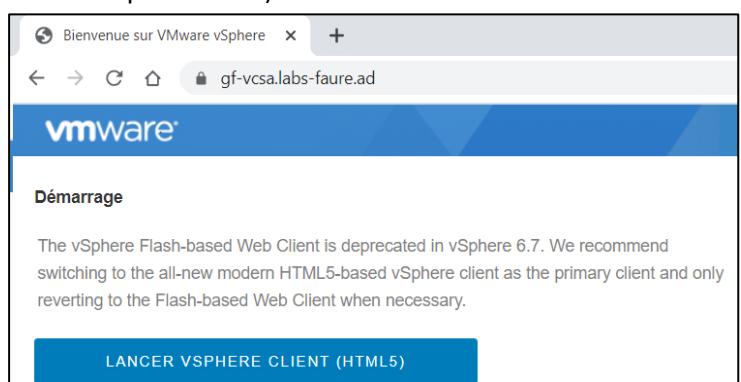
Chaque étudiant crée des Machines Virtuelles (VM) dans son dossier de nom **VM-SIO-XX** (exemple : VM-SIO-02).



On attribuera à chaque VM l'étiquette réseau **LAB-SIO-XX** correspondant au numéro **XX** de l'étudiant (exemple : LAB-SIO-02).

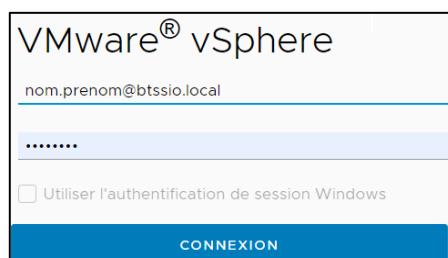
Chaque étudiant dispose de son routeur PfSense (déjà créé et opérationnel) d'adresse **10.0.2.254**.

Pour se connecter à la ferme de serveurs du lycée :



Si ce TP est réalisé avec VirtualBox, la configuration VirtualBox Réseau des machines virtuelles devra être **Réseau NAT** (nom :

NatNetwork, adresse réseau : **10.0.X.0/24**, **sans** support du DHCP) ; l'adresse du routeur sera alors 10.0.X.1.



Étape 1 : installation de Windows Server sur le serveur

Windows Server 2019 est normalement déjà installé sur le poste.

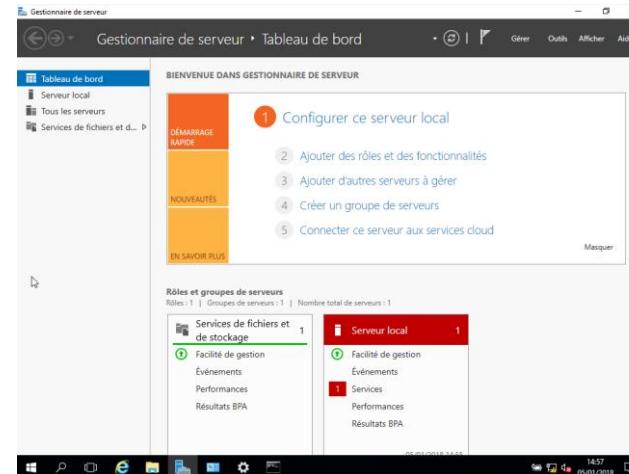
- a. Démarrer la machine *Windows Server 2019*.
- b. Ouvrir une session avec l'utilisateur *Administrateur* et le mot de passe *Windows2019*

Après installation, un nouvel écran apparaît : le gestionnaire



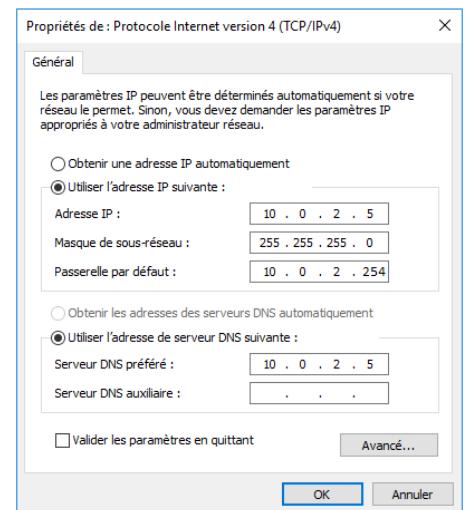
de serveur.

Celui-ci permet d'effectuer les principales opérations de configuration d'un serveur :



- c. Effectuer la configuration IP du serveur en sélectionnant Panneau de configuration / Réseau et Internet / Centre Réseau et partage (ou Paramètres / Réseau et Internet / Ethernet / Centre Réseau et partage) ;

cliquer sur le lien Ethernet : la fenêtre *Etat de Ethernet* s'ouvre : cliquer sur Propriétés ; sélectionner Protocole Internet version 4 (TCP/IPv4) puis cliquer sur le bouton Propriétés :



- d.Modifier le nom de cette machine (Panneau de configuration / Système et sécurité, Système , lien Paramètres système avancés ; dans la fenêtre qui s'ouvre, sélectionner l'onglet Nom de l'ordinateur, puis le bouton Modifier)
(ou Paramètres / Système / Informations système / Renommer le PC) :

Nom de l'ordinateur : *SERVEUR1*

- e. Laisser redémarrer le serveur.

Étape 2 : installation de Active Directory

Nous allons configurer le serveur *SERVEUR1* pour qu'il soit contrôleur d'un domaine *DOMAINE2019*.

Nous allons d'abord ajouter le rôle de serveur de domaine au serveur :

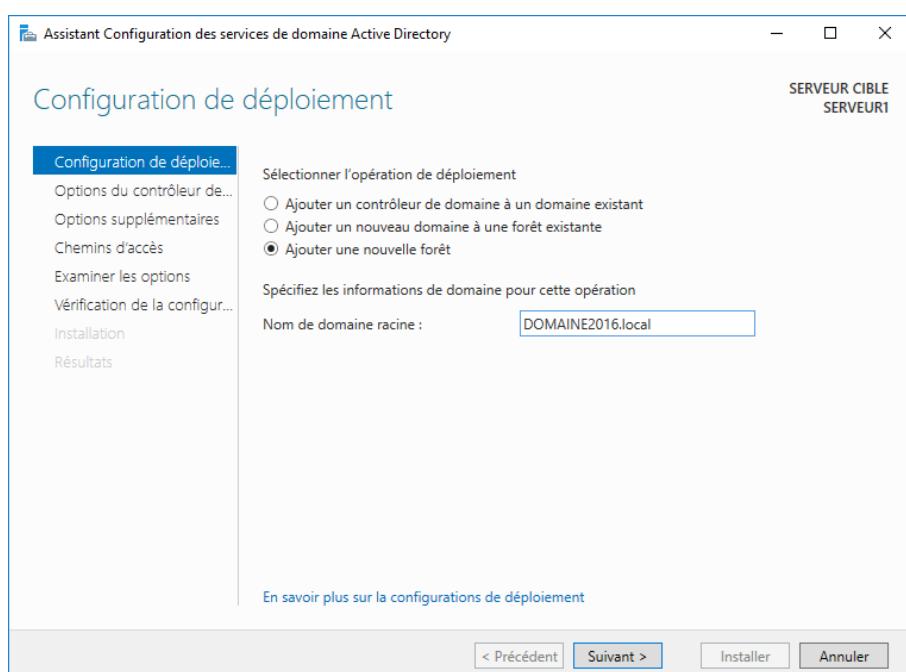
- a. Dans le tableau de bord Gestionnaire de serveur (cliquer sur  s'il n'est pas déjà ouvert), sélectionner Gérer, puis le lien Ajouter des rôles et fonctionnalités.
- b. Dans la fenêtre *Assistant Ajout de rôles et de fonctionnalités*, choisir une *Installation basée sur un rôle ou une fonctionnalité*.
- c. Sélectionner le serveur de destination sur lequel sera installé le rôle : *SERVEUR1*.
- d. Dans la liste des rôles, cocher le rôle *Services AD DS* (qui signifie *Services Active Directory Domain Services*), puis ajouter les fonctionnalités requises proposées par défaut pour ce rôle ; cocher aussi le rôle *Serveur DNS*.
- e. Ne pas sélectionner d'autres fonctionnalités.
- f. Cocher la case *Redémarrer automatiquement le serveur de destination si nécessaire* (si un redémarrage est nécessaire, le serveur redémarrera automatiquement), puis confirmer l'autorisation de redémarrage automatique.
- g. Confirmer l'installation de ce rôle en cliquant sur *Installer*.

Pour faire de cette machine Windows Server 2019 un contrôleur de domaine, il faut ensuite utiliser **l'icône d'avertissement représentée par le triangle jaune (Notifications)**  qui apparaît dans la fenêtre *Gestionnaire de serveur* :



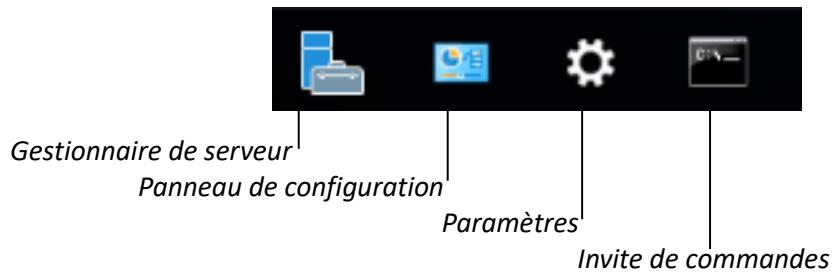
Avant cela, dans un vrai réseau physique, il faudrait s'assurer que le câble Ethernet est branché entre la carte réseau du serveur et le commutateur.

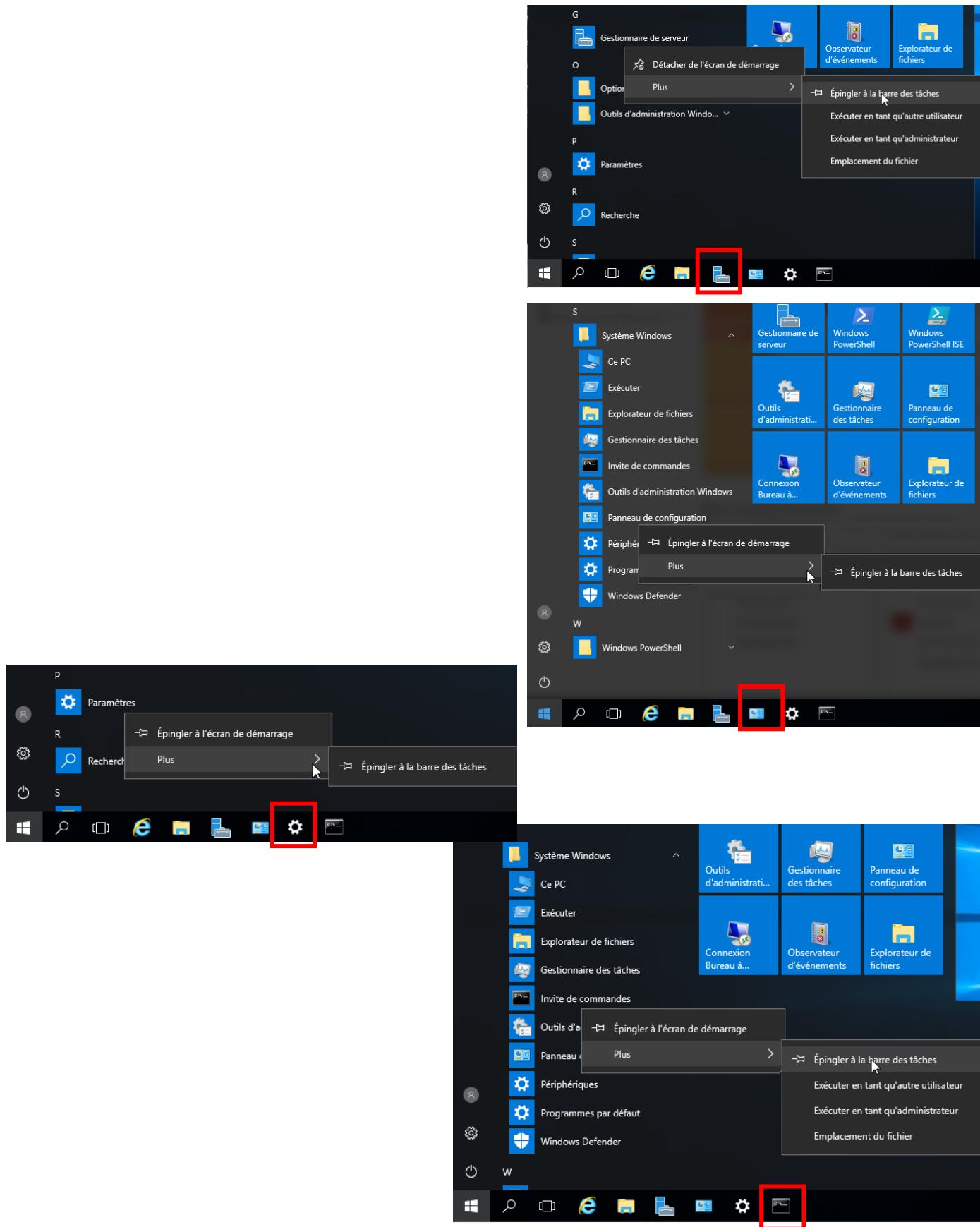
- h. Cliquer sur l'icône d'avertissement représentée par le triangle jaune (Notifications), puis sur le lien [Promouvoir ce serveur en contrôleur de domaine](#) :
 - Ajouter une nouvelle forêt
 - Nom de domaine racine : **DOMAINE2019.local**



- Choisir le niveau fonctionnel de la forêt et du domaine : *Windows Server 2016*
 - Cocher les cases
 - Serveur DNS pour installer le service Serveur DNS sur ce contrôleur de domaine
 - Catalogue global (annuaire central regroupant des éléments de tous les domaines de la forêt)
 - Entrer à nouveau le mot de passe administrateur : *Windows2019*
 - Ne pas tenir compte du message "Il est impossible de créer une délégation pour ce serveur DNS, ..."
 - Nom de domaine NetBIOS : **DOMAINE2019**
 - Accepter les noms de dossiers proposés pour la base de données, les fichiers journaux, et le dossier SYSVOL
 - Cliquer sur *Installer* lorsque la configuration requise a bien été validée.
- i. Laisser redémarrer la machine ; ouvrir une session avec l'utilisateur *DOMAINE2019\Administrateur* (ou plus simplement *Administrateur*) et le mot de passe *Windows2019*.

Remarque : il se peut que le système exige de changer de mot de passe ; dans ce cas seulement, changer le mot de passe en **Windows2019!** Avant de poursuivre, nous allons épingler quatre applications dans la barre des tâches, pour accéder plus rapidement aux principaux outils de configuration de la machine :





Pour épingler l'application **Gestionnaire de serveur** :

- f. Cliquer sur le bouton *Démarrer*, puis cliquer droit sur *Gestionnaire de serveur* ; dans le menu contextuel, sélectionner *Plus* puis *Epingler à la barre des tâches* :

Pour épingler l'application ***Panneau de configuration*** :

- g. Cliquer sur le bouton *Démarrer*, puis sélectionner *Système Windows* ; cliquer droit sur *Panneau de configuration* ; dans le menu contextuel, sélectionner *Plus* puis *Epingler à la barre des tâches* :

Pour épingler l'application ***Paramètres*** :

- h. Cliquer sur le bouton *Démarrer*, puis cliquer droit sur *Paramètres* ; dans le menu contextuel, sélectionner *Plus* puis *Epingler à la barre des tâches* :

Pour épingler l'application ***Invite de commandes*** :

- i. Cliquer sur le bouton *Démarrer*, puis sélectionner *Système Windows* ; cliquer droit sur *Invite de commandes* ; dans le menu contextuel, sélectionner *Plus* puis *Epingler à la barre des tâches* :

Étape 3 : connexion du poste client au réseau et au domaine

a. Mettre le poste client sous tension. Ouvrir une session avec le login *sio* et le mot de passe *sio*.

- f. Effectuer la configuration IP du poste en sélectionnant Panneau de configuration  / Réseau et Internet / Centre Réseau et partage (ou Paramètres  / Réseau et Internet / Ethernet / Centre Réseau et partage) ;

cliquer sur le lien Ethernet : la fenêtre *Etat de Ethernet* s'ouvre : cliquer sur Propriétés ; sélectionner Protocole Internet version 4 (TCP/IP v4) puis cliquer sur le bouton Propriétés :

cocher la case *Utiliser l'adresse IP suivante* :

Adresse IP : 10.0.2.15

Masque de réseau : (à déterminer)

Passerelle : (à déterminer)

DNS : 10.0.2.5 (c'est-à-dire l'adresse du serveur)

- g. Tester la connexion au serveur depuis le poste client à l'aide de la commande *ping* (tapée dans  l'invite de commandes) :

ping 10.0.2.5

Attention : il peut être nécessaire de désactiver le pare-feu du poste que l'on veut pinguer ou depuis lequel on pingue (le pare-feu peut bloquer les demandes ou réponses au **Ping** venant d'autres hôtes du réseau).

Pour désactiver le pare-feu sur un poste, sélectionner Panneau de configuration  / Système et sécurité,



Pare-feu Windows (ou Paramètres  / Réseau et Internet / Ethernet / Pare-feu Windows) ; cliquer sur le lien Activer ou désactiver le Pare-feu Windows : désactiver le pare-feu pour tous les types d'emplacement réseau.

Si cette commande n'aboutit pas, revoyez vos configurations !

On peut également faire un *ping* depuis le serveur vers le poste client (*ping* qui ne fonctionnera que si le pare-feu Windows du poste-client est désactivé, ou s'il est activé et autorise les demandes d'écho IPv4 entrantes !).

- h. Depuis le poste client, modifier le nom du poste, et connecter ce poste au domaine DOMAINE2019  / Système et sécurité, Système , lien Paramètres système avancés ; dans la fenêtre qui s'ouvre, sélectionner l'onglet Nom de l'ordinateur, puis le bouton Modifier :

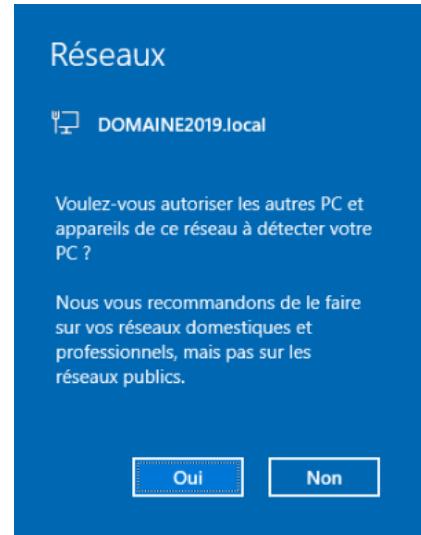


(ou Paramètres  / Système / Informations système / puis les boutons Renommer le PC et Joindre un domaine) :

Nom de l'ordinateur : *PC1*

Membre d'un domaine : **DOMAINE2019.local**

- i. Après avoir validé avec OK, ressaisir le nom et le mot de passe du compte administrateur : *Administrateur/Windows2019*
- j. Laisser redémarrer la machine, puis ouvrir une session administrateur en se connectant au domaine avec le login *DOMAINE2019\Administrateur* et le mot de passe *Windows2019*.
- k. Si un message s'affiche en bleu, demandant d'autoriser les autres PC de ce réseau à détecter ce PC, cliquer sur Oui.



- l. Sur le poste client, dans l'Explorateur, cliquer sur Réseaux : le serveur doit être visible !

S'il ne l'est pas, sélectionner Panneau de configuration  / Réseau et Internet / Centre Réseau et partage



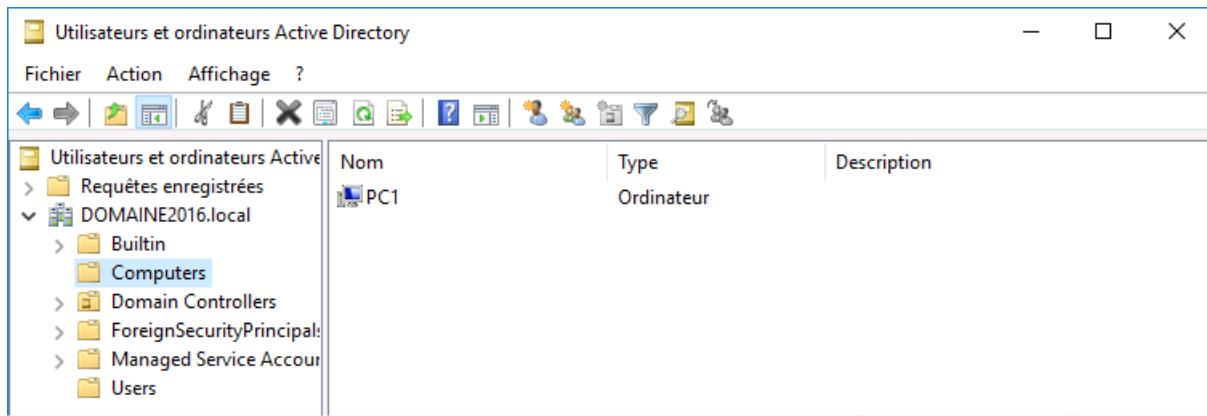
(ou Paramètres  / Réseau et Internet / Ethernet / Centre Réseau et partage), puis cliquer sur le lien Modifier les paramètres de partage avancé, et veiller à ce que les options de partage suivantes pour le profil *Domaine* soient cochées :

- *Activer la découverte de réseau*
- *Activer le partage de fichiers et d'imprimantes*

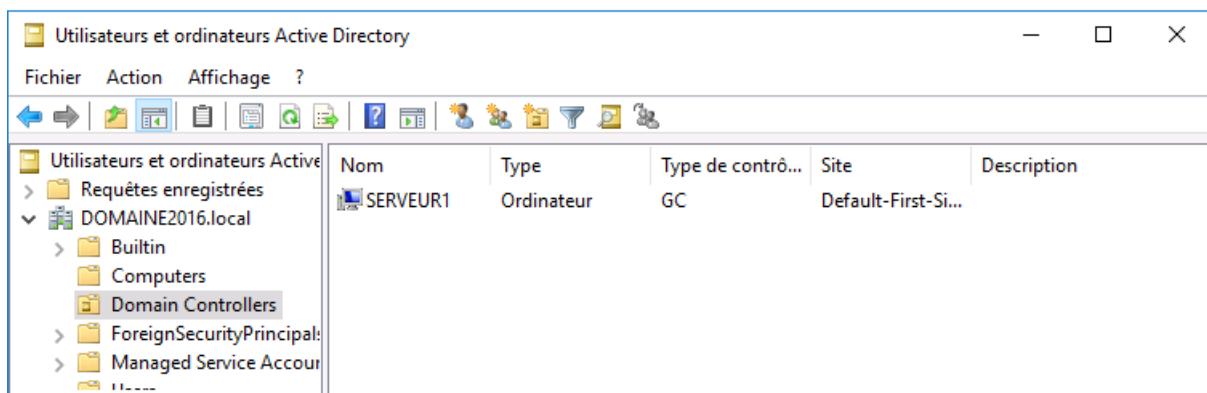
Nous allons vérifier que l'annuaire Active Directory contient bien tous les éléments :

- m. Sur le serveur, dans le Gestionnaire de serveur (cliquer sur  s'il n'est pas déjà ouvert), sélectionner Outils / Utilisateurs et ordinateurs Active Directory, puis cliquer sur **DOMAINE2019.local** :

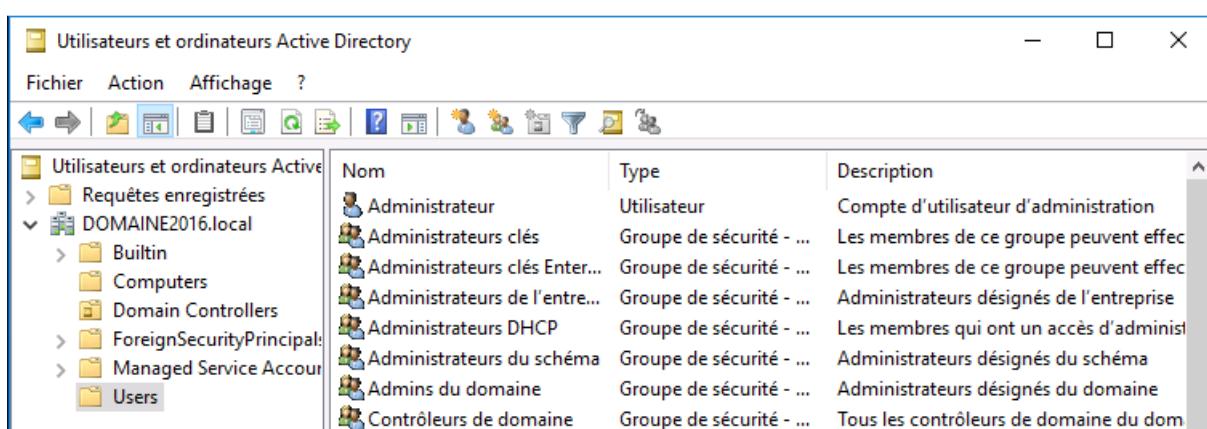
- dans le dossier *Computers*, le poste client *PC1* doit être visible ;
- dans le dossier *Domain Controllers*, le serveur contrôleur de domaine *SERVEUR1* doit être visible ;
- dans le dossier *Users*, l'utilisateur *Administrateur* doit être visible :



Nom	Type	Description
PC1	Ordinateur	



Nom	Type	Type de contrôl...	Site	Description
SERVEUR1	Ordinateur	GC	Default-First-Si...	



Nom	Type	Description
Administrateur	Utilisateur	Compte d'utilisateur d'administration
Administrateurs clés	Groupe de sécurité - ...	Les membres de ce groupe peuvent effec...
Administrateurs clés Enter...	Groupe de sécurité - ...	Les membres de ce groupe peuvent effec...
Administrateurs de l'entre...	Groupe de sécurité - ...	Administrateurs désignés de l'entreprise
Administrateurs DHCP	Groupe de sécurité - ...	Les membres qui ont un accès d'administ...
Administrateurs du schéma	Groupe de sécurité - ...	Administrateurs désignés du schéma
Admins du domaine	Groupe de sécurité - ...	Administrateurs désignés du domaine
Contrôleurs de domaine	Groupe de sécurité - ...	Tous les contrôleurs de domaine du dom...

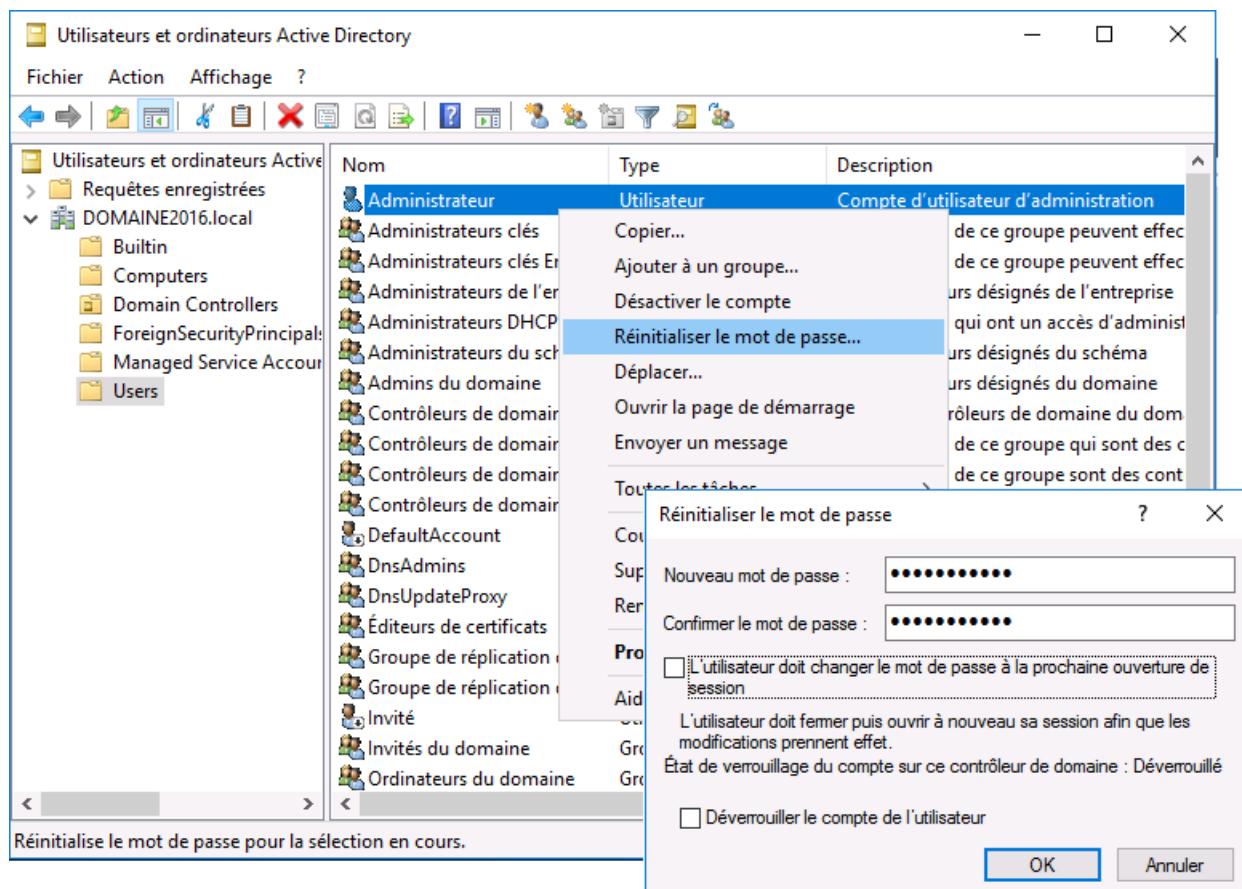
Étape 4 : modification du mot de passe d'un utilisateur depuis le serveur de domaine

L'administrateur a le droit de modifier le mot de passe de n'importe quel utilisateur (fonction indispensable car les utilisateurs oublient parfois leur mot de passe ...), y compris le sien.

Lorsque SERVEUR1 a été promu en contrôleur de domaine, le système a sans doute exigé que le mot de passe de l'Administrateur soit modifié ; nous allons remodifier ce mot de passe et le rétablir comme il était à l'origine : *Windows2019* :

- a. Sur le serveur, dans le Gestionnaire de serveur (cliquer sur  s'il n'est pas déjà ouvert), sélectionner Outils / Utilisateurs et ordinateurs Active Directory, puis cliquer sur *DOMAINE2019.local*, puis sur *Users* : la liste des utilisateurs du domaine s'affiche dans le volet de droite ;
- b. Cliquer avec le bouton droit de la souris sur *Administrateur* ; dans le menu contextuel qui s'affiche, sélectionner la commande *Réinitialiser le mot de passe* :

Nouveau mot de passe :	Windows2019
Confirmer le mot de passe :	Windows2019
Changer le mot de passe à la prochaine ouverture de session :	<i>Non (ne pas cocher)</i>



Étape 5 : configuration du compte Administrateur d'un serveur Microsoft Windows pour que le mot de passe n'expire jamais

Par défaut, le mot de passe du compte Administrateur du serveur Windows 2019 expire au bout de 42 jours ; après 42 jours, le système exigera que l'Administrateur modifie son mot de passe.

Nous allons modifier cette stratégie pour que le mot de passe n'expire jamais, et donc que le système ne demande pas à l'Administrateur de le modifier.

Sur le serveur Windows 2019 (SERVEUR1) :

- a. Exécuter la commande suivante (tapée dans  l'invite de commandes) pour vérifier que la durée de vie du mot de passe est actuellement de 42 jours :

net accounts

- b. Exécuter la commande suivante pour que le mot de passe n'expire jamais :

net accounts /maxpwage:unlimited

- c. Exécuter la commande suivante (tapée dans  l'invite de commandes) pour vérifier que la durée de vie du mot de passe est maintenant illimitée :

net accounts

```
C:\Users\Administrateur.WIN-4LG01B9BQ2U>net accounts
Fermeture forcée de la session après expiration ? : Jamais
Durée de vie minimale du mot de passe (jours) : 1
Durée de vie maximale du mot de passe (jours) : Pas de limite
Longueur minimale du mot de passe : 7
Nombre de mots de passe antérieurs à conserver : 24
Seuil de verrouillage : Jamais
Durée du verrouillage (min) : 30
Fenêtre d'observation du verrouillage (min) : 30
Rôle de l'ordinateur : PRINCIPAL
La commande s'est terminée correctement.
```

Il n'y a désormais plus d'expiration du mot de passe sur les comptes locaux de ce serveur.

Remarque :

Dans le cas où l'administrateur souhaite changer son mot de passe, on peut aussi ne plus lui interdire de reprendre le même mot de passe que les précédents en exécutant la commande :

net accounts /uniquepw:0

Toutes les possibilités de la commande *net accounts* :

http://idfixes26.free.fr/Extras_old_time/aide_windows-XP_cmd/aide_cmd_fichiers/net_accounts.htm

Étape 6 : configuration du DHCP

Nous allons ajouter le rôle de serveur DHCP au serveur *SERVEUR1* :

- d. Sur le serveur, dans le Gestionnaire de serveur (cliquer sur  s'il n'est pas déjà ouvert), sélectionner Gérer / Ajouter des rôles et fonctionnalités ;
- e. Dans la fenêtre *Assistant Ajout de rôles et de fonctionnalités*, choisir une *Installation basée sur un rôle ou une fonctionnalité*.
- f. Sélectionner le serveur de destination sur lequel sera installé le rôle : *SERVEUR1*.
- g. Dans la liste des rôles, cocher le rôle *Serveur DHCP*, puis ajouter les fonctionnalités requises proposées par défaut pour ce rôle.
- h. Ne pas sélectionner d'autres fonctionnalités.
- i. Cocher la case *Redémarrer automatiquement le serveur de destination si nécessaire*.
- j. Confirmer l'installation de ce rôle en cliquant sur *Installer*.

Après l'installation du DHCP, l'**icône d'avertissement représentée par le triangle jaune (Notifications)** apparaît.

- k. Cliquer sur l'icône d'avertissement représentée par le triangle jaune (Notifications alerte Configuration post-déploiement), puis cliquer sur *Terminer la configuration DHCP* ; valider tous les choix proposés.

Nous allons maintenant configurer ce DHCP :

- l. Sur le serveur, dans le Gestionnaire de serveur (cliquer sur  s'il n'est pas déjà ouvert), sélectionner Outils / DHCP.
- m. Dans l'arborescence de gauche de la fenêtre *DHCP*, cliquer sur *SERVEUR1.DOMAINE2019.local*, puis sur *IPv4*.
- n. Créer une nouvelle étendue (avec la commande Action Nouvelle étendue) :

Nom de l'étendue : *Etendue1*
Adresse IP de départ : *10.0.2.10*
Adresse IP de fin : *10.0.2.19*
Longueur (de la section réseau) : *24*
Masque de sous-réseau : *255.255.255.0*
Ne pas spécifier de plage d'adresses à exclure
Durée du bail : *8 jours*

Configurer les options DHCP (adresse de la passerelle (Routeur) et adresse du DNS à distribuer) pour cette étendue :

Routeur (adresse IP de la passerelle) :
10.0.2.254
(à Ajouter à la liste)

Assistant Nouvelle étendue

Routeur (passerelle par défaut)
Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.

Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

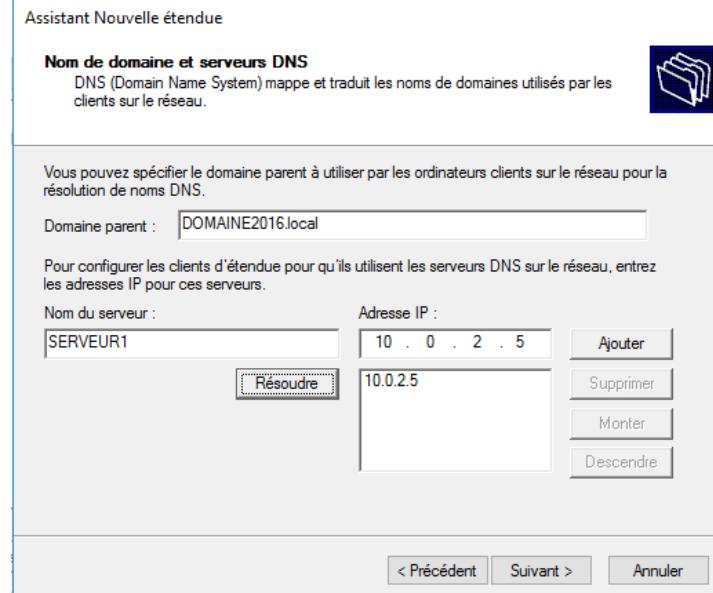
10 . 0 . 2 . 254	Ajouter
10.0.2.254	Supprimer
	Monter
	Descendre

< Précédent Suivant > Annuler

Nom de domaine (Domaine parent) :
DOMAINE2019.local

DNS (adresse IP) :
10.0.2.5
(déjà ajouté automatiquement à la liste)

Ne pas ajouter de serveurs WINS



o. Activer cette étendue.

Nous allons maintenant configurer le poste de travail avec une adresse IP obtenue automatiquement du DHCP :

p. Sur le poste de travail, configurer l'adressage IP automatique :

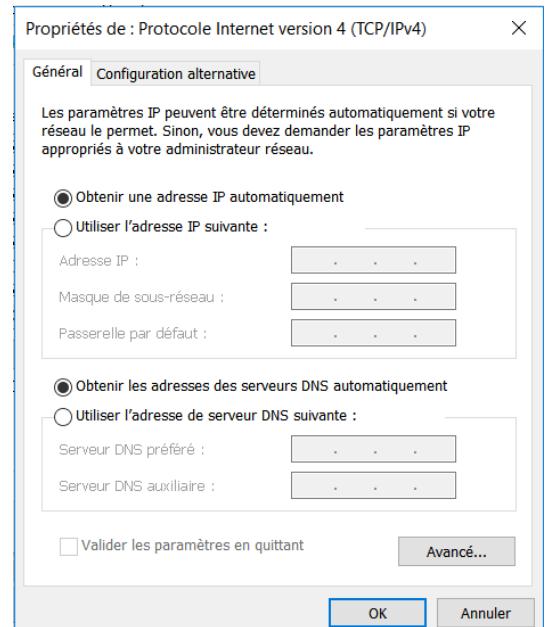
- sélectionner Panneau de configuration / Réseau et Internet / Centre Réseau et partage
(ou Paramètres / Réseau et Internet / Ethernet / Centre Réseau et partage) ;

cliquer sur le lien Ethernet : la fenêtre *Etat de Ethernet* s'ouvre : cliquer sur Propriétés ; sélectionner Protocole Internet version 4 (TCP/IP v4) puis cliquer sur le bouton Propriétés :

- cocher les cases :

Obtenir une adresse IP automatiquement
Obtenir les adresses des serveurs DNS automatiquement :

- Valider en cliquant sur *OK*.



- q. Mettre à jour la configuration IP du poste en exécutant les deux commandes suivantes (tapées dans



l'invite de commandes) :

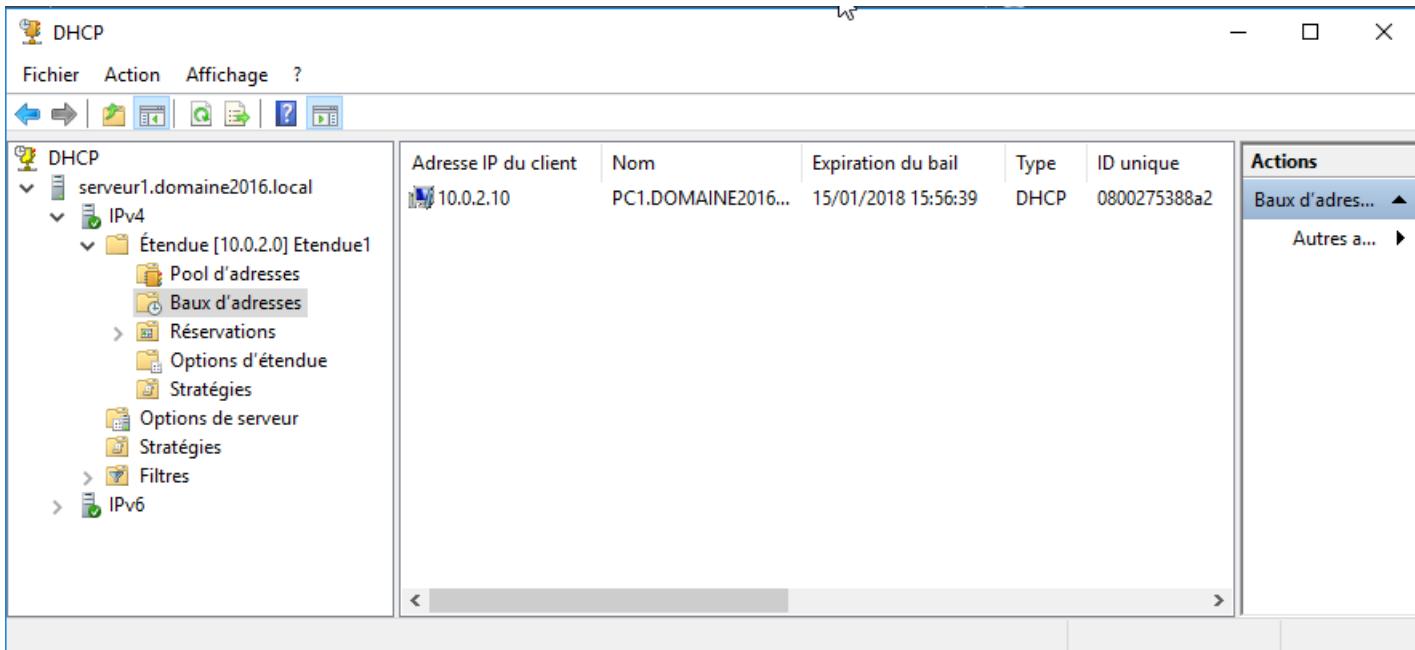
ipconfig /release pour libérer l'adresse IP actuelle,
ipconfig /renew pour renouveler la configuration IP du poste.

La nouvelle adresse IP du poste PC1 est 10.0.2.10.

- r. Vérifier ensuite sur le poste, avec la commande `ipconfig/all` (tapée dans l'invite de commandes) la nouvelle configuration :

La nouvelle adresse IP du poste PC1 est 10.0.2.10 ; elle a été attribuée par le serveur DHCP 10.0.2.5.

- s. Vérifier ensuite sur le serveur DHCP (avec Gestionnaire de serveur / Outils / DHCP), dans la rubrique Baux d'adresses, que l'adresse IP 10.0.2.10 a bien été affectée au poste PC1 (et qu'il existe donc bien un bail pour cette adresse) :



BTS SIO 1

SI5

TP 2 B - Installation d'un réseau Windows Server 2019 Création de comptes-utilisateurs

Objectifs

Le but de ce TP est d'administrer un serveur **Windows Server 2019**, en créant des utilisateurs et des dossiers personnels.

Ce TP s'appuie sur le réseau local client/serveur suivant, déjà installé lors d'un TP précédent, comprenant un serveur Windows Server 2019, et un poste de travail client Windows 10 :

Étape 1 : démarrage du serveur et vérification de l'accès à Internet

- a. Démarrer la machine *SERVEUR1 Windows Server 2019*.
- b. Ouvrir une session avec l'utilisateur *DOMAINE2019\Administrateur* et le mot de passe *Windows2019*
- c. Vérifier la configuration IP du serveur en sélectionnant Panneau de configuration  / Réseau et Internet / Centre Réseau et partage (ou Paramètres  / Réseau et Internet / Ethernet / Centre Réseau et partage) ;
cliquer sur le lien Ethernet : la fenêtre *Etat de Ethernet* s'ouvre : cliquer sur Propriétés ; sélectionner Protocole Internet version 4 (TCP/IP v4) puis cliquer sur le bouton Propriétés :

Adresse IP :	10.0.2.5
Masque de réseau :	255.255.255.0
Passerelle :	10.0.2.254
DNS :	10.0.2.5 (c'est-à-dire lui-même)

Pour qu'une machine puisse accéder à Internet, il faut avoir entré la configuration IP complète :

- une adresse IP (pour que le poste soit adressable et donc "reconnaissable" depuis le réseau)
- un masque (qui délimite la partie réseau et la partie hôte de l'adresse IP du poste)
- la passerelle (l'adresse IP du routeur qui permet de "sortir" du réseau)
- le DNS (l'adresse IP de l'annuaire qui permet de traduire un nom de domaine en une adresse IP)

Normalement, lorsque cette configuration IP est faite sur un serveur, dans le coin bas droit de l'écran, l'icône d'accès correct à Internet doit être présente :



et la commande *ping google.fr* doit fonctionner :

```
C:\Users\Administrateur.WIN-4LG01B9BQ2U>ping google.fr

Envoy d'une requête 'ping' sur google.fr [216.58.204.99] avec 32 octets de données :
Réponse de 216.58.204.99 : octets=32 temps=66 ms TTL=54
Réponse de 216.58.204.99 : octets=32 temps=69 ms TTL=54
Réponse de 216.58.204.99 : octets=32 temps=65 ms TTL=54
Réponse de 216.58.204.99 : octets=32 temps=64 ms TTL=54
```

Cependant, il est possible que l'accès à Internet soit défaillant ; dans ce cas, dans le coin bas droit de l'écran, l'icône d'accès défaillant à Internet est présente :



et la commande *ping google.fr* ne fonctionne pas.

Si tel est le cas, on peut essayer la solution suivante :

- Sur le serveur SERVEUR1, sélectionner Panneau de configuration  / Réseau et Internet / Centre Réseau et partage

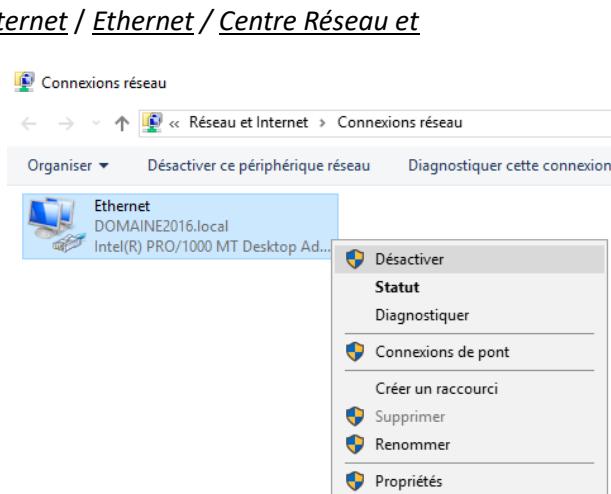


(ou Paramètres  / Réseau et Internet / Ethernet / Centre Réseau et partage) ;

cliquer sur le lien Modifier les paramètres de la carte : une icône représentant la carte réseau apparaît ;

- désactiver cette carte en cliquant droit sur la souris puis en sélectionnant la commande Désactiver du menu contextuel ;

- réactiver ensuite la carte en cliquant droit sur la souris puis en sélectionnant la commande Activer du menu contextuel.



Le fait de désactiver puis de réactiver la carte a souvent un effet bénéfique ; retenter la commande *ping google.fr* et vérifier que l'icône d'accès correct à Internet est rétabli.

- Vérifier le nom du serveur (Panneau de configuration  / Système et sécurité, Système)



(ou Paramètres  / Système / Informations système):

Nom complet de l'ordinateur : *SERVEUR1.DOMAINE2019.local*
Domaine : *DOMAINE2019.local*

Étape 2 : démarrage du poste client

- a. Démarrer la machine *PC1 Windows 10*.
- b. Ouvrir une session avec l'utilisateur *DOMAINE2019\Administrateur* et le mot de passe *Windows2019*
- c. Vérifier la configuration IP du poste :

Adresse IP : 10.0.2.15
Masque de réseau : 255.255.255.0
Passerelle : 10.0.2.254
DNS : 10.0.2.5 (c'est-à-dire l'adresse du serveur)

- d. Vérifier le nom de cette machine :

Nom complet de l'ordinateur : *PC1.DOMAINE2019.local*
Domaine : *DOMAINE2019.local*

- e. Effectuer un test de connectivité (avec la commande *ping*) entre *PC1* et *SERVEUR1* :
PC1 doit pouvoir pinguer *SERVEUR1* sans erreur ! Si ce n'est pas le cas, il faut revoir la configuration des machines !
- f. Sur le poste client, dans l'Explorateur, cliquer sur Réseaux : le serveur doit être visible !
S'il ne l'est pas, sélectionner Panneau de configuration  / Réseau et Internet / Centre Réseau et partage
(ou Paramètres  / Réseau et Internet / Ethernet / Centre Réseau et partage), puis cliquer sur le lien Modifier les paramètres de partage avancé, et veiller à ce que les options de partage suivantes pour le profil *Domaine* soient cochées :
j. *Activer la découverte de réseau*
k. *Activer le partage de fichiers et d'imprimantes*

- g. Sur le serveur, dans le Gestionnaire de serveur (cliquer sur  s'il n'est pas déjà ouvert), sélectionner Outils / Utilisateurs et ordinateurs Active Directory, puis cliquer sur *DOMAINE2019.local* :
 - dans le dossier *Computers*, le poste client *PC1* doit être visible ;
 - dans le dossier *Domain Controllers*, le serveur *SERVEUR1* doit être visible.

Étape 3 : création d'un nouvel utilisateur

- Sur SERVEUR1, vérifier que l'utilisateur Charles Dupont existe bien ; sinon, créer cet utilisateur

depuis le serveur (*Gestionnaire de serveur* / *Outils* / *Utilisateurs et ordinateurs Active Directory* ; cliquer ensuite sur le dossier *Users*, puis sélectionner la commande *Action Nouveau Utilisateur*) :

Prénom : *Charles*

Nom : *Dupont*

Nom d'ouverture de session : *cdupont*

Mot de passe : *Windows2019*

Décocher la case *L'utilisateur doit changer de mot de passe à la prochaine ouverture de session*

Cocher la case *Le mot de passe n'expire jamais*

- Après avoir fermé la session *Administrateur*, ouvrir une session sur le poste de travail PC1 avec l'utilisateur *cdupont* ; cet utilisateur ne possède pas encore de dossier personnel sur SERVEUR1.

Étape 4 : création d'un dossier personnel de base pour chaque utilisateur

Nous allons maintenant créer le dossier REPBASES qui contiendra le dossier personnel de base de chaque utilisateur, puis donner les autorisations de partage et les autorisations NTFS sur ce dossier.

- Sur SERVEUR1, créer le dossier **REPBASES** sur le disque C: du serveur, dans le dossier racine ;

- Partager ce dossier REPBASES (clic droit sur le dossier, puis sélectionner *Propriétés*, puis l'onglet *Partage* de la fenêtre) :

Cliquer sur le bouton *Partage avancé*

- Dans la fenêtre Partage avancé :

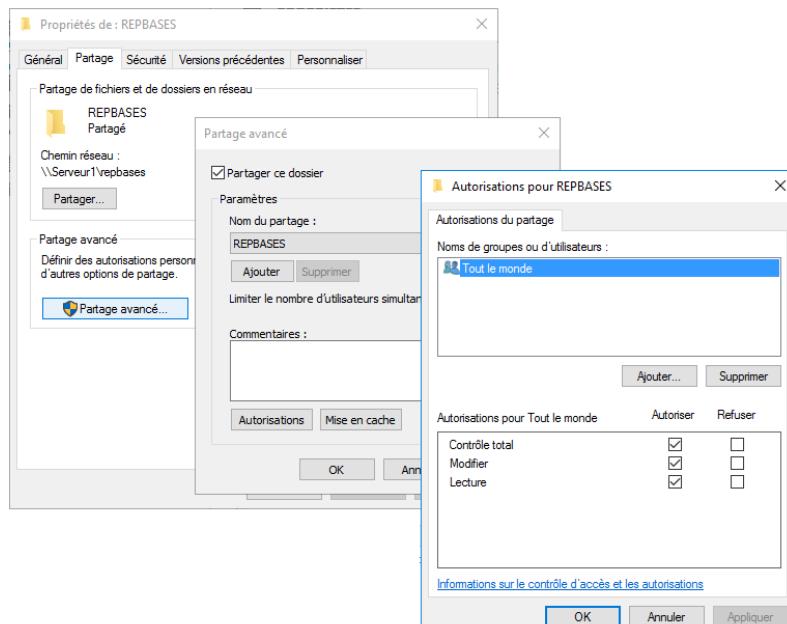
Cocher la case *Partager ce dossier*
Puis cliquer sur le bouton
Autorisations

- Dans la fenêtre Autorisations, donner l'autorisation *Contrôle total* à *Tout le monde*.

- Fermer la fenêtre des autorisations en cliquant sur *Appliquer* puis *OK*.

- Cliquer maintenant sur l'onglet *Sécurité* de la fenêtre *Propriétés* du dossier REPBASES pour afficher les autorisations NTFS accordées pour ce dossier, qui sont :

- CREATEUR PROPRIETAIRE :** possède le Contrôle Total (via les Autorisations spéciales) du dossier



- **Système :** possède le Contrôle Total
- **Administrateurs :** possède le Contrôle Total
- **Utilisateurs (du domaine) :** possède les droits de lecture, exécution, affichage du dossier, mais aussi les droits de création de fichiers et de dossiers (via les Autorisations spéciales).

Toutes ces autorisations sont héritées lors de la création du dossier à la racine C:\. Si l'une seulement de ces autorisations héritées n'est pas désirée par l'administrateur du réseau, il faut d'abord convertir ces autorisations héritées en autorisations explicites pour ensuite supprimer celles non désirées.

En effet, on ne peut pas modifier des autorisations héritées (qui apparaissent en grisé).

Les **Utilisateurs (du domaine)** disposent, sur le dossier REPBASES, des autorisations suivantes :

- *Lecture et exécution*
- *Affichage du contenu du dossier*
- *Lecture*
- *Création de fichiers et de dossiers (via les Autorisations spéciales).*

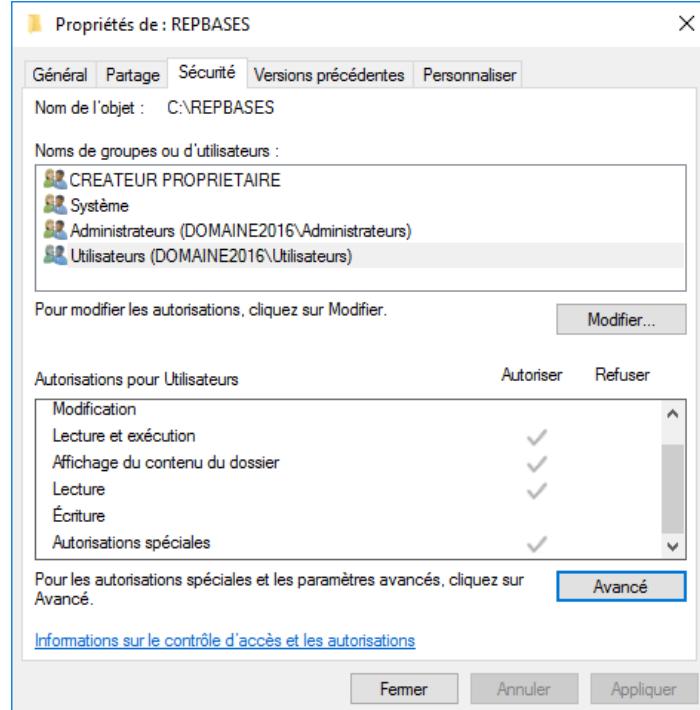
Les dossiers personnels de base, qui seront des sous-dossiers de REPBASES, vont hériter automatiquement des autorisations du dossier parent REPBASES.

Or, on ne veut pas que chaque utilisateur puisse lire le contenu des dossiers personnels de base des autres utilisateurs !

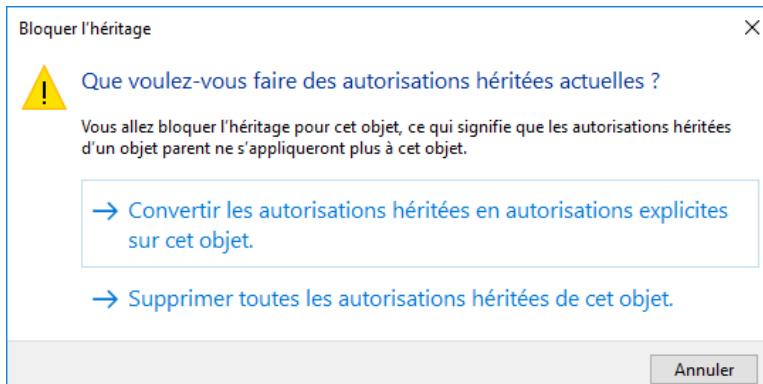
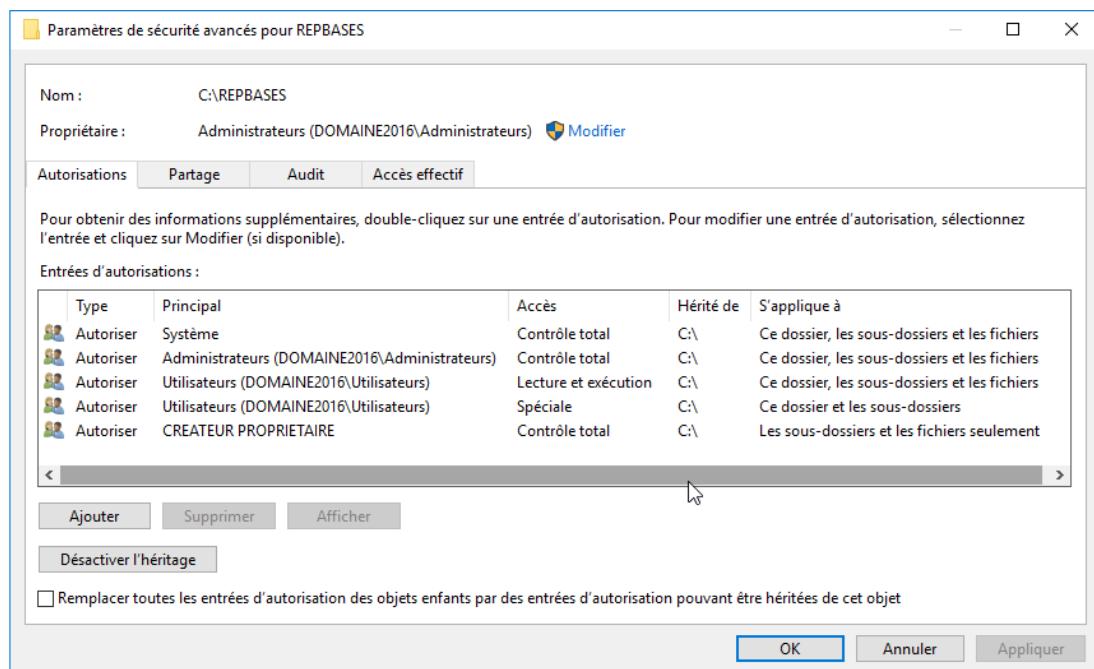
Nous allons donc devoir convertir tous les droits hérités en droits explicites, pour pouvoir ensuite supprimer les droits de **Utilisateurs (du domaine)**.

g. Cliquer sur le bouton *Avancé* de la fenêtre *Propriétés de REPBASES*.

- h. Puis cliquer sur le bouton
Désactiver l'héritage de la fenêtre
Paramètres de sécurité avancés
 pour REPBASES :



- i. Dans le message de sécurité qui s'affiche lors du blocage de l'héritage, cliquer sur le lien *Convertir les autorisations héritées en autorisations explicites sur cet objet.*



j. Fermer la fenêtre des autorisations en cliquant sur *Appliquer* puis *OK*.

Toutes les autorisations provenant d'un héritage sont maintenant des autorisations explicites.

- k. Supprimer toutes les autorisations accordées à *Utilisateurs (du domaine)* :
- cliquer sur le bouton *Modifier*
 - Sélectionner **Utilisateurs (du domaine)**
 - cliquer sur le bouton *Supprimer*.

The left screenshot shows the 'Propriétés de : REPBASES' dialog box with the 'Sécurité' tab selected. It lists four groups: 'CREATEUR PROPRIETAIRE', 'Système', 'Administrateurs (DOMAINE2016\Administrateurs)', and 'Utilisateurs (DOMAINE2016\Utilisateurs)'. Below is a note to click 'Modifier...' to change permissions. The 'Autorisations pour Utilisateurs' table shows checkboxes for 'Modification', 'Lecture et exécution', 'Affichage du contenu du dossier', 'Lecture', 'Écriture', and 'Autorisations spéciales'. The right screenshot shows the 'Autorisations pour REPBASES' dialog box with the 'Sécurité' tab selected. It has the same group list. The 'Utilisateurs (DOMAINE2016\Utilisateurs)' group is selected. Below is an 'Ajouter...' button and a 'Supprimer' button. The 'Autorisations pour Utilisateurs' table shows checkboxes for 'Contrôle total', 'Modification', 'Lecture et exécution', 'Affichage du contenu du dossier', and 'Lecture'. The 'Utilisateurs (DOMAINE2016\Utilisateurs)' row has all checkboxes checked.

Maintenant, pour le dossier REPBASES, *Utilisateurs (du domaine)* n'a plus aucun droits ; mais *CREATEUR PROPRIETAIRE*, *Système*, et *Administrateurs* 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.

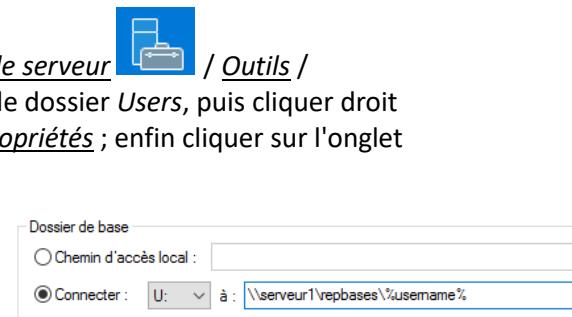
1. Fermer les fenêtres ouvertes en cliquant sur *Appliquer* et/ou sur *OK*.

Nous allons maintenant faire en sorte qu'un dossier personnel de base *cduPont* soit créé pour l'utilisateur Charles Dupont (seuls cet utilisateur, le système, et l'administrateur devront avoir accès à ce dossier personnel) :

- m. Modifier le profil de l'utilisateur Charles Dupont ([Gestionnaire de serveur](#) / [Outils](#) / [Utilisateurs et ordinateurs Active Directory](#) ; cliquer ensuite sur le dossier *Users*, puis cliquer droit sur l'utilisateur Charles Dupont et sélectionner la commande [Propriétés](#) ; enfin cliquer sur l'onglet [Profil](#) de la fenêtre) :

Connecter : U:

à \\SERVEUR1\REPBASES%\%username%

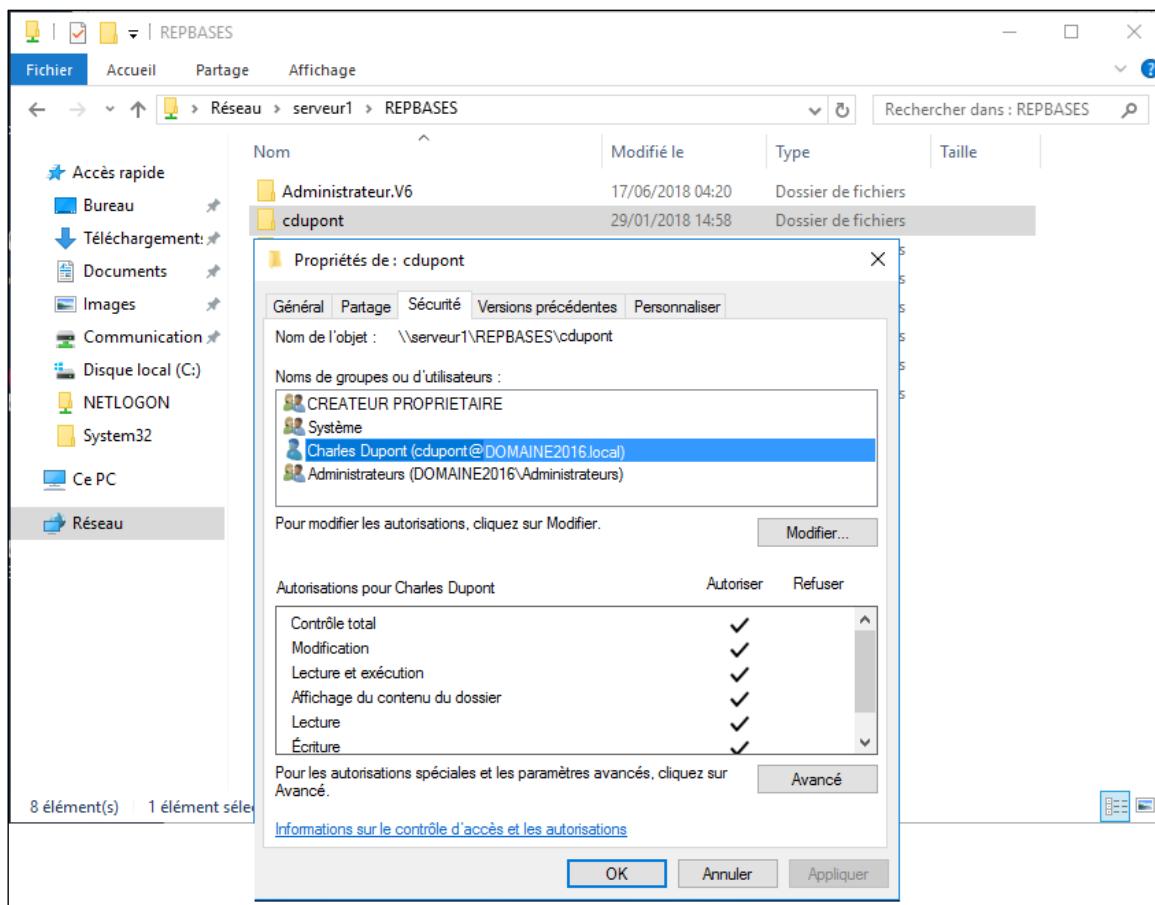


NB : la variable %username% contient le nom d'ouverture de session de l'utilisateur courant (ici : cduPont);

Cliquer sur le bouton *Appliquer* pour valider, puis sur le bouton *OK* pour fermer la fenêtre.

**Le dossier pour cet utilisateur est alors automatiquement créé dans le dossier REPBASES !
Et l'autorisation Contrôle total est automatiquement attribuée à ce dossier pour cet utilisateur !**

- n. Vérifier avec l'explorateur Windows depuis le serveur qu'un dossier *cduPont* a bien été créé dans le dossier REPBASES, puis vérifier que cet utilisateur a bien toutes les autorisations NTFS de lecture, écriture, ... : [Contrôle total](#) :



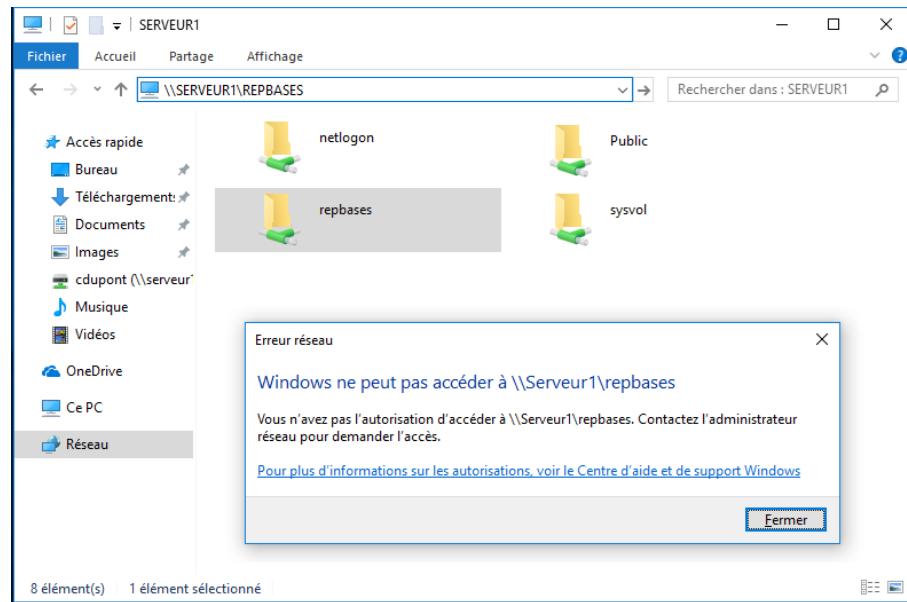
- o. Vérifier avec l'explorateur Windows depuis le poste de travail PC1, sur lequel une session a été ouverte par Charles Dupont, que ce dossier est accessible (grâce à U:).

Attention : si une session est déjà ouverte pour un utilisateur (exemple pour Charles Dupont), le lecteur réseau U: ne va pas apparaître ; il faut fermer la session, puis en ouvrir une nouvelle. En effet, les lecteurs-réseau sont toujours montés au démarrage d'une session.

- p. Toujours sur le poste de travail, vérifier que Charles Dupont a effectivement le droit de créer, modifier, ... en créant le fichier *Exemple1.txt* contenant le petit texte suivant "Ceci est un texte créé sur PC1 dans cdupont".

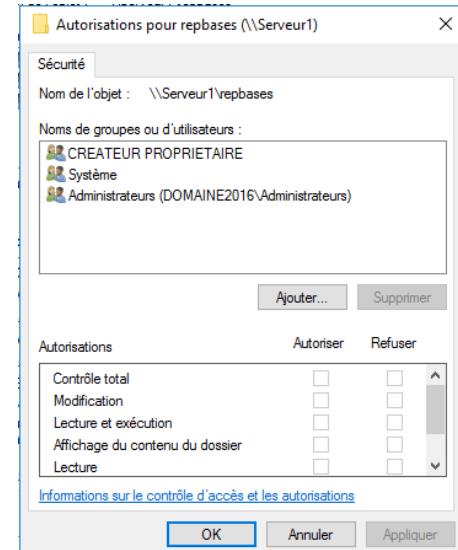
Attention : remarque importante !

- q. Vérifier avec l'explorateur Windows depuis le poste de travail PC1, sur lequel une session a été ouverte par Charles Dupont, que l'on ne peut pas accéder au dossier REPBASES (soit en tapant `\SERVEUR1\REPBASES` dans la barre de titres, soit en cliquant sur l'icône Réseau, puis sur le dossier REPBASES) :



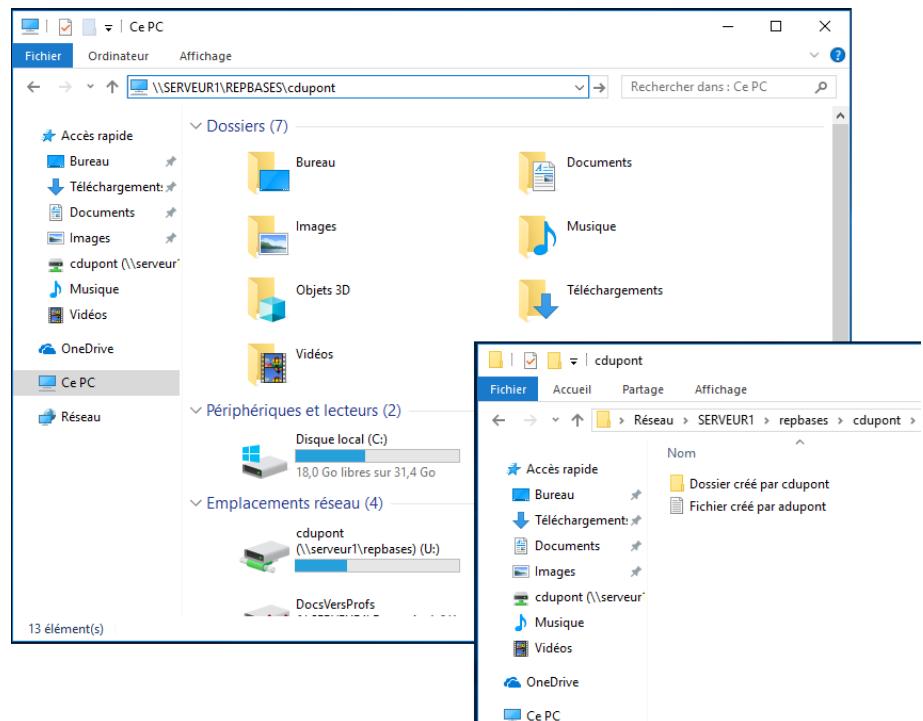
Ceci est normal, puisque Charles Dupont n'a aucune autorisation sur le dossier REPBASES.

Il ne peut donc pas accéder à son dossier personnel de base (qui est pourtant le sous-dossier \REPBASES\cdupont) via REPBASES (en passant par REPBASES).



- r. En revanche, Charles Dupont peut accéder à son dossier personnel REPBASES\cdupont **directement**
 (soit en tapant \\SERVEUR1\REPBASES\cdupont dans la barre de titres, soit en cliquant sur l'icône du connecteur réseau U:)

Ceci est normal puisque Charles Dupont a les autorisations sur son dossier personnel.

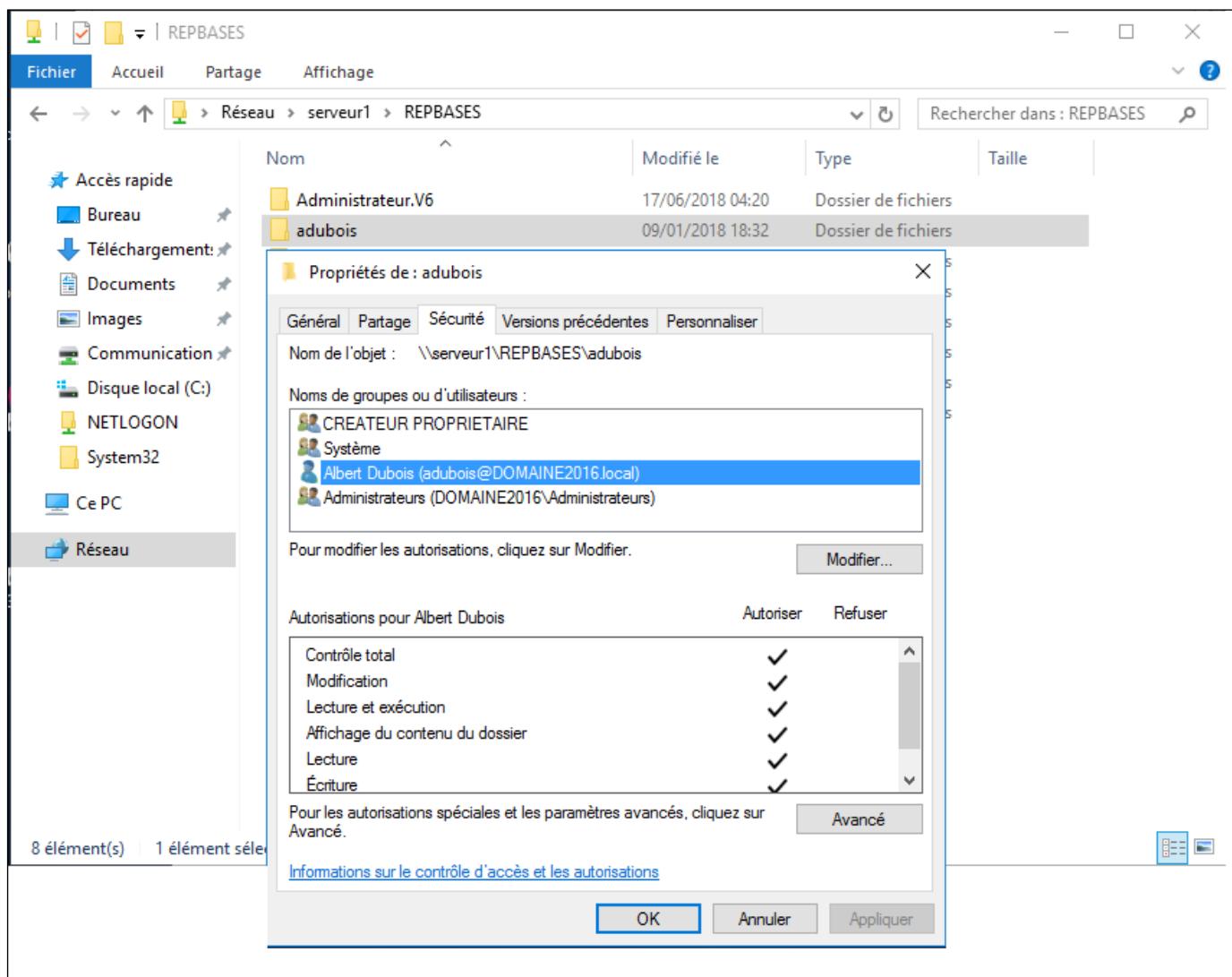


Étape 5 : création d'un nouvel utilisateur avec son dossier personnel de base

Nous allons créer les deux utilisateurs suivants :

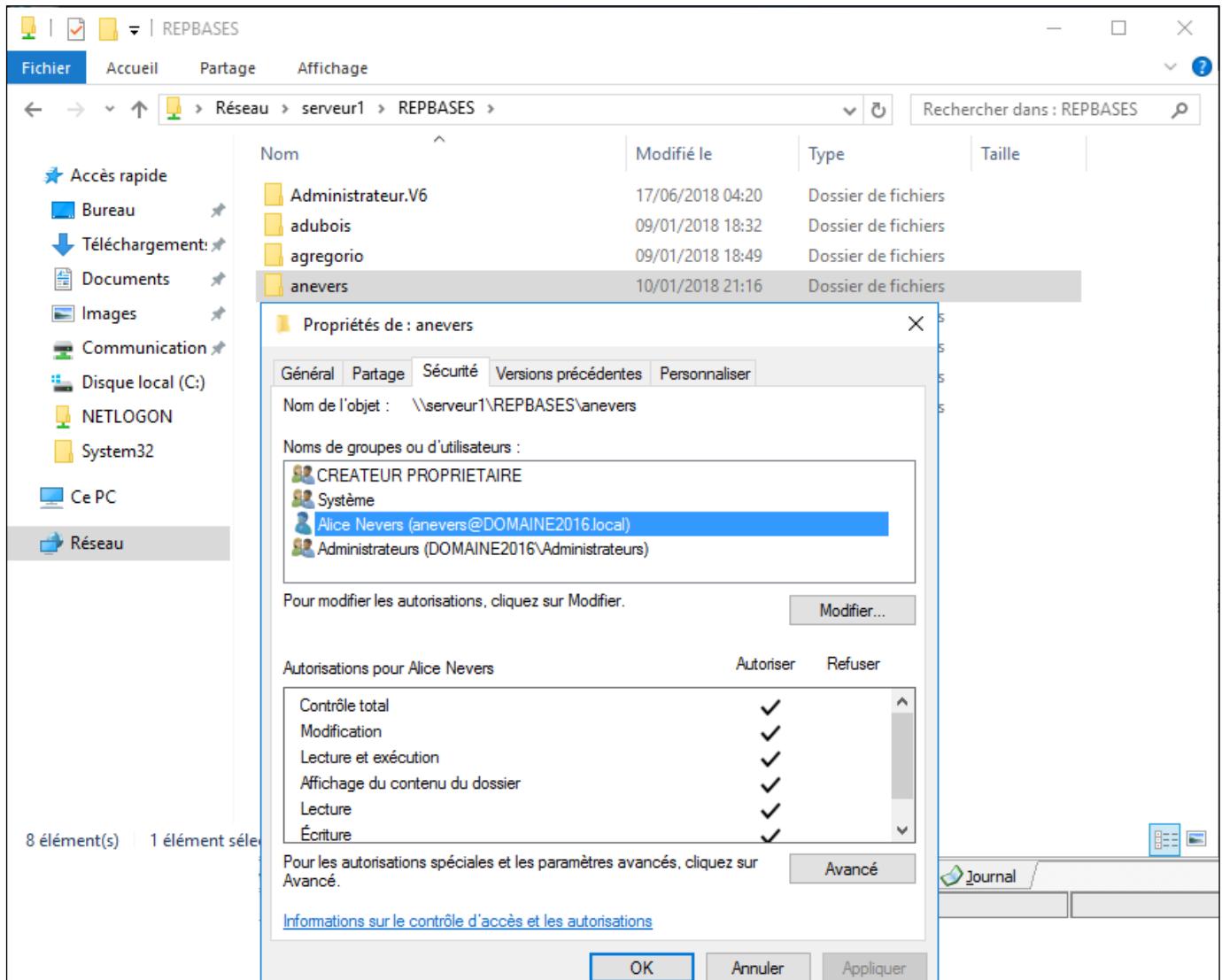
Nom et prénom	Nom d'ouverture de session	Nom du dossier personnel	Mot de passe
Albert Dubois	adubois	adubois	Windows2019
Alice Nevers	anevers	anevers	Windows2019

- a. Créer l'utilisateur **Albert Dubois** ayant pour nom d'ouverture de session *adubois*, mot de passe *Windows2019* (décocher la case *L'utilisateur doit changer de mot de passe à la prochaine ouverture de session* ; cocher la case *Le mot de passe n'expire jamais*), et ayant un dossier personnel de base *adubois* dans REPBASES ;
- b. Vérifier avec l'explorateur Windows depuis le serveur, que le dossier *adubois* a bien été créé dans C:\REPBASES, et que, mis à part les groupes Administrateurs, CREATEUR PROPRIETAIRE, et Système (représentés par), Albert Dubois est le seul utilisateur (représenté par) ayant des autorisations sur ce dossier (vérifier qu'il en a bien le Contrôle total, donc tous les droits !) :



- c. Sur PC1, ouvrir une session pour *adubois*, puis vérifier que cet utilisateur n'a accès qu'à son dossier et non aux dossiers des autres (il ne doit pas pouvoir accéder au dossier *cdupont*!).

- d. Créer l'utilisateur **Alice Nevers** ayant pour nom d'ouverture de session *anevers*, mot de passe *Windows2019* (décocher la case *L'utilisateur doit changer de mot de passe à la prochaine ouverture de session* ; cocher la case *Le mot de passe n'expire jamais*), et ayant un dossier personnel de base *anevers* dans REPBASES ;
- e. Vérifier avec l'explorateur Windows depuis le serveur, que le dossier *anevers* a bien été créé dans C:\REPBASES, et que, mis à part les groupes *Administrateurs*, *CREATEUR PROPRIETAIRE*, et *Système* (représentés par), Alice Nevers est le seul utilisateur (représenté par) ayant des autorisations sur ce dossier (vérifier qu'il en a bien le Contrôle total, donc tous les droits !).



- f. Sur PC1, ouvrir une session pour *anevers*, puis vérifier que cet utilisateur n'a accès qu'à son dossier et non aux dossiers des autres (il ne doit pas pouvoir accéder au dossier *cdupont*!).

***TP 1 SI7 : Gestion de parc informatique
Installation et configuration de GLPI***

Objectifs

Le DSI de GSB souhaite gérer son parc informatique à l'aide d'une solution open source (gratuite).

Le cahier des charges prévoit les contraintes suivantes :

- c. inventaire des différents matériels par remontée automatique périodique des informations de chaque matériel dans une base centralisée du système retenu pour la gestion de parc ;
- d. Importation de la base de données LDAP des utilisateurs du contrôleur de domaine GSB vers le système de gestion de parc (pour ne pas avoir à ressaisir les utilisateurs) ;
- e. gestion des pannes et interventions et suivi financier de chaque matériel avec calcul du TCO.

Schéma du réseau

Eléments techniques

- Téléchargement de .NET Framework 4.5 : <https://www.microsoft.com/en-us/download/details.aspx?id=42642>
 - Téléchargement du SGBD Mysql : <http://www.mysql.fr/>
 - Téléchargement du package redistribuable Microsoft Visual C++ : <http://www.microsoft.com/en-us/download/details.aspx?id=30679>
 - Téléchargement de PHP pour Windows : <http://windows.php.net/index.php>
 - Téléchargement de PHP Manager : <http://phpmanger.codeplex.com/releases/view/69115>
 - Téléchargement et documentation de GLPI : <http://www.glpi-project.org/?lang=fr>
 - Téléchargement et documentation de FusionInventory : <http://fusioninventory.org/documentation/>
-
- Identifiants et mots de passe à utiliser :
 - Serveur Windows 2016 : *Administrateur/Windows2016*
 - SGBD Mysql : *root/root*
 - Routeur-paraf feu PfSense : *admin/pfsense*
 - Serveur Debian : *root/root* et *debian/debian*
 - Windows 10 (administrateur local) : *sio/sio*

Prérequis

- b. Vérifier en préambule que le domaine *GSB.local* est bien créé sur le serveur Windows 2016 **SERVEUR1**, et que les utilisateurs suivants sont créés dans le conteneur *Users* (sinon les créer en décochant la case *L'utilisateur doit changer de mot de passe à la prochaine ouverture de session*) :

<i>Nom et prénom</i>	<i>Nom d'ouverture de session</i>	<i>Mot de passe</i>
Alex Durois	adurois	Windows2016
Alice Nevers	anevers	Windows2016
Arthur Rabelais	arabelais	Windows2016
Kevin Berry	kberry	Windows2016

- c. Vérifier que **SERVEUR2** est bien connecté au domaine GSB.local

Travail à faire

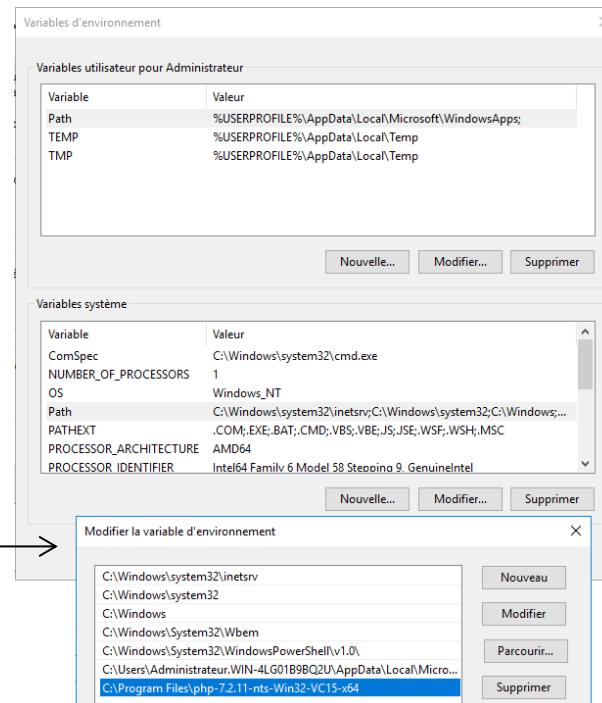
A - Installation de l'infrastructure logicielle : IIS, Mysql, PHP, et GLPI

Préparer et effectuer l'installation de GLPI sur le serveur membre SERVEUR2 (qui n'est pas contrôleur de domaine mais membre de GSB.local) 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.

Etapes à suivre :

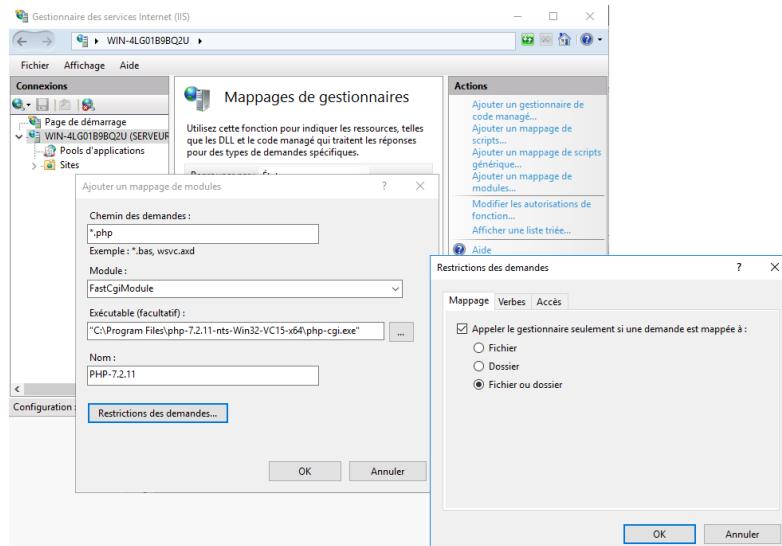
- a. Installer le rôle *Serveur web IIS* avec les services de rôle par défaut et le service de rôle *CGI*.
- b. Installer ensuite PHP 7 :
 - Copier la dernière version (Non-Thread Safe (NTS)) du dossier PHP 7 fourni (*php-7.2.11-nts-Win32-VC15-x64*) dans le dossier *C:\Program Files* (en Français *Programmes*) ;
 - 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*) ;
- c. 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\64\instantclient_12_1\ sdk\shared" "--with-oci8-12c=c:\builddeps_aux\oracle\64\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* !

Les trois sous-étapes suivantes permettent d'installer et d'utiliser Wincache, sensé améliorer les performances du PHP. Elles ne sont absolument pas indispensables dans le cadre de ce TP.

- Copier la dernière version du dossier de l'extension WinCache pour PHP fourni (*wincache-2.0.0.8-dev-7.2.beta2-nts-vc15-x64*) dans le sous-dossier *ext* du dossier PHP, c'est à dire *C:\Program Files\php-7.2.11-nts-Win32-VC15-x64\ext* (en fait, seul le fichier *php_wincache.dll* sera utilisé) ;
- Avec le bloc-notes, modifier le fichier **php.ini** et ajouter la ligne suivante à la fin du fichier :
extension = php_wincache.dll
- Si besoin, modifier les directives suivantes dans *php.ini* :

```
[opcache]
; Determines if Zend OPCache is enabled
opcache.enable=On

; Determines if Zend OPCache is enabled for the CLI version of PHP
opcache.enable_cli=On
```

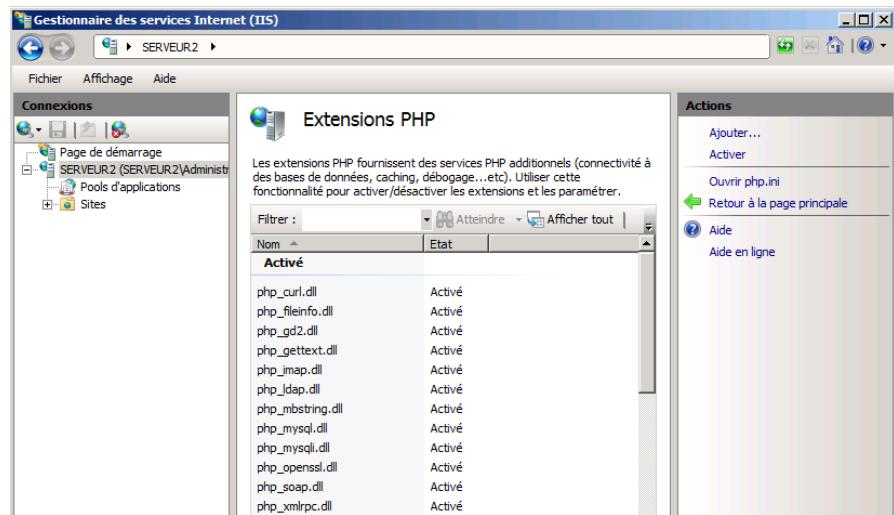
c. Installer le SGBD *Mysql* :

- a. Si l'installation se fait sur un serveur Windows Server 2008, installer d'abord le framework *.NET Framework 4.5* nécessaire pour le fonctionnement de *Mysql* (inutile sous Windows 2012 ou 2016).
- b. Installer la version MySQL Community Server (installer le serveur uniquement (et non tout le package)).
- c. Si besoin, installer PHPMyAdmin (qui nécessite PHP déjà installé).

- d. 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).



- e. 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*

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

- g. 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/

- h. 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).

Pour installer l'agent FusionInventory sous Windows et Pfsense, suivre les indications de l'[Annexe 3](#)

- i. Vérifier dans GLPI, l'historique des remontées des données par les agents ; pour cela sélectionner *Plugins / FusionInventory*, sélectionner alors *Général / Gestion des agents* : on voit ainsi les dernières remontées (on peut cliquer sur une machine et consulter l'historique de ses remontées, et éventuellement la restaurer si besoin !).

Glpi

The screenshot shows the Glpi software interface for managing IT assets. The top navigation bar includes links for Accueil, Parc, Assistance, Gestion, Outils, Plugins, and Administration. The main content area displays a table of computer assets with the following columns: Nom, Statut, Fabricant, Numéro de série, Type, Modèle, Système d'exploitation, Dernière modification, Composants - Processeur, and Réseau - IP. There are four entries listed:

Nom	Statut	Fabricant	Numéro de série	Type	Modèle	Système d'exploitation	Dernière modification	Composants - Processeur	Réseau - IP
PC1	VMware, Inc.	Vmware-42 0b 08 fa 6e 5f 94 71-c7 74 bc cf ee 63 af 68	Other	VMware Virtual Platform	Microsoft Windows 7 Professionnel	2017-02-06 14:42	Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz	192.168.3.12 fe80::608a:5f32:ae64:db50	
SERVEUR1	VMware, Inc.	Vmware-42 0b 6d 8a 41 57 02 71-63 67 12 9d fe f7 e6 a0	Other	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	2017-02-06 14:31	Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz	fe80::ad1f:778a:fc7d:da6 192.168.3.1	
SERVEUR2	VMware, Inc.	Vmware-42 0b 68 44 71 f4 ab 5d-87 69 c5 3a 27 44 c3 47	Other	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	2017-02-06 14:33	Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz	192.168.3.2 fe80::959b:2e3:db4c:53e6	
SERVEUR6	VMware, Inc.	Vmware-42 0b 51 ff 54 25 f4 7d-4f cd 3c c4 77 4b a0 fb	Other	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	2017-02-06 14:36	Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz	192.168.1.1 fe80::1042:9d2d:cf28:5839	

At the bottom left, a message says "Terminé, mais il existe des erreurs sur la page." At the bottom right, it shows "Intranet local | Mode protégé : désactivé" and a zoom level of "100%".

B -Importation dans GLPI des utilisateurs de l'annuaire LDAP (Active Directory) de GSB

Configurer cette importation qui sera faite périodiquement sur demande par l'administrateur de GLPI.

Etapes à suivre : Tutoriel d'importation dans GLPI des utilisateurs d'un annuaire LDAP (Active Directory) : [Annexe 2](#)

Annexe 1 : Tutoriel pour la première connexion à GLPI

Pour la première connexion à GLPI, procéder comme suit :

- a. Rentrer sous l'interface web de GLPI avec le navigateur, à l'adresse <http://localhost/glpi>
- b. Après avoir sélectionner la langue *Français*, configurer la connexion à la base de données :

Serveur Mysql: *localhost*
Utilisateur Mysql : *root*
Mot de passe Mysql : *root*

- c. Créer ensuite une nouvelle base de données de nom *glpi*
- d. Après avoir noté les identifiants et mots de passe, on peut maintenant utiliser GLPI et entrer dans le système avec l'identifiant *glpi* et le mot de passe *glpi*
- e. Modifier immédiatement les mots de passe de ces quatre utilisateurs (*glpi*, *post-only*, *tech* et *normal*) en leur donnant à tous le même : **Windows2016**

Actions	Identifiant	Nom de famille	Adresses de messagerie	Téléphone	Lieu	Actif
<input type="checkbox"/>	glpi					Oui
<input type="checkbox"/>	normal					Oui
<input type="checkbox"/>	Plugin_FusionInventory					Oui
<input type="checkbox"/>	post-only					Oui
<input type="checkbox"/>	tech					Oui

- f. Vérifier et valider la liste des informations devant apparaître pour chaque matériel (Informations générales) :

Tous <input type="button" value="Oui ▾"/>					
Informations générales		Composants		Informations administratives OCSNG	
Nom	<input type="button" value="Oui ▾"/>	Processeur	<input type="button" value="Oui ▾"/>	Numéro d'inventaire	<input type="button" value="HARDWARE_ID ▾"/>
Système d'exploitation	<input type="button" value="Oui ▾"/>	Mémoire	<input type="button" value="Oui ▾"/>	Lieu	<input type="button" value="fields_4 ▾"/>
Numéro de série du système d'exploitation	<input type="button" value="Oui ▾"/>	Disque dur	<input type="button" value="Oui ▾"/>	Groupe	<input type="button" value="Pas d'import ▾"/>
Numéro de série	<input type="button" value="Oui ▾"/>	Carte réseau	<input type="button" value="Oui ▾"/>	Usager numéro	<input type="button" value="Pas d'import ▾"/>
Modèle	<input type="button" value="Oui ▾"/>	Carte graphique	<input type="button" value="Oui ▾"/>	Réseau	<input type="button" value="Pas d'import ▾"/>
Fabricant	<input type="button" value="Oui ▾"/>	Carte son	<input type="button" value="Oui ▾"/>		
Type	<input type="button" value="Oui ▾"/>	Lecteurs	<input type="button" value="Oui ▾"/>		
Domaine	<input type="button" value="Oui ▾"/>	Modems	<input type="button" value="Oui ▾"/>		
Usager	<input type="button" value="Oui ▾"/>	Ports	<input type="button" value="Oui ▾"/>		
Commentaires	<input type="button" value="Oui ▾"/>				
IP	<input type="button" value="Oui ▾"/>				
UUID	<input type="button" value="Oui ▾"/>				
Moniteurs					
Commentaires	<input type="button" value="Oui ▾"/>	<input type="button" value="Sauvegarder"/>			

Annexe 2 : Tutoriel d'importation dans GLPI des utilisateurs d'un annuaire LDAP

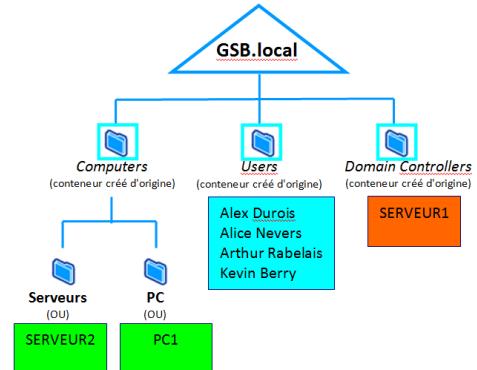
Au lieu de créer les utilisateurs un par un dans GLPI, nous allons importer ceux déjà créés dans l'Active Directory du domaine Windows 2016 (Active Directory est en effet un annuaire LDAP).

- a. 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 lien *Annuaires LDAP*) (ajouter un nouvel annuaire en cliquant sur le bouton “+” situé dans la barre de menu) :

Nom (du serveur LDAP) :	SERVEUR1
Serveur par défaut :	Oui
Actif :	Oui
Serveur (adresse IP) :	192.168.3.1
Port :	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 :	<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).



GLPI - Annuaire LDAP - Windows Internet Explorer

http://localhost/glpi/front/authldap.form.php?id=1

Favoris Sites suggérés Galerie de composants W...

GLPI - Annuaire LDAP

Parc Assistance Gestion Outils Plugins Administration Configuration

Annuaire LDAP - SERVEUR1 - ID 1

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	(&(objectClass=user)(objectCategory=person))((userAccountControl:1.2.840.113556.1.4.803:=0))		
BaseDN	CN=Users,DC=GSB,DC=local		
DN du compte (pour les connexions non anonymes)	CN=Administrateur,CN=Users,DC=GSB,DC=local		
Mot de passe du compte (pour les connexions non anonymes)	<input type="password"/>	Effacer	Champ de l'identifiant samaccountname
Commentaires	<div style="height: 40px; border: 1px solid #ccc; margin-top: 5px;"></div>		

Sauvegarder Supprimer

Annuaire LDAP

Tester Utilisateurs Groupes Informations avancées Réplicats Historique (3) Tous

- 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*) :

Identifier	Nom de famille	Dernière mise à jour dans l'annuaire LDAP	Date
kberry		2013-07-21 14:26	
arabelais		2013-07-21 23:50	
anevers		2013-08-19 18:46	
adurois		2013-07-21 15:40	

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

Identifier	Nom de famille	Adresses de messagerie	Téléphone	Lieu	Actif
adurois	Durois				Oui
anevers	Nevers				Oui
arabelais	Rabelais				Oui
glpi					Oui
kberry	Berry				Oui
normal					Oui
Plugin_FusionInventory					Oui
post-only					Oui
tech					Oui

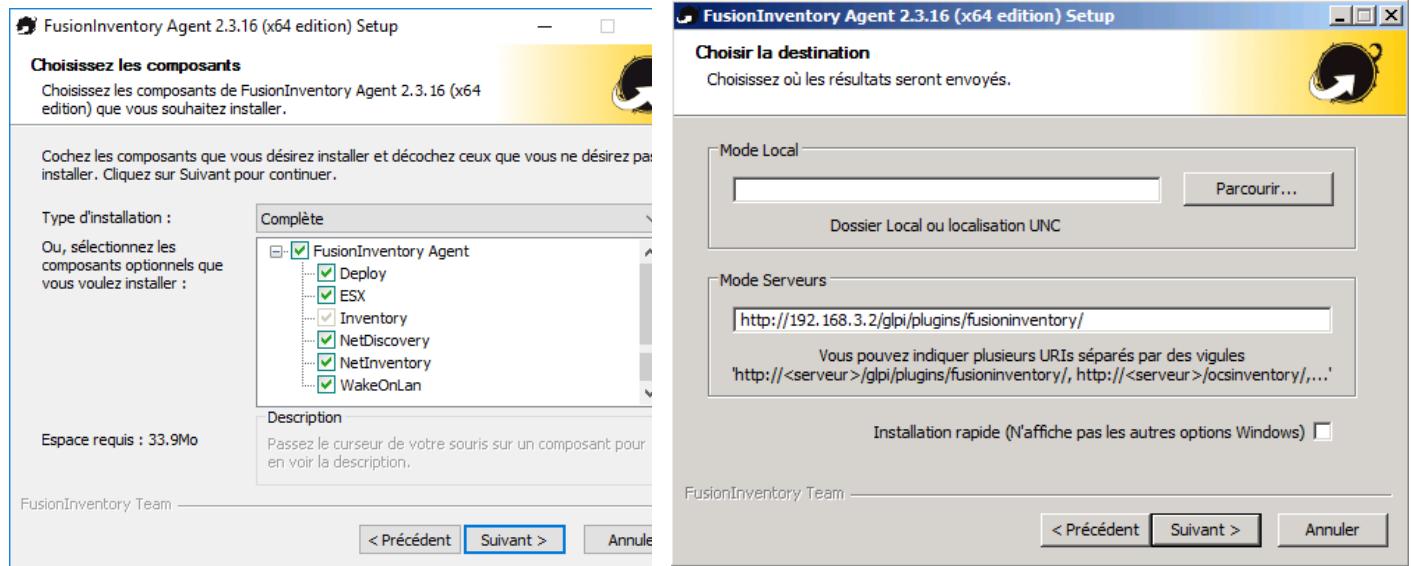
Cf documentation complète sur le site de GLPI : <http://www.glpi-project.org/wiki/doku.php?id=fr:config:ldap>

Annexe 3 : Installation de l'agent FusionInventory sous Windows et sous Pfsense

a - Installation et exécution de l'agent FusionInventory sous Windows

Installation manuelle de l'agent

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



Installation de l'agent par GPO :

(GPO *Configuration Ordinateur Stratégie Paramètres Windows* pour lancer automatiquement un script .bat permettant d'installer l'agent au démarrage de la machine)

Utiliser les options d'installation en ligne de commande suivantes :

/acceptlicense

Accepter par l'utilisateur les conditions d'utilisation de la licence de l'agent FusionInventory

/execmode=mode

Fixer le mode d'exécution de l'agent (en mode *Service*, l'agent s'exécutera en tant que service Windows ; en mode *Task*, l'agent s'exécutera en tant que tâche Windows)

/runnow

Lancer l'exécution de l'agent immédiatement après l'installation

/server=URI[,URI[...]]

Renvoyer les résultats de l'exécution de l'agent au serveur spécifié (ici :

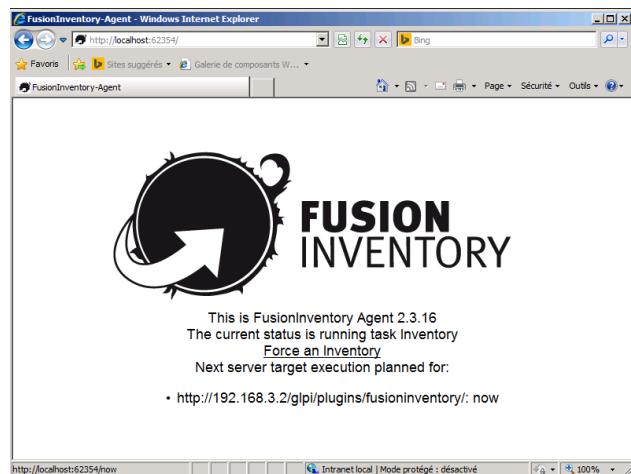
<http://192.168.3.2/glpi/plugins/fusioninventory/>

/S

Exécuter l'installation de l'agent en mode silencieux

Sur chaque poste, l'agent FusionInventory doit ainsi être installé.

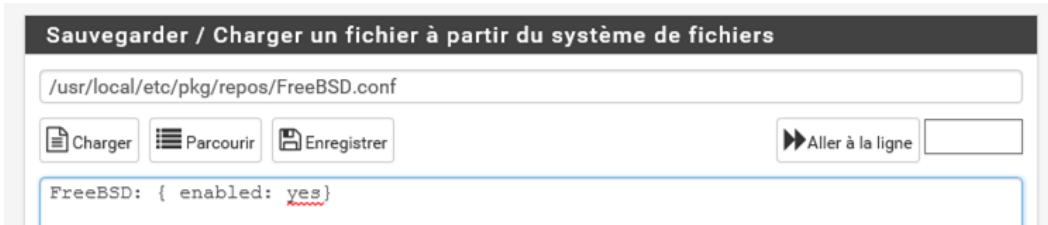
Exécution de l'agent **sur chaque poste du réseau** afin de remonter les données de chaque machine automatiquement vers le serveur.



b - Installation et exécution de l'agent FusionInventory sous PfSense

- Préparer l'installation de l'agent FusionInventory sur PfSense :

- A partir de l'interface graphique de Pfsense ([Diagnostics Edit File](#)), éditer le fichier `/usr/local/etc/pkg/repos/FreeBSD.conf` et mettre le dépôt FreeBSD à yes :



- Faire de même pour le fichier `/usr/local/etc/pkg/repos/pfSense.conf` : mettre le dépôt FreeBSD à yes ;

- Effectuer l'installation de l'agent FusionInventory sur PfSense, en exécutant la commande suivante directement sur la machine Pfsense (8 Shell) :

```
pkg install p5-FusionInventory-Agent p5-LWP-Protocol-https p5-Proc-Daemon
```

```
FreeBSD/amd64 (pfSense.localdomain) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 9becbc1e84b1546b5cc9
*** Welcome to pfSense 2.4.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4: 192.168.1.254/24
LAN (lan)      -> em1      -> v4: 10.0.2.254/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 8
[2.4.2-RELEASE]#root@pfSense.localdomain:~# pkg install p5-fusioninventory-agent p5-lwp-protocol-https p5-proc-daemon
```

- A partir de l'interface graphique de Pfsense ([Diagnostics Edit File](#)), ré-éditer les deux fichiers précédents et remettre le dépôt FreeBSD à no dans les deux fichiers.
- Créer le dossier suivant à partir de l'interface graphique de Pfsense ([Diagnostics Command Prompt](#)) :

```
mkdir -p /usr/local/etc/fusioninventory/
```

- Effectuer la configuration de l'agent en créant le fichier `agent.cfg` dans le dossier que l'on vient de créer, à partir de l'interface graphique de Pfsense ([Diagnostics Edit File](#)) :

Le fichier `agent.cfg` doit contenir les lignes suivantes :

```
server= http://192.168.3.2/glpi/plugins/fusioninventory/
no-task=ESX,Collect,WakeOnLan,NetDiscovery,Deploy,NetInventory
```

- f. Exécuter un premier inventaire manuel, en exécutant la commande suivante à partir de l'interface graphique de PfSense (*Diagnostics Command Prompt*) :

```
/usr/local/bin/fusioninventory-agent --debug
```

(Source : https://wiki.fws.fr/tuto/linux_divers/installer_fusioninventory_pfsense)

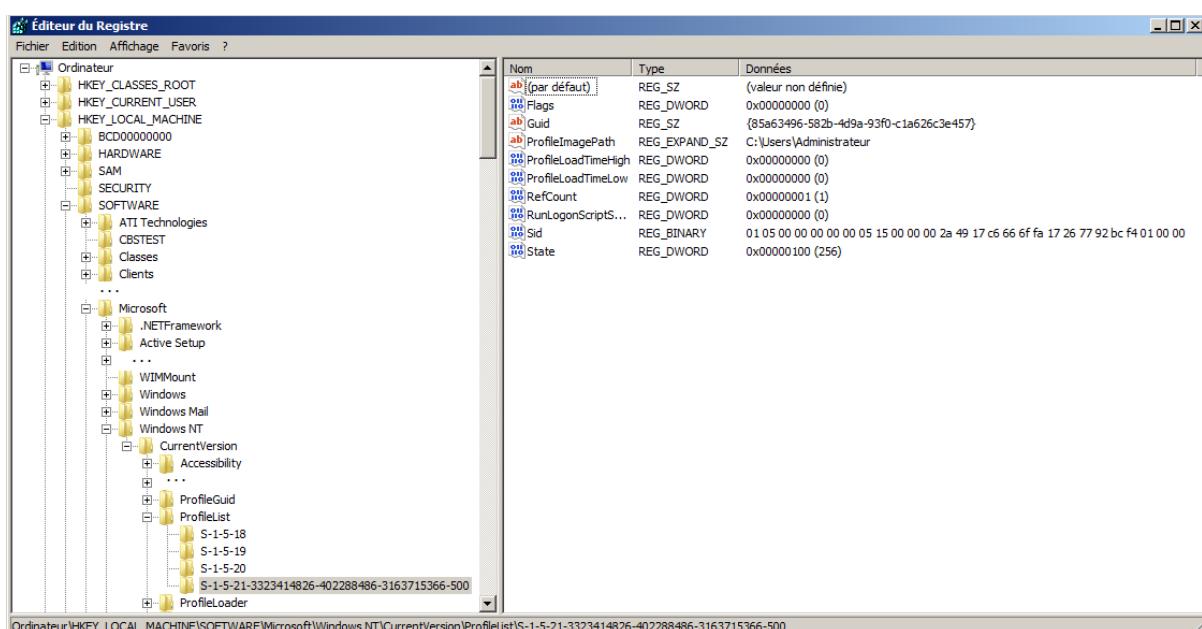
Annexe 4 : Modification du SID du serveur SERVEUR2 (si besoin)

Le SID pour **Security Identifier** (en Français **identifiant de sécurité**) est utilisé dans un environnement Microsoft Windows Server et est un identifiant unique attaché à une machine, un utilisateur ou un groupe de sécurité. Il doit être unique sous peine de rencontrer un jour ou l'autre des problèmes. L'environnement Microsoft se base sur cette information pour autoriser ou non l'accès à des ressources locales ou de l'annuaire d'où la nécessité de respecter ce principe d'unicité au sein d'un groupe de travail ou d'un domaine.

Pour connaître le SID correspondant à l'Administrateur du système, on peut télécharger un petit programme nommé *PsGetSid* (à l'adresse <https://technet.microsoft.com/en-us/sysinternals/bb897417.aspx>) ou consulter la base de registres à la rubrique

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList ;

sous la clé **ProfileList**, on voit les identificateurs de sécurité. En sélectionnant chacun d'eux individuellement, on peut consulter la rubrique **valuée** et voir quel nom d'utilisateur est associé à ce SID particulier ; le SID du compte Administrateur du système ou du domaine commence par S-1-5-21 :

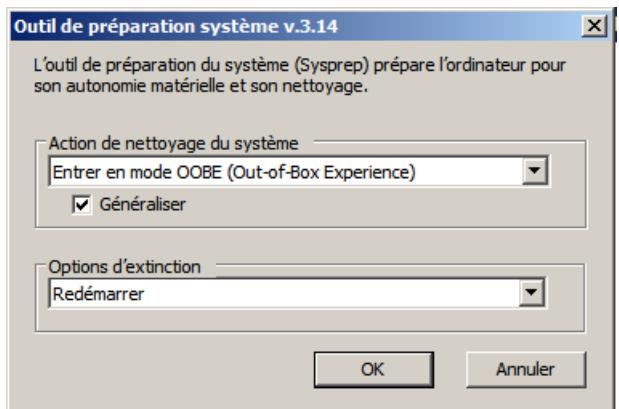


```
C:\Users\Administrateur\Desktop\PSTools>psgetsid
PsGetSid v1.44 - Translates SIDs to names and vice versa
Copyright <C> 1999-2008 Mark Russinovich
Sysinternals - www.sysinternals.com

SID for \\SERVEUR:
S-1-5-21-3323414826-402288486-3163715366-500
```

Travaillant avec des machines virtuelles sous VMWare, il est possible que le SID de l'administrateur du nouveau serveur soit le même que celui de la machine virtuelle SERVEUR. Nous allons donc modifier le SID sur ce nouveau serveur :

- a. Lancer la commande sysprep afin de modifier le SID. L'exécutable se trouve dans le répertoire c:\Windows\System32\sysprep\
- b. Une fois sysprep lancé, choisir l'option «**Entrer en mode OOB**E» et surtout cocher «**Généraliser**» car sinon le SID ne changera pas :
- c. Sysprep exécuté, la machine redémarre et Windows propose de paramétrier le système comme s'il s'agit de son premier démarrage (choix du pays, du clavier, de l'heure, ...).



Rappels sur LDAP :

Lightweight Directory Access Protocol (LDAP) est à l'origine un protocole pour les systèmes d'annuaires.

LDAP est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leurs valeurs.

La tendance actuelle est d'utiliser le nommage DNS pour les éléments de base de l'annuaire :

1. la racine, le domaine, le sous-domaine, ... : DC (Domain Components)
2. le conteneur créé par défaut (Computers, Users, ...) : CN (Common Name)
3. l'unité d'organisation : OU (Organizational Unit)
4. une personne : CN (Common Name) ou l'identifiant d'un utilisateur : UID (User IDentifier).

L'assemblage de tous les composants (du plus précis au plus général) d'un nom forme son DN (Distinguished Name).

Exemple :

```
dc=org
  |
dc=example
  /   |   \
ou=people  ou=groups  cn=Users
  |           |
uid=toto      cn=jiji
```

Le DN de toto est uid=toto,ou=people,dc=example,dc=org (sans espaces !).
Le DN de jiji est cn=jiji,cn=Users,dc=example,dc=org (sans espaces !).

Un client LDAP ouvre une session LDAP en se connectant sur le port TCP 389 du serveur LDAP.

BTS SIO 2
des services

SISR3 : Exploitation

TP 29 : VPN entre un client distant et un serveur OpenVPN avec authentification LDAP

Objectifs

Le DSI de GSB souhaite mettre à disposition de ses agents itinérants extérieurs plusieurs applications installées sur les serveurs GSB et utilisables à distance grâce à une connexion sécurisée VPN SSL/TLS de type nomade (entre un client distant et un serveur VPN).

Le serveur VPN sera installé sur le routeur-parefeu PfSense (il aurait aussi pu être installé sur un serveur indépendant placé dans une DMZ).

Les clients VPN seront installés sur des machines Windows ; ils recevront une adresse sur le réseau par défaut 192.168.100.0/24 et auront accès au réseau 192.168.3.0/24.

OpenVPN fonctionne sous un mode PKI (Public Key Infrastructure), c'est à dire avec sa propre autorité de certification. Selon ce mode, le serveur OpenVPN possède un certificat (avec une clé publique et une clé privée) qui lui est propre. Un certificat d'autorité de certification (master CA) et une clé privée sont utilisés pour signer les certificats de ce serveur VPN.

Dans ce TP, chaque client sera authentifié non pas par un certificat client ou un compte local créé sur le serveur VPN, mais par l'identifiant et le mot de passe de son compte-utilisateur créé dans l'Active Directory Windows 2019 du serveur de domaine GSB (qui est à la norme LDAP).

Travail à faire

A - Configuration du serveur VPN

Préparer et effectuer l'installation du VPN nomade en tenant compte des contraintes suivantes :

- t. Le serveur VPN sera OpenVPN ; il sera configuré sur le ROUTEUR-PAREFEU PfSense qui intègre d'origine OpenVPN. Il gérera sa propre autorité de certification et permettra de créer le certificat du serveur OpenVPN.
- u. On utilisera le port 1195 (et non 1194 qui est utilisé par défaut, mais qui est déjà pris) du serveur OpenVPN pour la transmission sécurisée.
- v. Dans le VPN, le serveur VPN recevra l'adresse virtuelle 192.168.100.1/24

B - Configuration du client VPN nomade

Préparer et effectuer l'installation du VPN nomade en tenant compte des contraintes suivantes :

- w. Chaque machine Windows souhaitant se connecter au serveur OpenVPN utilisera le client VPN *OpenVPN GUI for Windows* ;
- x. Chaque utilisateur utilisera l'identifiant et le mot de passe de son compte-utilisateur Windows 2019 pour s'authentifier lors de la connexion VPN.
 - On testera la connexion VPN depuis un poste test de la salle R211.
 - Dans le VPN, un client recevra une adresse virtuelle à partir de 192.168.100.2/24.

C -Configuration des applications pour être utilisables à distance, tests et vérification du tunnel (analyse de trames avec Wireshark)

- y. Les applications utilisables à distance seront installées sur le serveur hôte de session de bureau à distance SERVEUR1 et exécutées grâce à la fonction *Connexion Bureau à distance* des clients distants Windows ; on utilisera *Cisco Packet Tracer* comme application-test distante.
- z. On utilisera Wireshark pour vérifier que le tunnel est bien mis en place.

Eléments techniques

j.

Téléchargement du client OpenVPN GUI for Windows :

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

- k. Tutoriel pour la création d'une autorité de certification sur le routeur-parefeu PfSense, et la création du certificat de serveur : [Annexe 1](#)

aa. Tutoriel pour la configuration du serveur OpenVPN sur le routeur-parefeu PfSense : [Annexe 3](#)

bb. Tutoriel pour l'exportation de la configuration du client depuis PfSense : [Annexe 4](#)

cc. Tutoriel pour l'installation du client OpenVPN sur un poste client : [Annexe 5](#)

dd. Tutoriel pour la vérification du tunnel : [Annexe 6](#)

ee. Identifiants et mots de passe à utiliser :

1. Serveur Windows 2019 : *Administrateur/Windows2019*
2. SGBD Msql : *root/root*
3. Routeur-parefeu PfSense : *admin/pfsense*
4. Serveur Debian : *root/root* et *debian/debian*
5. Windows 10 (administrateur local) : *sio/sio*

Remarques importantes

Tous les certificats créés dans ce TP auront les caractéristiques suivantes :

- leur clé publique aura une taille de 2048 bits (soit 256 octets)
- ils utiliseront l'algorithme de hashage SHA à 256 bits (SHA256)
- ils utiliseront l'algorithme de chiffrement AES-CBC à 256 bits (AES-256-CBC)

Schéma du réseau

Annexe 1 : Création d'une autorité de certification CA_Acces_VPN sur le routeur-parefeu PfSense avec son certificat ; création du certificat du serveur OpenVPN

- b. Depuis le poste SERVEUR1 par exemple, se connecter à l'interface LAN du routeur-parefeu PfSense pour le configurer, avec le navigateur Mozilla Firefox.
- c. 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**) :

CAs Certificates Certificate Revocation

Create / Edit CA

<u>Descriptive name</u>	<input type="text" value="CA_Acces_VPN"/>
<u>Method</u>	<input type="button" value="Create an internal Certificate Authority"/>
<u>Trust Store</u>	<input type="checkbox"/> Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.
<u>Randomize Serial</u>	<input type="checkbox"/> Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

<u>Key type</u>	<input type="button" value="RSA"/>
	<input type="button" value="2048"/>
	The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
<u>Digest Algorithm</u>	<input type="button" value="sha256"/>
	The digest method used when the CA is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
<u>Lifetime (days)</u>	<input type="button" value="3650"/>
<u>Common Name</u>	<input type="text" value="CA_Acces_VPN"/>
	The following certificate authority subject components are optional and may be left blank.
<u>Country Code</u>	<input type="button" value="FR"/>
<u>State or Province</u>	<input type="text" value="test"/>
<u>City</u>	<input type="text" value="test"/>
<u>Organization</u>	<input type="text" value="test"/>
<u>Organizational Unit</u>	<input type="text" value="e.g. My Department Name (optional)"/>
<input type="button" value="Save"/>	

- d. 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***) :

[CAs](#) [Certificates](#) [Certificate Revocation](#)
Add/Sign a New Certificate
Method
Descriptive name
Internal Certificate
Certificate authority
Key type

The length to use when generating a new RSA key, in bits.

The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm

The digest method used when the certificate is signed.

The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

Lifetime (days)

The length of time the signed certificate will be valid, in days.

Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name

The following certificate subject components are optional and may be left blank.

Country Code
State or Province
City
Organization
Organizational Unit
Certificate Attributes
Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names

Type

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Annexe 3 : 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.

- a. 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*») :

<i>Nom</i>	<i>Nom d'ouverture de session</i>	<i>Mot de passe</i>
User_VPN_LDAP	User_VPN_LDAP	Windows2019

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

- b. 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* :

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

Select a container

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)

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

Select a container

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 currently 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 section containing a checkbox labeled "Use Authentication Server for Shell Authentication". It includes a note: "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: a blue "Save" button and a blue "Save & Test" button.

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

The screenshot shows the results of testing the pfSense LDAP settings. It displays three rows of status information:

Attempted Action	Result IP Address	Status
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 table, a section titled "Organization units found" lists the entry: "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	<div style="border: 1px solid #ccc; width: 150px; height: 100px; margin-bottom: 5px;"></div> <p>Paste in a shared TLS key if one has already been generated.</p>
DH Parameters Length	2048 bit <input type="button" value="▼"/>
<p>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.</p>	
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	<div style="background-color: #0072bc; color: white; padding: 5px; display: inline-block;"> AES-256-GCM AES-128-GCM CHACHA20-POLY1305 </div> <input type="button" value="▲"/> <input type="button" value="▼"/>
<p>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.</p>	
Fallback Data Encryption Algorithm	AES-256-CBC (256 bit key, 128 bit block) <input type="button" value="▼"/>
<p>The algorithm used to encrypt traffic between endpoints when data encryption negotiation is disabled or fails.</p>	
Auth Digest Algorithm	SHA256 (256-bit) <input type="button" value="▼"/>
<p>The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.</p>	
Hardware Crypto	No Hardware Crypto Acceleration <input type="button" value="▼"/>
<p>The hardware cryptographic accelerator to use for this VPN connection, if any.</p>	

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="checkbox"/> 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="checkbox"/> 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.

- Vérifier avec la commande [*Firewall Rules*](#) que ces règles ont bien été créées.
- 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) :

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

- sur l'interface **WAN** :

Floating	WAN	LAN	OpenVPN							
Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
<input 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* :

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)	

Informations Générales

Désactivé Désactiver ce serveur
Définissez cette option pour désactiver ce serveur sans le r

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.

Annexe 4 : Exportation de la configuration du client depuis PfSense

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.

- c. 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 is a section for 'DNS Servers' with a field containing '192.168.216.74'. To the right of this field is a 'DNS Hostname' input box. Below these fields, there is descriptive text about the purpose of DNS servers. At the bottom of the page, there are two buttons: 'Add DNS Server' and a green button labeled '+ Add DNS Server'.

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 :

- d. 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.

- e. 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 Android OpenVPN 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

- f. 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_Acces_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

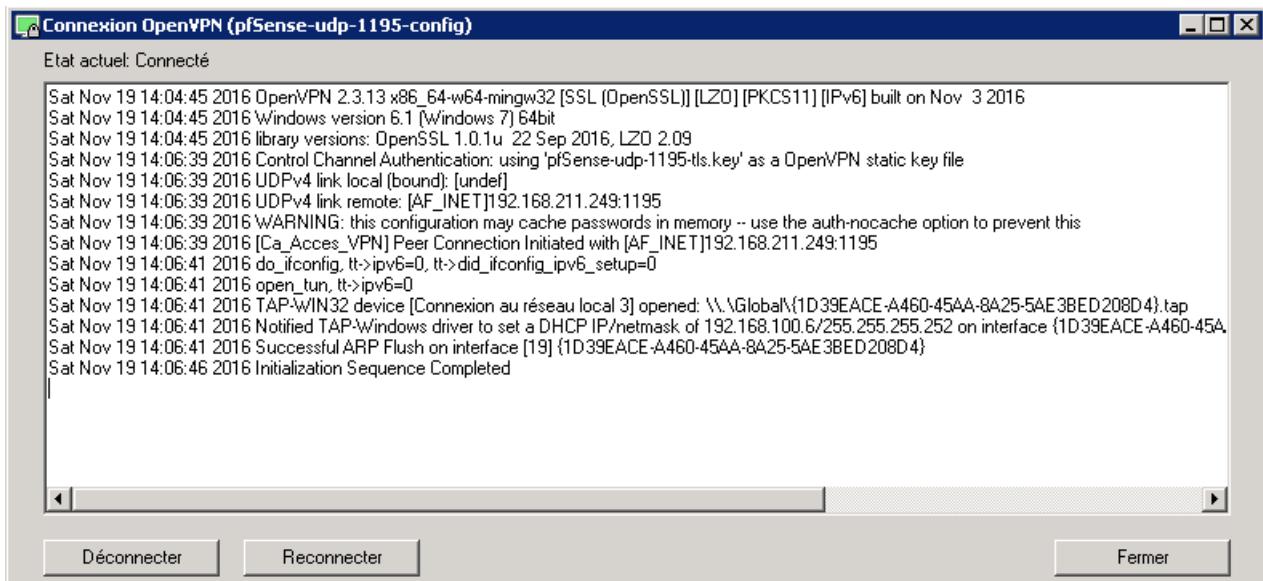
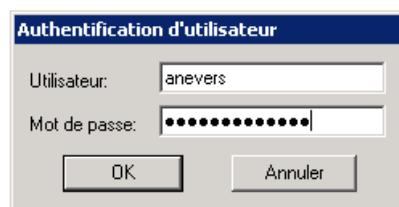
Annexe 5 : Installation du client OpenVPN sur un poste client

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

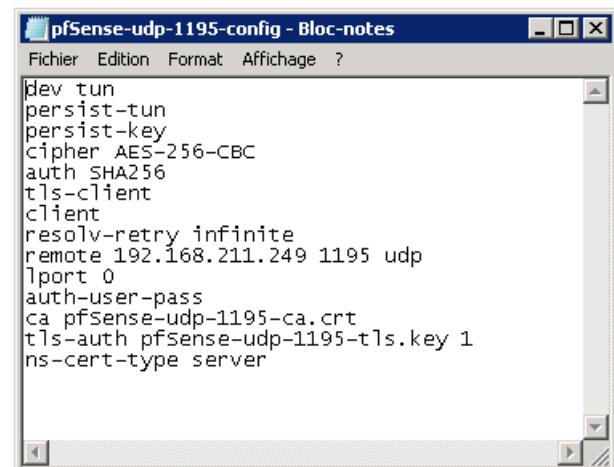
<http://openvpn.net/index.php/open-source/downloads.html>

- 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* :

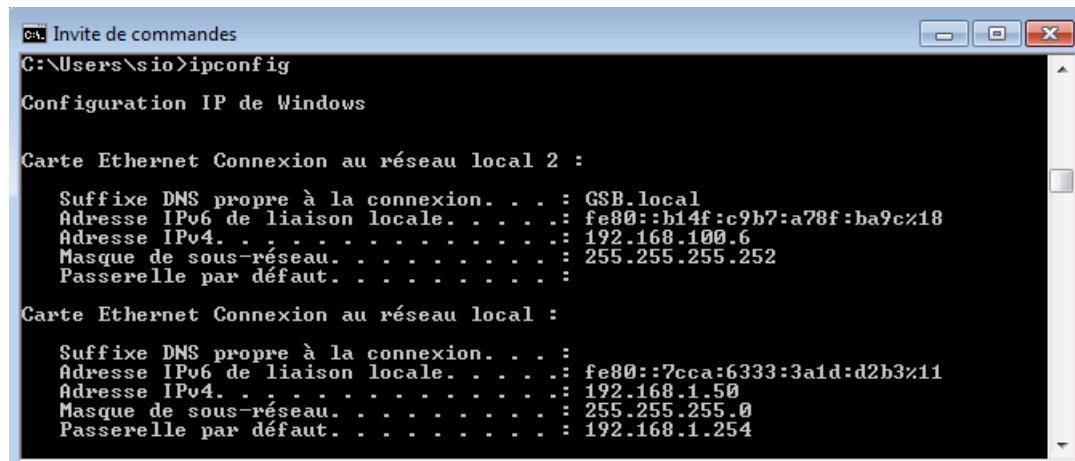


Pour info, le fichier de configuration du client OpenVPN,
de nom *pfSense-udp-1195-config.ovpn*
doit avoir le contenu suivant :



```
pfSense-udp-1195-config - Bloc-notes
Fichier Edition Format Affichage ?
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:\Users\sio>ipconfig

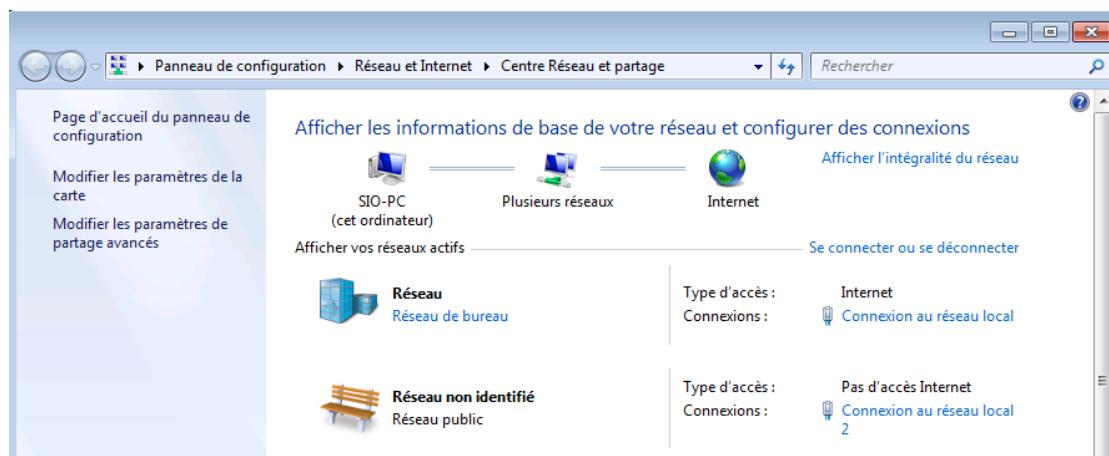
Configuration IP de Windows

Carte Ethernet Connexion au réseau local 2 :

    Suffixe 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 :

    Suffixe DNS propre à la connexion . . . . . : fe80::7cca:6333:3a1d:d2b3%11
    Adresse IPv6 de liaison locale . . . . . : fe80::7cca:6333:3a1d: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 :

  Suffixe DNS propre à la connexion . . . . . :
  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

Favoris | Sites suggérés | Galerie de composants W...

pfsense.localdomain - Diagnostics: Execute command

Sense System Interfaces Firewall Services VPN Status Diagnostics Help

```
$ 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 0xff000000
        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
        syncpeer: 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
```

Execute Shell command

Command: ifconfig

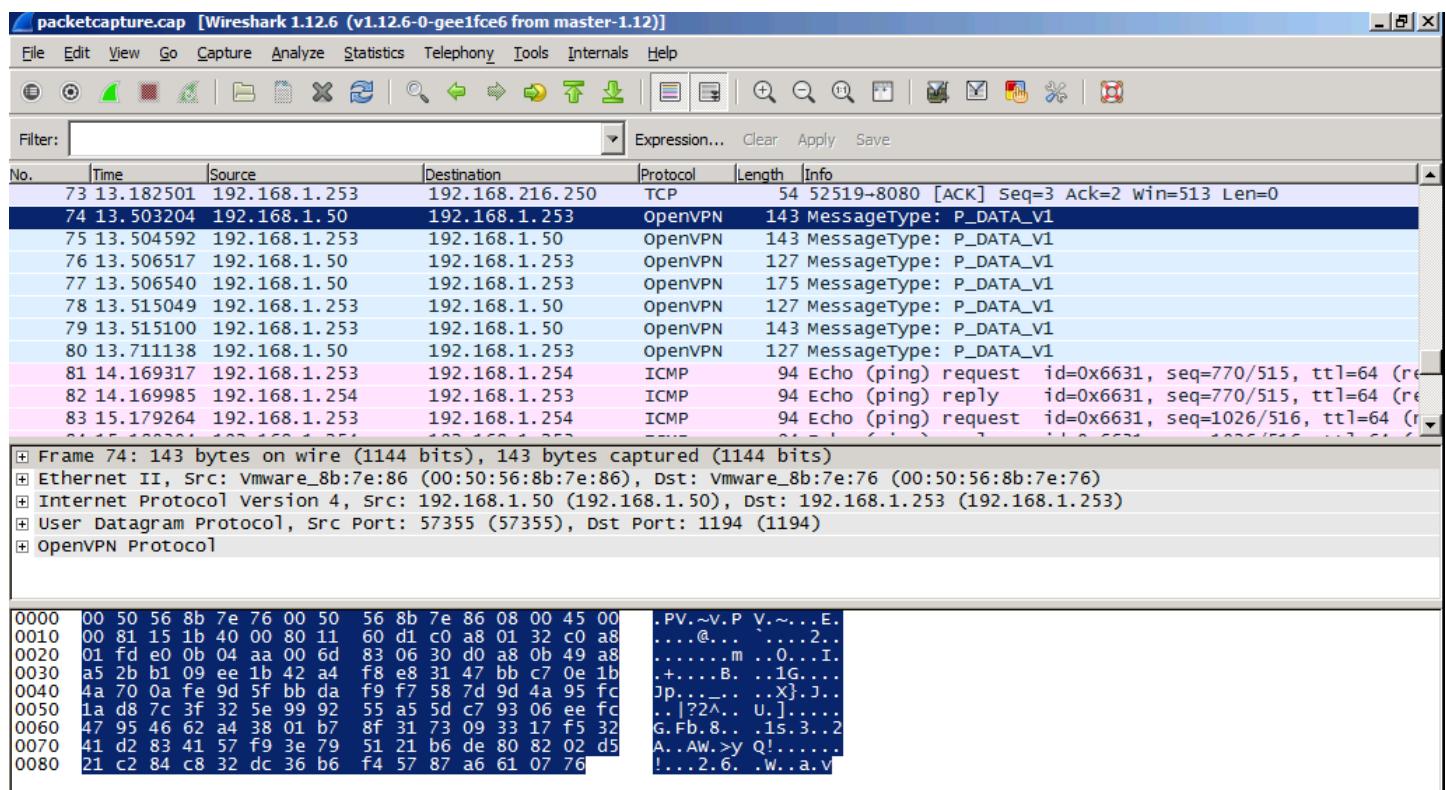
**On peut maintenant, depuis le poste client,
ouvrir une Connexion Bureau à distance vers le serveur 192.168.3.1 ou
toute autre machine du réseau LAN GSB !**

Annexe 6 : Vérification du tunnel

- a. Sur le poste SERVEUR1 par exemple, se connecter à l'interface LAN du routeur-parefeu Pfsense pour le configurer, avec le navigateur Mozilla Firefox ;
- b. Sur le même poste, télécharger et installer le logiciel de captures de trames Wireshark.
- c. Avec la commande PfSense Diagnostics Packet Capture, sélectionner les choix de capture suivants:

Interface (de capture) : WAN
Level of Detail : Full

- d. Lancer la capture avec *Start*.
- e. Depuis un poste client VPN, ouvrir une session de Connexion Bureau à distance sur SERVEUR1, puis la refermer.
- f. Toujours avec la commande PfSense Diagnostic Packet Capture, arrêter la capture avec *Stop* ; cliquer sur *Download capture*, puis sur *Ouvrir* : cela permet de lancer automatiquement Wireshark, et d'ouvrir le fichier de la capture ; vérifier que les trames échangées entre le routeur-parefeu Pfsense et le poste client VPN sont bien des trames OpenVPN.



Liens intéressants :

- <https://www.linkedin.com/pulse/setting-up-pfsense-openvpn-using-user-authentication-trevor-tye>
 - <https://www.ibisc.univ-evry.fr/~petit/Enseignement/AdminSystem/Administration-reseau-avancee/2010-2011-administration-reseau/openvpn.pdf>
 - <https://www.highlInk.com/2013/12/configuring-openvpn-on-pfsense/>
- push "route 192.168.100.0 255.255.255.0" ou cocher redirect gateway ??
<https://superuser.com/questions/1218330/how-to-use-push-route-10-0-0-0-255-255-0-on-pfsense>
<https://networkengineering.stackexchange.com/questions/37522/access-pfsense-lan-through-openvpn>

TP 19 : Installation d'un serveur hôte de session bureau à distance

Objectifs

Le DSI de GSB souhaite installer des serveurs de terminaux (appelés serveurs hôtes de session bureau à distance). Ces serveurs permettront d'exécuter des applications par des utilisateurs distants équipés de clients légers : PC avec navigateur web ou terminaux RDP (Remote Desktop Protocol).

Dans un premier temps, le cahier des charges prévoit l'installation d'un seul serveur hôte de session bureau à distance.

Travail à faire

Configuration du serveur hôte de session bureau à distance sur SERVEUR1

Installer un serveur hôte de session bureau à distance sur le serveur SERVEUR1 contrôleur du domaine GSB avec les contraintes suivantes :

- l.* Tous les utilisateurs du domaine devront pouvoir lancer des sessions bureau à distance sur SERVEUR1 depuis leur PC ;
- m.* Tous les utilisateurs du domaine devront pouvoir accéder aux applications RemoteApp installées sur SERVEUR1 via un navigateur Web ; on utilisera *Cisco Packet Tracer* comme application-test RemoteApp.

Eléments techniques

- Tutoriel de configuration d'un serveur hôte de session bureau à distance:
[Annexe 1](#)
 - Tutoriel d'ouverture d'une application distante RemoteApp depuis un PC :
[Annexe 2](#)
- n.* Identifiants et mots de passe à utiliser :
- | | |
|---|--|
| 6. Serveur Windows 2016 : | <i>Administrateur/Windows2016</i> |
| 7. SGBD Msql : | <i>root/root</i> |
| 8. Routeur-parefeu PfSense : | <i>admin/pfsense</i> |
| 9. Serveur Debian : | <i>root/root</i> et <i>debian/debian</i> |
| 10. Windows 10 (administrateur local) : | <i>sio/sio</i> |

Schéma du réseau

Prérequis

- I. Vérifier en préambule que le domaine *GSB.local* est bien créé sur le serveur Windows 2016 *SERVEUR1*, et que les utilisateurs suivants sont créés (sinon les créer en décochant la case *L'utilisateur doit changer de mot de passe à la prochaine ouverture de session*) :

<i>Nom et prénom</i>	<i>Nom d'ouverture de session</i>	<i>Mot de passe</i>
Alex Durois	adurois	Windows2016
Alice Nevers	anevers	Windows2016
Arthur Rabelais	arabelais	Windows2016
Kevin Berry	kberry	Windows2016

Annexe 1 : 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) !

- e. Ouvrir le Gestionnaire de serveur (s'il n'est pas déjà ouvert) en cliquant sur le bouton  de la barre des tâches actives.
- f. Dans ce tableau de bord, sélectionner Gérer, puis le lien Ajouter des rôles et fonctionnalités.
- g. 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*.
- h. Choisir le serveur SERVEUR1 parmi le pool de serveurs sur lequel seront installés les services.
- i. Cocher la case *Redémarrer automatiquement le serveur de destination si nécessaire* puis cliquer sur *Déployer*.
- j. 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).

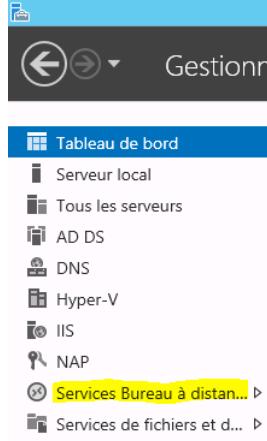
Sur le serveur hôte de session bureau à distance, il faut donc spécifier le serveur de licences qui sera utilisé : ce sera le même SERVEUR1 dans notre cas

- k. Dans le Gestionnaire de serveur, sélectionner Gérer, puis le lien Ajouter des rôles et fonctionnalités.
- l. Dans la fenêtre *Assistant Ajout des rôles*, choisir le type d'installation *Installation basée sur un rôle ou une fonctionnalité*.
- m. Choisir le serveur SERVEUR1 parmi le pool de serveurs sur lequel seront installés les services.

- n. Dans le rôle *Services Bureau à distance*, sélectionner le "sous-rôle" à installer : *Gestionnaire de licences des services Bureau à distance* (remarquer que les sous-rôles *Hôte de session Bureau à distance*, *Accès Bureau à distance par le Web*, et *Service Broker pour les connexions Bureau à distance* sont déjà installés).
- o. Ajouter les fonctionnalités requises proposées.
- p. Cocher la case *Redémarrer automatiquement le serveur de destination si nécessaire* puis cliquer sur *Installer*.
- q. Laisser l'installation se terminer.

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

- r. 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.

- s. Installer Packet Tracer sur le serveur SERVEUR1 (et non sur la station !).
- t. 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

Filtrer	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

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

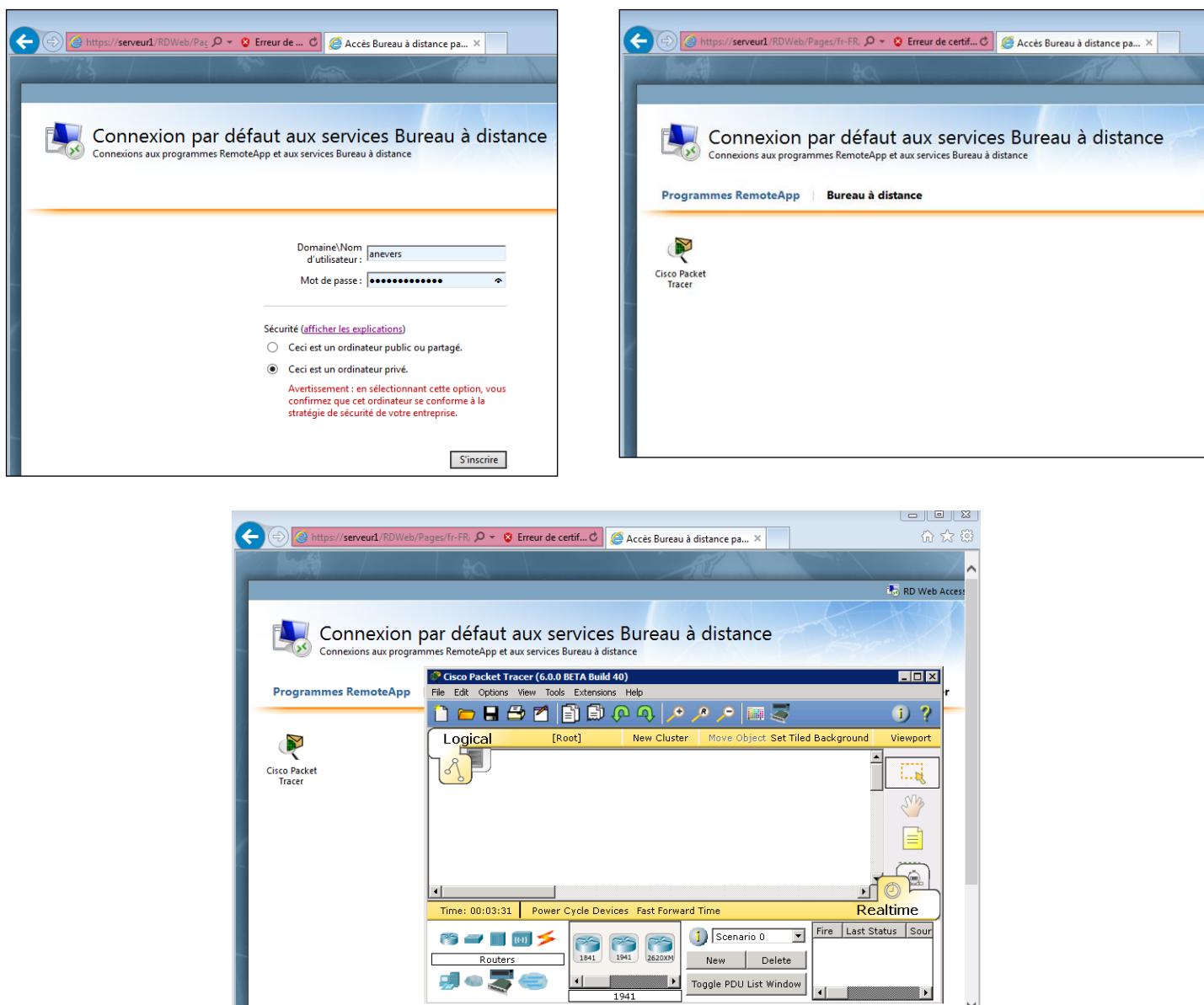
Annexe 2 : Ouverture d'une application RemoteApp (à distance) depuis PC1

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* :

- f. Démarrer la machine PC1 et ouvrir une session Windows avec l'utilisateur *anevers* et le mot de passe *Windows2016*
- g. 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 :

- h. 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', 'Collections', and 'QuickSessionCollection' (which is selected). The main area is divided into three sections:

- PROPRIÉTÉS**: Shows the collection type as 'Session', resources as 'Programmes RemoteApp', and user group as 'GSB\Utilisateurs du domaine'.
- CONNEXIONS**: Displays a table of active sessions. The table has columns: '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 available RemoteApp programs: Calculatrice, Paint, WordPad, and Cisco Packet Tracer, each with an alias and visibility status.
- SERVEURS HÔTES**: Shows a list of hosts: 'Tous les serveurs...'.

Remarques concernant une installation sous Windows Server 2008 R2 :

- j. Ajouter le rôle *Services Bureau à distance* sur le serveur SERVEUR1 (Démarrer / Outils d'administration / Gestionnaire de serveur) et sélectionner les services de rôles suivants :
- Hôte de session Bureau à distance
 - Gestionnaire de licences des services Bureau à distance
 - Service Broker pour les connexions Bureau à distance
 - Accès Bureau à distance par le Web

Méthode d'authentification pour le service Hôte de session Bureau à distance :

Ne nécessite pas l'authentification au niveau du réseau

Mode de licence : *par utilisateur*

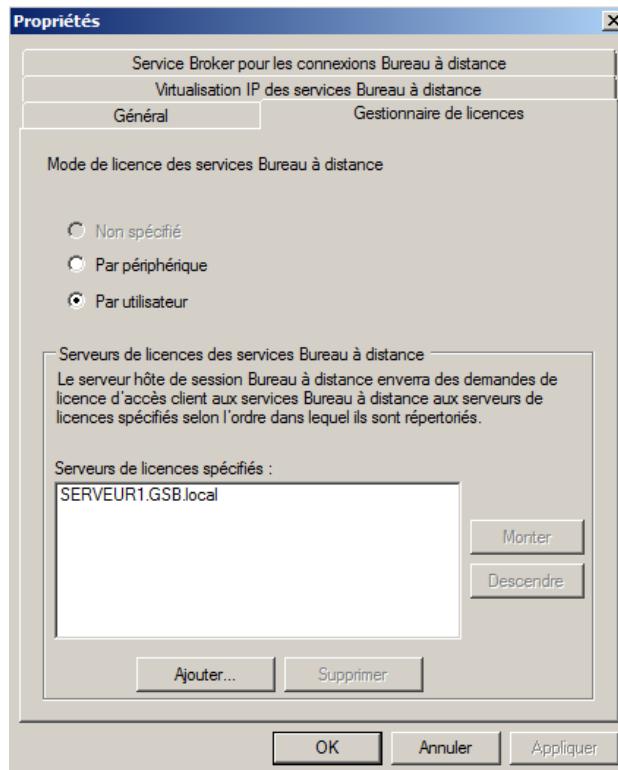
Groupe d'utilisateurs autorisés à accéder à ce serveur Hôte de session Bureau à distance:

- groupe *Administrateurs* (déjà ajouté)

Expérience client : -

Ne pas configurer d'étendue de découverte pour ce serveur de licences

- k. Sur SERVEUR1, ajouter le programme Packet Tracer à la liste des programme RemoteApp (Démarrer / Outils d'administration / Services Bureau à distance / Gestionnaire RemoteApp)
- l. Ajouter le serveur de licences des services Bureau à distance SERVEUR1 sur le serveur SERVEUR1 (Démarrer / Outils d'administration / Services Bureau à distance / Configuration d'hôte de session Bureau à distance; double-cliquer sur *Mode de licence des services Bureau à distance*) :
- Mode de licence : *Par utilisateur*
Serveurs de licences spécifiés : *[local] SERVEUR1.gsb.local* (à ajouter)



Il faut maintenant préciser les utilisateurs (ici, tous ceux du domaine GSB) qui pourront lancer des sessions sur le serveur hôte de session Bureau à distance, en configurant le groupe *Utilisateurs du Bureau à distance* :

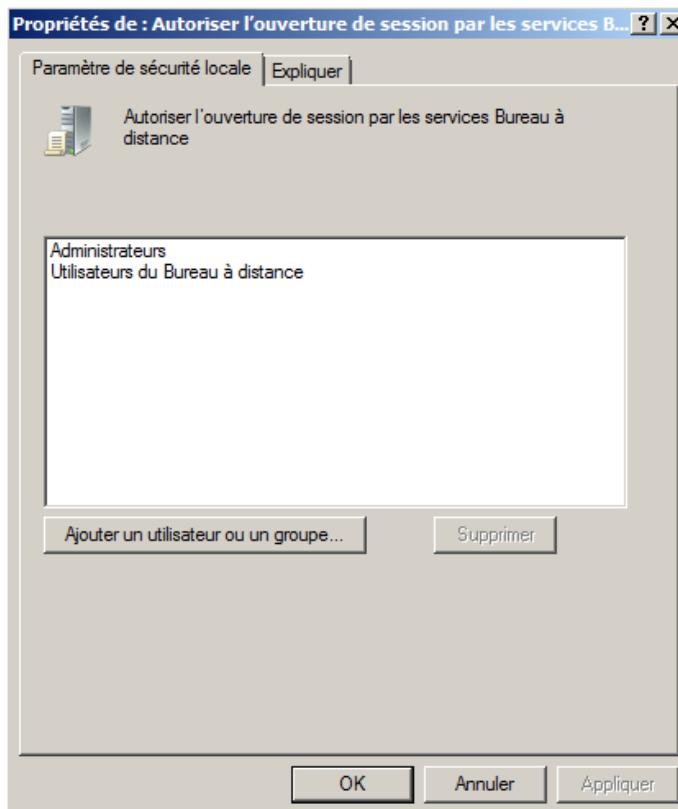
i. Pour effectuer cette autorisation sur SERVEUR1, procéder comme suit :

1. Cliquer sur *Démarrer / Panneau de configuration / Système et sécurité / Système / Paramètres système avancés / Utilisation à distance* ;
2. Cocher *Autoriser la connexion des ordinateurs exécutant n'importe quelle version du bureau à distance* ;
3. Cliquer sur le bouton *Sélectionnez des utilisateurs puis ajouter* le groupe *Utilisateurs du domaine* à cette liste d'utilisateurs.

Il faut aussi autoriser le groupe "Utilisateurs du Bureau à distance" dans la "Stratégie de sécurité locale" de chaque serveur hôte de session Bureau à distance. Par défaut, le groupe Utilisateurs du Bureau à Distance n'a pas cette autorisation dans Windows 2008 R2 (seul le groupe Administrateurs la possède).

j. Pour effectuer cette autorisation sur SERVEUR1, procéder comme suit :

1. Cliquez sur *Démarrer / Outils d'administration / Stratégie de sécurité locale*.
2. Dans le volet gauche, développer *Stratégies locales*, puis cliquer sur *Attribution des droits utilisateur*.
3. Dans le volet droit, double-cliquer sur *Autoriser l'ouverture de session par les services Bureau à distance*. Ajouter le groupe *Utilisateurs du Bureau à distance* à la liste des utilisateurs autorisés à ouvrir des sessions par les services Bureau à distance.
4. Cliquez sur *OK*.
5. Dans le volet droit, double-cliquer sur *Interdire l'ouverture de session par les services Bureau à distance*. S'assurer que le groupe *Utilisateurs du Bureau à distance* n'est pas répertorié (sinon, le supprimer de la liste), puis cliquer sur *OK*.



II) Mise en place des interfaces virtuelles

Je pars du principe que vous avez vos deux pfSense installés et configurés, c'est assez trivial et j'ai déjà fait plusieurs articles dessus.

La première étape est donc de créer nos deux interfaces virtuelles, sur chacun de nos hôtes. Pour cela on se rend sur **Firewall** puis **Virtual IPs** puis **Add** :



Ici on choisi donc le type **CARP**, car nous avons aussi la possibilité d'utiliser l'IP Alias ou encore le Proxy ARP, mais ce n'est pas le cas ici. On choisi ensuite notre interface, **WAN** pour commencer, puis on renseigne donc notre adresse. Ensuite, on renseigne un mot de passe qui sera utilisé pour le groupe VHID. On vient ensuite justement renseigner l'ID de ce fameux groupe, car un même pfSense peut faire parti de plusieurs clusters, ici nous nous contenterons de l'**ID 1**. Et enfin, nous laissons la valeur **Base à 1** (qui correspond au nombre de secondes avant qu'un hôte soit considéré comme down) et pour la valeur **Skew**, nous laissons à valeur à **0**. Cette valeur devra être incrémentée sur chacun des « esclaves » de notre cluster, ici nous sommes sur notre pfSense-01 qui sera le master donc nous laissons cette valeur.

Libre à vous de mettre ensuite une description ou non, puis nous réalisons la même chose pour l'IP virtuelle du LAN :

This screenshot image cannot be displayed. This file has been removed, renamed, or deleted. Note that this was probably due to a user error.

Normalement, si l'on se rend sur l'onglet **Status** puis **CARP (failover)** on devrait avoir ceci, après avoir réalisé la même manipulation sur le second pfSense :

Status / CARP

 Temporarily Disable CARP

 Enter Persistent CARP Maintenance Mode

CARP Interfaces

CARP Interface	Virtual IP
WAN@1	192.168.1.100/24
LAN@1	192.168.2.250/24

pfSync Nodes

pfSync nodes:

5481a732
5c5c3efe
81909412
bfef079b

Et pour le second :

The interface cannot be disabled. The interface must remain enabled in order to handle the traffic generated by the system.

Nous avons bien un Master, et un second en Backup. Parfait !

Ensuite nous devons dire à pfSense d'utiliser plutôt l'IP Virtuelle nouvellement créée plutôt que d'utiliser son IP LAN/WAN classique. Pour cela, on se rend dans **Firewall** puis **NAT**.

On choisit l'option **Hybrid Outbound NAT** plutôt qu'**Automatic Outbound NAT**, de cette manière nous allons pouvoir créer une règle qui sera prise en compte en cliquant sur **Add** juste en dessous de **Mappings** :



Ici, on choisit donc notre interface **WAN**, car c'est sur celle-ci que s'opère le NAT pour rappel, puis nous choisissons **Any** comme protocole, comme source nous prenons notre réseau LAN donc ici ce sera **192.168.2.0/24**, et enfin en dessous dans **Address** nous choisissons notre interface virtuelle WAN créée précédemment.

Comme d'habitude, une petite description ne fait pas de mal.

On peut ensuite soit répliquer cette configuration sur notre second pfSense, soit attendre un peu plus tard dans cet article quand nous activerons la réPLICATION de configuration, au choix.

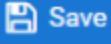
P.S: ici je ne traiterai pas de la configuration à modifier pour les protocoles VPN (OpenVPN, IPSec), mais il en va de même pour le DHCP par exemple: pensez à bien modifier l'IP du WAN/LAN par celle de la VIP !

III) Mise en place de la High-Availability

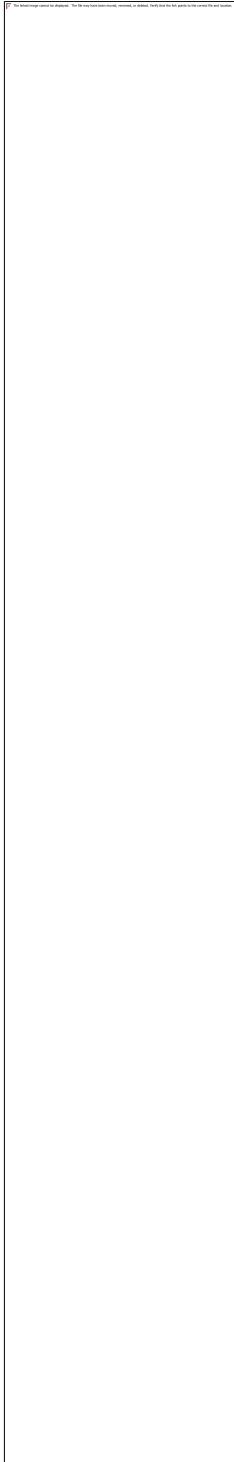
Bien, désormais nous allons nous attaquer à la partie synchronisation de configurations entre nos deux hôtes.

La première étape est d'activer notre interface « pfSync ».

Pour cela, on se rend d'abord sur **Interfaces**, puis **Assignments** :

Interface	Network port
WAN	em0 (00:0c:29:f8:3c:f0)
LAN	em1 (00:0c:29:f8:3c:fa)
Available network ports:	em2 (00:0c:29:f8:3c:04)
 Save	

On va donc cliquer sur **Add** pour rajouter notre interface :



On coche bien entendu la case **Enable**, puis on rajoute la description qui va bien, on lui assigne une adresse IP (dans mon cas ce sera en /30, car je n'ai que deux hôtes mais libre à vous d'adapter au besoin), et c'est à peu près tout. Pensez à faire de même sur le second pfSense en ajustant l'adresse IP et le tour est joué !

Ensuite, on se rend dans **System**, puis **High Avail. Sync** :



On coche la case **Synchronize states**, qui permet d'activer la fonctionnalité, on choisi ensuite notre interface (LAN ou bien une interface dédiée, dans notre cas ce sera donc **pfSync**), on défini ensuite l'IP de notre second pfSense (pour rappel, toutes les actions effectuées jusqu'ici sont réalisées sur le pfSense-01 !), et ensuite on renseigne à nouveau l'IP du second dans le champ **Synchronize Config to IP**, puis on ajoute plus bas les credentials et enfin on coche les fonctionnalités à répliquer. Pensez à cocher **NAT configuration**, de

cette manière vous pourrez voir par la suite si vos démarches fonctionnent en vous rendant sur le second pfSense.

Par rapport au second pfSense justement, il convient simplement de cocher la case pour activer le service, renseigner l'interface, puis l'IP du pfSense-01 dans **pfsync Synchroniez Peer IP** et rien de plus, car c'est le Master qui va répliquer les sur les slaves pour rappel

IV) Les règles de pare-feu

Car oui, c'est bien beau tout ça, mais vous vous rendrez vite compte que même en tapant dessus ce ne fonctionner pas... et oui, par défaut les interfaces sur pfSense bloquent tout le trafic, donc nous devons nous rendre sur l'onglet **Firewall** puis **Rules** et enfin **pfSync** (ou local) pour rajouter nos règles de pare-feu histoire d'autoriser ce trafic.

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreach) is returned to the sender whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

PFSYNC

Choose the interface from which packets must come to match this rule.

Address Family

IPv4+IPv6

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

Invert match.

any

Destination

Destination

Invert match.

any

Extra Options

Log

Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a log collector (see the Status: System Logs: Settings page).

Description

Autoriser tout le trafic sur pfSync

A description may be entered here for administrative reference. A maximum of 52 characters will be displayed in the status bar.

Ici, c'est un peu à vous de voir, en fin presque, je m'explique: pour la synchronisation via le protocole **XML-RPC**, normalement celle-ci s'effectue sur le port 443, et pour le **pfSync**, une option lui est dédiée dans la partie **Protocol**, le soucis est que personnellement, à l'heure où j'écris ces lignes, je n'ai pas réussi à faire fonctionner la synchro' en ouvrant seulement ces ports... et j'avoue avoir la flemme de chercher pour le moment haha, donc ici j'autorise tout le trafic.

Avec cette configuration, tout fonctionne, même si bien entendu ce n'est pas à faire en production, encore qu'ici nos pfSense sont comme « connectés en direct l'un sur l'autre », donc aucun risque ou presque (car le risque zéro n'existe pas etc etc).

Breeef, on autorise le trafic sur notre pfSense-01 ainsi que sur le second, et c'est bon !