

Sommaire :

Mission 1 : Installation du routeur-pare-feu PfSense.....	2
Assignation des interfaces sur Vsphere :	3
Mission 2 : Installation du serveur de domaine.....	3
Mission 2 A : Création du domaine MDL.local.....	3
Mission 2 B : Installation du poste client PC1.....	5
Mission 2 C : création des utilisateurs avec leur dossier personnel de base ; configuration d'autorisations spécifiques à certains dossiers.....	6
Création automatiques des répertoires des utilisateurs :	9
Mission 3 : Inventaire du matériel avec GLPI/FusionInventory.....	10
Installer le SGBD MySQL :	13
Installation de GLPI.....	14
Installation de FusionInventory.....	15
Installation manuelle de l'agent sur Windows.....	16
Importer dans GLPI tous les utilisateurs du domaine MDL.local.....	17
Création des tickets :	18
Mission 4 : Installation d'un VPN.....	20
Installation du package Export Utility.....	25
Mission 5 : Configuration d'un cluster de deux Pfsense redondants (en Haute Disponibilité).27	
Création de l'ip virtuelle du LAN :	31
Création de l'ip virtuelle du WAN :	33
Configuration de la synchronisation entre les Pfsense.....	34

Mission 1 : Installation du routeur-pare-feu PfSense

- Création du pfsense et assignations des cartes réseaux
- En 1^{er} on va assigner les interfaces ensuite on va leur assigner une ip avec la configuration 2

Configuration du WAN :

```

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

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

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.211.228

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.211.254

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address. Press <ENTER> for none:
>

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

```

Configuration du LAN :

```

LAN (lan)          -> vmx1          -> v4: 172.16.2.254/24

```

Configuration de la DMZ :

```

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) n

Please wait while the changes are saved to OPT1...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 OPT1 address has been set to 10.10.1.254/24

```

[Assignation des interfaces sur Vsphere :](#)

- Pour ce faire il faut regarder sur Pfsense par rapport aux adresses mac :

```


vmx0      00:50:56:90:6c:c5    (up) VMware VMXNET3 Ethernet Adapter
vmx1      00:50:56:90:22:d4    (up) VMware VMXNET3 Ethernet Adapter
vmx2      00:50:56:90:1c:9c    (up) VMware VMXNET3 Ethernet Adapter
vmx3      00:50:56:90:50:31   (down) VMware VMXNET3 Ethernet Adapter

```

> Contrôleur SCSI 0		LSI Logic SAS
▼ Adaptateur réseau 1 *	LAB-SISR-06-2 ▼	☑ Connecté
Statut	☑ Connecter lors de la mise sous tension	
Type d'adaptateur	VMXNET 3 ▼	
DirectPath I/O	☑ Activer	
Adresse MAC	00:50:56:90:22:d4	Automatique ▼
▼ Adaptateur réseau 2 *	LAB-SISR-06-3 ▼	☑ Connecté
Statut	☑ Connecter lors de la mise sous tension	
Type d'adaptateur	VMXNET 3 ▼	
DirectPath I/O	☑ Activer	
Adresse MAC	00:50:56:90:1c:9c	Automatique ▼
▼ Adaptateur réseau 3 *	LAB-SISR-06-4 ▼	☑ Connecté
Statut	☑ Connecter lors de la mise sous tension	

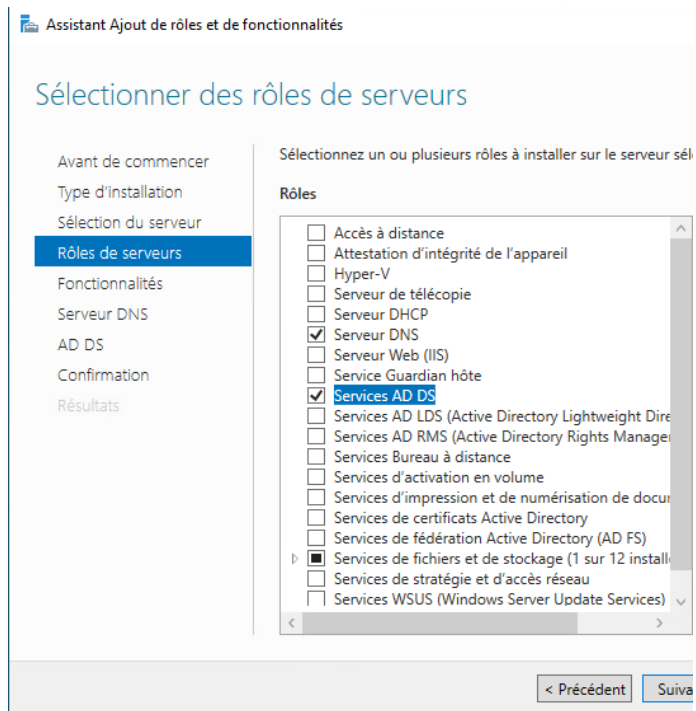
Mission 2 : Installation du serveur de domaine

Mission 2 A : Création du domaine MDL.local

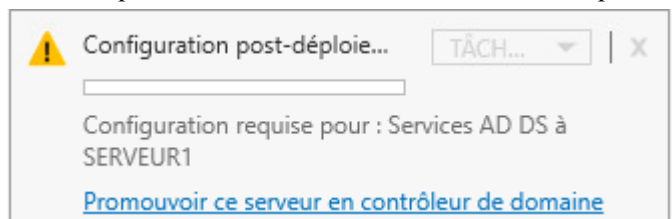
- Création de la machine avec la template suivante :  Windows 2022 - MODEL
- Assignation de l'étiquette réseau pour qu'il soit dans le LAN :

> Adaptateur réseau 1	LAB-SISR-06-2 ▼
-----------------------	-----------------

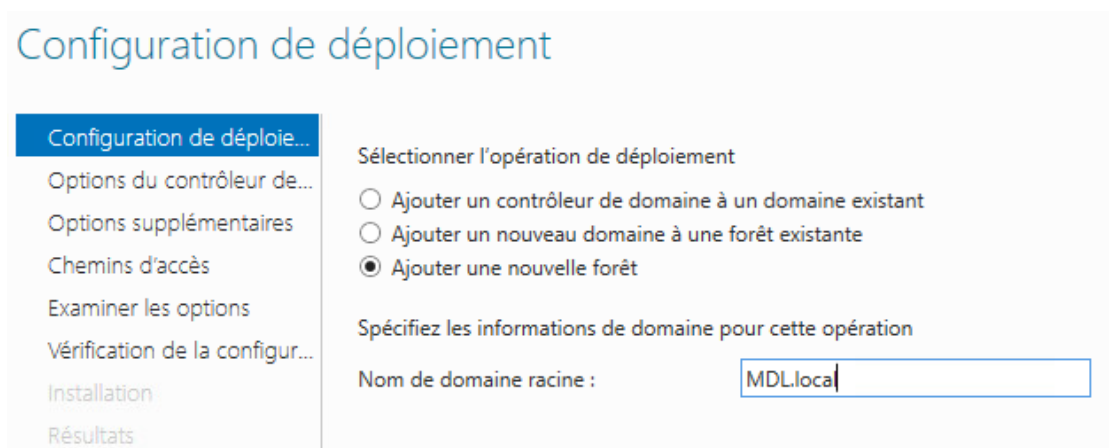
- On va maintenant lancer la machine pour lui changer le nom et la configuration IP
- On va lui installer **le rôle de contrôleur du domaine** MDL.local qui sera aussi serveur DNS



- Une fois que les rôles sont bien installés, on va cliquer sur

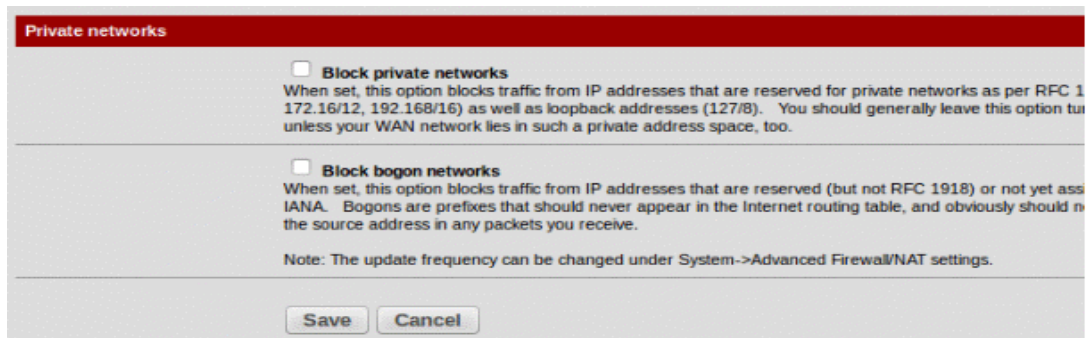


- Ajouter une nouvelle forêt et la nommer :



- Cocher les cases suivantes :
- **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 : Windows2022

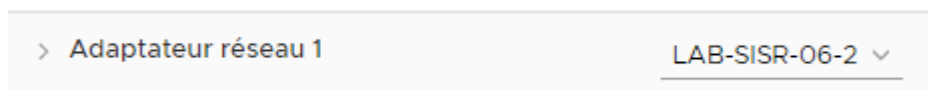
- Ne pas tenir compte du message "Il est impossible de créer une délégation pour ce serveur DNS, ..."
 - Nom de domaine NetBIOS : **MDL**
 - Accepter les noms de dossiers proposés pour la base de données, les fichiers journaux, et le dossier SYSVOL
 - Cliquer sur Installer lorsque la configuration requise a bien été validée.
 - Il faudra se rendre dans le gestionnaire de serveur puis dans notification
 - Terminer la configuration DHCP
-
- Rendre accessible le Pfsense depuis un poste ayant une adresse IP privée en décochant la case Block private networks de l'interface WAN (sur l'écran d'interface graphique accessible via un navigateur de la machine physique hôte) :



- Modifier si besoin les règles de filtrage en entrée de l'interface LAN pour autoriser toute communication à partir de n'importe quel poste de n'importe quel VLAN de MDL.

Mission 2 B : Installation du poste client PC1

- On va donc partir de la template **Windows 10 21H1** et on va lui assigner l'étiquette réseau qui va avec le LAN



- On va maintenant le renommer, changer sa configuration IP et l'ajouter au domaine

Pour la configuration IP :

Propriétés de : Protocole Internet version 4 (TCP/IPv4)

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 172 . 16 . 2 . 10

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 172 . 16 . 2 . 254

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 172 . 16 . 2 . 1

Serveur DNS auxiliaire : . . . |

Remarque : on a mis le contrôleur de domaine comme serveur DNS car il fait aussi serveur DNS et pour la passerelle on a mis l'ip de l'interface

Modification du nom ou du domaine de l'ordinateur ✕

Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influencer sur l'accès aux ressources réseau.

Nom de l'ordinateur : PC1

Nom complet de l'ordinateur : PC1

Autres...

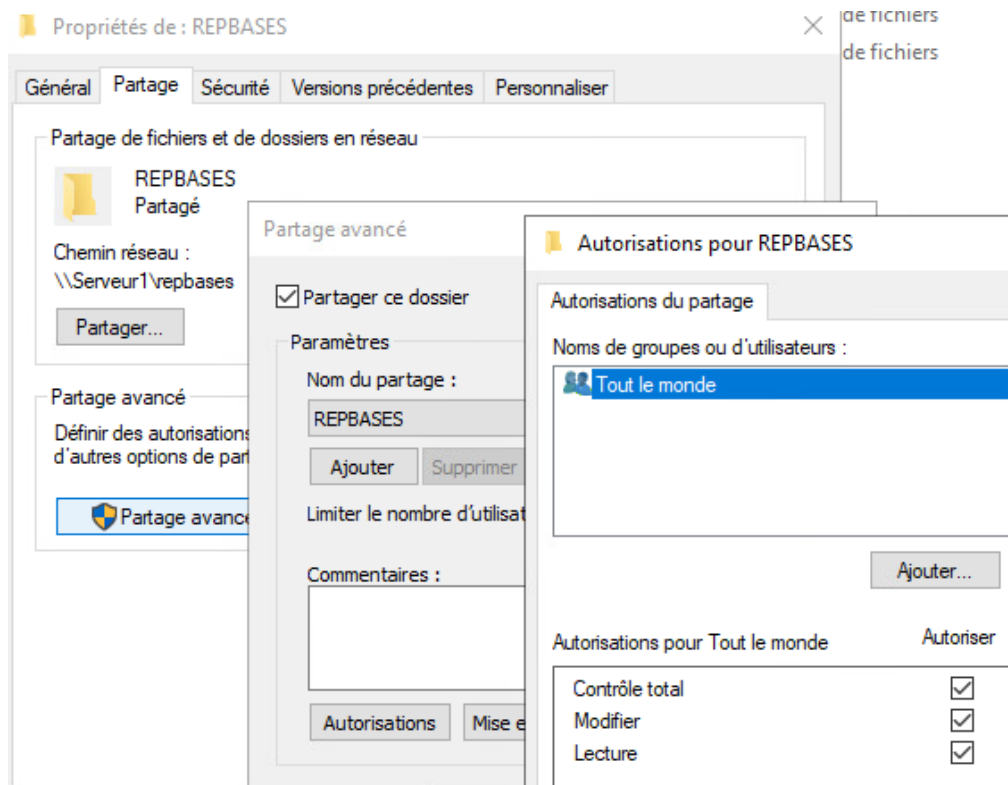
Membre d'un

☒ Domaine : MDL.local

☐ Groupe de travail : WORKGROUP

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

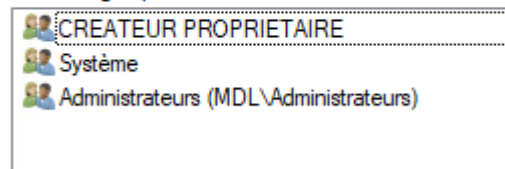
- Créer le dossier REPBASES et configurer les autorisations de partage et ses autorisations de sécurité NTFS ; REPBASES contiendra les dossiers personnels de base de chaque utilisateur.



- On va supprimer **Utilisateur du domaine**

Nom de l'objet : C:\REPBASES

Noms de groupes ou d'utilisateurs :

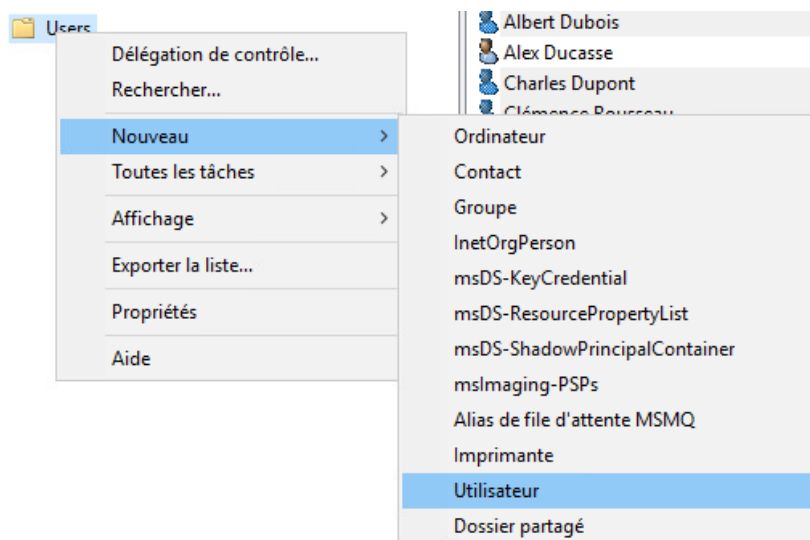


- Maintenant, pour le dossier REPBASES, Utilisateurs (du domaine) n'a plus aucuns droits ; mais CREATEUR PROPRIETAIRE, Système, et Administrateurs conservent le Contrôle Total.
- Les dossiers personnels de base des utilisateurs, qui seront des sous-dossiers de REPBASES, vont hériter automatiquement de ces autorisations du dossier parent REPBASES
- Créer les utilisateurs suivants (chacun avec son dossier personnel) (pour plus de simplicité, le mot de passe de chaque utilisateur ne changera jamais) ; vérifier ensuite que chaque utilisateur a son dossier dans REPBASES et qu'il est le seul à pouvoir y accéder, hormis les administrateurs et le système :

Utilisateurs

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

- Pour créer un utilisateur il faut se rendre dans le gestionnaire de serveur il faut aller dans Utilisateurs et ordinateurs Active Directory, puis faire clic droit sur Users



- Il faudra suivre répéter la même opération pour chaque utilisateur que l'on va créer

Nouvel objet - Utilisateur

Créer dans : MDL.local/Users

Prénom : Clément Initiales :

Nom : Ogier

Nom complet : Clément Ogier


Nom d'ouverture de session de l'utilisateur : cogier @MDL.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : MDL\ cogier

< Précédent Suivant > Annuler

- Cocher la case le mot de passe n'expire jamais et entrer le mot de passe Windows2019

Nouvel objet - Utilisateur X

 Créer dans : MDL.local/Users

Mot de passe :


Confirmer le mot de passe :

☐ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
☐ L'utilisateur ne peut pas changer de mot de passe
☒ Le mot de passe n'expire jamais
☐ Le compte est désactivé

Une fois que les utilisateurs sont créés on va configurer la création automatique des répertoires des utilisateurs.

Création automatique des répertoires des utilisateurs :

Nous allons maintenant faire en sorte qu'un dossier personnel de base soit créé pour chaque utilisateur (seuls l'utilisateur, le système, et l'administrateur devront avoir accès au dossier personnel)

- Il faut se rendre dans Gestionnaire de serveur  / Outils / Utilisateurs et ordinateurs Active Directory ; cliquer ensuite sur le dossier Users, puis cliquer droit sur l'utilisateur pour lequel on souhaite créer le dossier personnel, cliquer sur **Propriétés** puis cliquer sur **Profil**
- Cliquer sur Connecter, choisir D: puis après le « connecter à écrire » : <\\SERVEUR1\REPBASES%\%username%>
- La variable %username% contient le nom d'ouverture de session de l'utilisateur courant

Dossier de base

☐ Chemin d'accès local :

☒ Connecter : D: à : \\serveur1\REPBASES\dubreuil

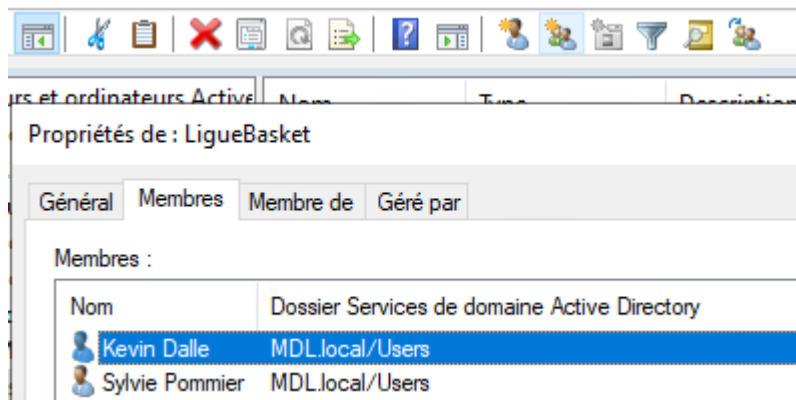
⚠ Bien mettre un lecteur réseau qui n'est pas utilisé ! ⚠

Le DSI demande ensuite de créer des dossiers (Public, Football, et Basket) pour la gestion des contrats et d'y affecter des droits d'accès NTFS différents à deux groupes d'utilisateurs (LigueFootball et LigueBasket).

- Créer les groupes d'utilisateurs et les dossiers, puis configurer les autorisations d'accès spécifiques suivantes :

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

- On va donc créer les groupes d'utilisateurs et ajouter les membres aux groupes



- On va faire la même opération pour le groupe LigueFootball

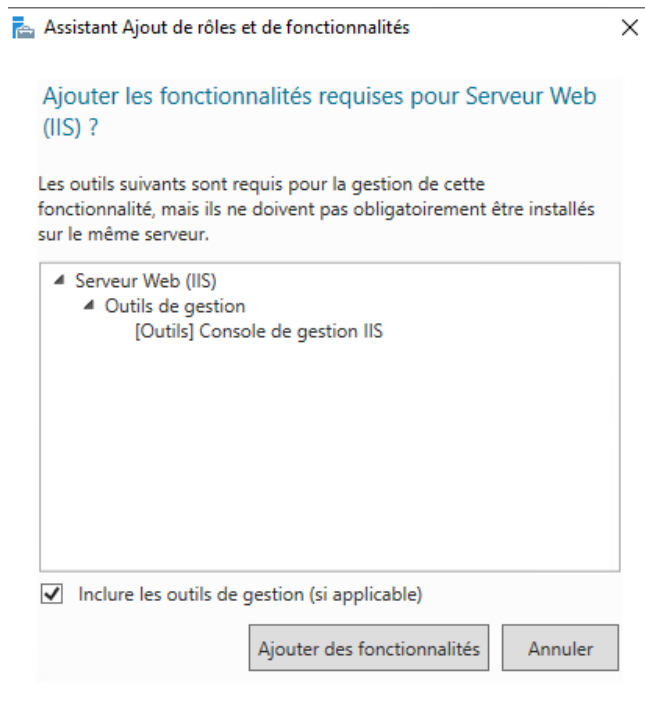
- Créer les 3 dossiers : C: \

🖥️ **Public** 🏈 **Football** 🏀 **Basket**

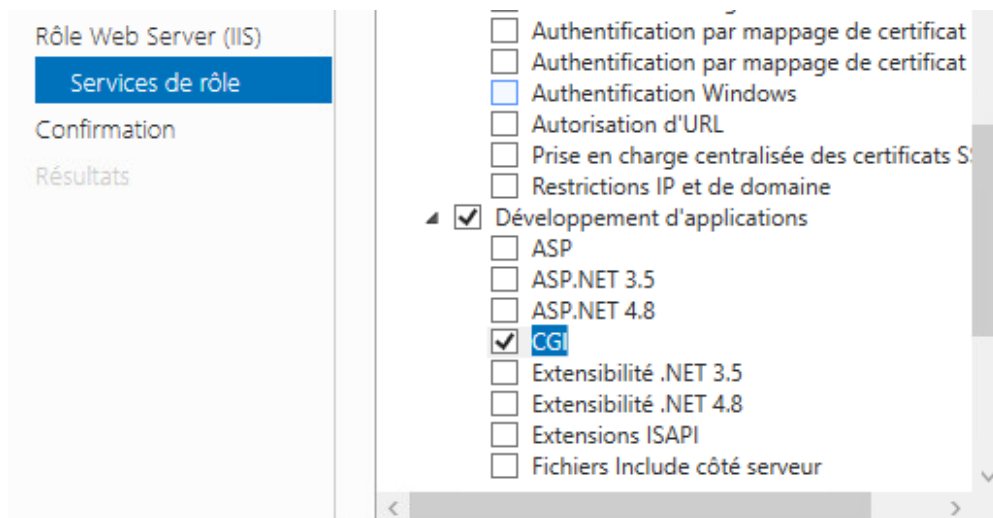
- Reprendre ici mettre les captures + attaquer glpi


[Mission 3 : Inventaire du matériel avec GLPI/FusionInventory](#)

- Installer le rôle Serveur web IIS avec les services de rôle par défaut et le service de rôle CGI.



Ainsi que CGI :



- Installer la dernière version (Non-Thread Safe (NTS)) du dossier PHP 7 fourni (php-7.2.11-nts-Win32-VC15-x64) dans le dossier C:\Program Files (en Français Programmes) ;
- Renommer le fichier php.ini-development en **php.ini** ;
- Ajouter le chemin du dossier C:\Program Files\php-7.2.11-nts-Win32-VC15-x64 à la variable d'environnement Path (Panneau de configuration  / Système et sécurité, Système, lien Paramètres système avancés ; dans la fenêtre qui s'ouvre, sélectionner l'onglet Avancé, puis le bouton Variables d'environnement ; dans Variables système, sélectionner la ligne Path, puis cliquer sur le bouton Modifier ; cliquer sur le bouton Nouveau pour ajouter le chemin C:\Program Files\php-7.2.11-nts-Win32-VC15-x64 à la variable Path) ;

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

Chemin demandes : **.php*

Module : *FastCgiModule*

Exécutable : taper le chemin d'accès

complet à Php-cgi.exe :

C:\Program Files\php-7.2.11-nts-Win32-VC15-x64\php-cgi.exe

Nom : entrer un nom pour le

mappage : *php-7.2.11*

- Cliquer ensuite sur le bouton *Restrictions des demandes* et cocher *Fichier ou dossier*.
- Ainsi, tous les fichiers d'extension. php seront envoyés au module *FastCGIModule* pour y être exécutés par le programme *php-cgi.exe*.
- Installer le package redistribuable Microsoft Visual C++ vc_redist.x64-2015.exe (c'est bien la version 2015 pour systèmes 64 bits qui est nécessaire ici) ;
- Pour vérifier l'installation de PHP, créer le fichier suivant avec le bloc-notes :

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

- *php_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).

- On va maintenant créer la base de données GLPI :

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| test |
+-----+
4 rows in set (0.00 sec)

mysql> create database glpi;
Query OK, 1 row affected (0.01 sec)
```

Installation de GLPI

- 1 On va télécharger la version 9.5 de GLPI il faudra utiliser 7zip pour dézipper le fichier
- 2 On va copier le dossier *glpi* dans *inetpub\wwwroot*
- 3 Dans l'explorateur Windows, attribuer l'autorisation *Modification* à *Utilisateurs et IIS_IUSRS* pour le dossier *C:\inetpub\wwwroot\glpi*

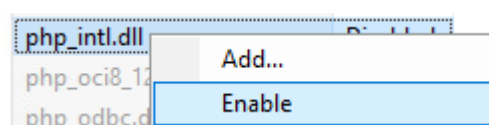


- 4 Sous IIS créer le site web sous le nom *glpi* on se connectera avec localhost

- Lors de l'installation de GLPI on peut rencontrer ce problème :

Test de l'extension intl	✗ L'extension intl est absente
--------------------------	--------------------------------

- Pour pallier à ce problème il faut aller dans les extensions IIS dans PHP Manager et cliquer sur add extension



- Avancé l'installation de GLPI

Paramètres de connexion à la base de données

Serveur SQL (MariaDB ou MySQL)

Utilisateur SQL

Mot de passe SQL

- Choisir la base de données créée au préalable

Veuillez sélectionner une base de données :

☒ **glpi**

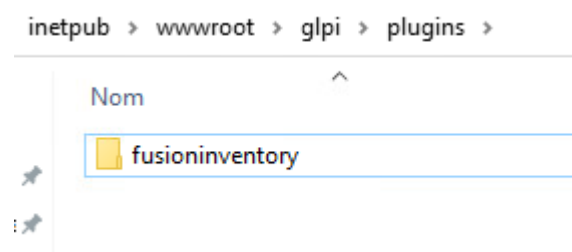
☐ **test**

☐ **Créer une nouvelle base ou utiliser une base existante**

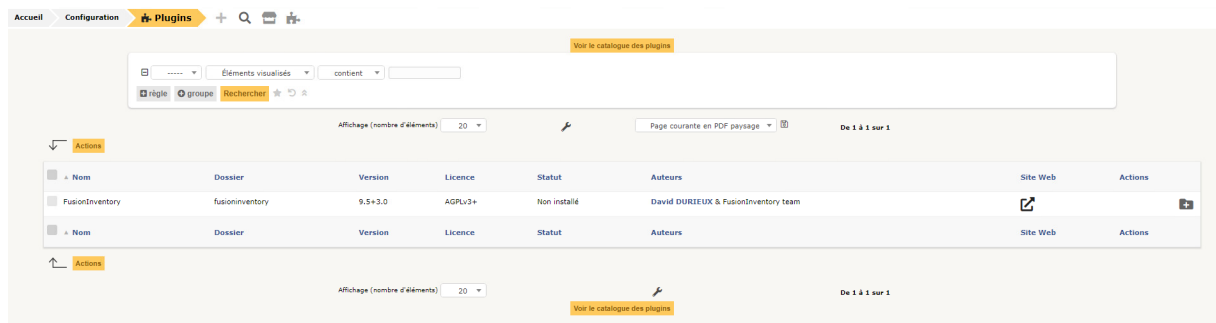
- Cliquer sur continuer jusqu'à la fin de l'installation puis se connecter avec glpi/glpi
- Installer l'agent FusionInventory sur chaque poste du réseau MDL (SERVEUR1, PC1, Pfsense) pour la remontée automatique des données des postes sur le serveur.

Installation de FusionInventory

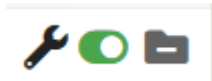
- Pour ce faire il faut coller le plugin dans : **glpi/plugins**



- On va maintenant se rendre sur GLPI



- Il faudra cliquer sur le dossier avec le +
- Puis une fois que le plugin est installé il faut l'activer



- 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://172.16.2.1/glpi/plugins/fusioninventory/>

Entité

Modèle pour le transfert automatique d'ordinateurs dans une autre entité : Pas de transfert automatique

URL d'accès au service : http://172.16.2.1/glpi/plugins/fusioninvent

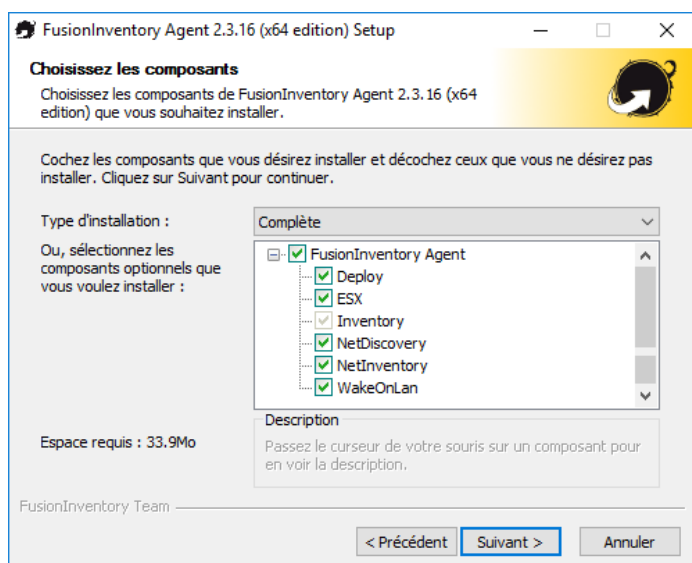
Sauvegarder

- Installer l'agent FusionInventory sur chaque poste du réseau MDL (SERVEUR1, PC1, Pfsense) pour la remontée automatique des données des postes sur le serveur.

- On peut le faire avec une GPO ou à la main

[Installation manuelle de l'agent sur Windows](#)

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



FusionInventory Agent 2.3.16 (x64 edition) Setup

Choisir la destination
Choisissez où les résultats seront envoyés.

Mode Local

Dossier Local ou localisation UNC

Mode Serveurs

Vous pouvez indiquer plusieurs URIs séparés par des virgules
'http://<serveur>/glpi/plugins/fusioninventory/, http://<serveur>/ocsinventory/,...'

Installation rapide (N'affiche pas les autres options Windows) ☐

FusionInventory Team

< Précédent Suivant > Annuler

Importer dans GLPI tous les utilisateurs du domaine MDL.local

Ajout de l'annuaire LDAP

- Pour ce faire il faut aller dans le menu dans authentification puis cliquer sur Annuaire LDAP, Il faut cliquer sur liaison annuaire LDAP

Utilisateurs + 🔍

Ajouter utilisateur... ... Depuis une source externe Liaison annuaire LDAP

----- Éléments visualisés contient

+ règle + groupe Rechercher

- Il faut remplir les champs comme ceci (par rapport à notre serveur)
- Une fois l'annuaire créé on va importer les nouveaux utilisateurs, il faut aller dans administration>utilisateurs
- Il faudra cliquer sur liaison annuaire LDAP

Annuaire LDAP

Nom	SERVEUR1	Dernière modification	2023-03-28 08:53
Serveur par défaut	Oui	Actif	Oui
Serveur	172.16.2.1	Port (par défaut 389)	389
Filtre de connexion	(&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))		
BaseDN	CN=Users,DC=MDL,DC=local		
DN du compte (pour les connexions non anonymes)	CN=Administrateur,CN=Users,DC=MDL,DC=local		
Mot de passe du compte (pour les connexions non anonymes)	<input type="password"/>	<input type="checkbox"/> Effacer	
Champ de l'identifiant	samaccountname	Commentaires	<input type="text"/>
Champ de synchronisation	<input type="text"/>		

- Il faut cliquer sur rechercher

L'utilisateur **gipi** attribue les tickets nouveaux au technicien **tech** qui va effectuer les travaux suivants :

Logiciel Gantt Project

Ticket - ID 2

Date d'ouverture	2023-04-25 08:41:50	Par	Dubreuil Laure
Dernière modification	2023-04-25 08:41 par Dubreuil Laure		
Temps de prise en charge		Temps de résolution	
Temps interne de prise en compte		Temps interne de résolution	
Type	Demande	Catégorie	
Statut	Nouveau	Source de la demande	Helpdesk
Urgence	Haute	Validation	Non soumis à validation
Impact	Moyen	Lieu	
Priorité	Haute		

Acteur	Demandeur +	Observateur +	Attribué à +
	Dubreuil Laure		tech

(En cours : 0)

Une fois les 2 tickets attribués on va se connecter sur l'utilisateur tech et traiter les tickets :

Attribué à - Technicien

tech

tech

Il faut donc se connecter à l'utilisateur tech

- Pour le premier ticket, il échange l'ancien lecteur de cdrom par un neuf (45 mn de main d'oeuvre à 160 €/h ; prix d'un lecteur : 80 €).

Lecteur cdrom défaillant...

Actions 1/2 > >>

New item - Cost

Name	cdrom	Begin date	
Duration	0h45	End date	
Time cost	160		
Fixed cost	0.00		
Material cost	80		
Budget			

Comments

160euros de main d'oeuvre + 80euros le cdrom neuf

- Pour le deuxième ticket, il installe le logiciel Gantt Project, et ne compte aucun temps passé.




SERVEUR1 a été acheté et mis en service le 01/01/2016. Son prix d'achat était de 1800 €. Son amortissement est linéaire sur 5 ans (aucune garantie connue).

Titre	Demande d'installation de Gantt Project sur SERVEUR1
Description ⓘ	<p>Bonjour,</p> <p>Je constate que le logiciel Gantt Project n'est pas installé sur le SERVEUR1, bien que j'en aie besoin pour mon travail. Je souhaiterais que l'équipe informatique installe Gantt Project sur ce serveur.</p> <p>Merci de bien vouloir prendre en compte ma demande dans les meilleurs délais et de me tenir informé de l'avancement de la situation.</p> <p>Cordialement.</p> <p>Laure DUBREUIL</p>




Mission 4 : Installation d'un VPN

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

- 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) :

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA_Acces_VPN	✓	self-signed	1	ST=test, O=test, L=test, CN=CA_Acces_VPN, C=FR ⓘ Valid From: Thu, 30 Mar 2023 08:57:18 +0000 Valid Until: Sun, 27 Mar 2033 08:57:18 +0000	LDAP Server	  

- 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**) :

Certificat_Acces_VPN Server Certificate CA: No Server: Yes	CA_Acces_VPN	ST=test, O=test, L=test, CN=Certificat_Acces_VPN, C=FR ⓘ Valid From: Thu, 30 Mar 2023 08:59:20 +0000 Valid Until: Sun, 27 Mar 2033 08:59:20 +0000	  
---	--------------	---	---

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

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

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

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

Server Settings

Descriptive name

Serveur AD GSB

Type

LDAP

LDAP Server Settings

Hostname or IP address

172.16.2.1

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.

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	<input type="checkbox"/> Enable extended query	
Bind anonymous	<input type="checkbox"/> 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	<input type="checkbox"/> 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	<input type="checkbox"/> 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	<input type="checkbox"/> Do not strip away parts of the username after the @ symbol e.g. user@host becomes user when unchecked.	
Allow unauthenticated bind	<input checked="" type="checkbox"/> 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		

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

Authentication Server :

Serveur AD MDL

System / User Manager / Settings

Users

Groups

Settings

Authentication Servers

Settings

Session timeout

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

Server AD GSB

Shell Authentication

☐ Use Authentication Server for Shell Authentication
 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

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.

Save

Save & Test

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

```

Attempting connection to      172.16.2.1  OK
Attempting bind to           172.16.2.1  OK
Attempting to fetch Organizational Units from 172.16.2.1  OK

Organization units found
CN=Users,DC=MDL,DC=local
OU=Domain Controllers,DC=MDL,DC=local

```

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

Type of Server :	LDAP
LDAP Servers :	Serveur AD MDL
Certificate Authority :	CA_Access_VPN
Certificate :	Certificat_Acces_VPN
Description :	Serveur VPN avec authentication LDAP GSB
Local Port :	1196

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

1194

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

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.

Tunnel Settings

Tunnel Network

192.168.10.0/24

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.

Redirect Gateway

☐

Force all client generated traffic through the tunnel.

Local Network

172.16.2.0

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.

Client Settings

Dynamic IP

☒

Allow connected clients to retain their connections if their IP address changes.

Topology

Subnet -- One IP address per client in a common subnet

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

MDL.local

Provide a default domain name to clients.

DNS Server 1

172.16.2.1

DNS server IP to provide to connecting clients.

- Il faudra cocher les cases suivantes car les cases *Firewall Rule* et *OpenVPN rule* ajoute automatiquement les règles de filtrage.

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 ☒

Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule ☒

Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

- 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

Authentication Server

Serveur AD GSB

Select the authentication server to test against.

Username

anevers

Password

●●●●●●●●●●

Test

- Les règles de filtrage qui ont été créées par l'assistant sont les suivantes :
- sur l'interface **OpenVPN** (créée 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	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

↑ Add

↓ Add

Delete

Save

Separator

- sur l'interface **WAN** :

Floating WAN LAN OpenVPN											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	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	
<div> Add Add Delete Save Separator </div>											

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

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

DNS Server : *172.16.2.1*

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

Installation du package Export Utility

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

- Installer le package *OpenVPN Client Export Utility* :
- Sélectionner la commande System Packages, puis cliquer sur l'onglet *Available Packages*. Sur la ligne *OpenVPN Client Export Utility*, cliquer sur le signe + pour ajouter le package. Après l'installation, cliquer sur l'onglet *Installed Packages* pour vérifier que le module a bien été installé.
- Sélectionner la commande VPN OpenVPN, dans l'onglet Client Export, pour le type d'utilisateur *Authentication Only (No Cert)*, afin de vérifier la présence de l'archive (contenant les trois fichiers de configuration), ou mieux encore, de l'exécutable *Windows Installer*, qui est à exporter sur les machines clientes (attention : sélectionner le bon serveur dans la zone *Remote Access Server*) :

Installed Packages

Name	Category	Version	Description	Actions
✓ openvpn-client-export	security	1.6_9	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	
Package Dependencies: openvpn-client-export-2.5.8 openvpn-2.5.4_1 zip-3.0_1 p7zip-16.02_3				

OpenVPN Clients

User	Certificate Name	Export
Authentication Only (No Cert)	none	- Inline Configurations: <div> Most Clients Android </div> <div> OpenVPN Connect (iOS/Android) </div> - Bundled Configurations: <div> Archive Config File Only </div>

- 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).
- On va coller les fichier de config dans OpenVPN>config

Ce PC > Disque local (C:) > Programmes > OpenVPN > config

Nom	Modifié le	Type	Taille
pfSense-UDP4-1194.ovpn	30/03/2023 11:22	OpenVPN Config ...	1 Ko
pfSense-UDP4-1194-ca.crt	30/03/2023 11:22	Certificat de sécur...	2 Ko
pfSense-UDP4-1194-tls.key	30/03/2023 11:22	Fichier KEY	1 Ko

- On va maintenant se connecter il faut lancer openvpn gui et se connecter avec un des utilisateurs de l'AD

pfSense-UDP4-1194

Utilisateur:

User_VPN

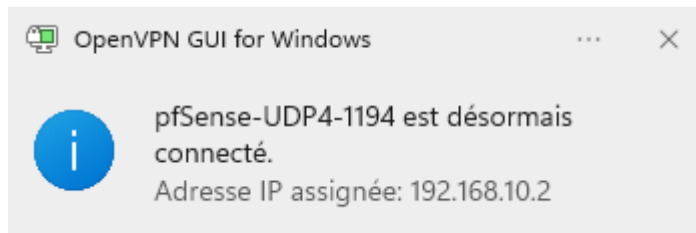
Mot de passe:

••••••••

☐ Se souvenir du mot de passe

OK

Annuler



Mission 5 : Configuration d'un cluster de deux Pfsense redondants (en Haute Disponibilité)

- Tout d'abord il faut faire une sauvegarde du Pfsense qui est fonctionnel en faisant un clone on va l'appeler Pfsense backup
- On va maintenant dupliquer le Pfsense une deuxième fois et l'appeler le Pfsense secondaire
- On va maintenant changer l'ip du LAN actuellement configuré car ce sera l'adresse IP virtuelle

Serveur maître LAN :

```
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 172.16.2.252/24
You can now access the webConfigurator by opening the following URL
browser:
      http://172.16.2.252/

Press <ENTER> to continue. █
```

Serveur secondaire LAN :

```

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 172.16.2.253/24
You can now access the webConfigurator by opening the following URL in your web
browser:
        http://172.16.2.253/

```

Changement de l'ip du pfsense secondaire de l'interface Wan (on ajoute +1 à celle qu'on nous a donné à la base)

```

Available interfaces:

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

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

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

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.211.229

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.211.254

```

Changement de l'ip de l'interface OPT1 (DMZ) du serveur maitre :

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

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

Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 10.10.1.252

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new OPT1 IPv6 address. Press <ENTER> for none:
> 
```

Changement de l'ip de l'interface OPT1 (DMZ) du serveur secondaire :

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

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

Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 10.10.1.253

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new OPT1 IPv6 address. Press <ENTER> for none:
> 
```

Configuration de OPT2 (Pfsyc = interface qui relie les 2 pfsense) sur le serveur maitre :

```

Enter an option: 2

Available interfaces:

1 - WAN (vnx0 - static)
2 - LAN (vnx1 - static)
3 - OPT1 (vnx2 - static)
4 - OPT2 (vnx3)

Enter the number of the interface you wish to configure: 4

Enter the new OPT2 IPv4 address. Press <ENTER> for none:
> 192.168.60.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT2 IPv4 subnet bit count (1 to 32):
> 30

For a WAN, enter the new OPT2 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> █

```

Configuration de OPT2 (Pfsyc = interface qui relie les 2 pfsense) sur le serveur secondaire :

```

Enter an option: 2

Available interfaces:

1 - WAN (vnx0 - static)
2 - LAN (vnx1 - static)
3 - OPT1 (vnx2 - static)
4 - OPT2 (vnx3)

Enter the number of the interface you wish to configure: 4

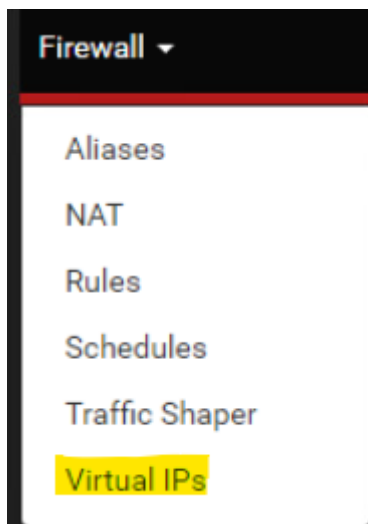
Enter the new OPT2 IPv4 address. Press <ENTER> for none:
> 192.168.60.2

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT2 IPv4 subnet bit count (1 to 32):
> 30

```

- On va maintenant attribuer l'adresse ip virtuelle au 2 serveurs Pfsense
- Il faut aller dans Firewall>Virtual IPs



[Création de l'ip virtuelle du LAN :](#)

Sur le serveur maitre :

pfSense.home.arpa - Firewall: Virtual IP

Non sécurisé | 172.16.2.252/firewall_virtual_ip_edit.php

pf

Non sécurisé

172.16.2.252/firewall_virtual_ip_edit.php

Aa

☆

🔖

👤

⋮

Edit Virtual IP

Type

☐ IP Alias

☒ CARP

☐ Proxy ARP

☐ Other

Interface

LAN

Address type

Single address

Address(es)

172.16.2.254

/

24

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password

Enter the VHID group password.

Confirm

Confirm

VHID Group

2

Enter the VHID group that the machines will share.

Advertising frequency

Base

1

Skew

0

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

Description

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

Save

Sur le serveur secondaire :

pfSense.home.arpa - Firewall: Virtual IP

Non sécurisé | 172.16.2.253/firewall_virtual_ip_edit.php

Edit Virtual IP

Type ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface LAN

Address type Single address

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

Virtual IP Password
Enter the VHID group password. Confirm

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

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

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







Save

[Création de l'ip virtuelle du WAN :](#)

Sur le serveur maître :

Firewall / Virtual IPs







The changes have been applied successfully.

Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
192.168.211.172/24 (vhid: 1)	WAN	CARP		 
172.16.2.254/24 (vhid: 2)	LAN	CARP		 
10.10.1.254/24 (vhid: 3)	OPT1	CARP		 

Sur le serveur secondaire :

Firewall / Virtual IPs ?

The changes have been applied successfully. ×

Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
192.168.211.172/24 (vhid: 1)	WAN	CARP		 
172.16.2.254/24 (vhid: 2)	LAN	CARP		 
10.10.1.254/24 (vhid: 3)	OPT1	CARP		 

- Maintenant que nous avons configuré les adresses ip virtuelles on va configurer la synchronisation entre les pfsenses

Configuration de la synchronisation entre les Pfsense

- Sur le serveur maître :

pfSense.home.arpa - System: Hig x +

Non sécurisé | 172.16.2.252/system_hasync.php

State Synchronization Settings (pfsync)

Synchronize states

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

Synchronize Interface

OPT2

▼

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

pfsync Synchronize Peer IP

192.168.60.2

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

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP

192.168.60.2

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

XMLRPC sync is currently only supported over connections using the same protocol and port

Select options
to sync

☒ User manager users and groups

☒ Authentication servers (e.g. LDAP, RADIUS)

☒ Certificate Authorities, Certificates, and Certificate Revocation Lists

☒ Firewall rules

☒ Firewall schedules

☒ Firewall aliases

☒ NAT configuration

☒ IPsec configuration

☒ OpenVPN configuration (Implies CA/Cert/CRL Sync)

☒ DHCP Server settings

☒ DHCP Relay settings

☒ DHCPv6 Relay settings

☒ WoL Server settings

☒ Static Route configuration

☒ Virtual IPs


☒ Traffic Shaper configuration

☒ Traffic Shaper Limiters configuration

☒ DNS Forwarder and DNS Resolver configurations

☒ Captive Portal

☒ Toggle All

 Save

- Il faut bien mettre l'adresse ip de l'interface OPT2 du serveur secondaire quand on est sur le serveur maitre et vice versa
- Pour le serveur secondaire :

State Synchronization Settings (pfsync)

**Synchronize
states**

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

**Synchronize
Interface**

OPT2

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

**pfsync
Synchronize
Peer IP**

192.168.60.1

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

Configuration Synchronization Settings (XMLRPC Sync)

**Synchronize
Config to IP**

192.168.60.1

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

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP

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

XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username

Enter the webConfigurator username of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password

Enter the webConfigurator password of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and password option on backup cluster members!

Confirm

Synchronize admin

☐ synchronize admin accounts and autoupdate sync password.

By default, the admin account does not synchronize, and each node may have a different admin password.

This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

- Il faut donc mettre l'adresse ip du serveur maître quand on configure le serveur secondaire (on met toujours l'adresse ip du serveur en face de celui qu'on configure)
- Il faut maintenant faire une règle de filtrage qui autorise tout car par défaut pfsync refuse tout on va donc faire la règle de filtrage

Firewall / Rules / OPT2

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor the filter reload progress.](#)

Floating WAN LAN OPT1 **OPT2** OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 0 B	IPv4	*	*	*	*	*	none		<div></div> <div></div> <div></div>

Add Add Delete Save Separator

- Il faut créer sur les deux pfsenses