



Projet BMS

(Laboratoire pharmaceutique Bristol Myers Squibb)



[Schéma complet du réseau](#)

Mission 1 : Installation du serveur de domaine BMS.local *ServeurDomBMS*, du serveur de fichiers *ServeurFicBMS*, de l'imprimante *HPLaserJet5N*, et du PC client *PC1***Error! Bookmark not defined.**

Mission 2 : Installation et configuration générale du Routeur-Pare-feu Pfsense**Error! Bookmark not defined.**

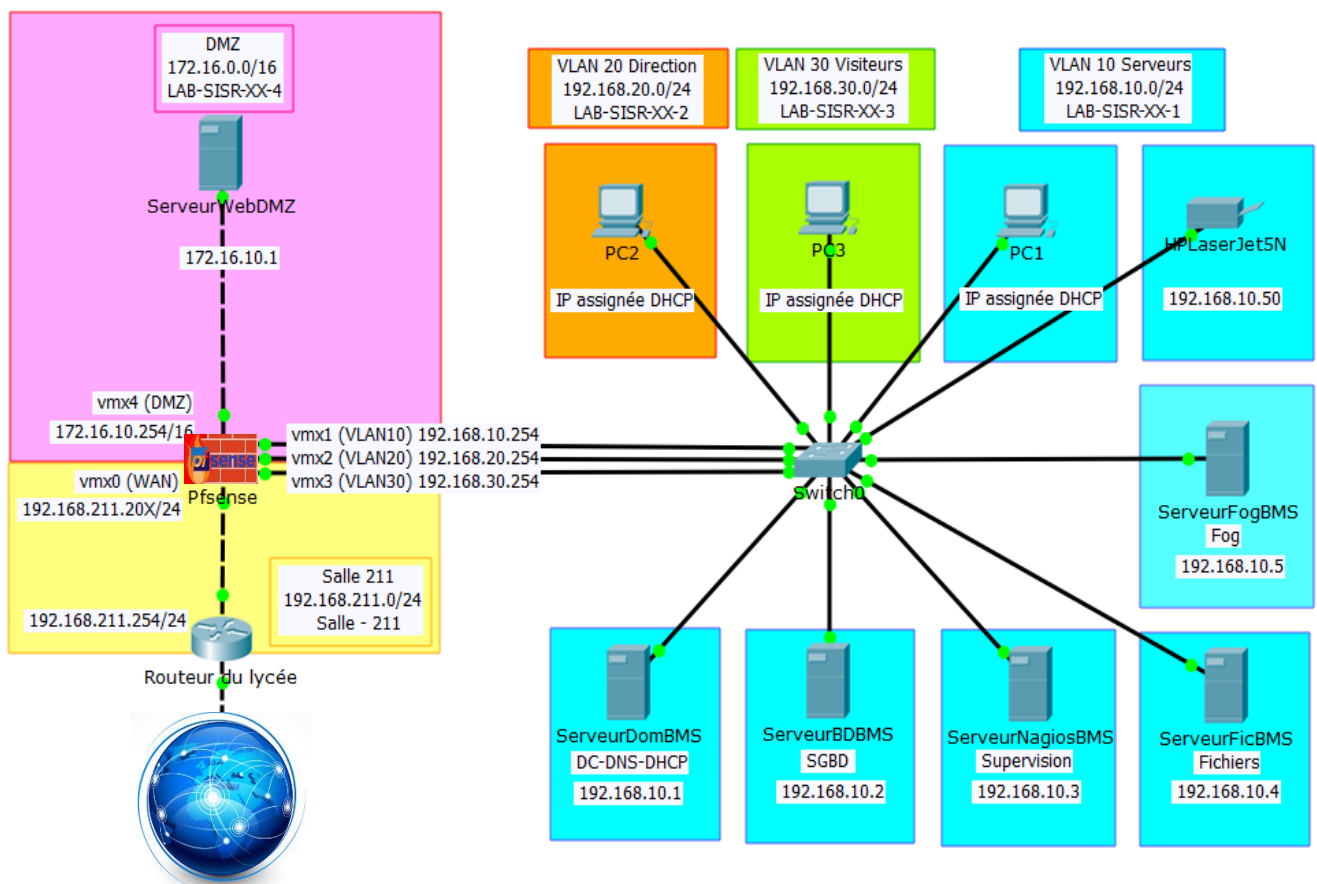
Mission 3 : Installation du serveur de Bases de Données *ServeurBDBMS*, du serveur Web *ServeurWebDMZ*, et de l'application de gestion des frais**Error! Bookmark not defined.**

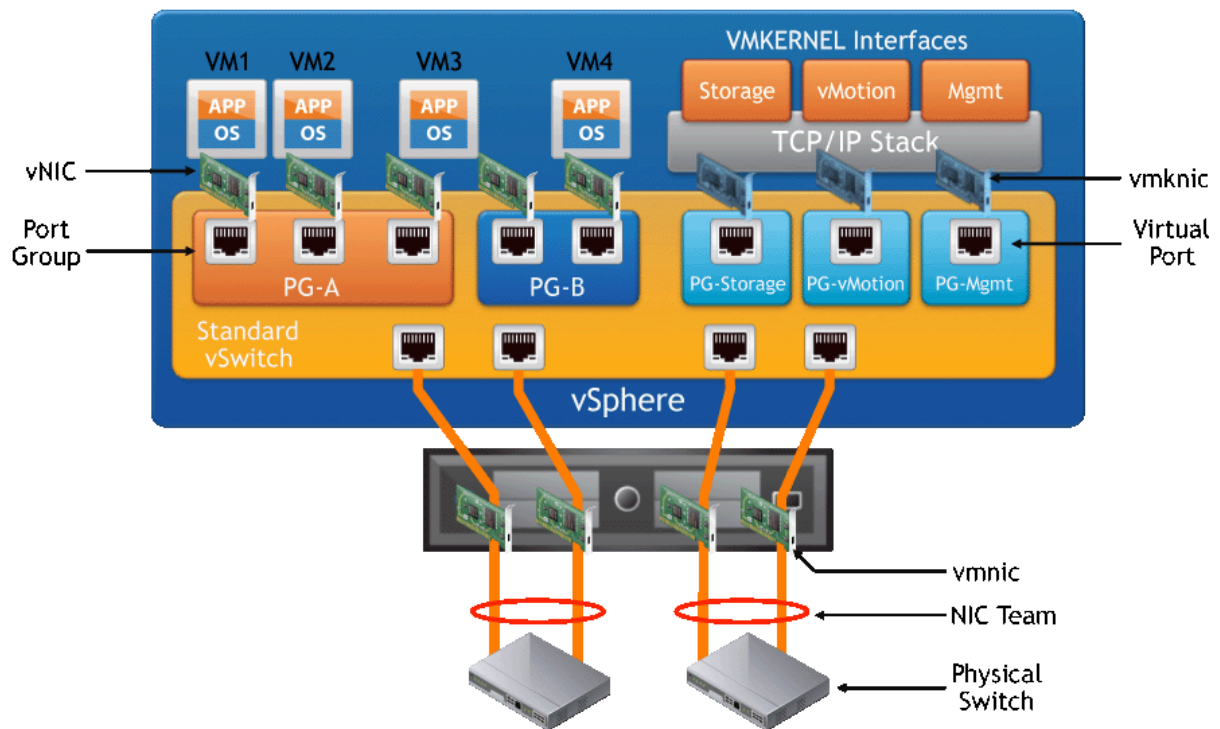
Mission 4 : Configuration des règles de filtrage du routeur-pare-feu Pfsense**Error! Bookmark not defined.**

Mission 5 : Supervision Nagios53

Environnement technique :

Chacun des serveurs virtuels sera créé grâce à Sphère, logiciel fourni avec l'hyperviseur VMware, qui assure la fonction de « tableau de bord » nous permettant d'administrer toutes nos machines virtuelles, L'ensemble des machines virtuelle sont stockés sur des serveurs physiques.





Nous travaillons dans un cluster

-Haute disponibilité

-hyperviseur : VMware (Sphère)

-Sphère tableau de bord qui permet d'administrer toutes les machines virtuelles se situant elle-même sur un serveur physique

-Création d'une nouvelle VM à partir du model win2019

Entrer un nom et l'endroit où stocker la VM

Windows 2019 - MODEL - Déployer depuis un modèle

1 Sélectionner un nom et u...

2 Sélectionner une ressource...

3 Sélectionner un stockage

4 Sélectionner les options ...

5 Prêt à terminer

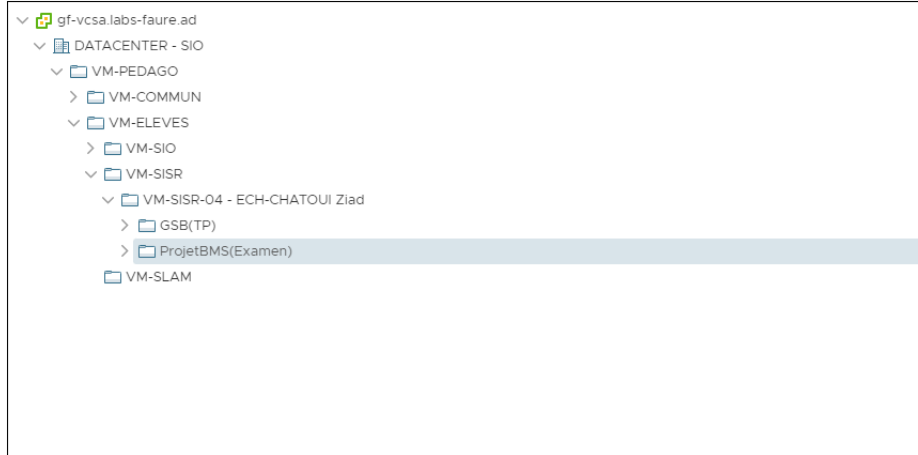
Sélectionner un nom et un dossier

Spécifiez un nom unique et un emplacement cible

Nom de la machine virtuelle :



Sélectionnez un emplacement pour la machine virtuelle.



CANCEL

BACK

NEXT

Sélectionner l'hébergement de base

Windows 2019 - MODEL - Déployer depuis un modèle

✓ 1 Sélectionner un nom et u...

2 Sélectionner une ressource...

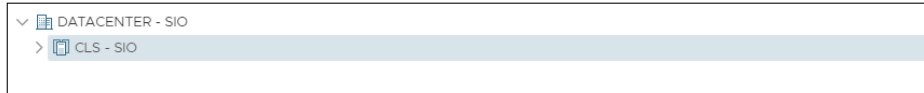
3 Sélectionner un stockage

4 Sélectionner les options ...

5 Prêt à terminer

Sélectionner une ressource de calcul

Sélectionnez la ressource de calcul de destination pour cette opération



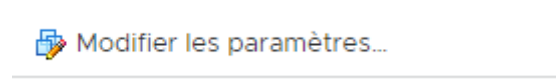
Sélectionnez SISR :

Nom	Capacité	Provisionné	Libre	Type	Cluster
 DS-COMMUN	931,25 Go	895,6 Go	238,07 Go	VMFS 6	
 DS-SISR	9,1 To	4,65 To	6,33 To	VMFS 6	

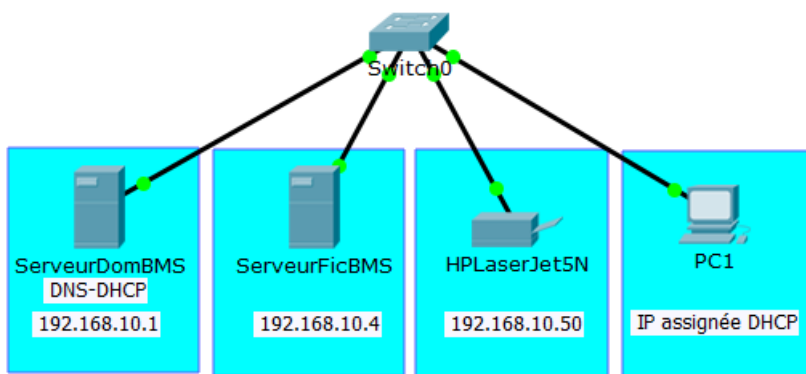
Puis terminer jusqu'à la création de la machine.

-Pensez à modifier l'étiquette de cette VM de cette manière

cliqué droit sur la machine puis



Mission 1 A : installation du contrôleur de domaine



Pourquoi ?

Tout d'abord qu'est-ce qu'un contrôleur de domaine ? Un contrôleur de domaine est un serveur qui répond aux demandes d'authentification et contrôle les utilisateurs des réseaux informatiques.

Nous installons un contrôleur de domaine afin de pouvoir gérer efficacement les utilisateurs, machines de notre réseau du réseau BMS.

- Installer le serveur *ServeurDomBMS* qui sera contrôleur du domaine *BMS.local*, et qui sera aussi serveur DNS et serveur DHCP.

- Pensez à modifier l'étiquette de cette VM (Lab-sisr-04-1)

- Modifier le nom de la machine (ServeurDomBMS)


- Effectuez la configuration IP du poste

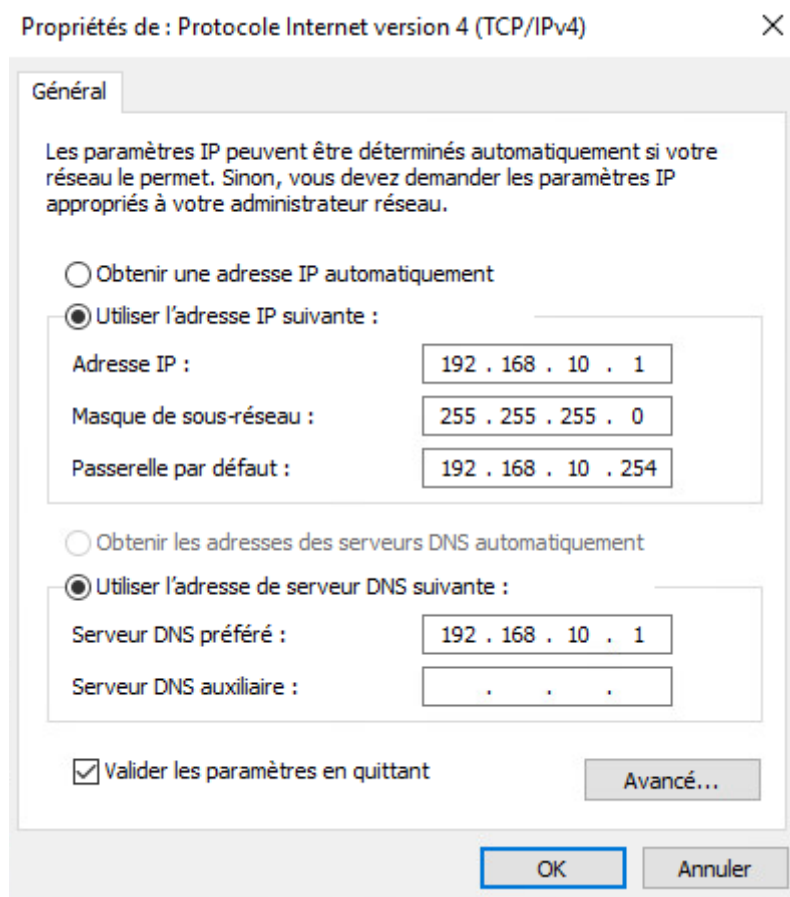
IP : 192.168.10.4

Masque : 255.255.255.0

Passerelle : 192.168.10.254

DNS : 192.168.10.1

Effectuer la configuration IP du serveur en sélectionnant Panneau de configuration  / Réseau et Internet / Centre Réseau et partage d cliquer sur le lien Ethernet : la fenêtre *Etat de Ethernet* s'ouvre : cliquer sur Propriétés ; sélectionner Protocole Internet version 4 (TCP/IP v4) puis cliquer sur le bouton Propriétés :



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

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 : 192 . 168 . 10 . 1

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

Passerelle par défaut : 192 . 168 . 10 . 254

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 192 . 168 . 10 . 1


Serveur DNS auxiliaire : . . .


☒ Valider les paramètres en quittant

Avancé...

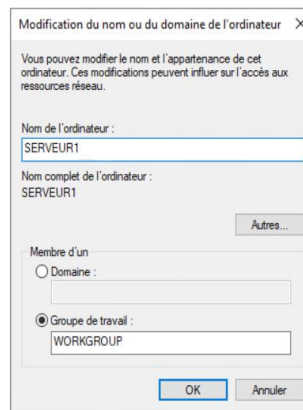
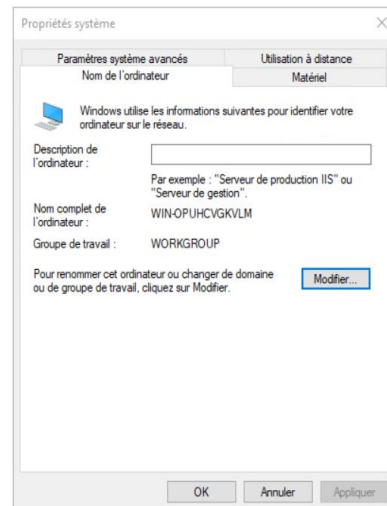
OK Annuler

Effectuer la configuration IP du serveur en sélectionnant Panneau de configuration / Réseau et Internet / Centre Réseau et partage

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

(ou Paramètres  / Système / Informations système / Renommer le PC) :

Nom de l'ordinateur : *SERVEUR1*



- b. Laisser redémarrer le serveur.

Étape 2 : installation de Active Directory

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

Dans la fenêtre *Assistant Ajout de rôles et de fonctionnalités*, choisir une *Installation basée sur un rôle ou une fonctionnalité*.

Sélectionner le serveur de destination sur lequel sera installé le rôle :

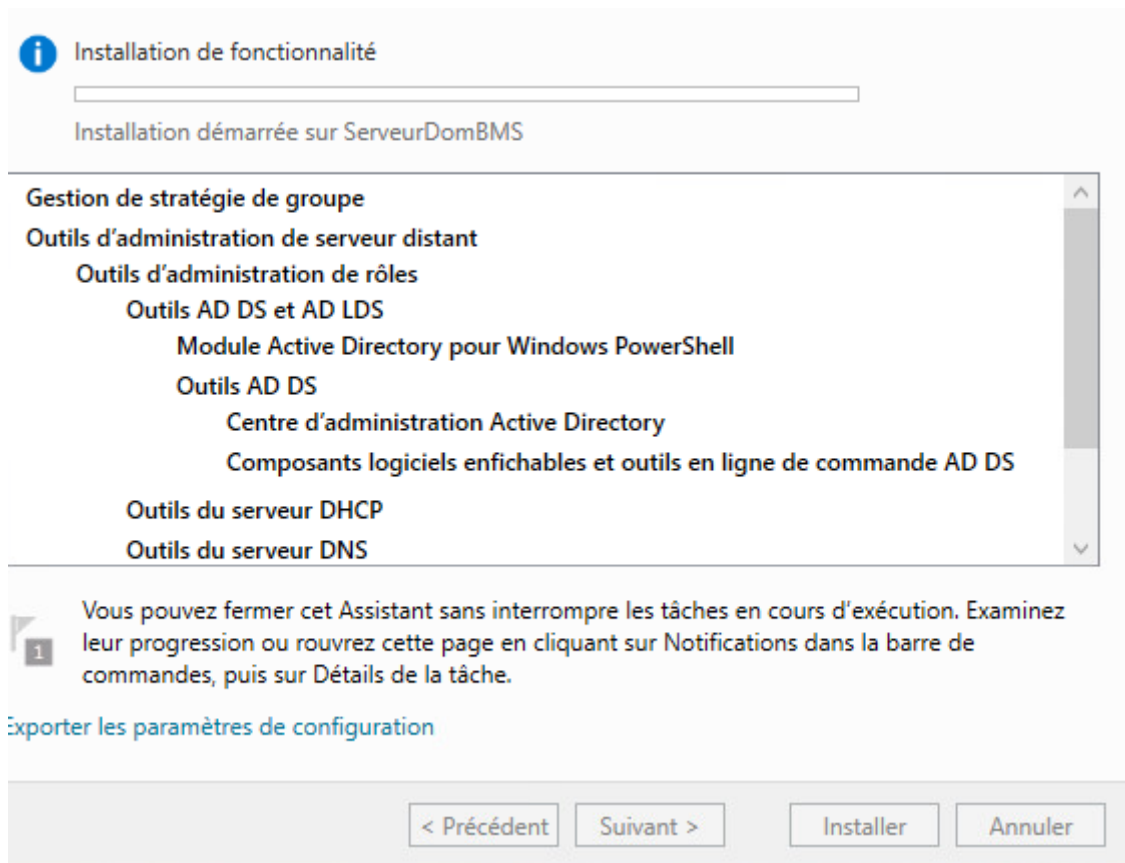
Filtre : <input type="text"/>		
Nom	Adresse IP	Système d'exploitation
ServeurDomBMS	192.168.10.1	Microsoft Windows Server 2019 Standard

Sélectionné

- ☐ Serveur de télécopie
- ☒ **Serveur DHCP**
- ☒ Serveur DNS
- ☐ Serveur Web (IIS)
- ☐ Service Guardian hôte
- ☒ Services AD DS

Ne pas sélectionner d'autres fonctionnalités.

Installation



Cocher la case *Redémarrer automatiquement le serveur de destination si nécessaire* (si un redémarrage est nécessaire, le serveur redémarrera automatiquement), puis confirmer l'autorisation de redémarrage automatique.

Confirmer l'installation de ce rôle en cliquant sur *Installer*.

Configurer le serveur de domaine en cliquant ici



Promouvoir ce serveur en contrôleur de domaine

Cliquer sur l'icône d'avertissement représentée par le triangle jaune (Notifications), puis sur le lien Promouvoir ce serveur en contrôleur de domaine :

- Ajouter une nouvelle forêt
- Nom de domaine racine : BMS.local

Sélectionner l'opération de déploiement

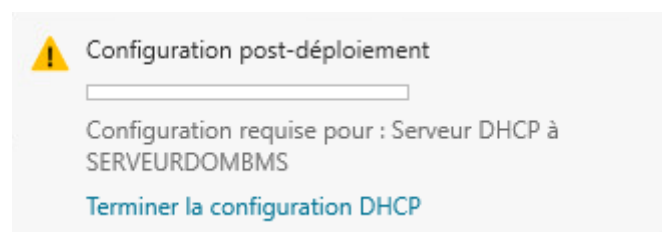
☐ Ajouter un contrôleur de domaine à un domaine existant
☐ Ajouter un nouveau domaine à une forêt existante
☒ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine :

- Choisir le niveau fonctionnel de la forêt et du domaine : *Windows Server 2016*
 - Cocher les cases
 - Serveur DNS* pour installer le service Serveur DNS sur ce contrôleur de domaine
 - Catalogue global* (annuaire central regroupant des éléments de tous les domaines de la forêt)
 - Entrer à nouveau le mot de passe administrateur : *Windows2019*
 - Ne pas tenir compte du message "Il est impossible de créer une délégation pour ce serveur DNS, ..."
 - Nom de domaine NetBIOS : **BMS**
 - 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.
- b. Laisser redémarrer la machine ; ouvrir une session avec l'utilisateur *DOMAINE2019\Administrateur* (ou plus simplement *Administrateur*) et le mot de passe *Windows2019*.

Configurer le serveur dhcp



-outils

DHCP

Mission 1 B : installation d'un serveur de fichiers

- Installer le serveur *ServeurFicBMS* qui sera le serveur de fichiers du domaine *BMS.local* : on stockera sur ce serveur tous les dossiers personnels de base des utilisateurs, ainsi que les dossiers partagés par les utilisateurs du domaine.

Crée une machine avec un SID différent a partir de cette VM


 Windows 2019 avec autre SID -

IP :192.168.10.4

Masque : 255.255.255.0

Passerelle : 192.168.10.254

DNS : 192.168.10.1

Effectuer la configuration IP du serveur en sélectionnant Panneau de configuration  / Réseau et Internet / Centre Réseau et partage d
cliquer sur le lien Ethernet : la fenêtre Etat de Ethernet s'ouvre : cliquer sur Propriétés ; sélectionner Protocole Internet version 4 (TCP/IP v4) puis cliquer sur le bouton Propriétés :

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

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 : 192 . 168 . 10 . 1

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

Passerelle par défaut : 192 . 168 . 10 . 254

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 192 . 168 . 10 . 1


Serveur DNS auxiliaire : . . .


☒ Valider les paramètres en quittant

Avancé...

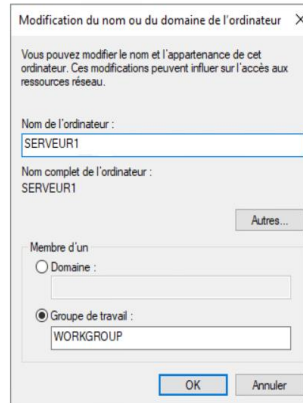
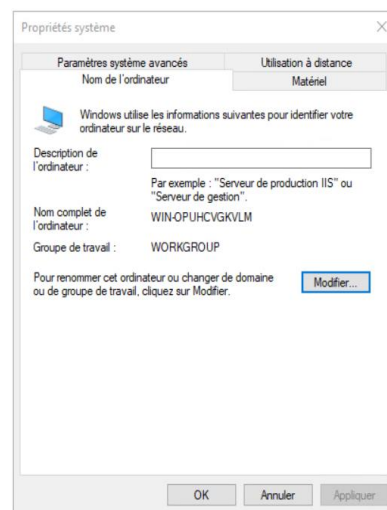
OK Annuler

Effectuer la configuration IP du serveur en sélectionnant Panneau de configuration / Réseau et Internet / Centre Réseau et partage

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

(ou Paramètres  / Système / Informations système / Renommer le PC) :

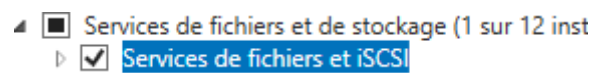
Nom de l'ordinateur : *ServeurFicBMS*



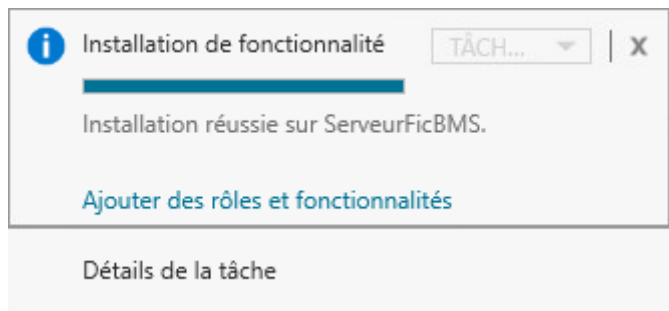
- a. Laisser redémarrer le serveur.

Étape 2 : installation

Cochez ses deux cases




Puis suivant, installer



Installation terminé

Connexion au serveur de domaine

Depuis le poste client, modifier le nom du poste, et connecter ce poste au domaine DOMAINE2019

(Panneau de configuration  / Système et sécurité, Système, lien Paramètres système avancés ; dans la fenêtre qui s'ouvre, sélectionner l'onglet Nom de l'ordinateur, puis le bouton Modifier) :



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

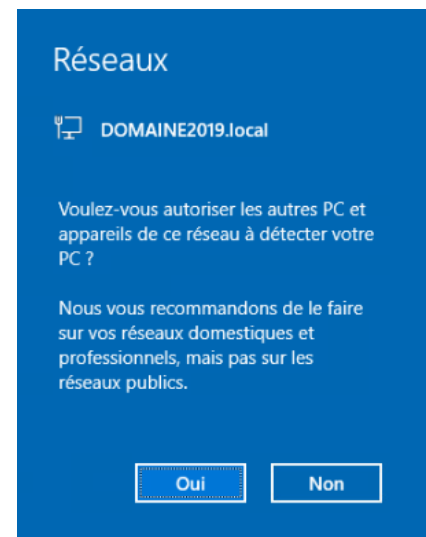
Nom de l'ordinateur : *PC1*

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

Après avoir validé avec OK, ressaisir le nom et le mot de passe du compte administrateur :
Administrateur/Windows2019

Laisser redémarrer la machine, puis ouvrir une session administrateur en se connectant au domaine avec le login *DOMAINE2019\Administrateur* et le mot de passe *Windows2019*.

- f. Si un message s'affiche en bleu, demandant d'autoriser les autres PC de ce réseau à détecter ce PC, cliquer sur Oui.



Mission 1 C : installation du poste client PC1

Création du pc1

Windows 10 21H1 - MODEL - Déployer depuis un modèle

✓ 1 Sélectionner un nom et u...
2 Sélectionner une ressource...
3 Sélectionner un stockage
4 Sélectionner les options ...
5 Prêt à terminer

Sélectionner une ressource de calcul

Sélectionnez la ressource de calcul de destination pour cette opération

▼

DATACENTER - SIO

>

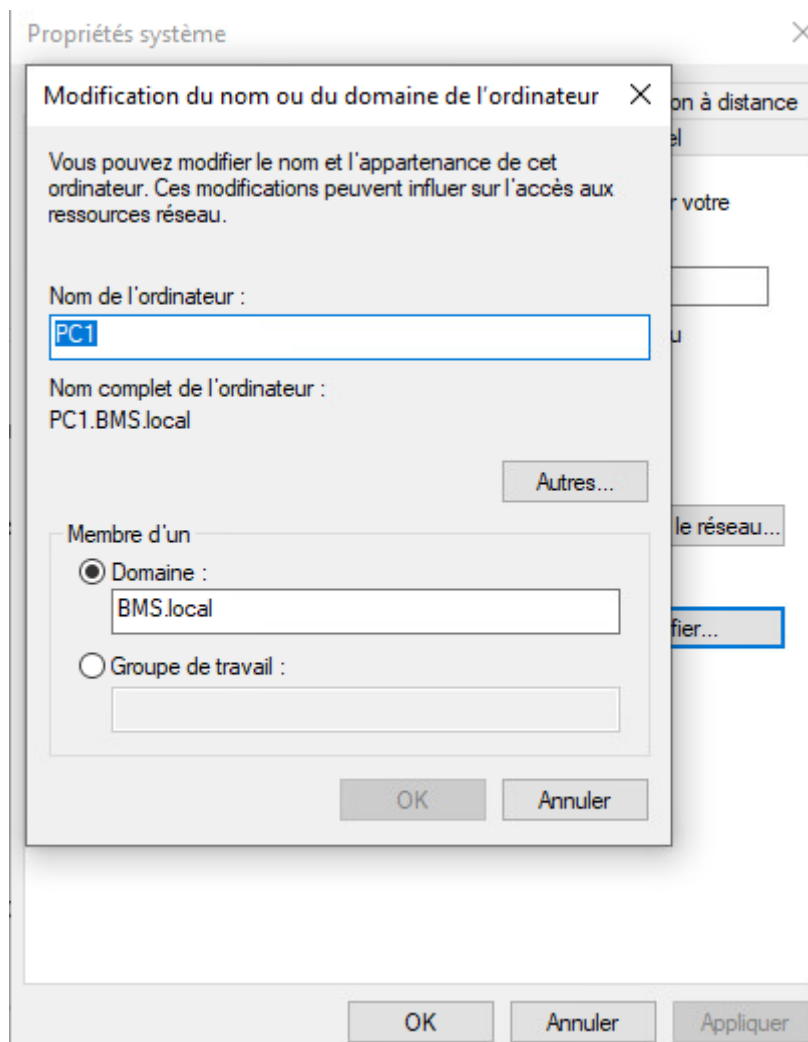
CLS - SIO

Sélectionné DS SISR

DS-SISR	9,1 To	6,38 To	5,63 To	VMFS 6
---------	--------	---------	---------	--------

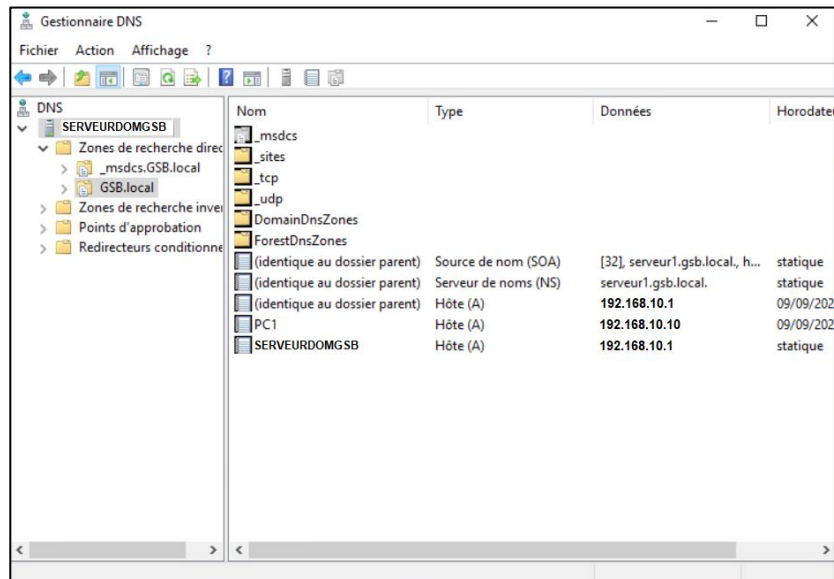
Puis passer à l'étape suivante

N'oubliez pas de modifier l'étiquette réseau :

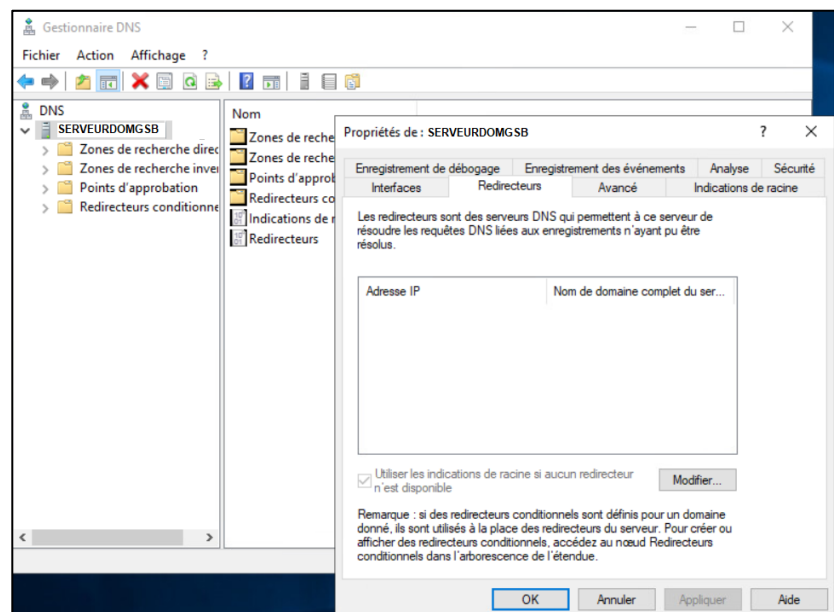


- Installer le PC (sa configuration IP doit être obtenue du DHCP ; il doit être connecté au domaine).

On vérifiera en particulier, que le DNS ne comporte pas d'enregistrements d'adresses 192.168.56.X attribuées par un autre DHCP (celui de VirtualBox par exemple) aux postes du réseau BMS :

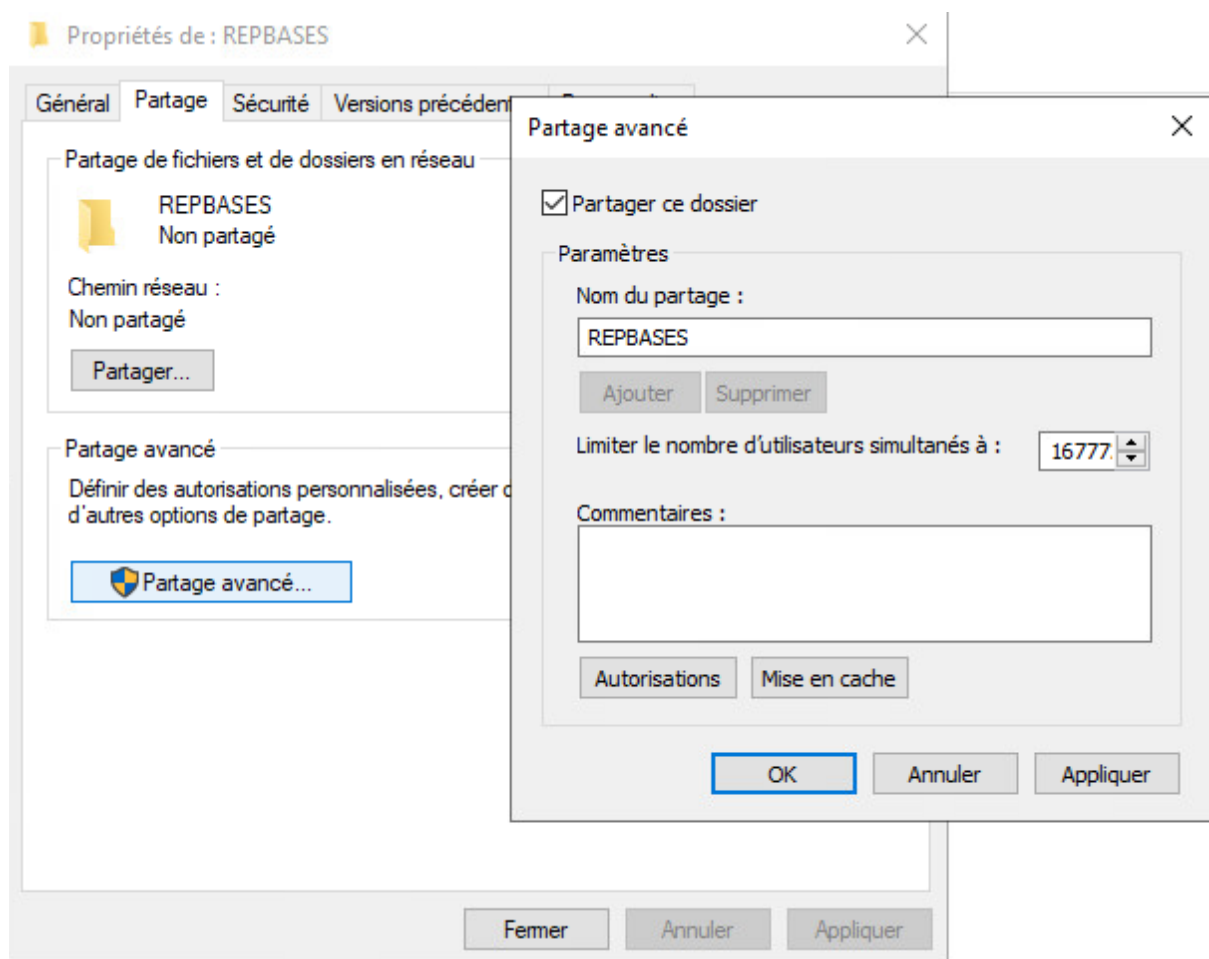


On vérifiera aussi dans les propriétés du DNS qu'il n'existe aucun redacteur "parasite" qui se serait rajouté automatiquement (sinon les supprimer) :



Mission 1 E: création des utilisateurs avec leur dossier personnel de base ; configuration d'autorisations spécifiques à certains dossiers :

- Sur le serveur *ServeurFicBMS*, créer le dossier REPBASES et configurer ses autorisations de partage et ses autorisations de sécurité NTFS ; REPBASES contiendra les dossiers personnels de base de chaque utilisateur (**TP SI5 de référence : [TP2 A - Création de comptes-utilisateurs](#)**).



- 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 :

<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	<i>Windows2019</i>
Albert Dubois	adubois	adubois	<i>Windows2019</i>
Clémence Rousseau	crousseau	crousseau	<i>Windows2019</i>
Vincent Ogier	vogier	vogier	<i>Windows2019</i>
Louis Ravignac	lravignac	lravignac	<i>Windows2019</i>

Le DSI demande ensuite de créer sur *ServeurFicBMS*, des dossiers (*DocCommerciaux*, et *DocJuridique*) pour la gestion des contrats et d'y affecter des droits d'accès NTFS différents à deux groupes d'utilisateurs (*Commerciaux* et *Juridique*).

C: \

DocCommerciaux

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

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

Les utilisateurs du groupe *Juridique* doivent pouvoir lire, créer, modifier et supprimer des fichiers et sous-dossiers dans le dossier *DocJuridique* ; les commerciaux ne doivent pouvoir que lire les fichiers de ce dossier ou de ses sous-dossiers.

Les utilisateurs du groupe *Commerciaux* doivent pouvoir créer des fichiers ou des sous-dossiers dans le dossier *DocCommerciaux* ; attention, un commercial ne doit pouvoir lire, modifier et supprimer que les fichiers et sous-dossiers qu'il a lui-même créés (et non ceux des autres utilisateurs).

Le groupe *Juridique* doit pouvoir lire, modifier et supprimer les fichiers et sous-dossiers de *DocCommerciaux*.

Mission 2 : Installation et configuration générale du Routeur-Pare-feu Pfsense

Mission 2 A : installation du Pfsense

- Vérifier que la machine virtuelle Pfsense dispose de 5 cartes réseau (si ce n'est pas le cas, mettre hors-tension la machine et ajouter les cartes nécessaires).
- Assigner les interfaces du Pfsense (fonction 1 : *Assign Interfaces* sur l'écran d'interface texte du Pfsense)

WAN : vmx0 salle 211

LAN : vmx1 lab 01

OPT1 : vmx2 lab 03

Modifier les paramètres... | Pfsense-projetBMS ×

Matériel virtuel Options VM

AJOUTER UN PÉRIPHÉRIQUE

> CPU	1	Go	
> Mémoire	2	Go	
> Disque dur 1	15	Go	
> Contrôleur SCSI 0	LSI Logic SAS		
> Adaptateur réseau 1	SALLE - 211		<input checked="" type="checkbox"/> Connecter...
> Adaptateur réseau 2 *	LAB-SISR-04-1		<input checked="" type="checkbox"/> Connecter...
> Nouveau réseau *	LAB-SISR-04-3		<input checked="" type="checkbox"/> Connecter...
> Lecteur CD/DVD 1	Fichier ISO banque de données		<input checked="" type="checkbox"/> Connecter...
> Carte vidéo	Spécifier les paramètres personnalisés		
Périphérique VMCI	Périphérique sur le bus PCI de la machine virtuelle fournissant la prise en charge pour l'interface de communication de la machine virtuelle		
> Autre	Matériel supplémentaire		

ANNULER OK

Modifier l'étiquette réseau de cette manière

Configuration pfsense

```
Should VLANs be set up now [y:n]? n
```

Pas de vlan pour l'instant

Configuration les interfaces

```
(vmx0 vmx1 vmx2 or a): vmx0
```

Correspond à salle 211

```
(vmx1 vmx2 a or nothing if finished): vmx1
```

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

```
Available interfaces:

1 - WAN (vmx0 - dhcp, dhcp6)
2 - LAN (vmx1 - static)
3 - OPT1 (vmx2)

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:
> 192.168.211.204

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
```

```
WAN    -> vmx0
LAN    -> vmx1
OPT1   -> vmx2

Do you want to proceed [y!n]? y
```

Configuration interfaces ip

Dans pfsense taper 2

```
Available interfaces:

1 - WAN (vmx0 - dhcp, dhcp6)
2 - LAN (vmx1 - static)
3 - OPT1 (vmx2)

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:
> 192.168.211.204

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
```

Entrer comme gateway : 192.168.211.254

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.254

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 LAN IPv4 subnet bit count (1 to 31):
> 24

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

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

```
Enter the new OPT1 IPv4 address. Press <ENTER> for none:  
> 172.16.10.254  
  
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):  
> 16
```

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

Après avoir effectuer ces manipulations rendez-vous sur votre navigateur et taper l'ip du WAN

192.168.211.204/24

Connectez vous avec « admin » « pfsense »



-Décocher cette case

Block RFC1918 Private Networks

☒ Block private networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

[Anonymous User Survey](#)

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

[Finish](#)

Finish

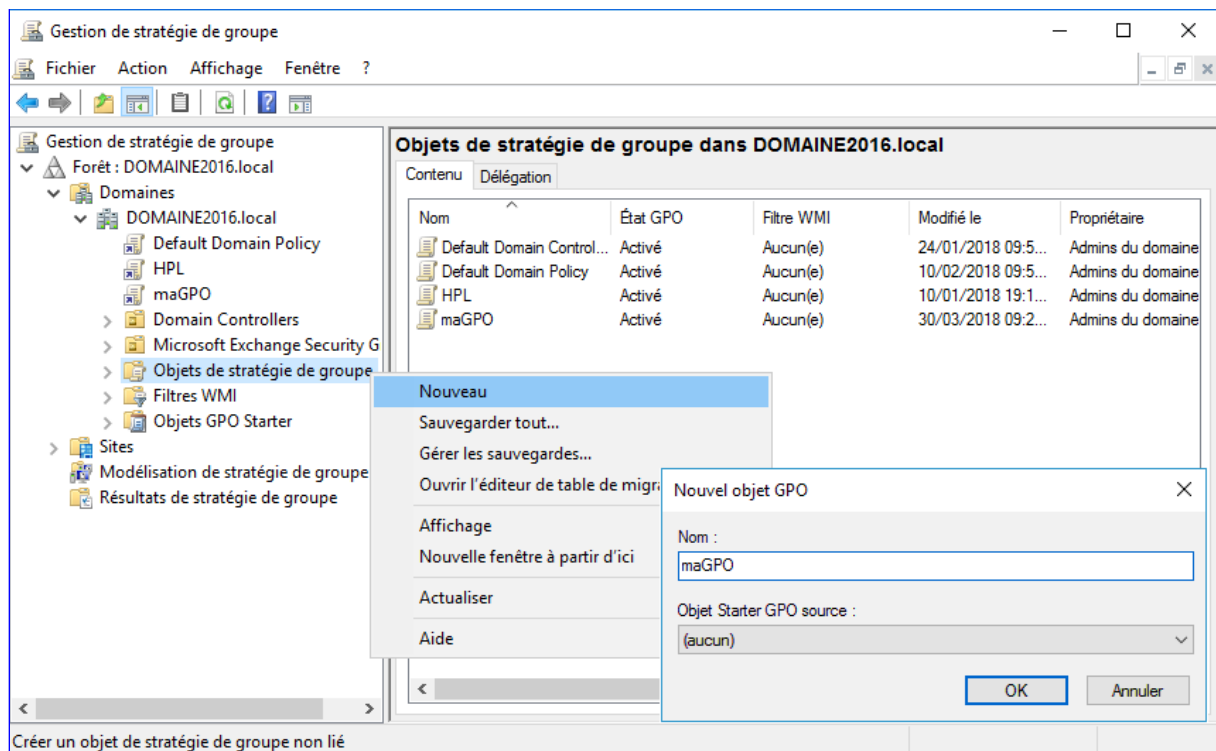
Mission 1 D : installation/déploiement de matériels et de logiciels sur les postes

Création GPO

Annexe : Création d'une GPO

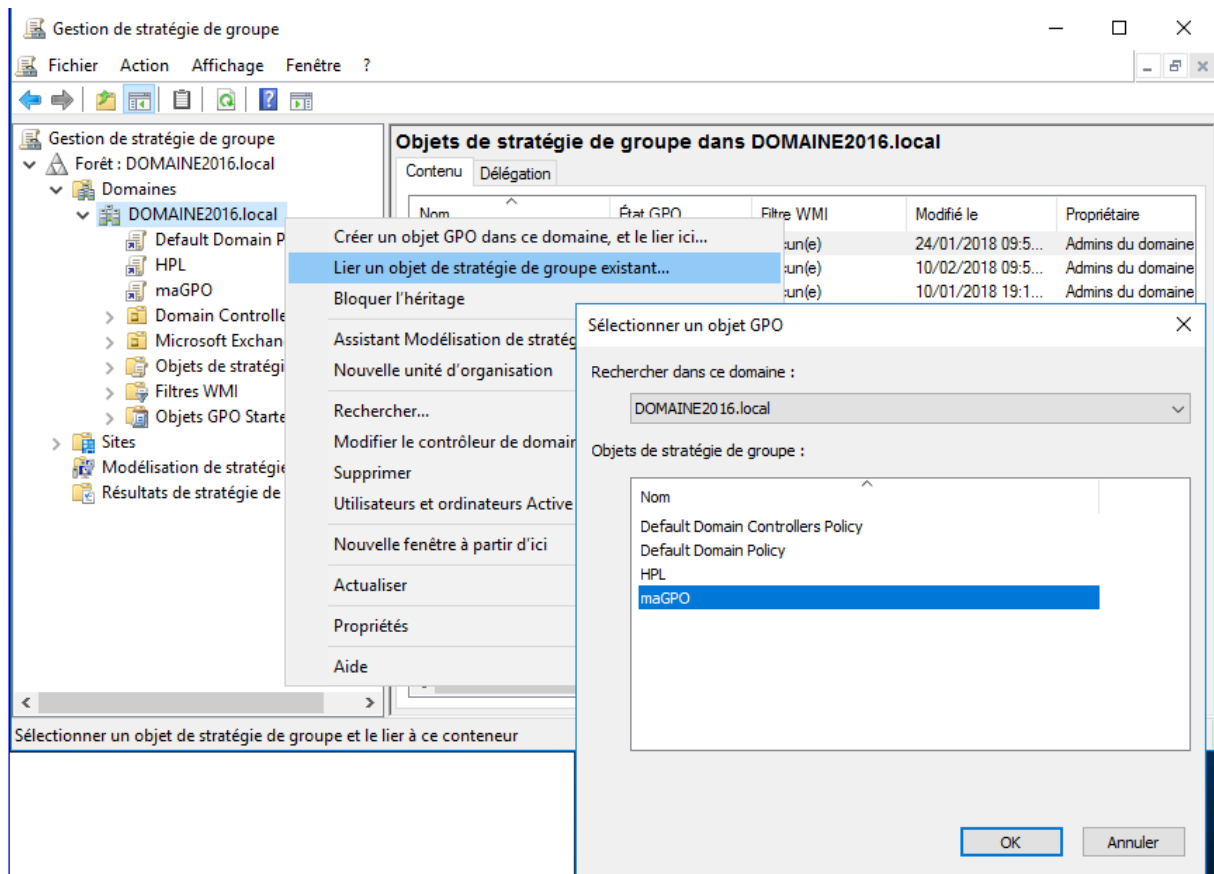
a) Création de la GPO :

cliquer droit sur le conteneur *Objets de stratégie de groupe*, puis sélectionner la commande contextuelle *Nouveau* ; dans la boîte de dialogue *Nouvel objet GPO*, entrer le nom de la GPO à créer :



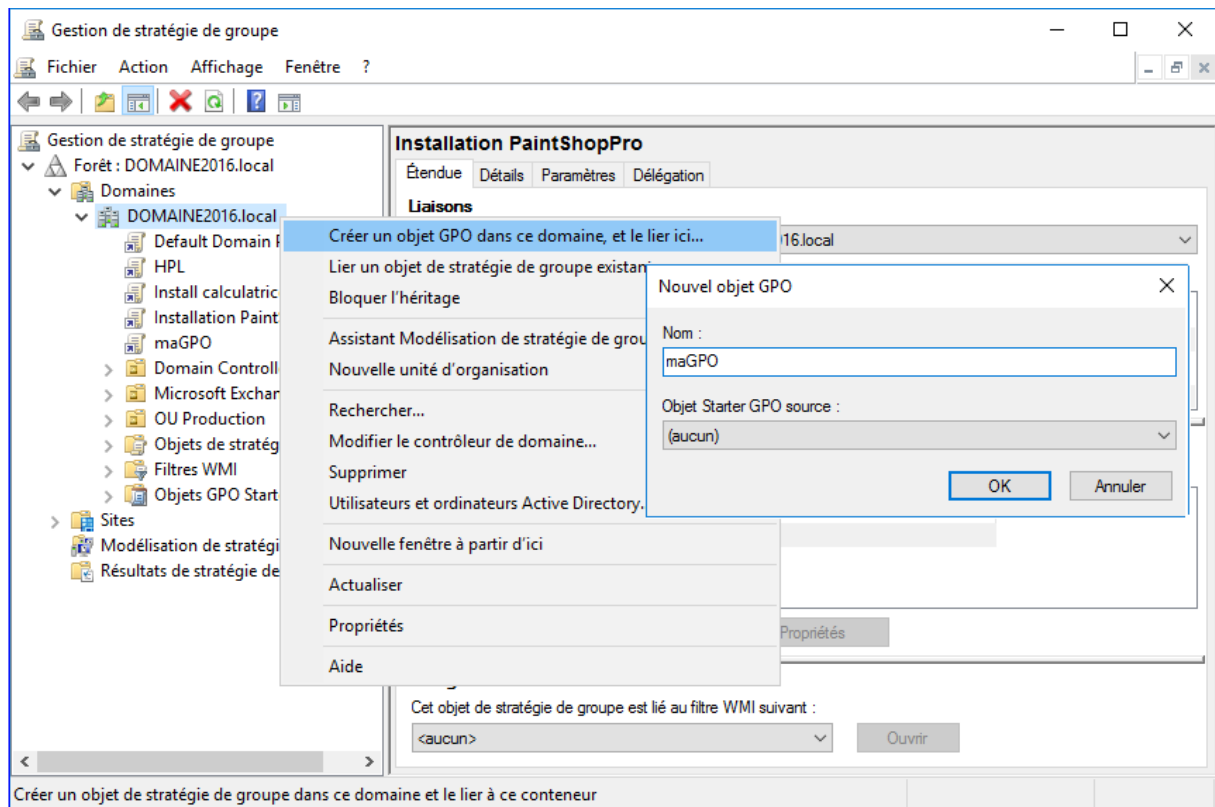
b) Application de la GPO à un domaine ou à une ou plusieurs OU :

- cliquer droit sur le domaine ou l'OU auquel on souhaite appliquer la GPO, puis sélectionner la commande contextuelle *Lier un objet de stratégie de groupe existant* ; dans la boîte de dialogue *Sélectionner un objet GPO*, sélectionner la GPO souhaitée :



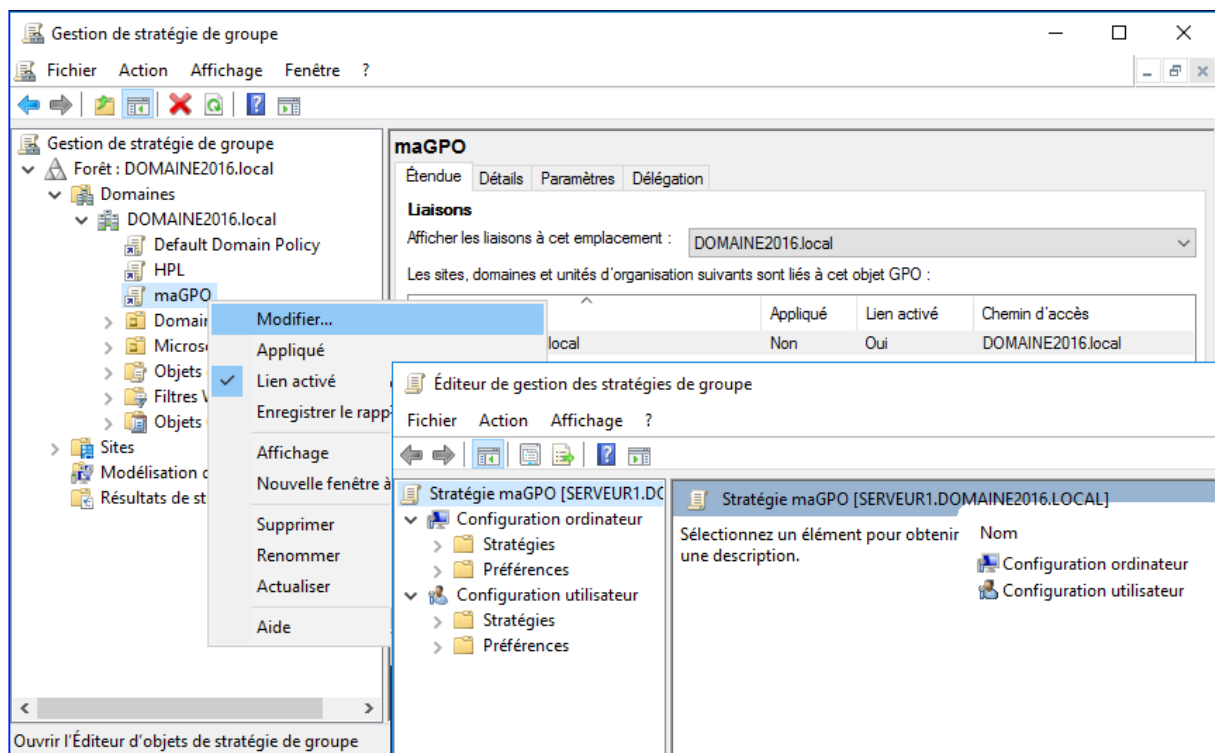
Remarque : on peut créer et appliquer une GPO à un domaine ou à une OU en une seule commande :

- cliquer droit sur le domaine ou l'OU auquel on souhaite appliquer la GPO, puis sélectionner la commande contextuelle *Créer un objet GPO dans ce domaine, et le lier ici ...* ; dans la boîte de dialogue *Nouvel objet GPO*, entrer le nom de la GPO à créer et à appliquer :



c) Spécification de l'application à exécuter par cette GPO :

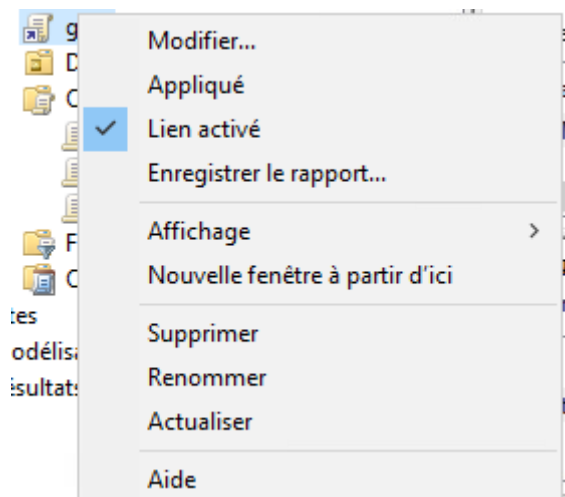
- cliquer droit sur la GPO à modifier, puis sélectionner la commande contextuelle *Modifier* ; la boîte de dialogue *Editeur de stratégies de groupe* s'ouvre :



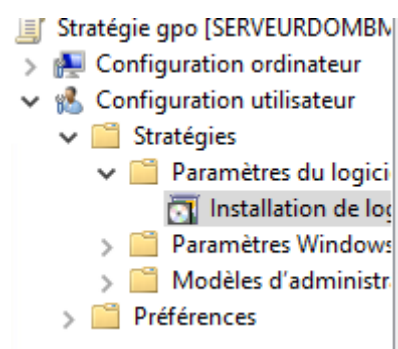
Pour installer un logiciel automatiquement vous devez d'abord avoir le msi du logiciel

Download	.msi	64-bit Windows x64
--------------------------	------	--------------------

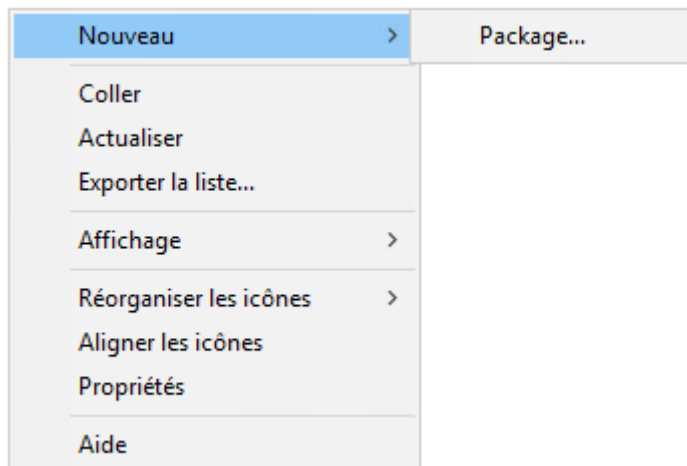
Modifier



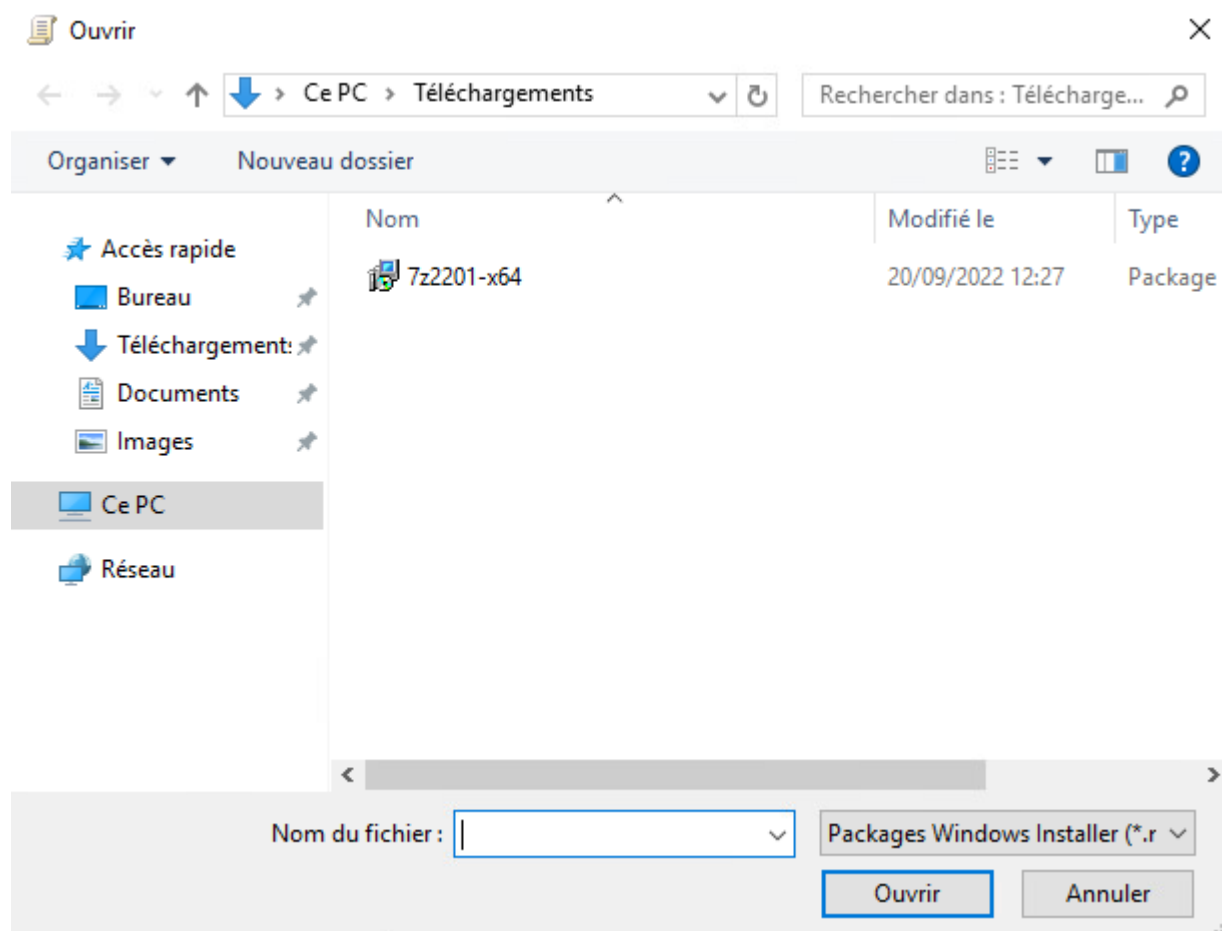
Puis aller dans installation logiciel



Puis



Importer vos .msi

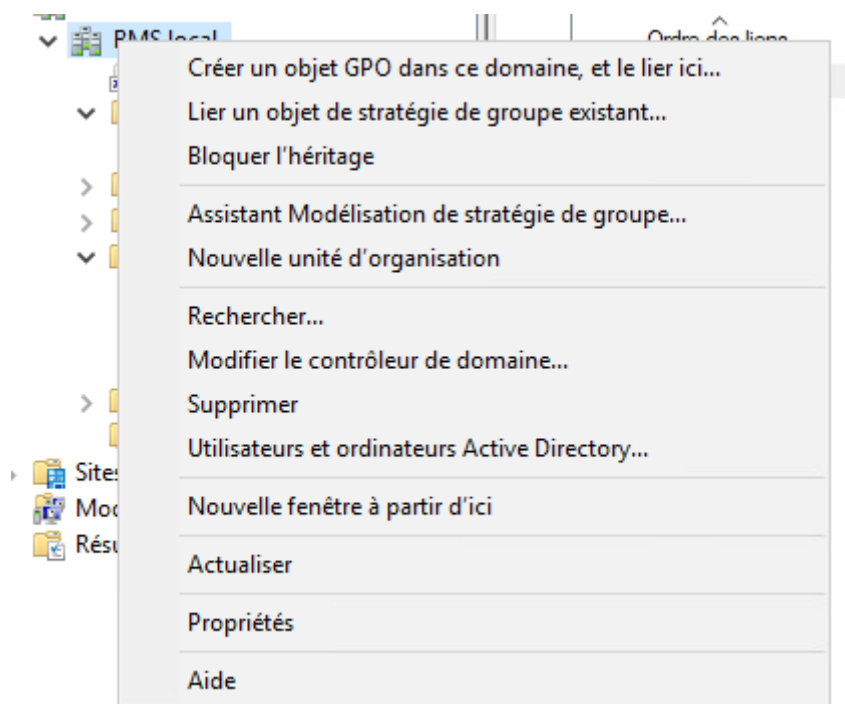


Mission 1 D : installation/déploiement de matériels et de logiciels sur les postes

Crée une OU pour pouvoir filtrer les gpos

Création d'une GPO :

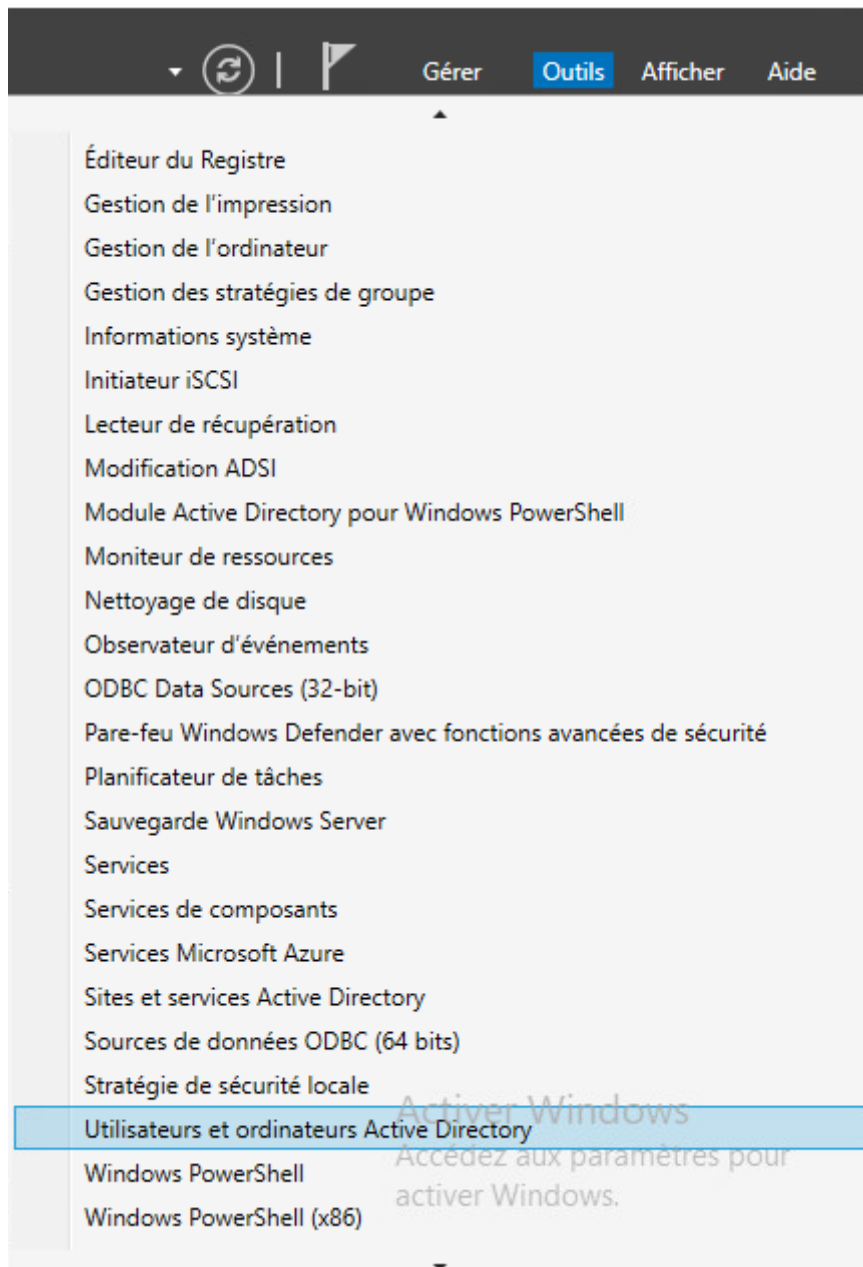
Cliquez droit sur « BMS.local » puis Nouvelle unité d'organisation



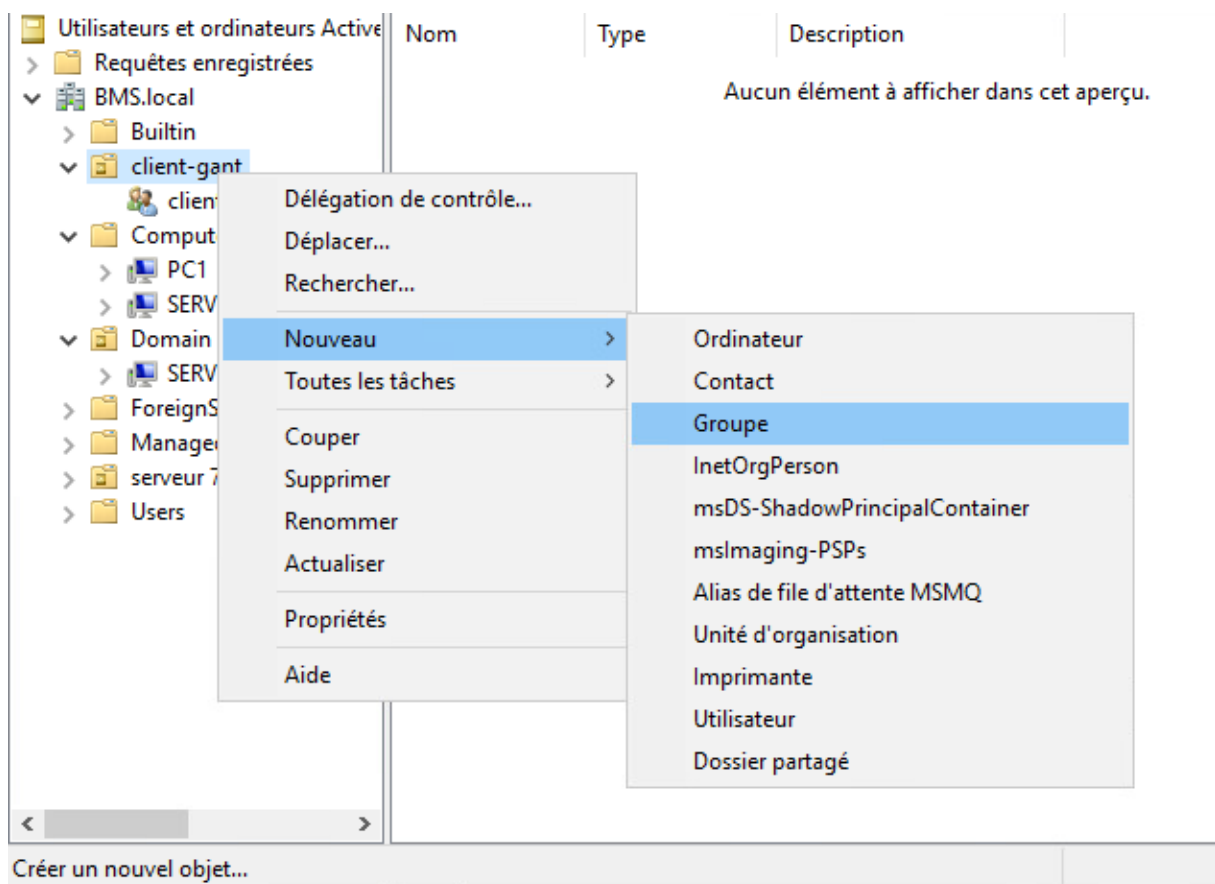
Entre un nom

Filtrage :

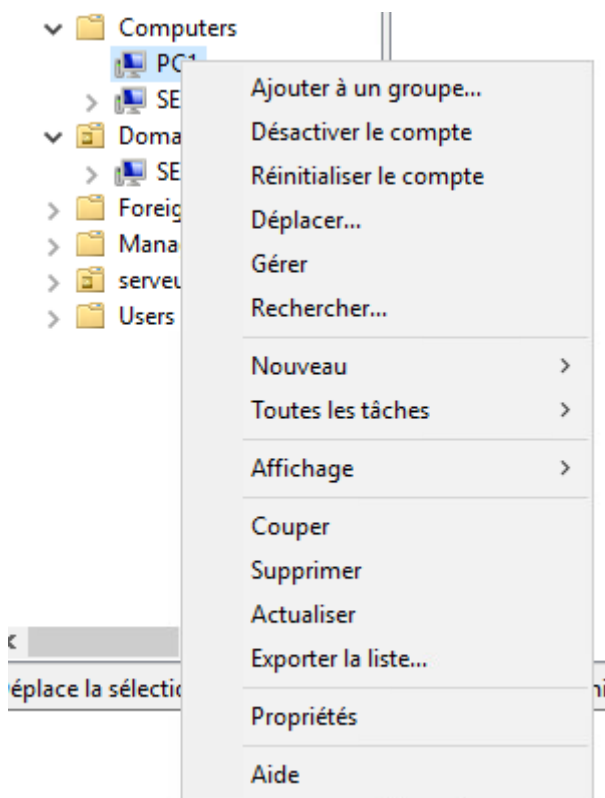
Rendez vous dans « utilisateurs active directory »



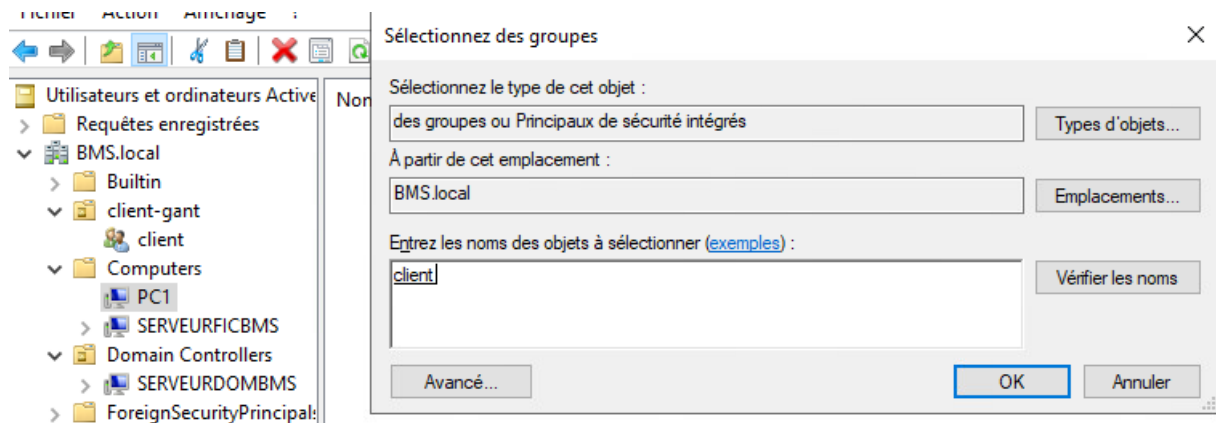
Crée un nouveau groupe



Puis déroulé le fichier « computer »



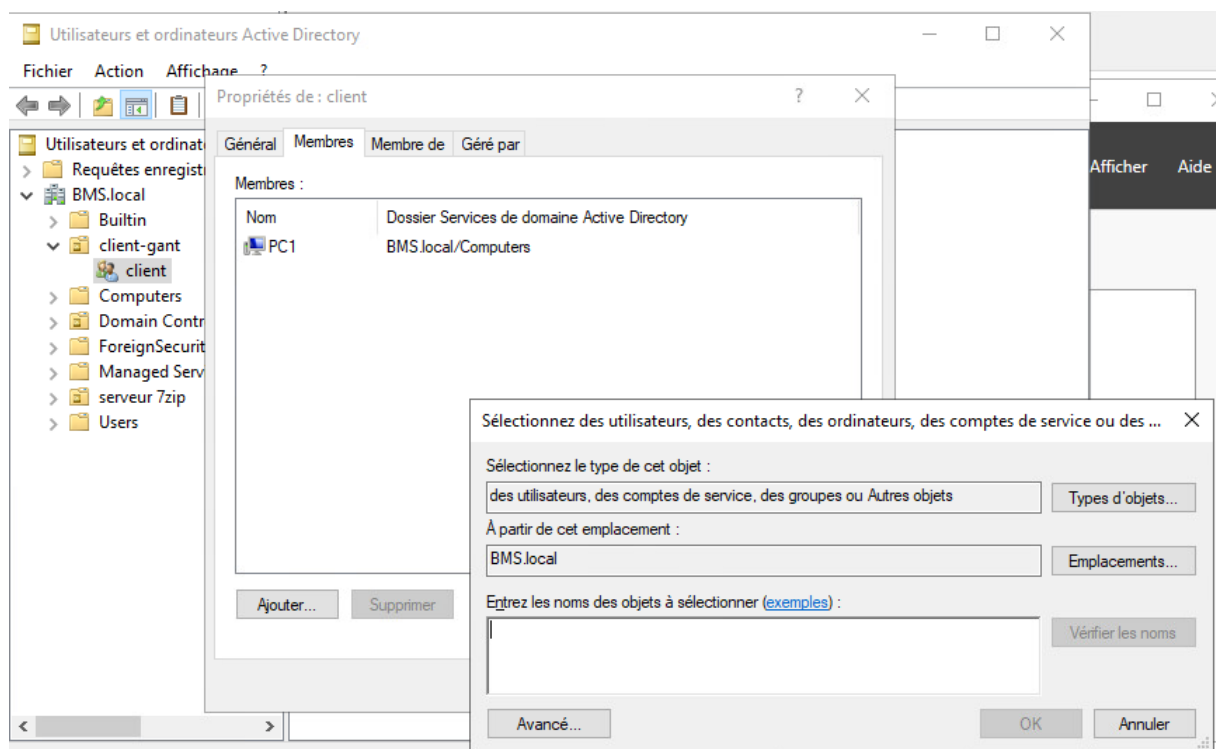
Clique droit sur la machine que vous voulez ajouter puis « ajouter à un groupe »



Ecrivez le groupe auquel vous voulez ajouter l'appareil puis « ok »

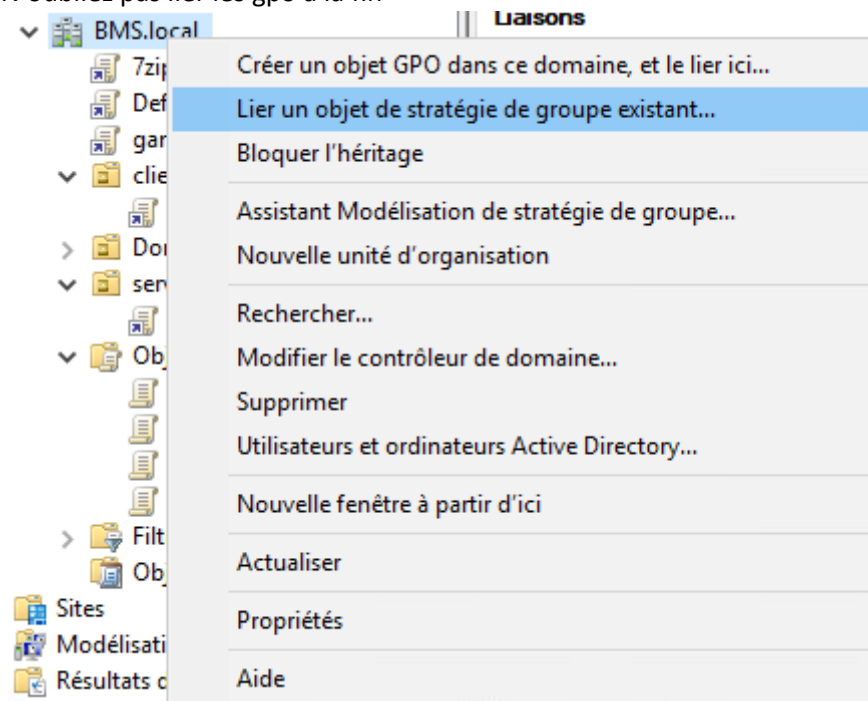
Puis réglé la GPO en reproduisant les manipulations ici (lien qui mène a comment crée une gpo)

(VOUS POUVEZ AUSSI LE FAIRE D'UNE ATRE MANIERE

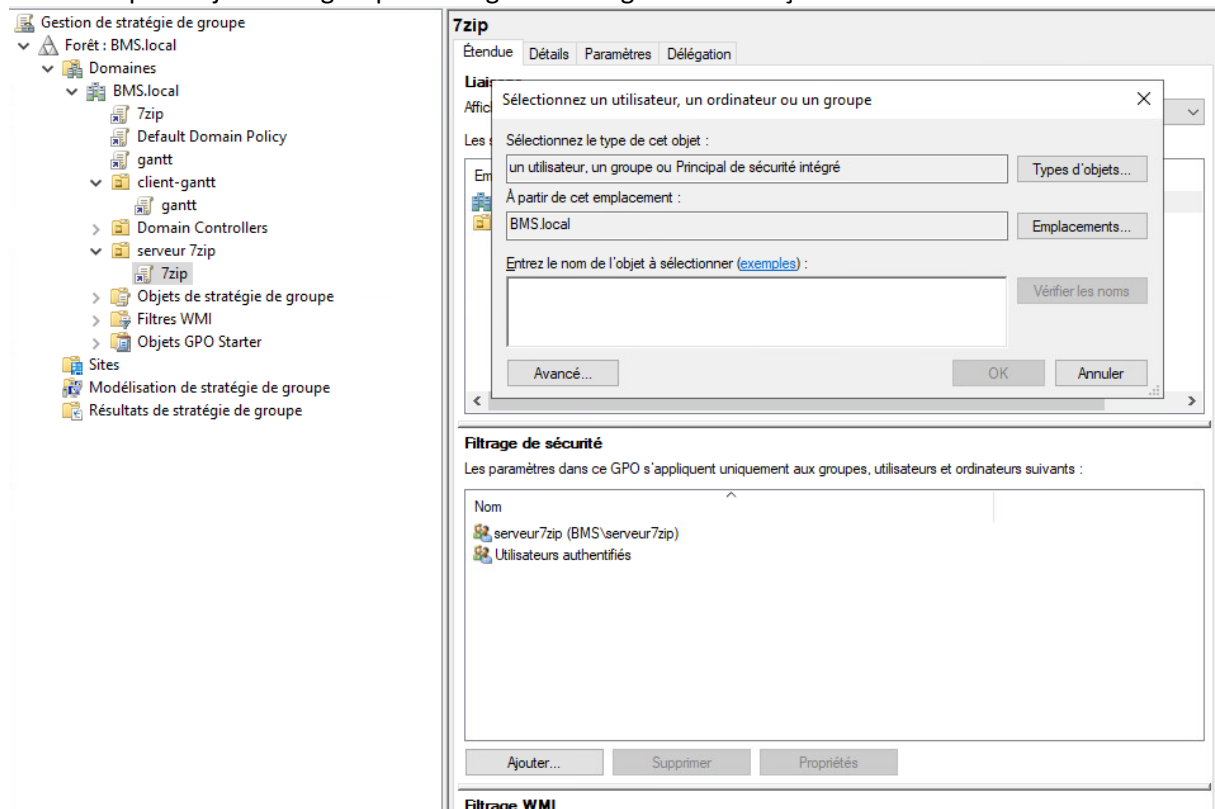


)

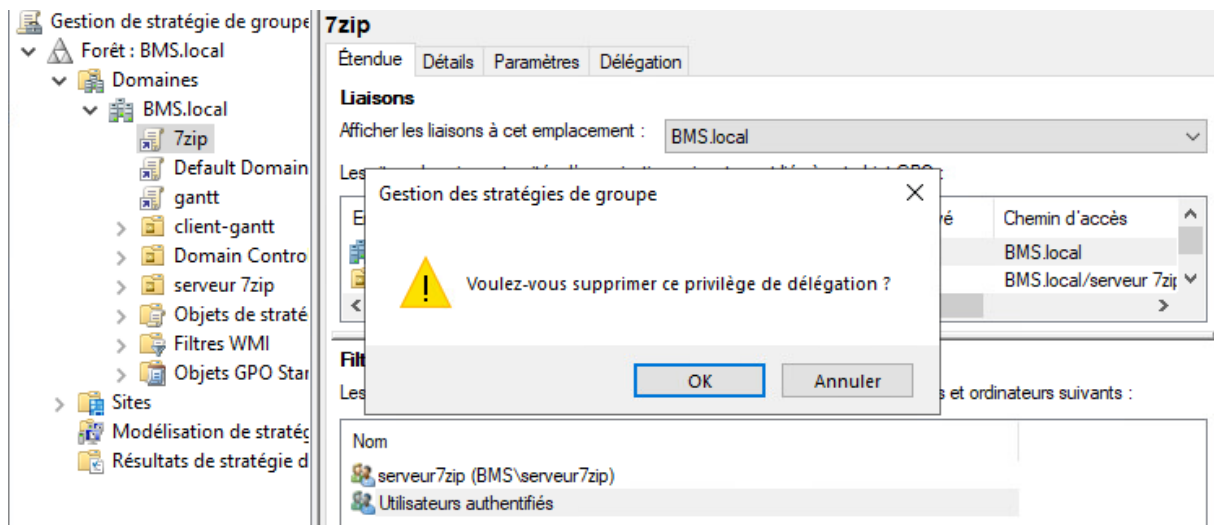
N'oubliez pas lier les gpo a la fin



N'oubliez pas d'ajouter le groupe aux règle de filtrage de cette façon



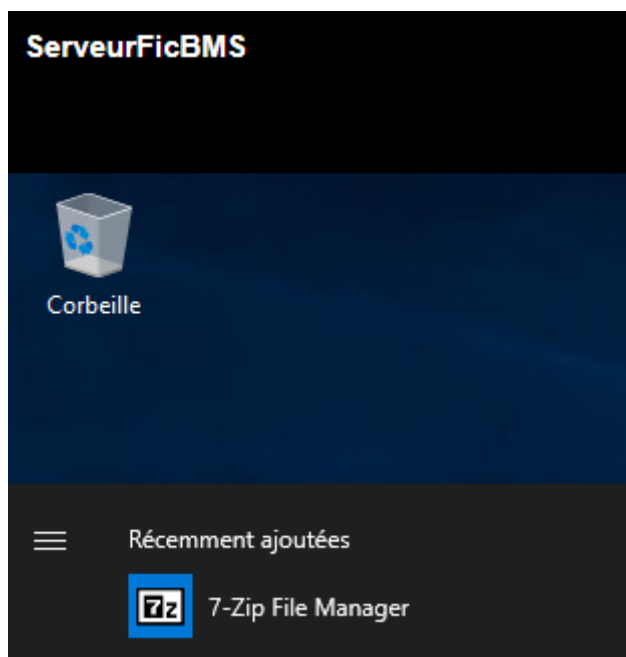
Il vous faut aussi supprimé « Utilisateurs authentifié » dans le menu « étendue »



On valide tout ça en redémarrant le service avec

```
C:\Users\Administrateur>gpupdate /force  
Mise à jour de la stratégie...
```

Vous pouvez maintenant vérifié que tout est bien installé




Installation de l'imprimante LaserJet 5200

Objectifs

Le but est l'installation complète d'une imprimante réseau.

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

Étape 1 : vérification de la configuration du DHCP

- c. Sélectionner Gestionnaire de serveur  / Outils / DHCP, puis vérifier que le serveur DHCP contient bien une étendue de nom *Etendue1* lui permettant de distribuer une adresse IP comprise entre 10.0.2.10 et 10.0.2.19 avec le masque de sous-réseau 255.255.255.0, la passerelle 10.0.2.254 et le DNS 10.0.2.5, à toute machine qui en fait la demande.

Étape 2 : réservation DHCP d'une adresse IP pour l'imprimante

Nous allons d'abord nous occuper de la configuration IP de l'imprimante HP LaserJet5N à installer sur le réseau.

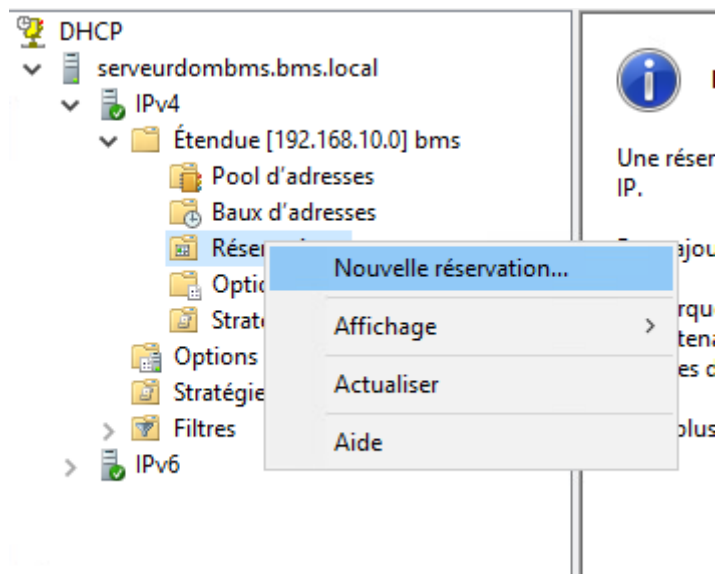
Cette imprimante est livrée avec une carte réseau configurée par défaut pour recevoir son adresse IP d'un serveur DHCP (cf figure 2 : impression auto-test avant installation sur le réseau).

Afin que cette imprimante reçoive toujours la même adresse IP fixe de la part du DHCP, il est possible de réserver une adresse IP fixe pour un client particulier sur le DHCP. La réservation se fait en fonction de l'adresse MAC du client (adresse physique de la carte réseau).

- a. Sur le serveur DHCP, effectuer une réservation d'adresse (dans l'arborescence de l'étendue *Etendue1*, clic droit sur le conteneur *Réservations* et sélection de la commande *Nouvelle réservation*) :

Nom de réservation : LaserJet 5200

Adresse MAC : 0060B06FB123



Description : *Imprimante HP LaserJet5N Administration*

Types pris en charge : *Les deux*

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 :

Types pris en charge

☒ Les deux

☐ DHCP

☐ BOOTP


Ajouter Fermer

- b. Cliquer sur *Ajouter* : la réservation d'adresse est terminée.

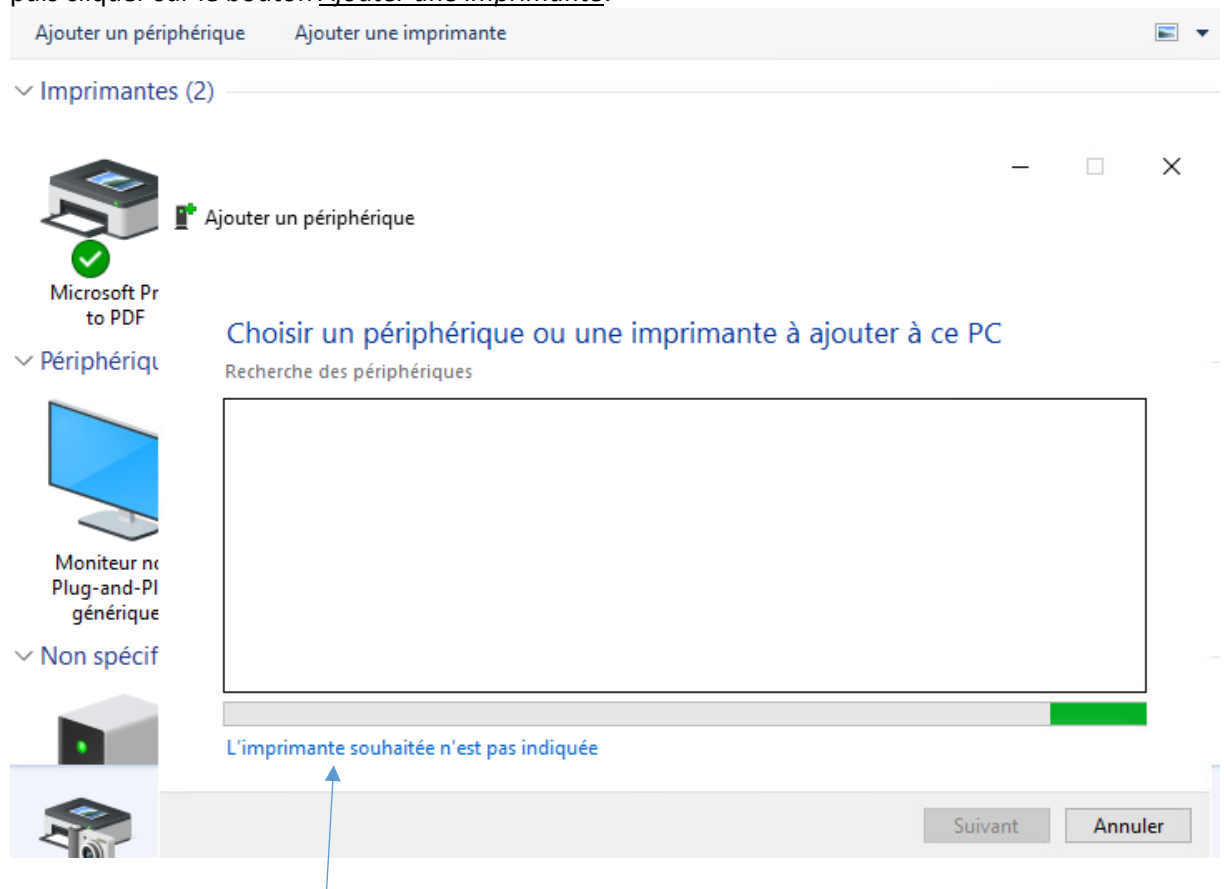
Étape 3 : installation de l'imprimante sur le réseau

Nous allons ensuite installer l'imprimante HP LaserJet5N sur le réseau, à partir du serveur SERVEUR1.

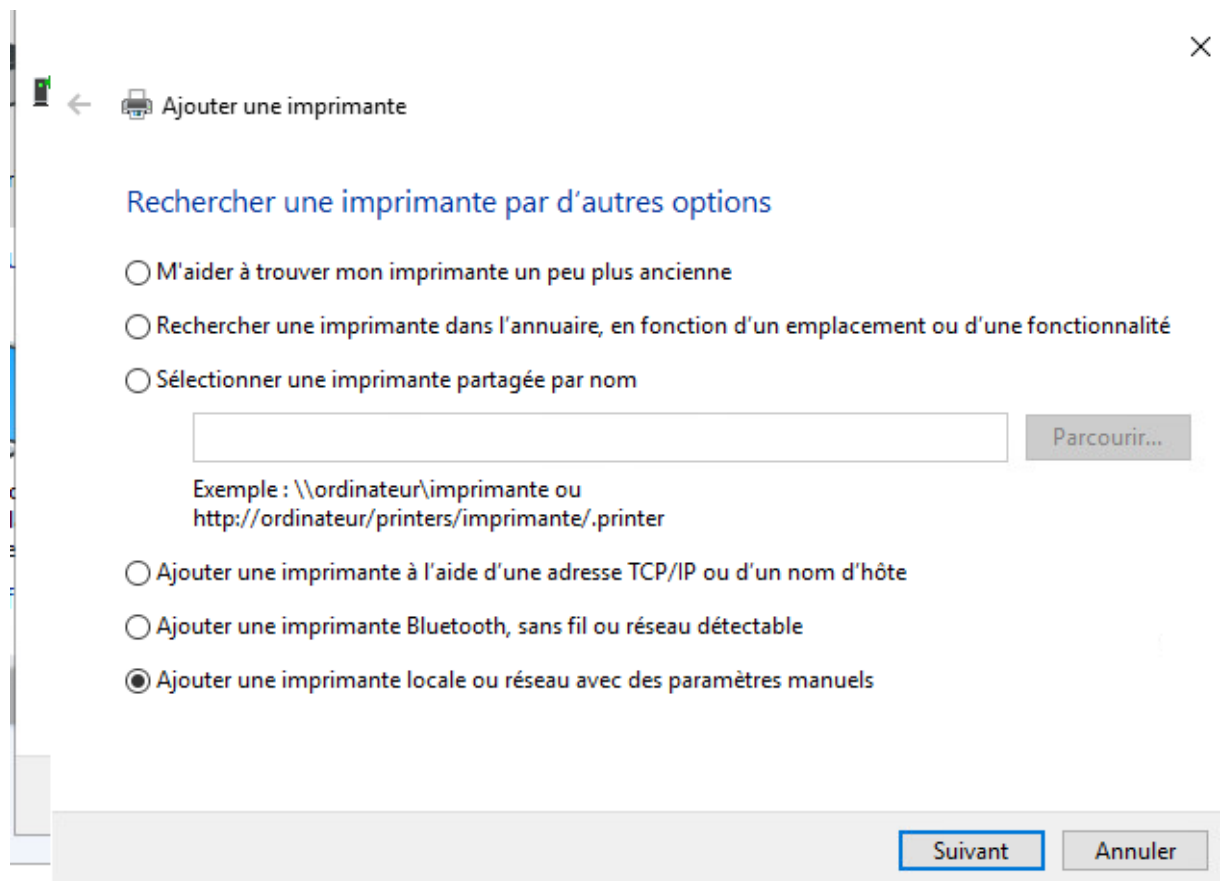
- a. Sélectionner Panneau de configuration  / Matériel, Périphériques et imprimantes

(ou Paramètres  / Périphériques / Imprimantes et scanners / Périphériques et imprimantes)

puis cliquer sur le bouton Ajouter une imprimante.

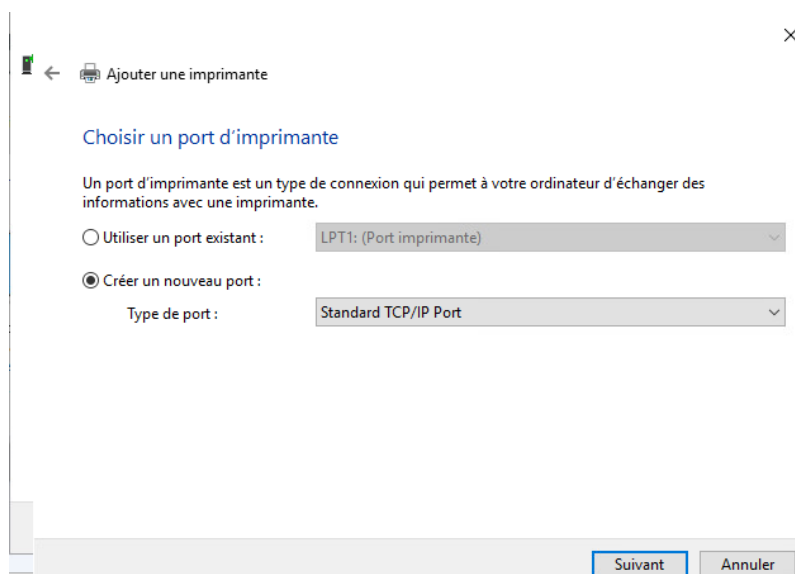


- b. Le serveur recherche alors l'imprimante ; comme il s'agit ici d'une imprimante "fictive", cliquer sur le lien *L'imprimante souhaitée n'est pas indiquée*.
- c. Dans la fenêtre de recherche d'imprimante, cocher la case *Ajouter une imprimante locale ou réseau avec des paramètres manuels*.



- d. Dans la fenêtre du choix du port, sélectionner *Créer un nouveau port* :

Type de port : *Standard TCP/IP Port*



- e. Dans la fenêtre suivante, configurer l'adresse IP et le nom de port suivants (l'imprimante doit être connectée au commutateur et sous tension à ce moment-là):

Adresse IP : 10.0.2.19

Nom du port : *HP LaserJet5N*

- f. Le serveur recherche alors l'imprimante ; comme il s'agit ici d'une imprimante "fictive", dans la fenêtre *Informations supplémentaires requises concernant le port*, effectuer le choix suivant :

Type de périphérique : *Standard (Generic Network Card)*

- g. Dans la fenêtre de choix du pilote de l'imprimante, sélectionner l'imprimante *HP LaserJet 5200 PCL6 Class Driver* de façon à sélectionner le pilote le plus connu PCL6.

- h. Donner le nom suivant à cette imprimante :

Nom de l'imprimante : ***HP LaserJet5N***
servira désormais à
réseau !)

(Bien noter ce nom car il
désignera l'imprimante sur le

- i. Cocher la case *Partager cette imprimante afin que d'autres personnes puissent l'utiliser* :


Nom du partage : *HP LaserJet5N*

L'imprimante est maintenant connectée au réseau, partagée, définie comme imprimante par défaut, et installée sur le serveur SERVEUR1.

Étape 4 : Configuration du serveur d'impression et de la console de Gestion de l'impression


Nous allons d'abord configurer le serveur *SERVEUR1* pour qu'il soit serveur d'impression.

Nous allons ajouter le rôle de serveur d'impression au serveur :

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

Nous allons maintenant utiliser la console de *Gestion de l'impression* (Printmanagement.msc) qui permet de gérer le serveur d'impression *SERVEUR1* (qui est désormais serveur d'impression local puisque nous avons installé ce rôle) mais aussi tous les autres serveurs d'impression éventuellement installés et connectés au réseau.

Cette console permettra également d'installer des connexions à des imprimantes sur un groupe d'ordinateurs clients de manière simultanée et de surveiller à distance les files d'attente d'impression, l'état des imprimantes et des serveurs d'impression connectés au réseau.

- c. Lancer la console de gestion de l'impression (avec Gestionnaire de serveur  / Outils / Gestion de l'impression).

Le serveur local SERVEUR1 doit apparaître dans la liste des serveurs d'impression gérés depuis cette console ; si ce n'est pas le cas, il faut l'y ajouter.

On doit maintenant retrouver l'imprimante HPLaserJet5N (que nous avons installée sur le réseau) dans le conteneur *Imprimantes* du serveur d'impression local SERVEUR1 :

Dans l'arborescence *Gestion de l'impression*, cliquer sur le conteneur *Imprimantes* du serveur d'impression local SERVEUR1, et vérifier que l'imprimante HPLaserJet5N est bien rattachée à ce serveur d'impression.

Remarque :

On pourrait aussi, selon les besoins, ajouter une autre imprimante au serveur d'impression (avec un clic droit sur le conteneur *Imprimantes* du serveur d'impression, puis sélection de la commande *Ajouter une imprimante*) ou faire migrer des imprimantes d'un serveur d'impression vers un autre (en exportant les imprimantes d'un serveur d'impression émetteur vers un fichier, puis en important les imprimantes d'un fichier vers un serveur d'impression destinataire).

Création d'un dossier personnel de base pour chaque utilisateur

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

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

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

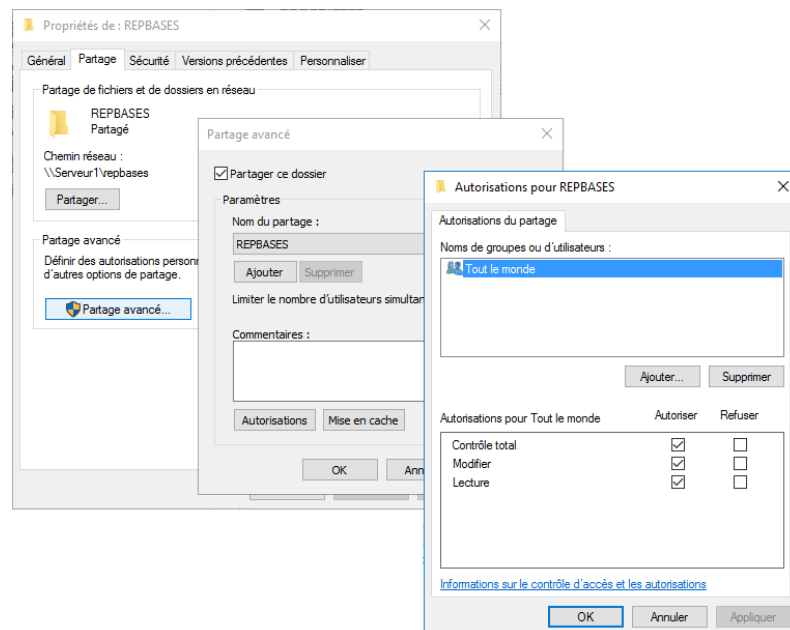
Cliquer sur le bouton *Partage avancé*

- c. Dans la fenêtre Partage avancé :
Cocher la case *Partager ce dossier*

Puis cliquer sur le bouton *Autorisation*

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

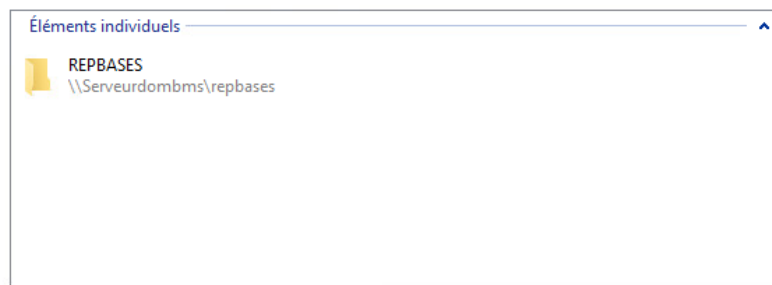
- e. Fermer la fenêtre des autorisations en cliquant sur *Appliquer* puis *OK*.



← Accès réseau

Votre dossier est partagé.

Vous pouvez [envoyer](#) à quelqu'un par courrier électronique ces liens vers des éléments partagés, ou [copier](#) et coller les liens dans une autre application.



[Afficher tous les partages réseau de cet ordinateur.](#)

Terminé

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

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

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

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

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

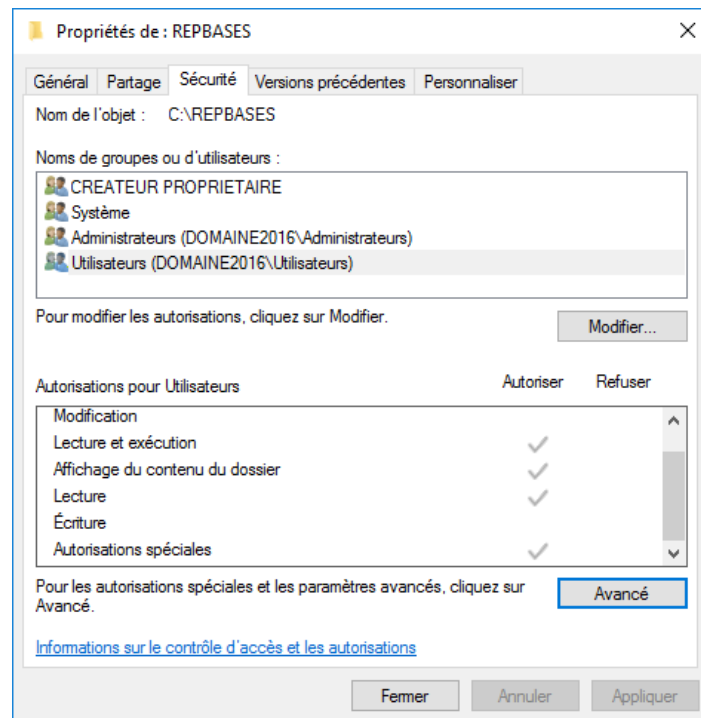
- *Lecture et exécution*
- *Affichage du contenu du dossier*
- *Lecture*
- *Création de fichiers et de dossiers (via les Autorisations spéciales).*

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

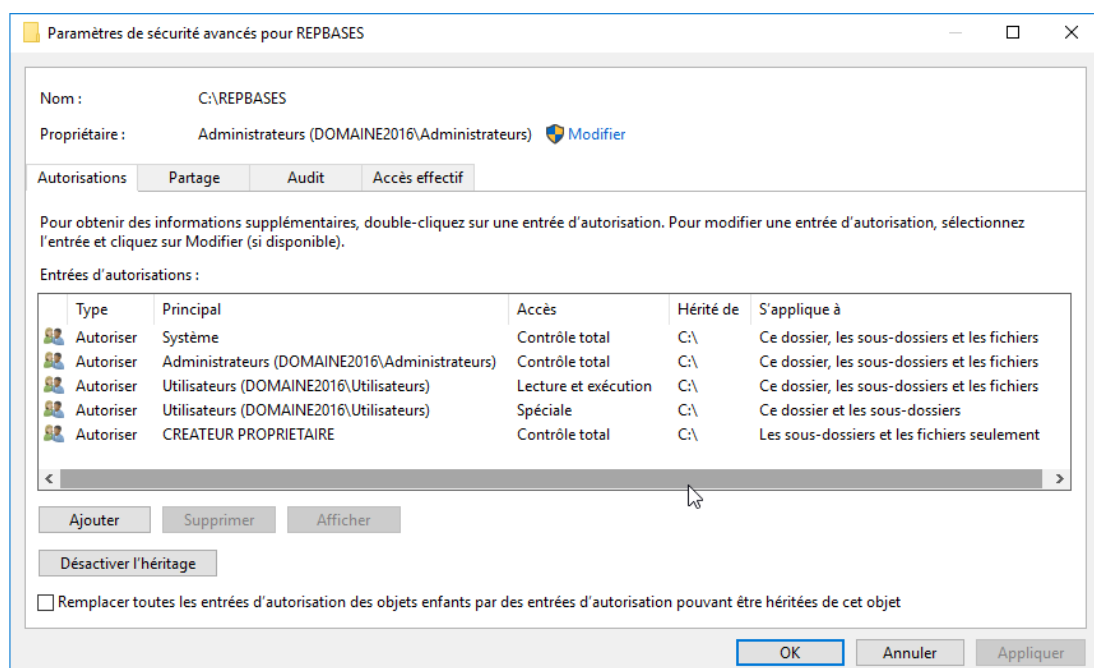
Or, on ne veut pas que chaque utilisateur puisse lire le contenu des dossiers personnels de base des autres utilisateurs !

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

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

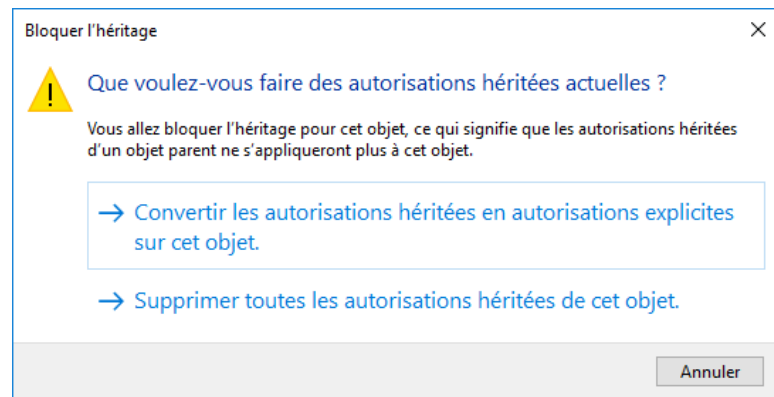


- h. Puis cliquer sur le bouton *Désactiver l'héritage* de la fenêtre *Paramètres de sécurité avancés* pour REPBASES :



- i. Dans le message de sécurité qui s'affiche lors du blocage de l'héritage, cliquer sur le lien

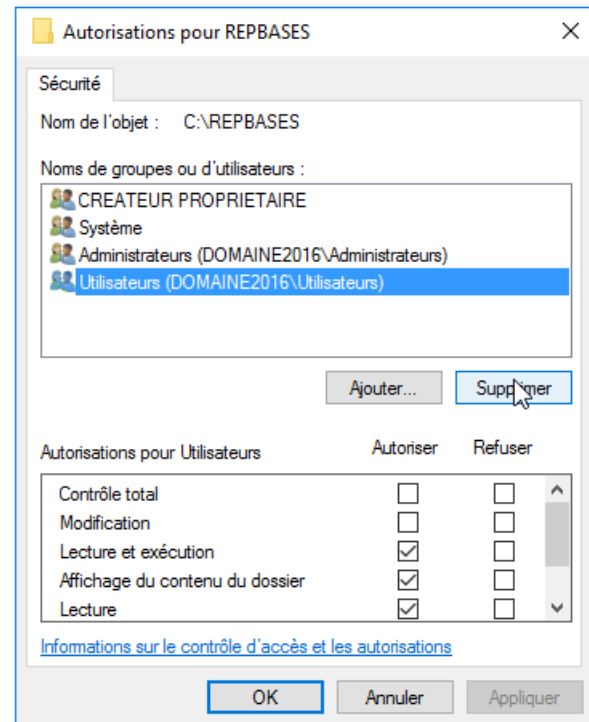
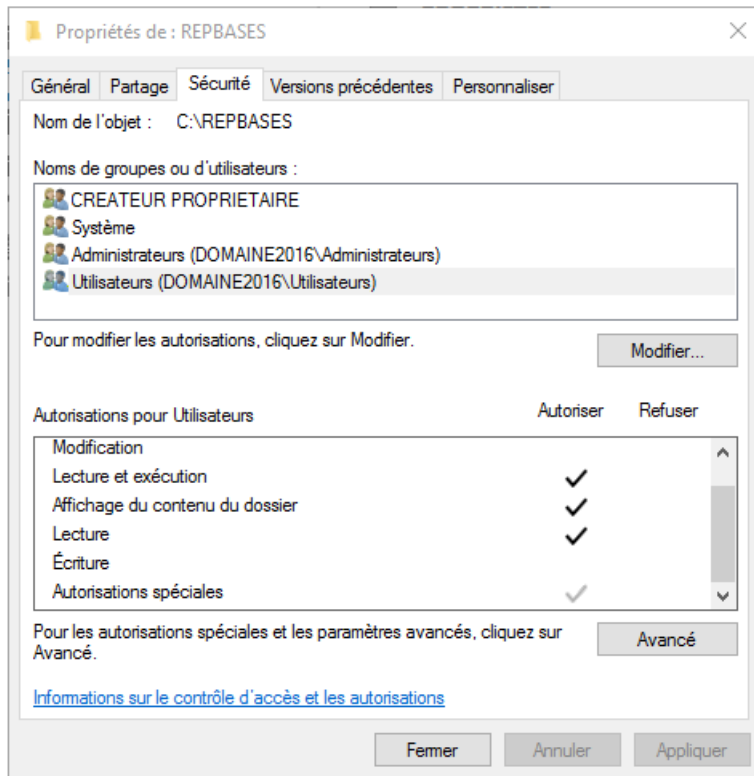
Convertir les autorisations héritées en autorisations explicites sur cet objet.



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

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

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




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

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

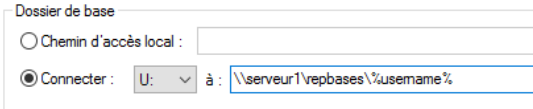
- l. Fermer les fenêtres ouvertes en cliquant sur *Appliquer* et/ou sur *OK*.

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

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

Connecter : U:

à \\SERVEUR1\REPBASES\%username%



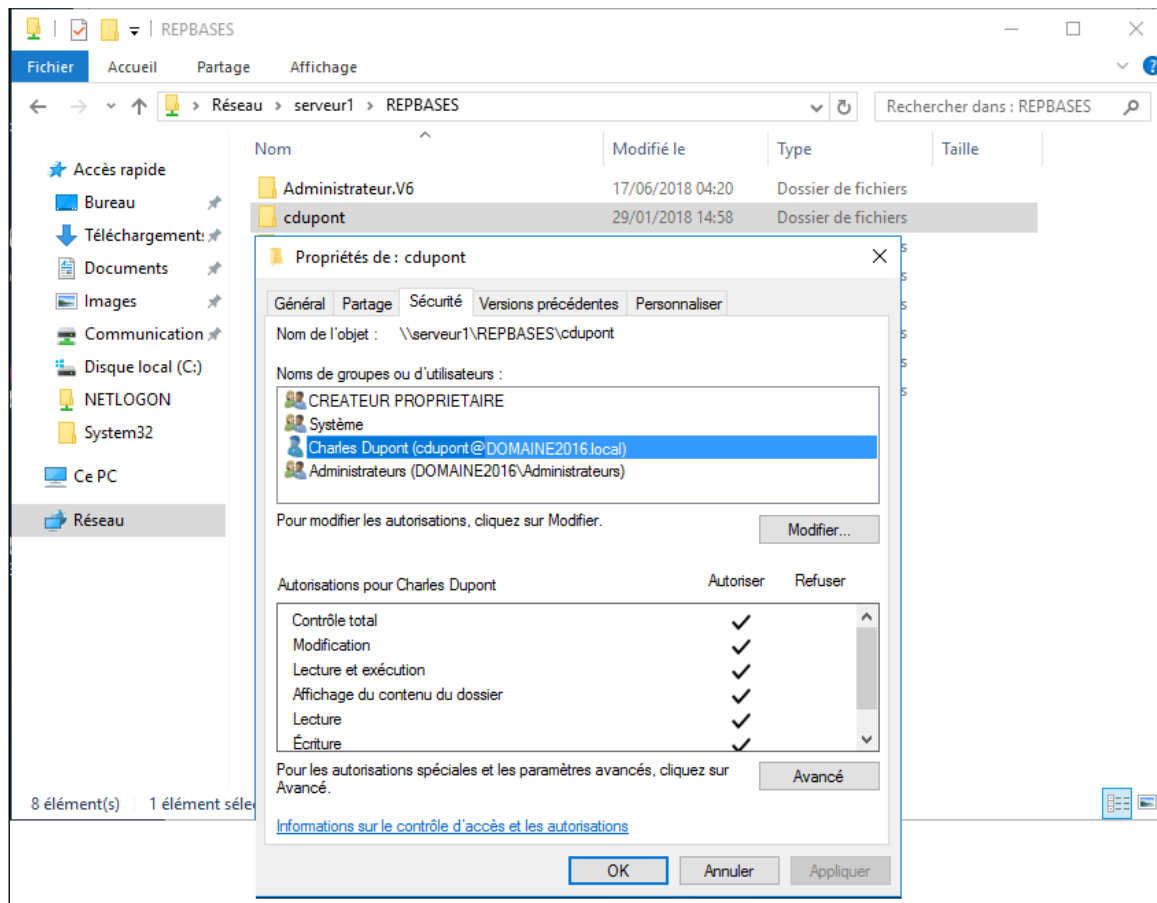
NB : la variable %username% contient le nom d'ouverture de session de l'utilisateur courant (ici : *cdupont*) ;

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

Le dossier pour cet utilisateur est alors automatiquement créé dans le dossier REPBASES !

Et l'autorisation *Contrôle total* est automatiquement attribuée à ce dossier pour cet utilisateur !

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



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

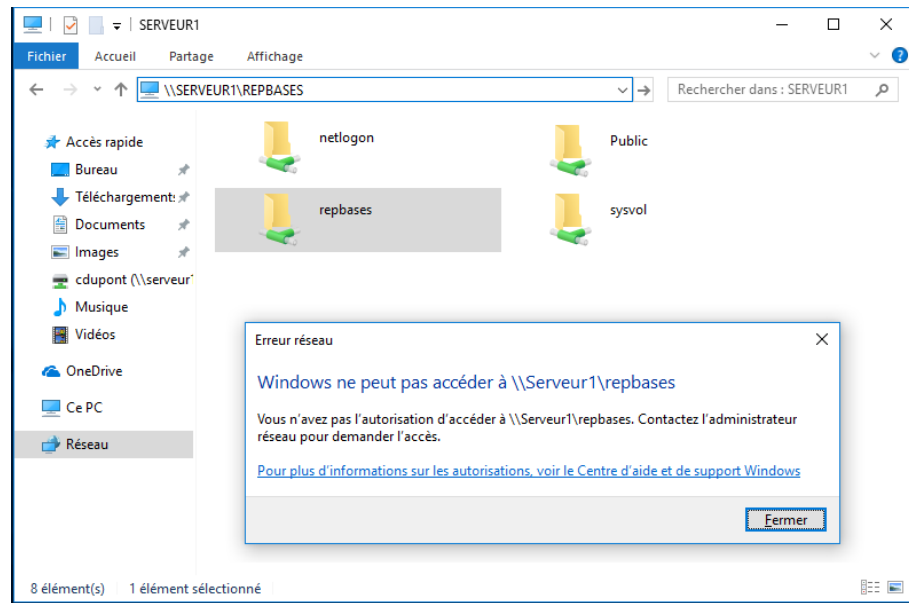
Attention : si une session est déjà ouverte pour un utilisateur (exemple pour Charles Dupont), le lecteur réseau U: ne va pas apparaître ; il faut fermer la session, puis en ouvrir une nouvelle.

En effet, les lecteurs-réseau sont toujours montés au démarrage d'une session.

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

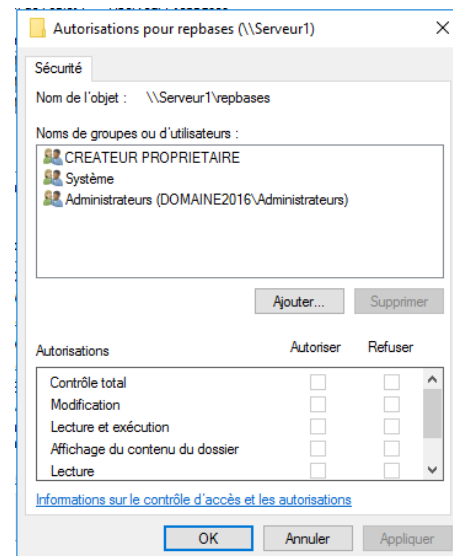
Attention : remarque importante !

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



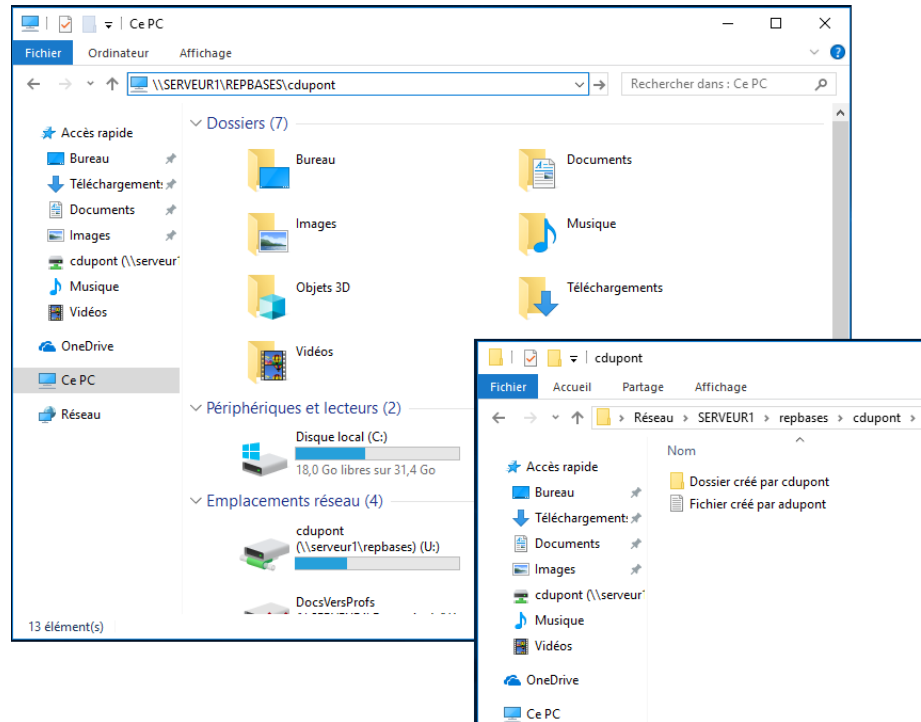
Ceci est normal, puisque Charles Dupont n'a aucune autorisation sur le dossier REPBASES.

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



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

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



Mission 5 : Supervision Nagios

Le but de cette mission est de réaliser la supervision des serveurs de BMS, ainsi que du Pfsense.

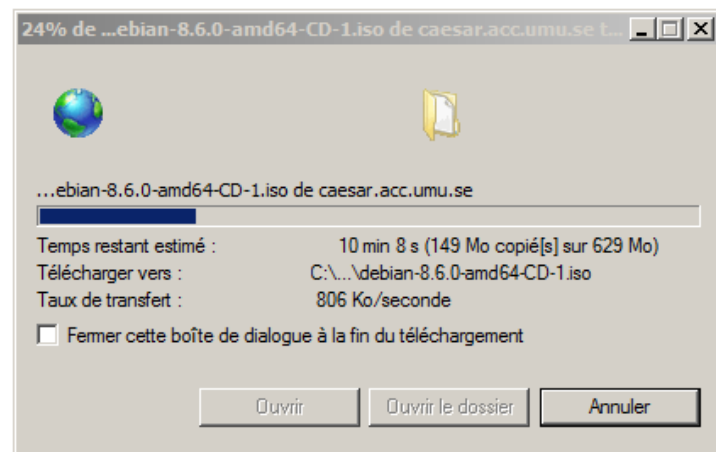
Travail à faire

- Installer Nagios sur un serveur Debian (**TP SISR de référence : [TP1 SISR5 - Installation de Nagios 4](#)**) ;
- Configurer la supervision des éléments du réseau dans le fichier *monReseau.cfg*
- Déclarer tous les postes de ce projet et superviser l'affichage de la description du système, ainsi que le taux d'occupation du disque dur de chacun.

On pourra aussi superviser en temps réel la bande passante (mesure du débit instantané du trafic réseau) des principales interfaces du routeur Pfsense pour surveiller tout trafic excessif sur ces interfaces, en utilisant le plugin `check_snmp_netint.pl`

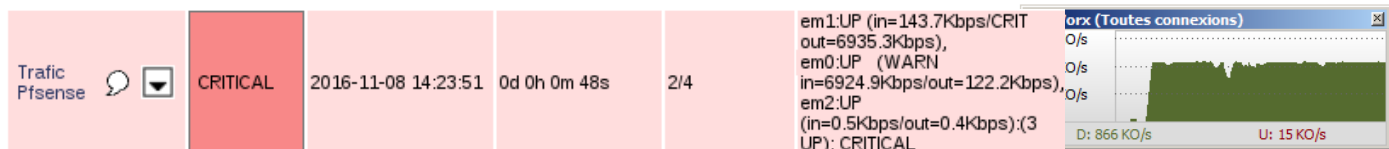
Exemple : lors du téléchargement d'un fichier depuis Internet sur un serveur du LAN :

- vitesse de téléchargement : 850 KO/s
- soit : 6800 Kbits/s



Ce téléchargement s'observe en mesurant en temps réel le débit du trafic réseau sur les interfaces suivantes :

- en entrée (IN) sur l'interface externe Pfsense `em0`
- en sortie (OUT) sur l'interface interne Pfsense `em1`



Création d'une machine debian à partir de se model



Puis la connecter au domaine en effectuant ces manipulations

Installation nagios

Tout d'abord modifier les paramètres dans nano /etc/network/interfaces comme ceci :

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

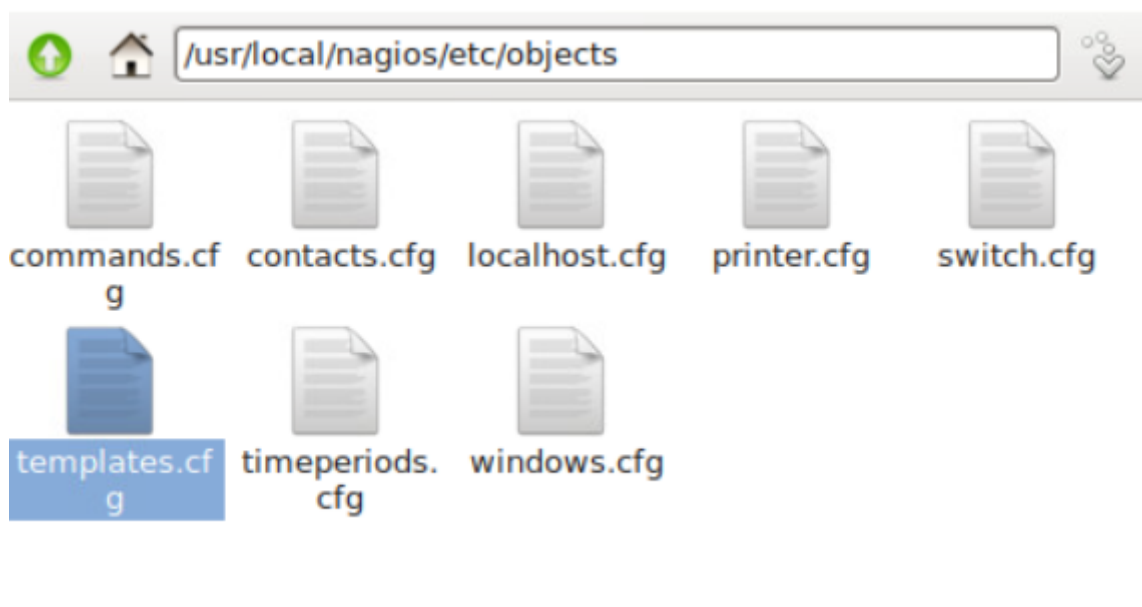
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens192
iface ens192 inet static
address 192.168.10.3/24
gateway 192.168.10.254
```

Puis lancer le programme

```
root@NagiosBMS:~# ./InstallNagios4v2.sh
```

Après avoir rentrer vos mots de passe lancer l'explorateur de fichier entrez
« /usr/local/nagios/etc/objects » puis ouvrir le fichier « templates.cfg



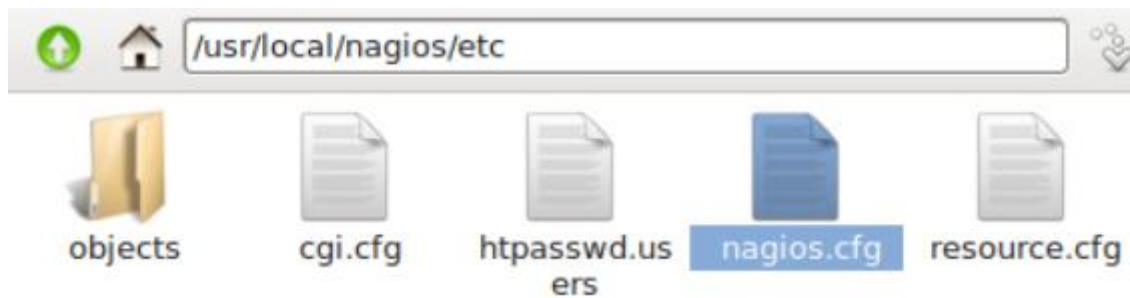
Ajouter ces lignes dans le dossiers .cfg

```
50
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 minutes
57     retry_interval        1                ; Schedule host check retries at 1 minute
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 program restarts
62     retain_nonstatus_information 1          ; Retain non-status information across program restarts
63     notification_period    24x7            ; Send host notifications at any time
64     register               0                ; DONT REGISTER THIS DEFINITION - ITS NOT A STANDARD HOST
65 }
66
```

Puis modifier ces paramètres après ça sauvegarder et quittez le fichier

```
154
155 define service{
156     name                generic-service      ; The 'name' of this service template
157     active_checks_enabled 1                ; Active service checks are enabled
158     passive_checks_enabled 1                ; Passive service checks are enabled
159     parallelize_check    1                ; Active service checks should be parallelized
160     obsess_over_service  1                ; We should obsess over this service (if possible)
161     check_freshness       0                ; Default is to NOT check service freshness
162     notifications_enabled 1                ; Service notifications are enabled
163     event_handler_enabled 1                ; Service event handler is enabled
164     flap_detection_enabled 1                ; Flap detection is enabled
165     process_perf_data      1                ; Process performance data
166     retain_status_information 1            ; Retain status information across program restarts
167     retain_nonstatus_information 1          ; Retain non-status information across program restarts
168     is_volatile           0                ; The service is not volatile
169     check_period          24x7            ; The service can be checked at any time
170     max_check_attempts    3                ; Re-check the service up to 3 times
171     check_interval        2                ; Check the service every 2 minutes
172     retry_interval        1                ; Re-check the service every minute
173     contact_groups         admins          ; Notifications get sent out to 'admins'
174     notification_options    w,u,c,r        ; Send notifications about warnings, unknown, critical and recovery
175     notification_interval   60              ; Re-notify about service problems every 60 seconds
176     notification_period    24x7            ; Notifications can be sent out at any time
177     register               0                ; DONT REGISTER THIS DEFINITION - ITS NOT A STANDARD SERVICE
178 }
179
```

En suite aller dans /usr/local/nagios/etc et ouvrir « nagios.cfg »



A l'intérieur ajouter y cette ligne

```
<nagios.cfg>
Fichier  Édition  Rechercher  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
```

Créer le fichier **monReseau.cfg** qui sera stocké dans le dossier **/usr/local/nagios/etc/objects/** avec la commande

ajouter les lignes nécessaires pour superviser les éléments souhaités :

```
1 define host {
2     use                generic-host
3     host_name          SERVEUR1
4     alias              PDC Windows 2016 SERVEUR1
5     address            192.168.10.3
6 }
```

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

```
systemctl restart nagios
```

Le résultat est immédiatement visible dans l'interface graphique de Nagios :

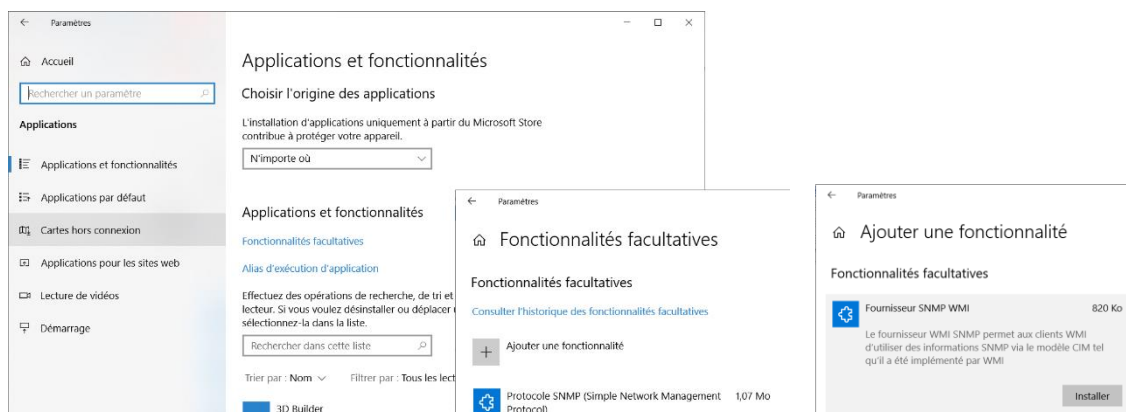


Effectué ces manipulations pour le reste du réseau

Installer l'agent SNMP sur toutes les machines du réseau



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 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)

Propriétés de Service SNMP (Ordinateur local)

Général Connexion Sécurité Récupération Agent

Interruptions

☒ Envoyer une interruption d'authentification

Noms de communautés acceptés

Communauté	Droits
private	LECTURE ECRITURE
public	LECTURE SEULE

Ajouter... Modifier... Supprimer

☒ Accepter les paquets SNMP provenant de n'importe quel hôte

☐ Accepter les paquets SNMP provenant de ces hôtes

Ajouter... Modifier... Supprimer

OK Annuler Appliquer

Propriétés de Service SNMP (Ordinateur local)

Interruptions Sécurité Dépendances

Général Connexion Récupération Agent

Les systèmes de gestion d'Internet peuvent demander au service SNMP d'indiquer la personne contact, l'emplacement du système et les services de réseau pour cet ordinateur.

Contact:

Emplacement:

Service

☒ Physique ☒ Applications ☒ Liaison de données et sous-réseau

☒ Internet ☒ Bout en bout

OK Annuler Appliquer

Mission 5 : Installation du serveur de Bases de Données *ServeurBDBMS*, du serveur Web *ServeurWebDMZ*, et de l'application de gestion des frais

Le but de cette mission est d'installer les machines, et l'application de gestion des frais BMS en mode client-serveur :

- le site Web sera installé sur le serveur Web DMZ ; on utilisera IIS pour le serveur Web.
- la base de données sera installée sur le serveur de Bases de Données du réseau local ; on utilisera Mysql pour le SGBD.

Travail à faire

Mission 5 A : installation et configuration du serveur de Bases de Données

- Installer le serveur *ServeurBDBMS* Windows 2019. Cette machine doit être connectée au domaine BMS.local (*ServeurBDBMS* sera donc un serveur membre du domaine BMS mais il ne sera pas contrôleur de domaine).
- Installer le serveur de Bases de données Mysql.
- Créer la base de données *BMS_frais*, puis créer les tables et leurs enregistrements à l'aide des scripts de création fournis.

Exemples de 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 5 B : installation et configuration du serveur Web DMZ

- Installer le serveur *ServeurWebDMZ* Windows 2019. Cette machine ne doit pas être connectée au domaine BMS.local.
- installer le rôle *Serveur Web IIS* avec le service de rôle *CGI* ;
- installer PHP;
- installer les pages du site *bmsMVC* (copier le dossier fourni *bmsMVC* dans *wwwroot*).

Ce site Web installé sur le serveur Web DMZ devra utiliser la base de données *BMS_frais* installée sur le serveur de Bases de Données. En conséquence, il est nécessaire de modifier le script PHP de connexion au serveur Mysql et à la base de données :

- | | |
|--|--------------------------------|
| ➤ adresse IP du serveur Mysql : | 192.168.10.2 |
| ➤ nom de la base de données : | <i>BMS_frais</i> |
| ➤ identifiant et mot de passe de l'utilisateur : | <i>utilisateurweb / secret</i> |

RAPPEL :



Pour que le site Web *bmsMVC* fonctionne correctement, il est indispensable d'installer et de configurer auparavant le routeur-pare-feu Pfsense, afin que le serveur Web ait accès au serveur de bases de données. N'oubliez pas d'installer l'extension

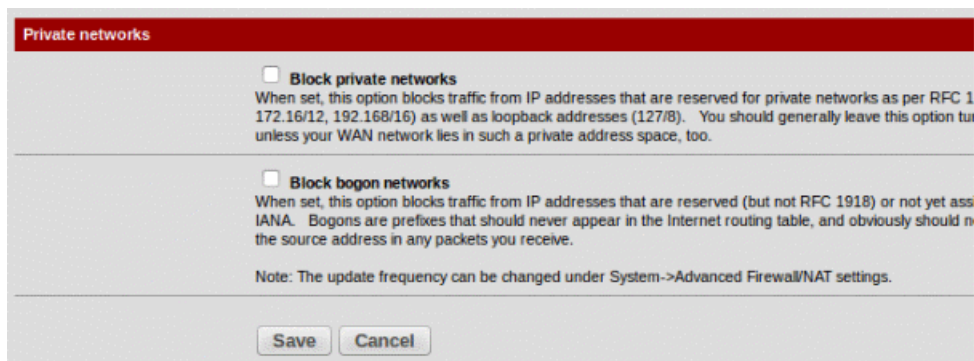
Mission 6 : Configuration des règles de filtrage du routeur-pare-feu Pfsense

Travail à faire

Configurer le Pfsense et implanter les règles de filtrage nécessaires pour protéger au maximum le réseau local, et protéger au mieux la DMZ.

Rappel : le serveur Web de la DMZ ne dispose pas d'adresse IP publique. On devra néanmoins pouvoir accéder à ce serveur à partir d'un poste de la salle R211.

Indication : penser à rendre accessible le Pfsense depuis un poste ayant une adresse IP privée (par exemple un poste de la salle R211) en décochant la case *Block private networks* de l'interface WAN :



Private networks

☐ **Block private networks**
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 172.16/12, 192.168/16 as well as loopback addresses (127/8). You should generally leave this option turned on unless your WAN network lies in such a private address space, too.

☐ **Block bogon networks**
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not be the source address in any packets you receive.

Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.

Save Cancel

Mission 6 A : Règles minimum à configurer sur l'interface DMZ du Pfsense

- a. le serveur Web DMZ peut interroger le serveur de BD sur le port 3306 ;
- b. le serveur Web DMZ ne peut émettre aucun autre trafic vers le LAN ;
- c. le serveur Web DMZ peut accéder à Internet (HTTP, HTTPS, FTP, messagerie électronique, ...).

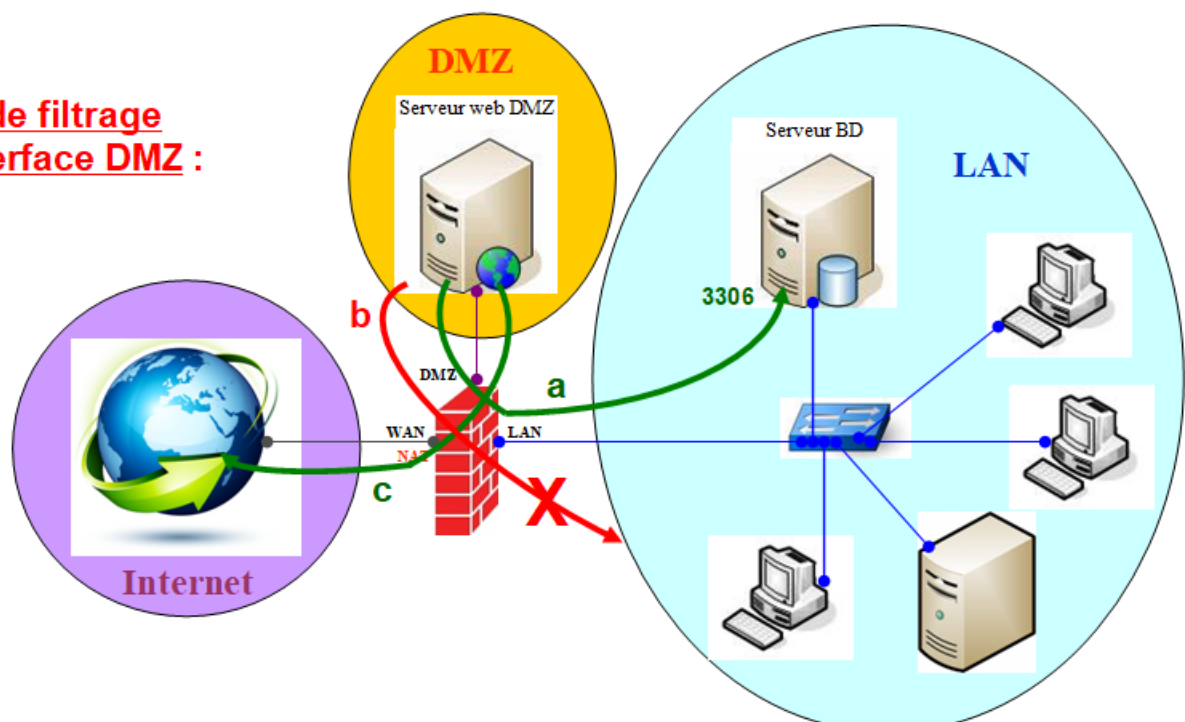


Pour la règle b, attention à bien résumer l'adresse du LAN (incluant tous les VLAN) sous peine de bloquer l'accès de tout le réseau à Internet !

Interface DMZ

N°	Interface	Sens	Protocole couche 3 ou 4	IP source	Port source	IP destination	Port destinat	Etat si TCP	Action
a	DMZ	E							
b	DMZ	E							
c	DMZ	E							
Def	DMZ	E	Tous (IP)	Toutes	Tous	Toutes	Tous		R

**Règles de filtrage
sur l'interface DMZ :**



a : Autoriser les nouvelles connexions entrantes de certains serveurs de la DMZ (exemple : serveur web) vers certains serveurs du LAN (ex : serveur BD) sur des ports nécessaires (par exemple, ports utilisés par MySQL, SQL Server...).

b : Interdire toute autre connexion entrante de la DMZ vers le LAN.

c : Autoriser si besoin les connexions entrantes des serveurs de la DMZ vers Internet.

Remarque : toute réponse venant de la DMZ et correspondant à une demande faite par un poste Internet ou du LAN est autorisée à entrer sur cette interface DMZ.

Remarque : on peut aussi rajouter une règle de filtrage qui permet au serveur Web DMZ de ping le serveur de BD.

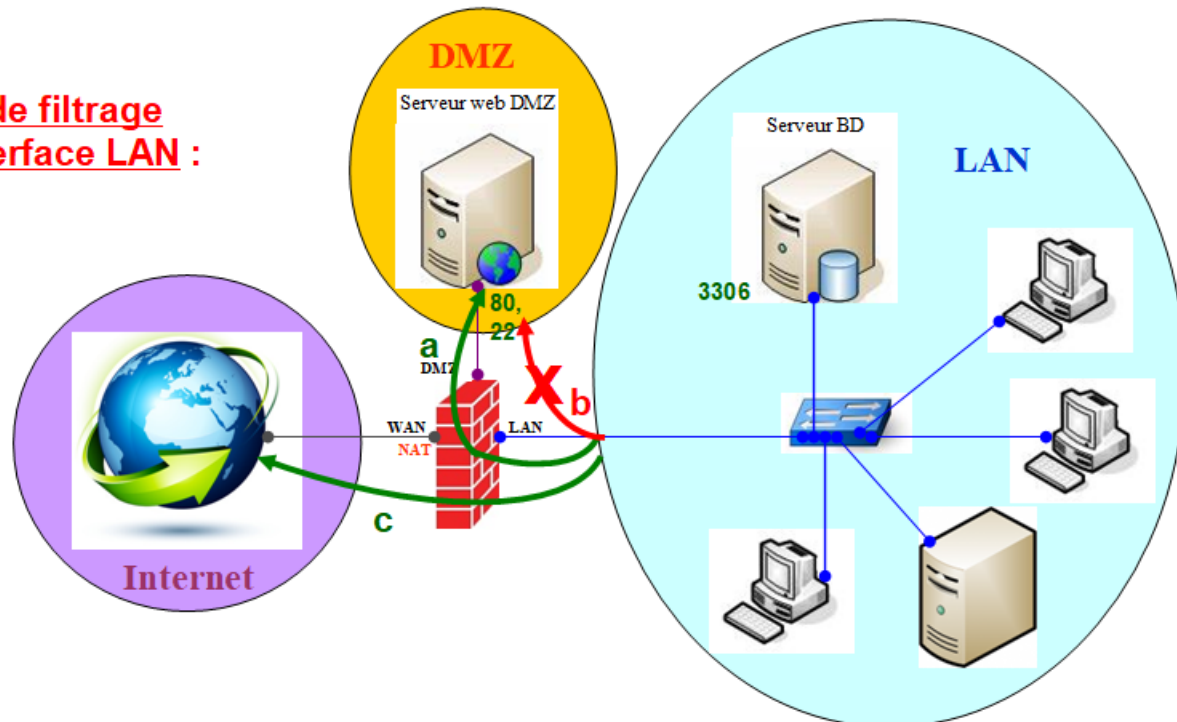
Mission 6 B : Règles minimum à configurer sur l'interface LAN du Pfsense

- a. le LAN peut interroger le serveur Web DMZ sur le port 80 ;
- b. le LAN ne peut émettre aucun autre trafic vers le serveur Web DMZ ;
- c. le LAN peut accéder à Internet (HTTP, HTTPS, FTP, messagerie électronique, ...).

Interface LAN

N°	Interface	Sens	Protocole couche 3 ou 4	IP source	Port source	IP destination	Port destinat	Etat si TCP	Action
a	LAN	E							
b	LAN	E							
c	LAN	E							
Def	LAN	E	Tous (IP)	Toutes	Tous	Toutes	Tous		R

**Règles de filtrage
sur l'interface LAN :**



a : Autoriser les nouvelles connexions entrantes du LAN vers les serveurs de la DMZ sur des ports prédéfinis pour utiliser normalement ces serveurs (par exemple, STMP, FTP, POP, HTTP...), ou seulement pour les mettre à jour (SSH, FTP, ...) depuis certains postes autorisés.

b : Interdire toute autre connexion entrante du LAN vers la DMZ.

c : Autoriser toute connexion entrante du LAN vers Internet.

Remarque : toute réponse venant du LAN (du serveur BD) et correspondant à une demande faite par un serveur de la DMZ est autorisée à entrer sur cette interface LAN.

Remarque : on peut aussi rajouter une règle de filtrage qui permet à toute machine du LAN de pinger le serveur Web DMZ.

Mission 6 C : Règles minimum à configurer sur l'interface WAN du Pfsense

- a. Internet peut interroger le serveur Web DMZ sur le port 80 ;
- b. Internet ne peut émettre aucune autre connexion entrante vers le LAN ou la DMZ.

Interface WAN (règles de redirection de port)

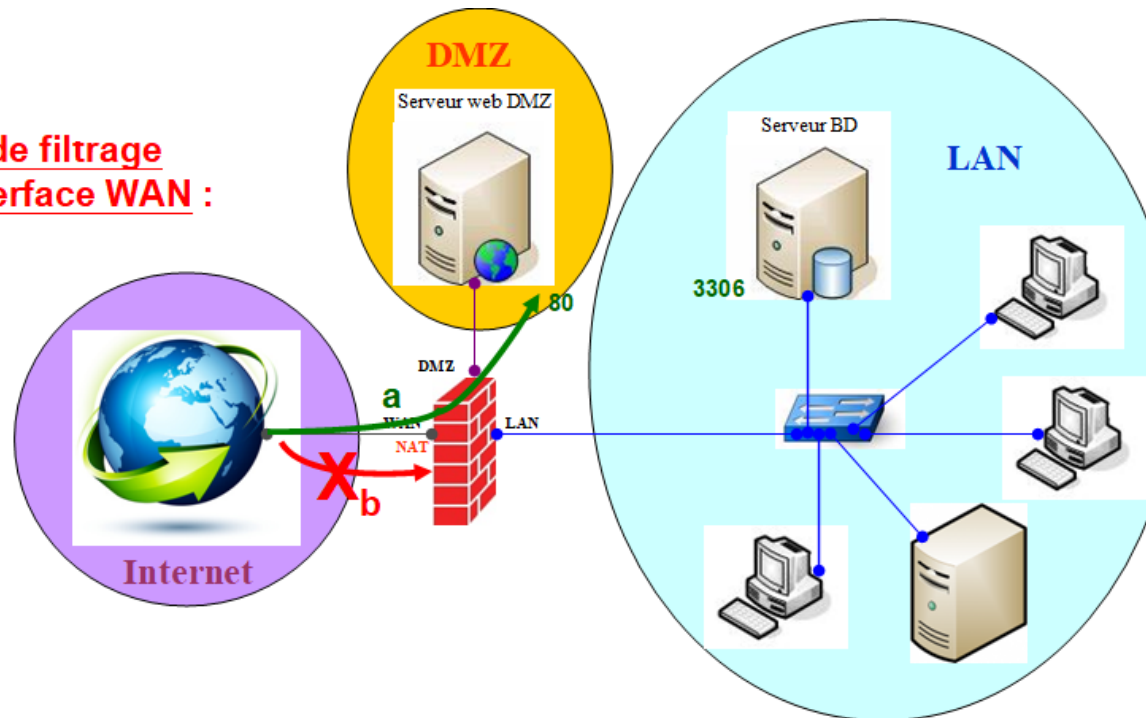
Interface d'arrivée - Adresse publique	Port public	Adresse privée	Port privé

La règle de filtrage a est créée automatiquement lorsqu'on crée la redirection de port !

Interface WAN

N°	Interface	Sens	Protocole couche 3 ou 4	IP source	Port source	IP destination	Port destinat	Etat si TCP	Action
a	WAN	E							
b	WAN	E	Tous (IP)	Toutes	Tous	Toutes	Tous		R

**Règles de filtrage
sur l'interface WAN :**



a : Autoriser les nouvelles connexions entrantes d'Internet vers les serveurs de la DMZ sur les ports nécessaires (HTTP, SMTP, FTP, POP, ...).

b : Interdire toute autre connexion entrante d'Internet vers la DMZ ou le LAN.

Remarque : toute réponse venant d'Internet et correspondant à une demande faite par un poste du LAN ou de la DMZ est autorisée à entrer sur cette interface WAN (connexion déjà existante et établie par ce poste).

Si l'adressage IP de la DMZ est privé :

→ NAT dynamique/PAT

→ NAT statique avec redirection de port