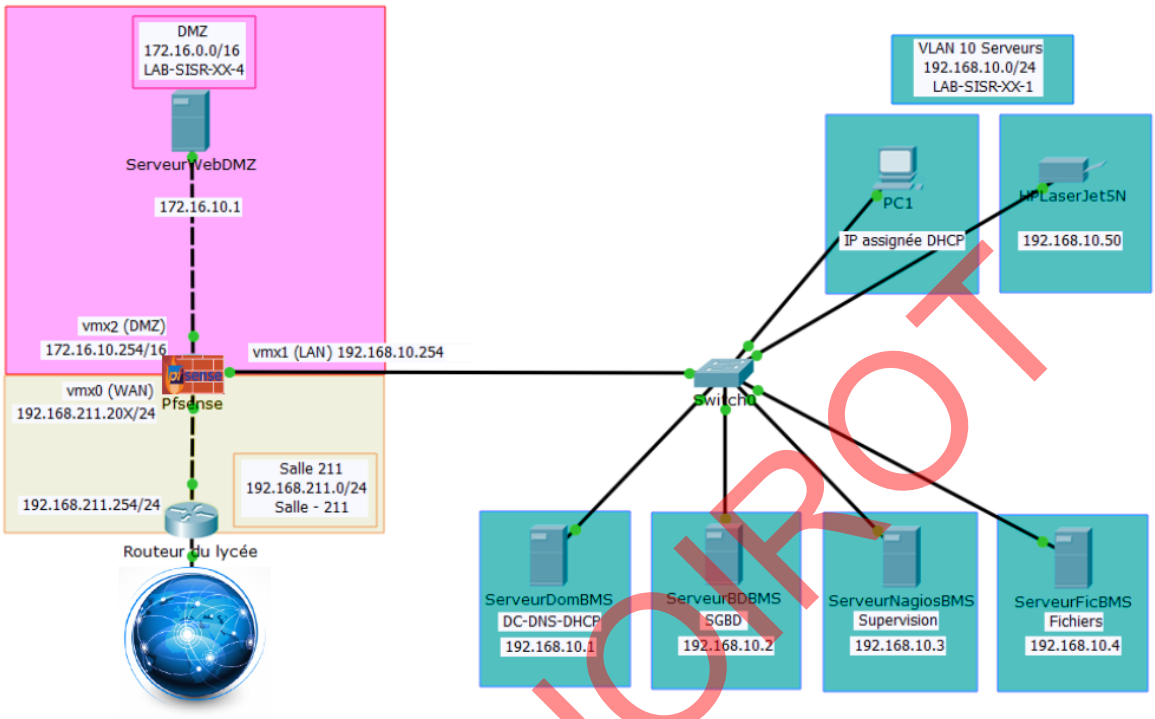
DOCUMENTATION PROJET BMS

Jolan Noirot BTS SIO 2

SOMMAIRE

INTRODUCTION

RÉSEAU À RÉALISER



SYSTÈMES D'EXPLOITATION

Machine Virtuelle	Système d'exploitation	IP	
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

Système d'exploitation	Identifiant	Mot de passe
Windows	Administrateur	Windows2022
Debian	root	root

RÉSEAUX :

SALLE – 211	LAB - SISR – 08 - 1	LAB - SISR – 08 - 4
• pfSense	• pfSense • ServeurDomBMS • ServeurBDBMS • ServeurFicBMS • ServeurNagiosBMS • PC1	• pfSense • ServeurWebDMZ

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 configurer 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 configurer 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).

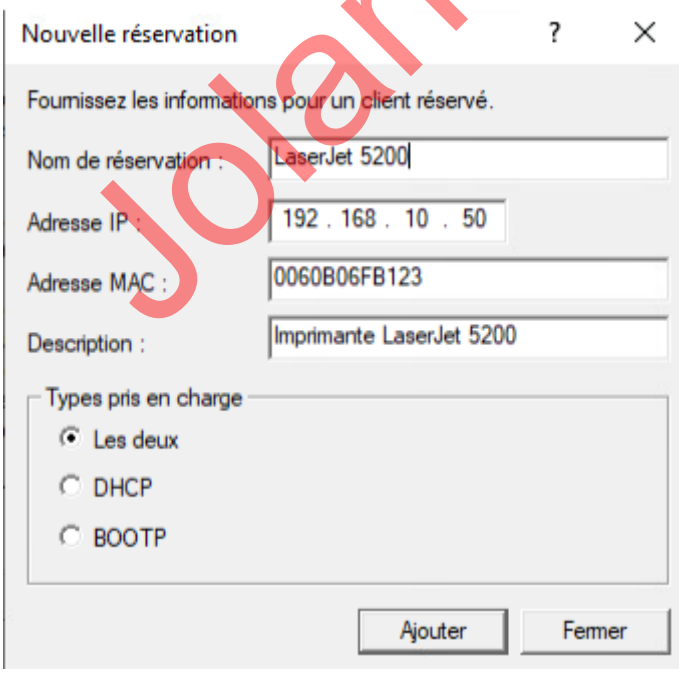
Cliquer sur le bouton Avancé de la fenêtre Propriétés de REPBASES. Puis cliquer sur le bouton : Désactiver l'héritage de la fenêtre Paramètres de sécurité avancés pour REPBASES
Dans le message de sécurité qui s'affiche lors du blocage de l'héritage, cliquer sur le lien : Convertir les autorisations héritées 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

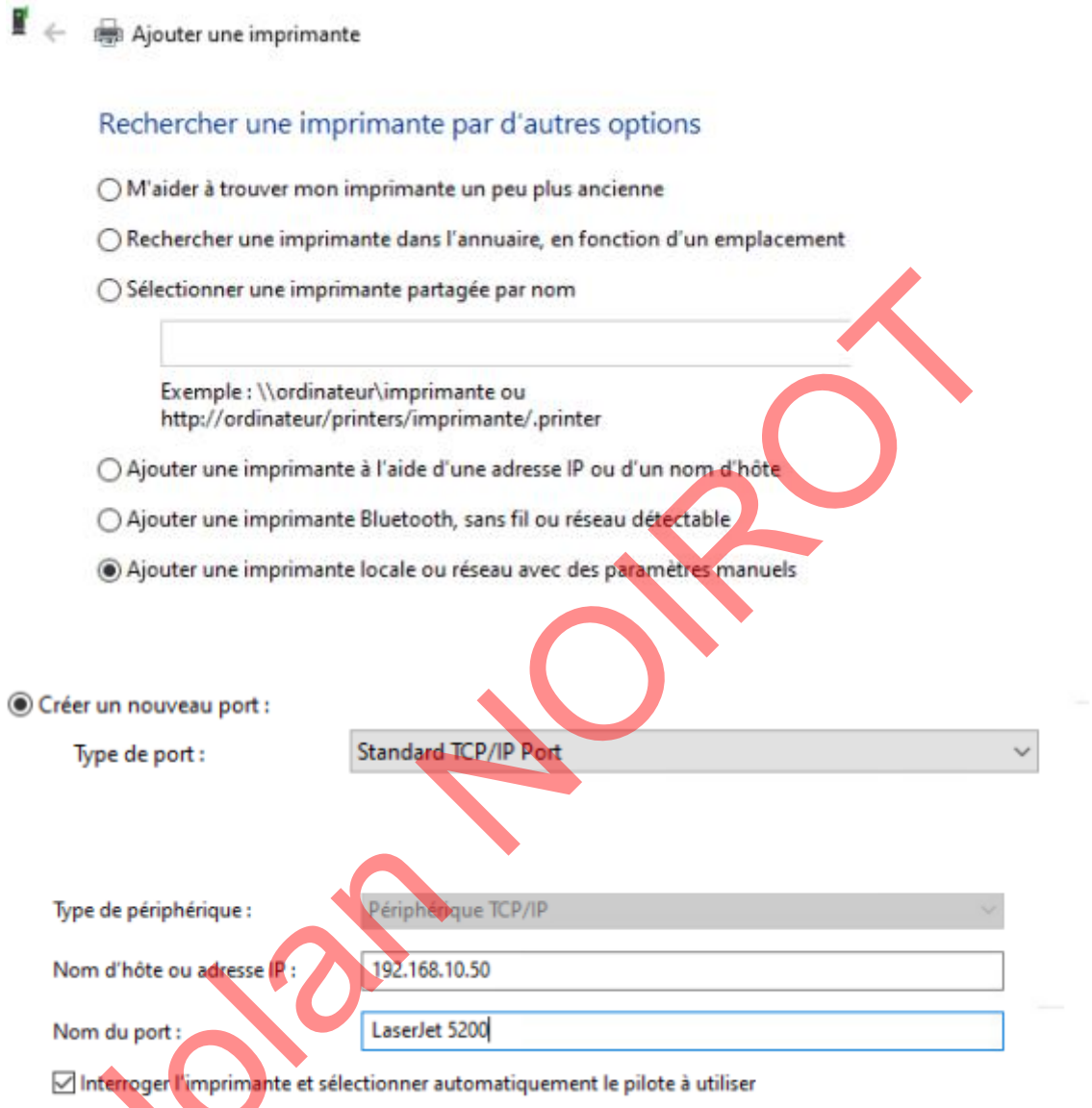
Configurer un nom une addresse IP et l'ajouter au domaine comme vue dans les précédents TPs.

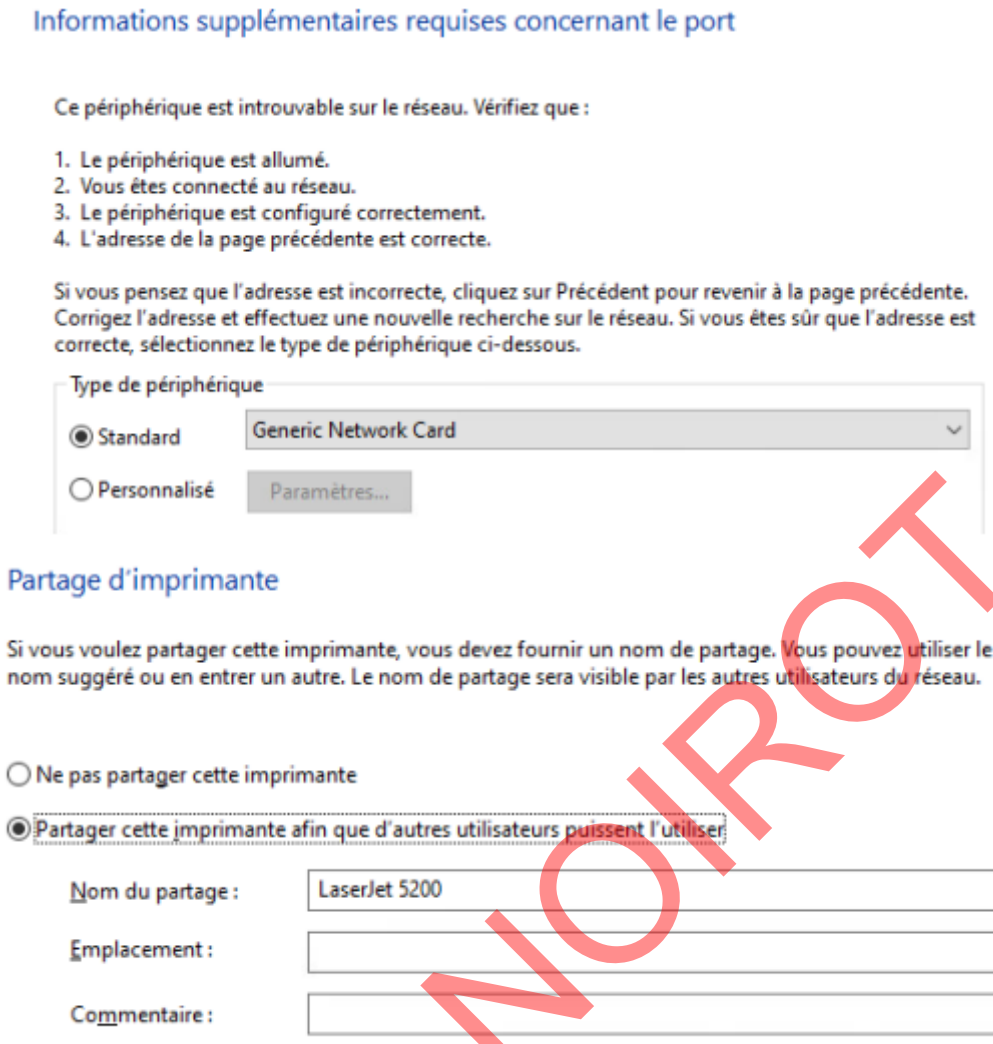
MISSION 1 D : INSTALLATION/DÉPLOIEMENT DE L'IMPRIMANTE SUR LES POSTES

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

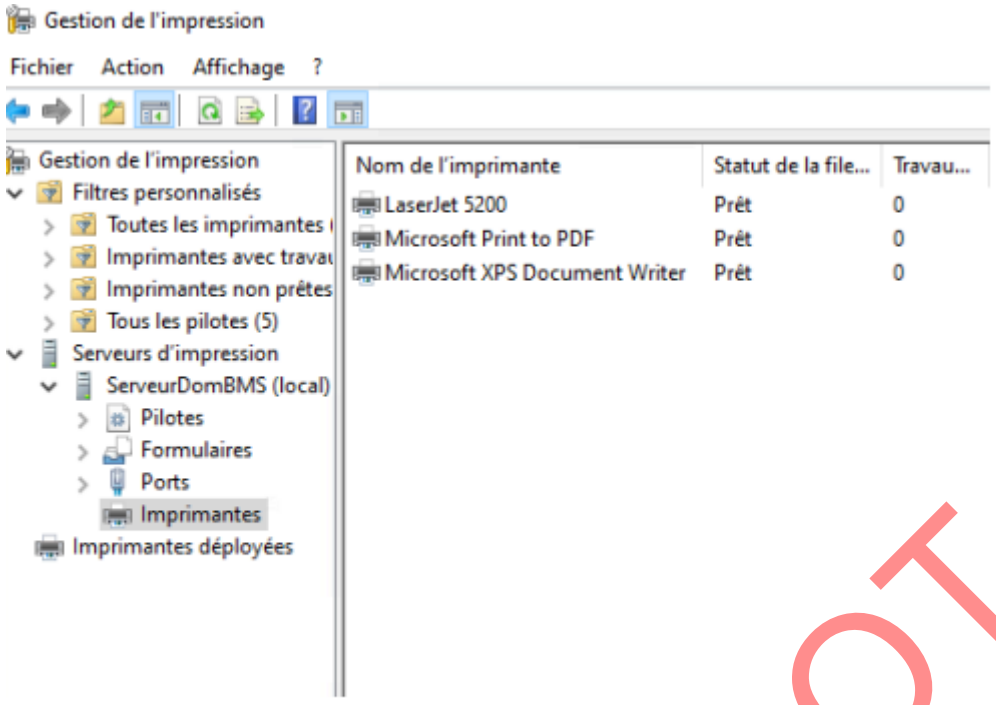


Sélectionner Panneau de configuration / Matériel, Périphériques et imprimantes le serveur recherche alors l'imprimante ; comme il s'agit ici d'une imprimante "fictive", cliquer sur le lien L'imprimante souhaitée n'est pas indiquée.

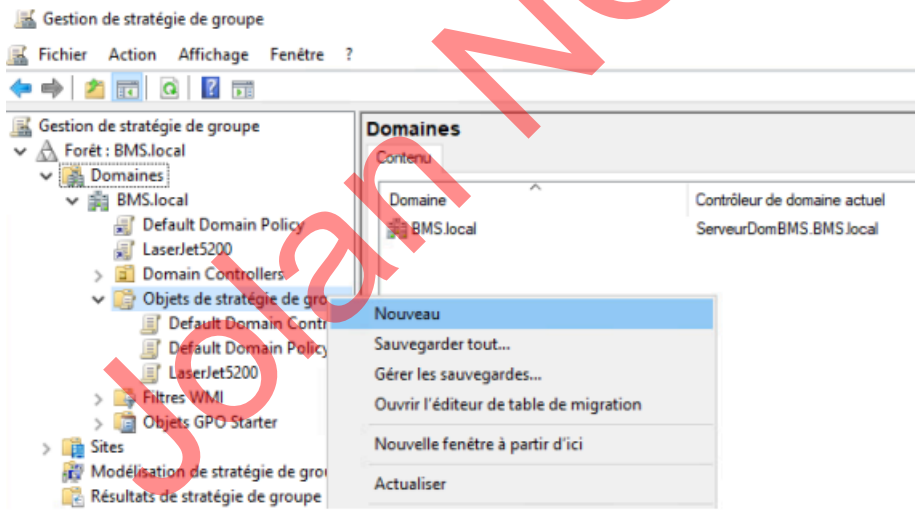




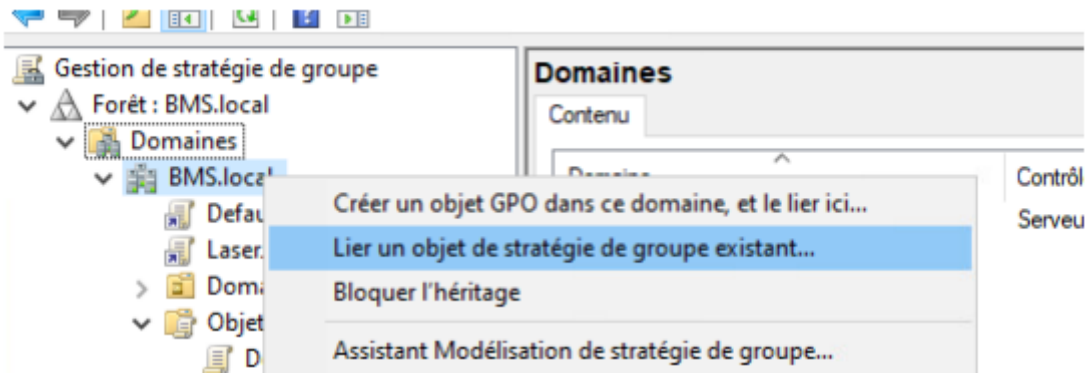
Ensuite dans outils du gestionnaire de serveurs, aller dans gestion de l'impression :

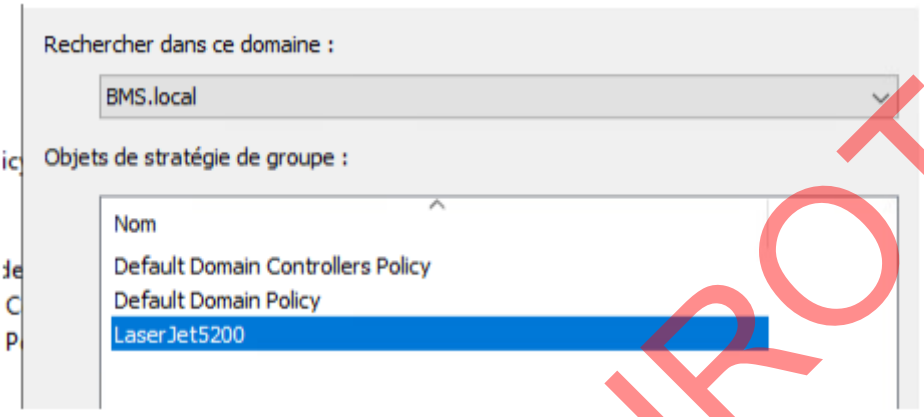


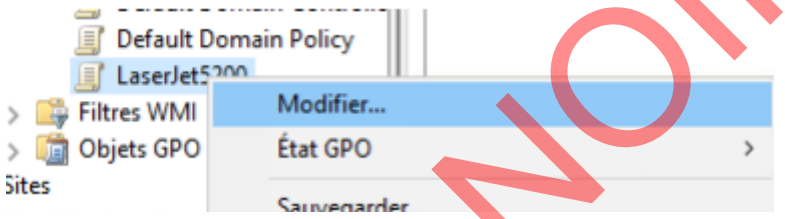
Une fois que l'imprimante est bien visible ici, retourner dans le gestionnaire de serveur/outils/Gestion des stratégies de groupe.

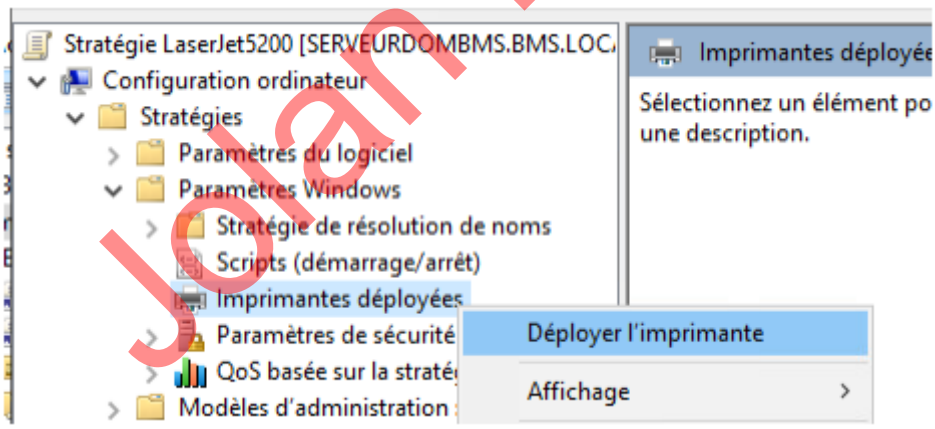


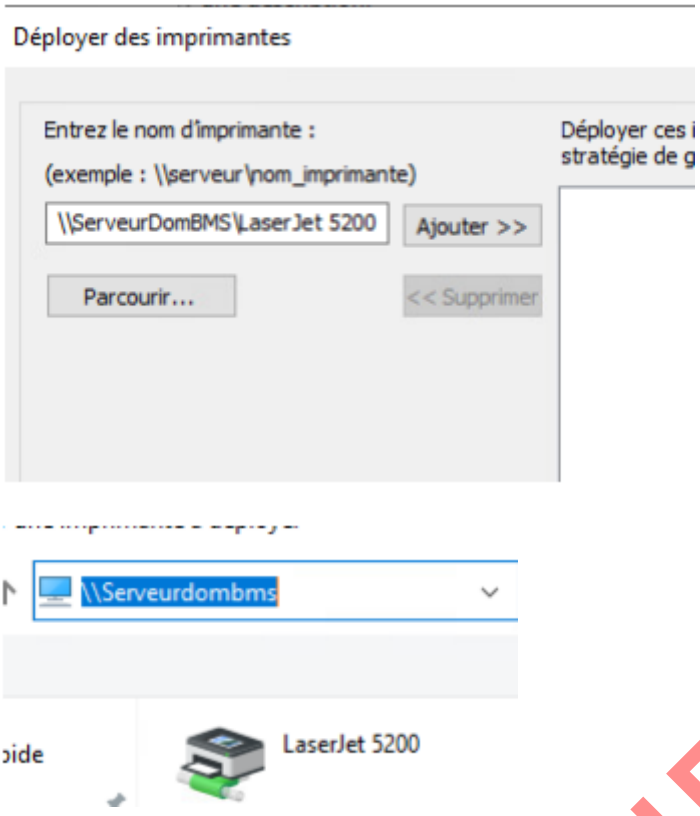
Nom : LaserJet5200
Objet starter GPO source : Aucun





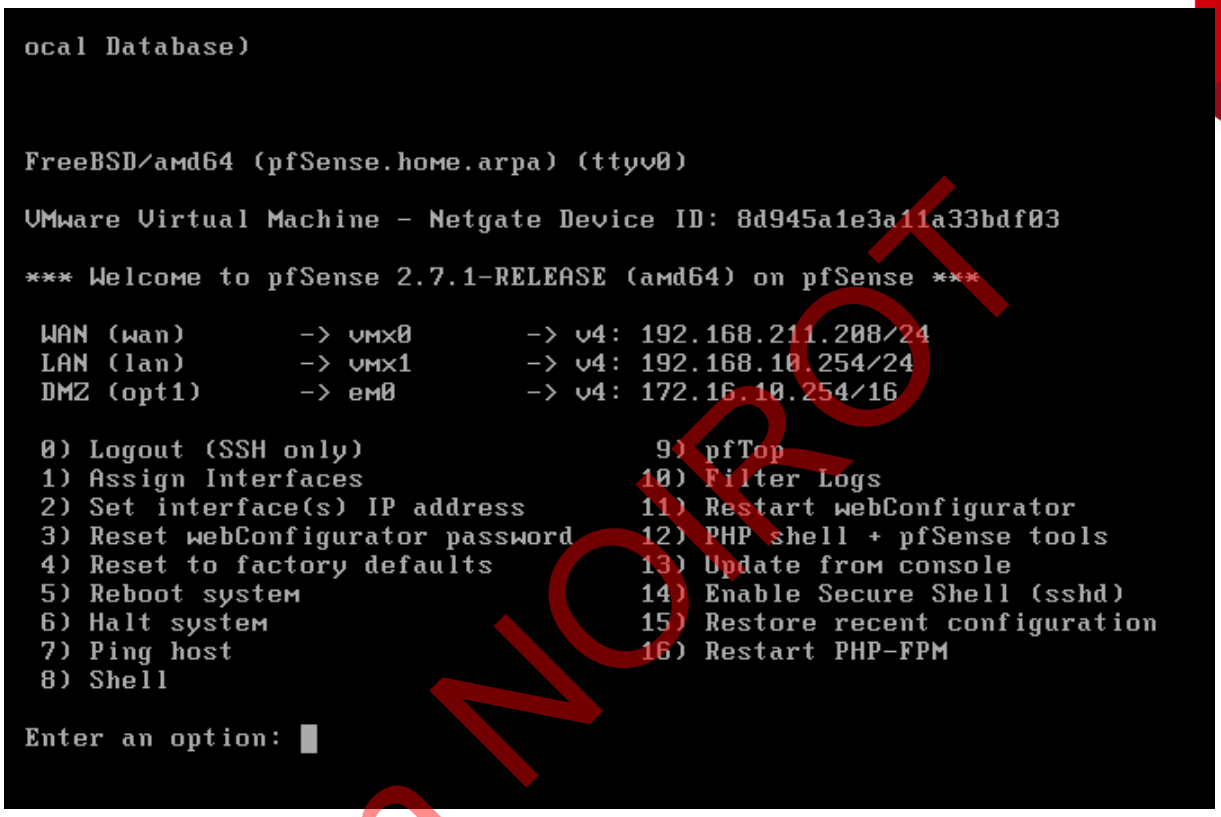




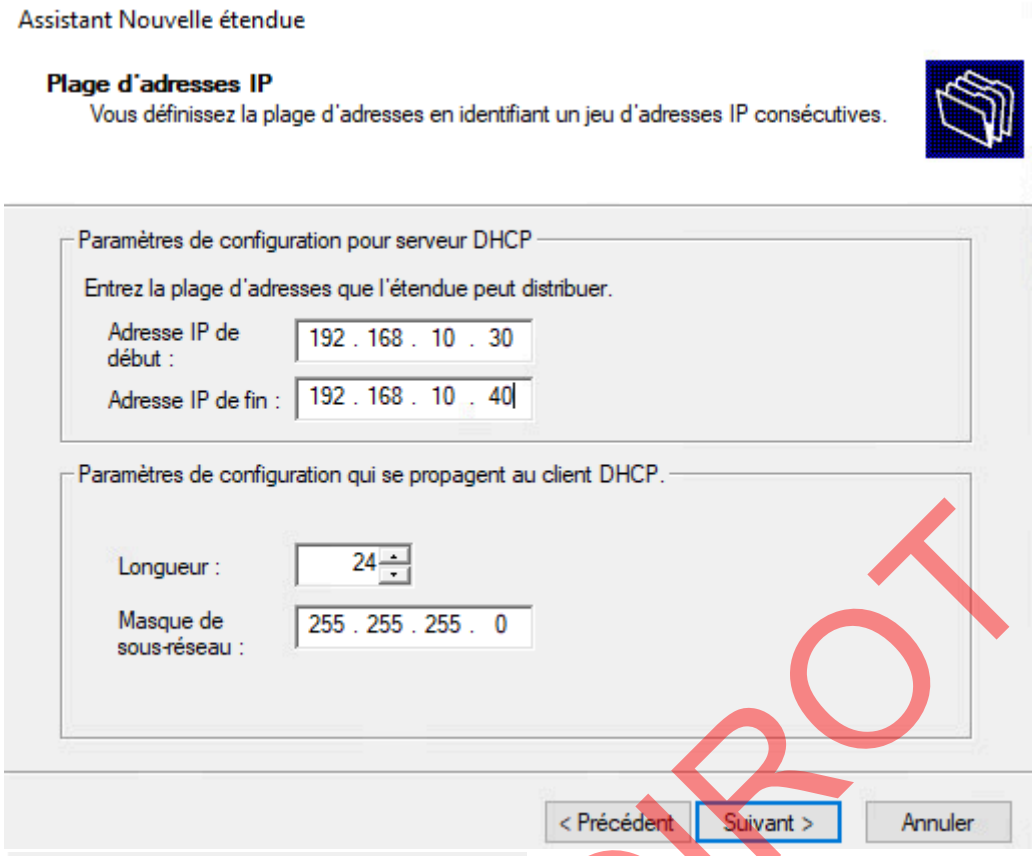


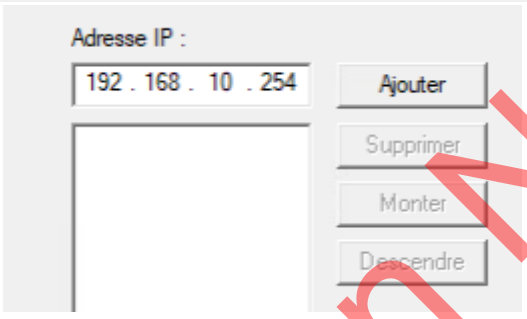
MISSION 2 : INSTALLATION ET CONFIGURATION GÉNÉRALE DU ROUTEUR-PARE-FEU PFSENSE

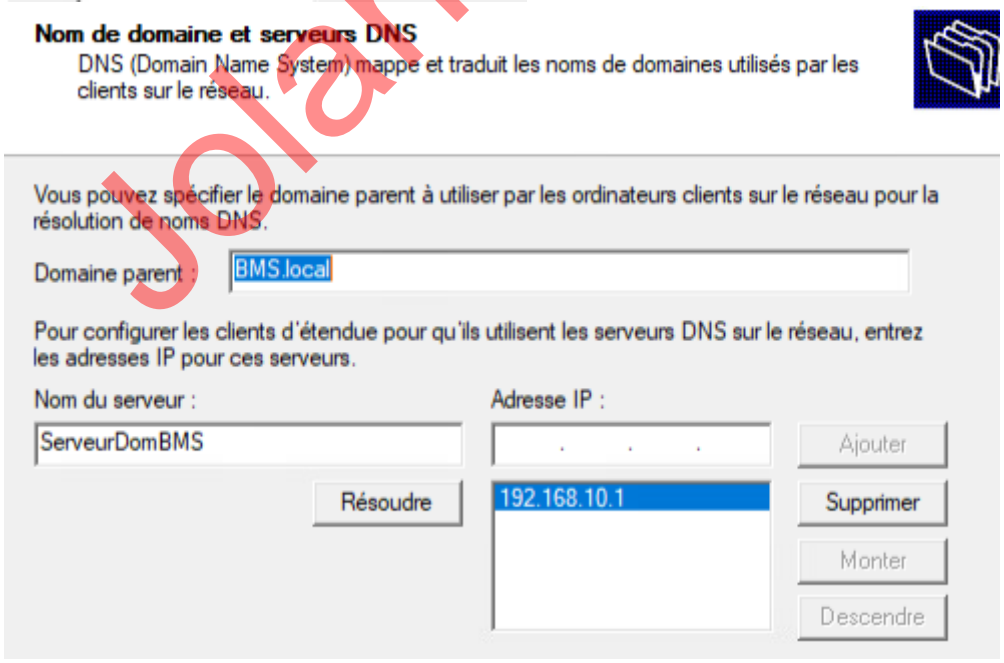
MISSION 2 A : INSTALLATION DU PFSENSE



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







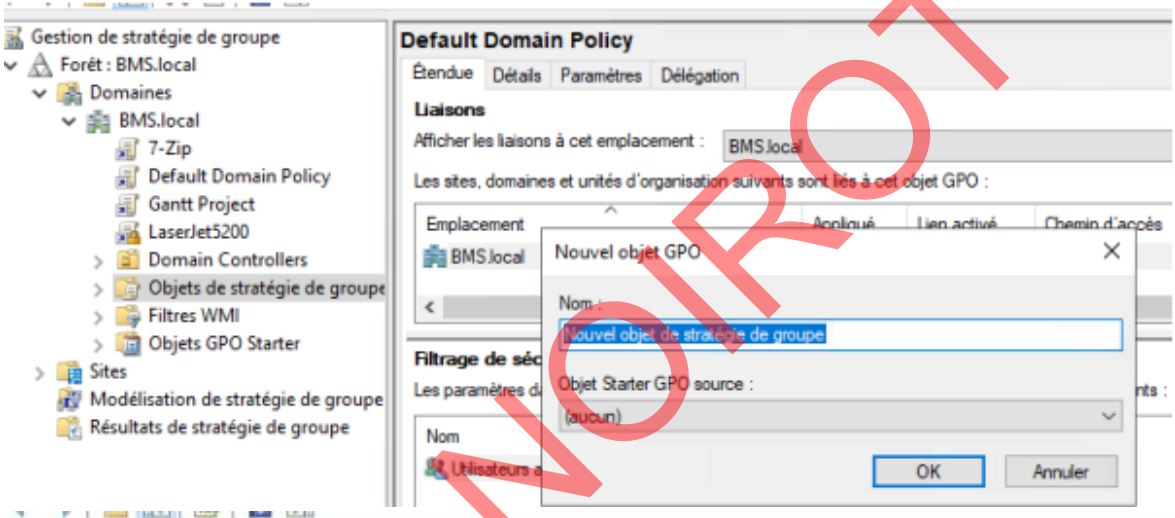
Ne pas ajouter de serveurs WINS

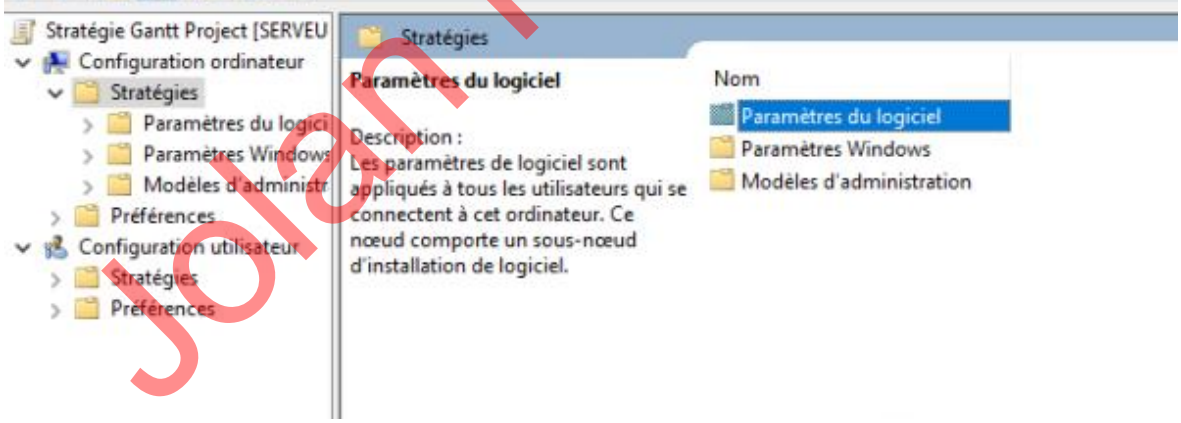
Activer le DHCP
Puis lancer le PC1 et vérifier avec ipconfig

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

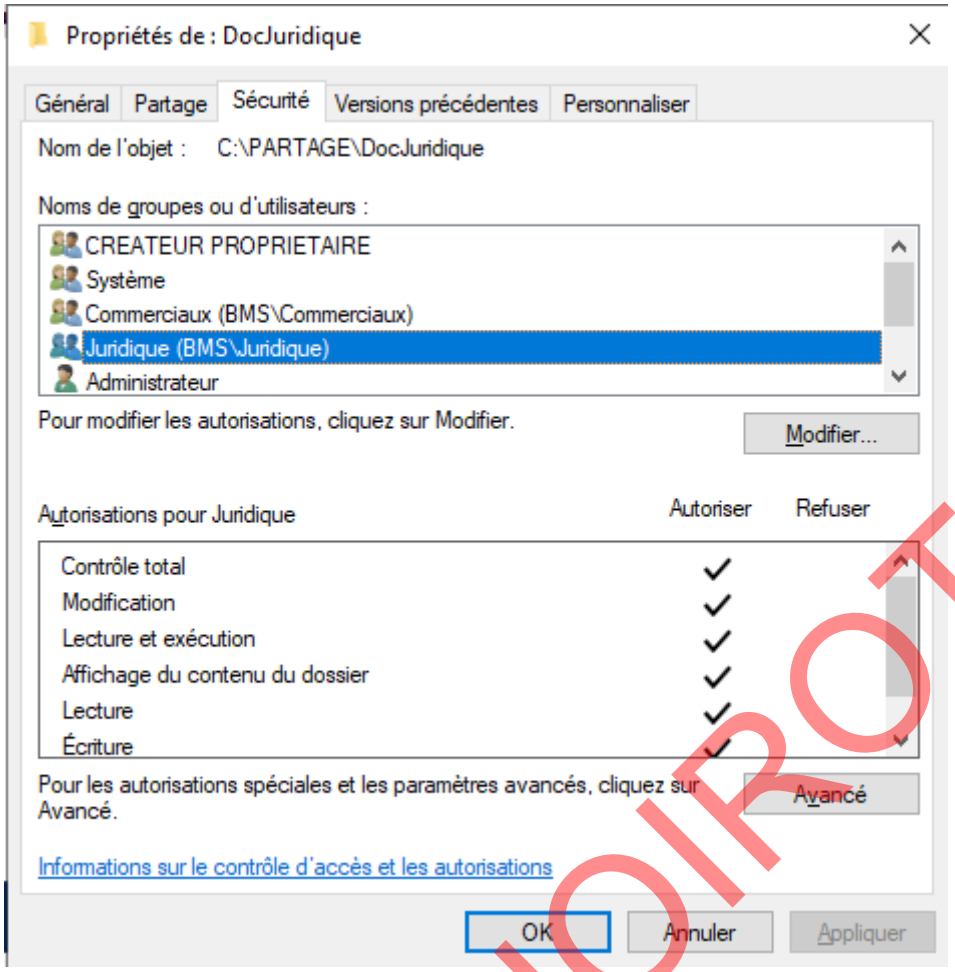
Créer les utilisateurs suivants dans l'AD :

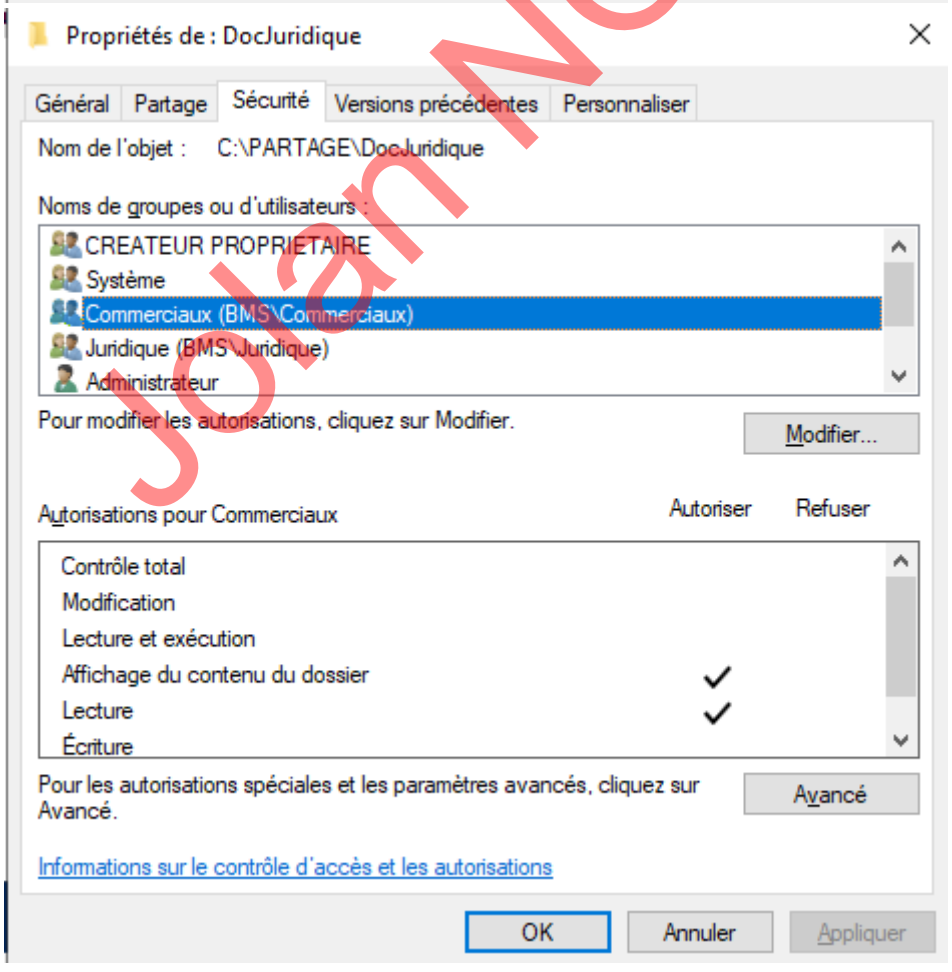
Nom et prénom	*Nom d'ouverture de session*	*Nom du dossier personnel*	*Mot de passe*
Charles Dupont	**cdupont**	cdupont	*Windows2019*
Albert Dubois	**adubois**	adubois	*Windows2019*
Clémence Rousseau	**crousseau**	crousseau	*Windows2019*
Vincent Ogier	**vogier**	vogier	*Windows2019*
Louis Ravignac	**lravignac**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

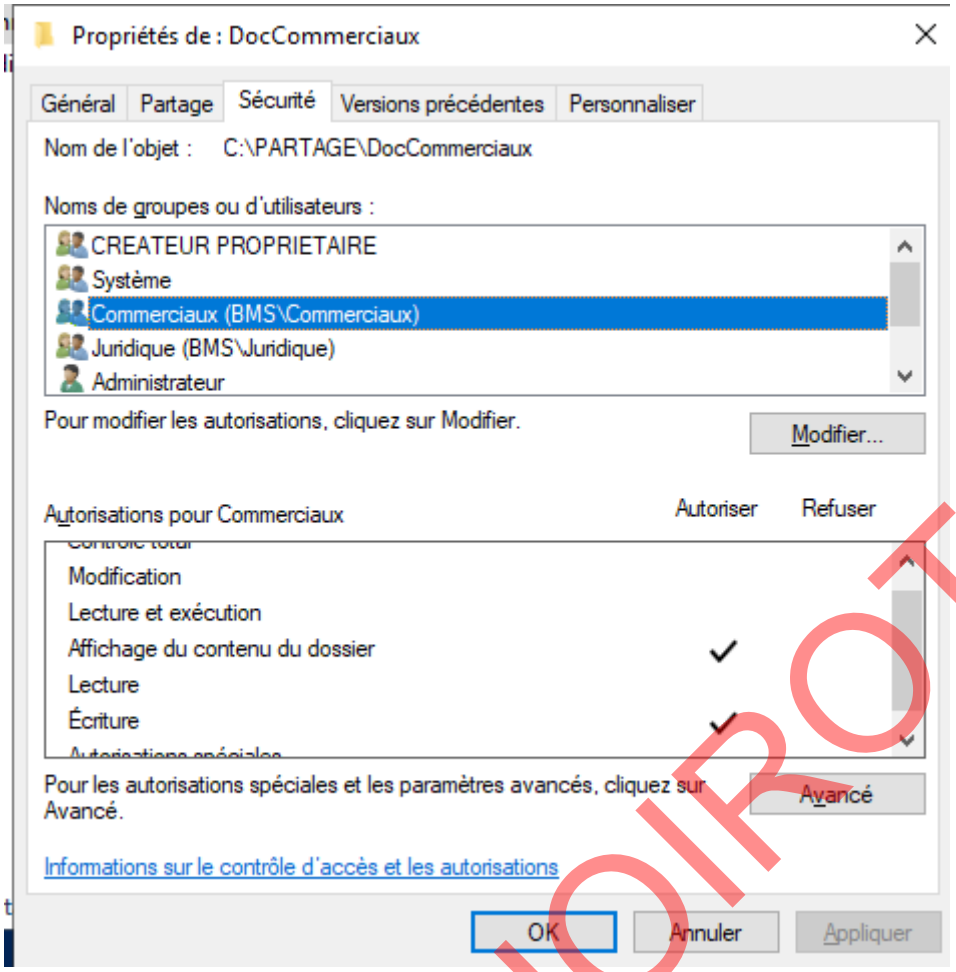
Créer les groupes suivants dans l'AD :

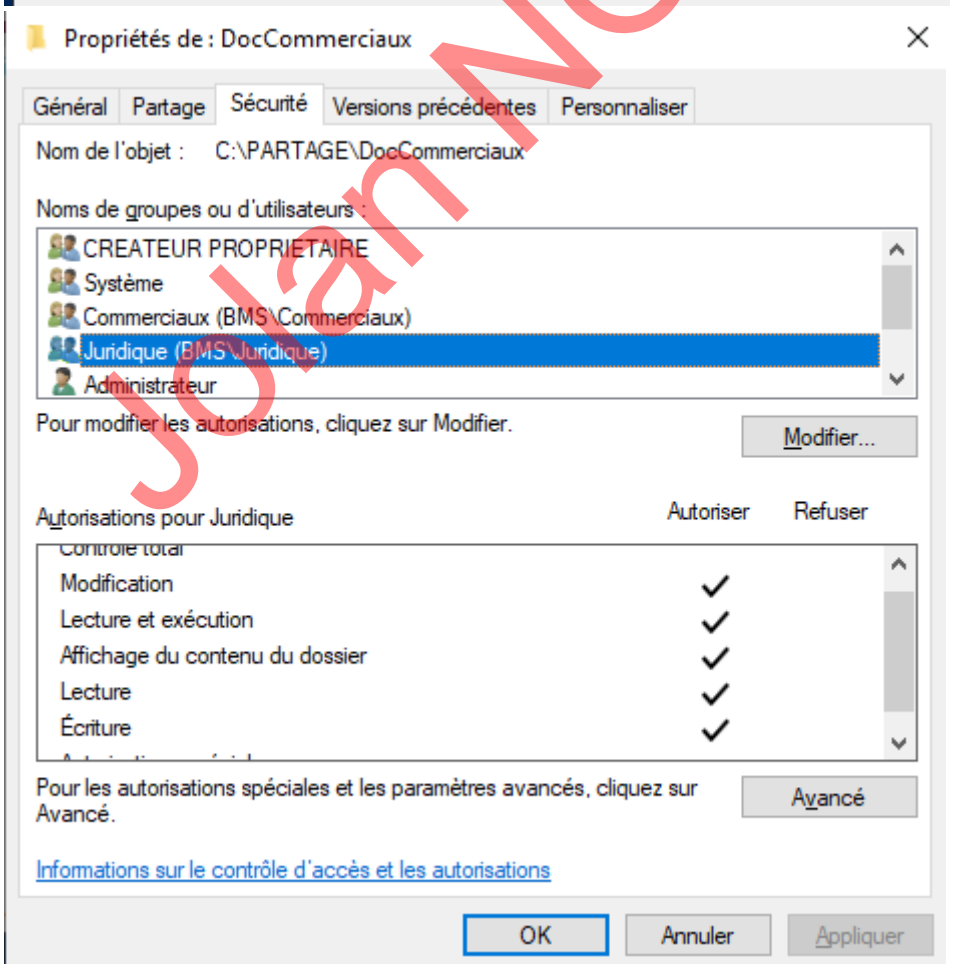
Nom de groupe	Etendue	Type	Membres du groupe
Commerciaux	Domaine local	Sécurité	Charles Dupont Clémence Rousseau
Juridique	Domaine local	Sécurité	Albert Dubois Vincent Ogier

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



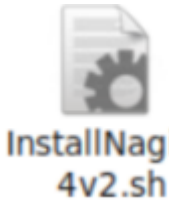




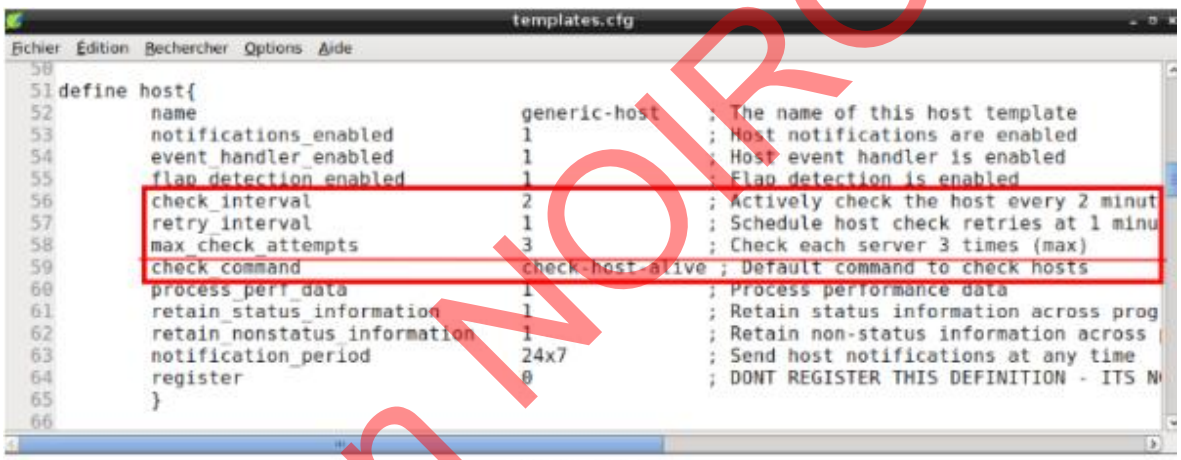


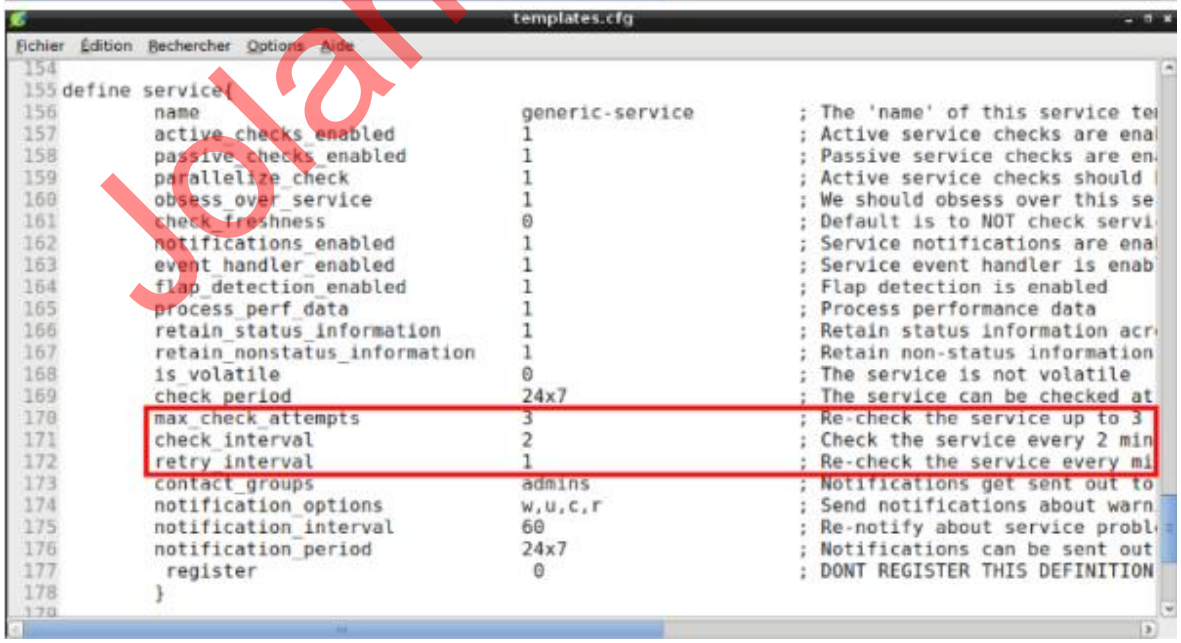
MISSION 4 : SUPERVISION NAGIOS

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 :

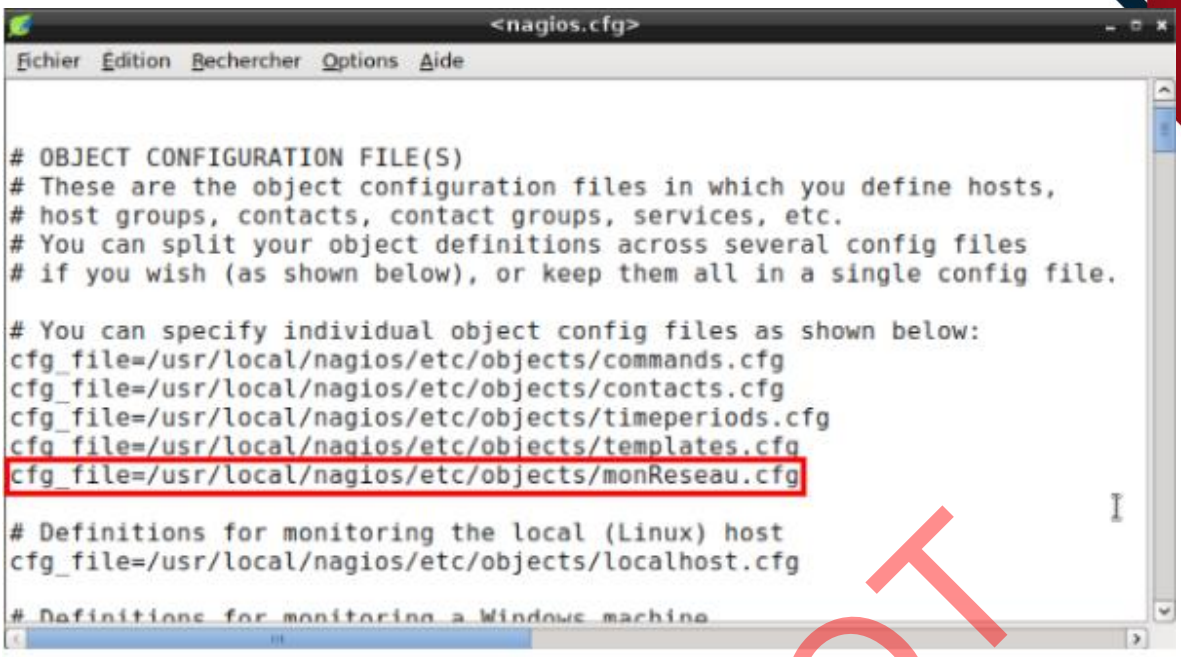


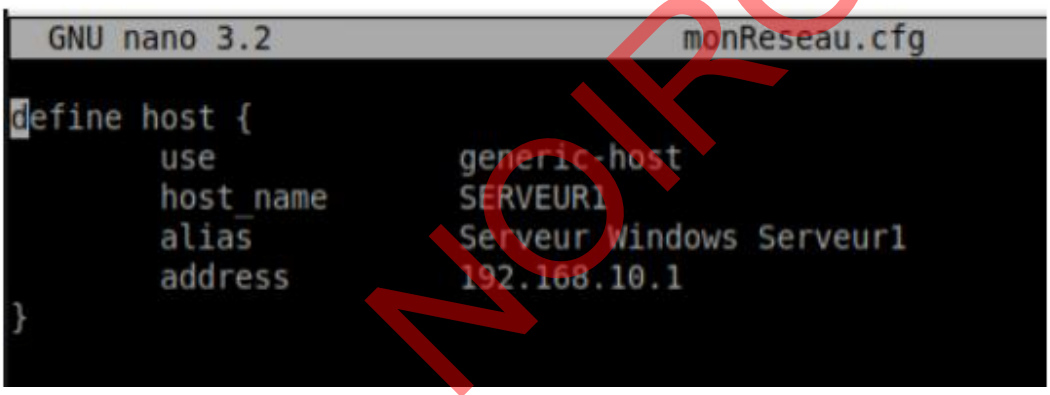
cd /root
./InstallNagios4v2.sh
reboot à la fin
/usr/local/nagios/etc/objects/templates.cfg





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





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
        vrml_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
```

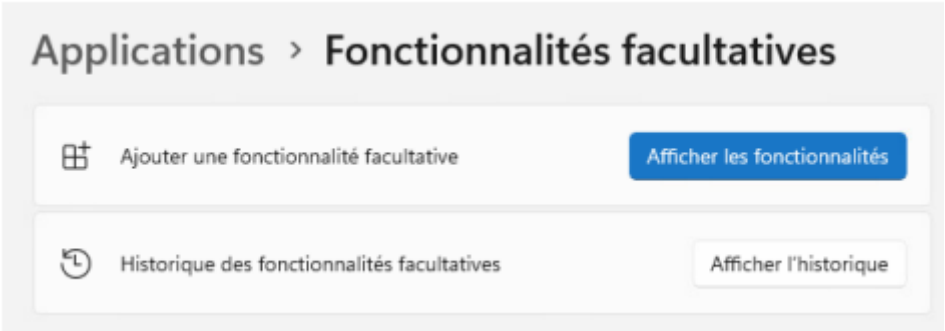
```
        command_line    $USER1$/check_dns  -H  SERVEUR1  -s
$HOSTADDRESS$
}

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
```

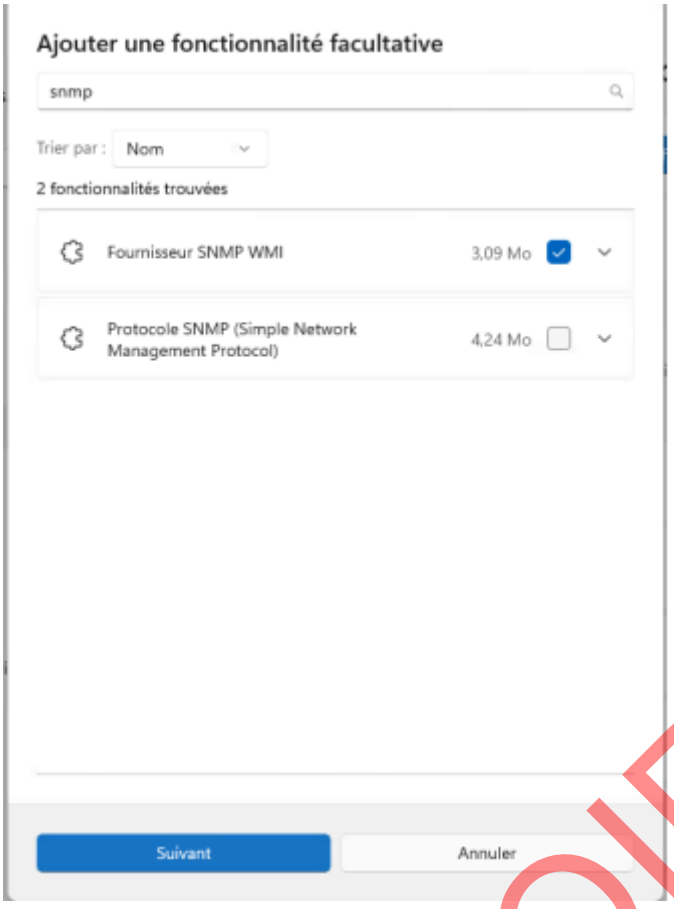
```
    service_description    FTP
    check_command          check_ftp1
}

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 :

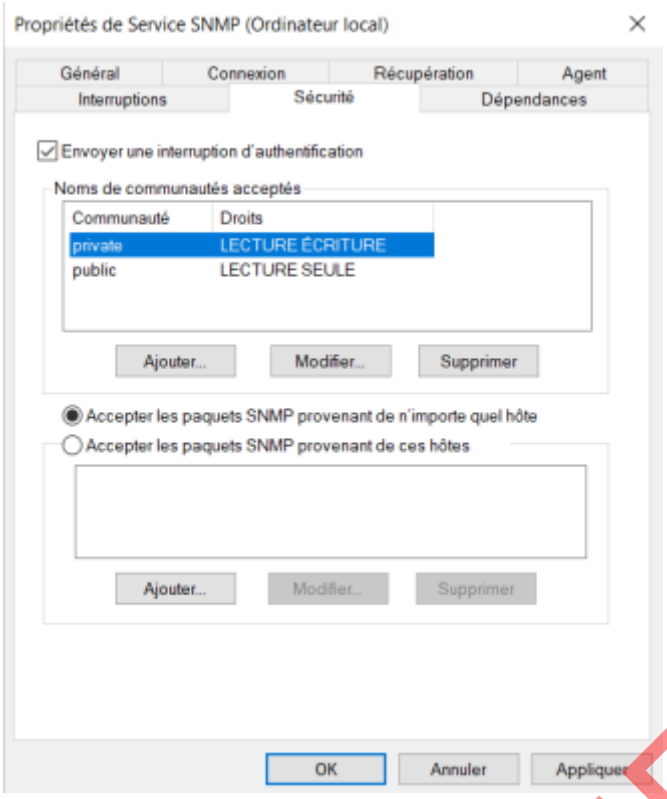
Se connecter en Administrateur, puis sélectionner Paramètres / Applications / Applications et fonctionnalités / Fonctionnalités facultatives ; vérifier que la fonctionnalité Protocole SNMP (Simple Network Management Protocol) est bien installée (sinon, l'installer) ; cliquer sur Ajouter une fonctionnalité,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



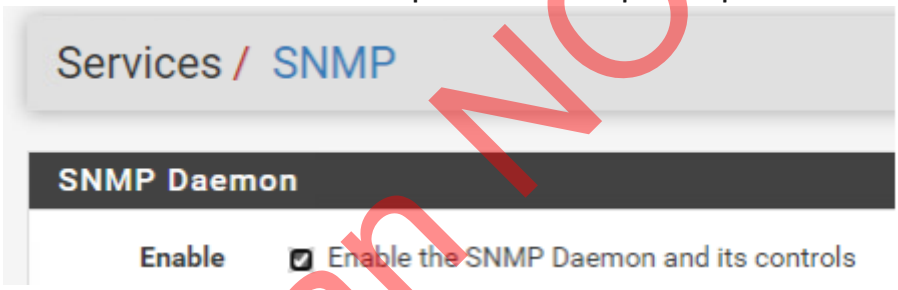
Dans l'onglet Sécurité, cocher la case Accepter les paquets SNMP provenant de n'importe quel hôte Dans l'onglet Sécurité, ajouter les deux noms de communauté suivants avec leurs droits respectifs :
private (lecture - écriture)
public (lecture seule)

Pour installer et configurer l'agent SNMP sur Microsoft Windows Server 2019/2022 :
a. 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).
b. 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 ;
c. Vérifier que le service est bien démarré (normalement le démarrage est automatique).
d. Dans l'onglet Agent, cocher tous les services
e. Dans l'onglet Sécurité, cocher la case Accepter les paquets SNMP provenant de n'importe quel hôte
f. 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 réfÂ©seau $driveLetter a éfÂ©téfÂ© mappéfÂ© vers
$folderPath"
    } else {
        Write-Host "Le lecteur $driveLetter est défÂ©jàfÂ  mappéfÂ©."
    }
}

# 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
```

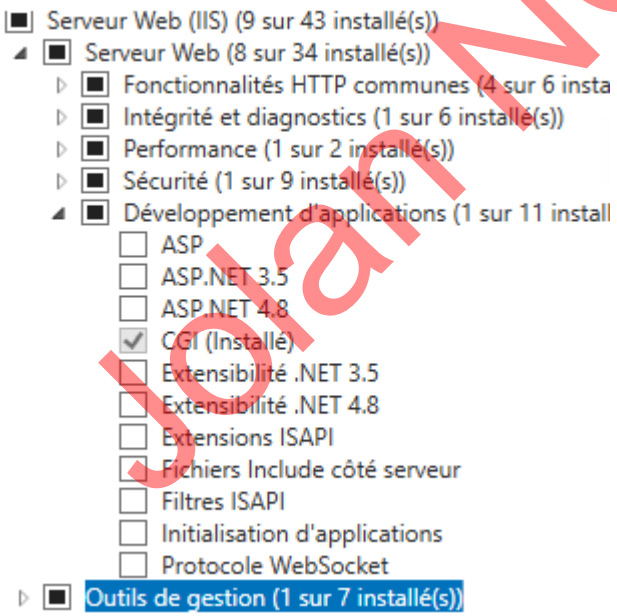
Cette stratégie autorise l'exécution des scripts locaux non signés, mais exige une signature numérique pour les scripts téléchargés ou venant de sources non locales.

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

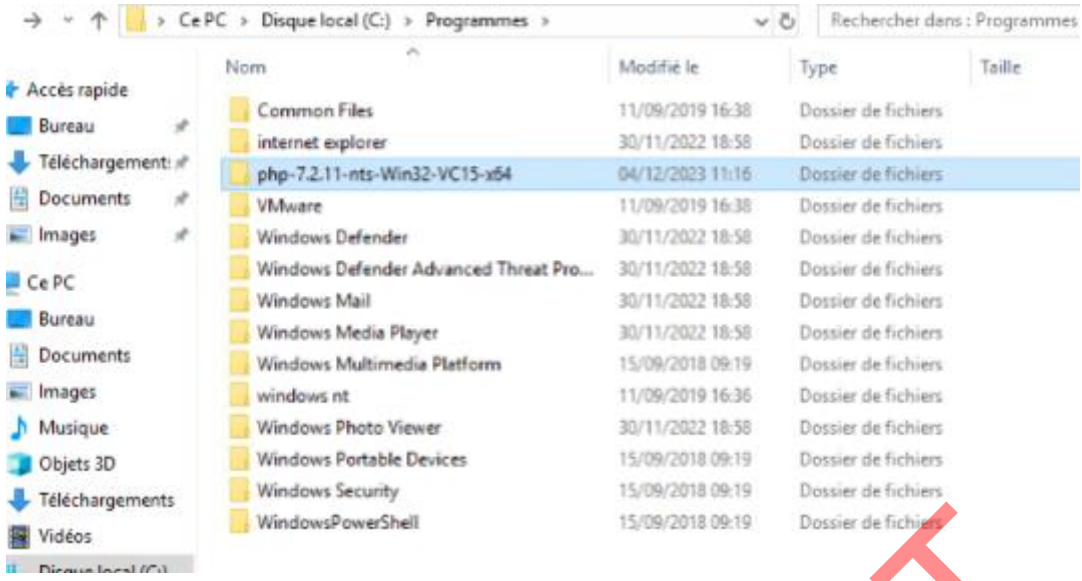
MISSION 6 : INSTALLATION DU SERVEUR DE BASES DE DONNÉES SERVEURBDBMS, DU SERVEUR WEB SERVEURWEBDMZ, ET DE L'APPLICATION DE GESTION DES FRAIS

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).

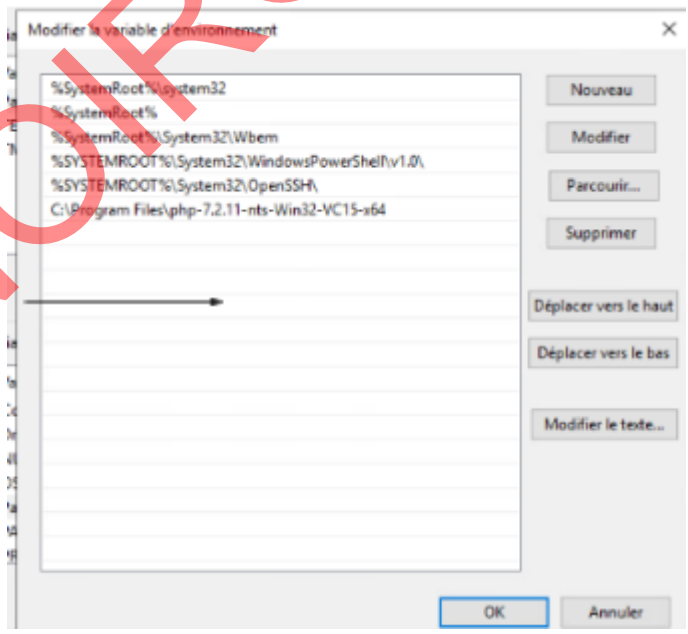


Installation de PHP 7 :
• Copier la dernière version (Non-Thread Safe (NTS)) du dossier PHP 7 fourni (php-7.2.11-nts-Win32-VC15-x64) dans le dossier C:\Program Files (en Français Programmes) ;



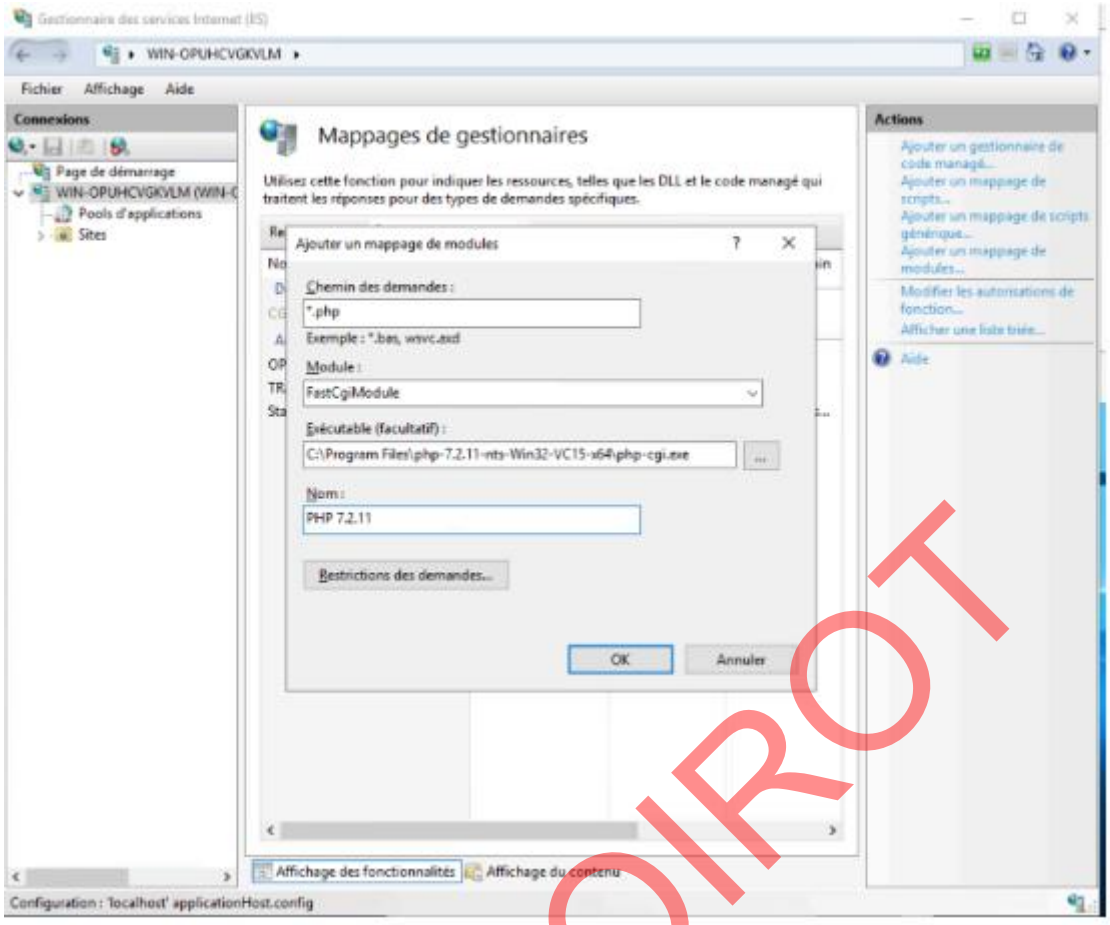
• Renommer le fichier php.ini-development en php.ini ;

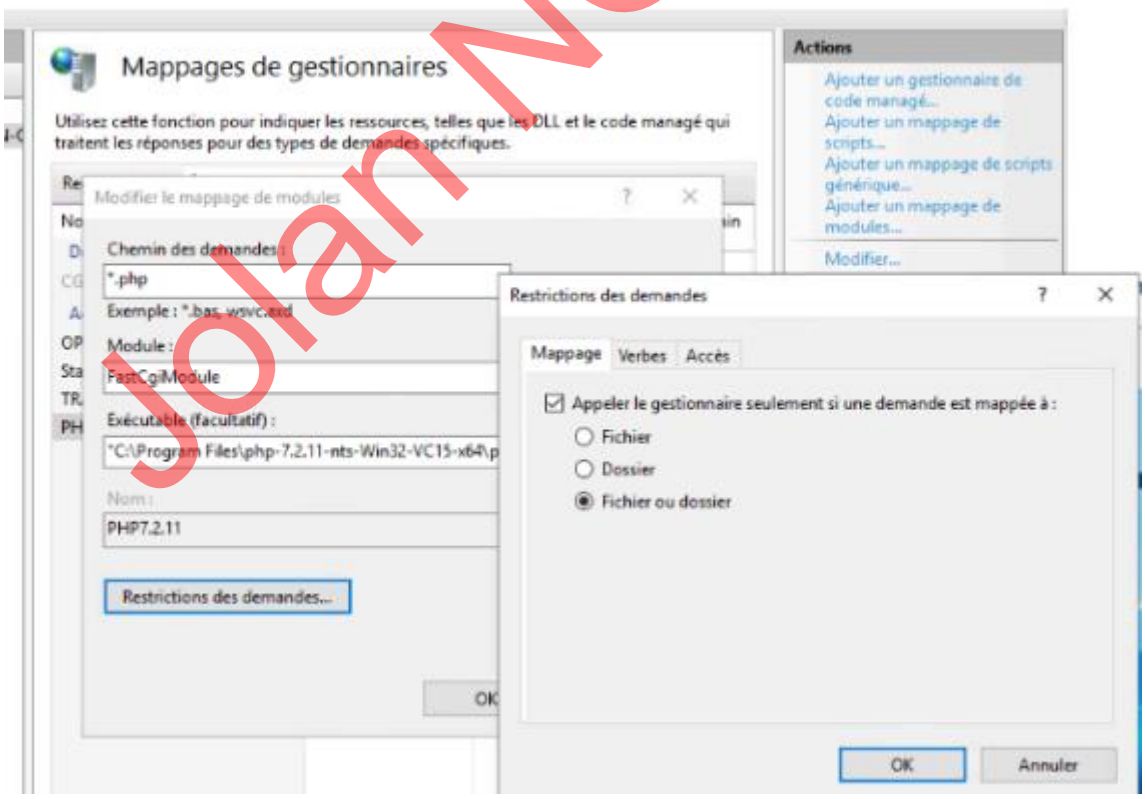
• Ajouter le chemin du dossier C:\Program Files\php-7.2.11-nts-Win32-VC15-x64 à la variable d'environnement Path (Panneau de configuration / Système et sécurité, Système , lien Paramètres système avancés ; dans la fenêtre qui s'ouvre, sélectionner l'onglet Avancé, puis le bouton Variables d'environnement ; 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

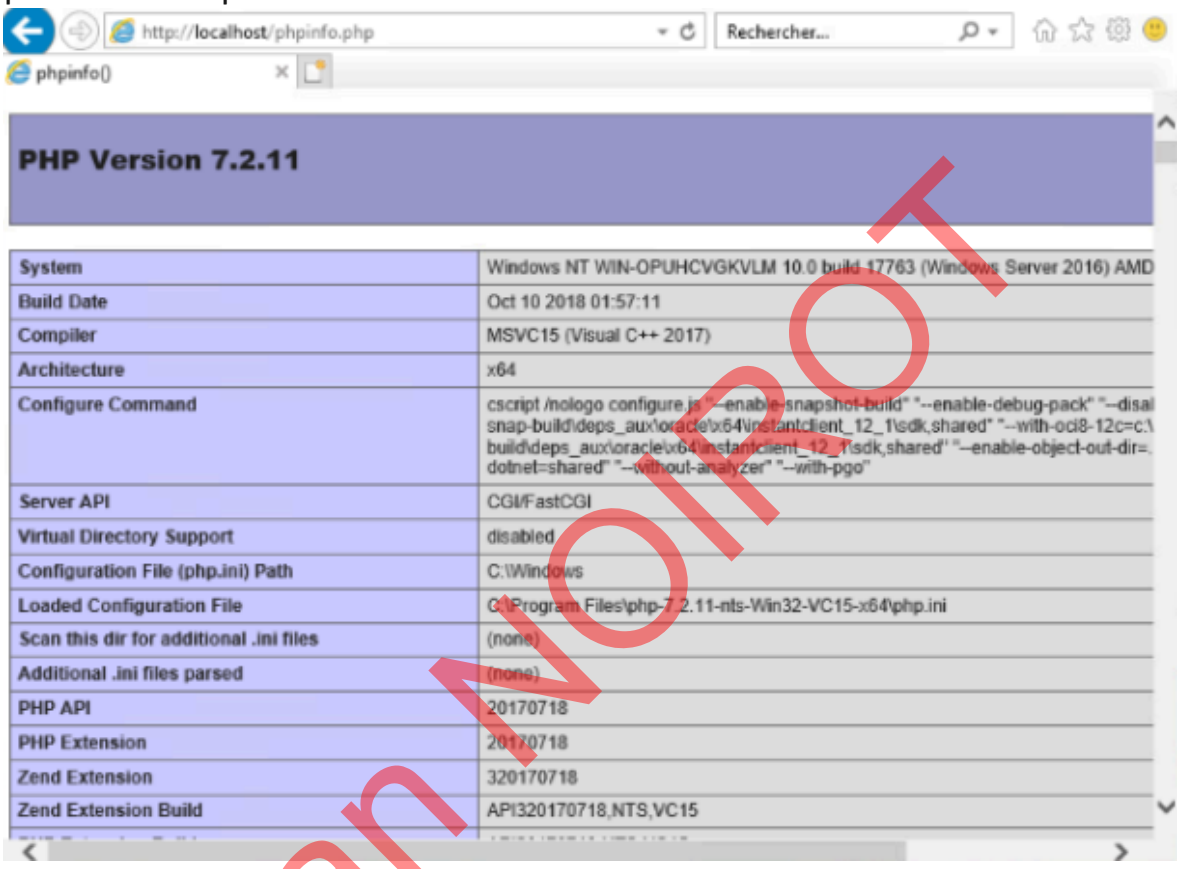




Cliquer ensuite sur le bouton Restrictions des demandes et cocher Fichier ou dossier. Ainsi, tous les fichiers d'extension .php seront

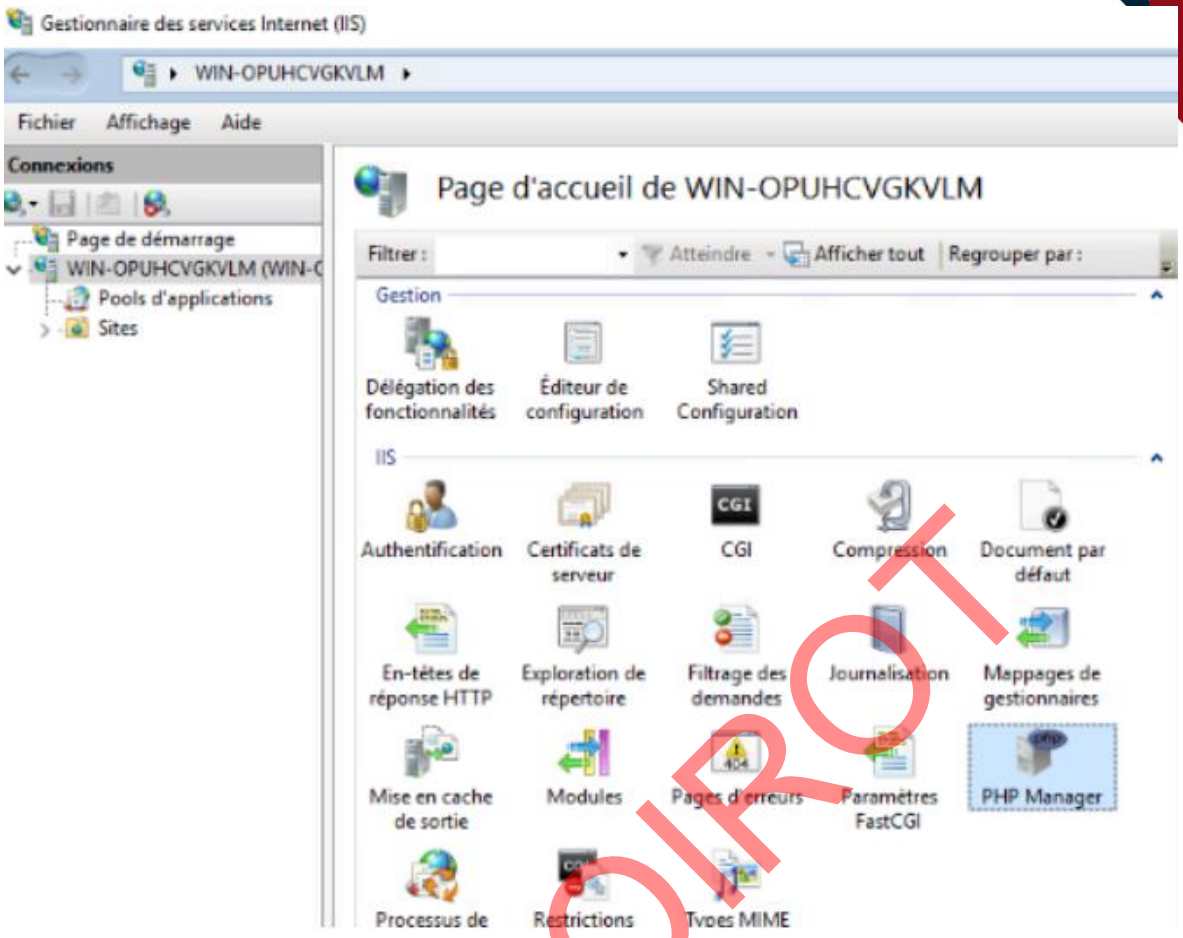
envoyés au module FastCGIModule pour y être exécutés par le programme php-cgi.exe.

• Pour vérifier l'installation de PHP, créer le fichier suivant avec le bloc-notes : 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 :



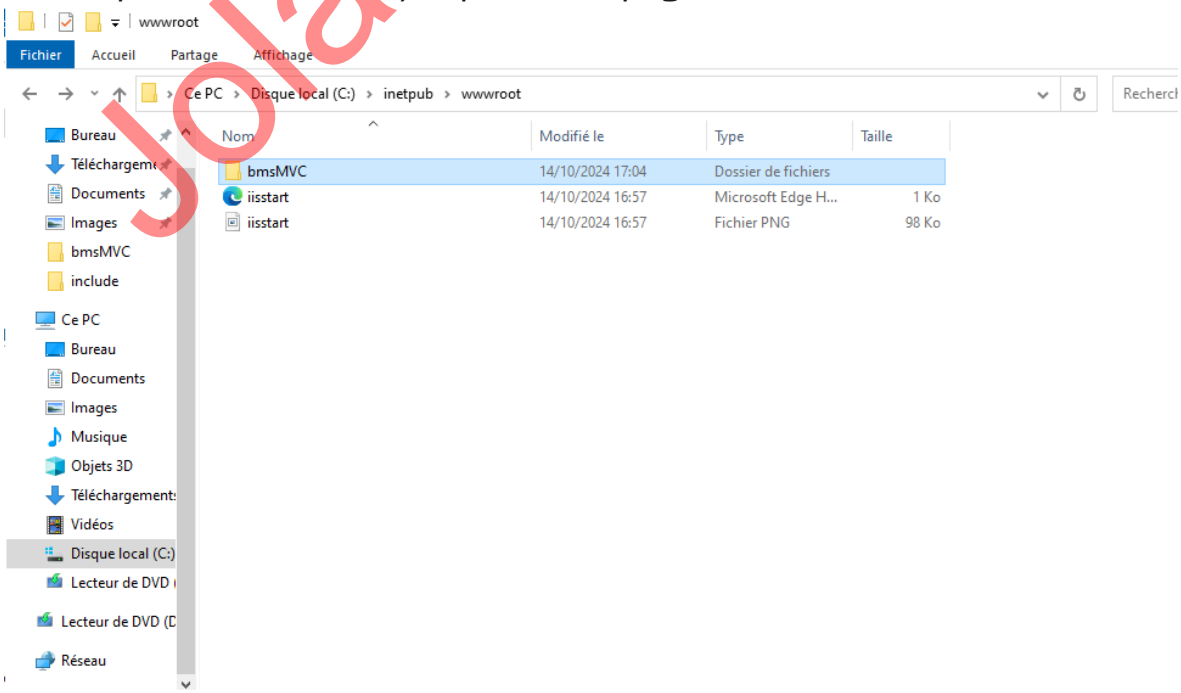
• Installer PHPManager version 1.5, qui fonctionne bien avec IIS version 10, avec le .msi fourni (PHP Manager pour IIS est un outil très pratique permettant de gérer une installation PHP sous Windows (configurer PHP, activer ou désactiver des extensions PHP, ...)).

• 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()) ;



• 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).



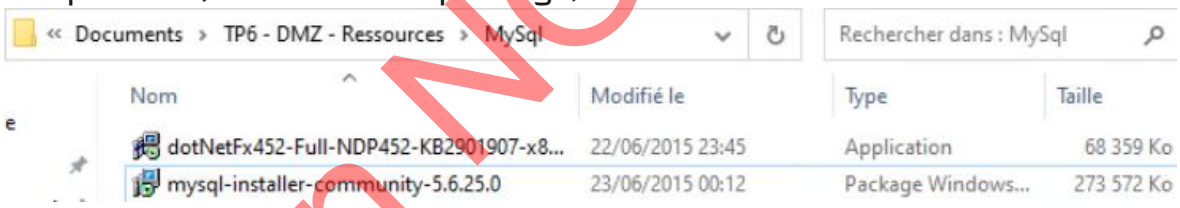
Modifier le script class.pdobms.inc dans le sous-dossier include pour spécifier :

- 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;
        }
```

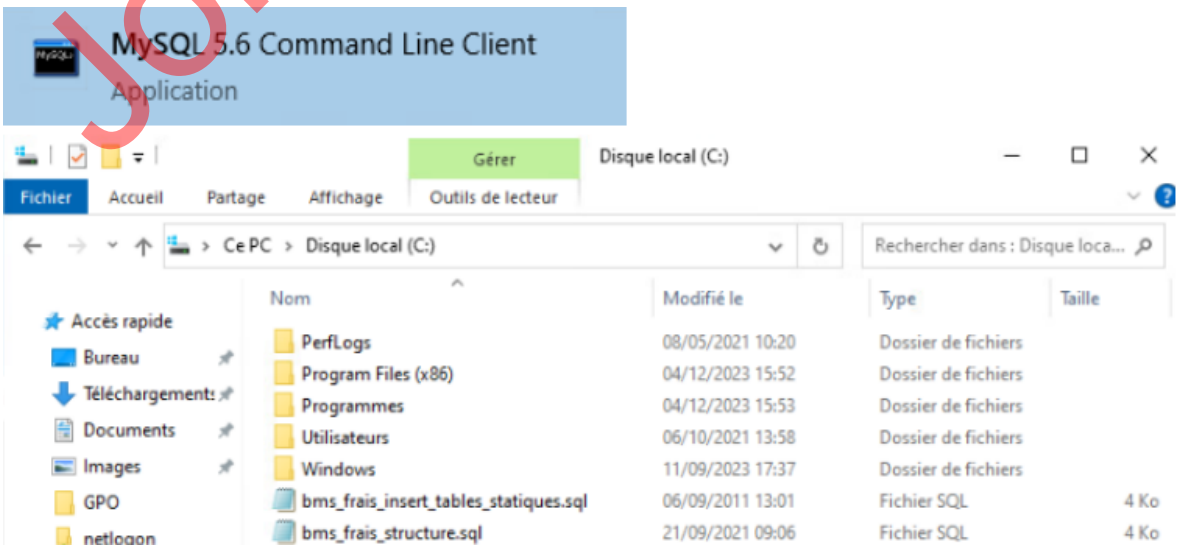
SUR ServeurBDBMS Etapes à suivre :

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



Login : admin/admin

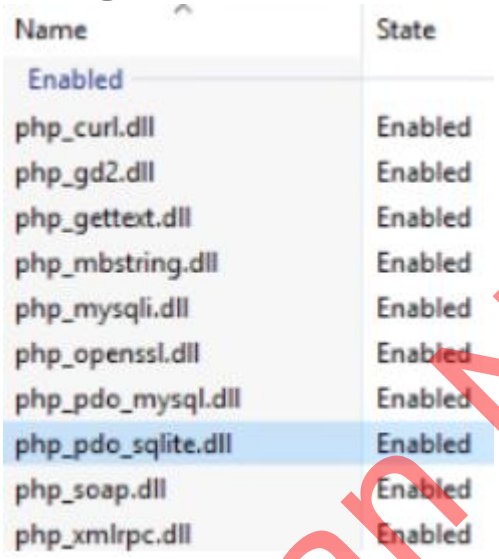
b. Créer la base cinema et exécuter le script de création des tables et des enregistrements (qui est à recopier sur C:\ pour être exécuté avec la commande source :



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";



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)

	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
☐	✓	0/806 B	IPv4 TCP	172.16.10.1	*	192.168.10.2	3306	*	aucun		
☐	✗	0/0 B	IPv4 *	172.16.10.1	*	LAN address	*	*	aucun		
☐	✓	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)

	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
	✓	2/3,57 MiB	*	*	*	LAN Address	80	*	*		Règle anti-blocage
☐	✓	0/43 KiB	IPv4 TCP	*	*	172.16.10.1	80 (HTTP)	*	aucun		
☐	✋	0/3 KiB	IPv4 *	*	*	172.16.0.0/16	*	*	aucun		
☐	✓	21/4,23 GiB	IPv4 *	LAN subnets	*	*	*	*	aucun		Default allow LAN to any rule
☐	✓	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)

	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
☐	✓	0/27 KiB	IPv4 TCP	*	*	172.16.10.1	80 (HTTP)	*	aucun		
☐	✋	0/10,64 MiB	IPv4 *	*	*	*	*	*	aucun		
☐	✓	0/0 B	IPv4 TCP	*	*	172.16.10.1	80 (HTTP)	*	aucun	NAT	

MISSION 7 D : REDIRECTION POUR ACCÉDER DEPUIS INTERNET AU SERVEURWEBDMZ