

DOCUMENTATION PROJET BMS

Jolan Noirot

BTS SIO 2

Jolan NOIROT

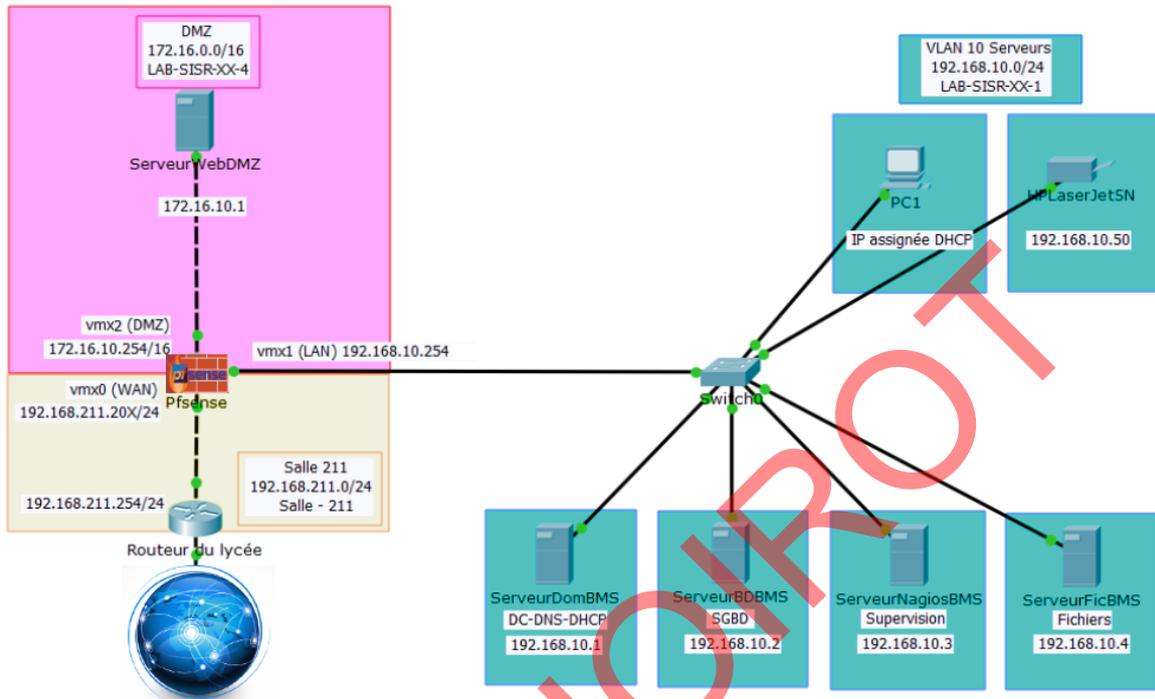


SOMMAIRE

INTRODUCTION	3
RESEAU A REALISER	3
SYSTEMES D'EXPLOITATION	3
IDENTIFIANTS	4
RESEAUX :	4
MISSION 1 : INSTALLATION DU SERVEUR DE DOMAINE BMS.LOCAL SERVEURDOMBMS, DU SERVEUR DE FICHIERS SERVEURFICBMS, DE L'IMPRIMANTE HPLASERJET5N, ET DU CLIENT PC1	5
MISSION 1 A : INSTALLATION DU CONTROLEUR DE DOMAINE	5
MISSION 1 B : INSTALLATION D'UN SERVEUR DE FICHIERS.....	5
MISSION 1 C : INSTALLATION DU POSTE CLIENT PC1	6
MISSION 1 D : INSTALLATION/DEPLOIEMENT DE L'IMPRIMANTE SUR LES POSTES.....	6
MISSION 2 : INSTALLATION ET CONFIGURATION GENERALE DU ROUTEUR-PARE-FEU PFSense.. 12	
MISSION 2 A : INSTALLATION DU PFSense.....	12
MISSION 3 : GESTION DE L'ACTIVE DIRECTORY (UTILISATEURS, DROITS D'ACCES AUX DOSSIERS, GPO)	15
MISSION 3 A : INSTALLATION/DEPLOIEMENT DE LOGICIELS SUR LES POSTES.....	15
MISSION 3 B : CREATION DES UTILISATEURS AVEC LEUR DOSSIER PERSONNEL DE BASE ; CONFIGURATION D'AUTORISATIONS SPECIFIQUES A CERTAINS DOSSIERS	16
MISSION 4 : SUPERVISION NAGIOS	19
MISSION 5 : MAPPAGE AUTOMATIQUE D'UN LECTEUR RESEAU	28
MISSION 5 A : CREATION D'UN SCRIPT POWERSHELL ET D'UNE GPO POUR MAPPAGE AUTOMATIQUE D'UN LECTEUR RESEAU	28
MISSION 6 : INSTALLATION DU SERVEUR DE BASES DE DONNEES SERVEURBDBMS, DU SERVEUR WEB SERVEURWEBDMZ, ET DE L'APPLICATION DE GESTION DES FRAIS	31
MISSION 6 A : INSTALLATION ET CONFIGURATION DU SERVEUR DE BASES DE DONNEES ET DE L'APPLICATION DE GESTION DES FRAIS.....	31
MISSION 7 : CONFIGURATION DES REGLES DE FILTRAGE DU ROUTEUR-PARE-FEU PFSense	38
MISSION 7 A : REGLES MINIMUM A CONFIGURER SUR L'INTERFACE DMZ DU PFSense	38
MISSION 7 B : REGLES MINIMUM A CONFIGURER SUR L'INTERFACE LAN DU PFSense.....	38
MISSION 7 C : REGLES MINIMUM A CONFIGURER SUR L'INTERFACE WAN DU PFSense	38
MISSION 7 D : REDIRECTION POUR ACCEDER DEPUIS INTERNET AU SERVEURWEBDMZ	39

INTRODUCTION

RÉSEAU À RÉALISER



SYSTÈMES D'EXPLOITATION

<u>Machine Virtuelle</u>	<u>Système d'exploitation</u>	<u>IP</u>	
ServeurDomBMS	Windows Serveur 2022 21H2	192.168.10.1	
ServeurBDBMS	Windows Serveur 2022 21H2	192.168.10.2	
ServeurNagiosBMS	Debian 11	192.168.10.3	
ServeurFicBMS	Windows Serveur 2022 21H2	192.168.10.4	
PC1	Windows 11 Education 22H2	DHCP	
ServeurWebDMZ	Windows Serveur 2022 21H2	172.16.10.1	
pfSense	FreeBSD	WAN	192.168.211.208/24
		LAN	192.168.10.254/24
		DMZ	172.16.10.254/16

IDENTIFIANTS

<u>Systeme d'exploitation</u>	<u>Identifiant</u>	<u>Mot de passe</u>
Windows	Administrateur	Windows2022
Debian	root	root

RÉSEAUX :

<u>SALLE - 211</u>	<u>LAB - SISR - 08 - 1</u>	<u>LAB - SISR - 08 - 4</u>
<ul style="list-style-type: none">• pfSense	<ul style="list-style-type: none">• pfSense• ServeurDomBMS• ServeurBDBMS• ServeurFicBMS• ServeurNagiosBMS• PC1	<ul style="list-style-type: none">• pfSense• ServeurWebDMZ

Jolan NOBROT

MISSION 1 : INSTALLATION DU SERVEUR DE DOMAINE BMS.LOCAL SERVEURDOMBMS, DU SERVEUR DE FICHIERS SERVEURFICBMS, DE L'IMPRIMANTE HPLASERJET5N, ET DU PC CLIENT PC1

MISSION 1 A : INSTALLATION DU CONTRÔLEUR DE DOMAINE

Une fois le ServeurDomBMS configuré en ip statique et avec un nom, aller dans le gestionnaire de serveur et ajouter les rôles :

- ADDS
- DNS
- DHCP

Promouvoir le serveur en Contrôleur de domaine. Ensuite on ajoute une forêt avec pour nom "BMS.local".

MDP : Windows2022

Et ont fini sa configuration comme d'habitude.

MISSION 1 B : INSTALLATION D'UN SERVEUR DE FICHIERS

Une fois le ServeurDomBMS configuré en ip statique et avec un nom et ajouter au domaine (on n'oublie pas que le domaine c'est BMS.local). Sur le ServeurDomBMS aller dans le gestionnaire de serveur et cliquer sur Ajouter d'autres serveurs à gérer et sélectionner ServeurFicBMS, ensuite retourner sur ServeurFicBMS et ouvrir l'explorateur de fichiers. Se rendre sur la racine du disque C: et créer un dossier REPBASES et un dossier PUBLIC. Partager les deux fichiers en faisant clic droit, propriétés et Partage avancé, cocher la case Partager ce dossier mettant contrôle total à tout le monde. On applique. 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).

Cliquer sur le bouton Avancé de la fenêtre Propriétés de REPBASES. Puis cliquer sur le bouton : Désactiver l'héritage de la fenêtre Paramètres de sécurité avancés pour REPBASES

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.

Supprimer toutes les autorisations accordées à Utilisateurs (du domaine):

- cliquer sur le bouton Modifier
- Sélectionner Utilisateurs (du domaine)
- cliquer sur le bouton Supprimer

MISSION 1 C : INSTALLATION DU POSTE CLIENT PC1

Configurer un nom une adresse IP et l'ajouter au domaine comme vue dans les précédents TPs.

MISSION 1 D : INSTALLATION/DÉPLOIEMENT DE L'IMPRIMANTE SUR LES POSTES

Sur le ServeurDomBMS, ajouter le rôle Serveur d'impression, une fois cela fait, dans le DHCP faire une nouvelle réservation pour l'imprimante :

Nouvelle réservation ? X

Fournissez les informations pour un client réservé.

Nom de réservation : LaserJet 5200

Adresse IP : 192 . 168 . 10 . 50

Adresse MAC : 0060B06FB123

Description : Imprimante LaserJet 5200

Types pris en charge

Les deux

DHCP

BOOTP

Ajouter Fermer

Sélectionner Panneau de configuration / Matériel, Périphériques et imprimantes le serveur recherche alors l'imprimante ; comme il s'agit ici d'une imprimante "fictive", cliquer sur le lien L'imprimante souhaitée n'est pas indiquée.

← Ajouter une imprimante

Rechercher une imprimante par d'autres options

- M'aider à trouver mon imprimante un peu plus ancienne
- Rechercher une imprimante dans l'annuaire, en fonction d'un emplacement
- Sélectionner une imprimante partagée par nom

Exemple : \\ordinateur\imprimante ou
http://ordinateur/printers/imprimante/.printer

- Ajouter une imprimante à l'aide d'une adresse IP ou d'un nom d'hôte
- Ajouter une imprimante Bluetooth, sans fil ou réseau détectable
- Ajouter une imprimante locale ou réseau avec des paramètres manuels

Créer un nouveau port :

Type de port :

Standard TCP/IP Port

Type de périphérique :

Périphérique TCP/IP

Nom d'hôte ou adresse IP :

192.168.10.50

Nom du port :

LaserJet 5200

- Interroger l'imprimante et sélectionner automatiquement le pilote à utiliser

Informations supplémentaires requises concernant le port

Ce périphérique est introuvable sur le réseau. Vérifiez que :

1. Le périphérique est allumé.
2. Vous êtes connecté au réseau.
3. Le périphérique est configuré correctement.
4. L'adresse de la page précédente est correcte.

Si vous pensez que l'adresse est incorrecte, cliquez sur Précédent pour revenir à la page précédente. Corrigez l'adresse et effectuez une nouvelle recherche sur le réseau. Si vous êtes sûr que l'adresse est correcte, sélectionnez le type de périphérique ci-dessous.

Type de périphérique

Standard Generic Network Card

Personnalisé Paramètres...

Partage d'imprimante

Si vous voulez partager cette imprimante, vous devez fournir un nom de partage. Vous pouvez utiliser le nom suggéré ou en entrer un autre. Le nom de partage sera visible par les autres utilisateurs du réseau.

Ne pas partager cette imprimante

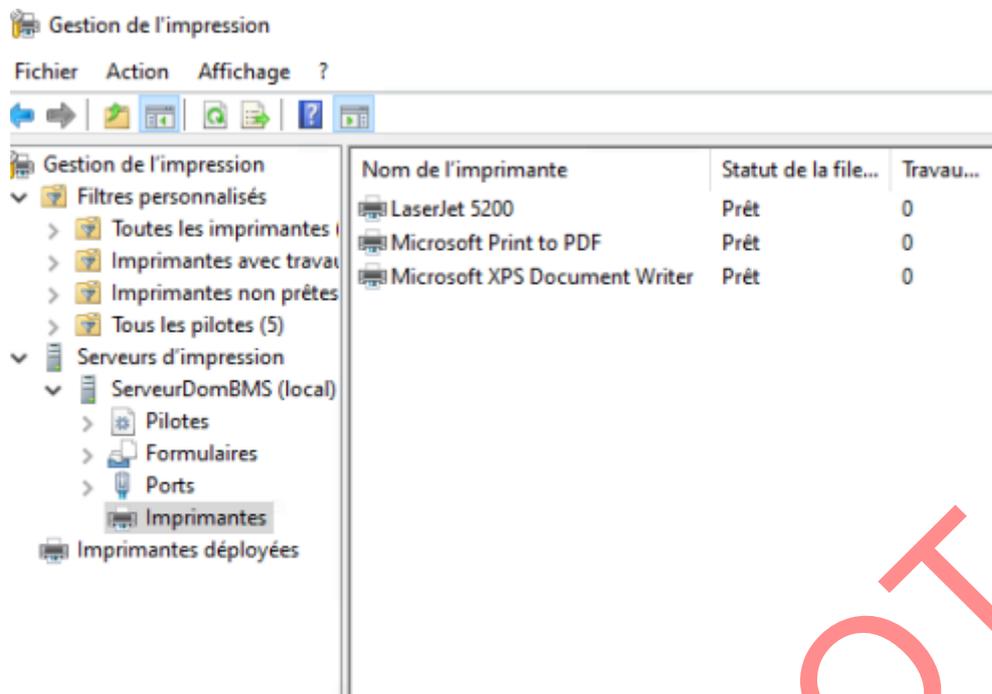
Partager cette imprimante afin que d'autres utilisateurs puissent l'utiliser

Nom du partage :

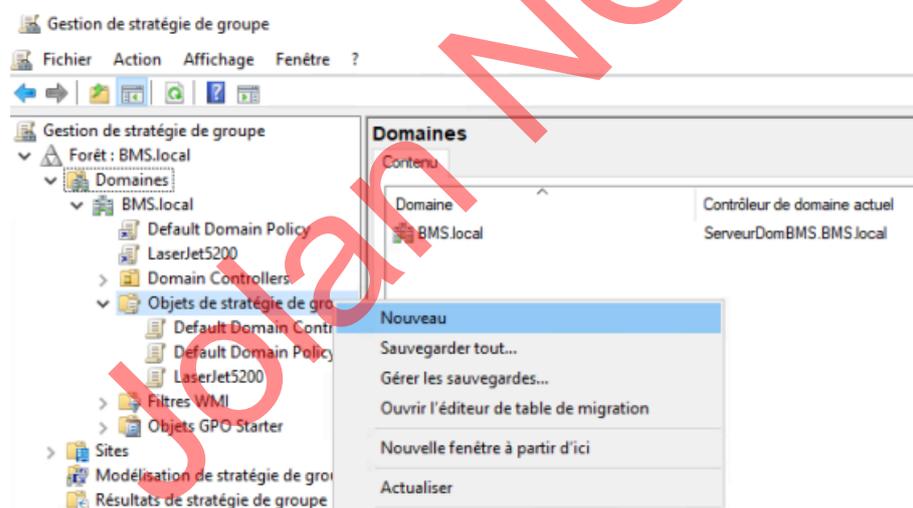
Emplacement :

Commentaire :

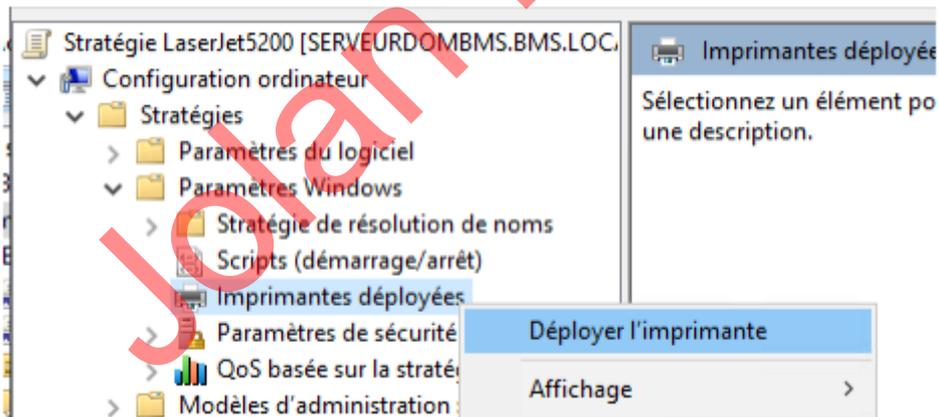
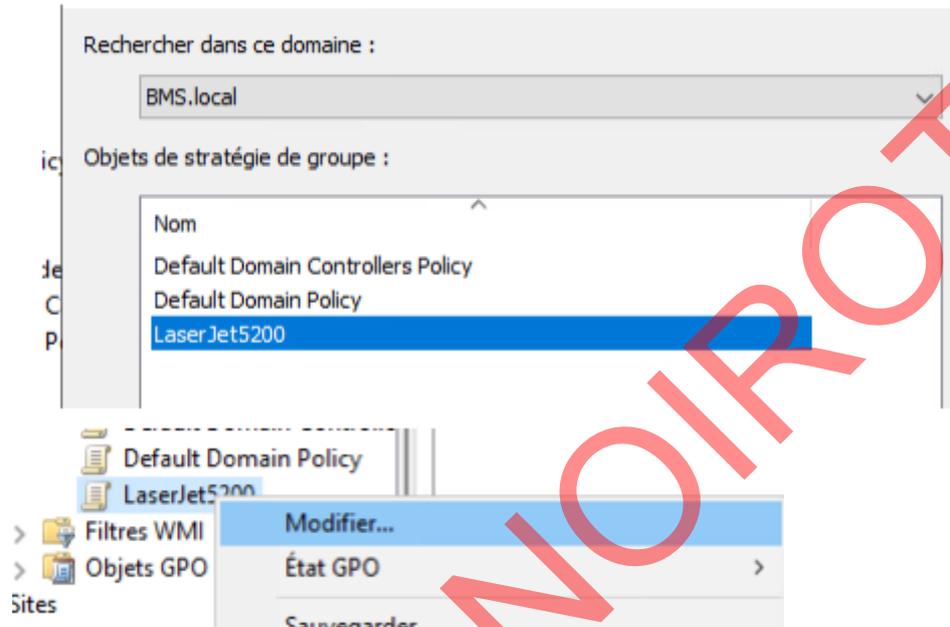
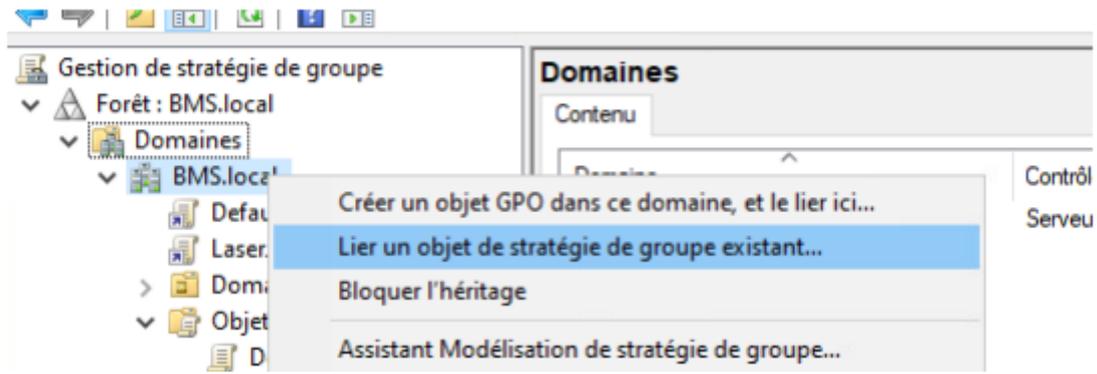
Ensuite dans outils du gestionnaire de serveurs, aller dans gestion de l'impression :



Une fois que l'imprimante est bien visible ici, retourner dans le gestionnaire de serveur/outils/Gestion des stratégies de groupe.



Nom : LaserJet5200
 Objet starter GPO source : Aucun



Déployer des imprimantes

Entrez le nom d'imprimante :
(exemple : \\serveur\nom_imprimante)

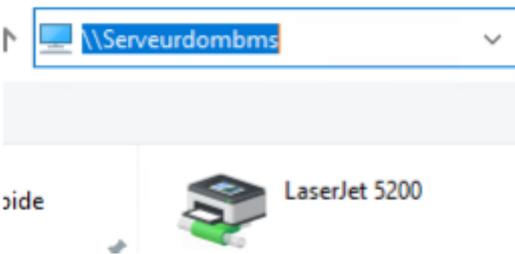
\\ServeurDomBMS\LaserJet 5200

Ajouter >>

Parcourir...

<< Supprimer

Déployer ces imprimantes
stratégie de gestion



Jolan NOIROU

MISSION 2 : INSTALLATION ET CONFIGURATION GÉNÉRALE DU ROUTEUR-PARE-FEU PFSENSE

MISSION 2 A : INSTALLATION DU PFSENSE

```
ocal Database)

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 8d945a1e3a11a33bdf03
*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vmx0      -> v4: 192.168.211.208/24
LAN (lan)      -> vmx1      -> v4: 192.168.10.254/24
DMZ (opt1)     -> em0       -> v4: 172.16.10.254/16

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: █
```

On va configurer le DHCP, aller sur ServeurDomBMS
Outil > DHCP puis serveurighbms > IPv4 (cliques droit dessus puis nouvelle étendue)

Plage d'adresses IP

Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.



Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début :

Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP.

Longueur :

Masque de sous-réseau :

< Précédent **Suivant >** Annuler

Adresse IP :

Ajouter

Supprimer

Monter

Descendre

Nom de domaine et serveurs DNS

DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.



Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

Domaine parent :

Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

Nom du serveur :	Adresse IP :	
<input type="text" value="ServeurDomBMS"/>	<input type="text" value=""/>	Ajouter
<input type="button" value="Résoudre"/>	<input type="text" value="192.168.10.1"/>	Supprimer
		Monter
		Descendre

Ne pas ajouter de serveurs WINS

Activer le DHCP
Puis lancer le PC1 et vérifier avec ipconfig

Jolan NOIROT

MISSION 3 : GESTION DE L'ACTIVE DIRECTORY (UTILISATEURS, DROITS D'ACCÈS AUX DOSSIERS, GPO)

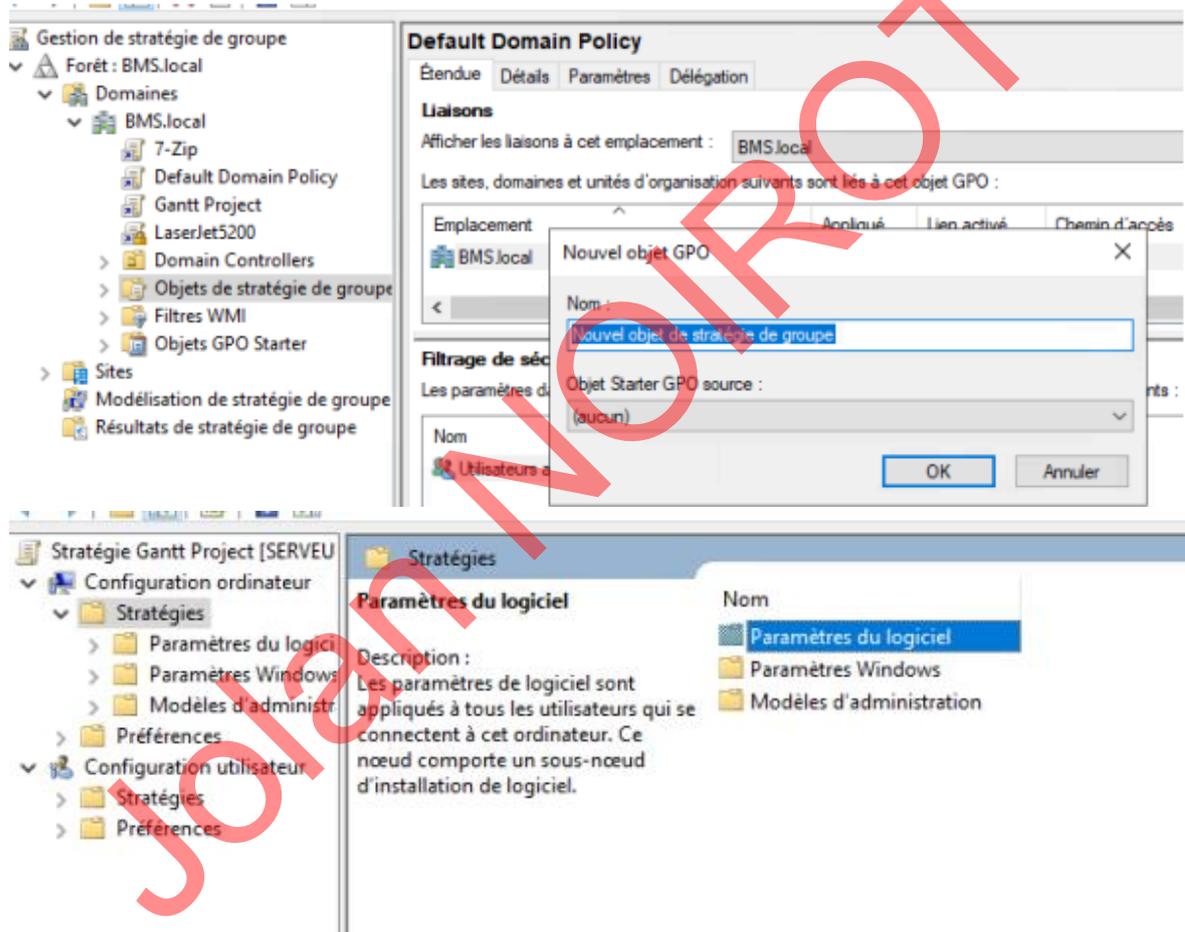
MISSION 3 A : INSTALLATION/DÉPLOIEMENT DE LOGICIELS SUR LES POSTES

Aller chercher les fichiers dans :

\\192.168.216.74/docs/dosDeProfs/Naville/BTS-SIO-2

Et les sauvegarder dans : \\ServeurDomBMS\NETLOGON

Ensuite aller dans le Gestionnaire de stratégies de groupe :



Ensuite dans un terminal en administrateur entrer la commande :
gpupdate /force

MISSION 3 B : CRÉATION DES UTILISATEURS AVEC LEUR DOSSIER PERSONNEL DE BASE ; CONFIGURATION D'AUTORISATIONS SPÉCIFIQUES À CERTAINS DOSSIERS

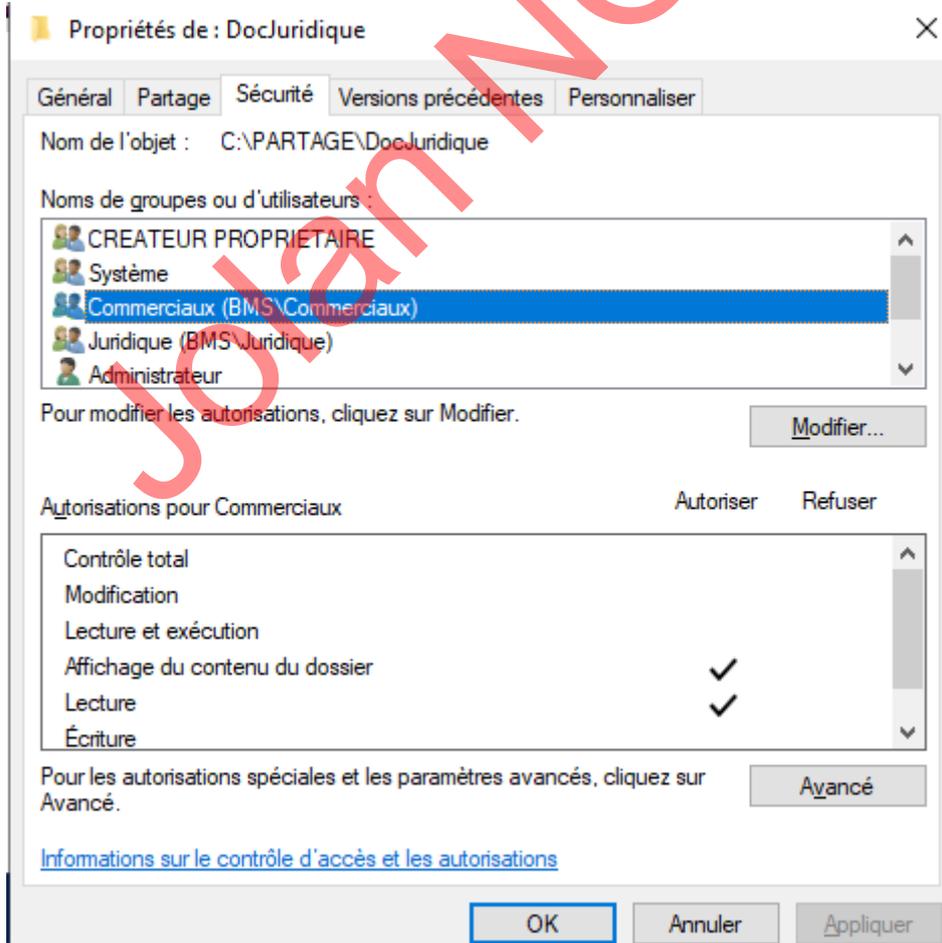
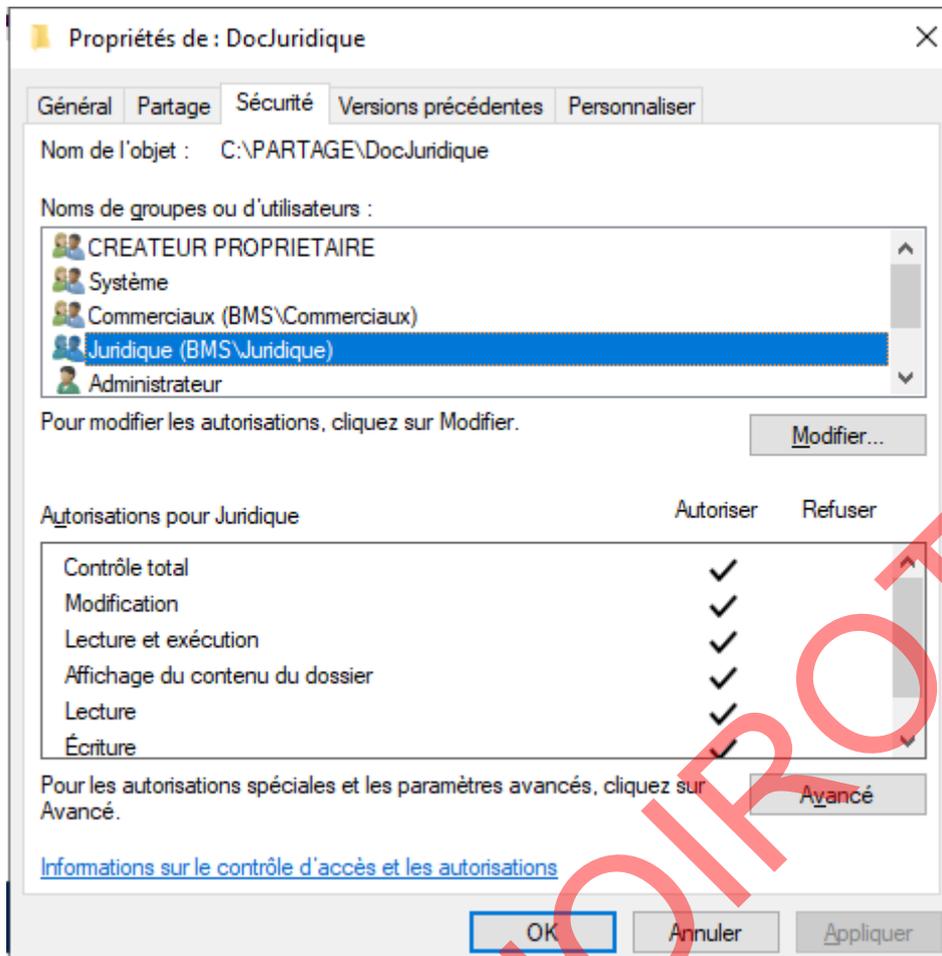
Créer les utilisateurs suivants dans l'AD :

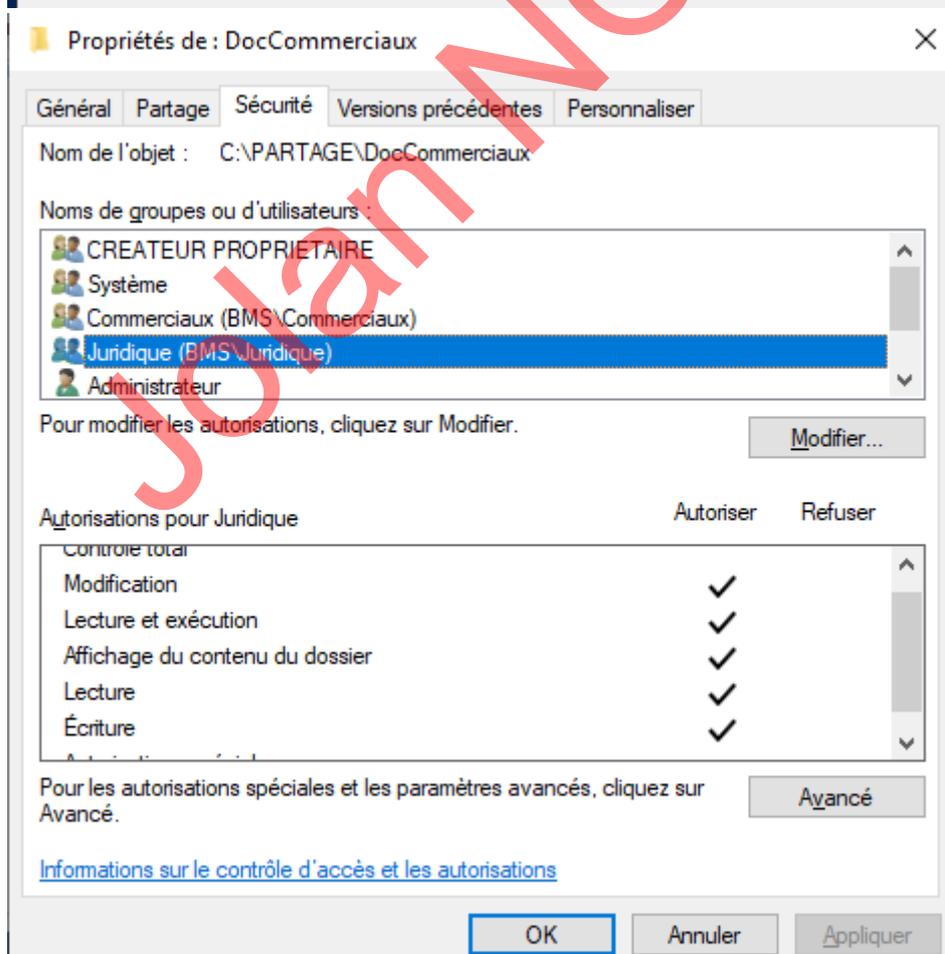
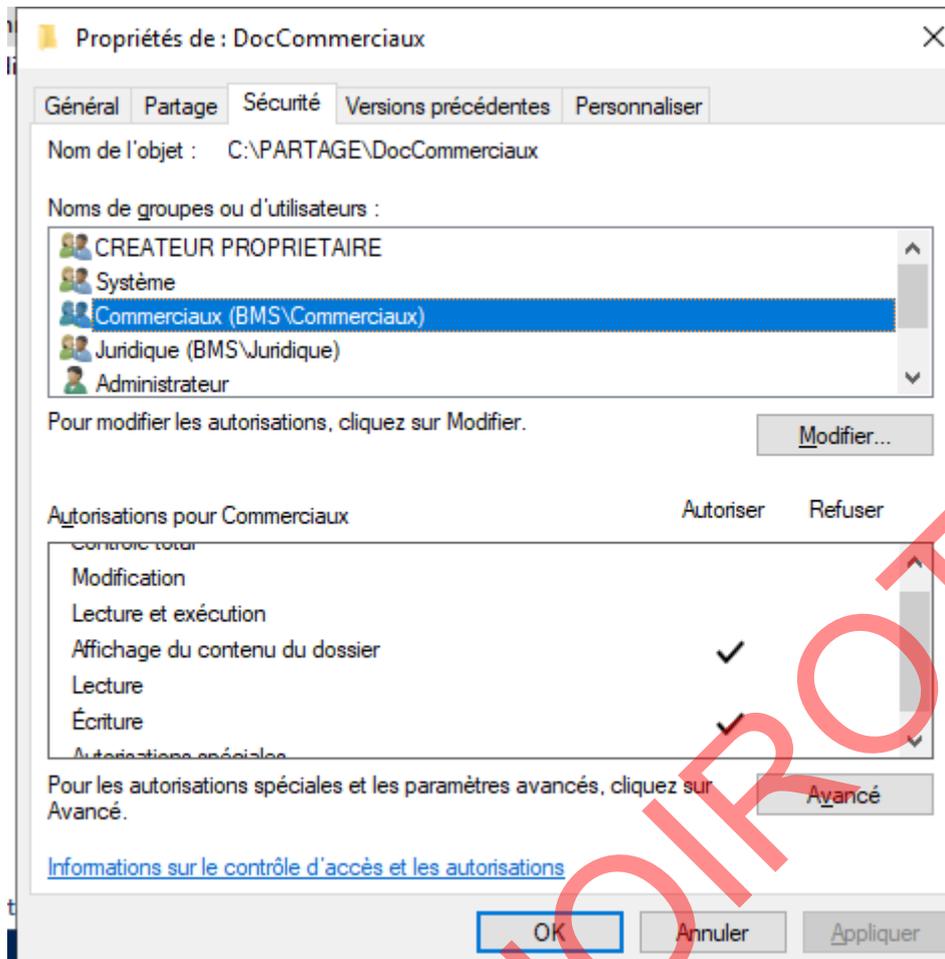
<i>Nom et prénom</i>	<i>Nom d'ouverture de session</i>	<i>Nom du dossier personnel</i>	<i>Mot de passe</i>
Charles Dupont	cdupont	cdupont	Windows2019
Albert Dubois	adubois	adubois	Windows2019
Clémence Rousseau	crousseau	crousseau	Windows2019
Vincent Ogier	vogier	vogier	Windows2019
Louis Ravignac	lravignac	lravignac	Windows2019

Créer les groupes suivants dans l'AD :

Nom de groupe	Etendue	Type	Membres du groupe
Commerciaux	Domaine local	Sécurité	Charles Dupont Clémence Rousseau
Juridique	Domaine local	Sécurité	Albert Dubois Vincent Ogier

Dans le répertoire Partage du ServeurFicBMS créer le répertoire DocJuridique et le répertoire DocCommerciaux avec les autorisations aux groupes suivant :





MISSION 4 : SUPERVISION NAGIOS

Dans l'explorateur de fichiers pcmanfm, pour accéder au serveur SRV-BTSSIO d'adresse 192.168.216.74, taper smb://192.168.216.74/docs :



InstallNagios
4v2.sh

```
cd /root
./InstallNagios4v2.sh
reboot à la fin
/usr/local/nagios/etc/objects/templates.cfg
```

```
templates.cfg
Fichier Édition Rechercher Options Aide
51 define host{
52     name                generic-host    ; The name of this host template
53     notifications_enabled 1            ; Host notifications are enabled
54     event_handler_enabled 1            ; Host event handler is enabled
55     flap_detection_enabled 1           ; Flap detection is enabled
56     check_interval       2            ; Actively check the host every 2 minut
57     retry_interval       1            ; Schedule host check retries at 1 minu
58     max_check_attempts   3            ; Check each server 3 times (max)
59     check_command        check_host_alive ; Default command to check hosts
60     process_perf_data    1            ; Process performance data
61     retain_status_information 1        ; Retain status information across prog
62     retain_nonstatus_information 1    ; Retain non-status information across
63     notification_period  24x7        ; Send host notifications at any time
64     register             0            ; DONT REGISTER THIS DEFINITION - ITS N
65 }
66

templates.cfg
Fichier Édition Rechercher Options Aide
154 define service{
155     name                generic-service ; The 'name' of this service te
156     active_checks_enabled 1            ; Active service checks are enal
157     passive_checks_enabled 1          ; Passive service checks are en
158     parallelize_check    1            ; Active service checks should
159     obsess_over_service  1            ; We should obsess over this se
160     check_freshness      0            ; Default is to NOT check servi
161     notifications_enabled 1            ; Service notifications are enal
162     event_handler_enabled 1            ; Service event handler is enab
163     flap_detection_enabled 1          ; Flap detection is enabled
164     process_perf_data    1            ; Process performance data
165     retain_status_information 1        ; Retain status information acr
166     retain_nonstatus_information 1    ; Retain non-status information
167     is_volatile          0            ; The service is not volatile
168     check_period         24x7        ; The service can be checked at
169     max_check_attempts   3            ; Re-check the service up to 3
170     check_interval       2            ; Check the service every 2 min
171     retry_interval       1            ; Re-check the service every mi
172     contact_groups       admins      ; Notifications get sent out to
173     notification_options w,u,c,r     ; Send notifications about warn
174     notification_interval 60         ; Re-notify about service probl
175     notification_period  24x7        ; Notifications can be sent out
176     register             0            ; DONT REGISTER THIS DEFINITION
177 }
178
179
```

Puis dans nano /usr/local/nagios/etc/nagios.cfg

```
<nagios.cfg>
Fichier  Edition  Recherche  Options  Aide

# OBJECT CONFIGURATION FILE(S)
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

# You can specify individual object config files as shown below:
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg
cfg_file=/usr/local/nagios/etc/objects/monReseau.cfg

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# Definitions for monitoring a Windows machine
```

```
GNU nano 3.2 monReseau.cfg

define host {
    use          generic-host
    host_name    SERVEUR1
    alias        Serveur Windows Serveur1
    address      192.168.10.1
}

}
```

Fichier monReseau.cfg :

```
define host {
    use          generic-host
    host_name    SERVEUR1
    alias        Serveur PDC Windows 2016 SERVEUR1
    address      192.168.3.1
    parents      VSWITCH
    icon_image   server.png
    icon_image_alt Server
    vml_image    server.png
}

}
```

```
define host {
    use          generic-host
    host_name    VSWITCH
    alias        VSWITCH
    address      192.168.3.1
}

}
```

```
    icon_image  switch40.png
    icon_image_alt Switch
    vrml_image  switch40.png
}

define host {
    use          generic-host
    host_name    ROUTEUR-PARE-FEU-PFSENSE
    alias        ROUTEUR-PARE-FEU-PFSENSE
    address      192.168.3.254
    parents      VSWITCH
    icon_image   router40.png
    icon_image_alt Routeur
    vrml_image   router40.png
}

define host {
    use          generic-host
    host_name    PC1
    alias        PC1
    address      192.168.3.10
    parents      VSWITCH
    icon_image   workstation.png
    icon_image_alt Workstation
    vrml_image   workstation.png
}

define hostgroup {
    hostgroup_name SystemesWindows
    alias          Groupe des serveurs et machines Windows
    members        SERVEUR1, PC1
}

define hostgroup {
    hostgroup_name SystemesLinux
    alias          Groupe des serveurs et machines Linux
    members        localhost, ROUTEUR-PARE-FEU-PFSENSE
}

define hostgroup {
    hostgroup_name Commutateurs
    alias          Groupe des commutateurs
    members        VSWITCH
}
```

```
define hostgroup {
    hostgroup_name Routeurs
    alias    Groupe des routeurs
    members  ROUTEUR-PARE-FEU-PFSENSE
}

define hostgroup {
    hostgroup_name ServeursHTTP
    alias    Groupe des serveurs HTTP
    members  SERVEUR1
}

define hostgroup {
    hostgroup_name ServeursDHCP
    alias    Groupe des serveurs DHCP
    members  SERVEUR1
}

define hostgroup {
    hostgroup_name ServeursDNS
    alias    Groupe des serveurs DNS
    members  SERVEUR1
}

define hostgroup {
    hostgroup_name ServeursFTP
    alias    Groupe des serveurs FTP
    members  SERVEUR1
}

define hostgroup {
    hostgroup_name ServeursSNMP
    alias    Groupe des serveurs SNMP
    members  SERVEUR1, localhost
}

define command {
    command_name check_http1
    command_line $USER1$/check_http -I 192.168.3.1
}

define command {
    command_name check_dns1
```

```

        command_line    $USER1$/check_dns -H SERVEUR1 -s
$HOSTADDRESS$
    }

define command {
    command_name    check_dhcp1
    command_line    $USER1$/check_dhcp -s 192.168.3.1 -i ens192
}

define command {
    command_name    check_ftp1
    command_line    $USER1$/check_ftp -H $HOSTADDRESS$
}

define command {
    command_name    check_snmp1
    command_line    $USER1$/check_snmp -H $HOSTADDRESS$ -C
public -o $ARG1$
}

define service {
    use                generic-service
    hostgroup_name     ServeursHTTP
    service_description HTTP
    check_command      check_http1
}

define service {
    use                generic-service
    hostgroup_name     ServeursDNS
    service_description DNS
    check_command      check_dns1
}

define service {
    use                generic-service
    hostgroup_name     ServeursDHCP
    service_description DHCP
    check_command      check_dhcp1
}

define service {
    use                generic-service
    hostgroup_name     ServeursFTP

```

```

    service_description  FTP
    check_command       check_ftp1
}

define service {
    use                 generic-service
    hostgroup_name     ServeursSNMP
    service_description  SNMP SysDesc
    check_command       check_snmp1!.1.3.6.1.2.1.1.1.0
}

define service {
    use                 generic-service
    hostgroup_name     ServeursSNMP
    service_description  SNMP Users
    check_command       check_snmp1!.1.3.6.1.2.1.25.1.5.0
}

```

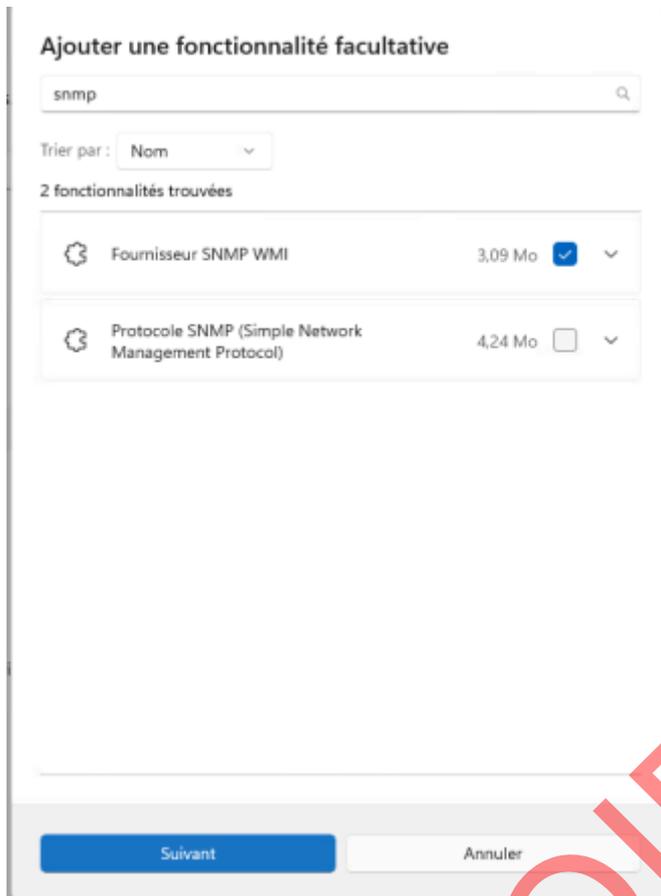
Redémarrer le service nagios avec la commande suivante (à faire après chaque modification d'un fichier de configuration .cfg) :

```
systemctl restart nagios
```

Installation de l'agent SNMP sur chaque poste du réseau à superviser avec SNMP Pour installer et configurer l'agent SNMP sur Microsoft Windows 10 :

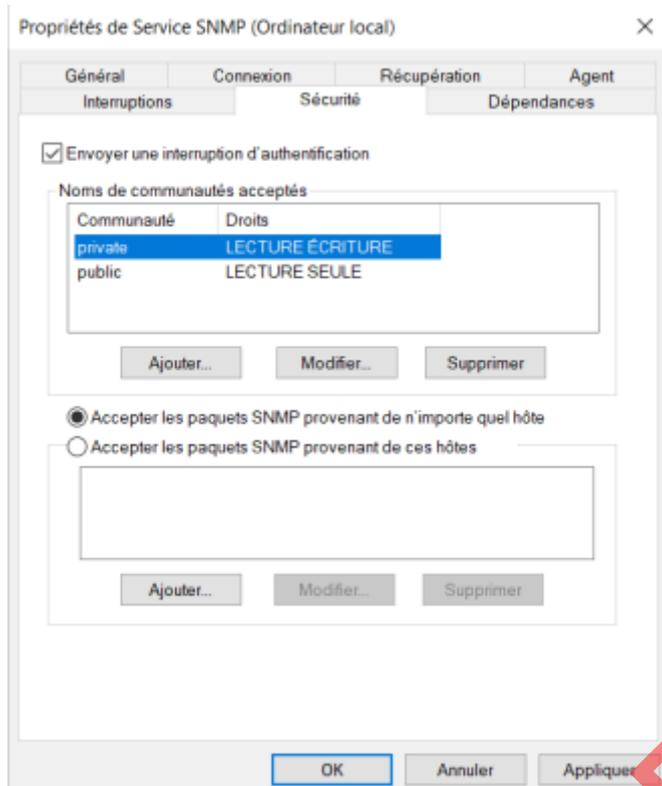
Se connecter en Administrateur, puis sélectionner Paramètres / Applications / Applications et fonctionnalités / Fonctionnalités facultatives ; vérifier que la fonctionnalité Protocole SNMP (Simple Network Management Protocol) est bien installée (sinon, l'installer) ; cliquer sur Ajouter une fonctionnalité, puis installer la fonctionnalité Fournisseur SNMP WMI ;





Sélectionner Panneau de configuration / Système et sécurité / Outils d'administration ; dans la liste des outils d'administration, sélectionner Services ; dans la liste des services, sélectionner Service SNMP ; Vérifier que le service a bien démarré (normalement le démarrage est automatique).

Dans l'onglet Agent, cocher tous les services



Dans l'onglet Sécurité, cocher la case Accepter les paquets SNMP provenant de n'importe quel hôte Dans l'onglet Sécurité, ajouter les deux noms de communauté suivants avec leurs droits respectifs : private (lecture - écriture) public (lecture seule)

Pour installer et configurer l'agent SNMP sur Microsoft Windows Server 2019/2022 :

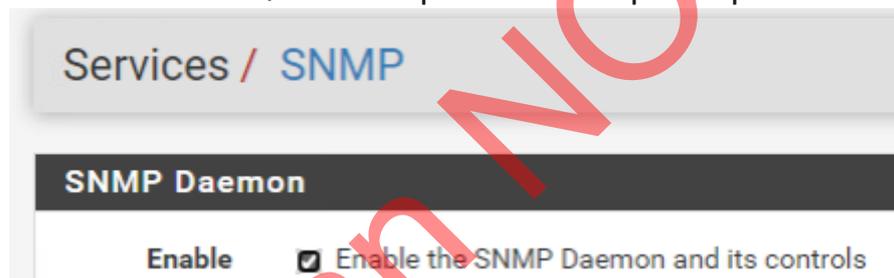
- Ajouter d'abord la fonctionnalité Service SNMP au serveur (Gestionnaire de serveur , Gérer, Ajouter des rôles et fonctionnalités ; sur SERVEUR1, ajouter la fonctionnalité Service SNMP).
- Sélectionner ensuite Panneau de configuration / Système et sécurité / Outils d'administration ; dans la liste des outils d'administration, sélectionner Services ; dans la liste des services, sélectionner Service SNMP ;
- Vérifier que le service est bien démarré (normalement le démarrage est automatique).
- Dans l'onglet Agent, cocher tous les services
- Dans l'onglet Sécurité, cocher la case Accepter les paquets SNMP provenant de n'importe quel hôte
- Dans l'onglet Sécurité, ajouter les deux noms de communauté suivants avec leurs droits respectifs : private (lecture - écriture) public (lecture seule)

Pour installer et configurer l'agent SNMP sur Linux :

- a. Exécuter la commande permettant l'installation du démon SNMP, du protocole et des Mibs : `apt-get install snmpd snmp`
- b. Configurer le démon `snmpd` de la machine à surveiller en modifiant le fichier `snmpd.conf` avec la commande `leafpad /etc/snmp/snmpd.conf`
 - Configurer le démon `snmpd` pour qu'il écoute le réseau : `AgentAddress udp:161,udp6:[::1]:161` (enlever le commentaire `#` devant la ligne) et qu'il n'écoute pas que l'hôte local (mettre en commentaire la ligne `AgentAddress udp:localhost:161`)
 - Lui indiquer la hiérarchie des OID à rendre visible à tous : ajouter `View systemonly included .1.3.6.1` et supprimer tous les autres `View Systemonly ...`
 - Vérifier que le nom de communauté publique est bien public : `rocommunity public default -V systemonly`
- c. Redémarrer le démon `snmpd` avec la commande `systemctl restart snmpd`.

Pour installer et configurer l'agent SNMP sur un routeur pare-feu PfSense :

- a. Sélectionner la commande **Services SNMP**, et cocher la case **SNMP Daemon Enable** ; vérifier que le mot de passe pour la lecture est public.



Pour autoriser certains plugins,

```
sudo chown -R root:root /usr/local/nagios/libexec/*  
sudo chmod -R u+s /usr/local/nagios/libexec/*
```

MISSION 5 : MAPPAGE AUTOMATIQUE D'UN LECTEUR RÉSEAU

MISSION 5 A : CRÉATION D'UN SCRIPT POWERSHELL ET D'UNE GPO POUR MAPPAGE AUTOMATIQUE D'UN LECTEUR RÉSEAU

Sur ServeurDomBMS

```
# Variables pour les chemins des dossiers partagés
$pathCommerciaux = "\\ServeurFicBMS.BMS.local\PARTAGE\DocCommerciaux"
$pathJuridique = "\\ServeurFicBMS.BMS.local\PARTAGE\DocJuridique"

# Groupes AD
$groupCommerciaux = "Commerciaux"
$groupJuridique = "Juridique"

# Récupérer le nom d'utilisateur actuel depuis les variables d'environnement
$login = $Env:USERNAME

# Importer le module Active Directory si nécessaire
Import-Module ActiveDirectory

# Vérifier si l'utilisateur fait partie d'un groupe spécifique
function Is-UserInGroup {
    param (
        [string]$username,
        [string]$groupName
    )

    # Récupérer les membres du groupe AD
    $groupMembers = Get-ADGroupMember -Identity $groupName | Select-Object -
ExpandProperty SamAccountName

    # Vérifier si l'utilisateur est membre du groupe
    return $groupMembers -contains $username
}

# Fonction pour mapper un lecteur réseau
function Map-NetworkDrive {
    param (
        [string]$driveLetter,
        [string]$folderPath
    )

    # Vérifier si le lecteur réseau est déjà mappé
    if (!(Get-PSDrive -Name $driveLetter -ErrorAction SilentlyContinue)) {
        New-PSDrive -Name $driveLetter -PSProvider FileSystem -Root $folderPath -
Persist -Scope Global
        Write-Host "Le lecteur réf@seau $driveLetter a été@mappé@ vers
$folderPath"
    } else {
        Write-Host "Le lecteur $driveLetter est déjà@mappé@."
    }
}

# Mapper les lecteurs réseau en fonction de l'appartenance aux groupes
if (Is-UserInGroup -username $login -groupName $groupCommerciaux) {
    Map-NetworkDrive -driveLetter "X" -folderPath $pathCommerciaux
}

if (Is-UserInGroup -username $login -groupName $groupJuridique) {
    Map-NetworkDrive -driveLetter "Y" -folderPath $pathJuridique
}
```

Générer un certificat auto-signé

Si vous n'avez pas de certificat de signature de code provenant d'une autorité de certification (CA), vous pouvez créer un certificat auto-signé.

Étape 1 : Générer un certificat auto-signé :

Ouvrir PowerShell en tant qu'administrateur et exécuter la commande suivante pour créer un certificat auto-signé pour la signature de scripts :

```
New-SelfSignedCertificate -CertStoreLocation  
Cert:\CurrentUser\My -Subject "CN=ScriptSigner" -KeyUsage  
DigitalSignature -Type CodeSigningCert
```

Cela va générer un certificat auto-signé et le stocker dans le magasin des certificats de l'utilisateur actuel sous Cert:\CurrentUser\My.

Étape 2 : Exporter le certificat dans le magasin de confiance

Accéder au certificat :

Ouvrir le Gestionnaire de certificats en tapant `certmgr.msc` dans la boîte de dialogue Exécuter (Windows + R).

Aller dans Certificats - Utilisateur actuel > Personnel > Certificats.

Vous devriez voir le certificat que vous venez de créer, nommé ScriptSigner.

Exporter le certificat dans les autorités de confiance :

Faire un clic droit sur le certificat ScriptSigner > Toutes les tâches > Exporter.

Suivre l'assistant d'exportation et choisir d'exporter le certificat sans la clé privée.

Une fois exporté, retourner dans Certificats - Utilisateur actuel.

Aller dans Autorités de certification racine de confiance > Certificats, puis importez le certificat que vous venez d'exporter. Cela permet à votre certificat d'être reconnu comme une autorité de confiance pour la signature de scripts.

Étape 3 : Signer le script PowerShell

Récupérer le certificat :

Exécuter cette commande dans PowerShell pour obtenir le certificat que vous venez de générer :

```
$cert = Get-ChildItem -Path Cert:\CurrentUser\My | Where-Object { $_.Subject -match "CN=ScriptSigner" }
```

Signer votre script :

Utiliser la commande suivante pour signer votre script avec le certificat :

```
Set-AuthenticodeSignature -FilePath  
"C:\chemin\vers\ton_script.ps1" -Certificate $cert
```

Cela va ajouter une signature numérique à votre script.

Étape 4 : Vérifier que le script est signé

Exécuter cette commande pour vérifier la signature du script :

```
Get-AuthenticodeSignature -FilePath  
"C:\chemin\vers\ton_script.ps1"
```

Le statut de la signature devrait être Valid.

Étape 5 : Exécuter le script avec la stratégie "RemoteSigned"

Maintenant que le script est signé, vous pouvez définir la stratégie d'exécution de PowerShell sur RemoteSigned pour autoriser uniquement les scripts signés à s'exécuter. Vous pouvez appliquer cette politique via GPO ou directement sur les postes clients.

Modifier la stratégie d'exécution :

Si ce n'est pas déjà fait, exécuter cette commande sur les postes concernés (ou via GPO) :

```
Set-ExecutionPolicy RemoteSigned -Scope LocalMachine
```

Cette stratégie autorise l'exécution des scripts locaux non signés, mais exige une signature numérique pour les scripts téléchargés ou venant de sources non locales.

Ensuite faire une GPO qui applique le script mais également la stratégie d'exécution à tous les ordinateurs du domaine.

MISSION 6 : INSTALLATION DU SERVEUR DE BASES DE DONNÉES SERVEURBDBMS, DU SERVEUR WEB SERVEURWEBDMZ, ET DE L'APPLICATION DE GESTION DES FRAIS

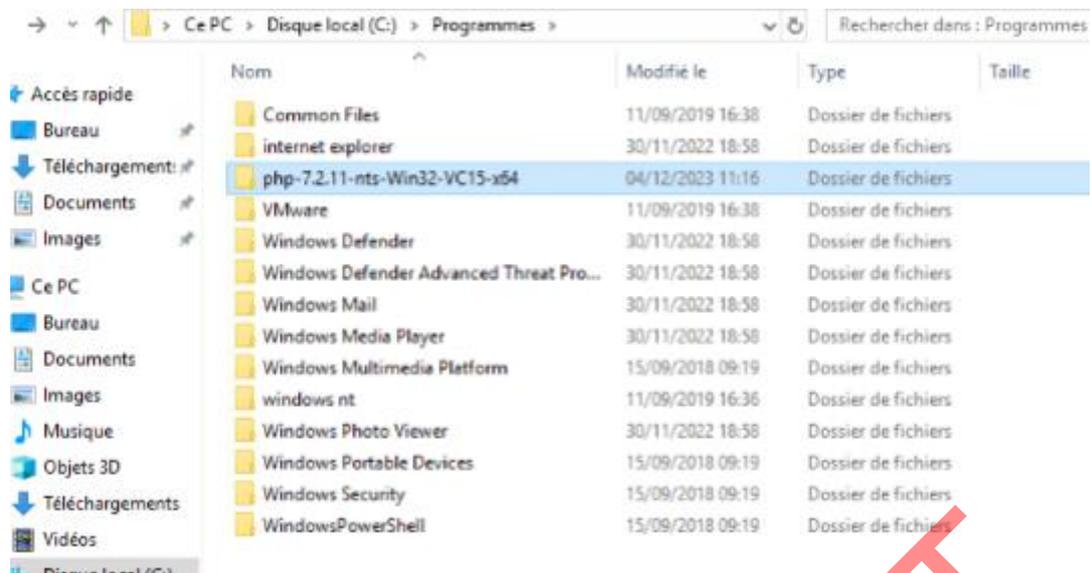
MISSION 6 A : INSTALLATION ET CONFIGURATION DU SERVEUR DE BASES DE DONNÉES ET DE L'APPLICATION DE GESTION DES FRAIS

Créer ServeurWebDMZ et ServeurBDBMS en configurant leur nom et leurs IP mais également en ajoutant ServeurBDBMS au domaine et en l'identifiant en tant que serveur comme vue précédemment.
Installer le rôle Serveur web IIS avec les services de rôle par défaut et le service de rôle CGI (CGI est une interface qui permet à un serveur HTTP de dialoguer avec des programmes externes tels que des programmes PHP).

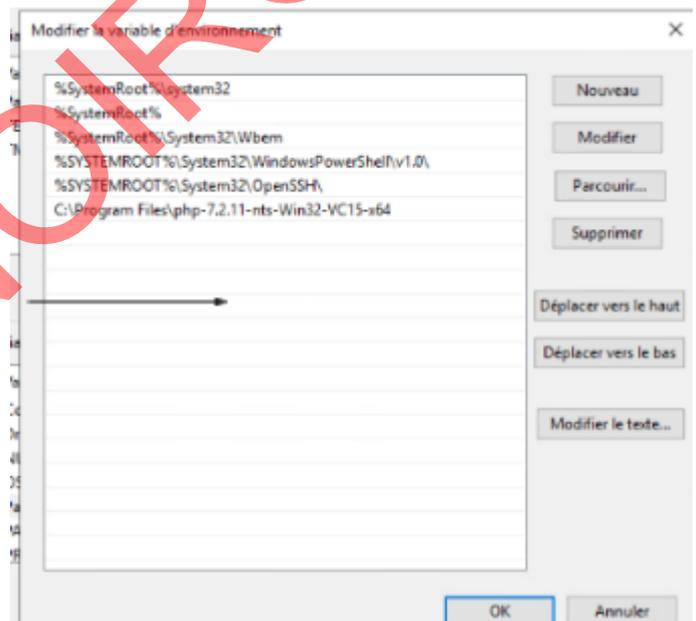
- Serveur Web (IIS) (9 sur 43 installé(s))
 - ▾ Serveur Web (8 sur 34 installé(s))
 - Fonctionnalités HTTP communes (4 sur 6 installé(s))
 - Intégrité et diagnostics (1 sur 6 installé(s))
 - Performance (1 sur 2 installé(s))
 - Sécurité (1 sur 9 installé(s))
 - ▾ Développement d'applications (1 sur 11 installé(s))
 - ASP
 - ASP.NET 3.5
 - ASP.NET 4.8
 - CGI (Installé)
 - Extensibilité .NET 3.5
 - Extensibilité .NET 4.8
 - Extensions ISAPI
 - Fichiers Include côté serveur
 - Filtres ISAPI
 - Initialisation d'applications
 - Protocole WebSocket
 - Outils de gestion (1 sur 7 installé(s))

Installation de PHP 7 :

- Copier la dernière version (Non-Thread Safe (NTS)) du dossier PHP 7 fourni (php-7.2.11-nts-Win32-VC15-x64) dans le dossier C:\Program Files (en Français Programmes) ;



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



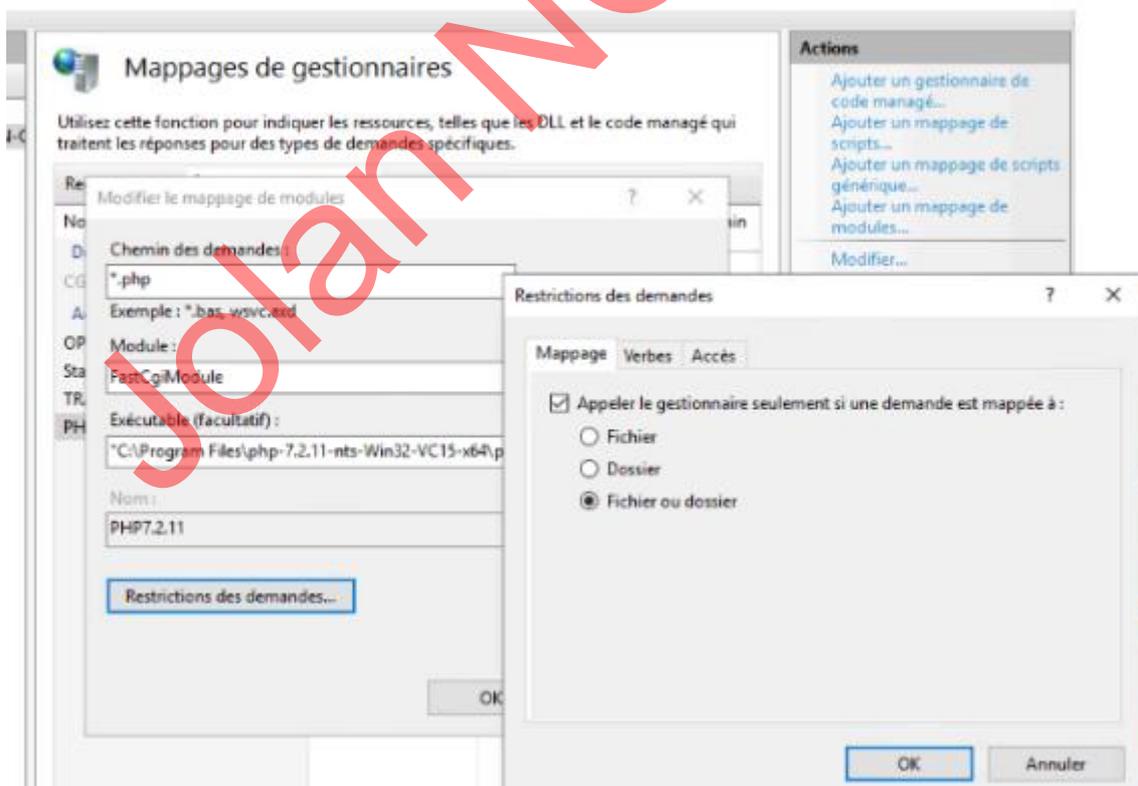
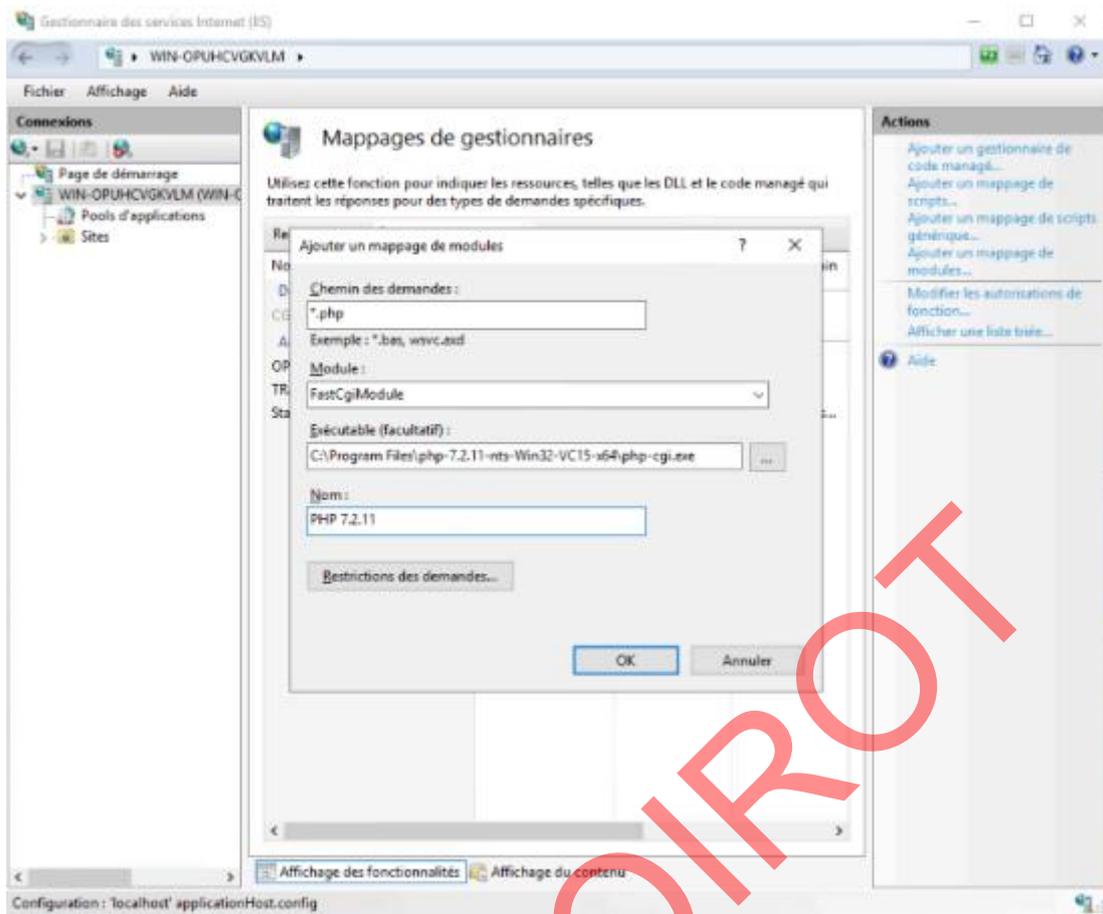
Dans le Gestionnaire IIS, configurer PHP comme suit : cliquer sur le nom du serveur, puis double-cliquer sur l'icône Mappages de gestionnaires ; dans le panneau Action, cliquer sur le lien Ajouter un mappage de module :

Chemin demandes : *.php

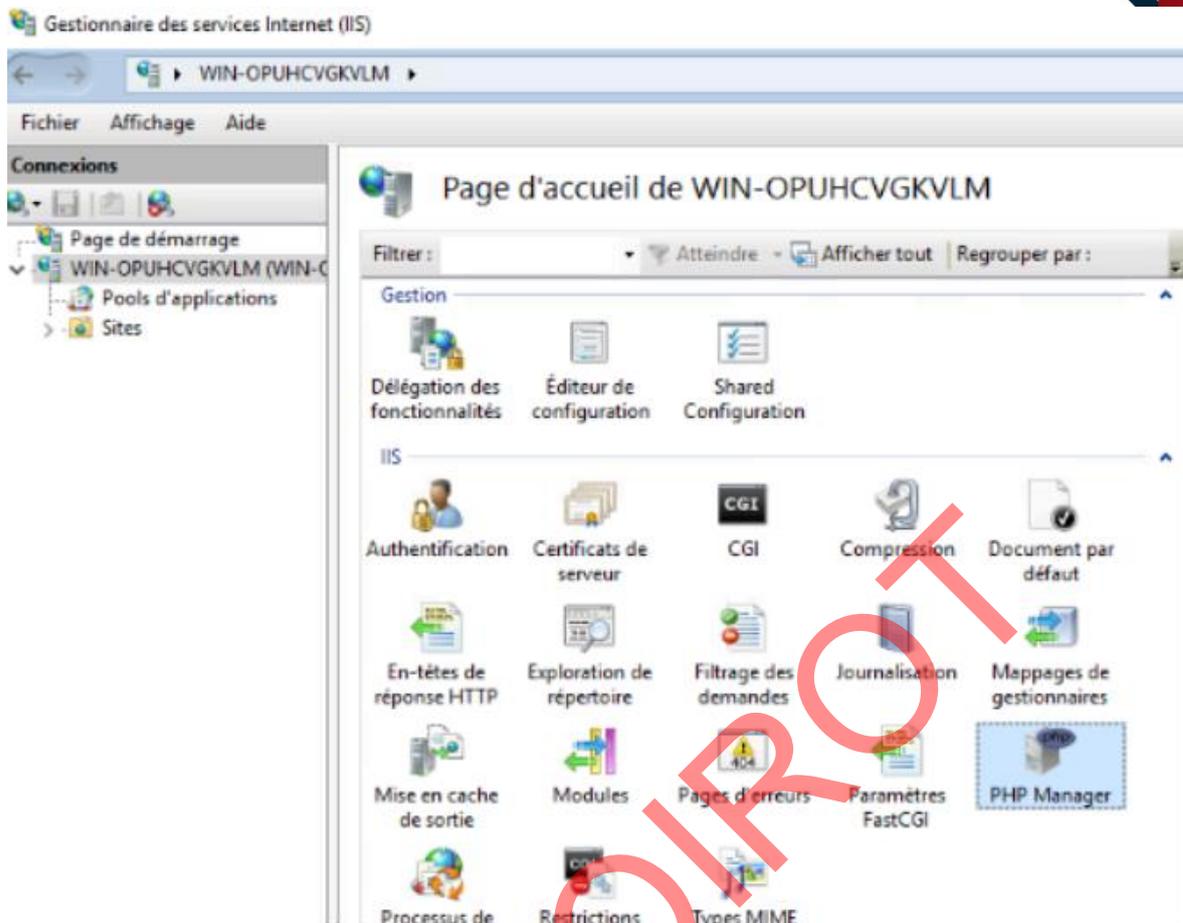
Module : FastCgiModule

Exécutable : taper le chemin d'accès complet à Php-cgi.exe : C:\Program Files\php-7.2.11-nts-Win32-VC15-x64\php-cgi.exe

Nom : entrer un nom pour le mappage : php-7.2.11

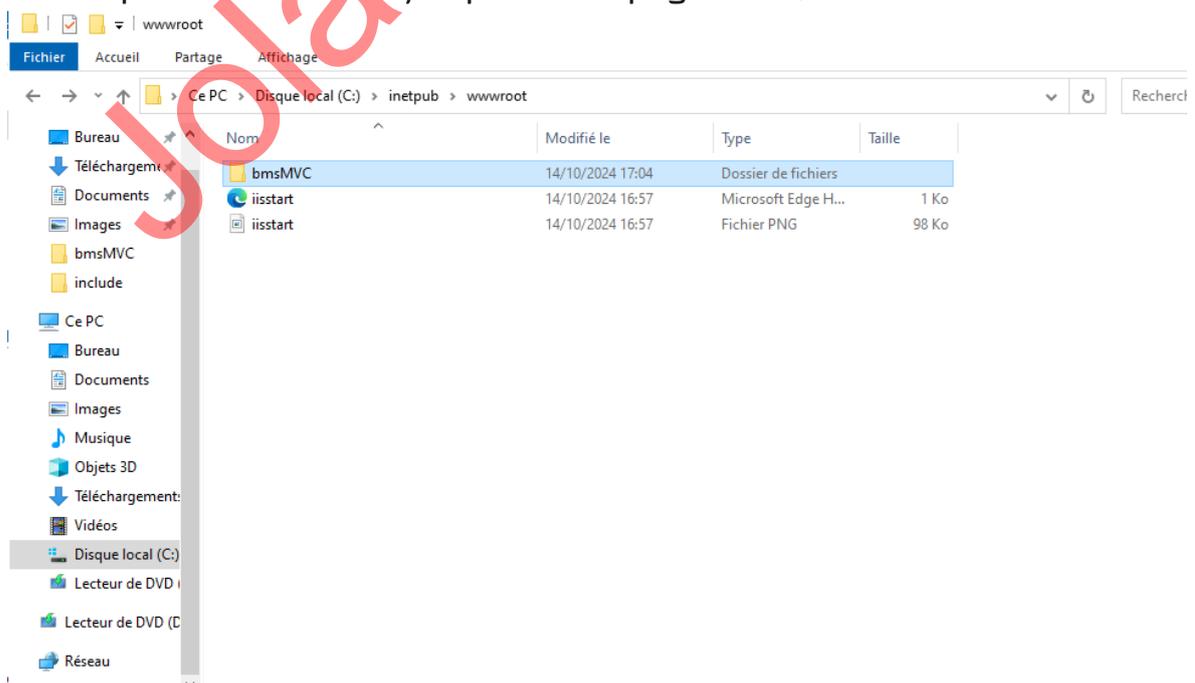


Cliquer ensuite sur le bouton Restrictions des demandes et cocher Fichier ou dossier. Ainsi, tous les fichiers d'extension .php seront



- Lancer PHP Manager, puis enregistrer PHP dans IIS (Enregistrer une nouvelle version de PHP), puis vérifier que PHP est bien fonctionnel (Vérifier phpinfo());

- a. Créer le site bmsMVC sous IIS (créer le dossier bmsMVC dans inetpub\wwwroot et y importer les pages web).



Modifier le script class.pdoBMS.inc dans le sous-dossier include pour spécifier :

- l'adresse IP du serveur Mysql utilisé
- l'identifiant et le mot de passe de l'utilisateur (créé dans le script cinema.sql)
- le nom de la base de données utilisée

```
class PDOBMS{
    private static $serveur='mysql:host=192.168.10.2';
    private static $bdd='dbname=bms_frais';
    private static $user='utilisateurweb' ;
    private static $mdp='secret' ;
    private static $monPdo;
    private static $monPdoBMS=null;

/**
 * Constructeur privé, crée l'instance de PDO qui sera sollicitée
 * pour toutes les méthodes de la classe
 */
    private function __construct(){
        PDOBMS::$monPdo = new PDO(PDOBMS::$serveur.'.PDOBMS::$bdd, PDOBMS::$user, PDOBMS::$mdp);
        PDOBMS::$monPdo->query("SET CHARACTER SET utf8");
    }
    public function _destruct(){
        PDOBMS::$monPdo = null;
    }
}
```

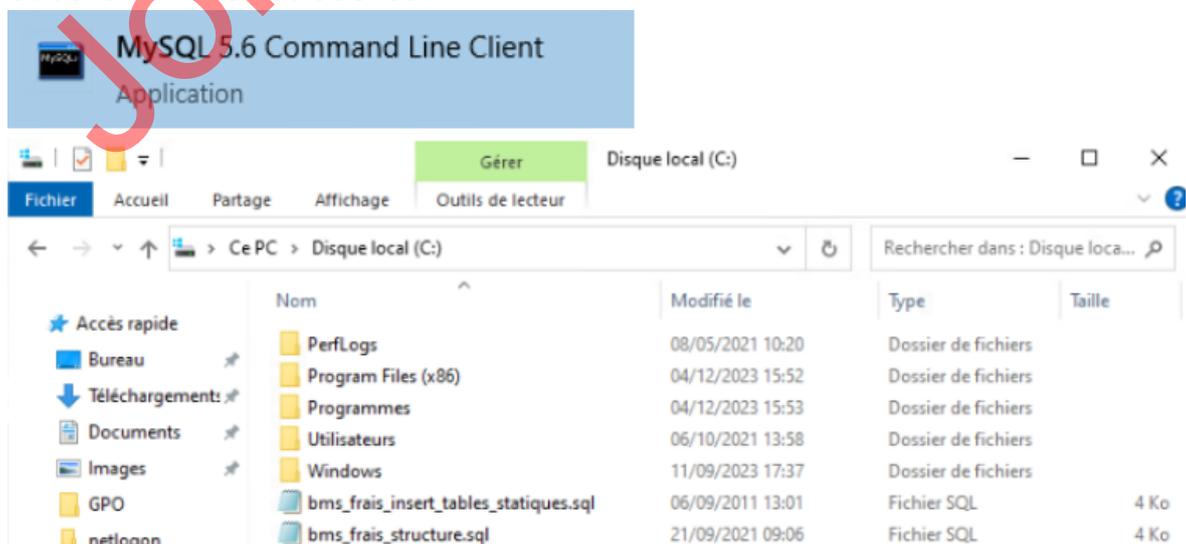
SUR ServeurBDBMS Etapes à suivre :

- a. Installer la version MySQL Community Server (installer le serveur uniquement, et non tout le package).



Login : admin/admin

- b. Créer la base cinema et exécuter le script de création des tables et des enregistrements (qui est à recopier sur C:\ pour être exécuté avec la commande source :



Les commandes à utiliser :

```
create database BMS_frais;
use BMS_frais;
show tables; source c:/BMS_frais_structure.sql show tables;
source c:/BMS_frais_insert_tables_statiques.sql
select * from visiteur;
```

- penser à configurer le SGBD Mysql en accordant tous les droits d'accès à la base de données BMS_frais à l'utilisateur nommé utilisateurWeb (qui est à créer) et ayant le mot de passe secret (c'est cet utilisateur qui est utilisé dans les scripts PHP du site Web bmsMVC qui permettent à un internaute de se connecter à la base de données):

```
create user "utilisateurweb" identified by "secret";
grant all privileges on BMS_frais.* to "utilisateurweb";
flush privileges; select user from mysql.user;
show grants for "utilisateurweb";
```

Name	State
Enabled	
php_curl.dll	Enabled
php_gd2.dll	Enabled
php_gettext.dll	Enabled
php_mbstring.dll	Enabled
php_mysqli.dll	Enabled
php_openssl.dll	Enabled
php_pdo_mysql.dll	Enabled
php_pdo_sqlite.dll	Enabled
php_soap.dll	Enabled
php_xmlrpc.dll	Enabled

MISSION 7 : CONFIGURATION DES RÈGLES DE FILTRAGE DU ROUTEUR- PARE-FEU PFSense

MISSION 7 A : RÈGLES MINIMUM À CONFIGURER SUR L'INTERFACE DMZ DU PFSense

Règles (Faire glisser pour changer l'ordre)											
<input type="checkbox"/>	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
<input type="checkbox"/>	✓	0/806 B	IPv4 TCP	172.16.10.1	*	192.168.10.2	3306	*	aucun		
<input type="checkbox"/>	✗	0/0 B	IPv4 *	172.16.10.1	*	LAN address	*	*	aucun		
<input type="checkbox"/>	✓	0/2,64 GiB	IPv4 *	*	*	*	*	*	aucun		

MISSION 7 B : RÈGLES MINIMUM À CONFIGURER SUR L'INTERFACE LAN DU PFSense

Pare-feu / Règles / LAN

Flottant(e) WAN LAN DMZ

Règles (Faire glisser pour changer l'ordre)											
<input type="checkbox"/>	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
<input checked="" type="checkbox"/>	✓	2/3,57 MiB	*	*	LAN Address	80	*	*		Règle anti-blocage	
<input type="checkbox"/>	✓	0/43 KiB	IPv4 TCP	*	172.16.10.1	80 (HTTP)	*	aucun			
<input type="checkbox"/>	👉	0/3 KiB	IPv4 *	*	172.16.0.0/16	*	*	aucun			
<input type="checkbox"/>	✓	21/4,23 GiB	IPv4 *	LAN subnets	*	*	*	aucun		Default allow LAN to any rule	
<input type="checkbox"/>	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	aucun		Default allow LAN IPv6 to any rule	

MISSION 7 C : RÈGLES MINIMUM À CONFIGURER SUR L'INTERFACE WAN DU PFSense

Pare-feu / Règles / WAN

Flottant(e) WAN LAN DMZ

Règles (Faire glisser pour changer l'ordre)											
<input type="checkbox"/>	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnement	Description	Actions
<input type="checkbox"/>	✓	0/27 KiB	IPv4 TCP	*	172.16.10.1	80 (HTTP)	*	aucun			
<input type="checkbox"/>	👉	0/10,64 MiB	IPv4 *	*	*	*	*	aucun			
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	172.16.10.1	80 (HTTP)	*	aucun		NAT	

MISSION 7 D : REDIRECTION POUR ACCÉDER DEPUIS INTERNET AU

SERVEURWEBDMZ

Pare-feu / NAT / Transfert de port ?

Les modifications ont été appliquées avec succès. Les règles du pare-feu sont en cours de rechargement en arrière-plan.
Surveiller le rechargement des filtres. ⌂

Transfert de port 1:1 Sortant NPt

Règles

<input type="checkbox"/>	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> WAN	TCP	*	*	WAN address	80 (HTTP)	172.16.10.1	80 (HTTP)		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Jolan NOIROT