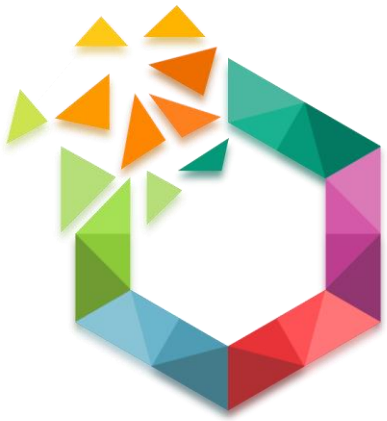
WINDOWS SERVER

DOCUMENTATION TECHNIQUE



YAM

VOTRE PARTENAIRE INFORMATIQUE

GMSI 2019-2021

LE CALVÉ YANNICK

LEFEUVRE ALEX

LE FRANC MORGANE

TABLE DES MATIÈRES

1- INSTALLATION WINDOWS SERVER

1-1- INSTALLATION

Nous installons donc notre serveur physique, sur lequel se retrouveront plusieurs machines virtuelles (VM).

Nous aurons donc, lié à notre serveur physique Windows Server 2019, plusieurs machines virtuelles Windows Server dont des hôtes RDS (pour l'environnement utilisateur) et une machine virtuelle Linux (pour les 2 postes du SAV).

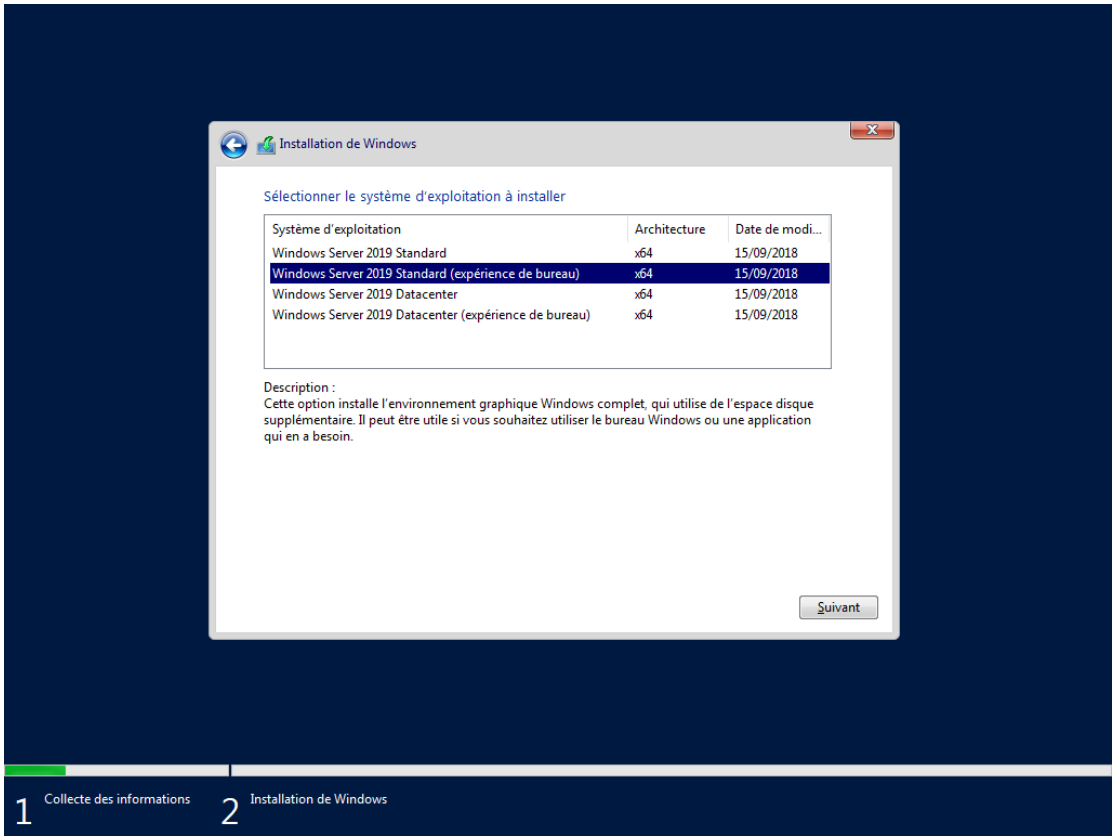
ÉTAPES PAS-À-PAS

Nous commençons donc l'installation de Windows Server.

La première étape concerne le choix de la langue. Nous sélectionnons **Français** en tant que langue, ainsi que pour l'horaire et le clavier. Nous passons ensuite à l'installation en cliquant tout simplement sur **Installer maintenant**.

Entrer la **clé de produit (Product Key)** fournie. Si nous ne la possédons pas encore, il nous faut cliquer sur **Je n'ai pas de clé de produit**.

Sélectionner **Windows Server 2019 Standard (expérience de bureau)** comme système d'exploitation à installer. Le choix de la version **expérience de bureau** nous permet de l'installer en mode graphique avec tous les outils de gestion.

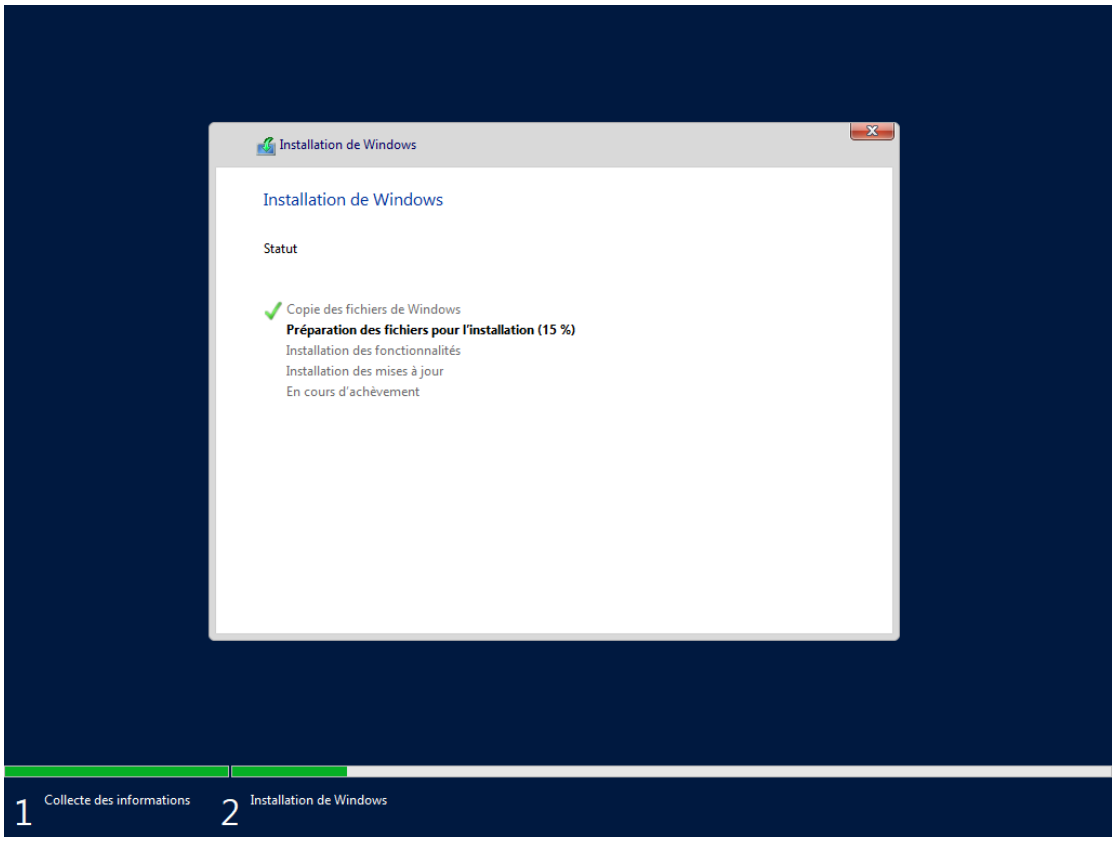


YAM
VOTRE PARTENAIRE INFORMATIQUE

Cocher la case **J'accepte les termes du contrat de licence** et cliquer sur **Suivant** puis choisir une installation **Personnalisée.**

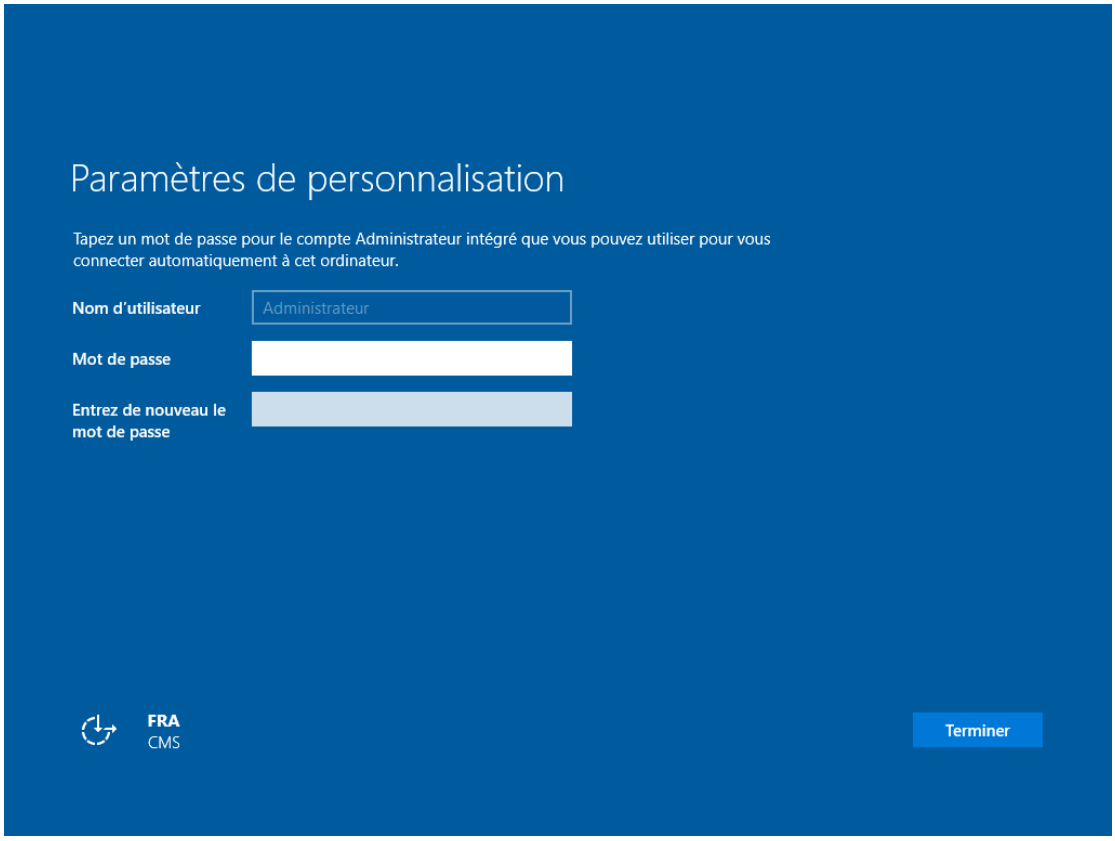
Nous sélectionnons le disque sur lequel s'installera Windows Server, puis cliquer sur **Suivant.**

L'installation se lance.



1-2- CONFIGURATION ET PRÉPARATION DU SERVEUR

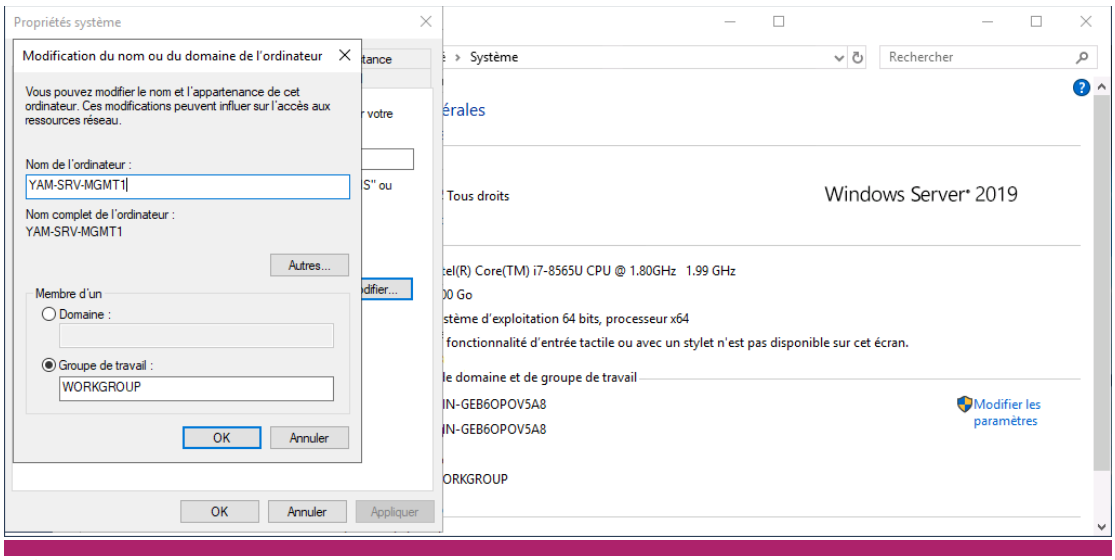
Nous pouvons désormais utiliser notre Windows Server 2019. Une fois le serveur installé, nous devons commencer par définir un mot de passe pour le compte Administrateur.



Afin de déverrouiller la session nous appuyons sur **Ctrl + Alt + Suppr**, puis nous entrons le mot de passe Administrateur que nous avons défini précédemment.

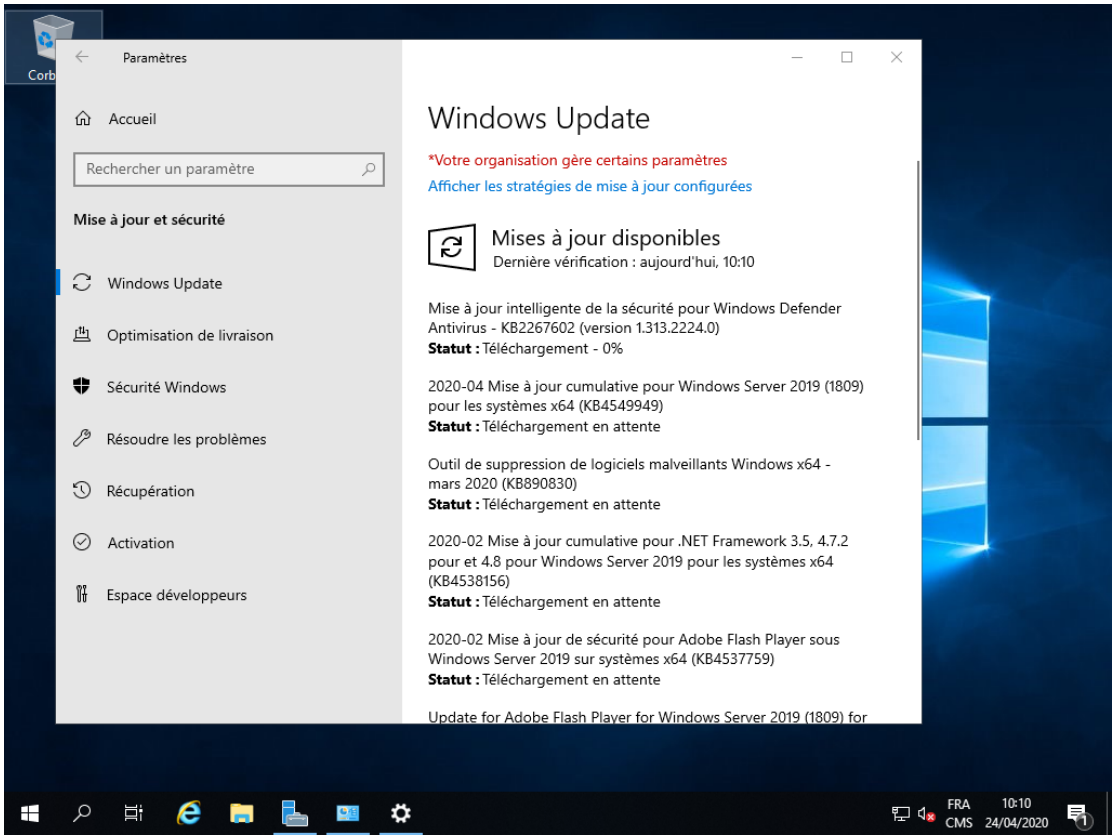
NOMMAGE DU SYSTÈME

L'étape suivante consiste à renommer notre serveur. Nous le nommerons selon le(s) rôle(s) attribué(s), en respectant la nomenclature établie. Pour ce faire nous allons dans les paramètres du système.



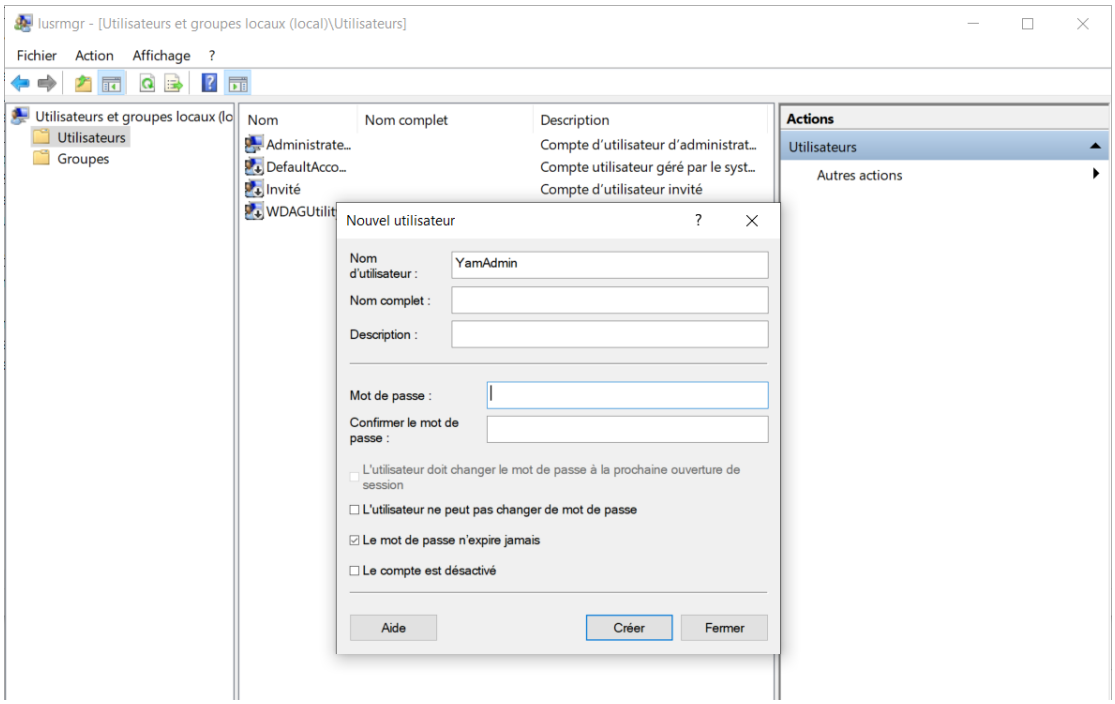
YAM
VOTRE PARTENAIRE INFORMATIQUE

Par la suite nous effectuons les mises à jour ainsi que l'installation des pilotes. Pour accéder à ces mises à jour nous allons dans les **Paramètres > Mise à jour et sécurité > Windows Update.**



CRÉATION DE L'ADMINISTRATEUR LOCAL

Nous devons ensuite créer un compte Administrateur local nommé **YamAdmin** et désactiver le compte **Administrateur.** Cette étape est obligatoire pour des raisons de sécurité. Pour accéder à ces paramètres nous ouvrons l'Invite de commandes et tapons **lusrmgr.msc.**

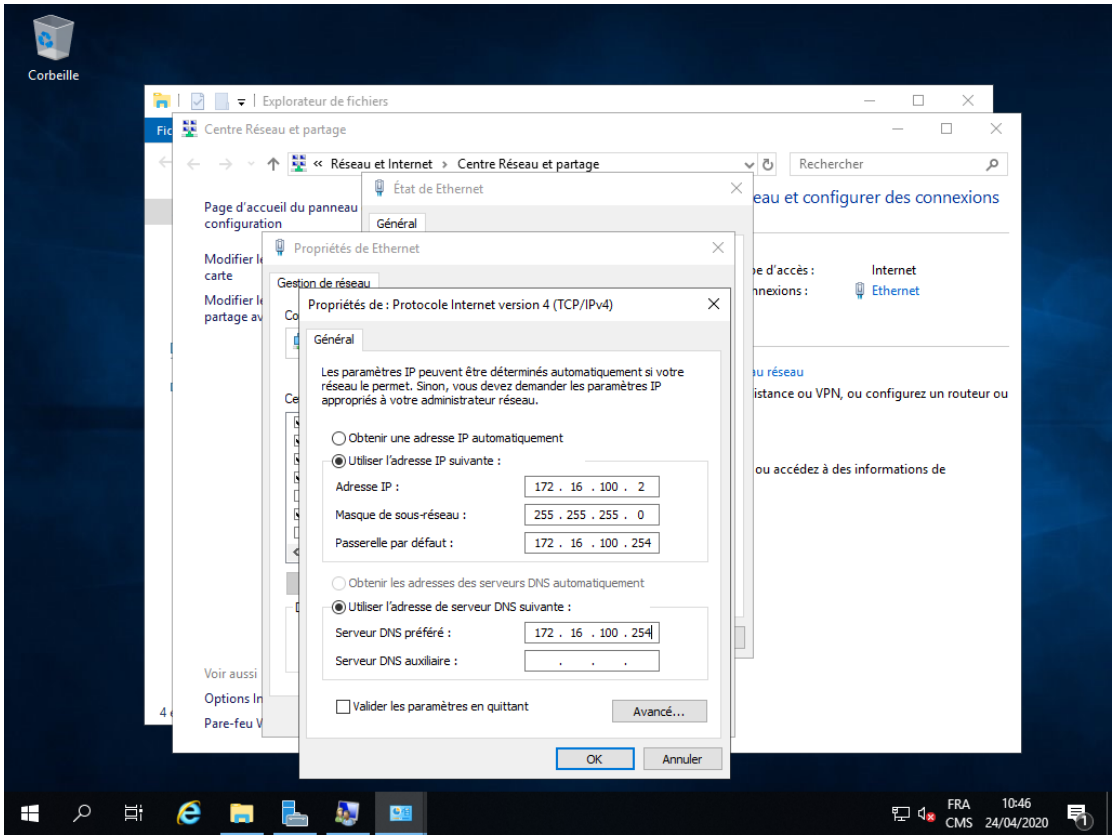


YAM
VOTRE PARTENAIRE INFORMATIQUE

Pour terminer cette configuration du serveur, nous devons désactiver l'IPv6 et attribuer une IP fixe IPv4.

FIXER L'ADRESSE IP

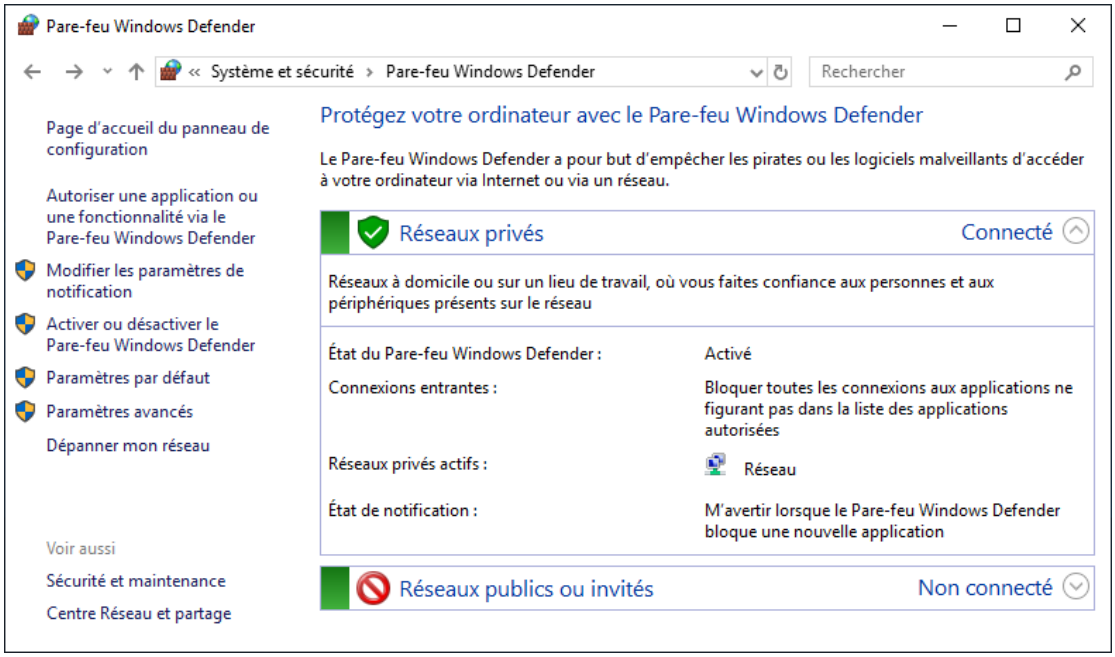
Pour accéder à ces paramètres nous allons dans **Réseau et Internet** puis dans **Centre Réseau et partage.** Nous allons ensuite dans les **Propriétés de Ethernet** et accédons aux modifications qui nous permettent de définir notre adresse IPv4.



1-3- PARE-FEU

CONFIGURATION

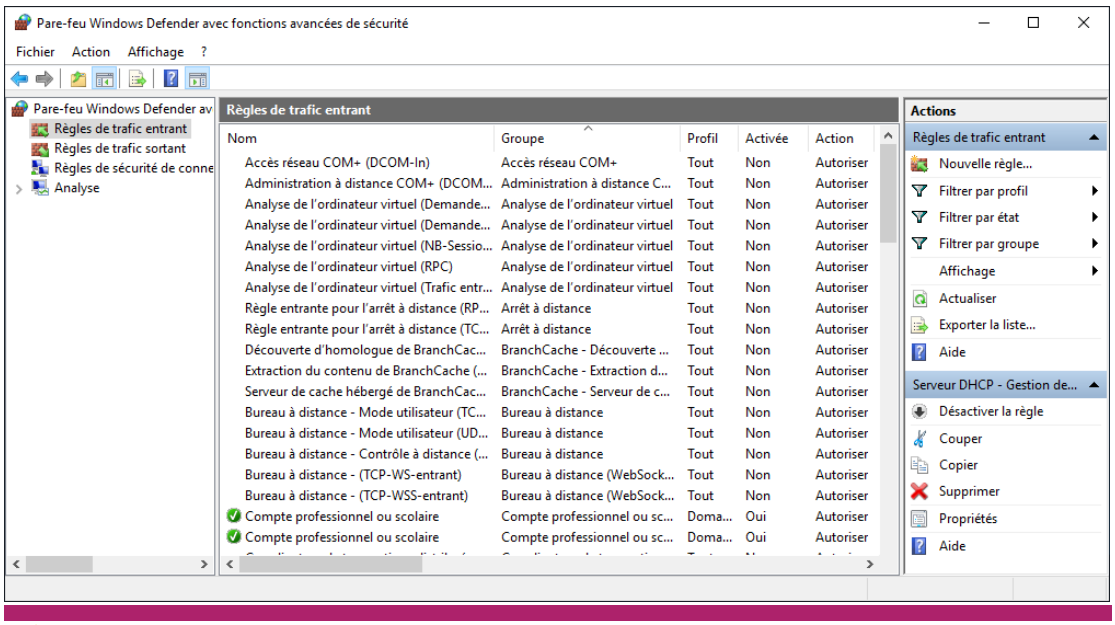
Afin d'éviter des problèmes de sécurité, nous devons bloquer les connexions entrantes du pare-feu sur réseau privé et public. Nous allons donc dans le **Panneau de configuration > Système et sécurité** puis dans **Pare-feu Windows Defender.**



Nous bloquons toutes les connexions entrantes des réseaux privés et des réseaux publics. Cliquer sur **Modifier les paramètres de notification** et cocher partout les options suivantes :

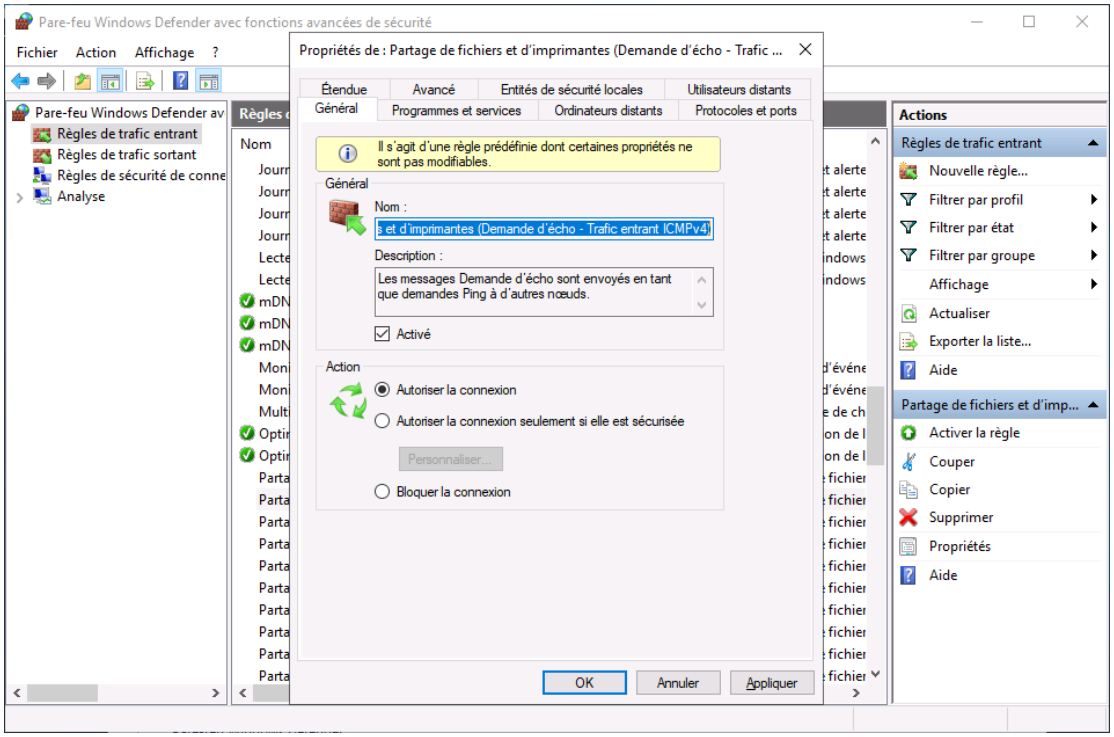
- **Bloquer toutes les connexions entrantes, y compris celles de la liste des applications autorisées**
- **M'avertir lorsque le Pare-feu Windows Defender bloque une nouvelle application.**

Nous allons ensuite dans les fonctions avancées de sécurité Pare-feu Windows Defender, afin d'établir des règles du trafic entrant. Cliquer sur **Paramètres avancés.**



YAM
VOTRE PARTENAIRE INFORMATIQUE

Afin d'activer la réponse aux requêtes ping nous allons rechercher la ligne **Partage de fichiers et d'imprimantes (Demande d'écho – Trafic entrant ICMPv4)** et double-cliquer dessus.



Dans l'onglet **Général,** cocher la case **Activé** puis dans l'onglet **Avancé** cocher uniquement les cases **Domaine** et **Privé** et cliquer sur OK.

Notre serveur est désormais prêt, installé et configuré. Nous allons maintenant pouvoir installer les rôles qui seront attribués à ce serveur.

2- INSTALLATION DES RÔLES

Les « Rôles » sont un ensemble de services, nativement pris en charge par les systèmes d'exploitation Windows Server.

Un serveur Windows va avoir un ou plusieurs rôle(s) dans une entreprise. Ces rôles peuvent par exemple fournir ou héberger des fichiers, gérer un annuaire, ou encore gérer la configuration réseau. De plus un rôle peut avoir besoin de différentes fonctionnalités.

2-1- RÔLE DHCP

INTRODUCTION

Le rôle DHCP (Dynamic Host Configuration Protocol) est un protocole réseau qui permet de d'attribuer dynamiquement les adresses IP aux différents équipements qui se connectent sur le réseau. C'est donc une sorte de distributeur automatique d'adresses IP. Il fournit également des paramètres réseau (masque de sous-réseau, adresse IP de la passerelle et DNS…). De plus, il délivre des informations tel que le Bail DHCP, qui est une durée de temps pour laquelle les informations sont allouées pour la machine (l'adresse IP fournie par le DHCP a une durée de temps limitée).

Le serveur DHCP permet aux administrateurs réseau de centraliser la gestion de la configuration réseau. Cela évite de devoir configurer manuellement chaque machine connectée au réseau, ce qui est très contraignant lorsqu'on a un grand nombre de machines.

INSTALLATION

Afin d'ajouter le rôle Serveur DHCP, nous nous rendons sur le tableau de bord du gestionnaire de serveur, puis cliquons sur **Gérer** puis sur **Ajouter des rôles et fonctionnalités**. Nous sélectionnons la case **Serveur DHCP** puis cliquons sur **Suivant**.

Pour le type d'installation nous choisissons l'installation basée sur un rôle ou une fonctionnalité. Le serveur de destination est notre serveur **YAM-SRV-MGMT1**. Nous cliquons ensuite sur **Suivant** puis sur **Installer.**

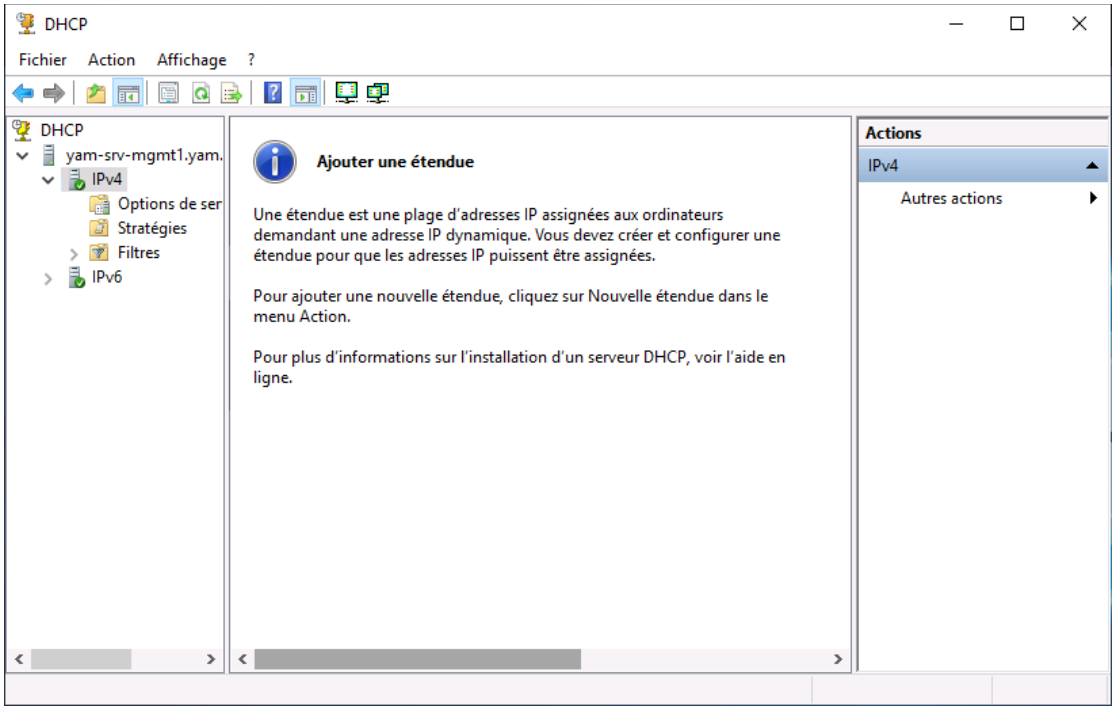
Notre rôle serveur DHCP est désormais installé et nous allons pouvoir le configurer.

CONFIGURATION

Notre serveur DHCP sera configuré avec les paramètres suivants :

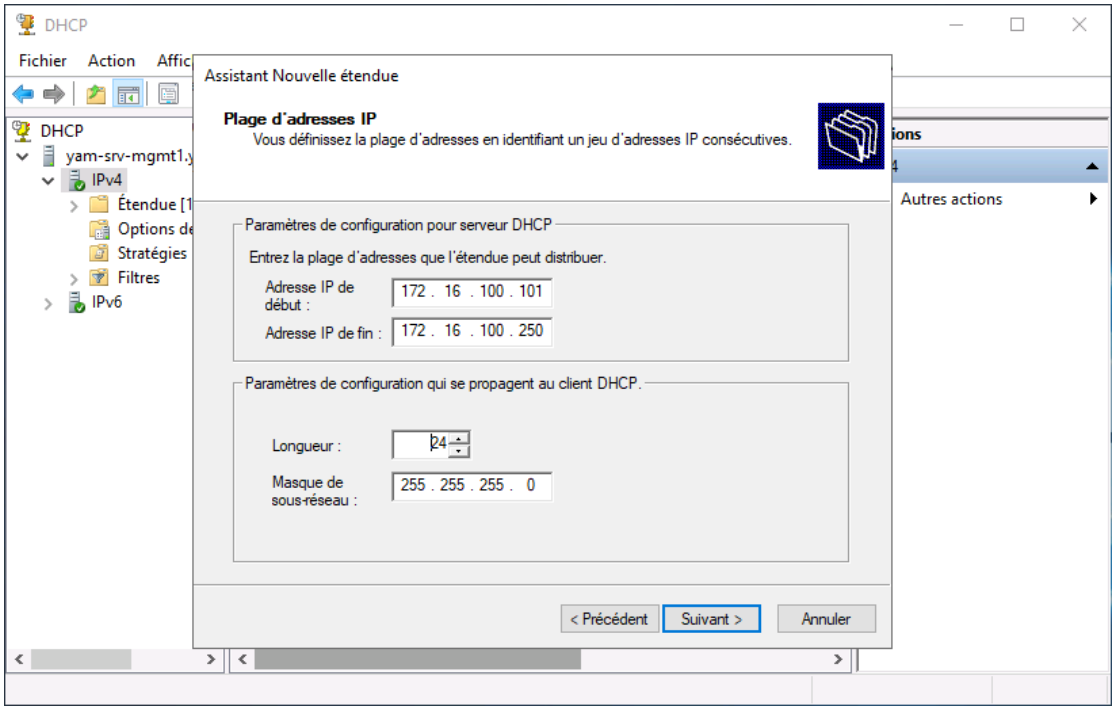
Paramètres	Valeurs
Réseau	172.16.100.0/24
Plage DHCP	172.16.100.101 jusqu'à 172.16.100.250
Exclusions	Aucune
Durée de bail	6 jours
Routeur	172.16.100.254
Serveur DNS	IP des contrôleurs de domaine

Pour ajouter une nouvelle étendue, faire un clic-droit sur **IPv4** et choisir **Nouvelle étendue.**



On nommera cette étendue **YAM_IP_150** et ajouter une description puis cliquer sur **Suivant.** En effet, nous disposons d'une plage DHCP de 150 adresses IP du réseau de l'entreprise.

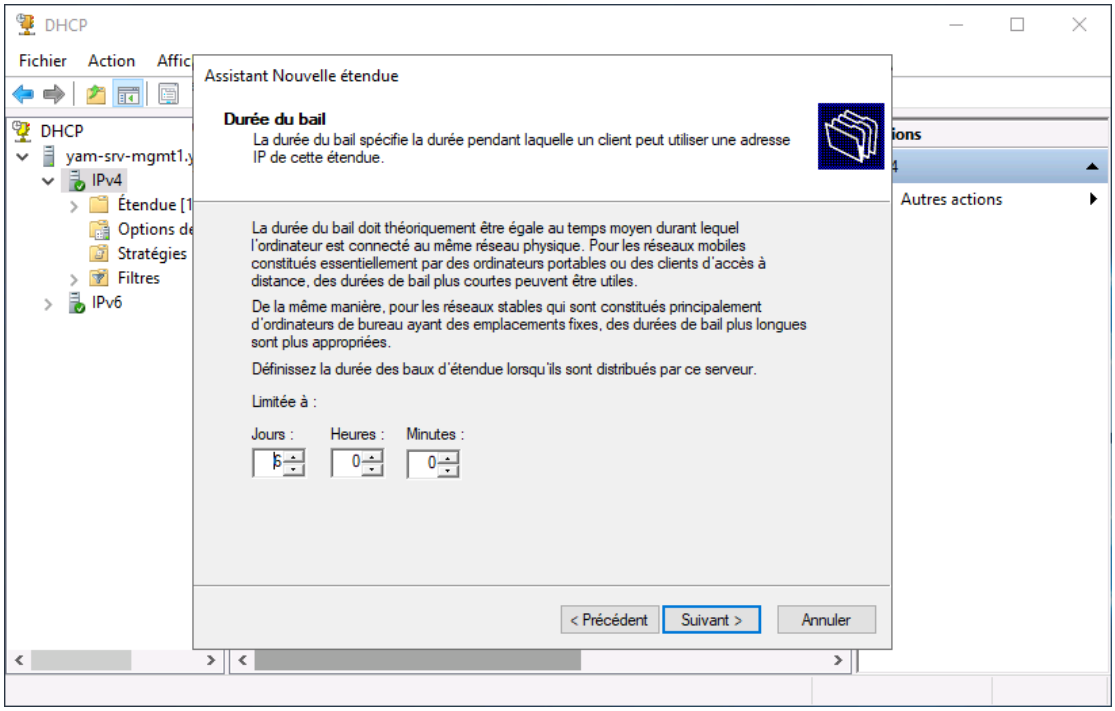
Préciser ensuite le masque de sous-réseau à **24** (correspond à **255.255.255.0**) puis cliquer sur **Suivant**, afin d'y mettre 254 adresses IP (pour les serveurs, le routeur, les imprimantes etc.).



Nous avons également la possibilité d'ajouter des exclusions d'adresses IP dans notre plage afin qu'elles ne soient pas distribuées par le serveur DHCP. Laisserons le champ vide et cliquer sur **Suivant.**

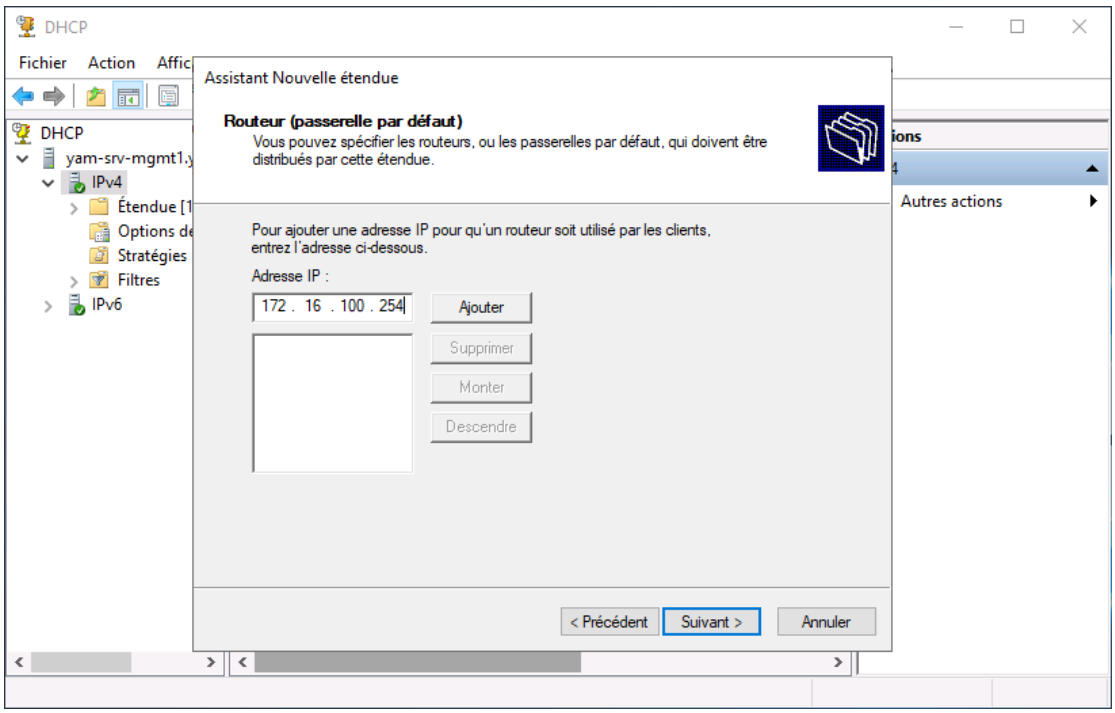
On définit ensuite la durée du bail. Nous choisissons de la limiter à 6 jours. Ainsi, à chaque reconnexion en début de semaine, les utilisateurs se verront attribuer une nouvelle adresse IP pour leur poste de travail.

En effet, à la fin du sixième jour (qui correspond au samedi) toutes les machines non connectées au réseau voient leurs adresses IP libérées et mises de nouveau à disposition. Il nous faudra donc établir une note de service, informant les utilisateurs de l'obligation de déconnecter leurs postes en fin de journée.



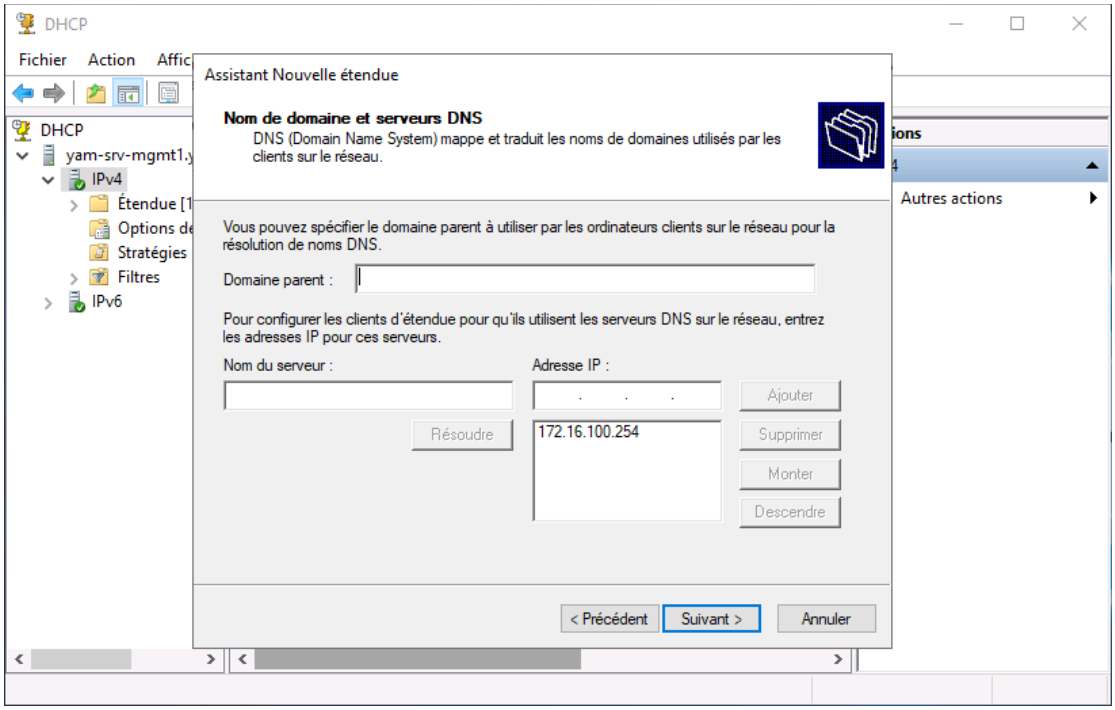
Choisir ensuite **Oui, je veux configurer ces options maintenant** puis cliquer sur **Suivant.**

Nous configurons ensuite l'adresse IP de notre routeur qui est : 172.16.100.254



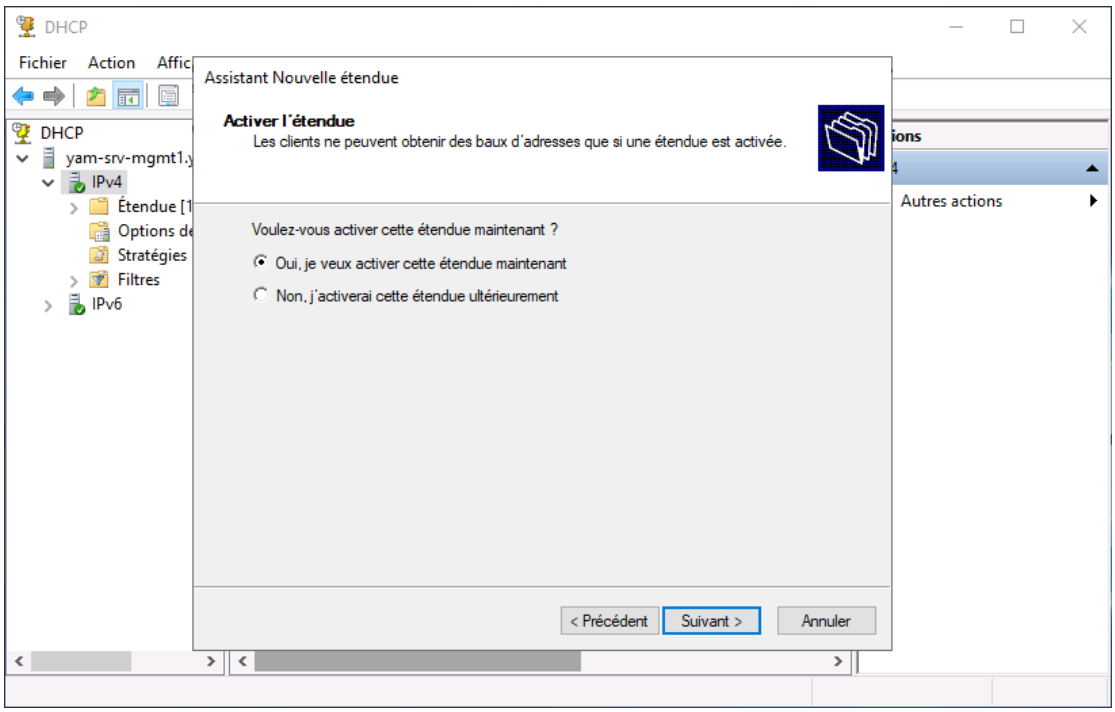
YAM
VOTRE PARTENAIRE INFORMATIQUE

Ajouter les serveurs DNS, on ajoutera les adresses IP des contrôleurs de domaine.



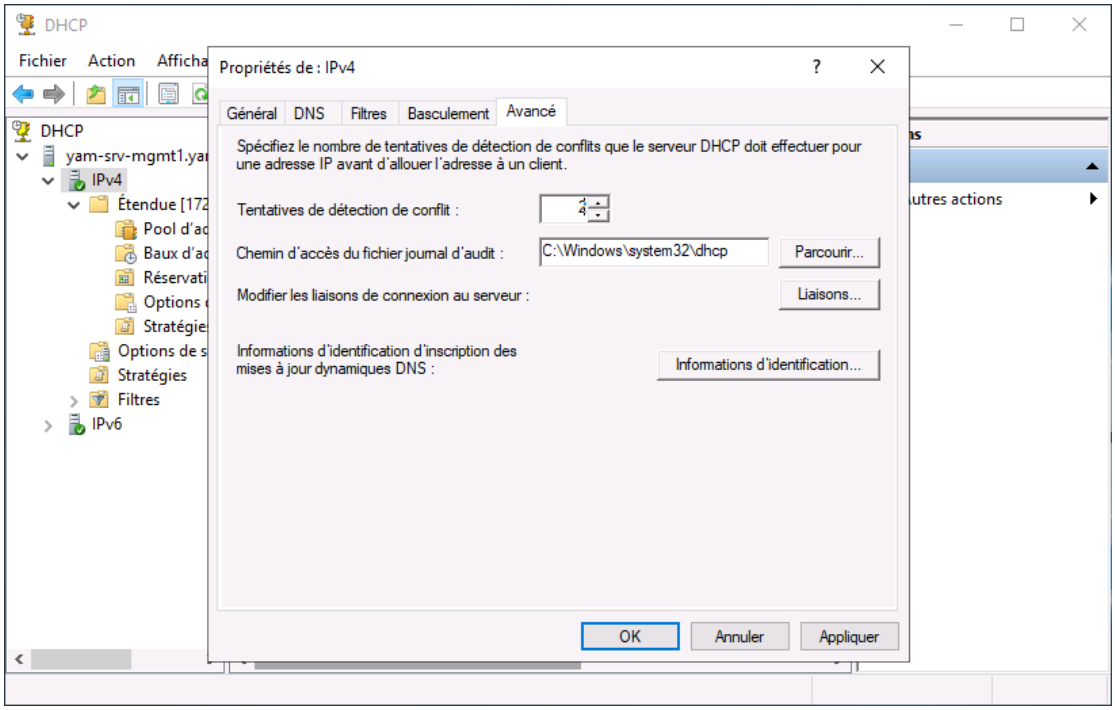
Nous avons ensuite la possibilité de configurer les serveurs WINS, mais cette fonction ne sera pas utilisée. Cliquer sur **Suivant**.

Nous pouvons maintenant activer l'étendue. Nous cliquons donc sur **Suivant** puis sur **Installer.**



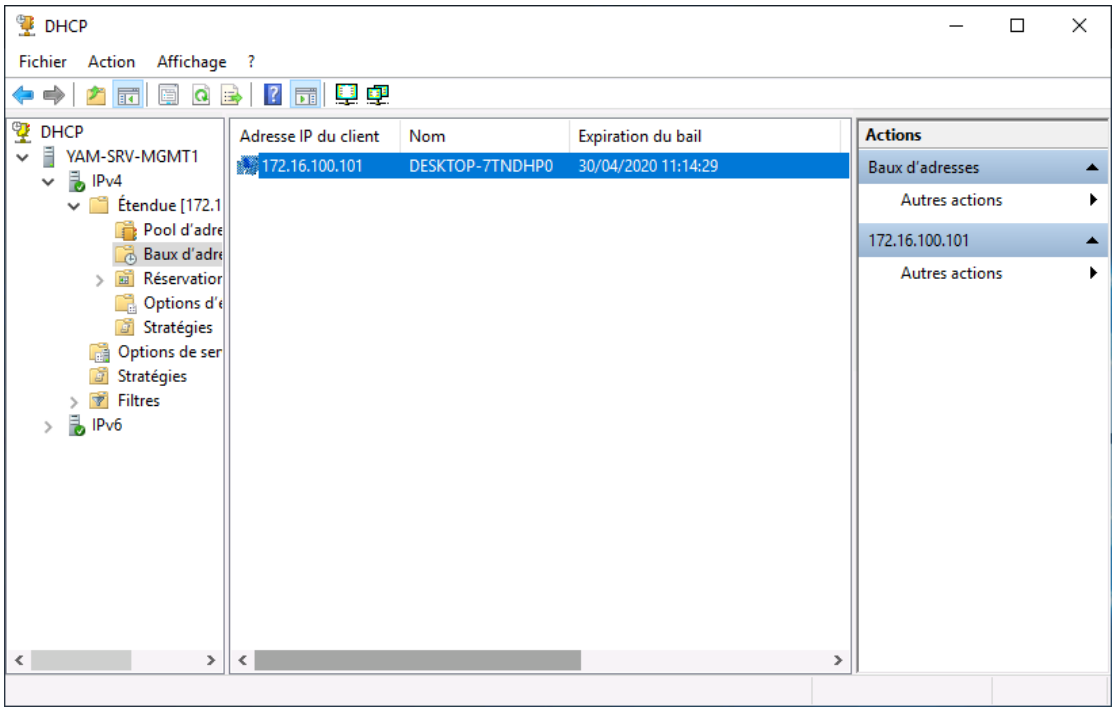
Notre serveur DHCP est désormais configuré mais il reste encore à gérer la détection des conflits d'adresses IP afin d'éviter que le serveur DHCP ne délivre à un ordinateur une adresse IP déjà attribuée.

Faire un clic-droit sur IPv4 puis se rendre dans l'onglet Avancé et mettre **Tentatives de détections de conflits sur 2** et cliquer sur **OK.**



ADMINISTRATION

Maintenant que le serveur DHCP est configuré, on peut observer la liste des appareils ayant une adresse IP attribuée.



Il est possible d'effectuer des réservations, c'est-à-dire qu'un périphérique se verra toujours attribué la même adresse IP.

2-2- RÔLE DNS

INTRODUCTION

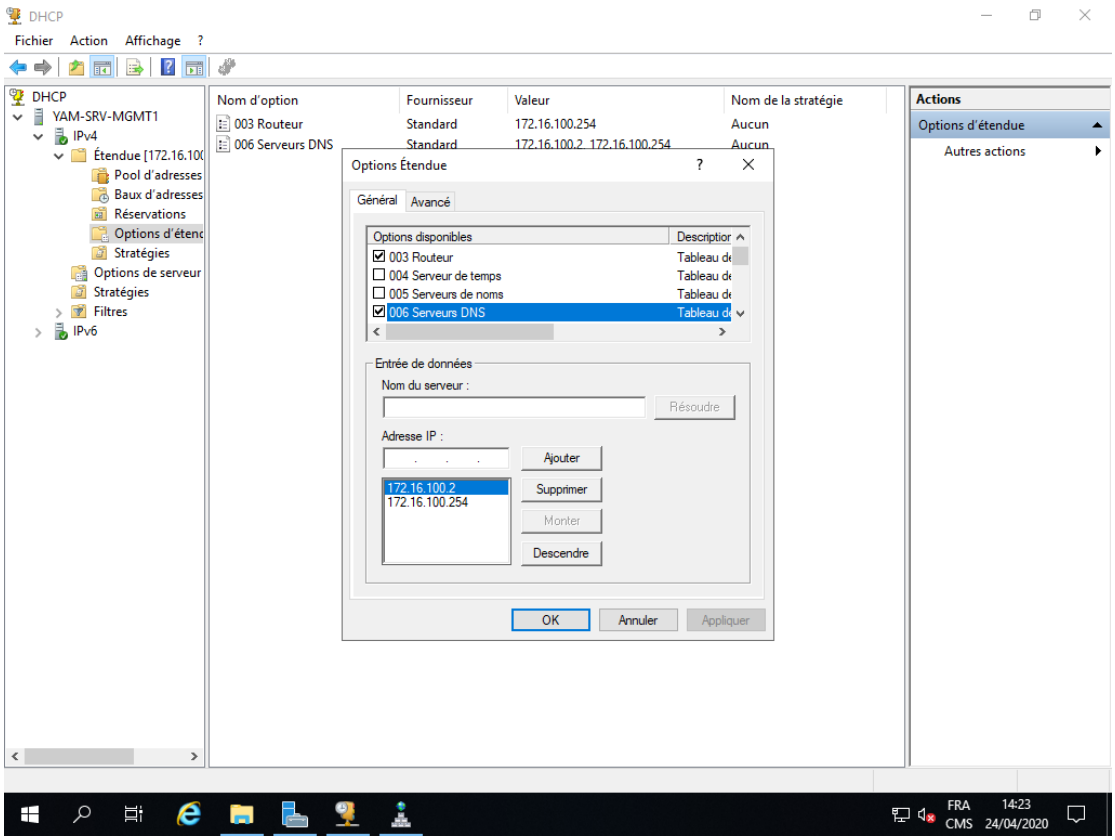
Le rôle DNS (Domain Name System) est un service dont la principale action de traduire des noms de domaines en adresses IP. Le DNS fait donc la correspondance entre les noms de domaines et les adresses IP. Le serveur DNS agit comme un annuaire que consulte un ordinateur, au moment d'accéder à un ordinateur via un réseau. Il est donc obligatoire dans un domaine Active Directory car il permet la résolution de noms en adresse IP et inversement.

INSTALLATION

Afin d'ajouter le rôle Serveur DNS, nous nous rendons sur le tableau de bord du gestionnaire de serveur, puis cliquons sur **Gérer** puis sur **Ajouter des rôles et fonctionnalités**. Nous sélectionnons la case **Serveur DNS** puis cliquons sur **Suivant**.

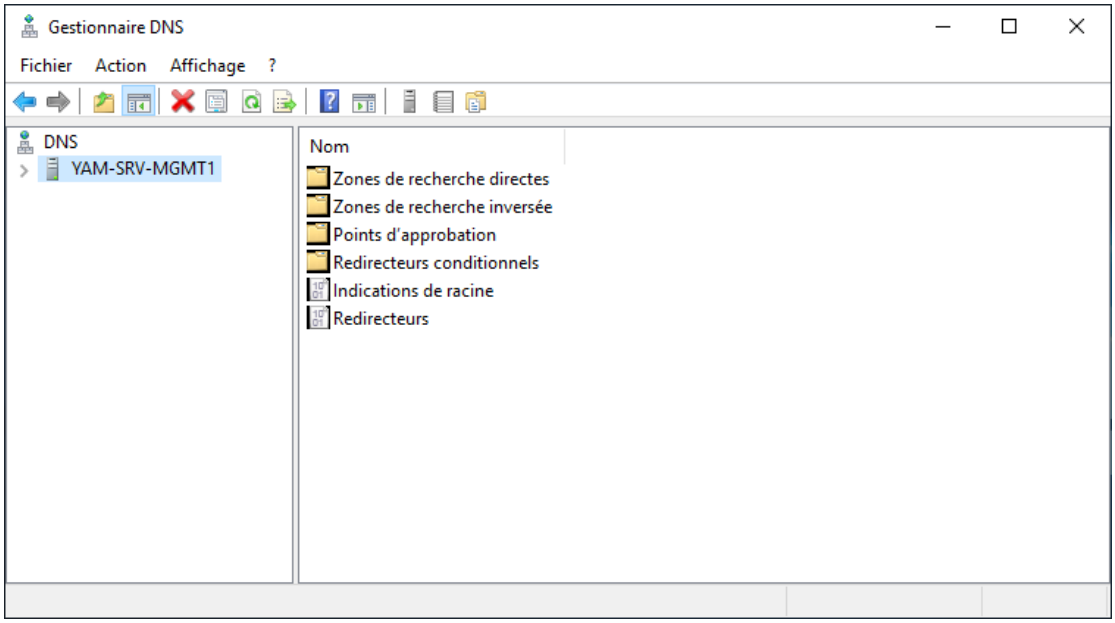
CONFIGURATION

Si le rôle DNS a été installé après le DHCP, il faudra ajouter dans le gestionnaire DHCP les informations relatives à notre serveur DNS. **On rouvrira donc le DHCP** puis se rendre dans Options d'étendues et dans **006 Serveur DNS** on ajoutera l'adresse IP du serveur ayant le rôle DNS en 1re place.



Puis dans les paramètres de la carte réseau **Protocole Internet version 4 (TCP/IPv4)** de la machine, on rajoutera comme adresse de serveur DNS principal.

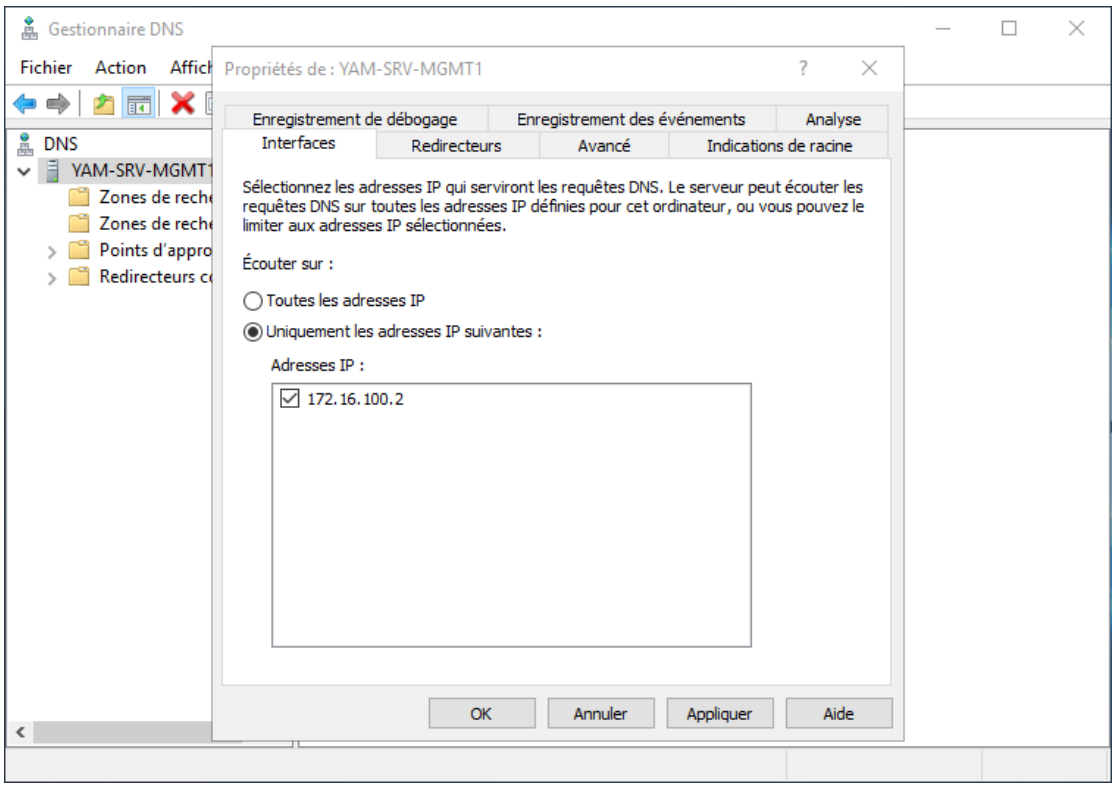
Afin de gérer le service nous devons nous assurer que le rôle DNS est correctement configuré. Nous devons donc créer une requête DNS que pourra écouter le serveur.



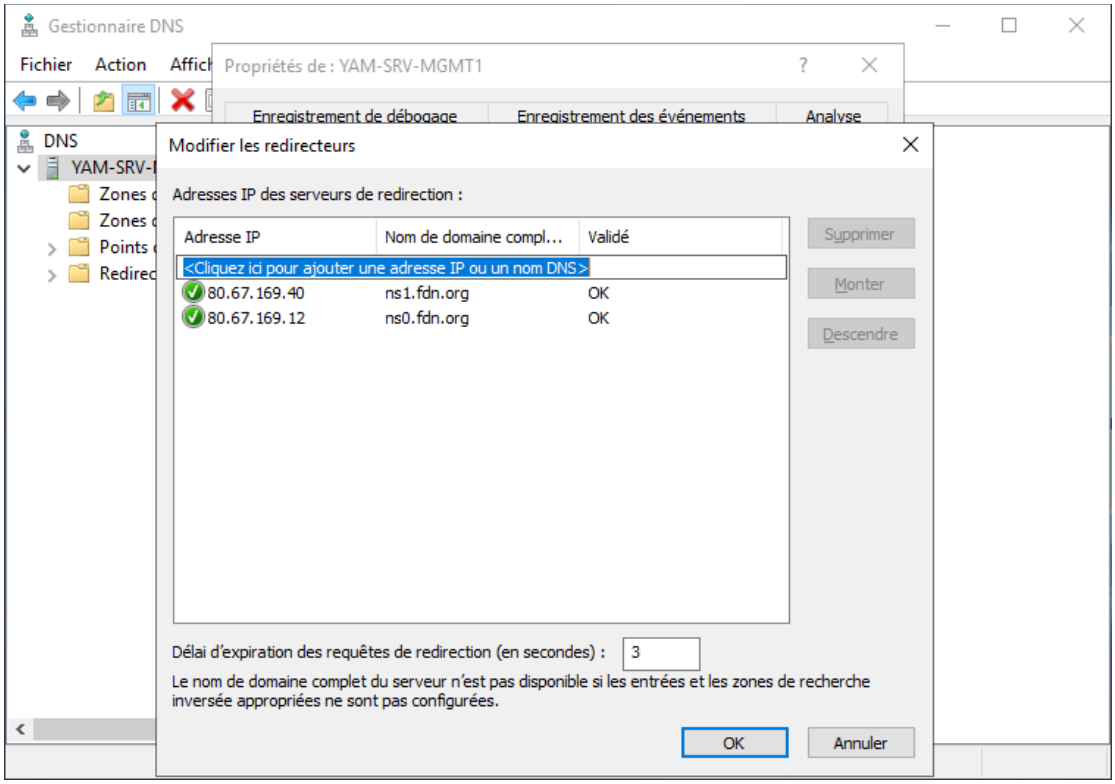
ZONE DE RECHERCHE INVERSÉE

Recommandations : Contrôleur de domaine déjà configuré.

Nous sélectionnons donc l'IP fixe que nous avons configuré pour notre réseau de production : Faire un **clic-droit sur le nom du serveur** et dans l'onglet **Interfaces** sélectionner **Uniquement les adresses IP suivante** et ajouter **172.16.100.2**

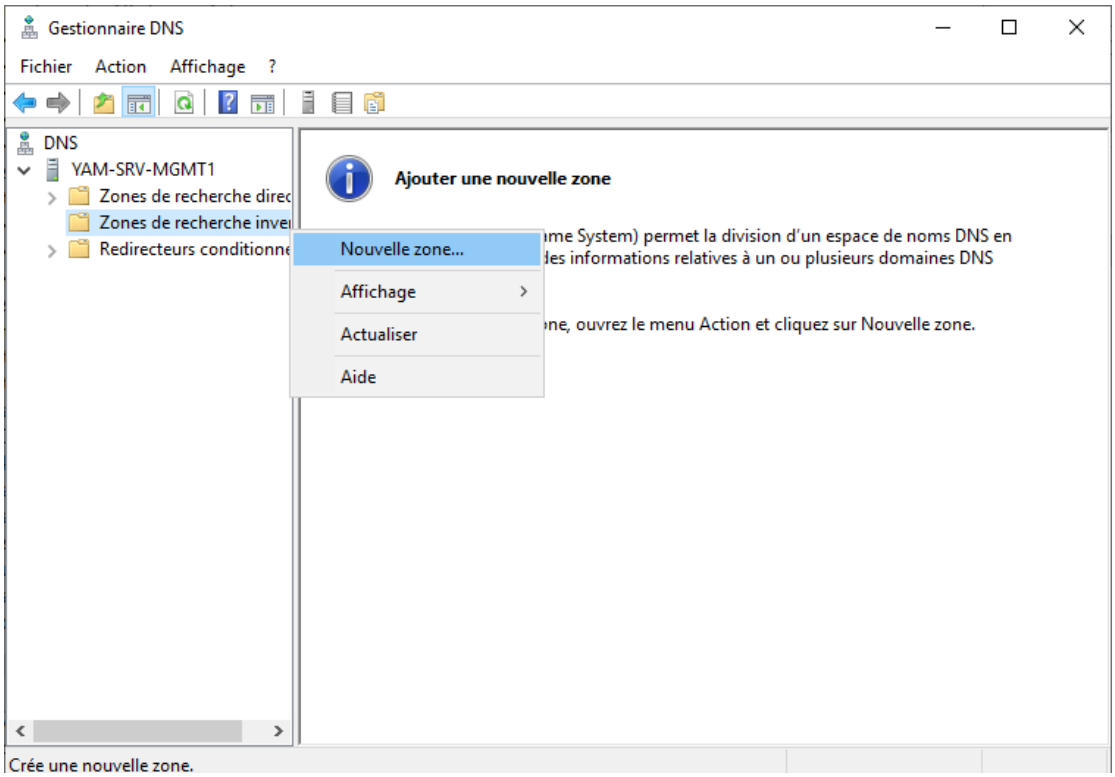


Nous ajoutons ensuite les redirecteurs, afin que le serveur DNS puisse interroger le serveur racine.

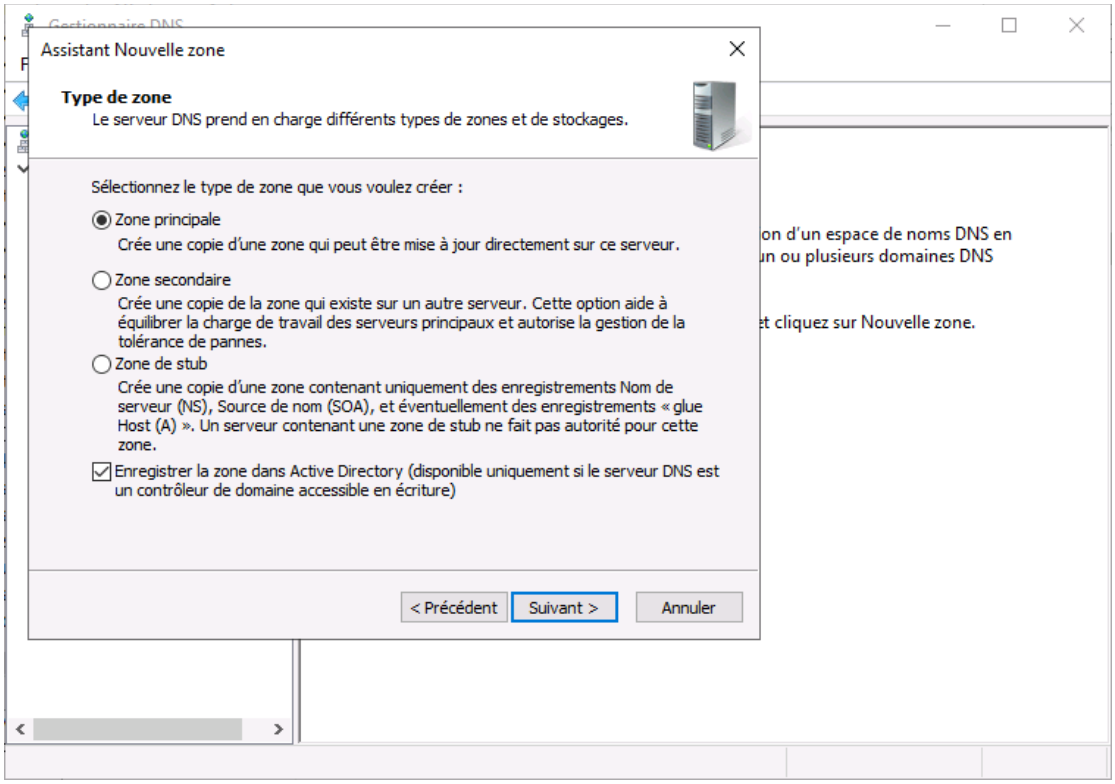


Nous créons par la suite une zone de recherche inversée. Cela nous permettra d'effectuer des recherches à partir d'adresses IP, c'est-à-dire que cette zone permet la résolution d'adresses IP en noms de postes.

Faire un clic-droit sur **Zone de recherche inversée** et choisir **Nouvelle zone...**

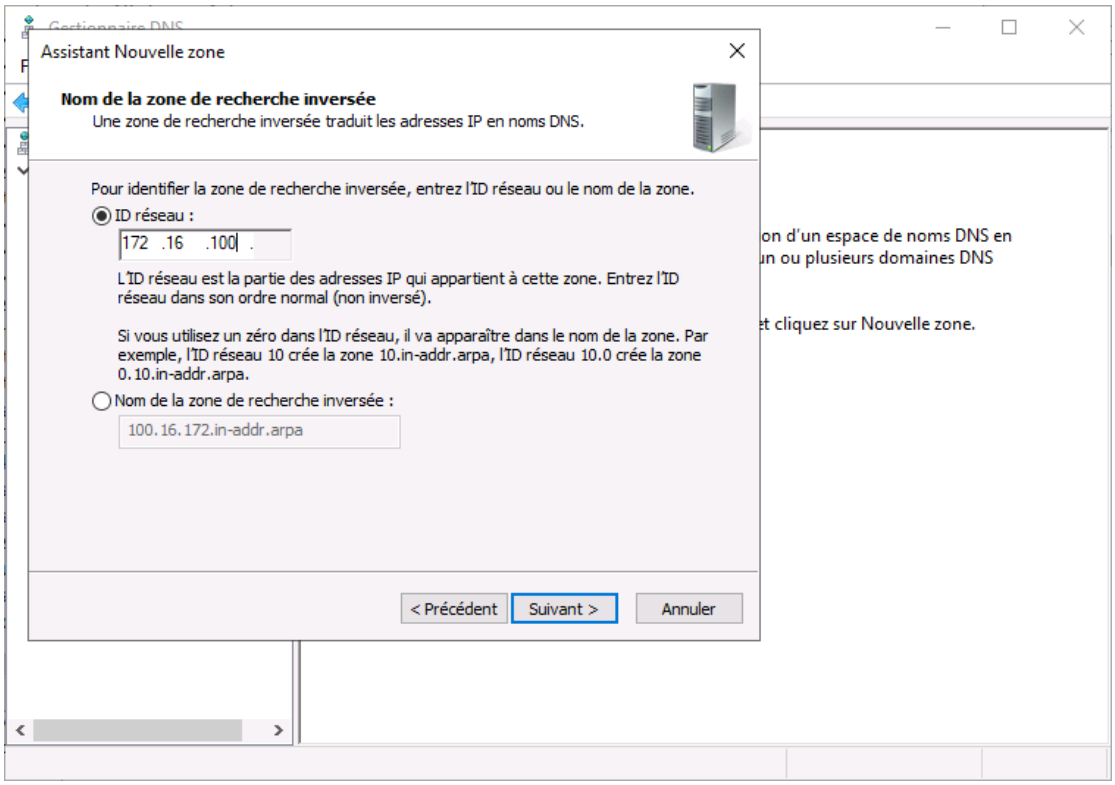


Dans l'assistant Nouvelle zone, Choisir **Zone principale** et cliquer sur **Suivant.**



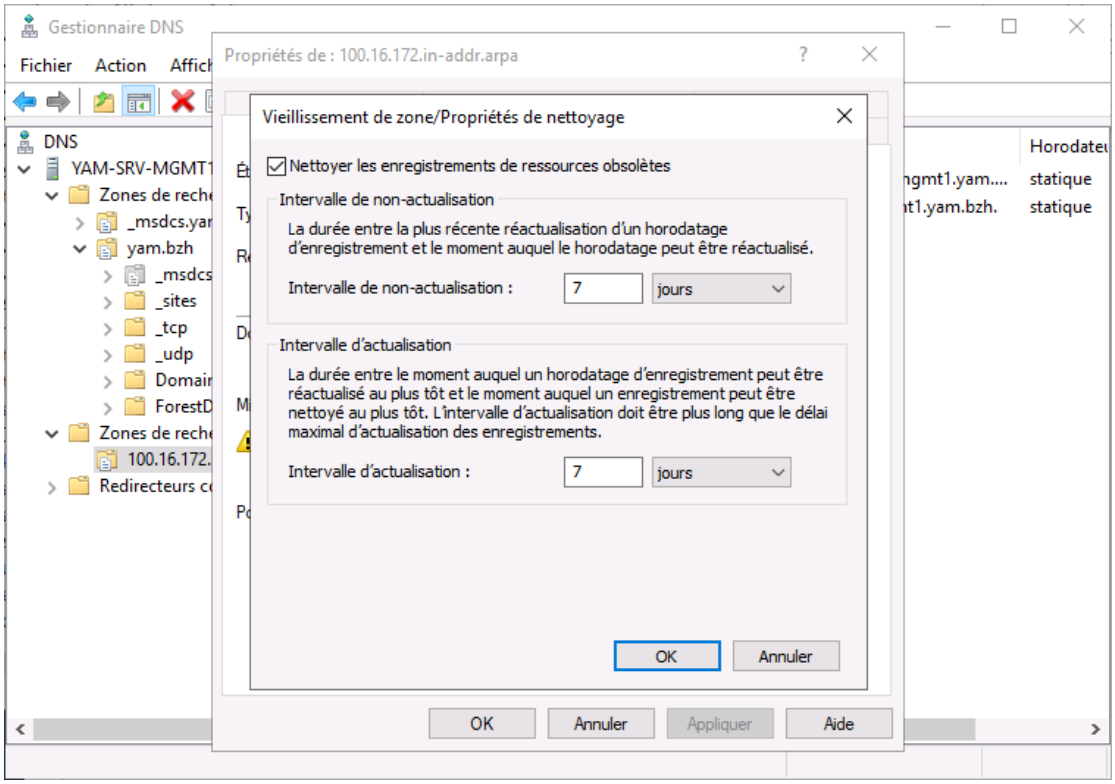
Puis sélectionner **Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : yam.bzh** puis cliquer sur **Suivant.**

Choisir **Zone de recherche inversée IPv4** et cliquer sur **Suivant,** puis indiquer comme **ID réseau : 172.16.100.**



Et enfin, pour terminer l'assistant, choisir **N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory).**

Pour finir nous appliquerons une gestion du nettoyage des zones que nous appliquerons également à la zone de recherche directe. Faire un **clic-droit sur la zone nouvellement créée,** choir **Propriétés** puis dans l'onglet Général cliquer sur **Vieillissement.**



Cocher **Nettoyer les enregistrements de ressources obsolètes** et laisser les intervalles sur 7 jours.

3- ACTIVE DIRECTORY (AD)

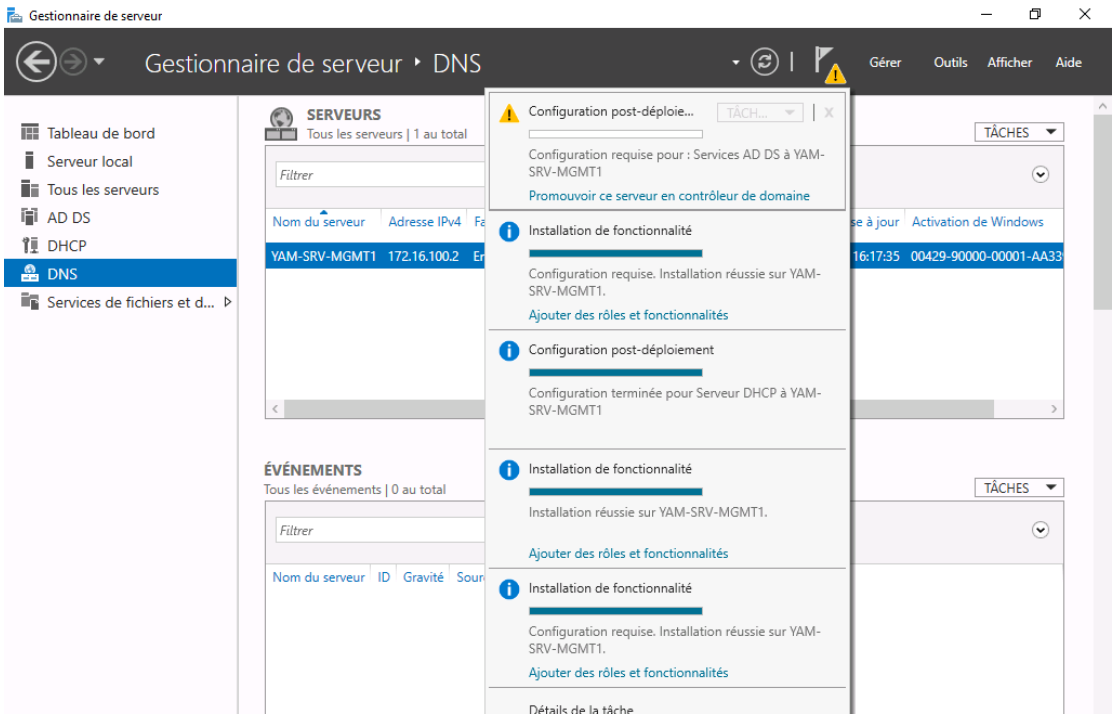
INTRODUCTION

L'infrastructure Active Directory fonctionne selon une hiérarchie qui représente une entité de sécurité, hébergeant les utilisateurs et les ordinateurs. Cette infrastructure forme donc une arborescence composée de domaines, d'arbres de domaine ou de forêts. Les différents domaines constituants une arborescence, communiquent entre eux via des relations d'approbation.

INSTALLATION DU RÔLE

Pour gérer notre domaine et les droits d'accès des utilisateurs, nous ajoutons donc la fonctionnalité AD DS (Active Directory Domain Service), de la même manière que nous avons ajouté les rôles DHCP et DNS.

Après l'installation, nous allons **promouvoir notre serveur en contrôleur de domaine.**



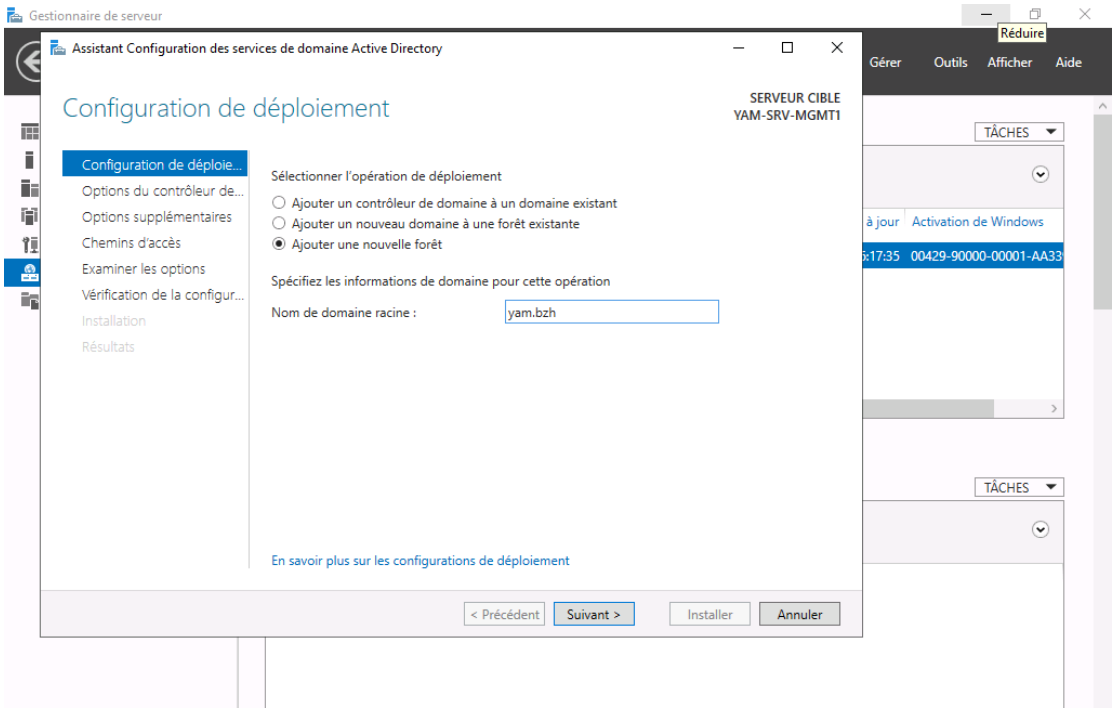
3-1- CRÉATION DE LA FORÊT

Une forêt est un regroupement de plusieurs domaines Active Directory. Le premier domaine installé dans une forêt est appelé domaine racine de la forêt. Plusieurs arbres de domaines dont l'espace de nom n'est pas continu, représentent une forêt.

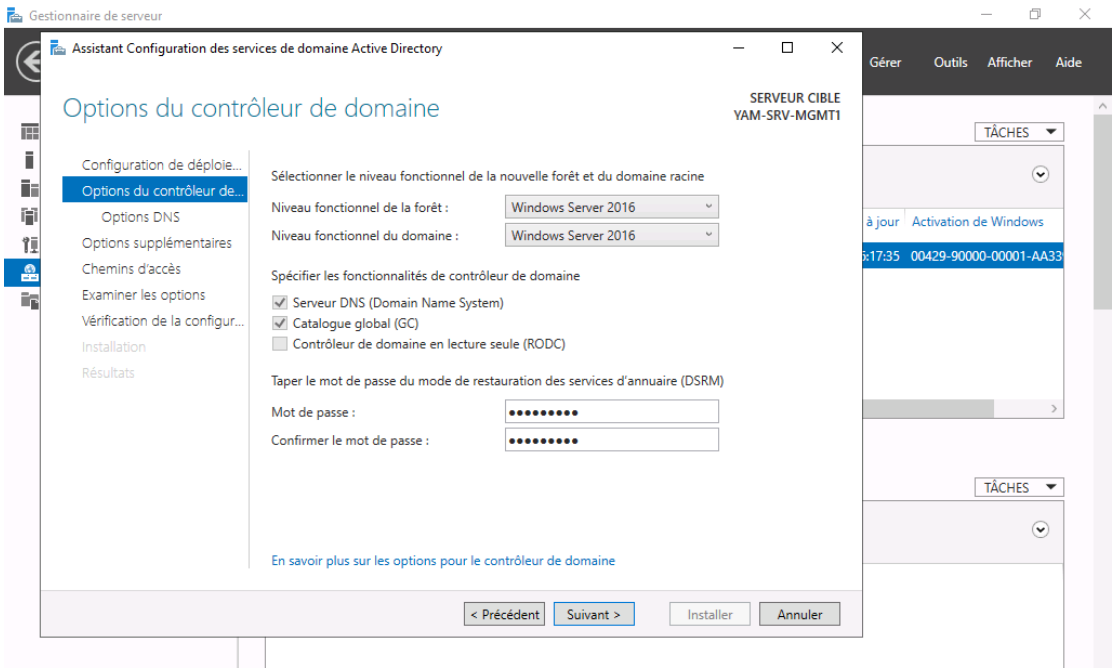
INSTALLATION PAS-À-PAS

Une fois avoir installé notre infrastructure Active Directory, nous pouvons la configurer.

Pour ce faire **nous ajoutons une nouvelle forêt,** et nommons notre domaine racine ***yam.bzh***

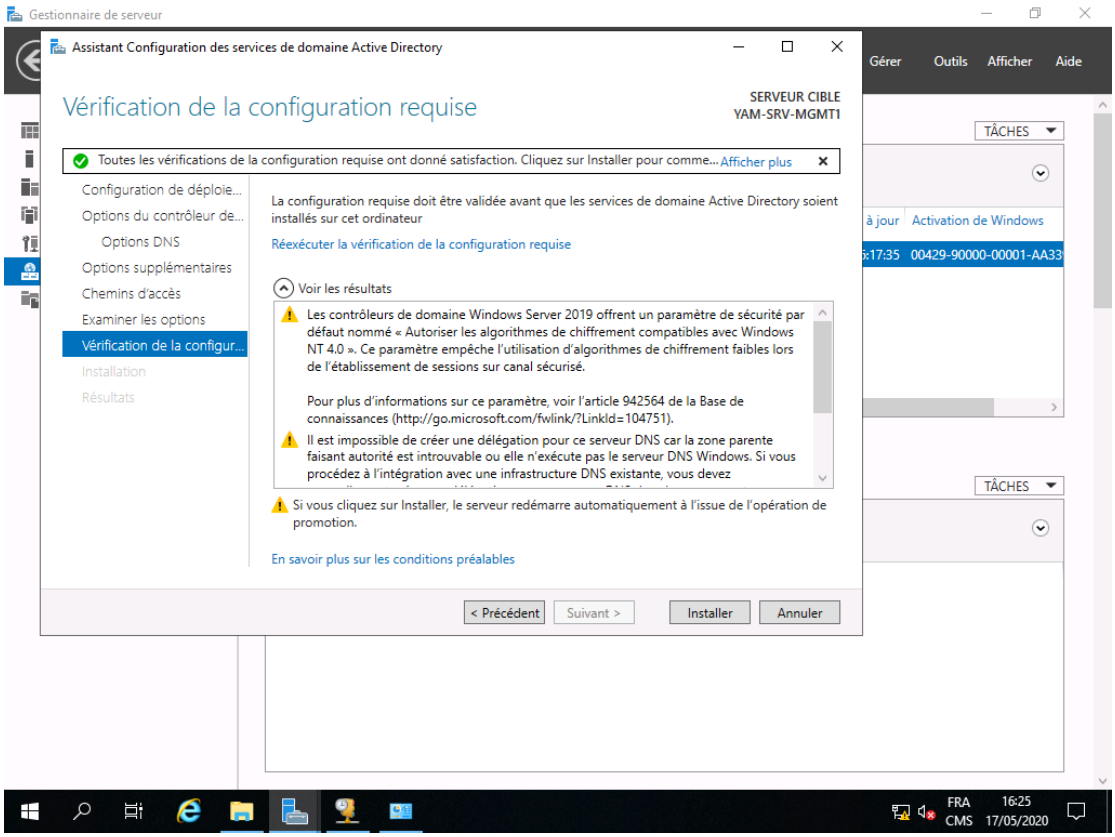


Pour le choix du **niveau fonctionnel de cette forêt,** ainsi que pour notre **domaine racine,** nous sélectionnons **Windows Server 2016.** De plus nous choisissons un mot de passe qui nous permettra la restauration des services d'annuaire si besoin.



Par la suite nous spécifions le nom de notre domaine NetBIOS ***YAM***, ainsi que l'emplacement de notre base de données AD DS, le dossier des fichiers journaux, et le dossier SYSVOL. Enfin, dans **Examiner les options**, nous avons un résumé de notre configuration.

Enfin, dans **Vérification de la configuration requise**, nous avons un résumé tu test de la validation ou non de notre configuration. Si tout est OK, nous pourrons cliquer sur **Installer**.



L'installation se poursuit puis le serveur redémarre.

Maintenant que notre fonctionnalité Active Directory est installée, nous pouvons créer des groupes locaux d'utilisateurs qui nous permettront de leur attribuer des droits spécifiques.

3-2- UTILISATEURS ET GROUPES

INTRODUCTION

Une partie importante de la sécurisation du réseau consiste à gérer les utilisateurs et les groupes qui ont un accès administratif au service d'annuaire Active Directory.

Les groupes tel que les groupes de sécurité, permettent de simplifier la gestion des objets en les regroupant selon des critères. On peut par exemple, regrouper tous les utilisateurs d'un même service, afin de gérer les accès aux répertoires partagés pour ce service

ORGANISER LE DOMAINE

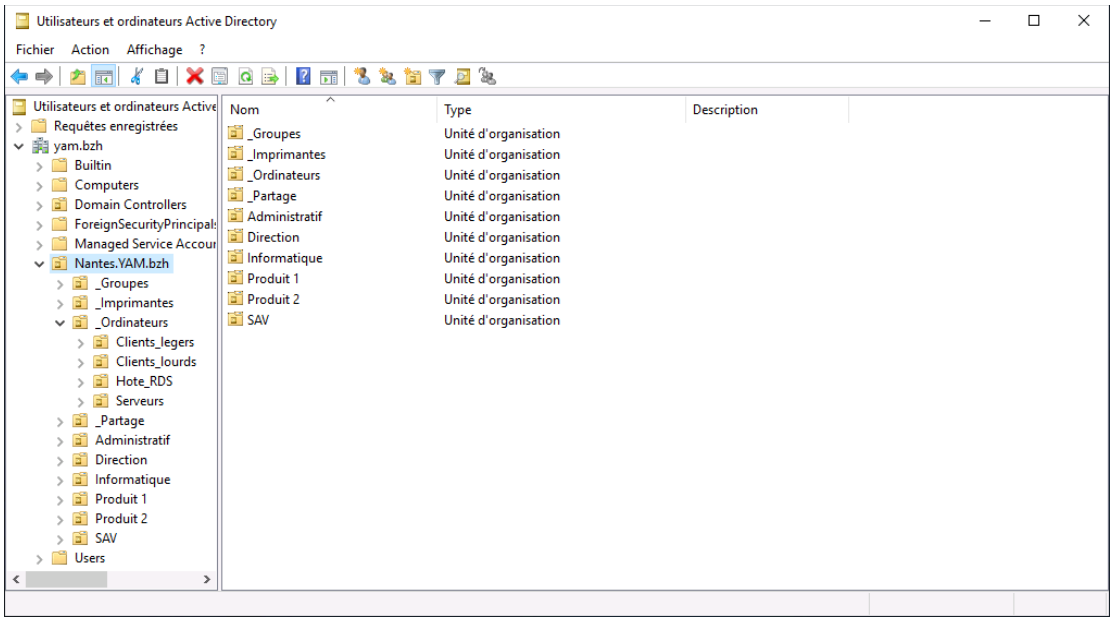
Afin de bien structurer notre domaine, nous créerons différentes **Unités d'organisation (OU)**, dans lesquelles sont regroupées les utilisateurs en fonction de leurs postes, les ordinateurs, et les groupes. Ceci nous permet de mettre en place des stratégies de groupes (GPO) afin de restreindre les actions des différents utilisateurs.

Ces OU sont établies de cette manière :

- **_Groupes** : Contient les groupes globaux (GG) regroupant les utilisateurs.
- **_Imprimantes** : Contient les groupes de domaine local (GDL) gérant les droits sur les imprimantes.
- **_Ordinateurs** : Contient les ordinateurs et serveurs du domaine.
  - **Clients_legers** : Contient les postes en client léger et compte utilisateur approprié.
  - **Clients_lourds** : Contient les postes utilisés en tant que client lourd.
  - **Hote_RDS** : Contient les VM hôte de session RDS.
  - **Serveurs** : Contient les autres serveurs membres du domaine.
- **_Partage** : Contient les GDL pour les droits d'accès aux dossiers partagés.
- **Administratif** : Contient les utilisateurs membres de ce service.
- **Direction** : Contient les utilisateurs membres de ce service.
- **Informatique** : Contient les utilisateurs membres de ce service.
- **Produit 1** : Contient les utilisateurs membres de ce service.
- **Produit 2** : Contient les utilisateurs membres de ce service.
- **SAV** : Contient les utilisateurs membres de ce service.

Nous créerons d'abord une OU à la racine de notre domaine que l'on nommera **Nantes.YAM.bzh** : Faire un clic-droit sur **yam.bzh** puis **Nouveau > Unité d'organisation**.

Puis dans cette OU Nantes.YAM.bzh, on crée des nouvelles OU correspondant à chaque service.



CRÉATION DES GROUPES DE DOMAINE LOCAL

La création des groupes de domaine local permet de fixer les droits d'accès sur des dossiers partagés ou d'utilisation sur des imprimantes.

Aussi pour chaque dossier partagé on créera les GDL suivants :

Nom du groupe	Niveau d'accès
GDL_NomDossier_CT	Contrôle total
GDL_NomDossier_LM	Modification (lecture et écriture)
GDL_NomDossier_LS	Lecture seule
GDL_NomDossier_LS_DS	Lecture seule sans héritage dans sous-dossiers

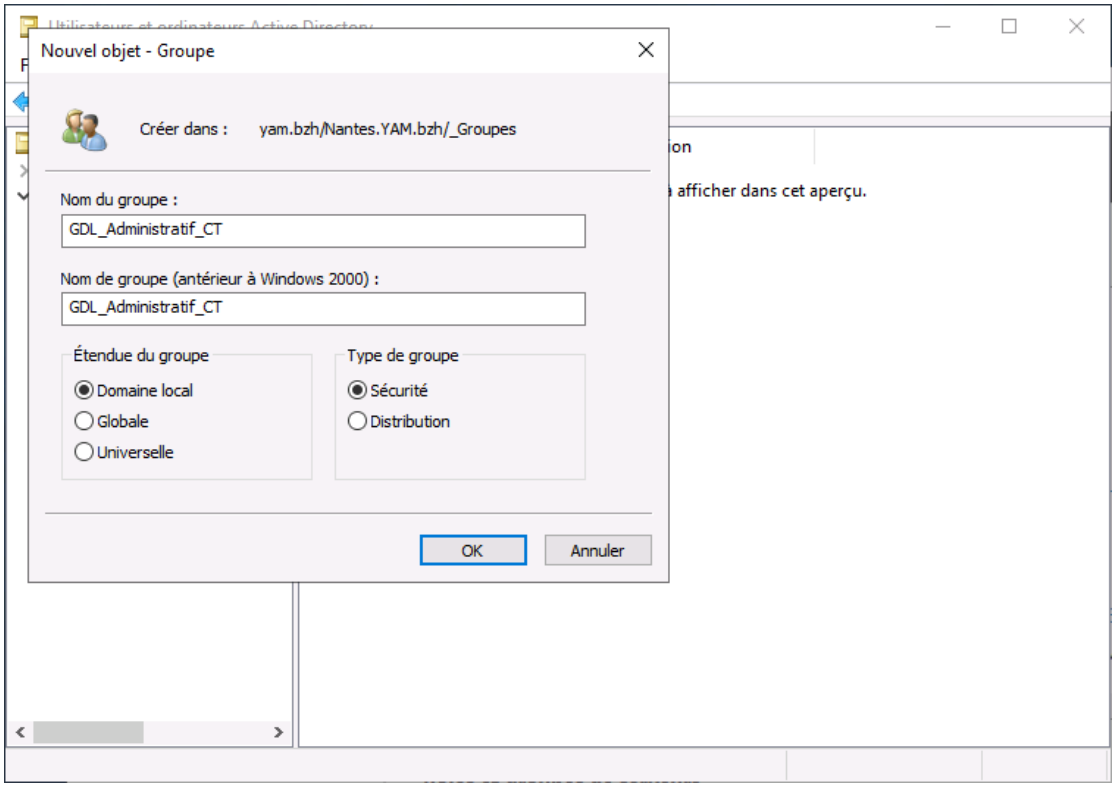
Les droits en lecture seule, uniquement sur les dossiers **GDL_NomDossier_LS_DS**, sont nécessaire afin que, lors de la création automatique du dossier de chaque utilisateur du service, **les collègues ne puissent pas y avoir accès**.

Et pour chaque imprimante partagée on créera les GDL suivants :

Nom du groupe	Niveau d'accès
GDL_Print_Service_CT	Contrôle total
GDL_Print_Service_GI	Gestion des imprimantes
GDL_Print_Service_IM	Impression seule

On appliquera ces droits par la suite aux dossiers et imprimantes correspondants et nous n'aurons plus besoin d'y revenir dessus.

Pour créer un GDL, faire un clic-droit dans l'OU **_Groupes** et choisir **Nouveau > Groupe.**



Nommer le groupe et sélectionner comme **Étendue du groupe : Domaine local** et laisser Type de groupe sur **Sécurité.**

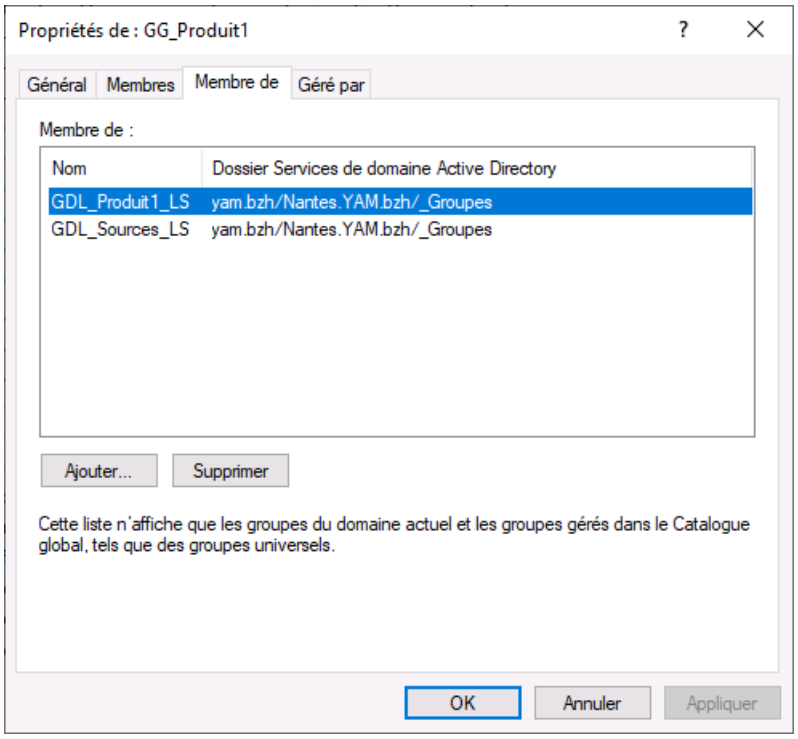
CRÉATION DES GROUPES GLOBAUX

Nous créons donc des groupes locaux d'utilisateurs différents, dans lesquels les salariés sont regroupés en fonction de leurs postes et donc de leurs différents niveaux de droits d'accès.

Ces groupes sont établis de cette manière :

Nom du groupe	Service
GG_Administratif	Administratif
GG_Direction	Direction
GG_Informatique	Informatique
GG_Produit1	Produit 1
GG_Produit2	Produit 2
GG_SAV	SAV

Afin d'appliquer les droits d'accès aux imprimantes et/ou dossiers partagés il suffit de rendre le GG membre du GDL correspondant aux droits d'accès.



Pour créer un GG, la procédure est identique à la création d'un GDL à la différence qu'il faudra choisir comme **Étendue du groupe : Globale.**

CRÉATION DES MODÈLES D'UTILISATEURS

Dans chaque unité d'organisation (OU) un créée un modèle d'utilisateur à partir duquel on se basera pour créer les utilisateurs de l'entreprise. On appliquera à chaque modèle les éléments suivants :

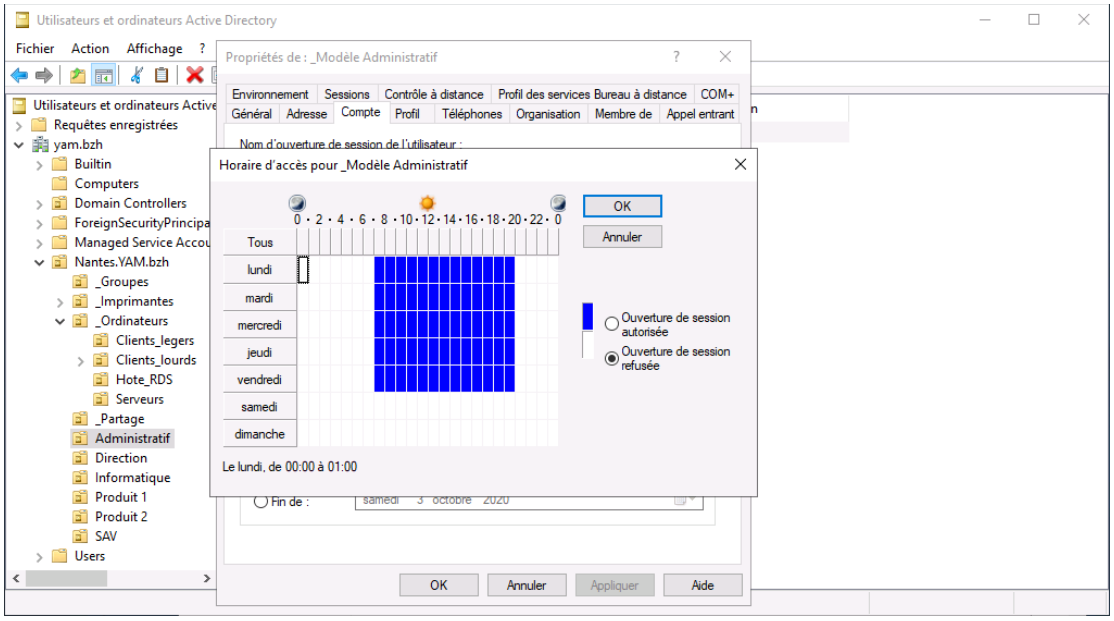
Nom	Groupe	Dossier de base	Horaires de connexion
_m.administratif	GG_ Administratif	\\YAM_SRV_DATA\Commun\Commun_Administratif\%username%	De 7h00 à 20h00
_m.direction	GG_Direction	\\YAM_SRV_DATA\Commun\Commun_Direction\%username%	24h
_m.informatique	GG_Informatique Admins du domaine	\\YAM_SRV_DATA\Commun\Commun_Informatique\%username%	24h
_m.produit1	GG_Produit1	\\YAM_SRV_DATA\Commun\Commun_Produit1\%username%	De 7h00 à 20h00
_m.produit2	GG_Produit2	\\YAM_SRV_DATA\Commun\Commun_Produit2\%username%	De 7h00 à 20h00
_m.sav	GG_SAV	\\YAM_SRV_DATA\Commun\Commun_SAV\%username%	24h

Pour créer un modèle, il suffit de créer un utilisateur dans l'OU spécifiée, faire un clic-droit dans l'OU **_Groupes** et choisir **Nouveau > Utilisateurs.**

Définir le nom puis un mot de passe générique et on coche **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session.**

Puis faire un clic-droit sur notre modèle nouvellement créé et choisir **Propriétés** :

Dans l'onglet **Compte,** si des restrictions horaires doivent être appliquées, cliquer sur **Horaires d'accès** et définir plage horaire d'accès.



Dans l'onglet **Profil,** se rendre dans **Dossier de base** et sélectionner **Connecter,** choisir la lettre de lecteur **U** et spécifier le chemin d'accès correspondant. Ce paramètre permet de créer automatiquement le répertoire utilisateur dans le dossier partagé avec les droits en contrôle total pour l'utilisateur.

Puis dans l'onglet **Membre de,** on ajoutera le groupe auquel notre modèle doit appartenir.

Répéter les opérations pour tous les services.

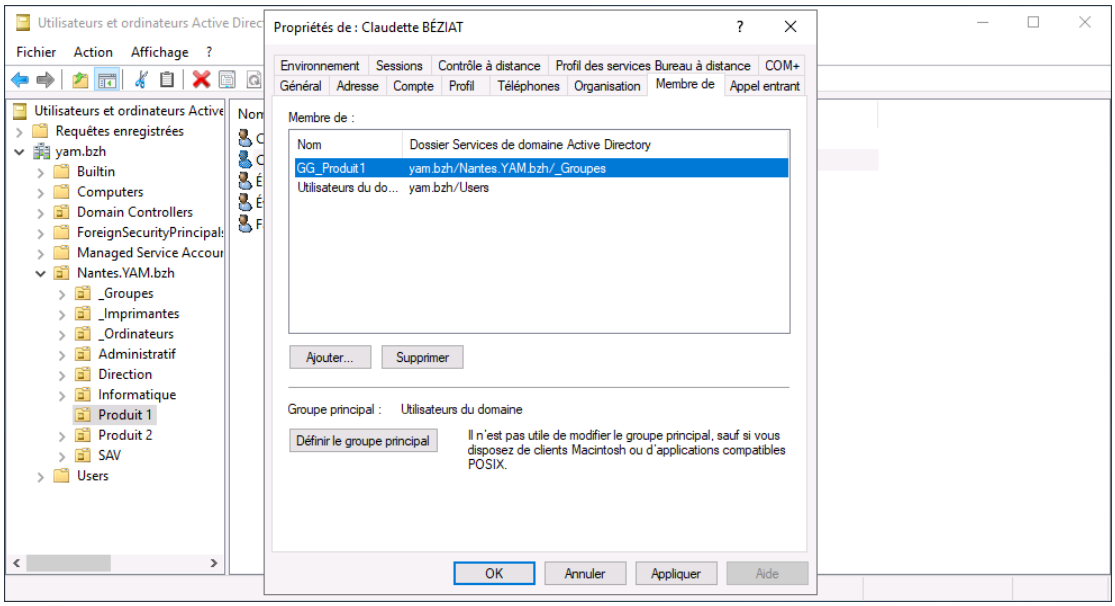
CRÉATION DES UTILISATEURS

Nous prenons en exemple l'utilisatrice Claudette BÉZIAT, qui est affiliée au service **Produit 1**. Elle a donc accès aux ressources partagées du dossier commun **Commun_Produit1**.

Pour créer un utilisateur, faire un clic-droit sur le modèle utilisateur correspondant au service et choisir **Copier.** Ceci permet de créer un nouvel utilisateur avec tous les paramètres du modèle (appartenance au groupe, dossier de base, restrictions horaires, etc.)

Définir le **nom, prénom, le nom complet** (celui qui s'affiche dans la session Windows) et le **nom d'ouverture de session qui sera normée sous la forme p.nom** (p : initiale du prénom).

On définit ensuite le mot de passe provisoire et on coche **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session.**



CRÉATION DU COMPTE UTILISATEUR DU CLIENT LÉGER

On crée un utilisateur qui sera placé dans l'OU Clients_legers, ce compte sera le compte par défaut des postes classés dans cette même OU. À l'ouverture de session avec ce compte, une fenêtre de connexion Bureau à distance (pour ouvrir sa session sur le serveur) se lancera automatiquement.

On attribuera, lors de la création, les paramètres suivants :

	Paramètre
Nom d'ouverture de session	client.yam
Nom complet	Client YAM
Options de mot de passe	L'utilisateur ne peut pas changer de mot de passe Le mot de passe n'expire jamais
Membre de :	GDL_Sources_LS Utilisateurs du domaine

3-3- JOINDRE UN ORDINATEUR AU DOMAINE

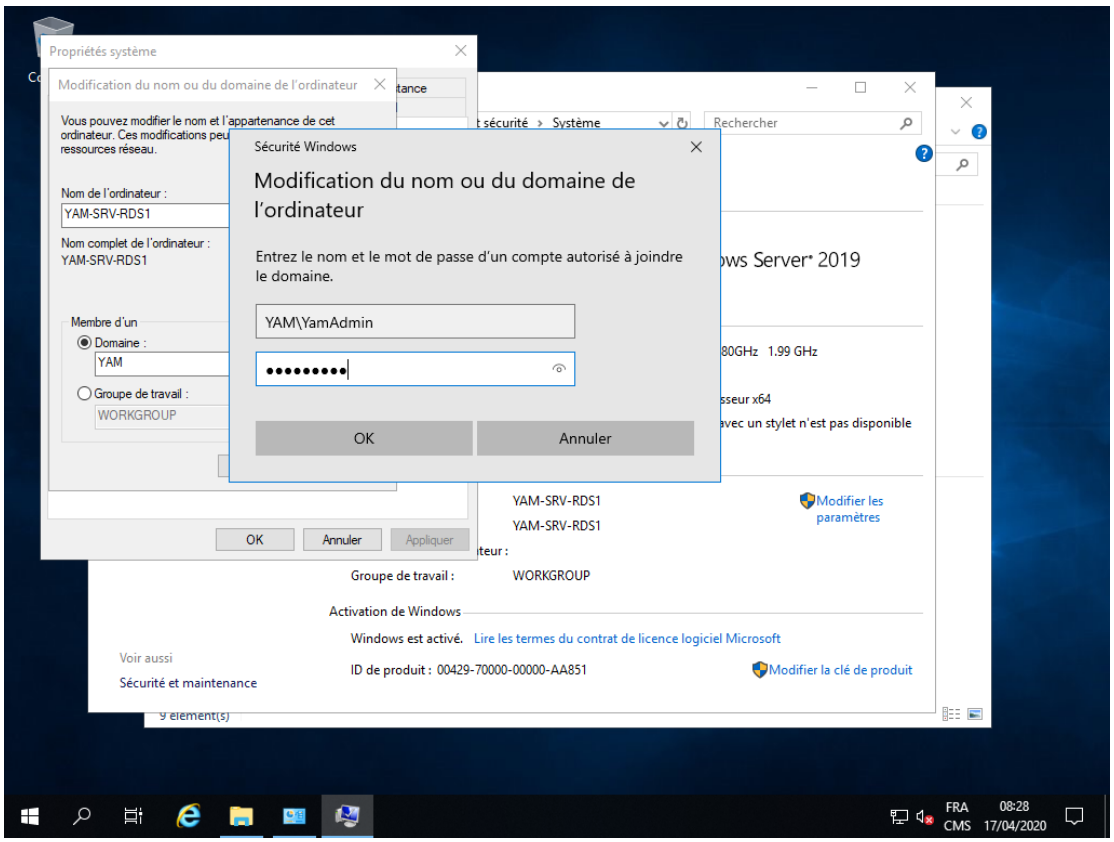
PRÉREQUIS

Avoir un serveur DHCP dans lequel les informations du serveur DNS principal distribuées correspondent au contrôleur de domaine ou bien, si l'adresse IP est attribuée manuellement renseigner le contrôleur de domaine comme DNS principal.

PROCÉDURE

Sur l'ordinateur cible, se rendre dans les **Informations système générales,** puis dans la ligne **Paramètres de nom d'ordinateur, de domaine et de groupe de travail,** cliquer dur **Modifier les paramètres.**

Dans la nouvelle fenêtre, s'assurer de bien être dans l'onglet **Nom de l'ordinateur** et cliquer sur **Modifier** puis, si cela n'a pas été fait, renommer l'ordinateur selon la nomenclature en place, et dans **Membre d'un** : choisir **Domaine** et renseigner **yam.bzh et s'authentifier avec un compte Administrateur du domaine** afin de permettre à l'ordinateur de devenir membre.



L'ordinateur redémarre ensuite, il restera plus qu'à le déplacer de l'OU Computers afin de le placer dans celle correspondante à son rôle, pour rappel :

- **Clients_legers** : Contient les postes en client léger et compte utilisateur approprié.
- **Clients_lourds** : Contient les postes utilisés en tant que client lourd.
- **Hote_RDS** : Contient les VM hôte de session RDS.
- **Serveurs** : Contient les autres serveurs membres du domaine.

3-4- STRATÉGIES DE GROUPES (GPO)

3-4-1- PRÉSENTATION GÉNÉRALE

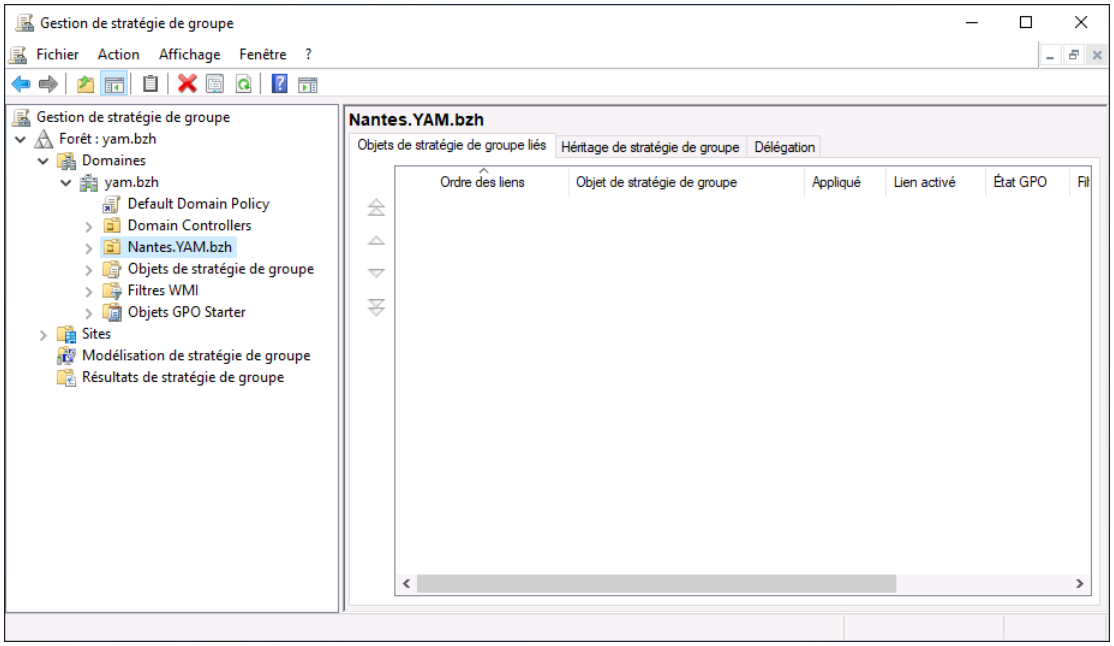
PRÉSENTATION

Les stratégies de groupes vont nous permettre d'automatiser la configuration de l'environnement utilisateur et ordinateur. Cela a pour but principal de simplifier l'administration, mais également homogénéiser la configuration du parc informatique.

Chaque stratégie dispose de ses propres paramètres, qui sont définis en amont par l'équipe informatique (plus précisément par l'administrateur système). Ces paramètres sont ensuite appliqués aux postes de travail, aux utilisateurs et/ou aux serveurs.

CRÉATION D'UNE GPO

La création d'une GPO s'effectue depuis la console Gestion des stratégies de groupe disponible dans les Outils d'administration.



Dérouler la **Forêt : yam.bzh > Domaines > yam.bzh** et se rendre sur **Objets de stratégie de groupe**. Faire un clic-droit et choisir Nouveau, puis nommer la GPO en respectant la nomenclature suivante :

- **GPO_O_RôleStratégie** : lorsqu'il s'agit d'une stratégie s'appliquant sur un Ordinateur.
- **GPO_U_RôleStratégie** : lorsqu'il s'agit d'une stratégie s'appliquant sur un Utilisateur.

Puis dérouler **Objets de stratégie de groupe** et sélectionner la GPO créée précédemment. Faire un clic-droit et choisir **Modifier,** cela ouvrira **l'Éditeur de gestion des stratégies de groupe** dans lequel on pourra appliquer les stratégies souhaitées.

Une fois notre stratégie configurée, il suffit de fermer l'Éditeur de gestion des stratégies de groupe puis d'effectuer **un glisser déposer de la GPO vers UO dans laquelle nous souhaitons appliquer la stratégie.**

On fera attention de ne pas appliquer trop de stratégies par GPO pour des soucis de lisibilité et de gestion de conflits ou d'incidents.

3-3-2- MISE À JOUR DU MAGASIN CENTRAL

Afin d'aligner la version du magasin central du contrôleur de domaine sur la version de Windows 10 la plus récente déployée dans le parc informatique pour avoir accès aux nouvelles stratégies locales, nous procéderons de la manière suivante :

Se connecter au contrôleur de domaine et copier **C:\Windows\PolicyDefinitions** dans **C:\Windows\SYSVOL\domain\Policies**. Cela permettra de publier sur l'ensemble du domaine les stratégies locales à jour.

Puis sur un **poste Windows 10** se connecter avec un compte Admins du domaine et récupérer le contenu de **C:\Windows\PolicyDefinitions** et copier son contenu dans **\\YAM-SRV_MGMT1\sysvol\yam.bzh\Policies\PolicyDefinitions**

3-4-3- MISE EN PLACE DES STRATÉGIES ENVIRONNEMENT UTILISATEUR

CONNEXION DES LECTEURS RÉSEAU

Se référer au paragraphe 5-3- du Serveur de fichiers.

DÉFINIR LE FOND D'ÉCRAN

Créer les GPO suivantes :

Nom GPO	Cible	OU d'application
GPO_U_FondEcran_CLeger	Utilisateur	Clients_legers
GPO_U_FondEcran_Sessions	Utilisateur	Administratif Direction Informatique Produit 1 Produit 2 SAV

Cette GPO permet d'appliquer un fond d'écran aux couleurs de l'entreprise et d'interdire aux utilisateurs sa modification.

Se rendre dans **Configuration utilisateur > Stratégies > Modèles d'administration > Bureau > Bureau > Papier peint du bureau.**

Activer la stratégie, mettre **Style du papier peint** sur **Remplir** et spécifier le chemin d'accès suivant :

- **GPO_U_FondEcran_CL** : \\YAM-SRV-DATA\Sources$\Bureau\PapierPeint\FondEcran_clair.jpg
- **GPO_U_FondEcran_Session** : \\YAM-SRV-DATA\Sources$\Bureau\PapierPeint\FondEcran_sombre.jpg

Fermer la session utilisateur puis se reconnecter pour appliquer la stratégie.

DÉFINIR LE MENU DÉMARRER SUR LES POSTES DE TRAVAIL

Créer les GPO suivantes :

Nom GPO	Cible	OU d'application
GPO_U_MenuDemarrer_CLeger	Utilisateur	Clients_legers
GPO_U_MenuDemarrern_RDS	Utilisateur	Administratif Direction Produit 1 Produit 2 SAV

Ces GPO permettent de définir l'organisation du Menu démarrer et de la barre des tâches. Elle bloque toute possibilité de modification par l'utilisateur de ces éléments.

GPO_U_MenuDemarrer_CLeger :

Se rendre dans le dossier **YAM-SRV-DATA\sources$\Bureau** dans lequel on crée un dossier **MenuDemarrer.** On créer un fichier XML nommé **Demarrer_CLeger.xml** dans lequel on enregistre la commande suivante :

```
<?xml version="1.0" encoding="utf-8"?>
<LayoutModificationTemplate
    xmlns="http://schemas.microsoft.com/Start/2014/LayoutModification"

xmlns:defaultlayout="http://schemas.microsoft.com/Start/2014/FullDefaultL
ayout"
    xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout"
    xmlns:taskbar="http://schemas.microsoft.com/Start/2014/TaskbarLayout"
    Version="1">
  <LayoutOptions StartTileGroupCellWidth="6" />
  <DefaultLayoutOverride>
    <StartLayoutCollection>
      <defaultlayout:StartLayout GroupCellWidth="6">
        <start:Group Name="Connexion à la session">
          <start:DesktopApplicationTile Size="2x2" Column="0" Row="0"
DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start
Menu\Programs\Session_RDS.lnk" />
        </start:Group>
      </defaultlayout:StartLayout>
    </StartLayoutCollection>
  </DefaultLayoutOverride>
  <CustomTaskbarLayoutCollection PinListPlacement="Replace">
    <defaultlayout:TaskbarLayout>
      <taskbar:TaskbarPinList>
        <taskbar:DesktopApp
DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start
Menu\Programs\Session_RDS.lnk" />
      </taskbar:TaskbarPinList>
    </defaultlayout:TaskbarLayout>
 </CustomTaskbarLayoutCollection>
</LayoutModificationTemplate>
```

Puis dans la GPO, se rendre dans **Configuration utilisateur > Stratégies > Modèles d'administration > Menu démarrer et barre des tâches.**

Activer la stratégie **Disposition de l'écran de démarrage** et renseigner l'emplacement du fichier XML : **\\YAM-SRV-DATA\sources$\Bureau\MenuDemarrer\Demarrer_CLeger.xml**

Activer la stratégie **Supprimer la liste Tous les programmes du menu Démarrer** et mettre le paramètre sur **Supprimer et désactiver le paramètre.**

Activer ensuite toutes les stratégies suivantes :

- Empêcher les utilisateurs de personnaliser leur écran de démarrage
- Masquer la zone de notification
- Supprimer l'accès aux menus contextuels pour la barre des tâches
- Supprimer la barre contacts de la barre des tâches
- Supprimer le dossier des utilisateurs du menu Démarrer
- Verrouiller tous les paramètres de la barre des tâches

GPO_U_MenuDemarrern_RDS :

Se rendre dans le dossier **\\YAM-SRV-DATA\sources$\Bureau** dans lequel on crée un dossier **MenuDemarrer**. On créer un fichier XML nommé **Demarrer_RDS.xml** dans lequel on enregistre la commande suivante :

```
<?xml version="1.0" encoding="utf-8"?>
<LayoutModificationTemplate
    xmlns="http://schemas.microsoft.com/Start/2014/LayoutModification"

xmlns:defaultlayout="http://schemas.microsoft.com/Start/2014/FullDefaultL
ayout"
    xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout"
    xmlns:taskbar="http://schemas.microsoft.com/Start/2014/TaskbarLayout"
    Version="1">
  <LayoutOptions StartTileGroupCellWidth="6" />
  <DefaultLayoutOverride>
    <StartLayoutCollection>
      <defaultlayout:StartLayout GroupCellWidth="6">
        <start:Group Name="Bureautique">
          <start:DesktopApplicationTile Size="1x1" Column="4" Row="2"
DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start
Menu\Programs\Accessories\Calculator.lnk" />
```

```
          <start:DesktopApplicationTile Size="2x2" Column="4" Row="0"
DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start
Menu\Programs\PowerPoint.lnk" />
          <start:DesktopApplicationTile Size="2x2" Column="2" Row="0"
DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start
Menu\Programs\Excel.lnk" />
          <start:DesktopApplicationTile Size="1x1" Column="2" Row="2"
DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start
Menu\Programs\Access.lnk" />
          <start:DesktopApplicationTile Size="1x1" Column="1" Row="2"
DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start
Menu\Programs\OneNote 2016.lnk" />
          <start:DesktopApplicationTile Size="2x2" Column="0" Row="0"
DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start
Menu\Programs\Word.lnk" />
          <start:DesktopApplicationTile Size="1x1" Column="3" Row="2"
DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start
Menu\Programs\Publisher.lnk" />
          <start:DesktopApplicationTile Size="1x1" Column="0" Row="2"
DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start
Menu\Programs\Outlook.lnk" />
        </start:Group>
        <start:Group Name="Navigation">
          <start:DesktopApplicationTile Size="2x2" Column="0" Row="0"
DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start
Menu\Programs\Microsoft Edge.lnk" />
          <start:DesktopApplicationTile Size="2x2" Column="2" Row="0"
DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start
Menu\Programs\Firefox.lnk" />
          <start:DesktopApplicationTile Size="2x2" Column="4" Row="0"
DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start
Menu\Programs\OneDrive Entreprise.lnk" />
        </start:Group>
      </defaultlayout:StartLayout>
    </StartLayoutCollection>
  </DefaultLayoutOverride>
  <CustomTaskbarLayoutCollection PinListPlacement="Replace">
    <defaultlayout:TaskbarLayout>
      <taskbar:TaskbarPinList>
        <taskbar:DesktopApp
DesktopApplicationLinkPath="%ALLUSERSPROFILE%\Microsoft\Windows\Start
Menu\Programs\Microsoft Edge.lnk" />
        <taskbar:DesktopApp
DesktopApplicationLinkPath="%APPDATA%\Microsoft\Windows\Start
Menu\Programs\System Tools\File Explorer.lnk" />
      </taskbar:TaskbarPinList>
    </defaultlayout:TaskbarLayout>
 </CustomTaskbarLayoutCollection>
</LayoutModificationTemplate>
```

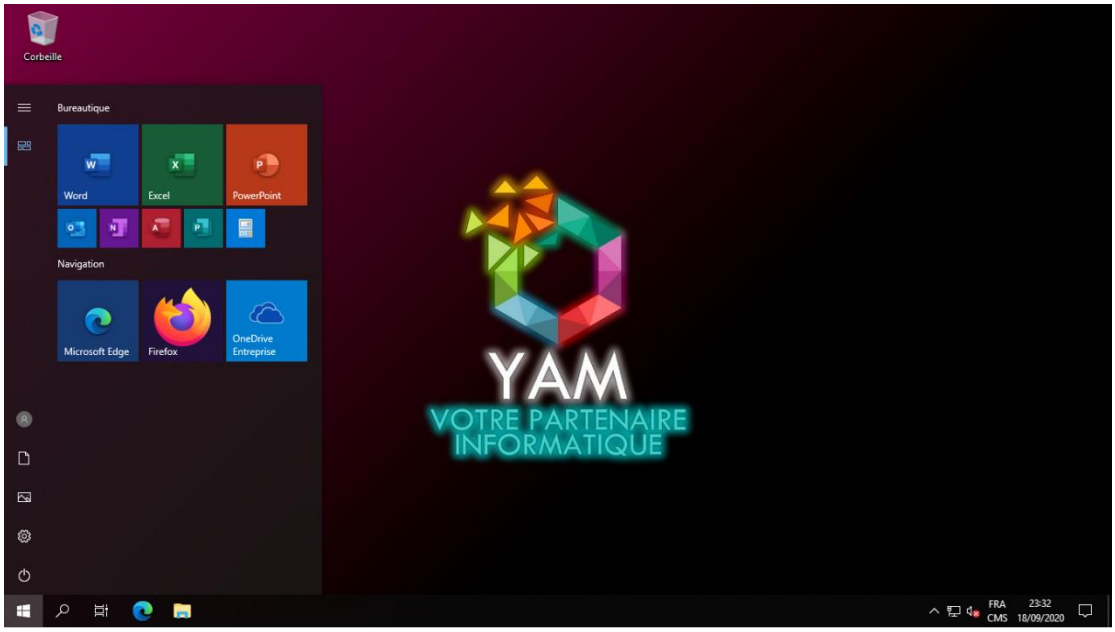
Puis dans la GPO, se rendre dans **Configuration utilisateur > Stratégies > Modèles d'administration > Menu démarrer et barre des tâches.**

Activer la stratégie **Disposition de l'écran de démarrage** et renseigner l'emplacement du fichier XML : **\\YAM-SRV-DATA\sources$\Bureau\MenuDemarrer\Demarrer_CLeger.xml**

Activer la stratégie **Supprimer la liste Tous les programmes du menu Démarrer** et mettre le paramètre sur **Supprimer et désactiver le paramètre.**

Activer ensuite toutes les stratégies suivantes :

- Empêcher les utilisateurs de déplacer la barre des tâches vers un autre point d'ancrage à l'écran
- Ne pas autoriser l'épinglage de programmes à la barre des tâches
- Verrouiller la barre des tâches



Fermer la session utilisateur puis se reconnecter pour appliquer la stratégie.

INSTALLER LES IMPRIMANTES RÉSEAU

Se référer au paragraphe 4-3- des Services d'impressions.

LANCER LA CONNEXION RDS AU DÉMARRAGE DU CLIENT LÉGER

Créer la GPO suivante :

Nom GPO	Cible	OU d'application
GPO_U_Demarrer_ConnexionRDS	Utilisateur	Clients_legers

Cette GPO permet **dès l'ouverture de session locale de démarrer la connexion Bureau à distance** pour que les utilisateurs puissent s'authentifier et ouvrir leur session distante.

Se rendre dans le dossier **YAM-SRV-DATA\Sources$** dans lequel on crée un dossier **Logiciels** puis à l'intérieur un autre dossier **RDP**.

Puis ouvrir Connexion Bureau à distance (mstsc.exe) et renseigner les informations suivantes :

- **Onglet Général** : Dans Ordinateur, saisir l'IP du serveur RDS
- **Onglet Affichage** : Cocher Utiliser tous les moniteurs pour la session à distance
- **Onglet Ressources locales** : Dans Ressources locales, décocher Imprimantes et Presse-papier, puis cliquer sur autres et tout décocher.

Puis retourner sur l'onglet Général et cliquer sur Enregistrer sous pour créer le fichier RDS.rdp dans **YAM-SRV-DATA\sources$\Logiciels\RDP**.

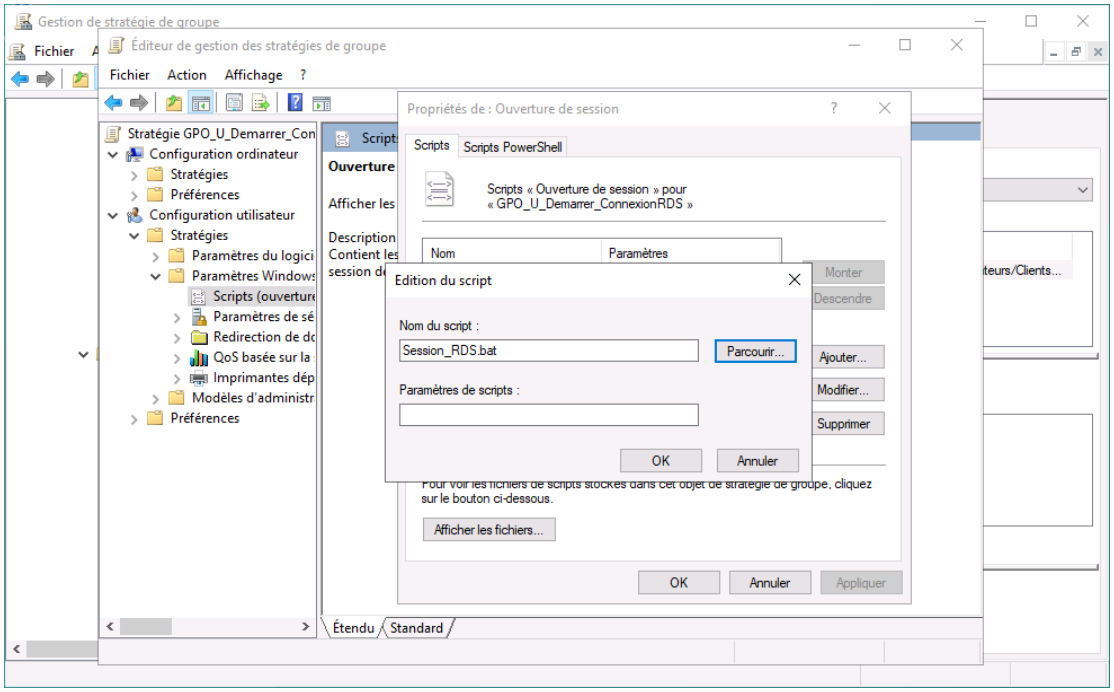
On créer un script nommé Session_RDS.bat dans lequel on enregistre la commande suivante :

```
\\YAM-SRV-DATA\sources$\Logiciels\RDP\RDS.rdp
```

On l'enregistre (l'emplacement n'a pas d'importance à ce stade).

Puis, dans la GPO, se rendre **dans Configuration utilisateur > Stratégies > Paramètres Windows > Scripts**.

Double-cliquer sur **Ouverture de session** et dans l'onglet Scripts, cliquer sur **Ajouter** puis dans la nouvelle fenêtre sur **Parcourir**. L'emplacement proposé par défaut est celui utilisé pour publier la GPO, on y collera donc le script créé précédemment puis on le sélectionne. En enfin on clique sur OK dans les fenêtres ouvertes.



Fermer la session utilisateur puis se reconnecter pour appliquer la stratégie.

3-4-4- MISE EN PLACE DES STRATÉGIES DE SÉCURITÉ

APPLIQUER LA POLITIQUE DE MISES À JOUR WINDOWS

Se référer au paragraphe 6-3- des Services WSUS.

CRÉER UN AUDIT DE SÉCURITÉ

Créer la GPO suivante :

Nom GPO	Cible	OU d'application
GPO_O_Audit_Securite	Ordinateur	Domain Controllers

Cette GPO permet d'inscrire dans l'observateur d'événement du contrôleur de domaine tous les échecs de tentative de connexion au serveur ainsi que tous les échecs de connexion aux comptes de l'AD.

Dans la GPO, se rendre dans **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Stratégies d'audit**.

Définir les paramètres de stratégies pour :

- Auditer les événements de connexion : **Échec**
- Auditer les événements de connexion aux comptes : **Échec**

DÉFINIR LA STRATÉGIE DE MOTS DE PASSE

Créer la GPO suivante :

Nom GPO	Cible	OU d'application
GPO_O_MotDePasse	Ordinateur	Clients_lourds Hote_RDS

Cette GPO définit les exigences de sécurité des mots de passe utilisateur :

- Au moins 8 caractères avec 3 des 4 types suivants : Minuscules, Majuscules, Chiffres, Symboles
- À modifier tous les 90 jours.
- Session bloquée pendant 30 min si 5 échecs de connexion.

Dans la GPO, se rendre dans **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes**.

Dans **Stratégie de mot de passe,** définir les paramètres suivants :

- Durée de vie maximale du mot de passe : **90 jours**
- Durée de vie minimale du mot de passe : **0 jours**
- Le mot de passe doit respecter des exigences de complexité : **Activé**
- Longueur minimale du mot de passe : **8 caractères**

Dans **Stratégie de verrouillage de compte,** définir les paramètres suivants :

- Durée de verrouillage des comptes : **30 minutes**
- Réinitialiser le compteur de verrouillage du compte après : **30 minutes**
- Seuil de verrouillage du compte : **5 tentatives d'ouverture de session**

Redémarrer les ordinateurs concernés pour appliquer la stratégie.

DÉSACTIVER LE MONITEUR D'ÉVÉNEMENT DE MISE HORS TENSION

Créer la GPO suivante :

Nom GPO	Cible	OU d'application
GPO_O_MoniteurHT	Ordinateur	Hote_RDS

Cette GPO désactive sur les hôtes de session RDS le moniteur d'événement de mise hors tension. La boite de dialogue demandant la raison de l'arrêt ou du redémarrage ne s'affichera plus ni

celle apparaissant sur toutes les sessions utilisateur au redémarrage lorsque le système a redémarré de manière imprévue.

Dans la GPO, se rendre dans **Configuration ordinateur > Stratégies > Modèles d'administration > Système.**

Désactiver la stratégie **Afficher le moniteur d'événements de mise hors tension.**

Redémarrer les ordinateurs concernés pour appliquer la stratégie.

DROITS D'OUVERTURE DE SESSION SUR CLIENT LÉGER

Créer la GPO suivante :

Nom GPO	Cible	OU d'application
GPO_O_Groupe_CLegers	Ordinateur	Clients_legers

Cette GPO permet **d'interdire la direction d'ouvrir une session à tout groupe en dehors du compte dédié à l'ouverture de session et au service informatique** et d'accorder les droits d'administrateur local aux membres de l'informatique.

Dans la GPO, se rendre dans **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur**. Chercher les lignes **Interdire l'ouverture d'une session locale** et **Interdire l'ouverture de session par les services Bureau à distance** et y ajouter les groupes suivants :

- GG_Administratif
- GG_Direction
- GG_Produit1
- GG_Produit2
- GG_SAV

Puis se rendre dans **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Groupes restreints.** Faire un clic-droit dans volet droit > **Ajouter un groupe…**, sélectionner **GG_Informatique** et cliquer sur OK, puis sur la nouvelle fenêtre ajouter le groupe **Administrateurs** dans **Ce groupe est membre de :**, et cliquer sur OK.

Redémarrer les ordinateurs concernés pour appliquer la stratégie.

DROITS D'OUVERTURE DE SESSION ET PRIVILÈGES SUR CLIENT LOURD

Créer la GPO suivante :

Nom GPO	Cible	OU d'application
GPO_O_Groupe_CLourds	Ordinateur	Clients_lourds

Cette GPO permet **d'autoriser uniquement la direction et les services administratifs et informatique d'ouvrir une session** sur n'importe quel poste client lourd avec les **droits d'Administrateur local** autorisant ainsi l'installation de logiciels ou la modification de l'heure.

Dans la GPO, se rendre dans **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur**. Chercher les lignes **Interdire l'ouverture d'une session locale** et **Interdire l'ouverture de session par les services Bureau à distance** et y ajouter les groupes suivants :

- GG_Produit1
- GG_Produit2
- GG_SAV

Puis se rendre dans **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Groupes restreints.** Faire un clic-droit dans volet droit > **Ajouter un groupe…**, sélectionner **GG_Direction** et cliquer sur OK, puis sur la nouvelle fenêtre ajouter le groupe **Administrateurs** dans **Ce groupe est membre de :**, et cliquer sur OK.

Faire de même pour le groupe **GG_Informatique.**

Redémarrer les ordinateurs concernés pour appliquer la stratégie.

DROITS D'OUVERTURE DE SESSION SUR SESSION RDS

Créer la GPO suivante :

Nom GPO	Cible	OU d'application
GPO_O_Groupe_RDS	Ordinateur	Hote_RDS

Cette GPO permet **d'interdire la direction et le service administratif d'ouvrir une session RDS** et d'accorder les droits d'administrateur local aux membres de l'informatique.

Dans la GPO, se rendre dans **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur.** Chercher les lignes **Interdire l'ouverture d'une session locale** et **Interdire l'ouverture de session par les services Bureau à distance** et y ajouter les groupes suivants :

- GG_Direction
- GG_Administratif

Puis se rendre dans **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Groupes restreints.** Faire un clic-droit dans volet droit > **Ajouter un groupe…**, sélectionner **GG_Informatique** et cliquer sur OK, puis sur la nouvelle fenêtre ajouter le groupe **Administrateurs** dans **Ce groupe est membre de :**, et cliquer sur OK.

Redémarrer les ordinateurs concernés pour appliquer la stratégie.

INTERDIRE L'ACCÈS AUX LECTEURS AMOVIBLES

Créer la GPO suivante :

Nom GPO	Cible	OU d'application
GPO_U_Refuser_LecteurAmovible	Utilisateur	Clients_legers Produit 1 Produit 2 SAV

Cette GPO **interdit l'accès à tous les lecteurs amovibles** (Lecteurs CD/DVD/BD, clé USB ou disque dur externe, lecteur de disquettes (oui ça existe encore), etc.) qu'un utilisateur pourrait brancher sur son poste, ceci afin d'éviter un risque d'attaque du réseau de l'entreprise par un périphérique infecté par exemple et limiter les risques de vol de données confidentielles.

Elle permet également de **masquer les lecteurs locaux** de manière que les utilisateurs utilisent uniquement les lecteurs partagés mis à leur disposition.

Dans la GPO, se rendre dans **Configuration utilisateur > Stratégies > Modèles d'administration** :

Pour l'interdiction accès aux lecteurs amovibles : **Système > Accès au stockage** amovible et activer la stratégie **Toutes les classes de stockage amovible : refuser tous les accès.**

Pour masquer les lecteurs locaux : **Composants Windows > Explorateur de fichiers** et activer la stratégie **Dans Poste de travail, masquer ces lecteurs spécifiés** et choisir **Restreindre aux lecteurs A, B, C et D.**

Fermer la session utilisateur puis se reconnecter pour appliquer la stratégie.

MODIFICATION DE L'HEURE SYSTÈME

Créer les GPO suivantes :

Nom GPO	Cible	OU d'application
GPO_O_ModifHeure_Client	Ordinateur	Clients_legers Clients_lourds
GPO_O_ModifHeure_Serveur	Ordinateur	Hote_RDS Serveurs

Cette GPO permet de définir les utilisateurs autorisés à modifier l'heure du système.

Dans la GPO, se rendre dans **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur,** et appliquer les paramètres suivants dans Modifier l'heure système :

- GPO_O_ModifHeure_Client : Groupes Admins du domaine, GG_Direction et GG_Informatique
- GPO_O_ModifHeure_Client : Groupe Admins du domaine

Redémarrer les ordinateurs concernés pour appliquer la stratégie.

NETTOYAGE AUTOMATIQUE DU DOSSIER UTILISATEUR DU CLIENT LÉGER

Créer la GPO suivante :

Nom GPO	Cible	OU d'application
GPO_U_Script_Nettoyage_CLeger	Utilisateur	Clients_legers

Cette GPO permet **la suppression automatique de tout fichier enregistré dans le dossier utilisateur du compte Client YAM du client léger dès la fermeture de session.** Ce compte ne servant qu'à ouvrir une session sur le serveur, il n'est donc pas destiné à l'enregistrement de fichiers.

On créer un script PowerShell nommé **Nettoyage.ps1** dans lequel on enregistre la commande suivante :

```
$username = $env:UserName
Remove-Item C:\Users\$username\Desktop\*.* -Force
Remove-Item C:\Users\$username\Contacts\*.* -Force
```

```
Remove-Item C:\Users\$username\Documents\*.* -Force
Remove-Item C:\Users\$username\Favorites\*.* -Force
Remove-Item C:\Users\$username\Pictures\*.* -Force
Remove-Item C:\Users\$username\Links\*.* -Force -Exclude desktop.lnk,
downloads.lnk
Remove-Item C:\Users\$username\Music\*.* -Force
Remove-Item "C:\Users\$username\3D Objects\*.*" -Force
Remove-Item "C:\Users\$username\Saved Games\*.*" -Force
Remove-Item C:\Users\$username\Searches\*.* -Force
Remove-Item C:\Users\$username\Downloads\*.* -Force
Remove-Item C:\Users\$username\Videos\*.* -Force
```

On l'enregistre (l'emplacement n'a pas d'importance à ce stade).

Puis, dans la GPO, se rendre **dans Configuration utilisateur > Stratégies > Paramètres Windows > Scripts**.

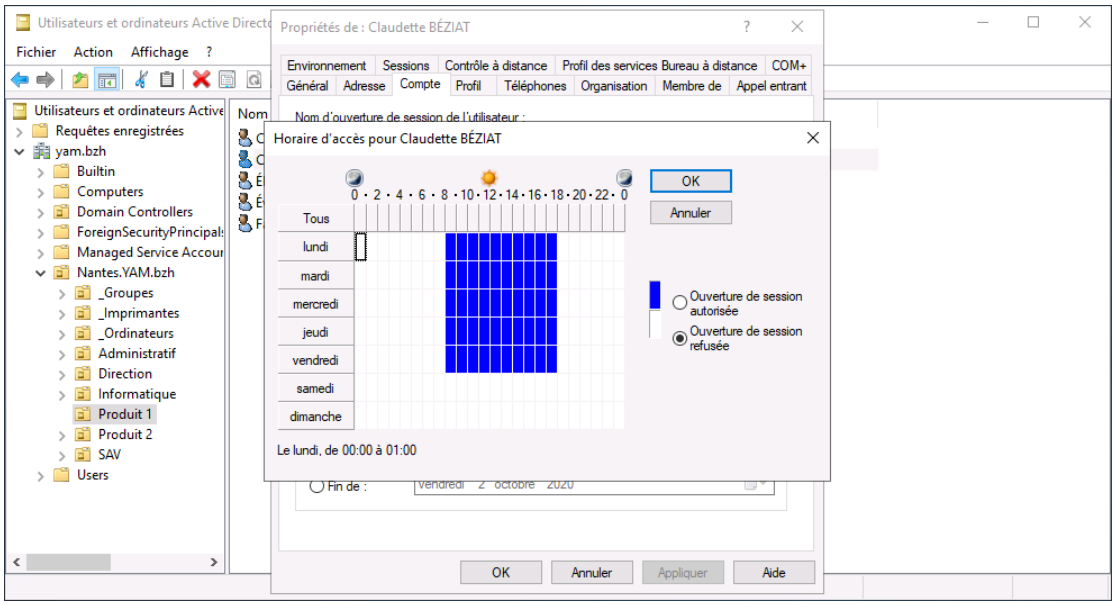
Double-cliquer sur **Fermeture de session** et dans l'onglet **Scripts PowerShell,** cliquer sur **Ajouter** puis dans la nouvelle fenêtre sur **Parcourir**. L'emplacement proposé par défaut est celui utilisé pour publier la GPO, on y collera donc le script créé précédemment puis on le sélectionne. En enfin on clique sur OK dans les fenêtres ouvertes.

Fermer la session utilisateur puis se reconnecter pour appliquer la stratégie.

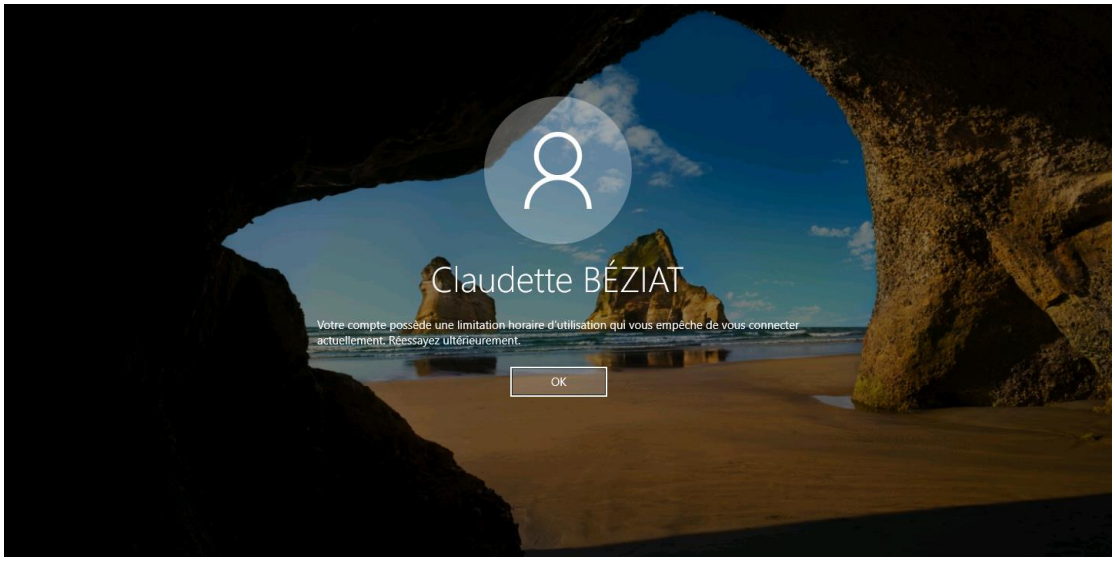
RESTRICTIONS D'HORAIRES DE CONNEXION

Afin de respecter le cahier des charges certains utilisateurs sont soumis à des restrictions horaires.

Dans cet exemple, l'utilisatrice Claudette BÉZIAT, est autorisée à ouvrir sa session du lundi au vendredi, de 8h à 18h (zone en bleu). **Ce paramétrage ne s'applique qu'à l'ouverture de session, et ne la ferme pas automatiquement**. Cela veut dire que si cette utilisatrice est connectée à sa session avant 18h, elle ne sera pas déconnectée passer cette heure.



En revanche, si Claudette BÉZIAT tente d'ouvrir sa session après 18h, un message lui indiquera qu'elle n'est pas autorisée à se connecter à sa session :



FORCER LA FERMETURE DE SESSION À UNE HEURE FIXE

Créer la GPO suivantes :

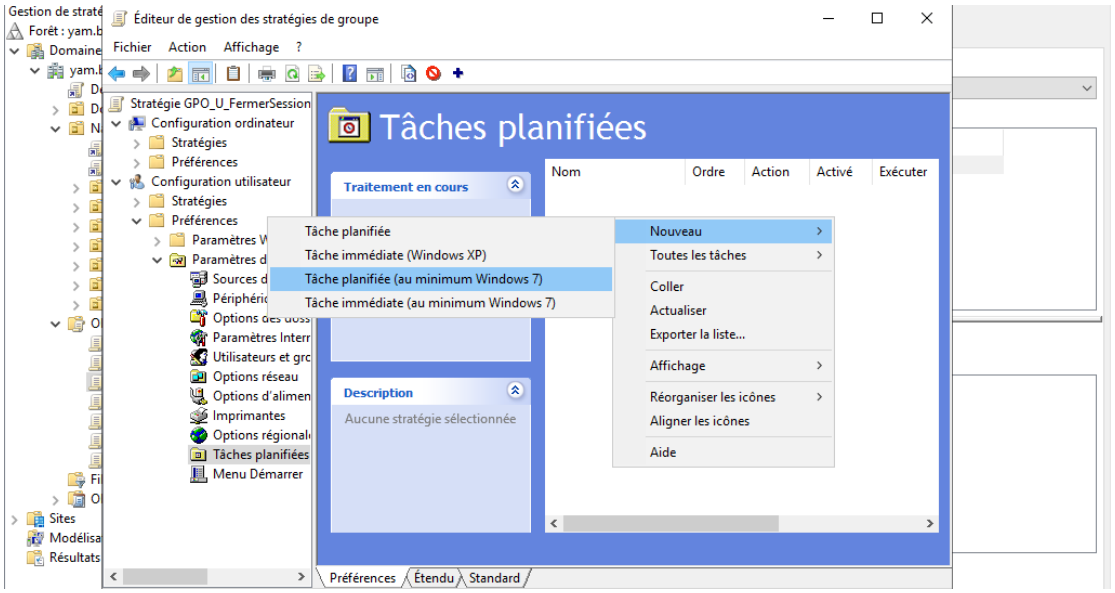
Nom GPO	Cible	OU d'application
GPO_U_FermerSession	Utilisateur	Administratif Produit 1et Produit 2

Nous mettons en place un script qui paramètre une fermeture forcée de la session à l'heure définie (19h ou 20h). Cette commande a donc pour but de fermer la session ainsi que tous les programmes ouverts. Nous enregistrons cela dans le **dossier caché partagé \\YAM-SRV-DATA\Sources$\Scripts\FermerSession.bat** accessible en lecture seule à tous les utilisateurs.

Le script contiendra la commande suivante :

```
Shutdown.exe /l /f
```

Modifier la GPO **GPU_U_FermerSession** et se rendre dans **Configuration utilisateur > Préférences > Paramètres du panneau de configuration > Tâches planifiées**. Puis faire un **clic-droit > Nouveau > Tâche planifiée (au minimum Windows 7).**



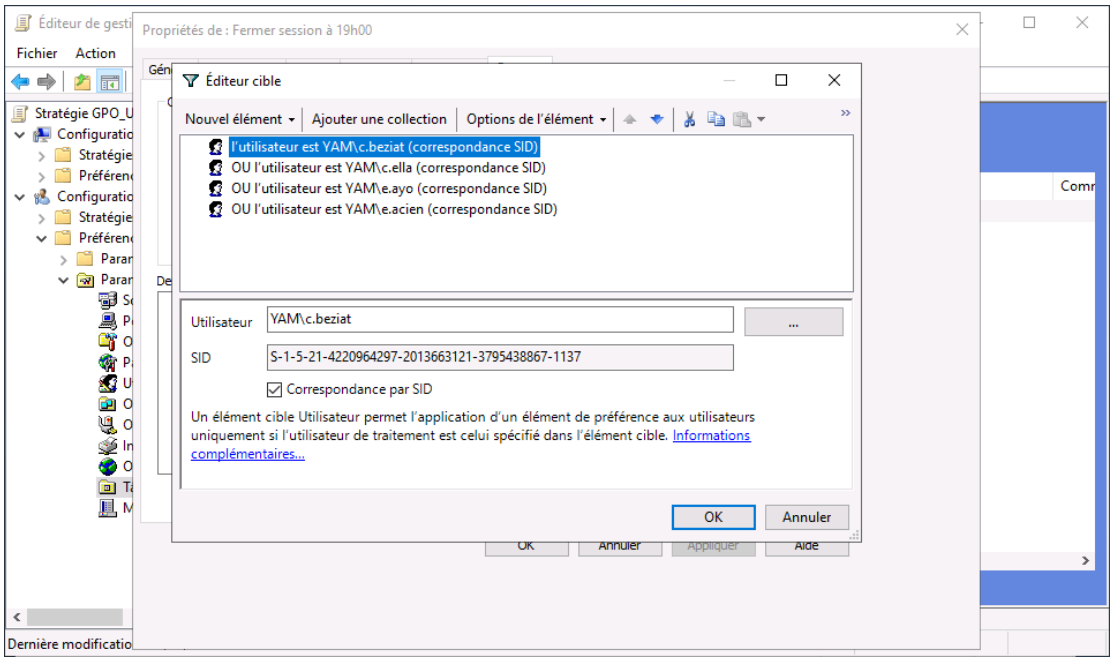
Dans l'onglet **Général,** nommer la tâche : **Fermer session à 19h00** et sélectionner **N'exécuter que si l'utilisateur est connecté**.

Dans l'onglet **Déclencheur,** cliquer sur **Nouveau…** puis dans la nouvelle fenêtre choisir **Commencer la tâche : À l'heure programmée,** dans Paramètres sélectionner **Tous les jours** et régler l'heure sur **19h00** et cocher la case **Activée** en bas puis cliquer sur **OK**.

Depuis l'onglet **Actions,** nous cliquons sur **Nouveau,** on sélectionne **Action : Démarrer un programme** et allons pointer sur notre fichier .bat

Uniquement pour la tâche planifiée à 19h : Puis dans l'onglet **Commun,** cocher **Ciblage au niveau de l'élément** et cliquer sur le bouton **Ciblage…**

Dans la fenêtre Éditeur cible cliquer sur **Nouvel élément > Utilisateur** et sélectionner **c.beziat,** puis ajouter **c.ella, e.ayo** et **e.acien** et faire un clic-droit sur ces trois derniers utilisateurs une fois ajoutés dans la liste et choisir **Option de l'élément > Ou**.



Cliquer sur OK pour fermer l'Éditeur cible, faire de même pour la tâche planifiée.

Puis **recréer une autre tâche planifiée pour 20h,** procéder de la même manière en appliquant nom et horaires sur 20h00 à l'exception de l'onglet Commun qui ne s'applique pas pour cette heure.

Fermer la session utilisateur puis se reconnecter pour appliquer la stratégie.

3-5- QUOTAS

INTRODUCTION

Afin de limiter la quantité de données enregistrées par les utilisateurs sur leurs postes, nous créons une règle de quotas. La décision a été prise de fixer une limite de 5Go par utilisateur avec une alerte en cas de dépassement.

Nous appliquons ensuite automatiquement le modèle de cette règle de quotas, à chaque dossier Commun propre à chaque service. Ce quota s'applique également aux sous-dossiers existants, et s'appliquera aussi à chaque sous-dossier créé ultérieurement. Cela nous évitera de devoir appliquer manuellement cette règle à chaque création de sous-dossier.

CRÉATION DU MODÈLE

Prérequis : Avoir installé le rôle **Service de fichiers et de stockage** avec le **gestionnaire de ressources du serveur de fichiers.**

Dans la console Gestionnaire de ressources du serveur de fichiers, se rendre dans **Gestion de quotas > Modèle de quotas** afin de créer un modèle qui sera appliqué à tous les dossiers cibles.

Cliquer sur Créer un modèle de quotas et le nommer **Limite 5 Go avec alerte en cas de dépassement**. Définir la limite d'espace à **5 Go** et cocher **Quotas conditionnel.**

Dans **Seuils de notification** on appliquera un avertissement en cas d'utilisation de **100% ou plus** de la capacité de stockage et on génèrera une alerte dans le **Journal des évènements.**

MISE EN PLACE

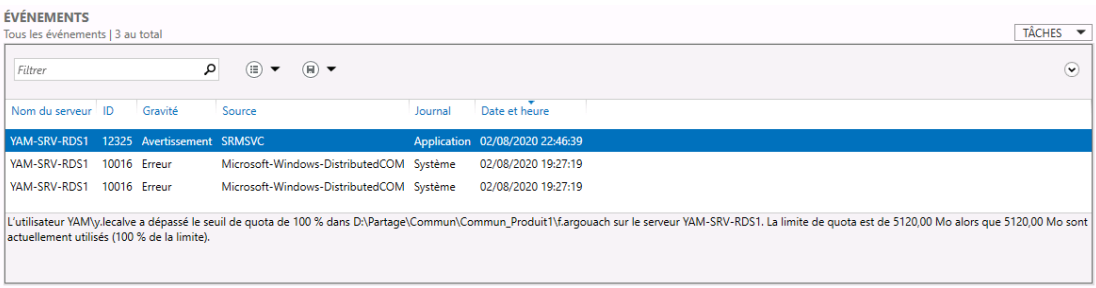
Se rendre dans **Gestion de quotas > Quotas** et cliquer sur **Créer un quota.**

Sélectionner **Appliquer automatiquement le modèle et créer des quotas sur les sous-dossiers existants et nouveaux.**

Puis choisir dans la liste déroulante le modèle créé précédemment.

SUIVI DES ALERTES

Et enfin lorsqu'un utilisateur atteint le seuil de ce quota, voici l'exemple d'avertissement reçu par l'équipe informatique dans le gestionnaire de serveur :



YAM
VOTRE PARTENAIRE INFORMATIQUE

4- SERVICE D'IMPRESSION

INTRODUCTION

Sur le même principe que pour le partage des dossiers, nous avons fait le choix de créer une unité d'organisation pour la gestion des droits des imprimantes et des impressions.

CONTEXTE

Nous avons aussi des contraintes de priorité d'impressions à mettre en place pour l'équipe de direction. Nous avons donc choisi de créer 3 imprimantes ***Commun*** qui pointent toutes vers la même imprimante ***PRINT_COMMUN_DIR***, mais sur laquelle la direction est prioritaire (priorité 1). Cela veut dire que si plusieurs utilisateurs issus de différents services, lancent en même temps une impression sur la même imprimante, c'est l'utilisateur faisant parti du groupe ***Direction*** qui verra s'effectuer son impression en premier.

Nous mettons également en place une GPO pour l'installation automatique des imprimantes. À noter que les administrateurs (l'équipe informatique) ont un droit d'accès total sur l'ensemble des imprimantes.

INSTALLATION DU RÔLE

Nous commençons donc par ajouter le rôle **Services d'impression et de numérisation des documents**, puis nous sélectionnons le service du rôle **Serveur d'impression**, ce qui va nous permettre de gérer plusieurs imprimantes.

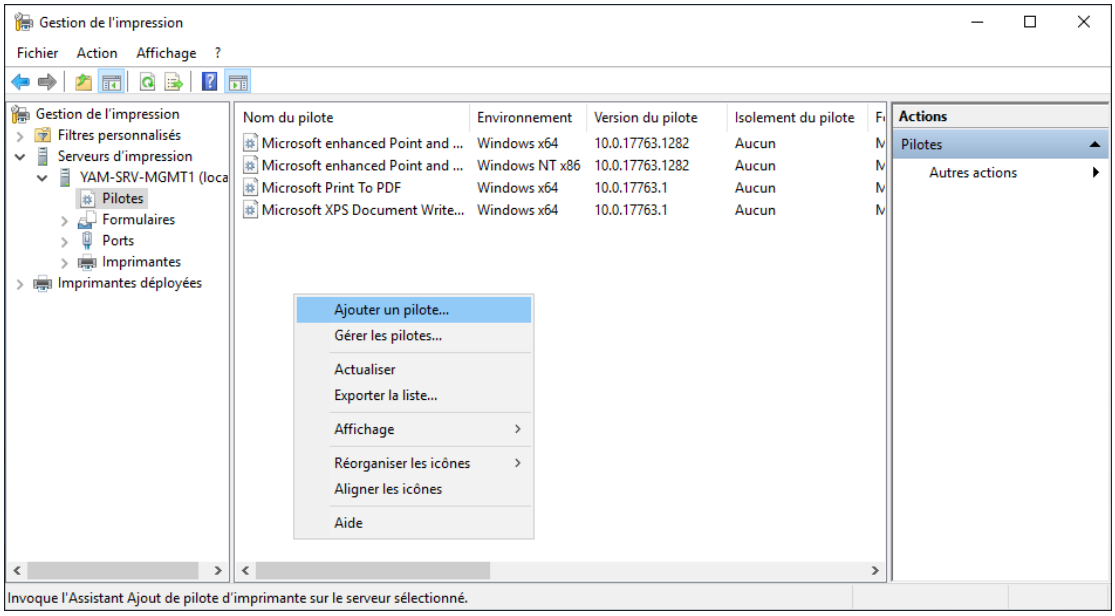
4-1- INSTALLATION DES IMPRIMANTES

Le tableau ci-dessous résume la liste des imprimantes à installer avec leurs propriétés :

Nom imprimante	Port	IP	Priorité
PRINT_COMMUN_0817	PRINT_COMMUN	172.16.100.20	2
PRINT_COMMUN_24	PRINT_COMMUN	172.16.100.20	2
PRINT_COMMUN_DIR	PRINT_COMMUN	172.16.100.20	1
PRINT_ADMINISTRATIF	PRINT_ADMINISTRATIF	172.16.100.21	1
PRINT_DIRECTION	PRINT_DIRECTION	172.16.100.22	1
PRINT_INFORMATIQUE	PRINT_INFORMATIQUE	172.16.100.23	1
PRINT_PRODUIT1	PRINT_PRODUIT1	172.16.100.24	1
PRINT_PRODUIT2	PRINT_PRODUIT2	172.16.100.25	1
PRINT_SAV	PRINT_SAV	172.16.100.26	1

Démarrer la console **Gestion de l'impression.**

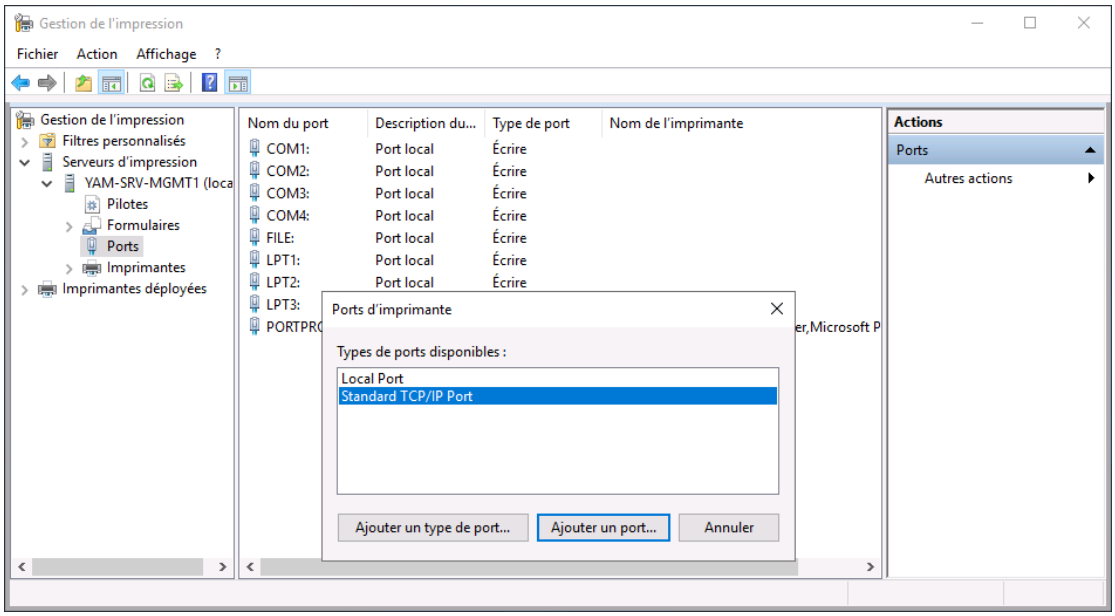
1- Nous ajoutons le **pilote de l'imprimante.** Se déplacer dans **Serveurs d'impression > YAM-SRV-MGMT > Pilotes** puis faire un clic-droit et choisir **Ajouter un pilote…**



Dans l'assistant, Nous choisissons uniquement comme architecture de processeur **x64** car le parc informatique est sur ce type de processeur.

Puis dans la sélection du pilote, cliquer sur **Windows Update** afin de charger tous les pilotes disponibles, patienter le temps que la recherche en ligne s'effectue puis sélectionner la marque et le modèle de l'imprimante. Notre pilote est désormais ajouté.

2- Nous ajoutons ensuite les **ports** par rapport à leurs adresses IP. Se déplacer dans **Serveurs d'impression > YAM-SRV-MGMT > Ports** puis faire un clic-droit et choisir **Ajouter un port…**

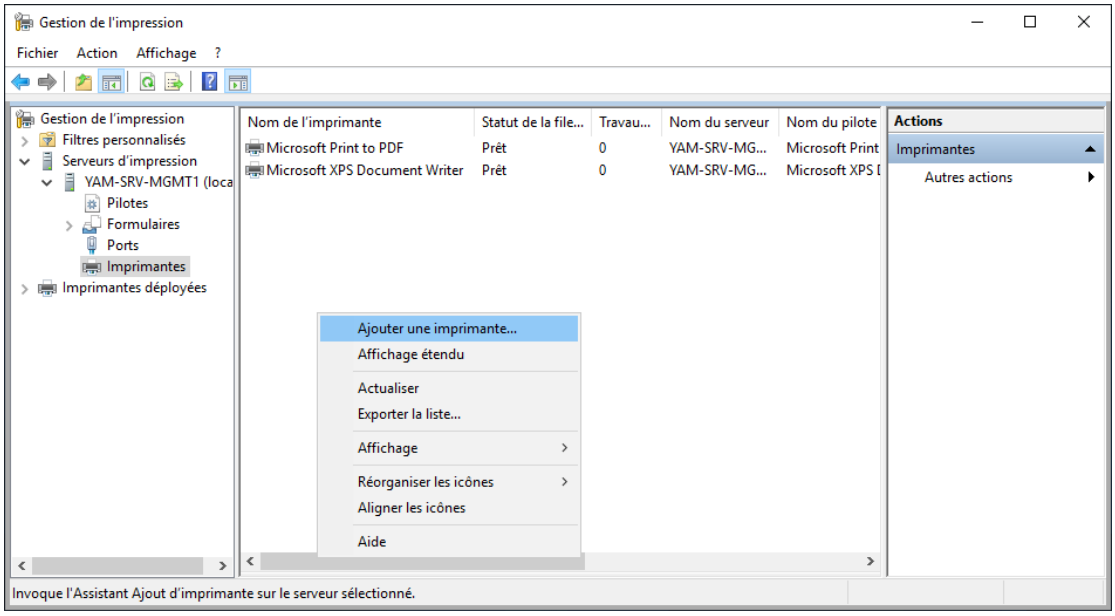


Choisir **Standard TCP/IP Port** et cliquer sur **Ajouter un port.** Nous entrons ensuite l'adresse IP de l'imprimante puis nous nommons son port.

L'opération est à répéter pour l'ensemble des imprimantes.

3- Nous devons ensuite ajouter les imprimantes une à une, cette fois-ci en choisissant de les ajouter via les ports existants que nous venons de créer. Se déplacer dans **Serveurs**

d'impression > YAM-SRV-MGMT > Imprimantes puis faire un clic-droit et choisir **Ajouter une imprimante…**



Sélectionner dans la liste déroulante **le port existant correspondant à l'imprimante à installer,** puis choisir ensuite le pilote que nous venons d'installer.

Nous activons le partage des imprimantes (qui servent aux différents utilisateurs des différents groupes), et nommons ces partages à l'identique du nommage des imprimantes.

Nous terminons l'installation.

L'opération est à répéter pour l'ensemble des imprimantes.

4-2- GESTION DES DROITS

DROITS D'ACCÈS

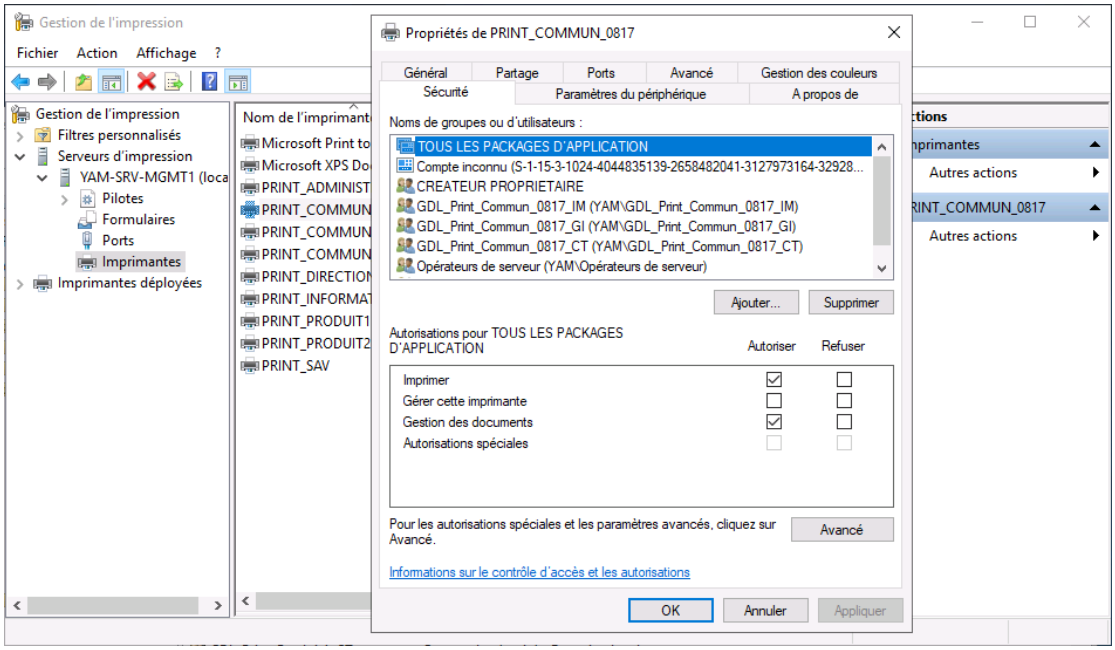
En ce qui concerne la gestion des imprimantes, les droits sont gérés, comme vu précédemment, depuis la console **Utilisateurs et ordinateurs Active Directory** dans l'OU _Imprimantes. Pour rappel les différents droits d'accès sont :

Nom du groupe	Niveau d'accès
GDL_Print_Service_CT	Contrôle total
GDL_Print_Service_GI	Gestion des imprimantes
GDL_Print_Service_IM	Impression seule

Une fois les GDL créés pour chacune des imprimantes partagées, nous rendons membre les GG des services du GDL de l'imprimante correspondant aux droits que nous souhaitons appliquer.

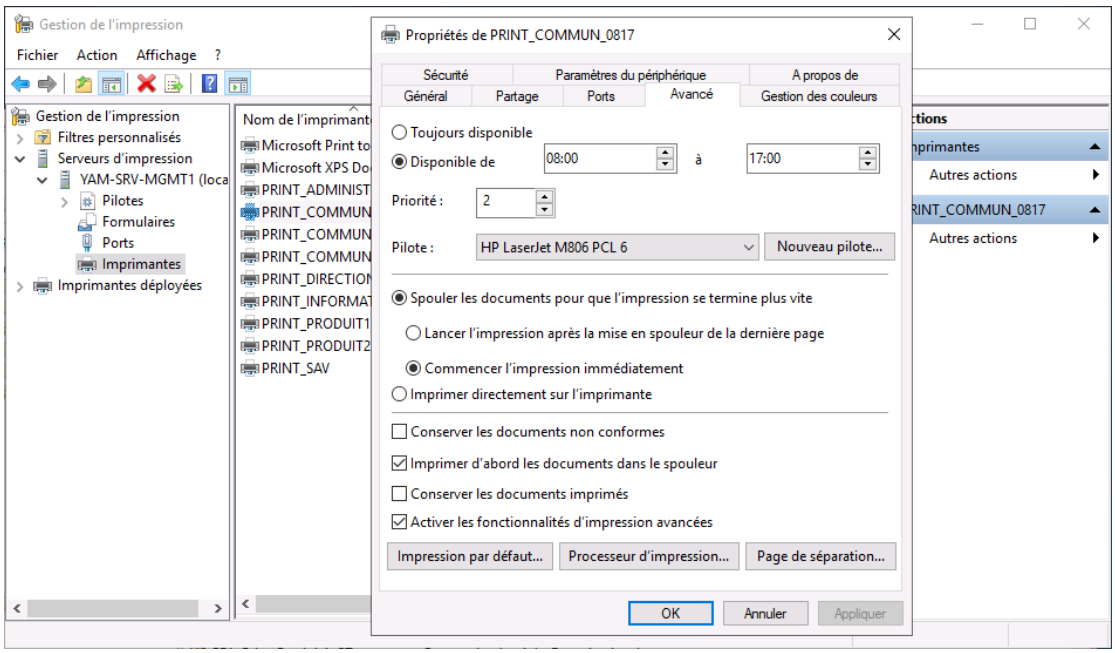
Pour cela, faire un clic-droit sur l'imprimante et choisir **Propriétés** :

Se rendre dans l'onglet **Sécurité** et y ajouter nos GDL et leur attribuer les droits correspondants.



S'il y a des restrictions horaires et/ou des priorités à appliquer, se rendre dans l'onglet **Avancé.**

Sélectionner **Disponible de** et indiquer le créneau horaire, puis **régler la priorité sur 2** si on souhaite abaisser la priorité de l'imprimante. Nous prenons exemple ici de l'imprimante de la direction, mais pour laquelle les utilisateurs définis ne sont pas prioritaires (priorité 2) et ont des restrictions horaires d'utilisation (de 8h à 17h).



YAM
VOTRE PARTENAIRE INFORMATIQUE

ATTRIBUTION DES DROITS AUX SERVICES

On attribue maintenant les droits aux GG_Services selon les indications du tableau ci-dessous :

Groupe global (GG)	Membre de :
GG_ Administratif	GDL_Print_Administratif_IM GDL_Print_Commun_24_IM
GG_Direction	GDL_Print_Commun_Dir_IM GDL_Print_Direction_24_IM
GG_Informatique	GDL_Print_Administratif_CT GDL_Print_Commun_0817_CT GDL_Print_Commun_24_CT GDL_Print_Commun_Dir_CT GDL_Print_Informatique_CT GDL_Print_Produit1_CT GDL_Print_Produit2_CT GDL_Print_SAV_CT
GG_Produit1	GDL_Print_Commun_0817_IM GDL_Print_Produit1_IM
GG_Produit2	GDL_Print_Commun_0817_IM GDL_Print_Produit2_IM
GG_SAV	GDL_Print_Commun_24_IM GDL_Print_SAV_IM
Utilisateurs a.ada et l.laporte	GDL_Print_Informatique_IM GDL_Print_Produit1_IM GDL_Print_Produit2_IM

4-3- MISE EN PLACE DE LA STRATÉGIE DE GROUPE

Nous nous rendons ensuite dans l'éditeur de gestion des stratégies de groupe. Nous ajoutons une imprimante partagée, afin de mettre en place la stratégie pour installer automatiquement les imprimantes sur les différents postes de travail.

Créer la GPO suivante :

Nom GPO	Cible	OU d'application
GPO_U_Imprimante	Utilisateur	Administratif Direction Informatique Produit 1 Produit 2 SAV

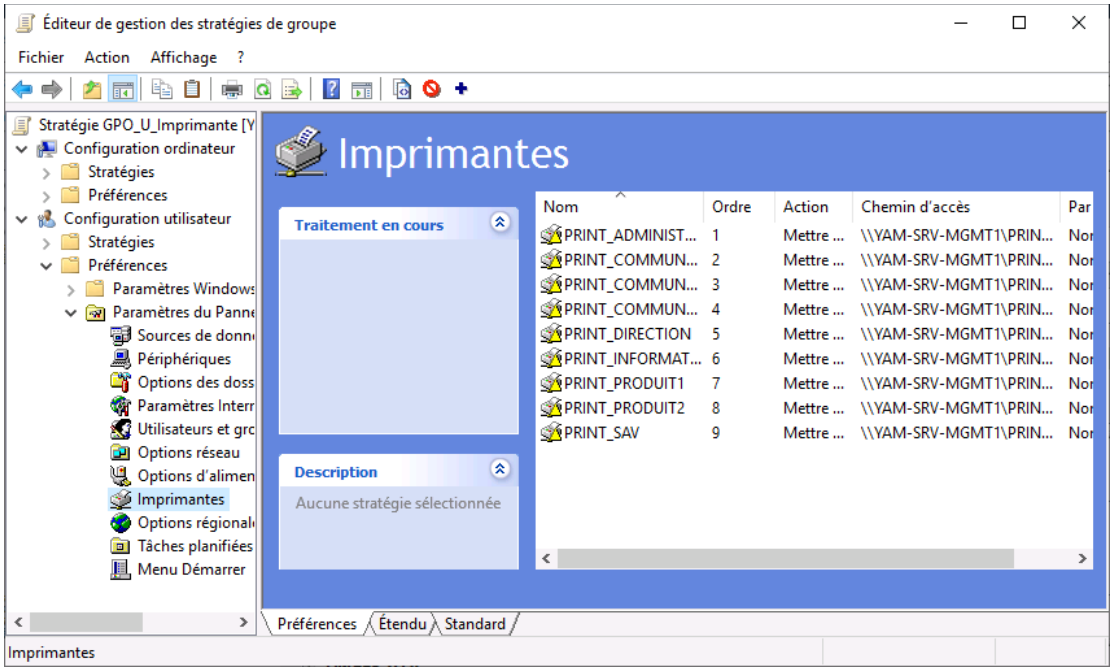
Cette GPO permet l'installation automatique des imprimantes partagé. Seules les imprimantes pour lesquelles l'utilisateur connecté a les droits d'impression seront installées.

Se rendre dans **Configuration utilisateur > Préférences > Paramètres du Panneau de configuration > Imprimantes**

Faire un clic-droit dans la liste des imprimantes (qui doit être vide) **Nouveau > Imprimante partagée.**

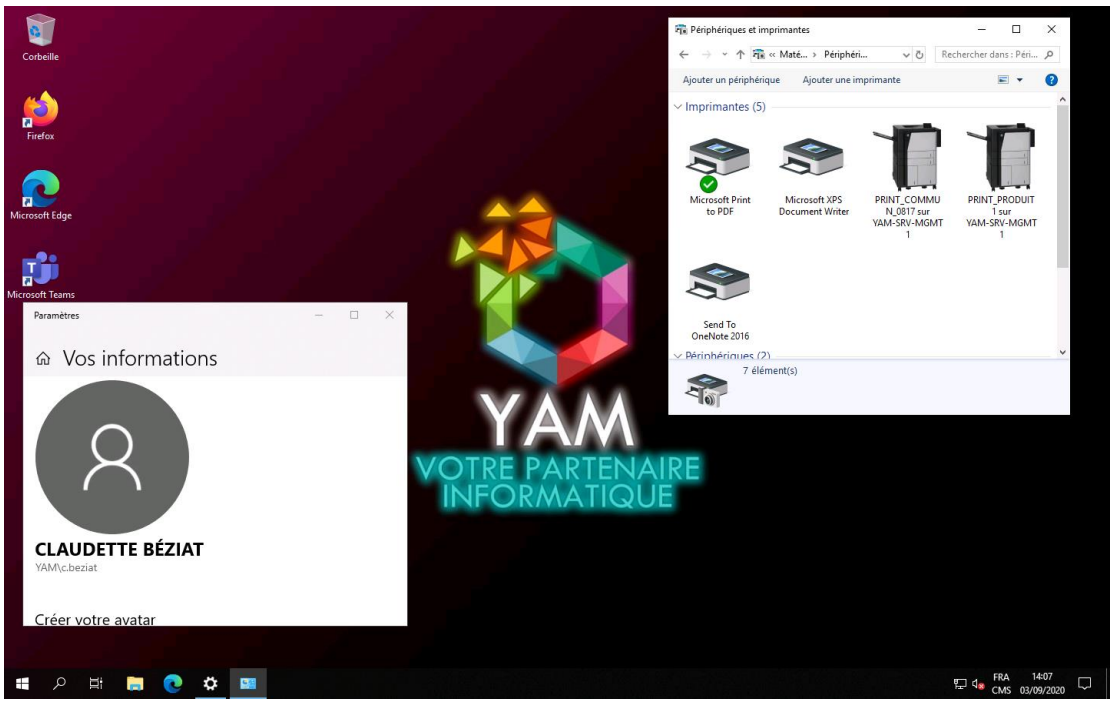
Laisser **Mettre à jour** dans **Action** et spécifier l'emplacement de l'imprimante **\\YAM-SRV-MGMT\PRINT_ADMINISTRATIF** et dans l'onglet **Commun** cocher **Exécuter dans le contexte de sécurité de l'utilisateur connecté.**

Faire de même pour l'ensemble des imprimantes partagées.



Fermer la session utilisateur puis se reconnecter pour appliquer la stratégie.

Ici par exemple, l'utilisatrice Claudette BÉZIAT voit sur son poste les différentes imprimantes auquel elle a accès.



5- SERVEUR DE FICHIERS

INTRODUCTION

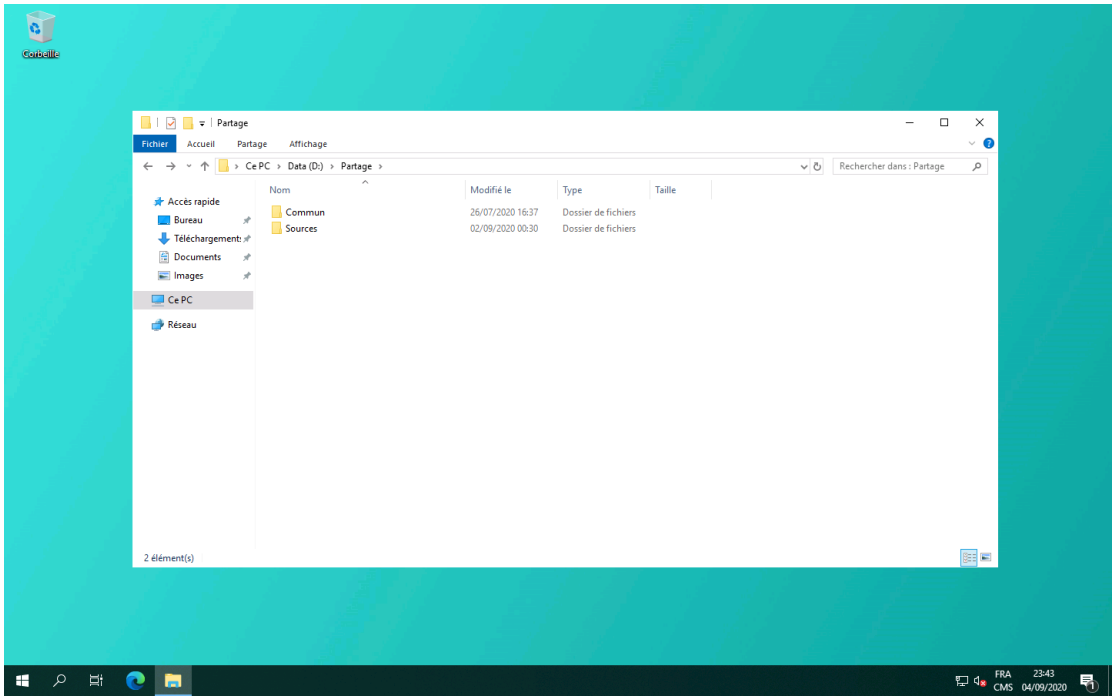
Le serveur de fichiers est en lien avec l'Active Directory. En effet c'est un répertoire centralisé qui permet la gestion des droits utilisateurs, ou encore la gestion des stratégies locales. Ce serveur permet le partage des données à travers notre réseau. Grâce à cela les différents utilisateurs peuvent accéder aux ressources qui y sont stockées, depuis leur session.

5-1- PRÉPARATION DU PARTAGE

PRÉPARATION DES DOSSIERS À PARTAGER

Nous commençons par créer un dossier **Partage**, sur un volume différent du système (qui est sous C:) pour des raisons de sécurité et de performances et éviter en cas de saturation du stockage de bloquer le système.

Nous choisissons le volume D: pour créer le dossier à la racine du volume. Dans ce dossier Partage, nous créons un dossier **Commun** ainsi qu'un dossier **Sources**.



Nous créons par la suite tous les sous-dossiers correspondants aux services au sein du dossier Commun :

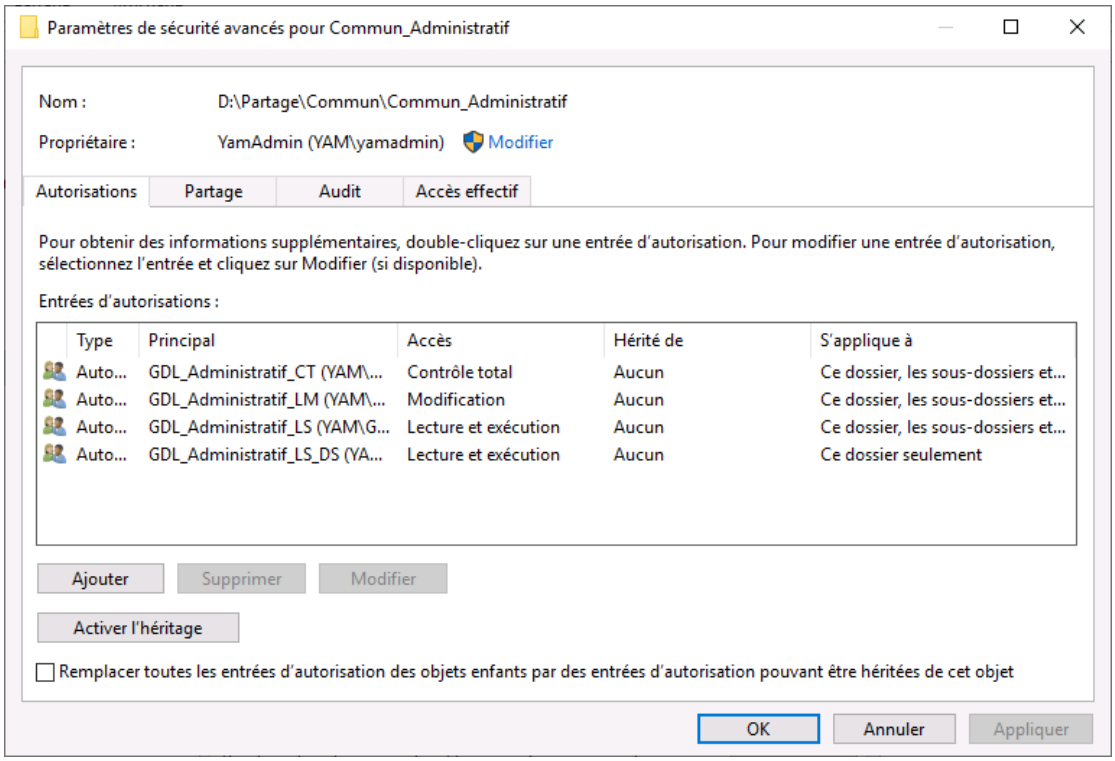
- Commun_Administratif
- Commun_Direction
- Commun_Informatique
- Commun_Produit1
- Commun_Produit2
- Commun_SAV

Dans ces dossiers on associe les GDL propres à chaque dossier en attribuant les droits correspondants.

Pour rappel pour chaque dossier partagé :

Nom du groupe	Niveau d'accès
GDL_NomDossier_CT	Contrôle total
GDL_NomDossier_LM	Modification (lecture et écriture)
GDL_NomDossier_LS	Lecture seule
GDL_NomDossier_LS_DS	Lecture seule sans héritage dans sous-dossiers

Par la suite nous nous rendons dans les paramètres de sécurité de chaque dossier **Commun_*Service*** avancés afin de désactiver les héritages et ne garder dans les autorisations que les GDL correspondant au service avec les droits indiqués.



Les droits appliqués sur les dossiers sont définitifs puisque tout changement de droit d'accès pour un utilisateur ou l'ensemble d'un service s'effectuera depuis la console Utilisateurs et ordinateurs Active Directory.

ATTRIBUTION DES DROITS

On attribue maintenant les droits aux GG_Services selon les indications du tableau ci-dessous :

Groupe global (GG)	Membre de :
GG_ Administratif	GDL_Administratif_LS_DS GDL_Sources_LS
GG_Direction	GDL_Administratif_LS GDL_Direction_LS GDL_Informatique_LS GDL_Produit1_LS GDL_Produit2_LS GDL_SAV_LS

	GDL_Sources_LS
GG_Informatique	GDL_Administratif_CT GDL_Direction_CT GDL_Informatique_CT GDL_Produit1_CT GDL_Produit2_CT GDL_SAV_CT GDL_Sources_CT
GG_Produit1	GDL_Produit1_LS_DS GDL_Sources_LS
GG_Produit2	GDL_Produit2_LS_DS GDL_Sources_LS
GG_SAV	GDL_SAV_LS_DS GDL_Sources_LS

Pour rappel, les droits en lecture seule, uniquement sur les dossiers **GDL_NomDossier_LS_DS**, sont nécessaire afin que, lors de la création automatique du dossier de chaque utilisateur du service, **les collègues ne puissent pas y avoir accès.**

De plus, la règle pour chaque utilisateur automatisant la création du **Dossier de base** au nom de cet utilisateur dans le répertoire partagé du service auquel il appartient lui **attribue automatiquement les droits en control total sur son propre dossier.**

5-2- MISE EN PLACE DES DOSSIERS PARTAGÉS

INSTALLATION DU RÔLE

On installe sur le serveur YAM-SRV-DATA le rôle **Services de fichiers et iSCSI**

Nous avons choisi d'installer une option qui est intéressante pour gérer les dossiers partagés, dans le cas où nous avons plusieurs serveurs, l'option des **Espaces de noms DFS.** En plus de l'option **Gestionnaire de ressources du serveur de fichiers,** nous cochons également l'option **Déduplication des données.** Cela va nous servir à réduire de manière significative l'espace occupé par les données. En effet, si des doublons sont présents sur les structures des fichiers, ils seront répertoriés automatiquement et ne seront comptés plus qu'une seule fois.

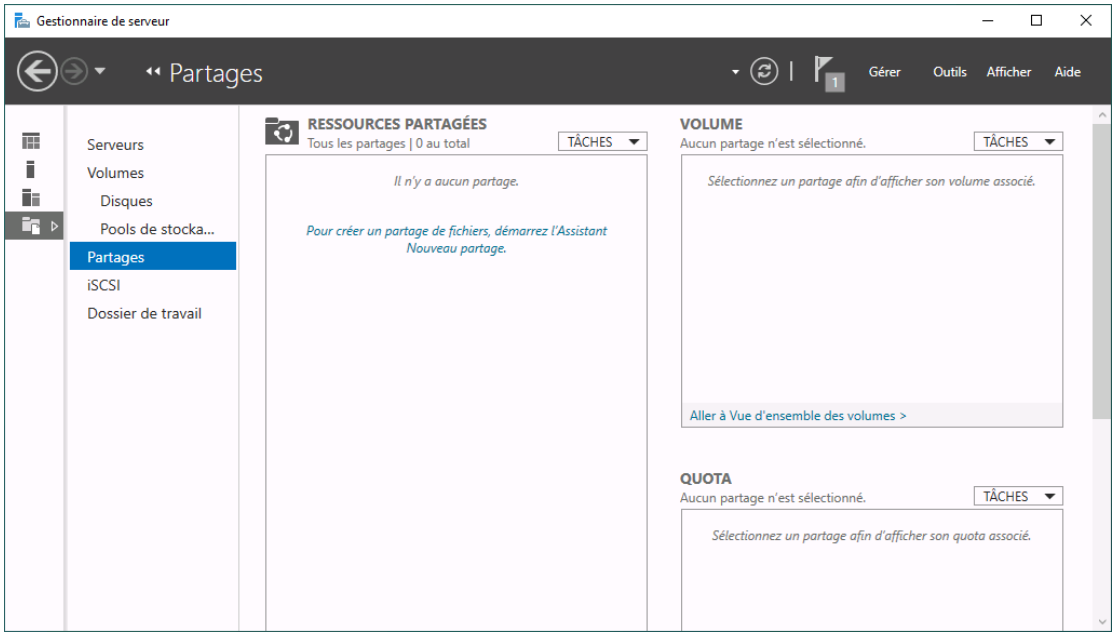
CRÉATION DES PARTAGE DE DOSSIERS

Il s'agit de mettre en partage les deux dossiers suivants :

Nom du partage	Chemin d'accès local	Notes
\\YAM-SRV-DATA\Commun	D:\Partage\Commun	Dossier partagé commun à tous les services.
\\YAM-SRV-DATA\Sources$	D:\Partage\Sources$	Dossier masqué

Nous créons ensuite le partage pour les ressources partagées. Dans **Gestionnaire de serveur,** se rendre dans **Service de fichiers et de stockage > Partages.**

Puis dans **Ressources partagées,** cliquer sur **Tâches > Nouveau partage.**



Nous sélectionnons le profil du partage des fichiers, en choisissant le partage **SMB rapide**.

Nous sélectionnons ensuite **Tapez un chemin personnalisé** et spécifions le chemin d'accès au partage en cliquant sur **Parcourir**.

Nous indiquons ensuite le nom de ce partage en conservant le terme **Commun**.

Pour le partage du dossier Sources on le nommera **Source$**, le fait de rajouter le symbole **$** à la fin du nom de partage permet de **masque ce dossier partagé dans l'explorateur de fichiers.** C'est dans ce dossier que nous mettrons des fichiers tels que l'image de fond d'écran des postes, ou les scripts par exemple.

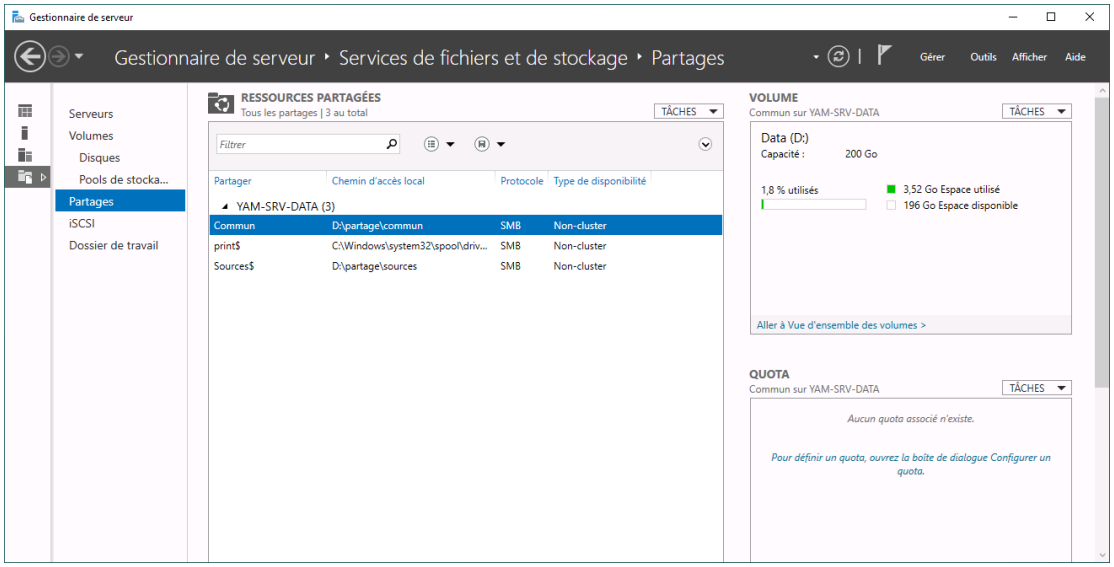
Nous activons l'énumération basée sur l'accès. Ainsi, les sous-répertoires du dossier partagé Commun (Commun_Administratif, Commun_Direction, etc.) seront visibles en fonction des droits d'accès utilisateurs. Par exemple si un utilisateur du groupe administratif est connecté, il ne peut voir et n'avoir accès uniquement qu'au dossier Commun_Administratif. En revanche si nous n'activons pas cette option, l'utilisateur pourra voir tous les dossiers, même ceux auxquels il n'a pas de droits d'accès. Mais s'il tente d'ouvrir ces dossiers sans droits, un message d'accès refusé apparaitra. Cette option a été mise en place depuis la version 2012 de Windows Server.

Nous activons également l'option d'autorisation de mise en cache du partage. En effet cela est utile aux utilisateurs souhaitant avoir un accès hors connexion (par exemple pour les postes nomades qui peuvent avoir des pertes de connexion). L'activation de cette option permet donc à l'utilisateur de charger sur son PC tout le contenu du répertoire. Il peut ainsi modifier un fichier, même s'il n'est pas connecté au serveur. Ensuite lorsqu'il se reconnecte, la synchronisation s'effectue automatiquement.

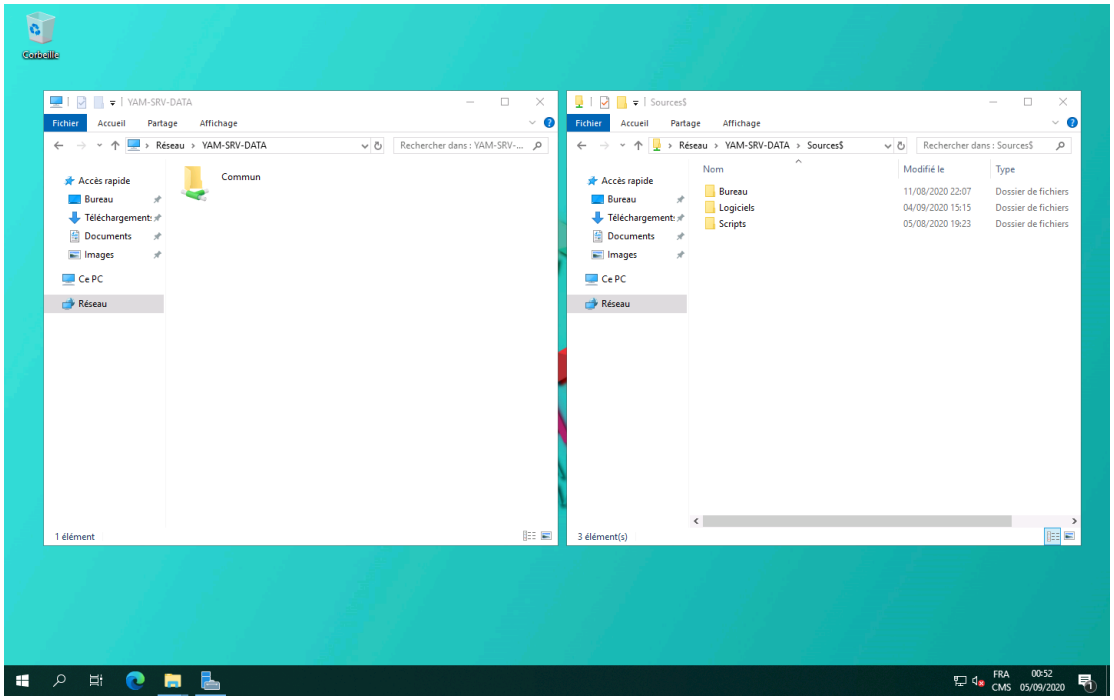
Au niveau de la **spécification des autorisations pour contrôler l'accès**, nous ne touchons à rien car nous avons déjà défini ces autorisations au préalable.

Nous confirmons le paramétrage du partage en cliquant sur **Créer**.

Une fois les deux partages créés, nous les retrouvons dans les ressources partagées.



Nous retrouvons ci-dessous le résultat du partage des dossiers avec, à gauche le dossier Sources$ non visible mais accessible, et à droite son contenu.



5-3- ACTIVER LA DÉDUPLICATION

INTRODUCTION

La déduplication permet un gain d'espace disque significatif, en effectuant une optimisation de l'espace de stockage en supprimant les fichiers ou parties de fichiers en plusieurs exemplaires pour n'en garder qu'un. La déduplication des données permet d'optimiser les redondances sans compromettre la fidélité ni l'intégrité des données.

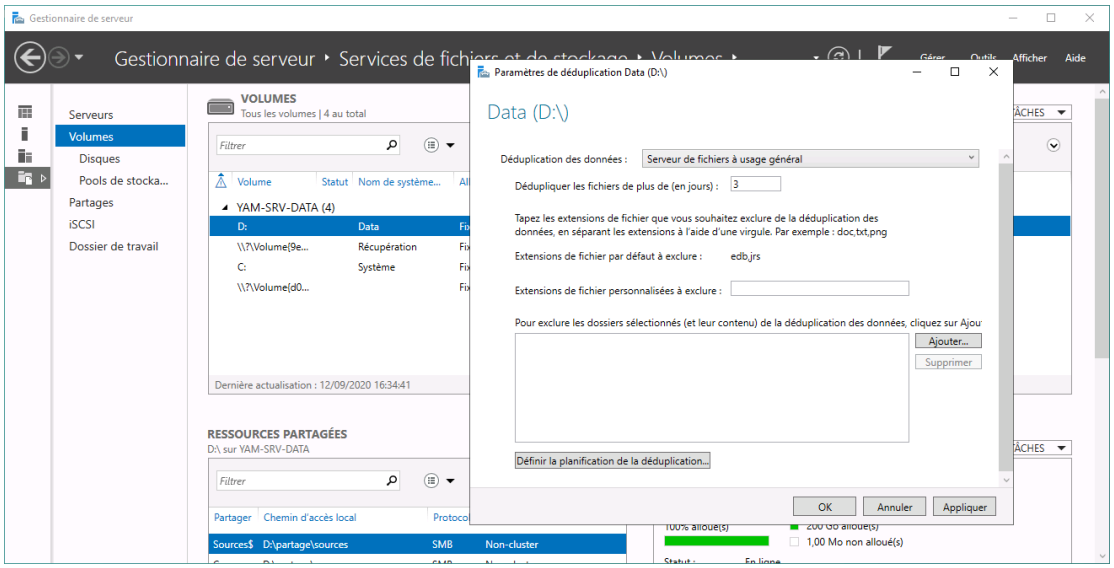
PRÉREQUIS

La déduplication doit obligatoirement s'appliquer sur un volume différent du système.

INSTALLATION

Pour activer cette fonctionnalité, se rendre dans le **Gestionnaire de serveur > Service de fichiers et de stockage > Volumes** puis sélectionner le volume souhaité et faire un **clic-droit > Configurer la déduplication des données**.

Puis dans la nouvelle fenêtre, choisir **Serveur de fichier à usage général**, laisser les autres options par défaut et cliquer sur **OK**



5-4- MISE EN PLACE DE LA STRATÉGIE DE GROUPE

Nous créons ensuite une GPO (stratégie de groupe) pour tous les utilisateurs, afin de mapper les lecteurs réseaux. Tout le monde va avoir un seul lecteur réseau commun, sur lequel il y aura les différents droits (sur le lecteur R:).

Créer la GPO suivante :

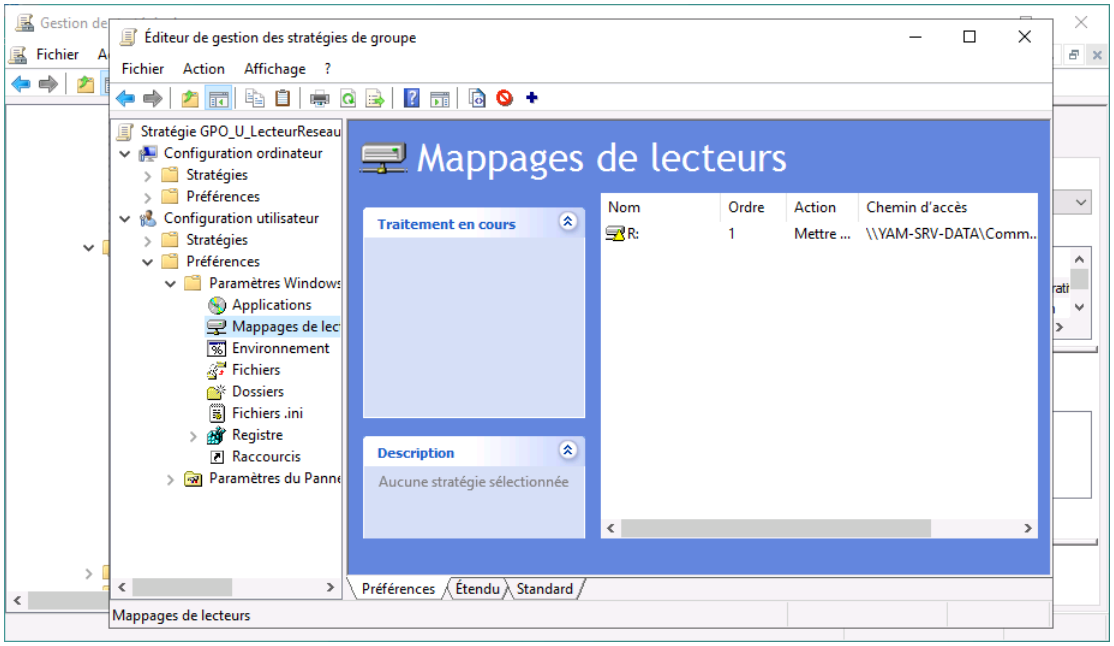
Nom GPO	Cible	OU d'application
GPO_U_LecteurResau	Utilisateur	Administratif Direction Informatique Produit 1 Produit 2 SAV

Cette GPO permet le mappage automatique du lecteur réseau commun.

Se rendre dans **Configuration utilisateur > Préférences > Paramètres Windows > Mappages de lecteurs**

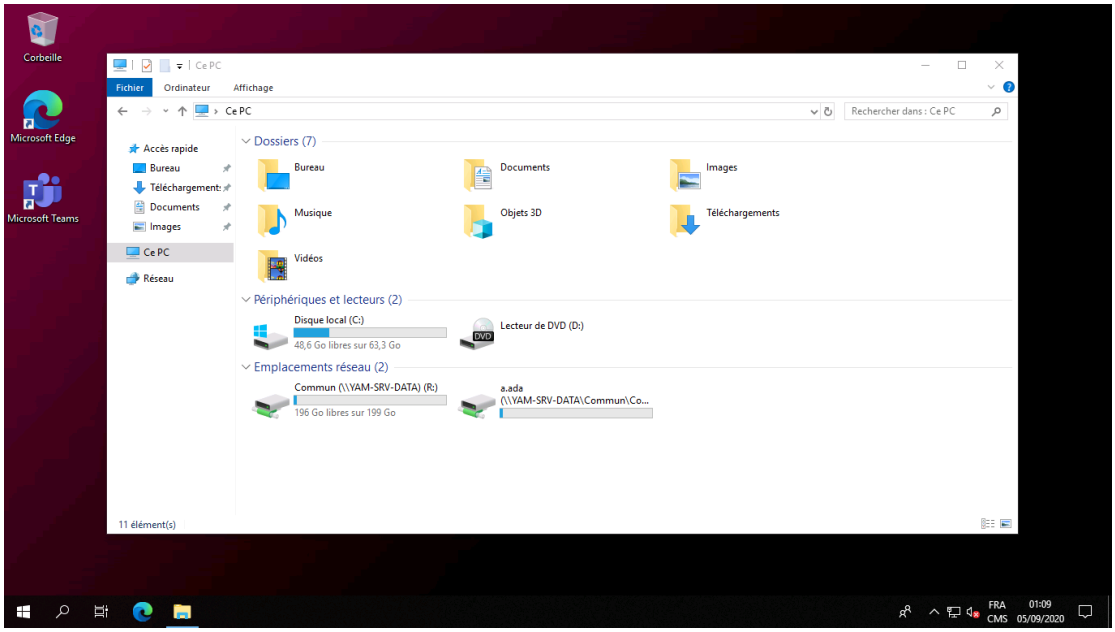
Faire un clic-droit dans la liste des lecteurs (qui doit être vide) **Nouveau > Lecteur mappé.**

Laisser **Mettre à jour** dans **Action** et spécifier l'emplacement du dossier partagé **\\YAM-SRV-DATA\Commun** et lui attribuer **R** comme lettre de lecteur.



Fermer la session utilisateur puis se reconnecter pour appliquer la stratégie.

La capture ci-dessous montre le résultat du montage du lecteur réseau sur le poste client.



6- WINDOWS SERVER UPDATE SERVICES (WSUS)

INTRODUCTION

Le rôle WSUS permet la gestion centralisée de la distribution des mises à jour de sécurité des produits Microsoft (Windows, Windows Server, Office, etc.). À l'échelle de l'entreprise, il y a deux principaux avantages :

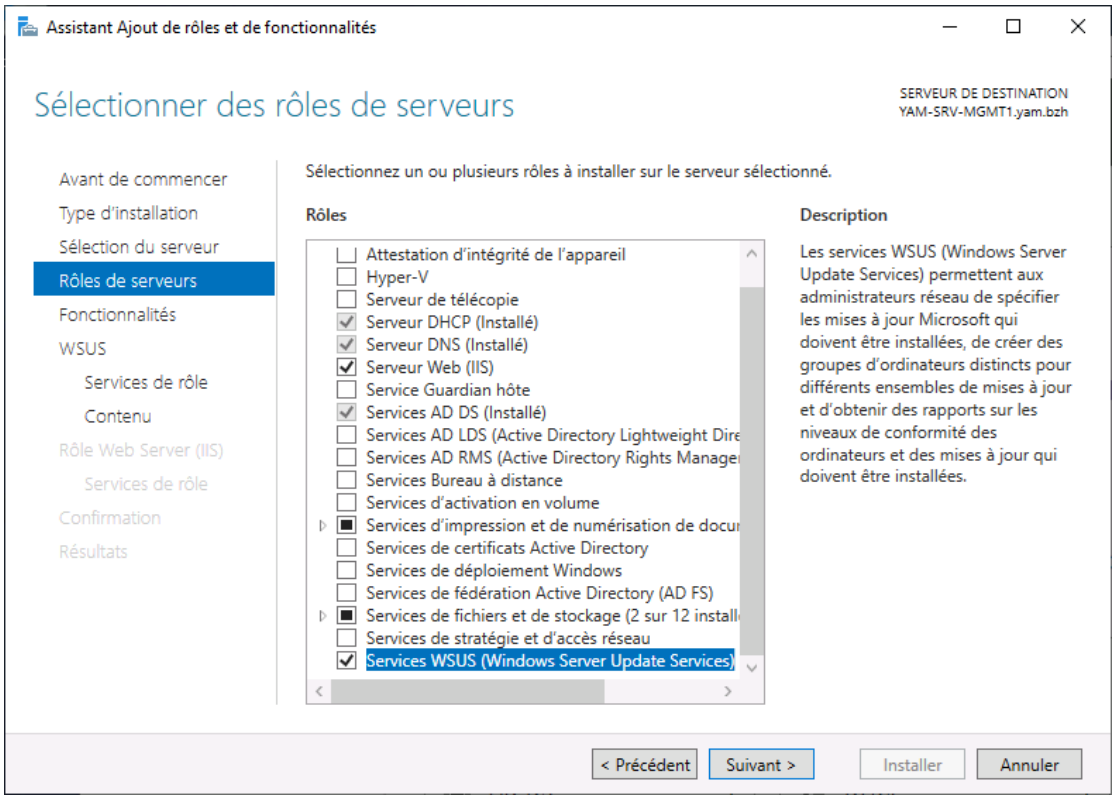
- **Maitriser l'installation des mises à jour nouvellement publiées par Microsoft** : on testera dans un environnement « Labo » ces nouvelles mises à jour afin de s'assurer du bon fonctionnement des logiciels métier après leur application. Cela permet ainsi de préserver la stabilité des postes de travail.
- **Ne télécharger les mises à jour nécessaire qu'une seule fois depuis l'extérieur** : les mises à jour qui auront été validées seront téléchargées et stockées sur le serveur WSUS pour être ensuite distribuées aux clients.

PRÉREQUIS

Attacher un disque au serveur virtuel qui accueillera le rôle WSUS afin d'avoir un espace dédié au stockage des mises à jour approuvées. Formater ce disque en NTFS puis créer un dossier à la racine nommé WSUS.

6-1- INSTALLATION DU RÔLE

Se rendre dans le Gestionnaire de Serveur et choisir **Gérer > Ajouter des rôles et fonctionnalités.** Choisir ensuite **Services WSUS (Windows Server Update Services).**



Puis dans **Sélectionner des services de rôle,** on laissera **WID Connectivity** et **WSUS Services** cochés par défaut.

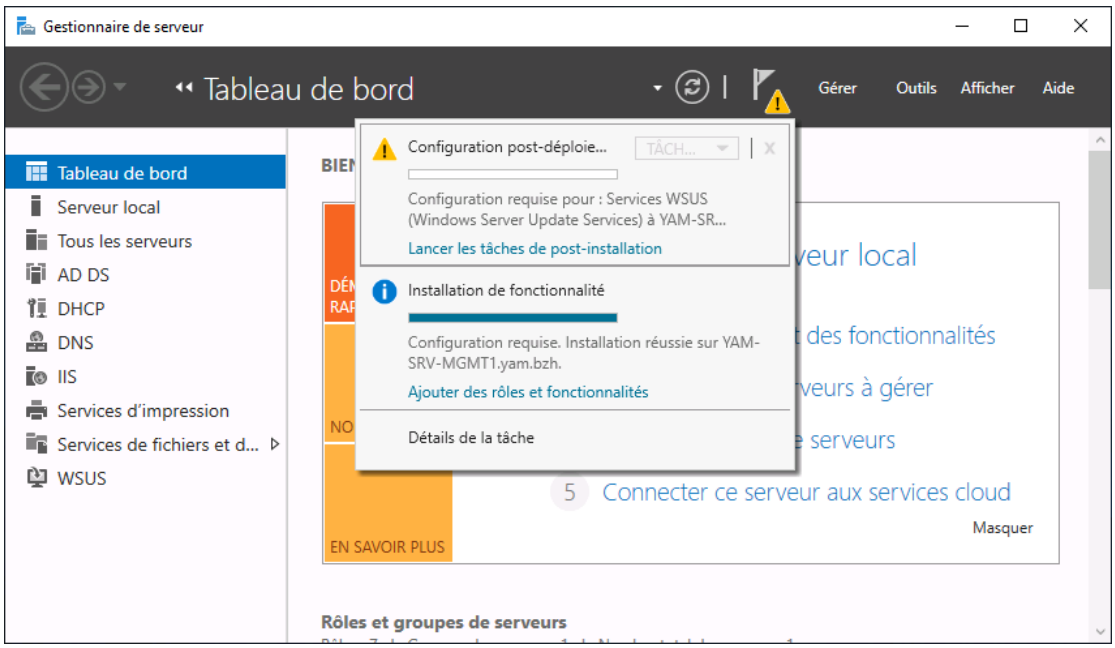
On sélectionne l'**emplacement de stockage** où seront téléchargées les mises à jour approuvées. On choisit le dossier WSUS créé sur le nouveau disque.

Le Rôle Web Server (IIS) est installé par le Service WSUS, on laissera les choix par défaut. Puis cliquer sur **Installer** dans la page suivante.

6-2- CONFIGURATION POST-INSTALLATION

6-2-1- ASSISANT DE CONFIGURATION

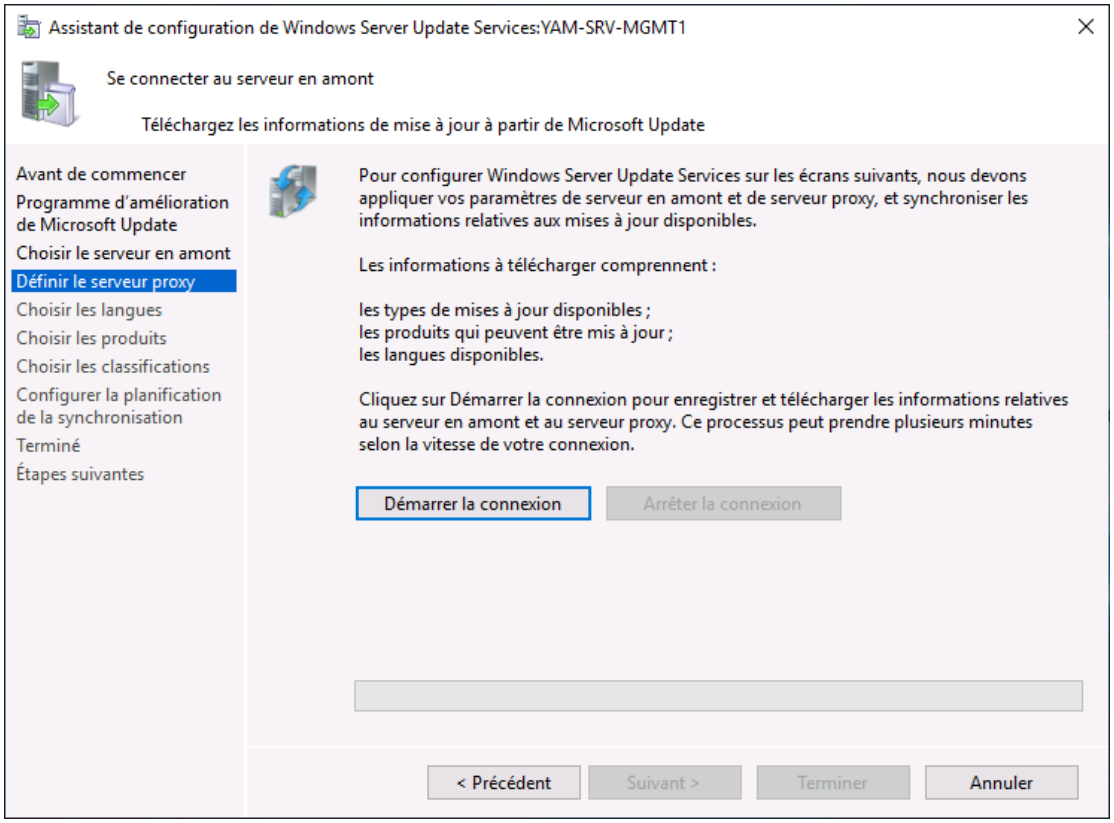
Après l'installation du rôle Service WSUS, retourner dans le gestionnaire de serveur puis cliquer sur le drapeau situé à gauche du bouton Gérer, et cliquer sur lancer les tâches de post-installation.



S'ouvre alors l'assistant de configuration de Windows Server Update Services.

Sur la page **Avant de commencer,** on s'assurera que le serveur virtuel est bien connecté à internet puis cliquer sur Suivant. Ensuite, **on ne cochera pas** la case **Oui, je souhaite participer au Programme d'Amélioration Microsoft Update.**

Sur la page **Choisir le serveur en amont,** sélectionner **Synchroniser à partir de Microsoft Update,** puis ne rien cocher dans Définir le serveur proxy. Et enfin cliquer sur Démarrer la connexion puis patienter le temps que l'assistant télécharge les informations de mises à jour.



Sur la page suivante, **Choisir les langues,** sélectionner **Télécharger les mises à jour dans ces langues uniquement** et cocher Anglais et Français.

Sur la page **Sélectionner les produits Microsoft à mettre à jour,** choisir uniquement les éléments suivants :

- Office 365 Client
- Microsoft Defender Antivirus
- Microsoft Edge
- Windows 10 and later Drivers
- Windows 10 and later Upgrade & Servicing Drivers
- Windows 10 LTSB
- Windows 10
- Windows Server 2019 and later, Servicing Drivers
- Windows Server 2019 and later, Upgrade & Servicing Drivers
- Windows Server 2019

Puis, sur la page **Sélectionner les classifications à télécharger,** cocher les éléments suivants :

- Mise à jour critique
- Mise à jour de la sécurité
- Mise à jour
- Mise à jour de définitions

Dans **Configurer la planification de la synchronisation,** choisir **Synchroniser automatiquement** et définir l'horaire sur 22h00. On laissera le nombre de synchronisation sur 1 par jour.

Enfin, sur la page **Terminé,** cocher la case **Commencer la synchronisation initiale.**

6-2-2- CONSOLE WSUS

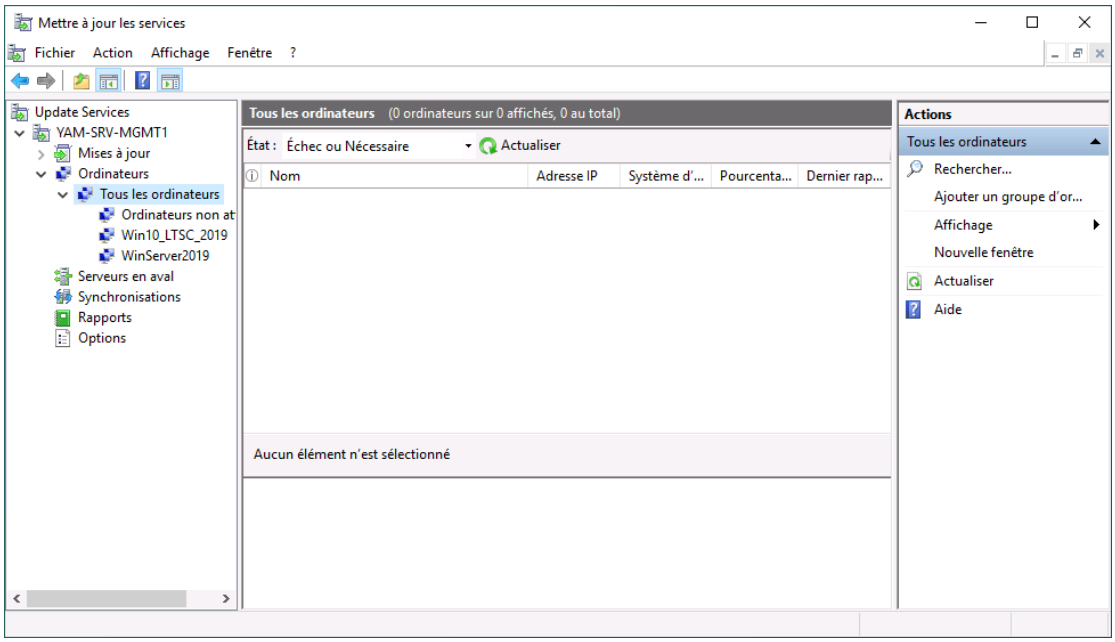
Nous allons démarrer la console WSUS afin de terminer la configuration. Se rendre dans Menu démarrer > Outils d'administration > Services WSUS.

CRÉATION DES GROUPES D'ORDINATEUR

L'intérêt est de pouvoir cibler les mises à jour à appliquer selon le groupe auquel appartiennent les ordinateurs. Ainsi, dans le cas d'un groupe d'ordinateurs ayant par exemple une application métier très sensible à toute modification du système, on peut dans ce cas créer un groupe spécifique pour ce groupe sur lequel on adaptera la l'application des mises à jour.

Une fois la console d'administration ouverte, dans le volet de gauche, se rendre dans Ordinateurs > Tous les ordinateurs. Faire un clic-droit sur tous les ordinateurs et choisir Ajouter un groupe d'ordinateurs. Nous créons deux groupes :

- **Win10_LTSC_2019** : où seront classés tous les postes clients légers et lourds.
- **WinServer2019** : où seront classés tous les serveurs sous Windows Server.

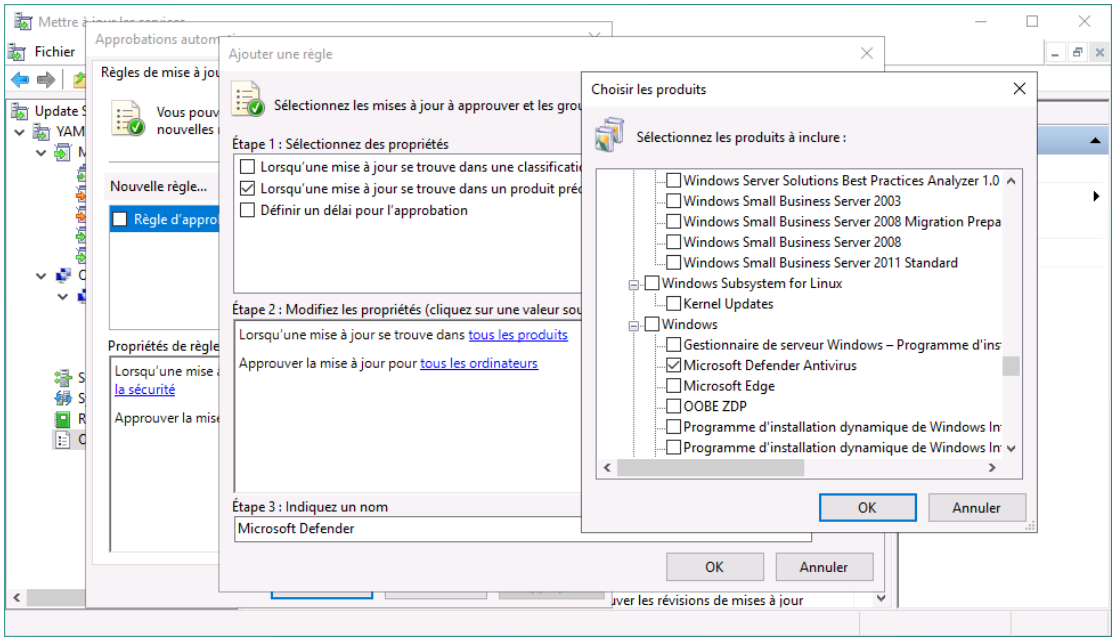


APPROBATIONS AUTOMATIQUES

Cela permet, pour une famille de produit de mise à jour, d'approuver automatiquement les nouvelles mises à jour publiées. Nous appliquerons cette politique pour les mises à jour Microsoft Defender.

Dans la console d'administration WSUS, dans le volet de gauche, se rendre dans **Options** puis dans le volet central, cliquer sur **Approbations automatiques**.

Nans la nouvelle fenêtre intitulée **Approbations automatiques**, cliquer sur **Nouvelle règle** puis dans la fenêtre **Ajouter une règle**, on coche **Lorsqu'une règle se trouve dans un produit précis**, et dans le bas de cette même fenêtre cliquer sur **tous les produits**. Dans la fenêtre Tous les produits cocher uniquement **Microsoft Defender Antivirus**. Enfin, cliquer sur OK sur chaque fenêtre pour appliquer les choix.



6-3- MISE EN PLACE DE LA STRATÉGIE DE GROUPE

Nous nous rendons ensuite dans l'éditeur de gestion des stratégies de groupe afin d'appliquer aux ordinateurs du domaine la stratégie de mises à jour.

Créer les GPO suivante :

Nom GPO	Cible	OU d'application
GPO_O_WSUS_Win10	Ordinateur	Clients_legers Clients_lourds
GPO_O_WSUS_WinServer2019	Ordinateur	Hote_RDS Serveurs

Ces GPO permettent de spécifier aux ordinateurs d'effectuer les recherches de mises à jour auprès du serveur local sur lequel se trouve le service WSUS, et de les classer automatiquement dans les groupes d'ordinateurs créés dans la console WSUS.

Se rendre dans **Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Update.**

Activer **Autoriser le ciblage côté client** et spécifier comme nom de groupe :

- GPO_O_WSUS_Win10 : **Win10_LTSC_2019**
- GPO_O_WSUS_WinServer2019 : **WinServer2019**

Puis activer **Spécifier l'emplacement intranet du service de mise à jour** Microsoft et indiquer les éléments suivants :

- Configurer le service de mise à jour pour la détection des mises à jour : **http://172.16.100.4:8530/**
- Configurer le serveur intranet de statistiques : **http://172.16.100.4:8530/**

Et enfin, activer **Ne pas se connecter à des emplacements Internet Windows Update**

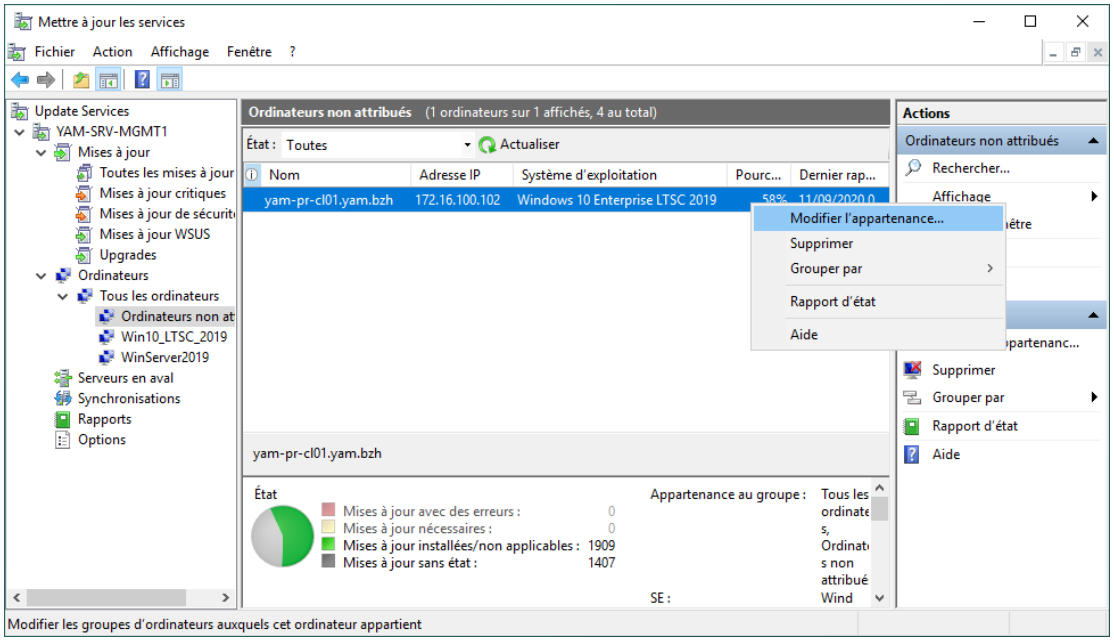
Redémarrer les ordinateurs concernés pour appliquer la stratégie.

CLASSER MANUELLEMENT UN ORDINATEUR

Si un ordinateur n'est pas classé par la stratégie de groupe, il se retrouvera dans la liste Ordinateurs non attribués de la console WSUS.

Pour le mettre dans le bon groupe, dans la console WSUS se rendre, dans le volet de gauche dans **Ordinateurs > Tous les ordinateurs > Ordinateurs non attribuées**.

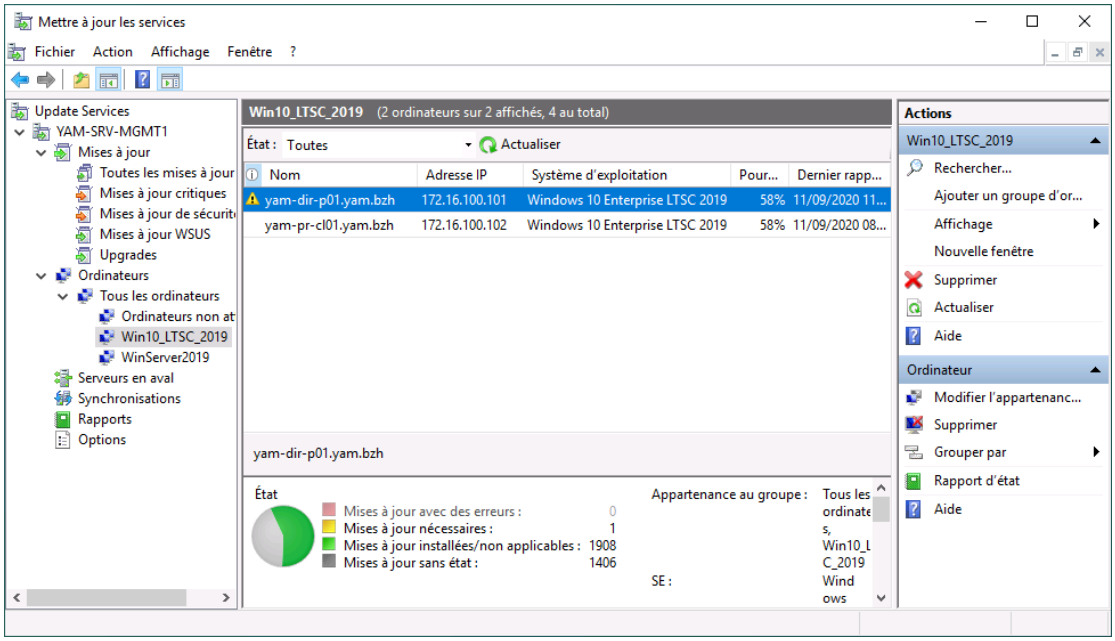
Sélectionner l'ordinateur souhaité et faire un **clic-droit > Modifier l'appartenance** puis choisir le groupe correspondant.



6-4- VUE D'ENSEMBLE ET APPROBATION DE MISE À JOUR

VUE D'ENSEMBLE DE L'ÉTAT DES ORDINATEURS

Dans la partie Ordinateurs de la console d'administration, on peut observer l'état d'application des mises à jour des ordinateurs et identifier les postes sur lesquels des mises à jour approuvées n'auraient pas encore été installées. Dans l'exemple ci-dessous le poste YAM-DIR-P01, identifié par un triangle jaune n'a pas installé toutes ses mises à jour.

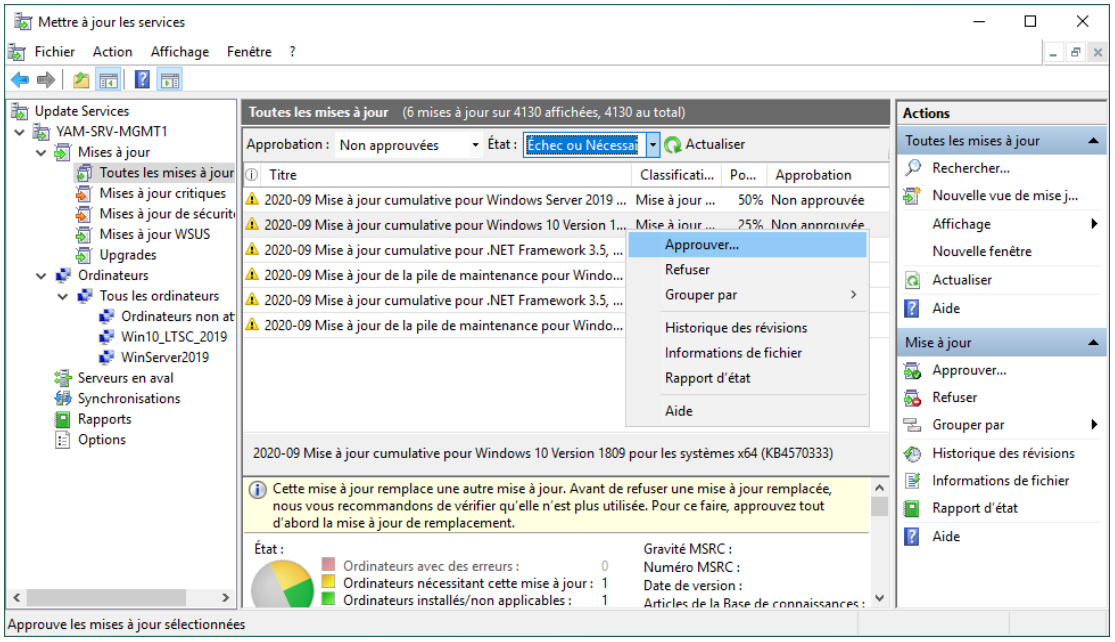


APPROUVER UNE MISE À JOUR

Tant qu'une mise à jour ne sera pas approuvée, elle ne sera pas téléchargée sur le serveur ni déployée sur les postes concernés.

Se rendre dans **Mises à jour > Toutes les mises à jour** et filtrer la vue par **Approbation : Non approuvées** et **État : Échec ou Nécessaire** afin de n'avoir que les mises à jour en attente pour les postes du parc (dans tous les cas, les mises à jour nécessaires sont identifiées par un triangle jaune).

Puis sélectionner la mise à jour concernée et faire un **clic-droit > Approuver**, puis dans la nouvelle fenêtre, sélectionner le groupe d'ordinateurs cible et choisir **Approuvée pour l'installation** puis cliquer sur OK.



À partir de ce moment, le serveur WSUS télécharge les mises à jour approuvées, qui seront ensuite redistribuées aux ordinateurs concernés.