PROJET EVOLUTION

Bundle

CAMPUS
D'ENSEIGNEMENT SUPÉRIEUR
ET DE FORMATION PROFESSIONNELLE

Govrian Pilard

Teguy Ekenza

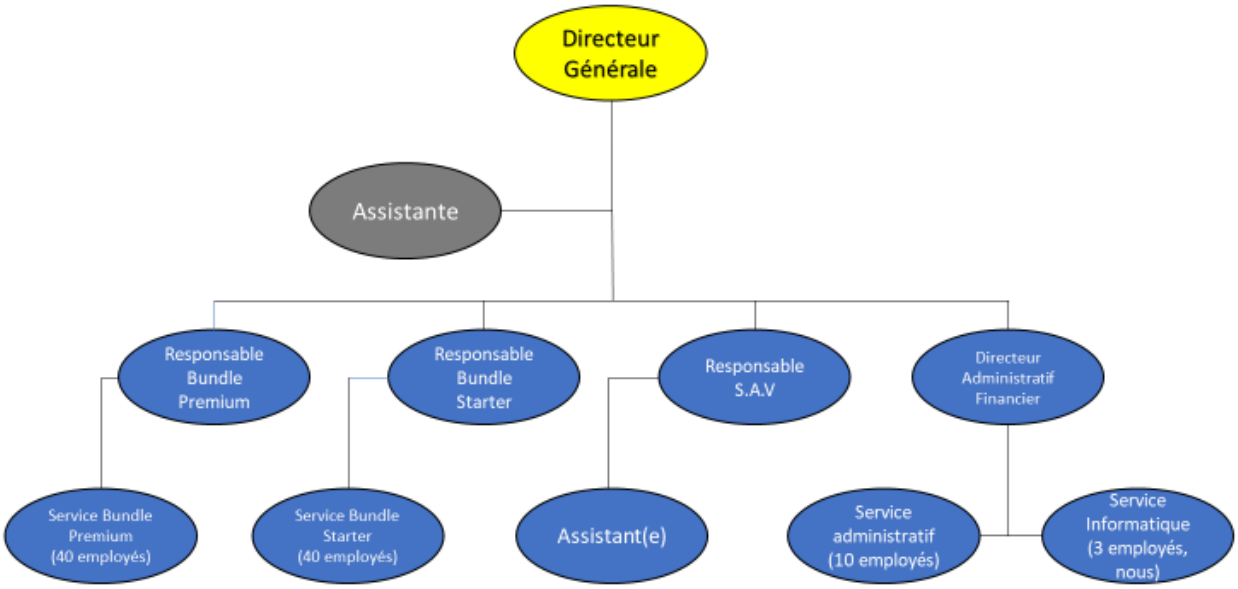
Rafael Chauviere

Clément Barbe

Table des matières

Présentation de l'entreprise.

La société « Bundle » fut créée en 1998, elle est spécialisée dans les liseuses électroniques. Son siège est situé à Bordeaux, plus exactement 24 Rue Sainte-Catherine 33000 et compte parmi elle 90 employés. Son chiffre d'affaire annuel est de 3 451 200,00€ sur 2019 et a un capital social de 38 000,00€.



Charte Graphique

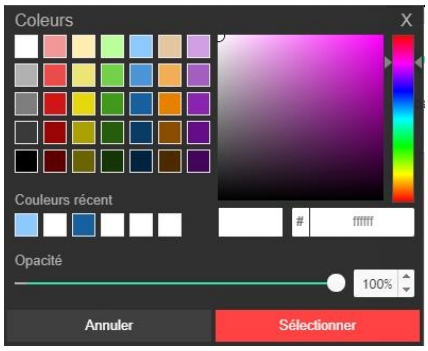
Qu'est-ce que la charte Graphique.

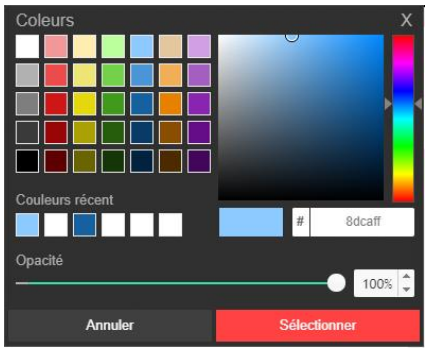
Une charte graphique, dont le nom correct est « cahier des normes graphiques », est un document de travail qui contient toutes les règles de base pour l'utilisation des caractères graphiques qui constituent l'identité graphique d'une organisation, d'un projet, ou d'une entreprise.

Le logo de l'entreprise

Le logo de notre entreprise contient aussi son nom à l'intérieur pour renforcer l'identité de la marque ainsi que pour mieux se faire reconnaître par les potentiels clients.

Les couleurs utilisées sont :





Le logo est donc composé de 3 couleurs différentes avec comme effet le dégradé.

Nous avons du blanc (#FFFFFF) ainsi que du bleu (#8DCAFF, #1761A0)

La disposition du logo dans les documents sera toujours placée dans le coin supérieur droit de chaque document, comme cela il pourra toujours être identifié lors de la lecture de ce dernier.

La typographie de l'entreprise.

Nous avons fait le choix de prendre une typographie à la fois simple et épurée. Pour que la lecture soit agréable et professionnelle.

Pour les titres nous avons donc pris la couleur bleue qui rappelle aussi notre logo.

1er Titre (Grand titre) :

TEST DE TITRE 1

- La police utilisée : Calibri Light
- Taille de la police : 16
- Couleur de la police : Bleu, Accentuation1, Plus sombre 25%

2ème Titre :

TEST DE TITRE 2

- La police utilisée : Calibri Light
- Taille de la police : 13
- Couleur de la police : Bleu, Accentuation1, Plus sombre 25%

3ème Titre

TEST DE TITRE 3

- La police utilisée : Calibri Light
- Taille de la police : 12
- Couleur de la police : Bleu, Accentuation1, Plus sombre 50%

Premier TITRE

DEUXIEME TITRE

TROISIEME TITRE

Corps de texte du document :

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec vel iaculis magna. Vivamus aliquet ac est eget vestibulum. Nam consequat semper neque, eleifend ultrices dolor laoreet et. Phasellus eu nibh at nibh finibus mattis. Phasellus eget dui sodales, blandit eros nec, aliquet diam. Aliquam erat volutpat. In eget vehicula nibh.

-La police utilisée : Calibri

-Taille de la police : 11

Couleur de la police : Noir

Le cahier des charges

Pour mener à bien notre projet nous avons un cahier des charges qui nous a été fourni, reprenant l'ensemble des tâches et obligations sur lesquelles nous devons apporter des solutions précises.

- L'équipe informatique court partout… Et se trompe souvent de lieu pour dépanner les utilisateurs. En plus, il n'y a pas d'informations stockées quelques part sur le parc (Noms d'hôtes, type de machines…).
- Il n'y a pas de gestion de droits utilisateurs.
- Le siège social a besoin d'un serveur ftp (ils veulent récupérer des fichiers dessus), c'est le moment de tester la mise en place d'un serveur linux.
- Vous devez implémenter Active Directory dans l'entreprise (voir ci-dessous vous avez certaines consignes plus précises).
- Vous avez 6 sessions pour faire aboutir les projets.
- Il veut un compte rendu mensuel sur votre avancé (un tableau d'indicateurs, un planning, le qui fait quoi par exemple, etc…).
- Il veut un rapport d'activité globale sur la faisabilité et les solutions mises en place suivant le cahier des charges ; les procédures d'installation, de déploiement, le prix, et tout cela en suivant la charte de l'entreprise.

Réponse proposée au cahier des charges :

Afin d'éviter des déplacements inutiles et de gagner du temps, nous mettrons en place un serveur de base de données pour ajouter tout le matériel informatique dont nous disposons, ses utilisateurs, ses emplacements ainsi que ses descriptions et fonctionnalités.

De plus, nous créerons une application web qui se reliera à la base de données afin de pouvoir la gérer plus facilement, et permettre aux utilisateurs d'y avoir un accès limité lors de la consultation. L'application sera disponible sur l'intranet.

Nous allons créer un serveur ftp afin que le siège puisse collecter des données facilement et rapidement et de manière sécurisée.

Afin de gérer les autorisations des utilisateurs, nous allons mettre en place un serveur, qui installera des machines virtuelles pour gérer la partie Active Directory, mais aussi qui nous permettra d'utiliser des GPO et des scripts pour gérer les autorisations des utilisateurs.

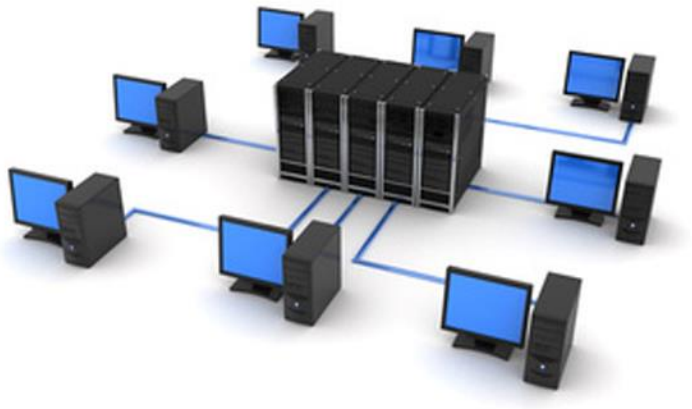
Dans ce dossier vous pourrez y trouver plus en détail les différentes solutions apportées pour répondre le plus fidèlement possible au cahier des charges.

Le réseau

Le réseau informatique fait référence à la mise en relation de plusieurs équipements informatiques qui peuvent ainsi partager des données entre eux, notamment dans le monde de l'entreprise.

Exemple : Le réseau informatique permet d'accéder à nos fichiers de n'importe quel ordinateur.

Et pour que cela fonctionne il faut le configurer pour qu'il puisse correctement communiquer.



La plage IP

Nous avons sélectionné la plage d'adressage suivante : 192.168.10.0/24

Avec une plage IP comme celle-ci nous disposons de 254 adresses disponibles, puisque nous avons un masque qui est /24 ou bien 255.255.255.0

La société a un effectif de moins de 100 personnes ce qui nous laisse largement assez d'IP disponibles pour le matériel tels que les serveurs ou les imprimantes.

Classe Réseau	Début	Fin
Classe A	0.0.0.0	127.255.255.255
Classe B	128.0.0.0	191.255.255.255
Classe C	192.0.0.0	223.255.255.255
Classe D	224.0.0.0	239.255.255.255
Classe E	240.0.0.0	255.255.255.255

Le choix du système d'exploitation du server Windows : Windows 2019 server

Windows 2019: Microsoft a mis à jour son système d'exploitation serveur vers la nouvelle version ce qui apporte de nouvelles fonctionnalités importantes. Dans le cadre des Long Term Servicing Channels (LTSC), une mise à jour est désormais effectuée tous les deux ans et introduit partiellement de nouvelles fonctionnalités importantes. Microsoft s'est appuyé sur le développement des fonctionnalités existantes.

Quelles sont les nouvelles fonctionnalités du système?

Il existe plusieurs piliers sur lesquels repose la nouvelle version du système d'exploitation de Microsoft. Plus de possibilités de travailler dans un Cloud hybride, un meilleur support pour Linux, plus de sécurité via les Shielded Virtual Machines (machines virtuelles blindées en français), des

nouveautés dans le sous-système de stockage et la création du **Windows Admin Center**.

- Pas tout à fait nouveau mais composante importante de Windows 2019 : Windows Admin Center. Il s'agit d'une console graphique pour la gestion du serveur. Le logiciel peut être contrôlé via le navigateur, peut être utilisé à distance et permet aux administrateurs de contrôler le matériel connecté.

Nous avons donc de nombreuses améliorations par rapport à la version précédente, certaines fonctions sont ajoutées à la version 2019, d'autres supprimées ou bien modifiées.

Le tableau récapitulatif ci-dessous montre les différences par rapport à Windows Server 2016.

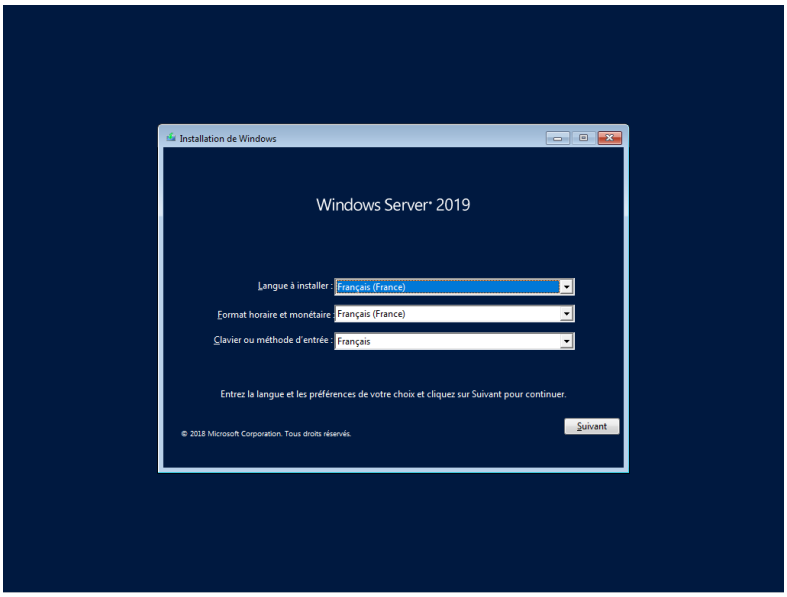
C'est pourquoi nous avons choisi pour notre projet de prendre la dernière version de Windows server.

Fonctions	Windows Server 2016	Windows Server 2019
Windows Admin Center	✓	✓
System Insight	x	✓
Cloud hybride	✓	✓ (étendu)
Support Azure	✓	✓ (étendu)
Support Linux	✓	✓ (étendu)
Kubernetes	✓	✓ (étendu)
« windows » - Image	✓	✓
Windows Defender ATP	✓	✓
Shielded VMs	✓	✓ (aussi pour Linux)
Chiffrement entre machines virtuelles	✓	✓
Storage Migration Service	x	✓
Storage Space Direct	x	✓ (étendu)
Storage Replica	✓ (Edition Datacenter uniquement)	✓
Business Scanning	✓	x
Internet Storage Name Service	✓	x
Remote Desktop Connection Broker / Virtualization Host	✓	x

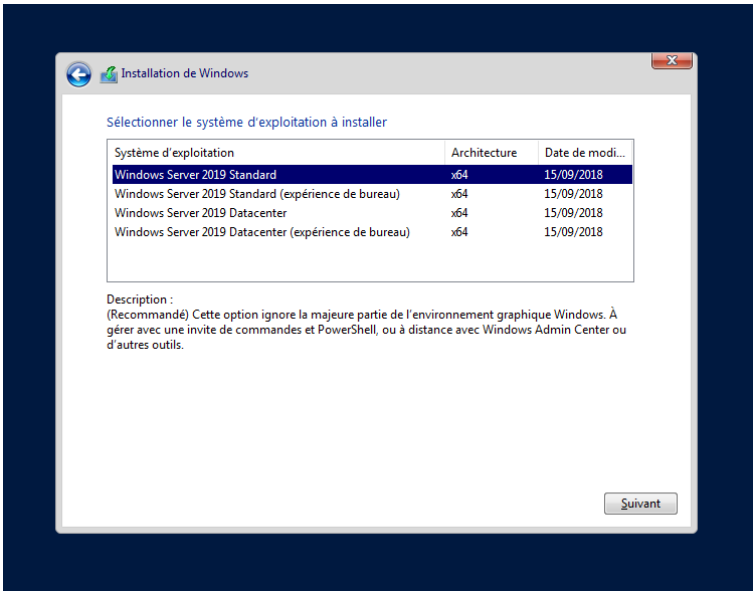
Installation de Windows Server 2019

Installation de base

Lors de l'installation, dans un premier temps, il nous faut choisir une langue à installer ainsi que le format horaire et monétaire qui va être utilisé.



Pendant l'installation de Windows Server 2019, plusieurs options s'offrent à nous : l'installation avec une interface graphique ou en mode Core (installation minimale). Mais aussi quelle version de Windows prendre, c'est-à-dire la Standard ou bien la Datacenter.



Les contrôleurs de domaines : ADC1 et ADC2

Nous allons donc utiliser ADC1 et ADC2 qui seront tous deux des contrôleurs de domaine. ADC1 sera le contrôleur de domaine principal et ADC2 le réplica.

Qu'est-ce qu'un contrôleur de domaine

Une fois le domaine créé, le serveur à partir duquel le domaine est créé sera promu au rôle de «contrôleur de domaine». Il sera le contrôleur du domaine, ce qui signifie qu'il sera au cœur des requêtes pour ce domaine. Par conséquent, il devra vérifier l'identité de l'objet, traiter les demandes d'authentifications, assurer l'application de la stratégie de groupe ou stocker une copie d'Active Directory.

Le contrôleur de domaine est essentiel bon fonctionnement du domaine. Si le contrôleur de domaine est arrêté ou endommagé, le domaine deviendra indisponible.

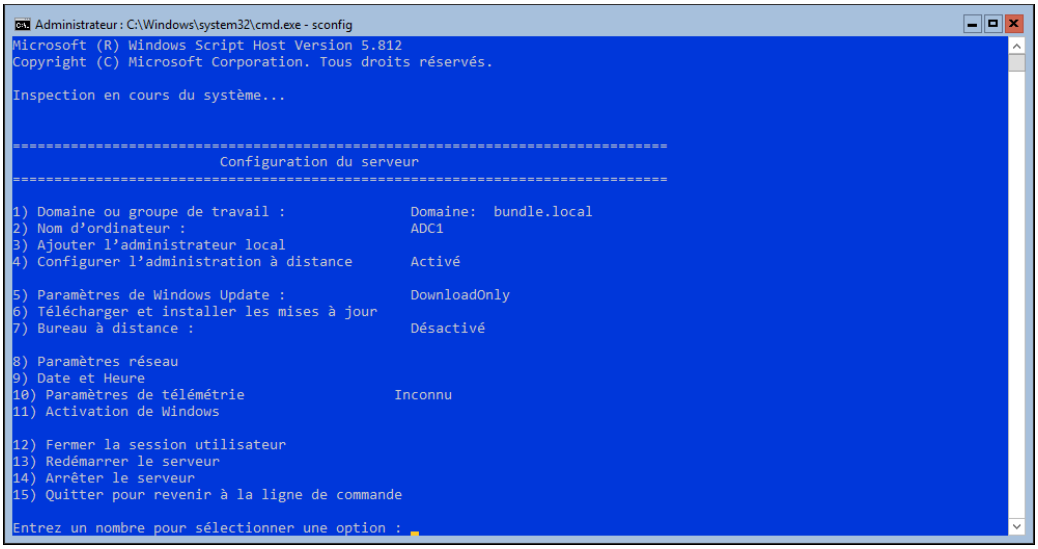
Comme mentionné ci-dessus, ADC1 deviendra notre contrôleur de domaine principal ADC2 sera son équivalent répliqué. Voici les rôles qui seront installés:

Active Directory ***DNS***

Installation du contrôleur de domaine principale (ADC1) et d'Active directory

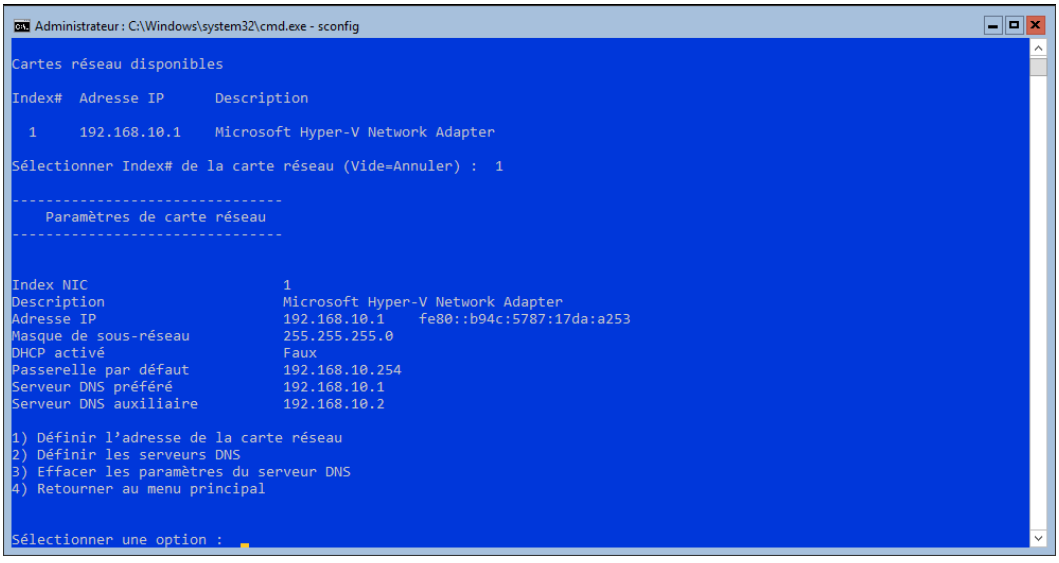
Pour l'installation de Windows server sur ADC1 nous avons choisi la version minimale c'est-à-dire le mode Core. Cette version ne présente pas de mode graphique. C'est une installation qui nécessite moins de ressources que ce soit au niveau processeur, mémoire virtuelle ou même en espace de stockage sur le disque dur. La version Core ne possédant pas d'interface graphique nous allons devoir taper des lignes de commandes pour la configuration du serveur.

Dans un premier temps nous allons écrire « **sconfig** » pour accéder à la configuration du serveur.



Nous configurons une IP statique sur notre serveur avec la fonctionnalité « 8 » : Paramètres réseau.

L'IP de notre contrôleur de domaine est 192.168.10.1 avec pour masque /24 (255.255.255.0). Le fait de choisir le masque en 24 nous laisse 254 IP disponible pour le reste du parc informatique. En ayant 90 utilisateurs c'est un choix favorable.



Nous allons par la suite configurer le Serveur DNS préféré. Avec l'IP 192.168.10.1

Pour la suite nous allons changer le nom du Serveur en ADC1. Pour que le changement soit effectif nous avons besoin de redémarrer la machine.

Gestion des disques de ADC1

Nous allons gérer les disques de ADC1. Il y aura un disque qui contiendra l'installation du système. Ensuite, il y aura le disque nommé "BASE" avec la base AD. Le disque "LOGS", où nous aurons une trace de chaque événement ayant lieu sur le serveur. Et pour finir "SYSVOL" là où il y aura les scripts et GPO stockés. Ces différents lecteurs vont assurer une certaine sécurité. Autrement dit, si le système d'exploitation est endommagé, nous aurons tous les composants nécessaires sur les autres lecteurs.

Pour faire ceci nous utiliserons « **DISKPART** »

Puis il faudra écrire une certaine suite de commande.

```
1   select disk 1
2   online disk
3   attributes disk clear readonly
4   convert gpt
5   covert dynamic
6   create volume simple
7   format quick fs=ntfs label=base
8   assign letter="B"
9
10  select disk 2
11  online disk
12  attributes disk clear readonly
13  convert gpt
14  covert dynamic
15  create volume simple
16  format quick fs=ntfs label=LOGS
17  assign letter="L"
18
19  select disk 3
20  online disk
21  attributes disk clear readonly
22  convert gpt
23  covert dynamic
24  create volume simple
25  format quick fs=ntfs label=SYSVOL
26  assign letter="BS"
```

- On sélectionne le disque que l'on veut configurer.
- On le met en ligne.
- On enlève le fait qu'il soit en lecture seule.
- On l'initialise en GPT.
- On le convertit en dynamique.
- On crée le volume du disque.
- On formate le disque en NTFS et on le nomme.
- On lui attribue une lettre.

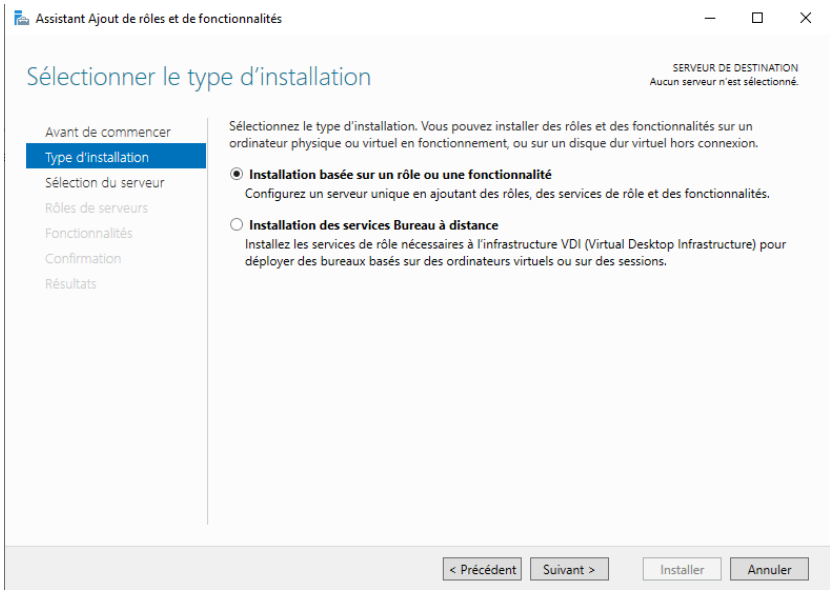
```
C:\Users\Administrateur>diskpart

Microsoft DiskPart version 10.0.17763.1

Copyright (C) Microsoft Corporation.
Sur l'ordinateur : ADC1

DISKPART> list disk

  N° disque  Statut         Taille   Libre    Dyn  GPT
  ---------  -------------  -------  -------  ---  ---
  Disque 0    En ligne        127 G octets      0 octets        *
  Disque 1    En ligne       4096 M octets      0 octets   *    *
  Disque 2    En ligne       4096 M octets      0 octets   *    *
  Disque 3    En ligne       4096 M octets      0 octets   *    *

DISKPART>
```

Installation du rôle Active Directory

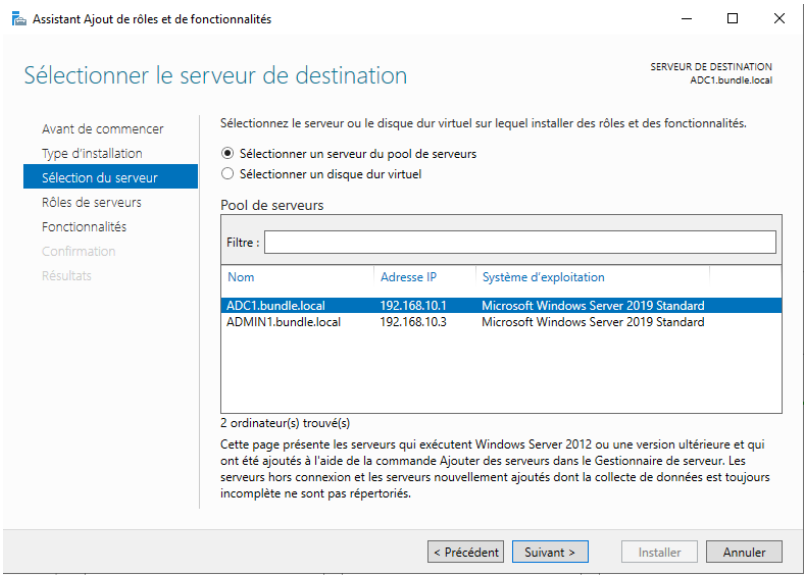
Le but des services de domaine Active Directory est de stocker les données d'annuaire et de gérer les communications. Les services de domaine Active Directory ou AD et DS gèrent la communication entre les utilisateurs, le processus de connexion, la recherche dans l'annuaire et l'authentification.

Nous allons voir comment installer et configurer AD DS depuis l'interface graphique et en mode Core (minimale avec ligne de commande)

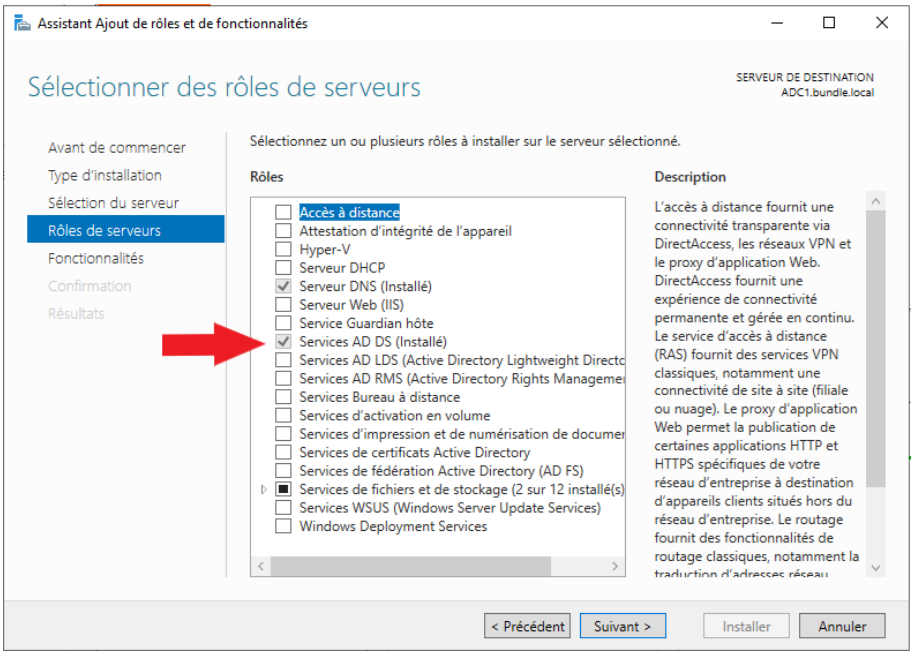
Dans un premier temps nous allons utiliser l'assistant d'ajout de rôles et de fonctionnalités



Après avoir cliqué sur suivant nous allons choisir le serveur sur lequel nous voulons installer AD DS dans notre cas sur ADC1 (Domain Contrôler)



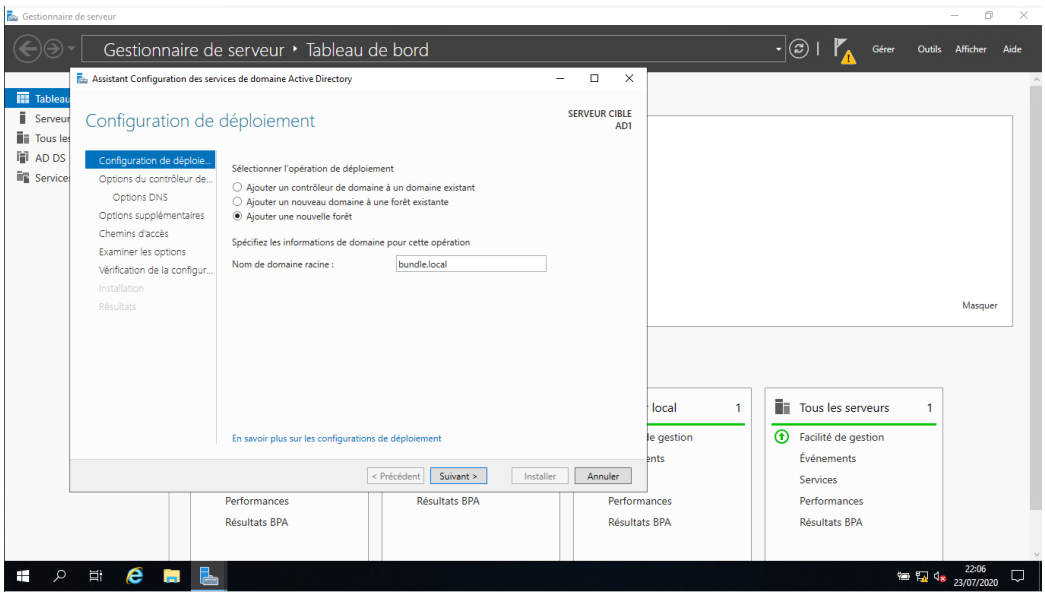
Et pour finir nous allons choisir le rôle en question : « Services AD DS »



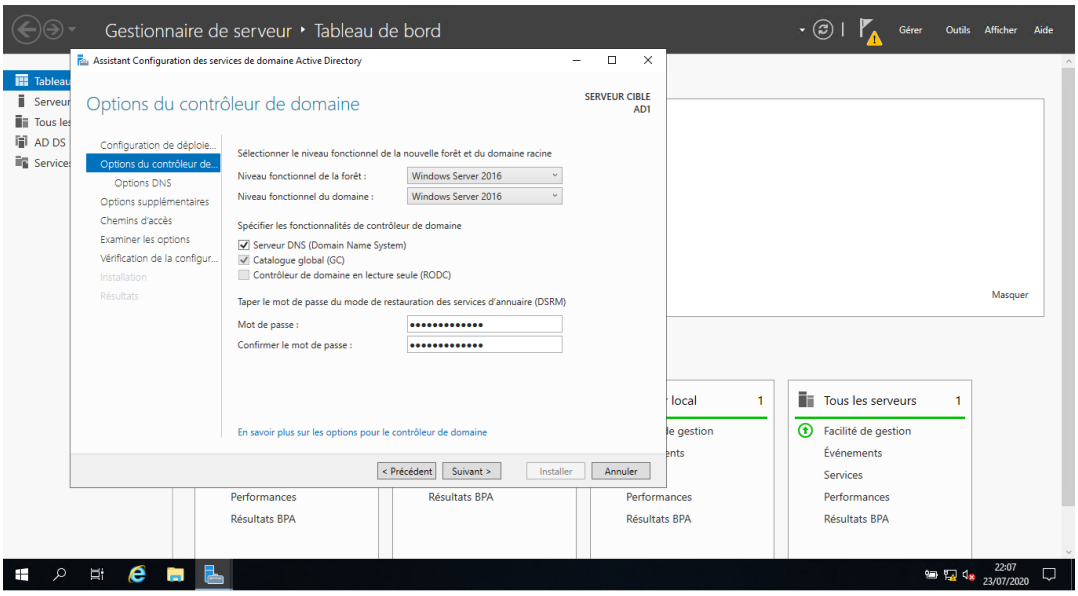
Nous avons bien installé le rôle, cependant il n'est pas encore configuré donc nous allons devoir le promouvoir !

Il faudra ensuite cliquer sur le drapeau avec le panneau jaune et puis choisir « Promouvoir ce serveur en contrôleur de domaine »

Il faut ensuite choisir d'ajouter une nouvelle forêt et renseigner notre nom de domaine « bundle.local »



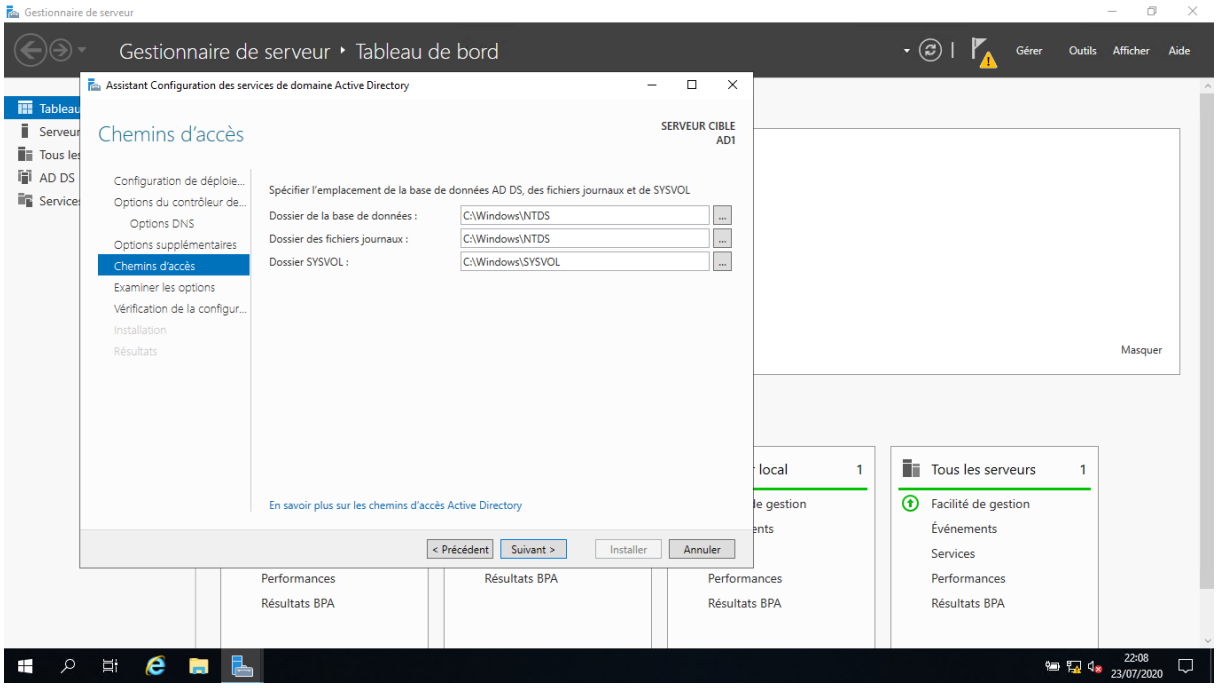
Après avoir appuyé sur suivant on va spécifier les fonctionnalités de ce contrôleur de domaine et lui ajouter un mot de passe



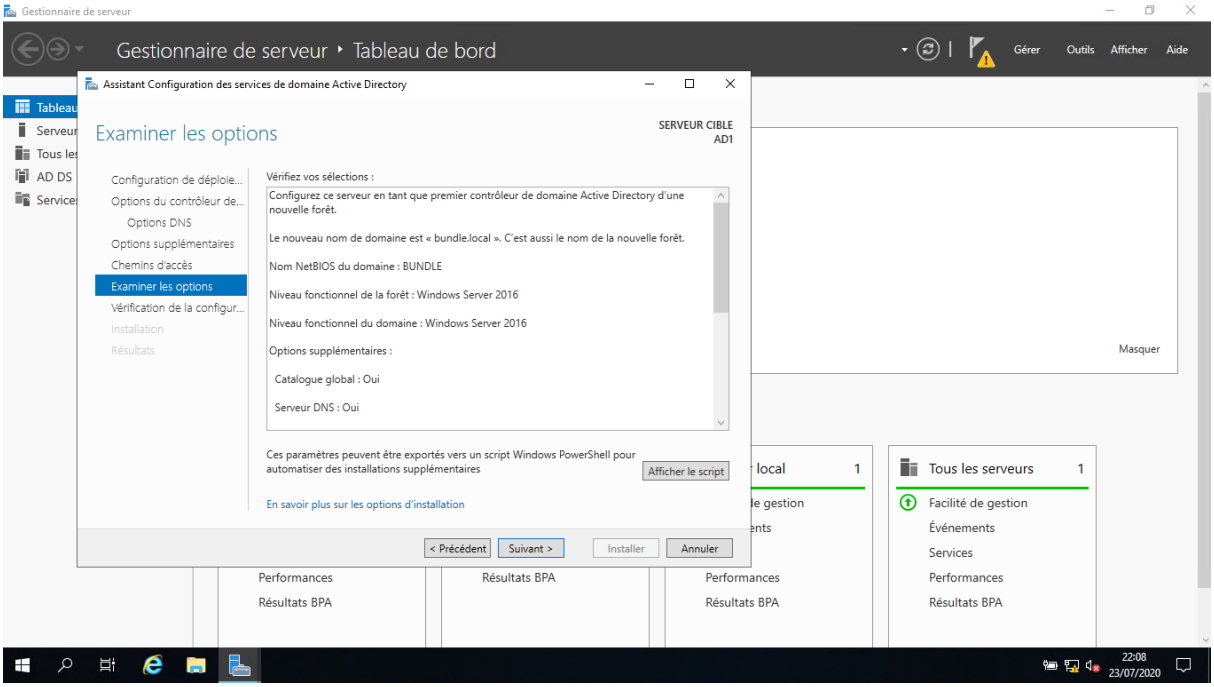
Vérifier le nom NetBIOS, en l'occurrence BUNDLE

Puis choisir un chemin d'accès de la base de données, des logs et de Sysvol.

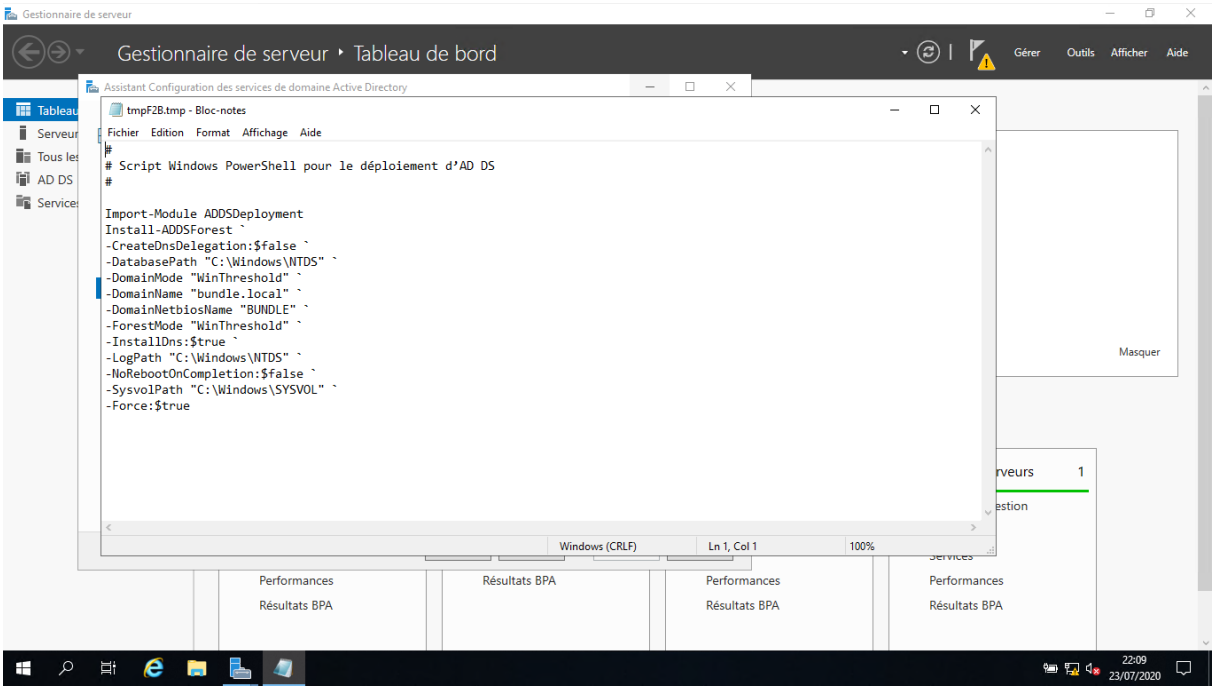
(Dans ce cas image non contractuelle, ne pas prendre en compte NTDS, nous avons installé ADDS en ligne de commande)



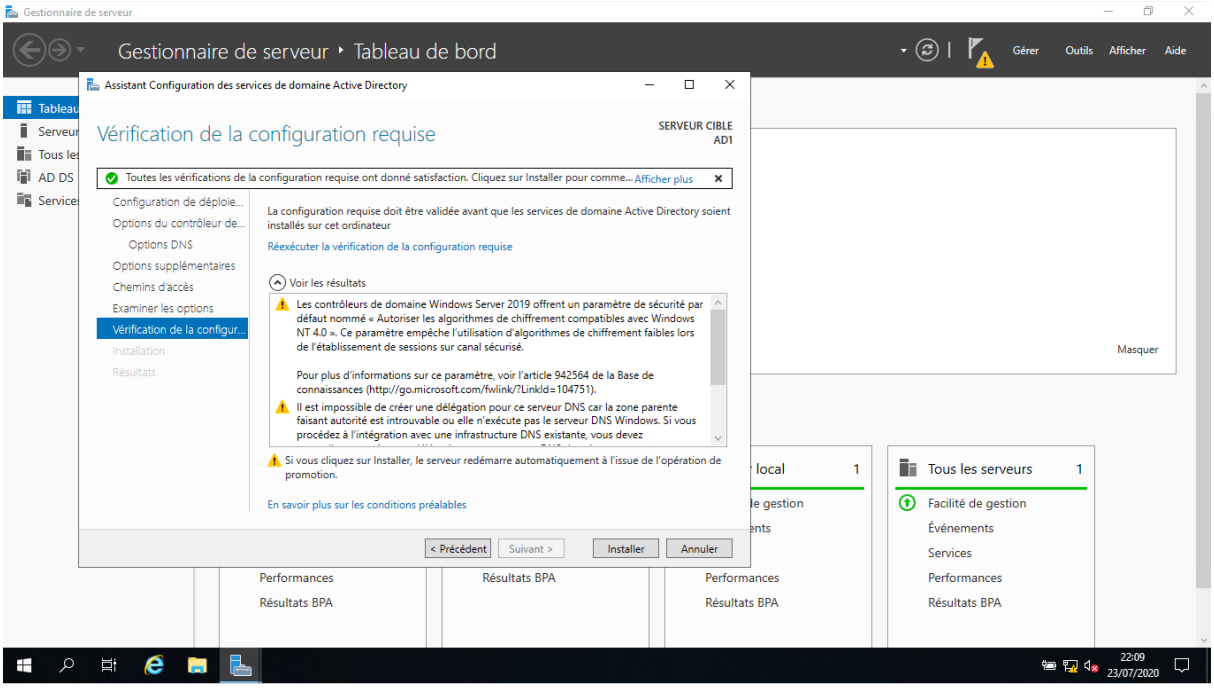
Une fois avoir fait ça, nous pouvons voir un récapitulatif de nos différents choix avant validation.



Nous pouvons aussi cliquer sur « Afficher le script » pour voir les lignes de commandes à écrire si nous voulons l'installer sans le mode graphique.



Toutes les vérifications de la configuration requise ont donné satisfaction, nous allons donc cliquer sur Installer.



Le DHCP

Qu'est-ce que le DHCP et pourquoi l'utiliser.

DHCP signifie Dynamic Host Configuration Protocol. C'est un protocole qui permet à un ordinateur qui se connecte à un réseau d'obtenir de manière dynamique, (c'est-à-dire sans intervention particulière) sa configuration (principalement la configuration du réseau). Il vous suffit de dire à l'ordinateur de trouver l'adresse IP lui-même via DHCP. L'objectif principal est de simplifier l'administration du réseau.

Quel que soit le mode d'attribution le service DHCP est particulièrement utile.

- Pour éviter les erreurs liées à la configuration manuelle des clients.
- Pour permettre de cloner des ordinateurs qui n'ont pour seule différence que leur configuration réseau.
- Pour faciliter les modifications de configurations réseaux comme le changement d'adresse d'un routeur ou d'un serveur de noms.

En conclusion Le service DHCP se compose de deux parties :

- Une méthode d'attribution de numéro IP à la machine cliente.
- Un protocole permettant la transmission de paramètres de configuration complémentaires.

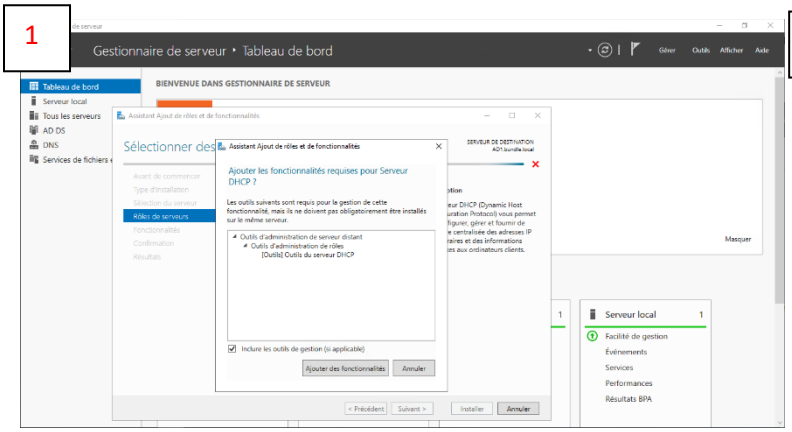
Le service DHCP est construit sur un modèle Client/serveur.

- Serveur qui fournit des paramètres d'initialisation réseau.
- Client qui demande l'obtention de paramètres d'initialisation pour s'intégrer au réseau local.

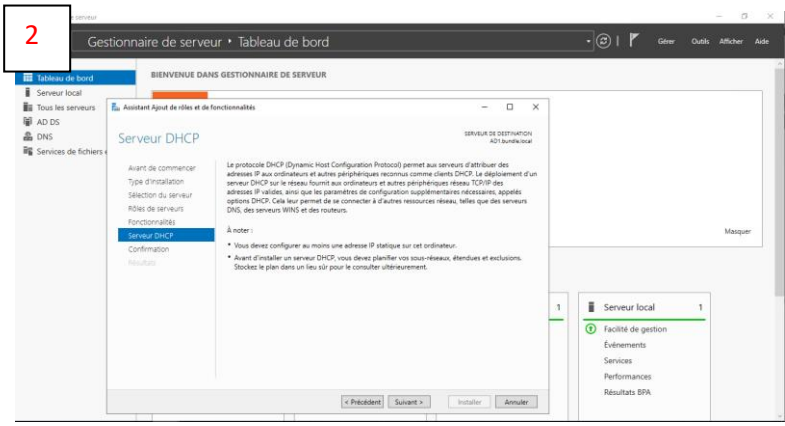
Installation DHCP

Pour commencer nous allons installer le rôle DHCP avec l'assistant ajout de rôle et fonctionnalité.

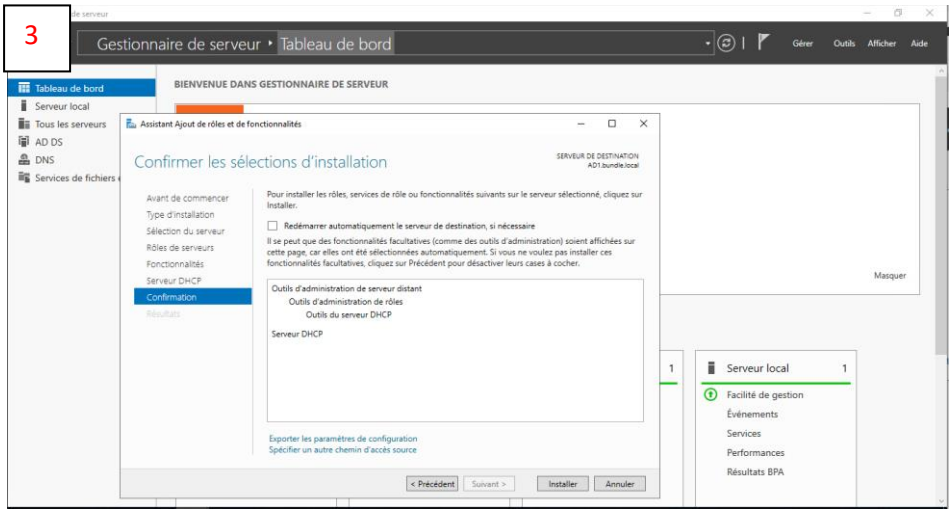
1



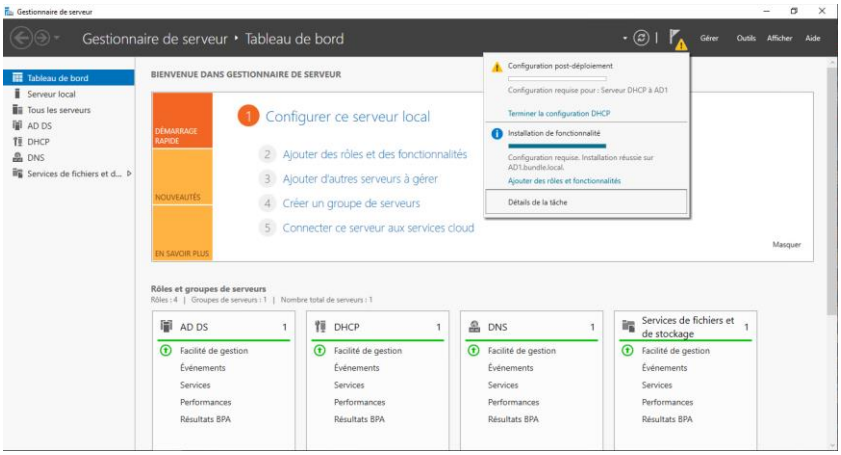
2



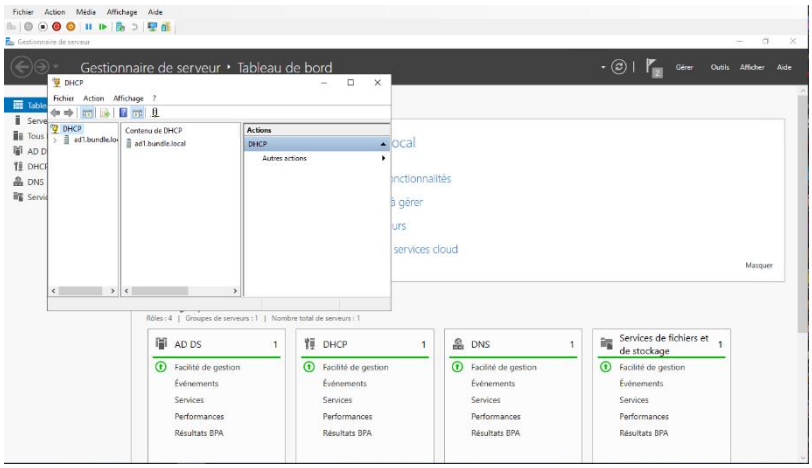
3



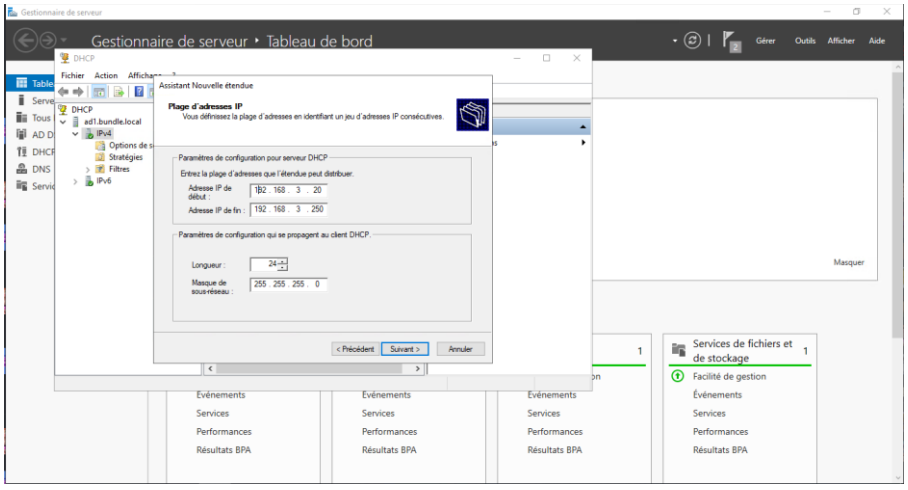
Nous allons ensuite cliquez sur « Terminer la configuration du DHCP »



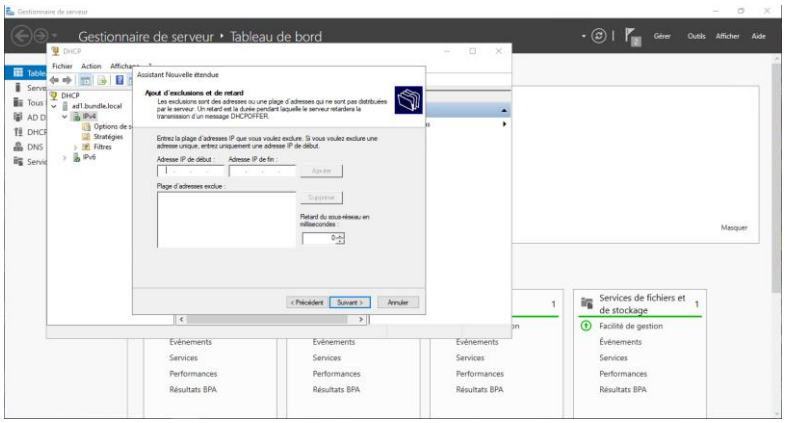
Nous avons donc la console DHCP où nous pourrons le configurer plus en détail et le mettre en action.



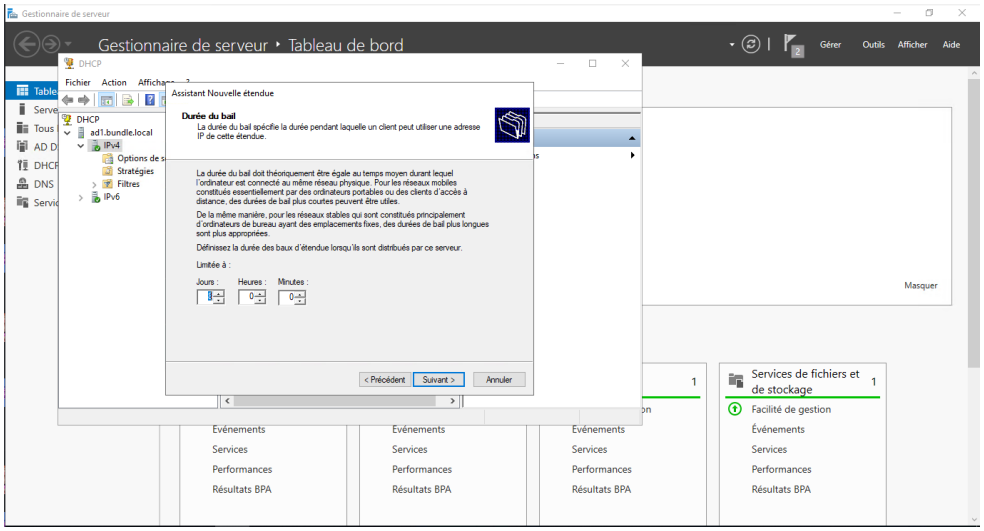
Il faut créer une nouvelle étendue, après avoir cliqué sur suivant nous devons renseigner la plage d'adresse à distribuer dans notre cas 192.168.10 20 à192.168.10.250 (l'image avec comme IP 192.168.3 est la première maquette que nous n'avons pas retenu, mais le principe est le même pour la configuration du DHCP)



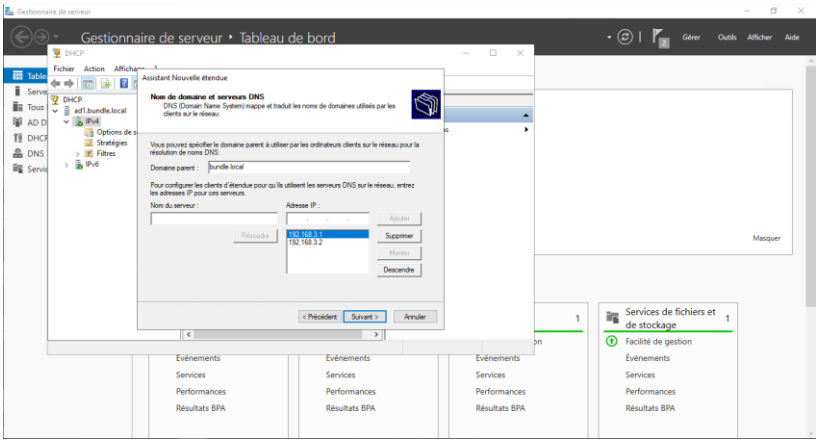
Nous pouvons aussi exclure une plage d'adresse ou une adresse qui n'est pas distribuée par le service DHCP.

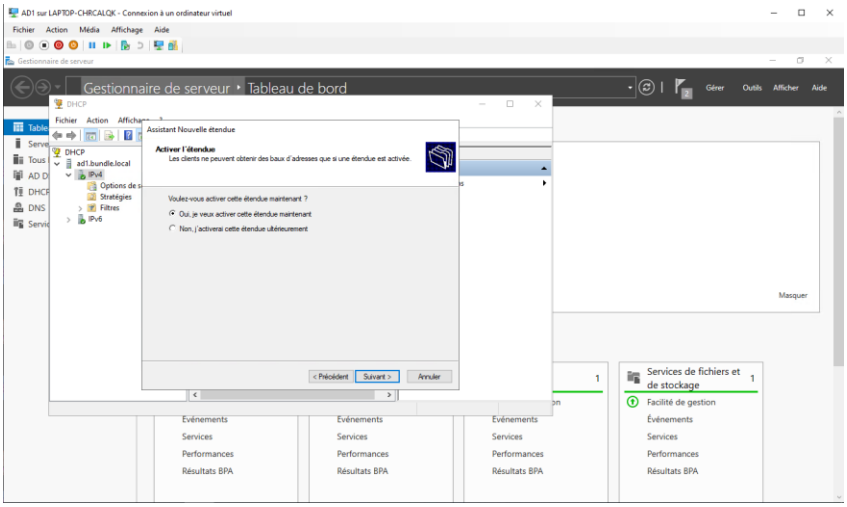


La prochaine étape est de choisir la durée du bail c'est-à-dire la durée que va conserver une machine avec la même adresse IP, dans notre cas 8 jours.



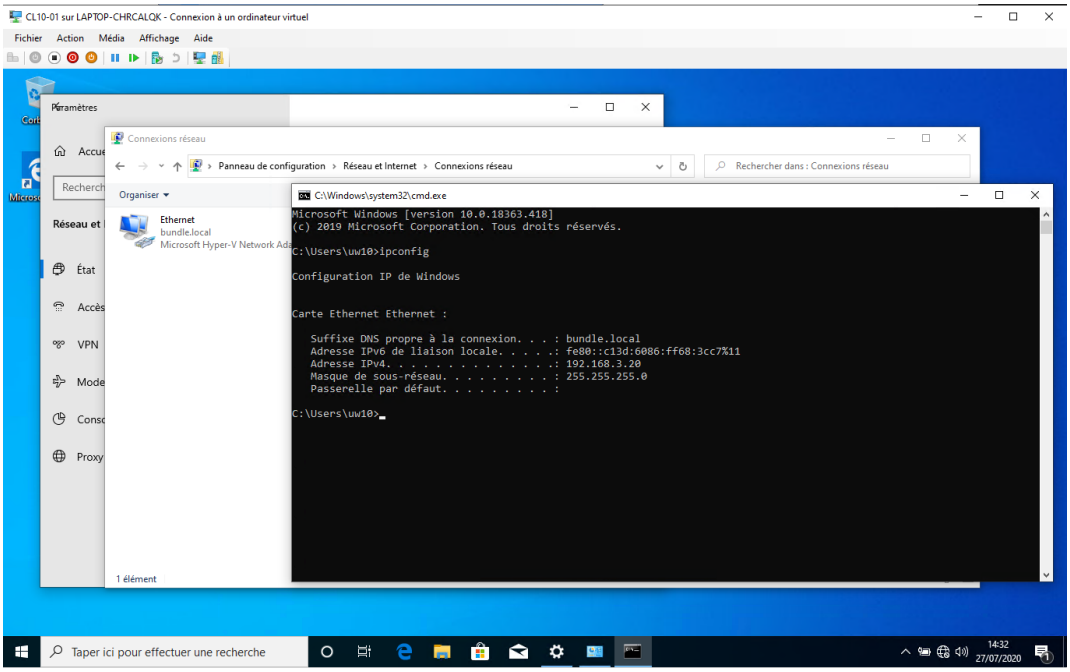
Nous allons lui indiquer le DNS à prendre et choisir d'activer l'étendue maintenant.





Nous voyons en faisant le test sur une machine client avec la configuration d'adressage IP automatique (utilisation du DHCP pour avoir une IP) qu'elle est en 192.168.3.20.

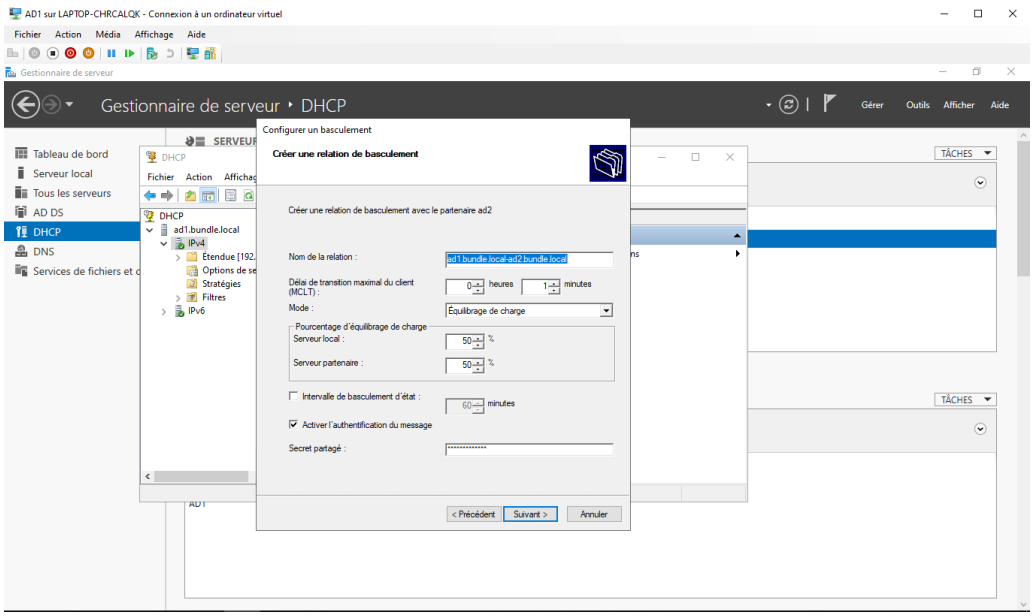
Comme on a configuré l'étendue du DHCP au début à cette même IP.



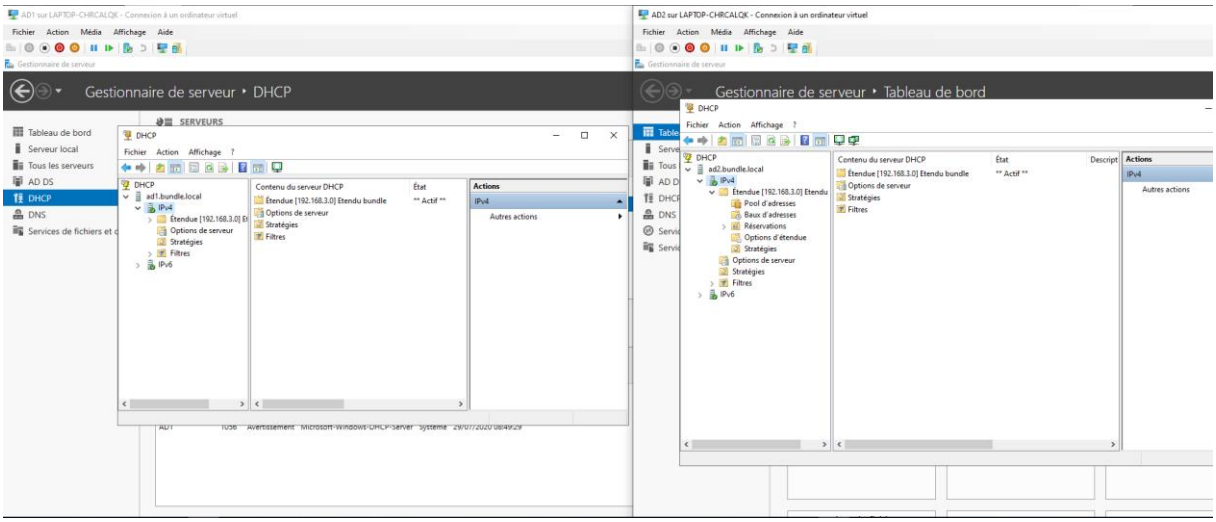
Le 2éme serveur DHCP

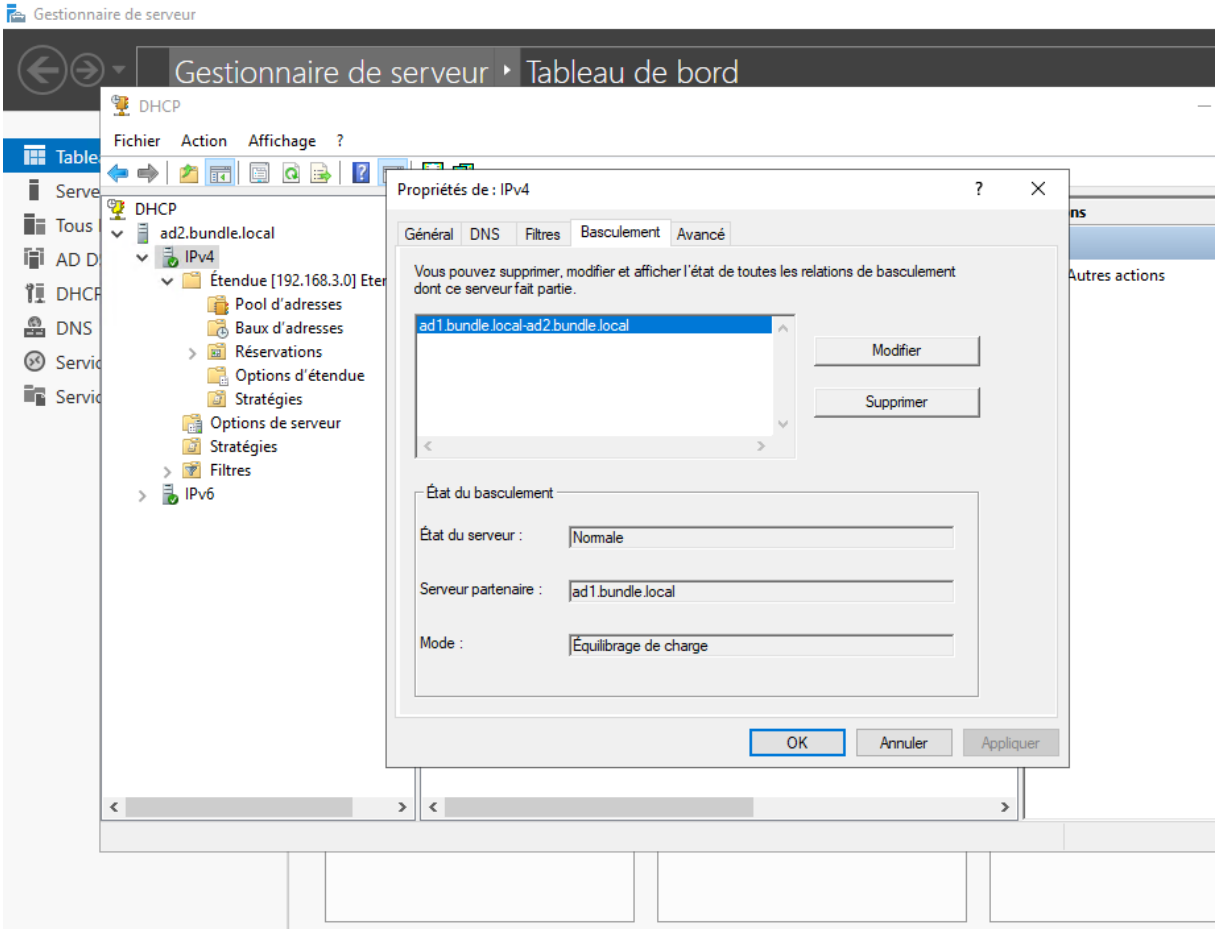
Pour des raisons de sécurité et de tolérances aux pannes, nous installons le rôle DHCP sur un deuxième serveur qui va prendre le relai si le premier serveur à quelques soucis.

Nous configurons le basculement dans un premier temps.



On remarque que le deuxième serveur à effectivement pris la même étendue pour la distribution des IP.

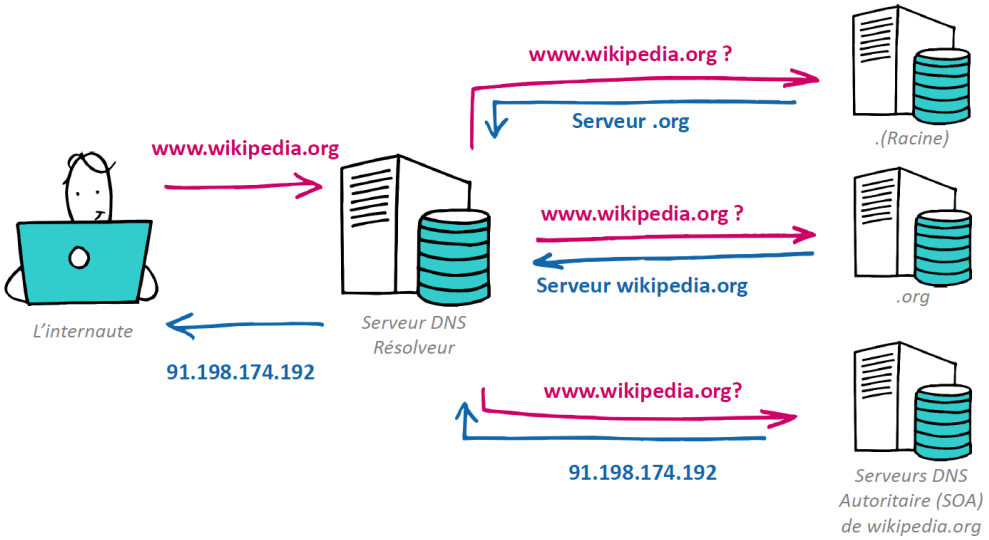




Les serveurs DNS

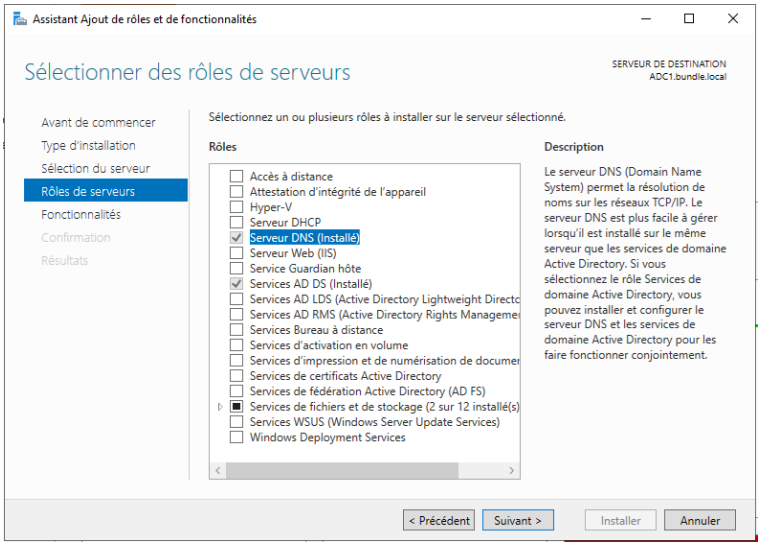
Quel est le rôle d'un serveur DNS ?

Le serveur DNS (Domain Name System) est un service dont la fonction principale est de traduire un nom de domaine en une adresse IP. En termes simples, un serveur DNS agit comme un répertoire qu'un ordinateur utilise pour accéder à un autre ordinateur sur le réseau. Plus precisément, le serveur DNS est ce service qui vous permet d'associer un site Web (ou un ordinateur ou un serveur connecté) à une adresse IP, comme un répertoire téléphonique vous permet d'associer un numéro de téléphone au nom d'un abonné.



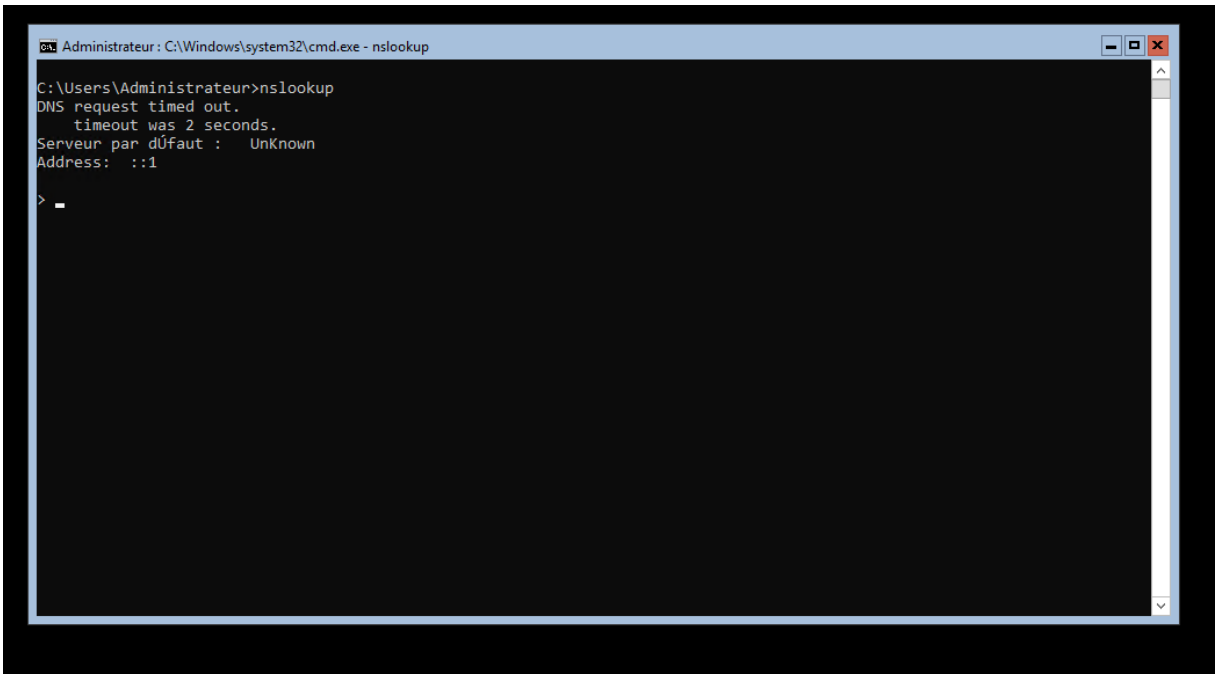
Installation et configuration du DNS

Nous allons donc installer le rôle DNS sur le serveur ADC1 (puis dans un second temps sur le serveur ADC2 pour la réplication).



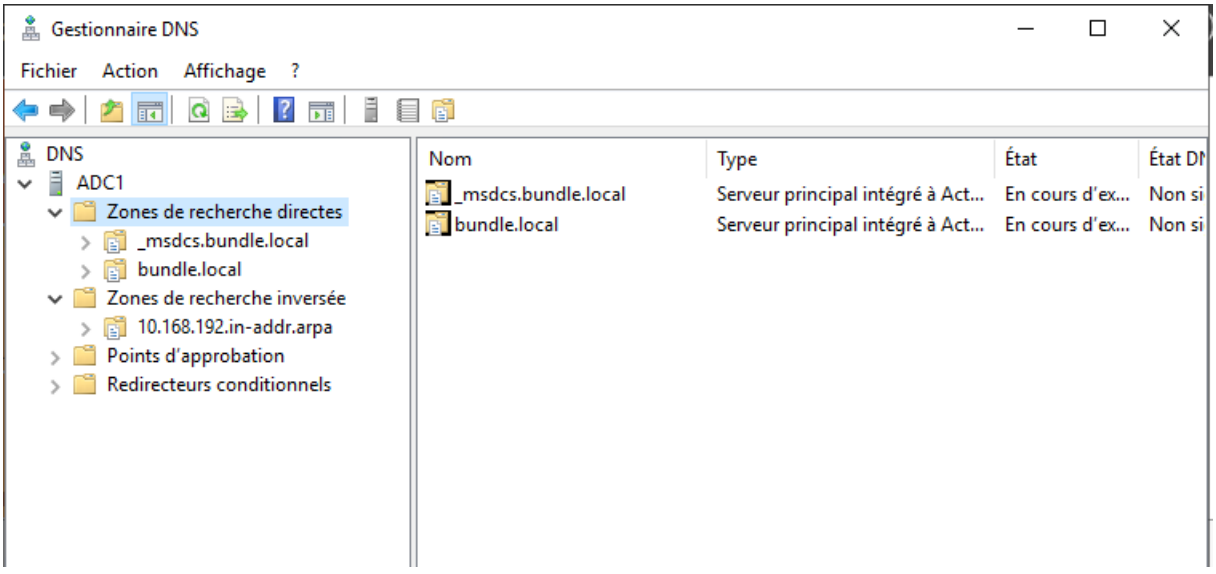
Configuration du DNS

Après installation du rôle DNS nous devons le configurer au préalable, car il n'est pas opérationnel au début. Nous pouvons tester avec la commande « nslookup ».



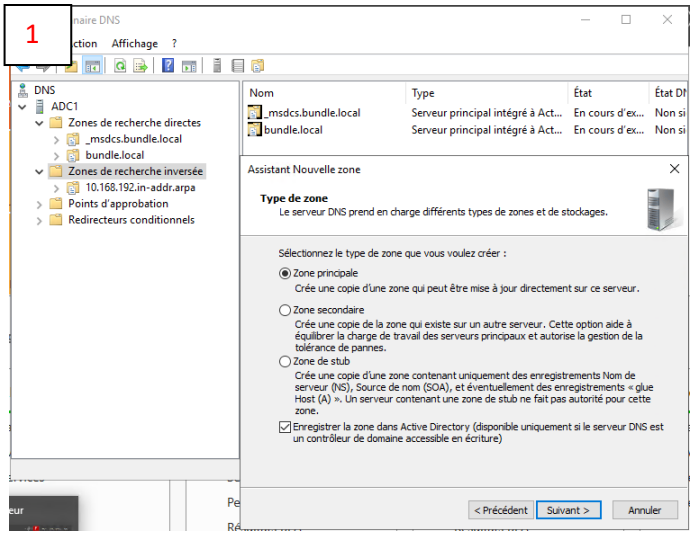
Nous remarquons que le server est « UnKnown » , nous voyons donc qu'il n'est pas encore configuré.

Pour résoudre le problème nous allons créer la zone inverse depuis le ***gestionnaire DNS***.

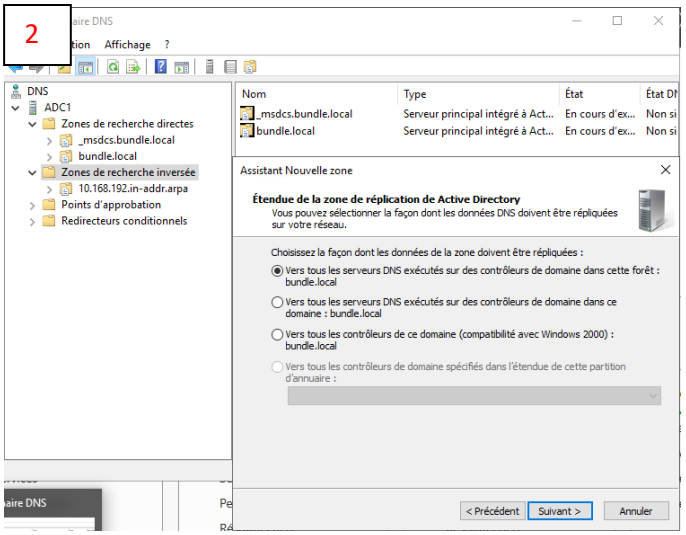


Il faut effectuer un clic droit sur la Zone de recherche inversée, pour faire une nouvelle zone.

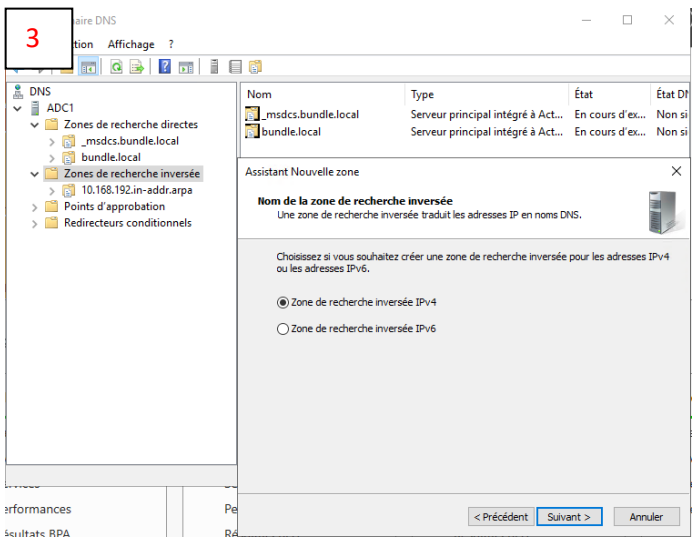
1


Assistant Nouvelle zone
Type de zone
Le serveur DNS prend en charge différents types de zones et de stockages.
Sélectionnez le type de zone que vous voulez créer :
Zone principale
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.
Zone secondaire
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.
Zone de stub
Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.
Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)
< Précédent
Suivant >
Annuler

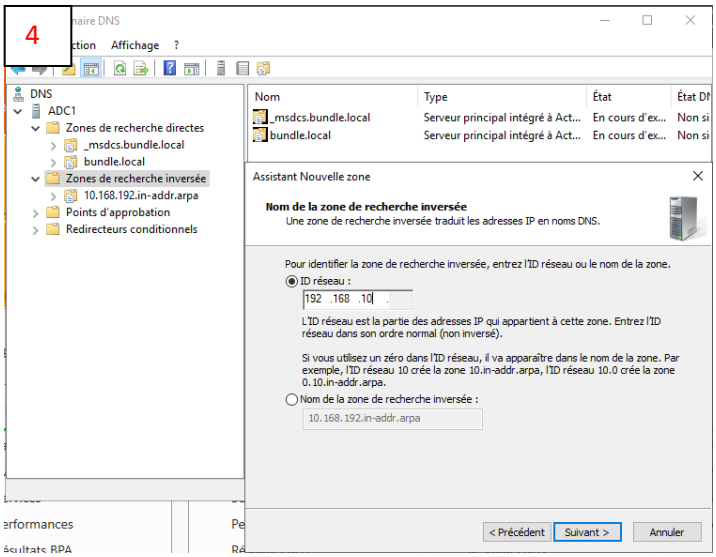
2


Assistant Nouvelle zone
Étendue de la zone de réplication de Active Directory
Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.
Choisissez la façon dont les données de la zone doivent être répliquées :
Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : bundle.local
Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : bundle.local
Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : bundle.local
Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :
< Précédent
Suivant >
Annuler

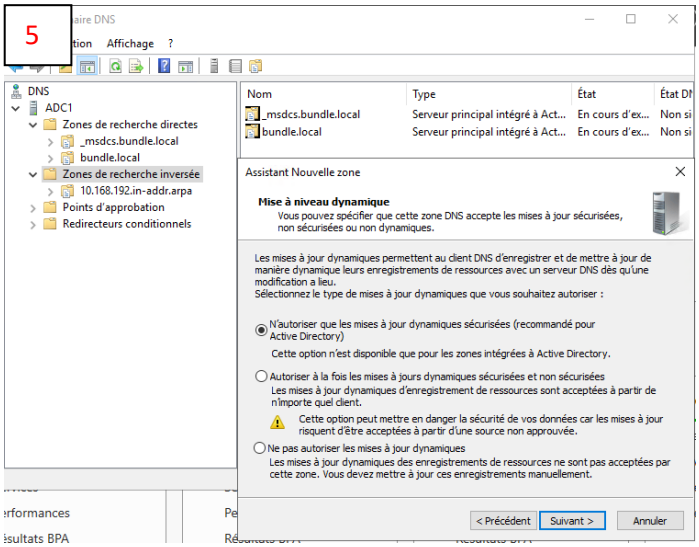
3


Assistant Nouvelle zone
Nom de la zone de recherche inversée
Une zone de recherche inversée traduit les adresses IP en noms DNS.
Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.
Zone de recherche inversée IPv4
Zone de recherche inversée IPv6
< Précédent
Suivant >
Annuler

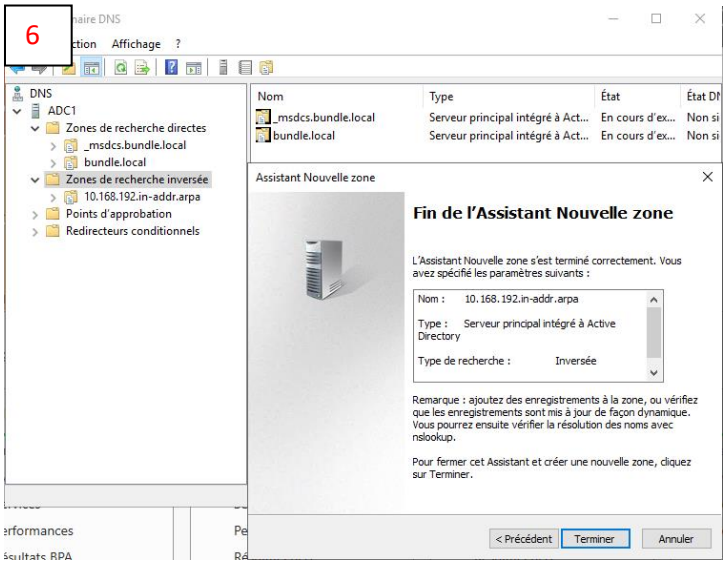
4


Assistant Nouvelle zone
Nom de la zone de recherche inversée
Une zone de recherche inversée traduit les adresses IP en noms DNS.
Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.
ID réseau :
192 .168 .10
L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).
Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.
Nom de la zone de recherche inversée :
10.168.192.in-addr.arpa
< Précédent
Suivant >
Annuler

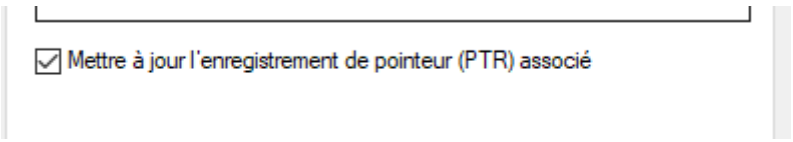
5


Assistant Nouvelle zone
Mise à niveau dynamique
Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.
Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :
N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)
Cette option n'est disponible que pour les zones intégrées à Active Directory.
Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.
Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.
Ne pas autoriser les mises à jour dynamiques
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.
< Précédent
Suivant >
Annuler

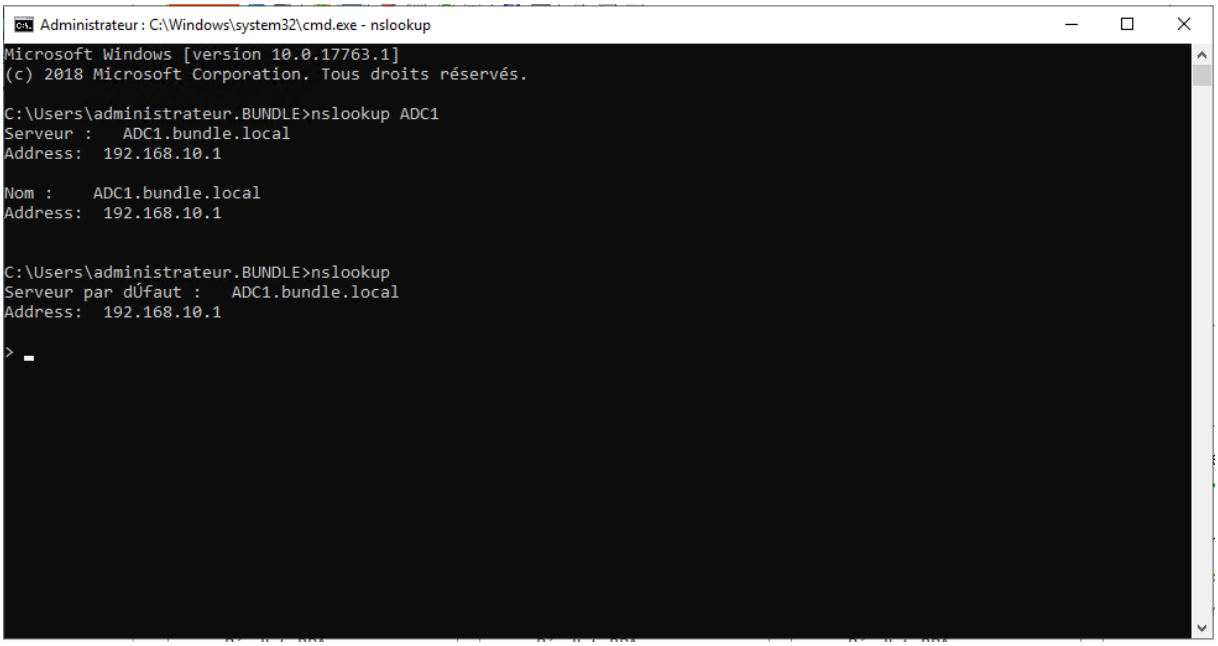
6


Assistant Nouvelle zone
Fin de l'Assistant Nouvelle zone
L'Assistant Nouvelle zone s'est terminé correctement. Vous avez spécifié les paramètres suivants :
Nom : 10.168.192.in-addr.arpa
Type : Serveur principal intégré à Active Directory
Type de recherche : Inversée
Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.
Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.
< Précédent
Terminer
Annuler

Une fois avoir après avoir créé la zone inverse nous devons actualiser le pointeur associé.



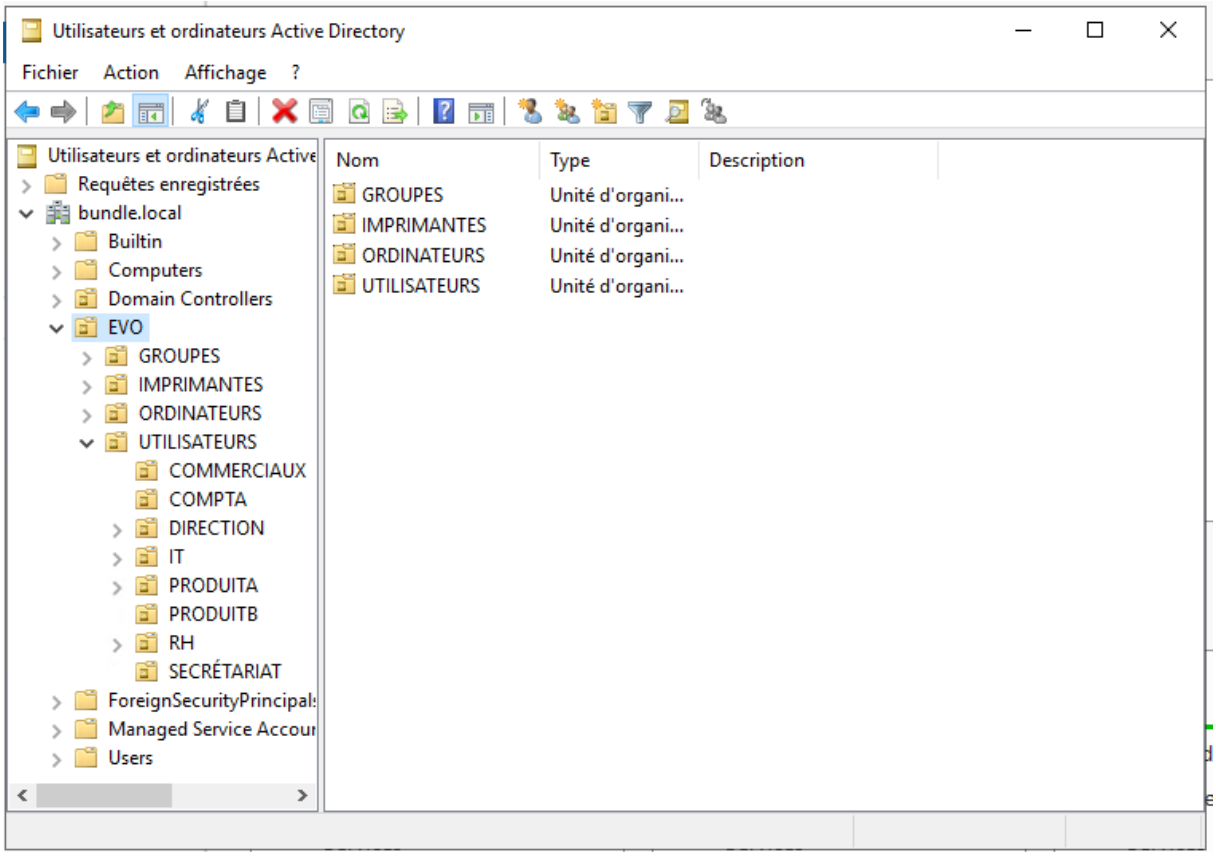
Nous pouvons de nouveau tester la configuration du DNS avec la commande « nslookup ». Dans ce cas, nous voyons le bon message, ce qui confirme que le DNS est bien configuré.



Gestion du parc informatique : Les unités d'organisation

Qu'est-ce qu'un OU (unité d'organisation)

Une unité d'organisation (OU) est un conteneur dans un domaine Microsoft Active Directory qui peut contenir des utilisateurs, des groupes et des ordinateurs. Il s'agit de la plus petite unité par laquelle un administrateur peut attribuer des paramètres de stratégie de groupe ou des autorisations à un compte. Une unité d'organisation peut avoir plusieurs sous unités d'organisation, mais tous les attributs de l'unité d'organisation contenant doivent être uniques.



Nous avons donc créé un OU du nom « EVO » qui contient dans notre cas :

- GROUPES
- IMPIMANTES
- ORDINATEURS
- UTILISATEURS

Nous pouvons aussi remarquer qu'il y différents types d'utilisateurs que nous avons triés en fonction de leurs rôles dans l'entreprise.

Création d'une OU

Nous utilisons des unités d'organisation pour regrouper des comptes, afin de les administrer en tant qu'unité unique. Cela permet de simplifier considérablement la gestion des comptes. Par exemple, on peut joindre un contrôle basé sur la politique à un OU, et tous les comptes au sein de l'OU héritent automatiquement de la politique.

Nous pouvons créer plusieurs unités d'organisation au sein d'une seule organisation. On peut également créer des unités d'organisation au sein d'autres unités d'organisation. Chaque unité d'organisation peut contenir plusieurs comptes, et vous pouvez déplacer des comptes d'une unité à une autre.

Pour réaliser cela nous utilisons un script de création d'OU. Nous avons reçu une liste des employés ainsi que différentes informations les concernant.

```
####### CREATION DES VARIABLES GLOBALES #########
$cheminbase=(Get-ADDomain).distinguishedName   ### Récupération du champ LDAP DN pour le chemin de l'ou
$liste=import-csv -Path "./liste.csv" -Delimiter ";" -Encoding UTF8
$nomou=Read-host "Saisir votre Nom de l'OU de BASE ?"
$cheminou="OU="+$nomou+","+$cheminbase   # Pour le chemin de la première ou racine à créer
$cheminutils="OU=UTILISATEURS,"+$cheminou
$cheminordis="OU=ORDINATEURS,"+$cheminou
$chemingroupes="OU=GROUPES,"+$cheminou

#####################################

function creation_ous()
{
  write-host "Creation des Ous STRUCTURE DE BASE 1er Niveau et Second Niveau"

  #### CREATION 1er NIVEAU OU DE BASE #######
  New-ADOrganizationalUnit -name $nomou -Path $cheminbase -ProtectedFromAccidentalDeletion $false -Verbose

  #### CREATION 2nd NIVEAU OU #######
  New-ADOrganizationalUnit -name "ORDINATEURS" -Path $cheminou -ProtectedFromAccidentalDeletion $false -Verbose
  New-ADOrganizationalUnit -name "UTILISATEURS" -Path $cheminou -ProtectedFromAccidentalDeletion $false -Verbose
  New-ADOrganizationalUnit -name "GROUPES" -Path $cheminou -ProtectedFromAccidentalDeletion $false -Verbose
  New-ADOrganizationalUnit -name "IMPRIMANTES" -Path $cheminou -ProtectedFromAccidentalDeletion $false -Verbose

  ######### CREATION OU 3ème NIVEAU ##################

  New-ADOrganizationalUnit -name "PORTABLES" -Path $cheminordis -ProtectedFromAccidentalDeletion $false -Verbose
  New-ADOrganizationalUnit -name "STATIONS" -Path $cheminordis -ProtectedFromAccidentalDeletion $false -Verbose
  New-ADOrganizationalUnit -name "SERVEURS" -Path $cheminordis -ProtectedFromAccidentalDeletion $false -Verbose
  New-ADOrganizationalUnit -name "NOUVEAUX" -Path $cheminordis -ProtectedFromAccidentalDeletion $false -Verbose

  foreach ($ligne in $liste)
  {
$service=$ligne.service.toUpper()
try {
New-ADOrganizationalUnit -name $service -Path $cheminutils -ProtectedFromAccidentalDeletion $false -Verbose
    }
    catch {}
  }
}

function creation_groupes()
{
 write-host "Creation des groupes"
 ######################### CREATION D'un GROUPE POUR TOUS LES USERS ##################
 New-ADGroup -GroupCategory Security -GroupScope Global -Name GG_TOUS -Path $chemingroupes -Verbose
 New-ADGroup -GroupCategory Security -GroupScope DomainLocal -Name GDL_R_TOUS -Path $chemingroupes -Verbose
 New-ADGroup -GroupCategory Security -GroupScope DomainLocal -Name GDL_RW_TOUS -Path $chemingroupes -Verbose

 ######################### CREATION DES GROUPES PAR SERVICES ######################
 foreach ($ligne in $liste)
 {
```

```
    $service=$ligne.service.toUpper()
    $GG="GG_"+$service #GLOBAL
    $GU="GU_"+$service # UNIVERSEL
    $GDL_R="GDL_R_"+$service  #LECTURE Read
    $GDL_RW="GDL_RW_"+$service #LECTURE ECRITURE Read Write
    $GDL_M="GDL_M_"+$service  #MODIFICATION Modify /Suppression
    $GDL_F="GDL_F_"+$service  #Controle Total Full Admin


try{
New-ADGroup -GroupCategory Security -GroupScope Global -Name $GG -Path $chemingroupes -Verbose
    } catch {}
try{
New-ADGroup -GroupCategory Security -GroupScope Universal -Name $GU -Path $chemingroupes -Verbose
 } catch {}
try{
New-ADGroup -GroupCategory Security -GroupScope DomainLocal -Name $GDL_R -Path $chemingroupes -Verbose
 } catch {}
try{
New-ADGroup -GroupCategory Security -GroupScope DomainLocal -Name $GDL_RW -Path $chemingroupes -Verbose
 } catch {}
try{
New-ADGroup -GroupCategory Security -GroupScope DomainLocal -Name $GDL_M -Path $chemingroupes -Verbose
 } catch {}
try{
New-ADGroup -GroupCategory Security -GroupScope DomainLocal -Name $GDL_F -Path $chemingroupes -Verbose
  } catch {}


 ################## Ajout des groupes dans les groupes (imbrication des membres) ###############

 Add-ADGroupMember $GU -Members $GG -Verbose
 Add-ADGroupMember $GDL_R -Members $GU -Verbose
 Add-ADGroupMember $GDL_RW -Members $GU -Verbose
 Add-ADGroupMember $GDL_M -Members $GU -Verbose
 Add-ADGroupMember $GDL_F -Members $GU -Verbose

 ######## Pour le Groupe GG_TOUS ajout de tous les GG Services ####
 Add-ADGroupMember GG_TOUS -Members $GG -Verbose
 }

 Add-ADGroupMember GDL_R_TOUS -Members GG_TOUS -Verbose
 Add-ADGroupMember GDL_RW_TOUS -Members GG_TOUS -Verbose
}

function creation_users()
{ write-host "Creation des users"

 $password=ConvertTo-SecureString("Form@tion2020") -AsPlainText -Force

foreach ($ligne in $liste)
{
 $prenom=$ligne.prenom.substring(0,1).toUpper()+$ligne.prenom.substring(1).toLower()
 $nom=$ligne.nom.toUpper()
 $nomcomplet=$prenom+" "+$nom
 $sam=$prenom.toLower()+"."+$nom.toLower()
 $upn=$sam+"@"+$env:USERDNSDOMAIN.ToLower()
 $fonction=$ligne.fonction
 $service=$ligne.service.toUpper()
 $description=$ligne.description
 $email=$upn
 $cheminuser="OU="+$service+","+$cheminutils
 $groupe="GG_"+$service

 new-aduser -GivenName $prenom -name $nomcomplet -Surname $nom -DisplayName $nomcomplet `
 -SamAccountName $sam -UserPrincipalName $upn -Title $fonction -Department $service `
 -Description $description -EmailAddress $email -AccountPassword $password `
 -ChangePasswordAtLogon $true -Enabled $true -Path $cheminuser -Verbose

 Add-ADGroupMember $groupe -Members $sam -Verbose


}


}

function permissions()
{ write-host "Permissions NTFS"
}

function suppression()
{ write-host "Suppression Globale"
}

function pause($message="Appuyer sur 1 touche pour poursuivre...")
{
    write-host -NoNewline $message
    $touche=$host.UI.RawUI.ReadKey("NoEcho,IncludeKeyDown")
    write-host ""
}

function menu()
{
 clear-host
 write-host "         MENU PRINCIPAL"
 write-host "         ##############"
 write-host "1 : Création Arborescence des Ous par lot"
 write-host "2 : Création des Groupes de Sécurité par lot"
 write-host "3 : Création des Utilisateurs et Dossiers par lot"
 write-host "4 : Permissions NTFS (Sfic) des dossiers Users et Services"
 write-host "9 : Suppression Globale (Ous/Groupes/Users)"
```

Les GPO

Qu'est-ce qu'une GPO ?

La stratégie de groupe peut contrôler les clés de registre, la sécurité NTFS, les stratégies de sécurité et d'audit, l'installation de logiciels, les scripts d'ouverture de session et de déconnexion, la redirection de dossier et les paramètres d'Internet Explorer. Les paramètres sont stockés dans la stratégie de groupe. Chaque stratégie de groupe a un identifiant unique appelé GUID («Global Unique Identifier»). Chaque stratégie de groupe peut être liée à un ou plusieurs domaines, sites ou unités organisationnelles. Cela permet à plusieurs ordinateurs ou objets utilisateurs d'être contrôlés avec une seule stratégie de groupe et réduit par conséquent le coût global d'administration de ces éléments.

Création et édition des stratégies de groupe :

Les stratégies de groupe peuvent être éditées au travers de deux outils – le Group Policy Object Editor (Gpedit.msc) et la Group Policy Management Console (gpmc.msc). GPEdit est utilisé pour créer et éditer une stratégie de groupe de façon unitaire. La GPMC simplifie grandement la gestion des stratégies de groupe en fournissant un outil permettant une gestion centralisée et collective des objets. La GPMC inclut de nombreuses fonctionnalités telles que la gestion des paramètres, un panneau pour la gestion du filtrage par groupe de sécurité, des outils de sauvegarde et de restauration et d'autres outils graphiques intégrés à la MMC. Le nom d'une stratégie de groupe peut être déterminé en utilisant l'outil GPOTool.exe.

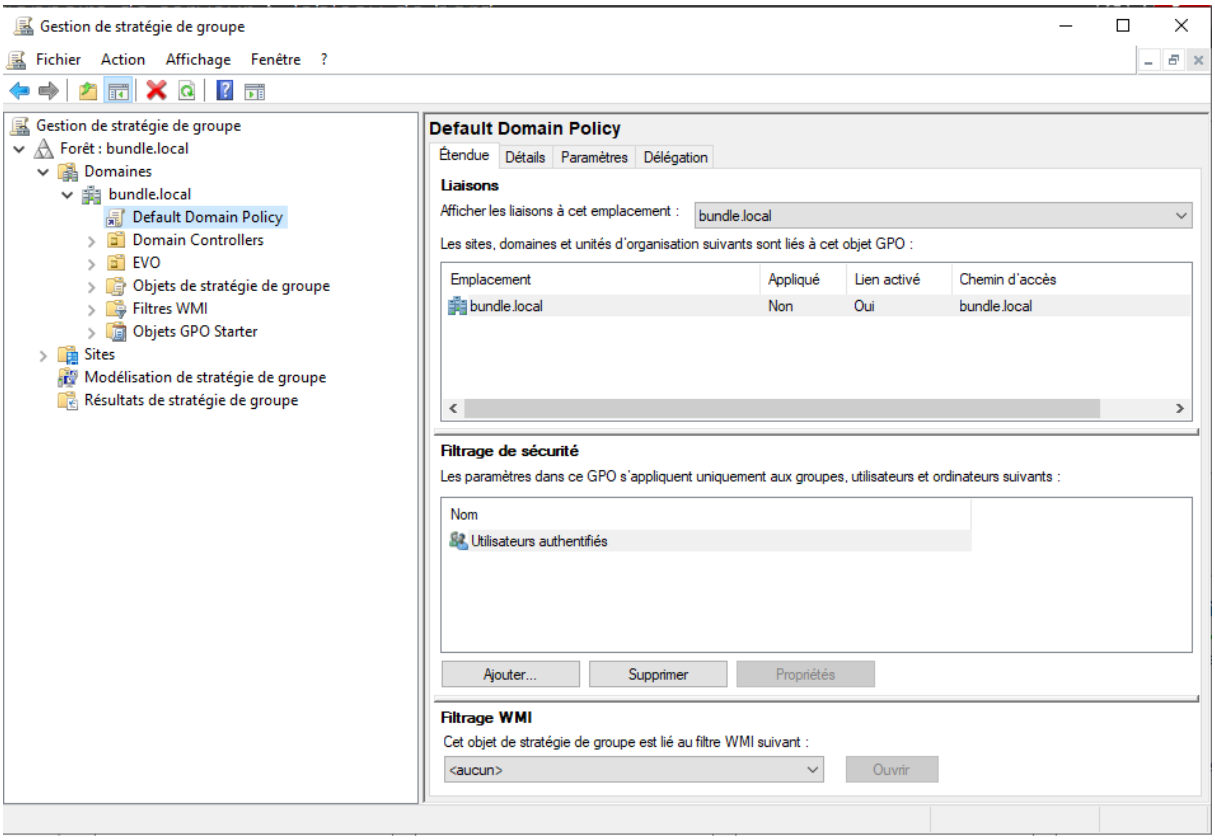
Liaison des stratégies de groupe :

Après avoir créé une stratégie de groupe, elle peut être liée à un site Active Directory, à un domaine, ou à une unité d'organisation (UO).

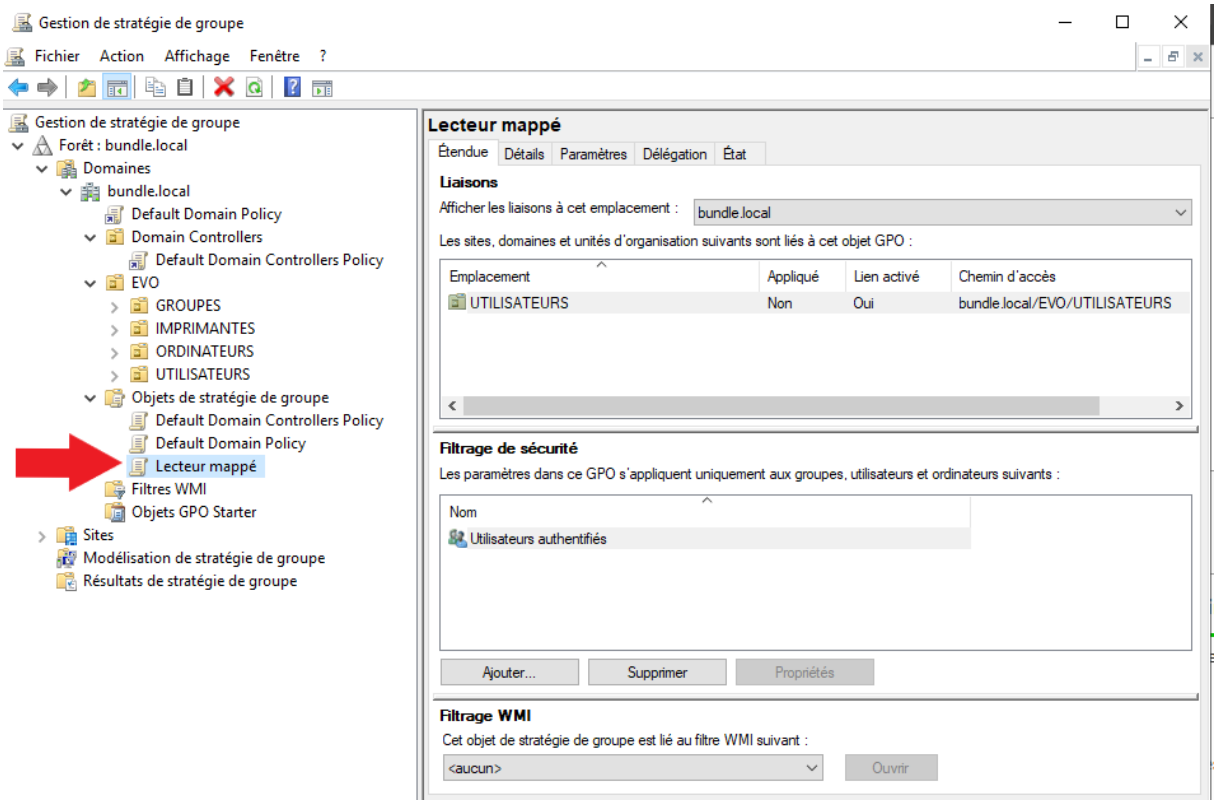
Application des stratégies de groupe :

Le client de stratégie de groupe du poste récupère la configuration (de base dans un intervalle aléatoire compris entre 1h et 2h , mais cela est configurable via les stratégies de groupe) qui est applicable à l'ordinateur et à l'utilisateur connecté et l'applique en tenant compte des différents critères de filtre, de sécurité et d'héritage.

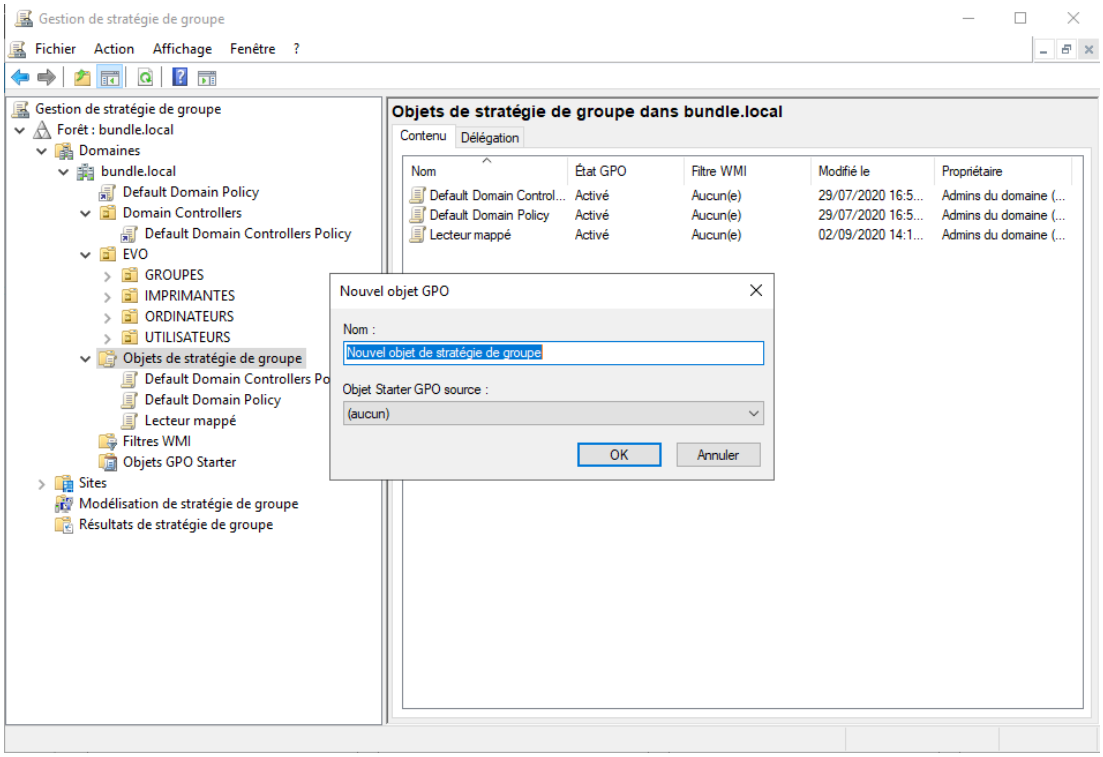
Nous arrivons donc sur la fenêtre de Gestion de stratégie de Groupe, ou nous pouvons voir où sont les GPO.



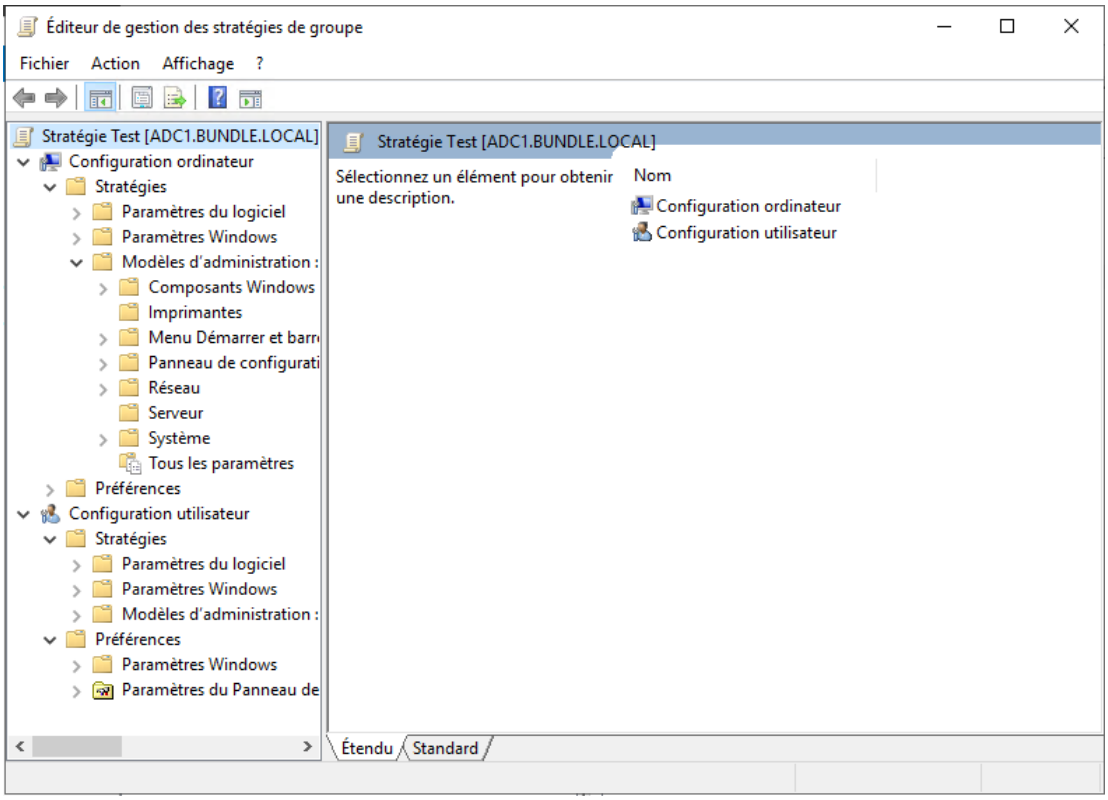
Comme par exemple avec la GPO qui fait remonter un lecteur réseau.



Pour la création d'une GPO il faut faire un clic droit puis sélectionner « Nouveau »



Après avoir fait la GPO, elle ne sera pas effective de suite. Il faut donc la configurer en faisant un clic droit sur la GPO en question puis faire « modifier ». Après avoir fait cela nous arrivons sur une fenêtre ou nous pouvons choisir la configuration de notre future GPO.



Les GPO vont faire respecter certains prérequis du cahier des charges. Comme par exemple :

Surveillance de ce qui se passe sur les ordinateurs, nous avons mis en place des journaux d'évènements qui regroupent les évènements. Nous avons configuré :

- Journal de sécurité

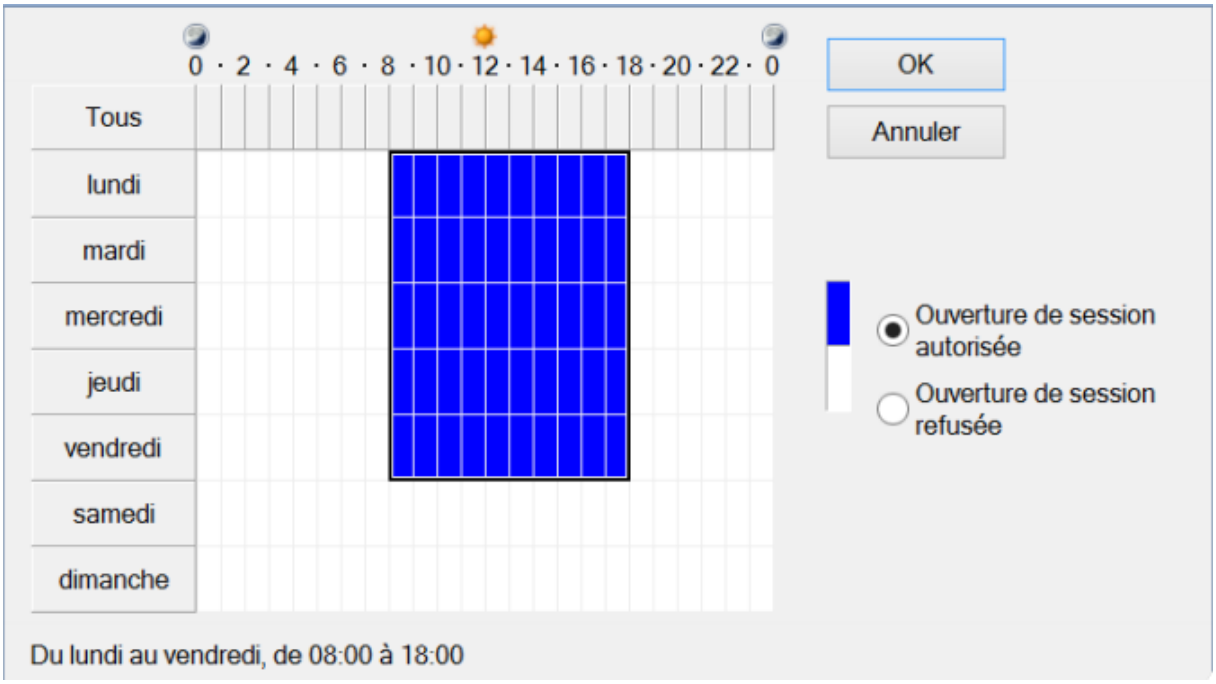
- Journal des applications

- Journal d'évènement système

Comme demandé dans le cahier des charges, nous avons désactivé le moniteur d'évènement à la mise hors tension.

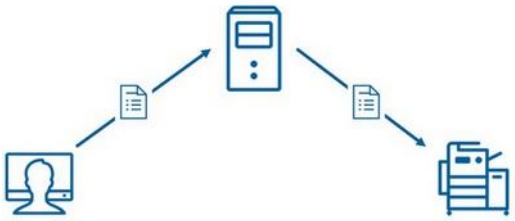
Afin de respecter le cahier des charges, nous avons mis en place des restrictions d'horaires pour l'ouverture et la fermeture de sessions.

- Mme BEZIAT, ELLA, AYO et ACIEN ne peuvent se connecter qu'entre 08 heures et 18 heures et à 19 heures elles doivent être déconnectées (elles sont du service Produit A)



Le serveur d'impression

Un serveur d'impression est un serveur qui permet de partager une ou plusieurs imprimantes entre plusieurs utilisateurs (ou ordinateurs) situés sur un même réseau informatique.



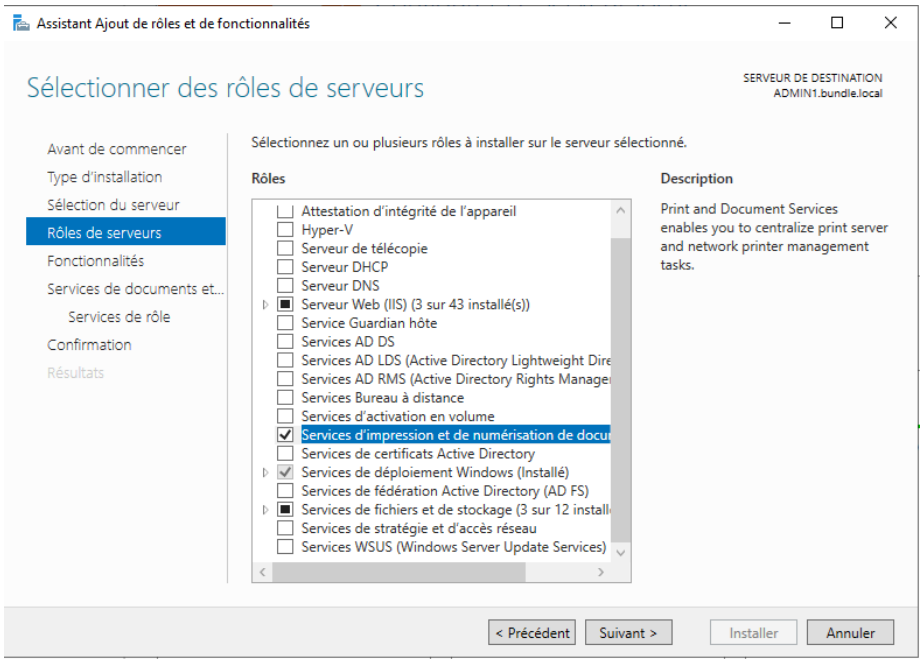
C'est sans doute le moyen le plus courant aujourd'hui, et de manière écrasante avec le système d'exploitation Windows. Leur intérêt principal est de centraliser la gestion des pilotes d'impression. Une fois les imprimantes et leurs pilotes configurés sur le serveur, cela leur permet d'être installés rapidement sur un ou plusieurs postes clients, l'autre avantage de cette technologie est que tout changement dans la configuration des pilotes sur le serveur s'appliquera automatiquement à tous les postes de travail.

Installation du serveur d'impression

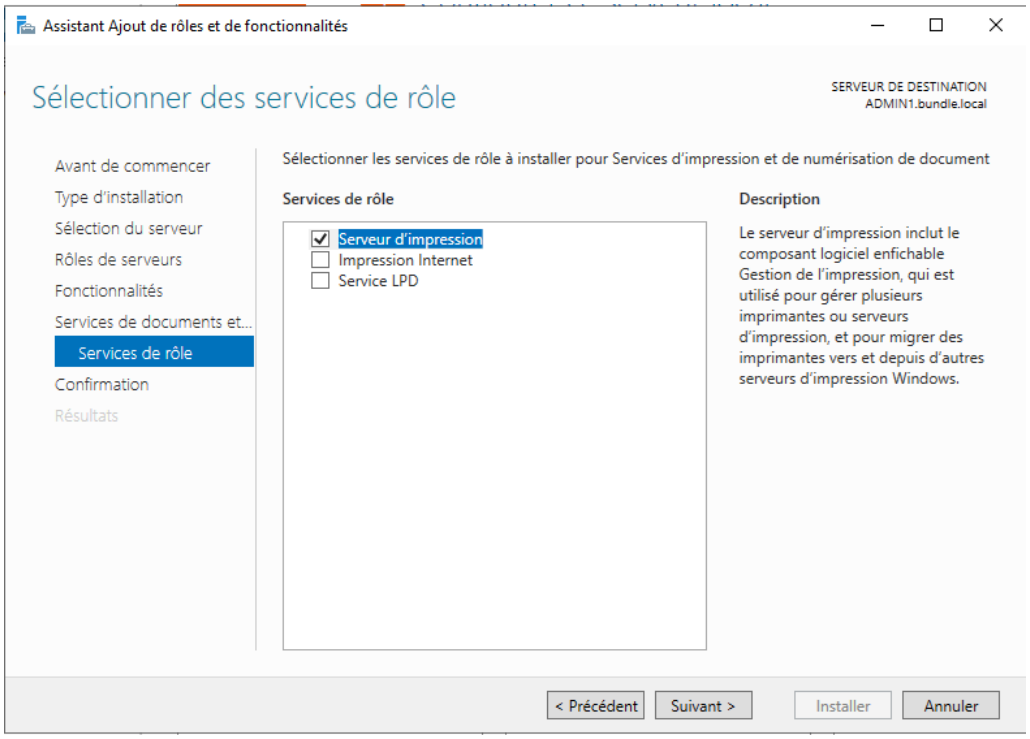
Dans le Gestionnaire du serveur, cliquer sur « Gérer »,

Puis « ajouter des rôles et des fonctionnalités ».

Sélectionner « Services d'impression et de numérisation de document »



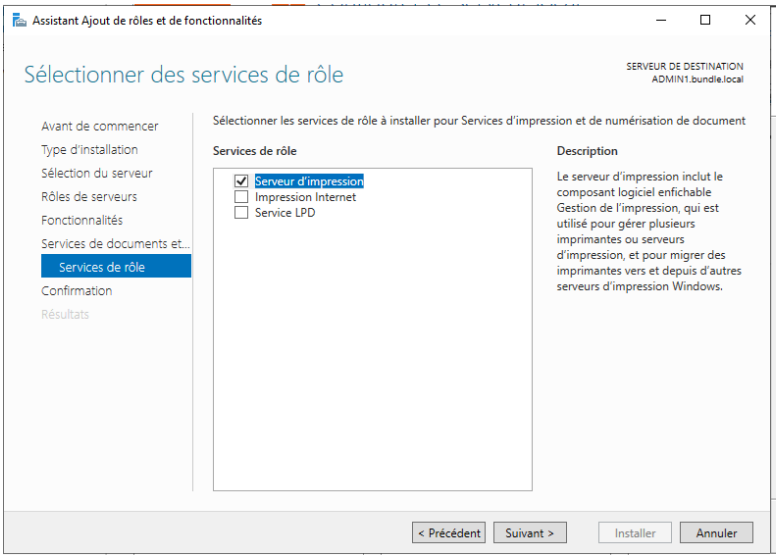
Puis dans service de rôle il faut choisir « Serveur d'impression »

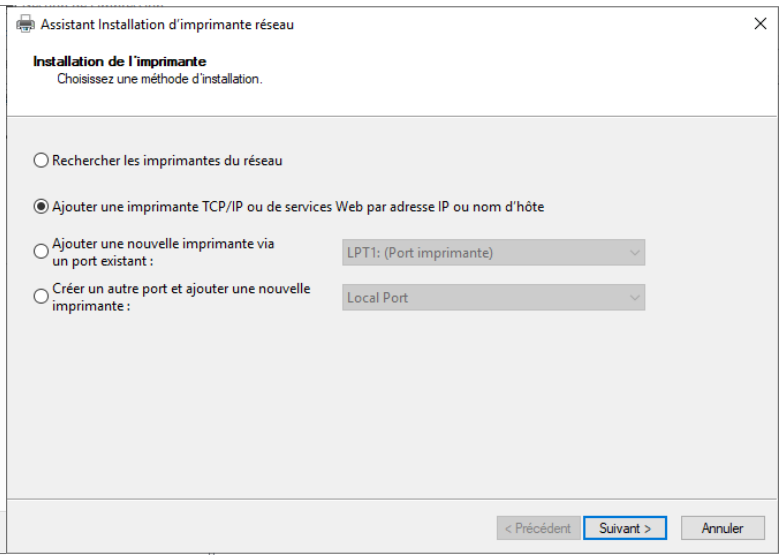


Configuration et gestion de l'impression

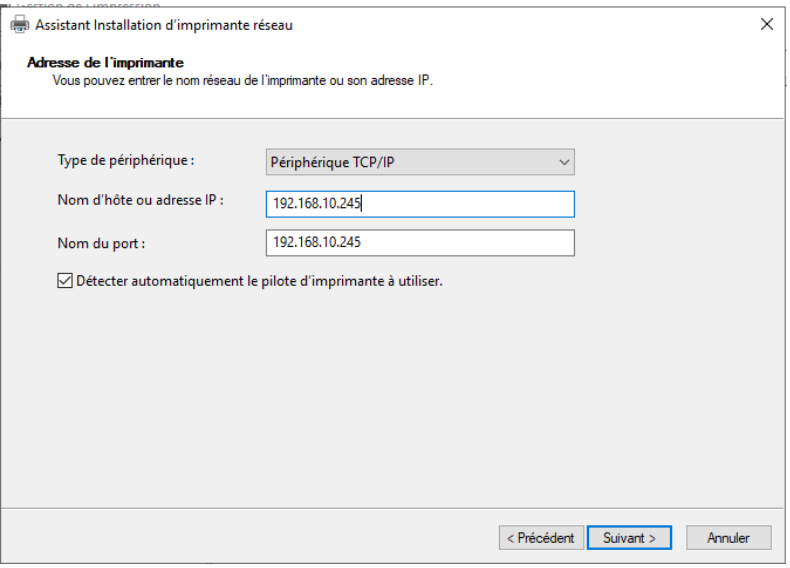
Dans un premier temps il va falloir ouvrir la console de gestion de l'impression puis y ajouter une nouvelle imprimante (ou copieur).

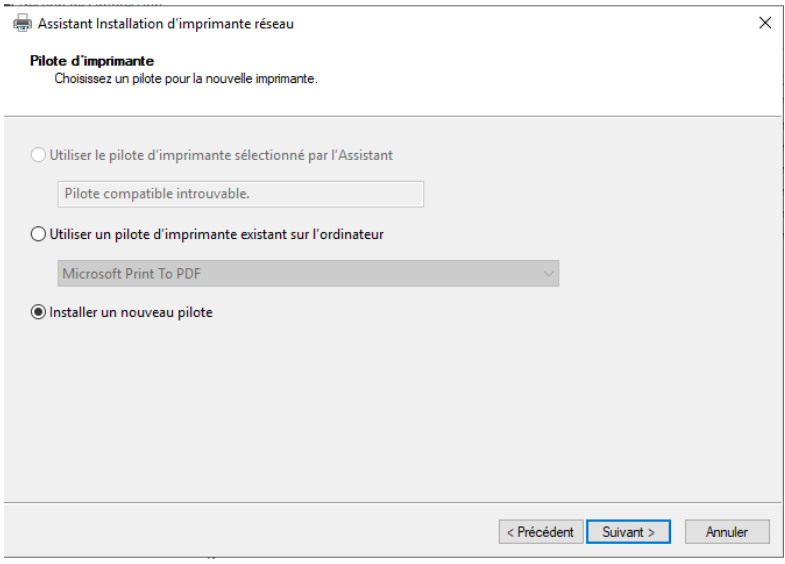
Ensuite il faudra choisir l'option TCP/IP





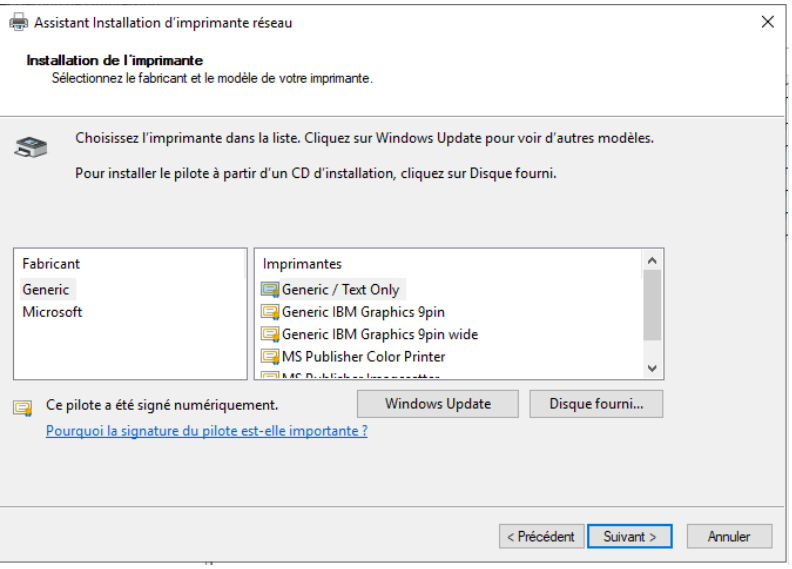
Ensuite il faut mettre l'adresse IP de l'imprimante et installer le nouveau pilote.

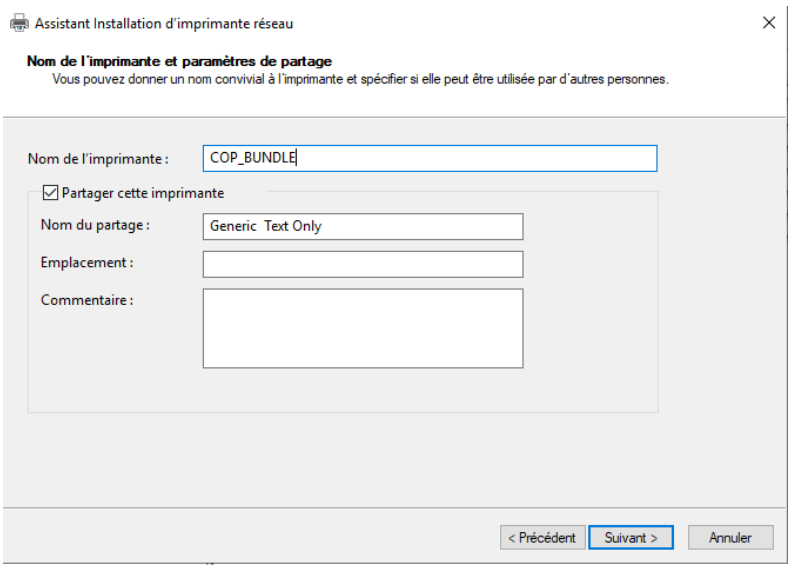




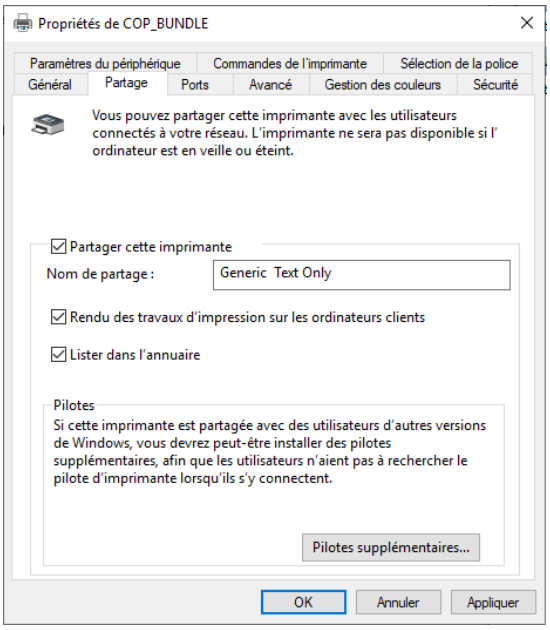
Puis nous allons choisir le type d'imprimante par rapport au pilote proposé.

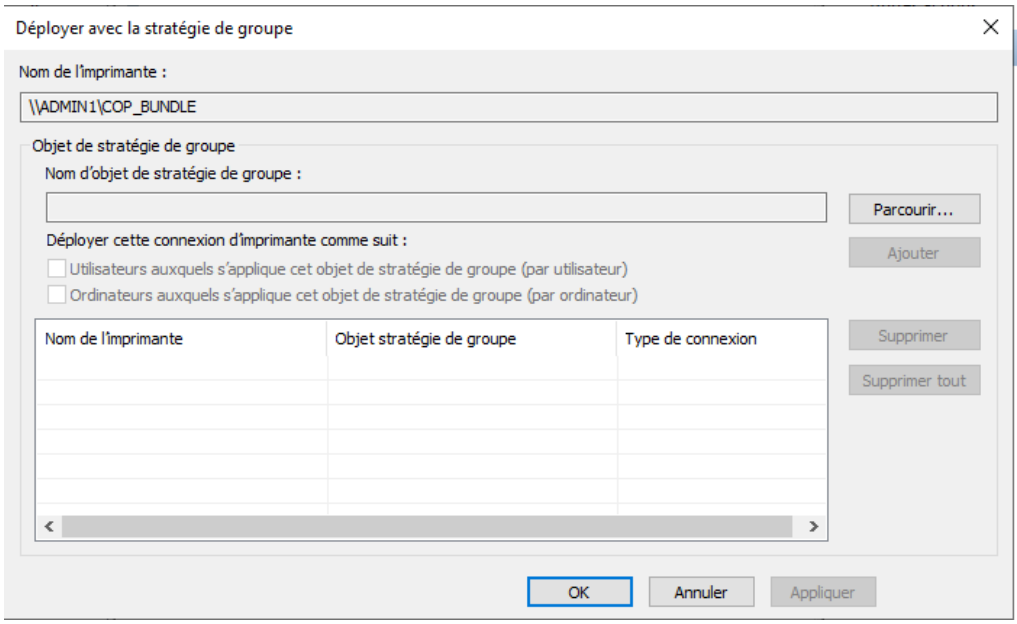
Nous allons aussi pouvoir renseigner le nom de l'imprimante dans notre cas « COP_BUNLDE », sans oublier de cocher la case Partager cette imprimante



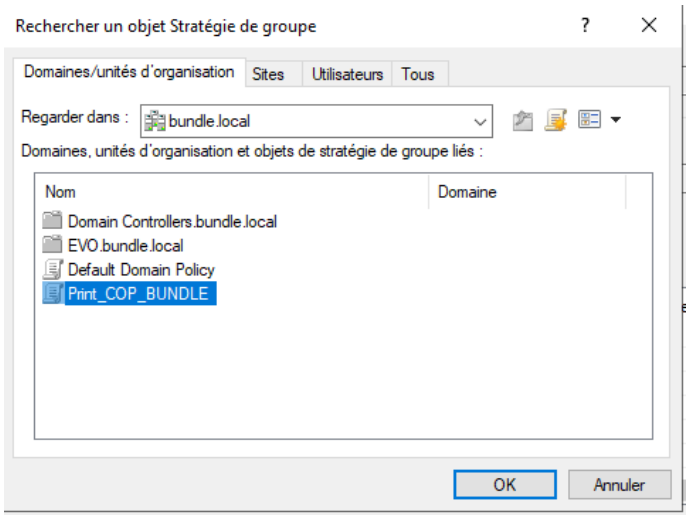


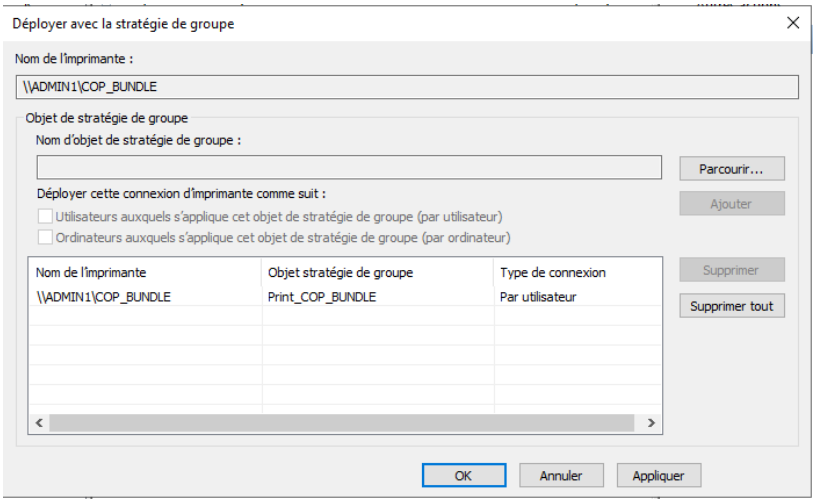
Nous allons cocher la case lister dans l'inventaire et dans la fenêtre « Déployer avec la stratégie de groupe » nous allons cliquer sur parcourir.



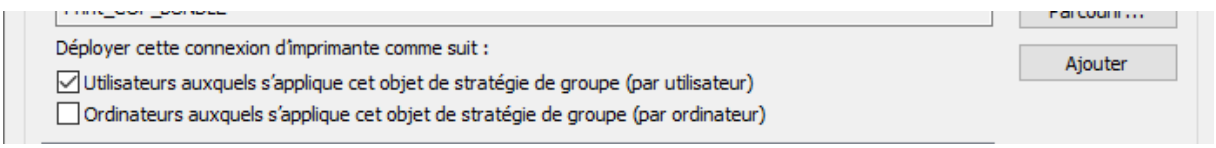


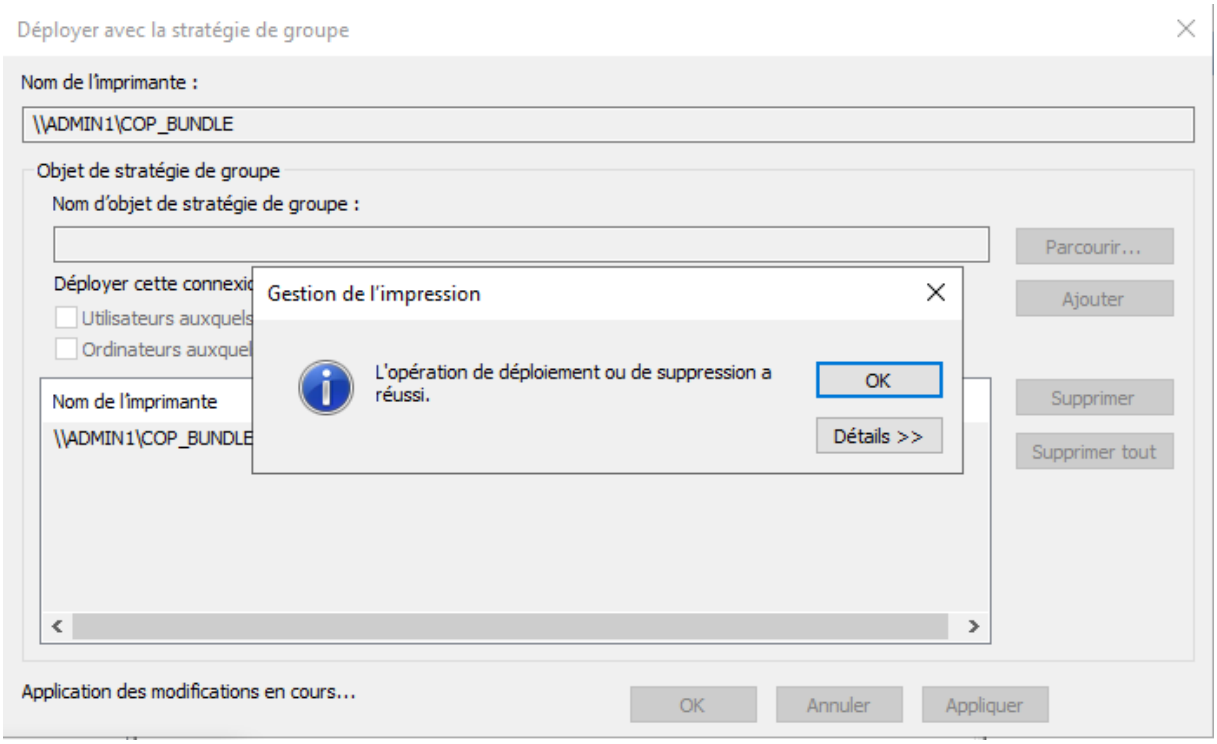
Nous sélectionnons « Print_COP_BUNDLE » que nous avons fait au préalable.





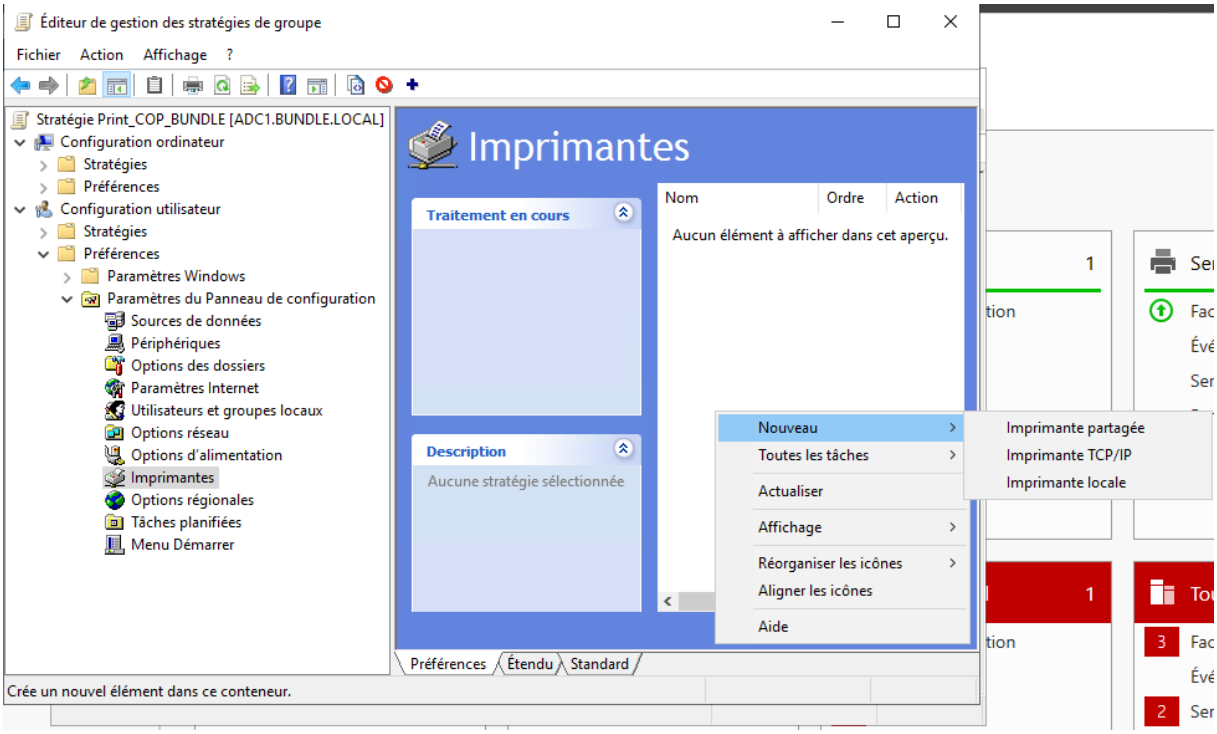
Nous précisons que la stratégie s'appliquera aux utilisateurs





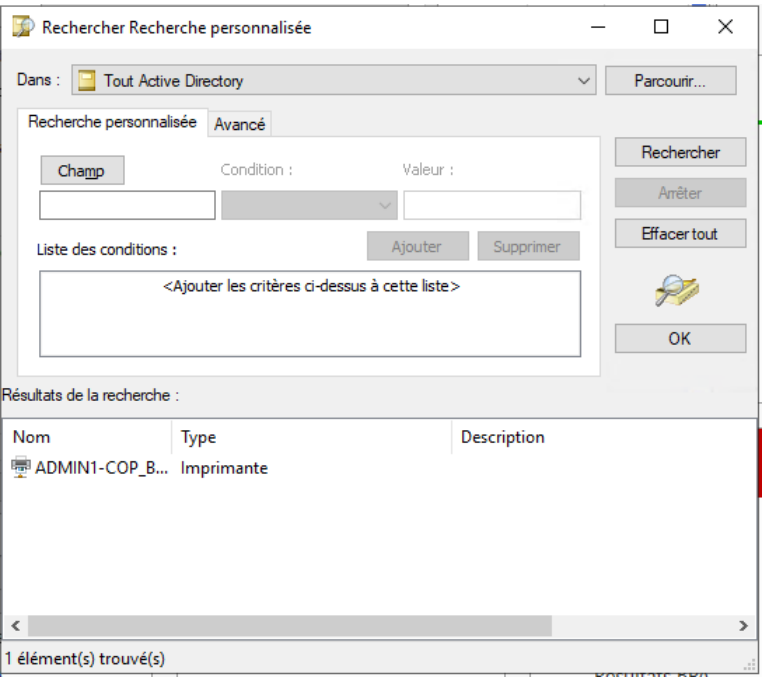
Nous allons maintenant associer l'imprimante à des utilisateurs ou bien à des groupes.

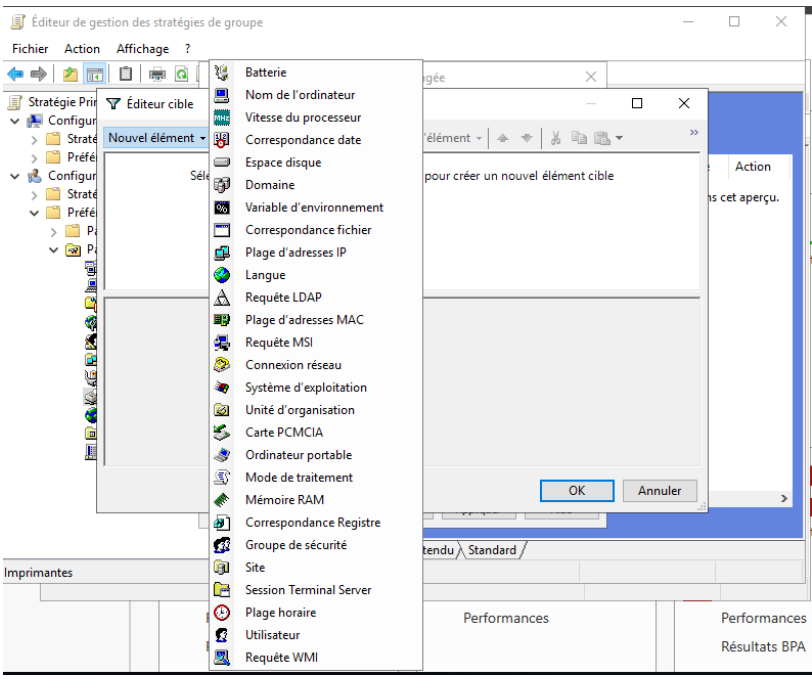
Il faut se rendre dans l'éditeur de gestion de stratégies de groupe. Et faire Nouveau > Imprimante partagée



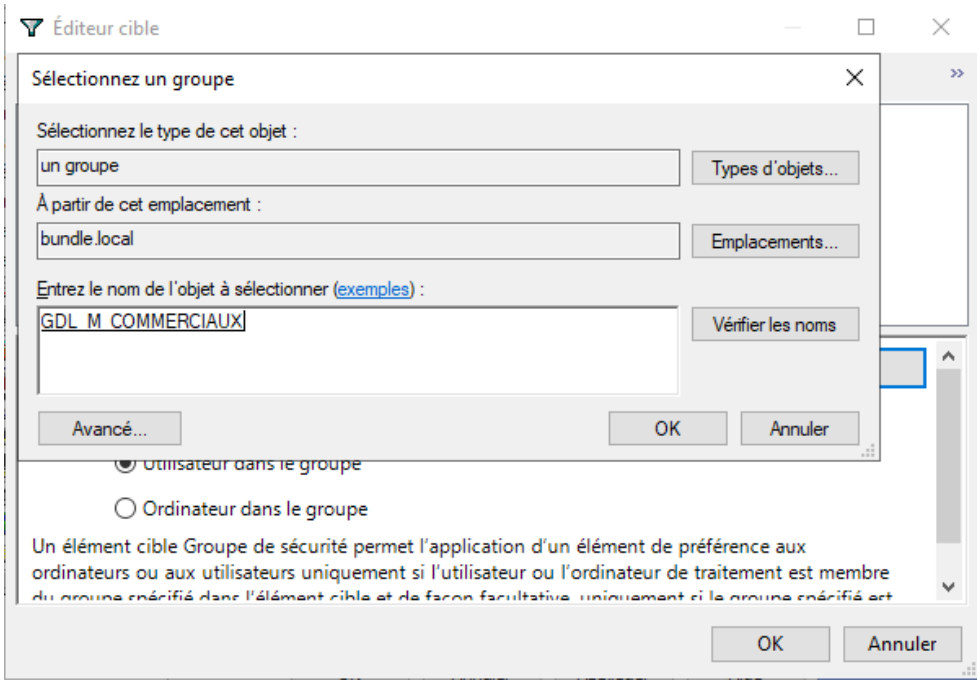
Nous allons ensuite chercher ADMIN1-COP_BUNDLE pour renseigner le chemin du partage

Et choisir le ciblage en sélectionnant Groupe de sécurité.





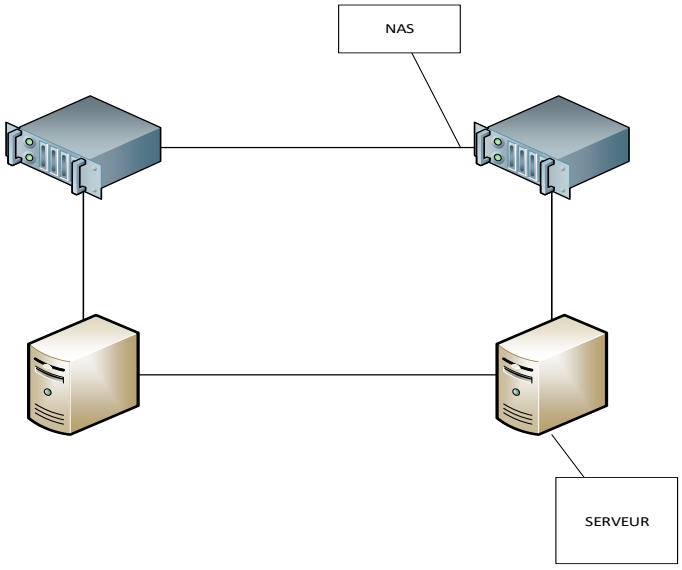
Dans l'éditeur de cible nous allons pouvoir choisir quel groupe rajouter pour finaliser la configuration.



Solution de sauvegarde et de tolérance aux pannes

Les erreurs humaines et défaillances techniques sont des sources importantes de pertes de données. La question n'est plus de savoir pourquoi sauvegarder mais comment faut-il s'y prendre.

Nous allons aborder deux types de sauvegardes qui diffèrent en fonction de leurs fichiers et des besoins de l'utilisateur.



Voici un schéma explicatif pour une potentielle solution de sauvegarde.

Nous utilisons nos NAS déjà présents, nous allons utiliser du RAID 5 matériels sur nos 2 serveurs Windows. Nous configurons à l'identique les deux contrôleurs RAID pour avoir une redondance.

SAUVEGARDES :

Les données sont sauvegardées:

- Sur le serveur principal en raid 5
- Sur le serveur réplique en raid 5
- Sur le NAS : 1 fois/semaine

Nous pouvons utiliser un utilitaire pour simplifier le système de sauvegarde à l'aide de VEEAM par exemple.

Tolérances aux pannes comment y palier ?

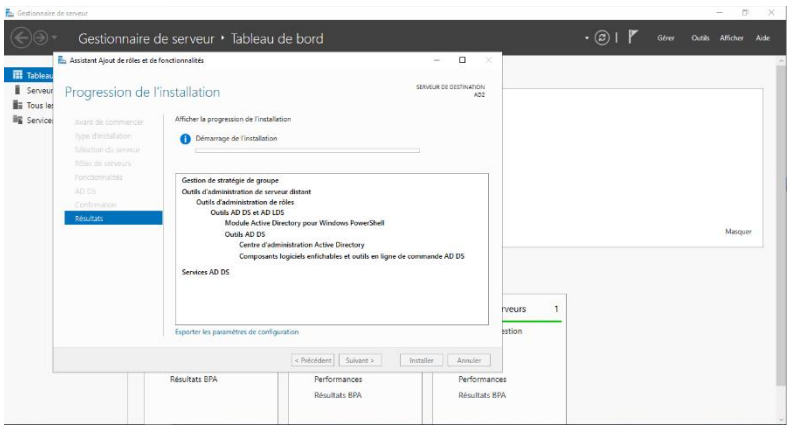
Nous avons utilisé 2 serveurs physiques avec pour chacun un serveur AD DS, DNS , DHCP ainsi que la réplication DFS sur nos serveurs de fichiers.

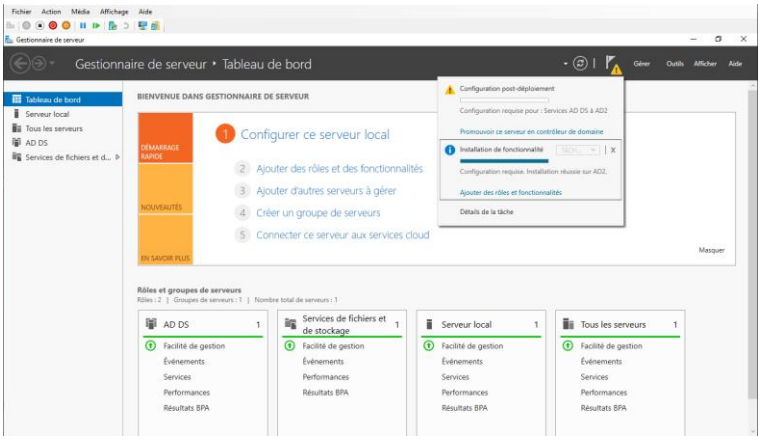
Dans le cas où un des serveurs a un problème celui qui va être répliqué pourra prendre le relai, ce qui n'aura pas d'impact direct sur l'utilisateur qui pourra continuer à utiliser les différents services.

Nous avons donc ADC2 qui est notre contrôleur de domaine 2. Avec le rôle AD DS aussi présent.

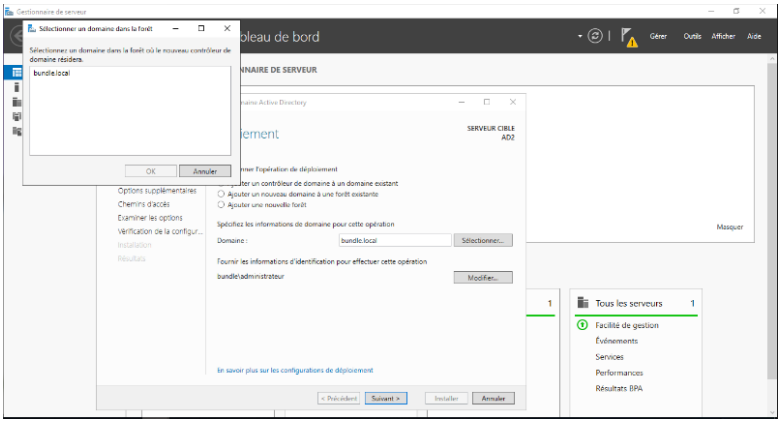
Nous allons le configurer à cet effet.

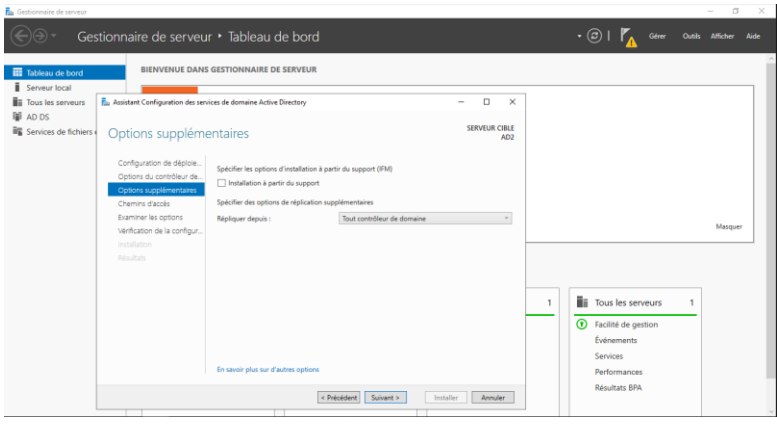
Dans un premier temps nous lui installer son rôle pour ensuite le configurer.





Contrairement au premier contrôleur de domaine nous allons l'ajouter à un domaine déjà existant et le répliquer au contrôleur de domaine existant





En faisant cette opération si le serveur ADC1 a un problème le serveur ADC2 peut reprendre le rôle AD DS et ainsi les utilisateurs peuvent s'authentifier sans problème.

Pour ce qui est du DNS nous faisons la même chose avec un DNS primaire sur ADC1 et un DNS secondaire sur ADC2. La résolution de nom peut donc être maintenue en toute circonstance.

Nous avons vu précédemment l'installation du 2ème serveur DHCP ainsi que sa configuration, il va pouvoir attribuer des adresses IP même si l'un des deux serveurs est en panne par exemple.

Qu'est-ce que le risque et comment l'évaluer

Le risque est un concept économique , la probabilité de pertes financières pour l'organisation est-elle élevée, moyenne, faible ou nulle ? Trois facteurs entrent en ligne de compte dans la détermination du risque : la nature de la menace, la vulnérabilité du système et l'importance de l'actif qui pourrait être endommagé ou rendu indisponible.

Voici quelques manières courantes de subir des dommages :

- **Perte de données**. Le vol de fichier peut faire perdre des marchés au profit des concurrents. Le vol d'informations peut entraîner une perte de confiance et une érosion de la confiance que la clientèle place dans l'entreprise.
- **Interruption du système ou des applications**. Si un système ne remplit pas sa fonction première, il est possible que les utilisateurs n'aient pas la possibilité de travailler et que les employés ne soient pas en mesure de faire leur travail ou de communiquer. Ce qui engendre des pertes financières.

Il faut donc identifier les différentes sources de problèmes qui peuvent survenir et faire une priorisation.

Il faut ensuite identifier les menaces que ce soit catastrophes naturelles (déclenchement d'un feu) , défaillance du système ou bien erreur humaine.

De ce fait il faut déterminer la probabilité d'un accident et les catégoriser en élevé, moyen et faible.

Aves ces éléments il faut aussi trouver un une solution pour avoir le contrôle sur les différents incidents qui pourraient survenir.

Nous pouvons donc faire un tableau qui liste ces différents points (exemple) :

Menace	Vulnérabilité	Actif	Impact	Probabilité	Risque	Recommandation	Niveau
Défaillance système – Surchauffe dans la salle de serveurs	Le système de climatisation a dix ans	Serveurs	Tous les services (site Web, messagerie, etc.) seront indisponibles	ÉLEVÉE La température de la salle est trop élevée	Perte potentielle de 45 000 €	Achat d'un nouveau climatiseur	Elevé
Interférence humaine accidentelle – suppressions accidentelles de fichiers	Les autorisations sont correctement configurées, un logiciel d'audit informatique est en place, des sauvegardes sont réalisées régulièrement	Fichiers sur un partage de fichiers	Des données critiques seront peut-être perdues, mais pourront presque certainement être restaurées	MOYENNE	FAIBLE	Continuer à surveiller les modifications apportées aux autorisations et privilège	Faible

Gestion de la disponibilité

Nous pouvons classer les différentes catégories de disponibilité en fonction de la durée estimée

En nous servant du tableau et des recommandations proposées nous pouvons avoir un plan d'action à utiliser dans chacun des cas possibles.

Il y a de nombreuses solutions pour la gestion des VM, que ce soit les exportations de ces dernières ou bien la mise en place des points de contrôles, qui peuvent nous aider dans ce cas-là.

Pour ce qui va être des solutions au niveau physique nous avons utilisé la réplication.

Ces éléments nous permettent d'avoir la plus haute disponibilité possible.

Le DFS (serveur de fichier)

Les serveurs de fichiers

Un serveur de fichiers est une instance de serveur centrale dans un réseau d'ordinateurs qui permet aux clients connectés d'accéder aux ressources qui y sont stockées. Le terme regroupe aussi bien le matériel que les logiciels nécessaires à la mise en place d'un tel serveur. S'ils bénéficient des autorisations correspondantes, les utilisateurs accédant au serveur peuvent ouvrir et, le cas échéant, également lire, modifier, et supprimer des dossiers et des fichiers sur un serveur de fichiers. Ils peuvent aussi charger leurs propres fichiers sur le serveur.

Nous allons donc créer deux serveurs de fichiers SVF1 et SVF2. L'utilisation de deux serveurs va nous permettre une réplication des données sur plusieurs serveurs physiques et ainsi sur différents disques durs.

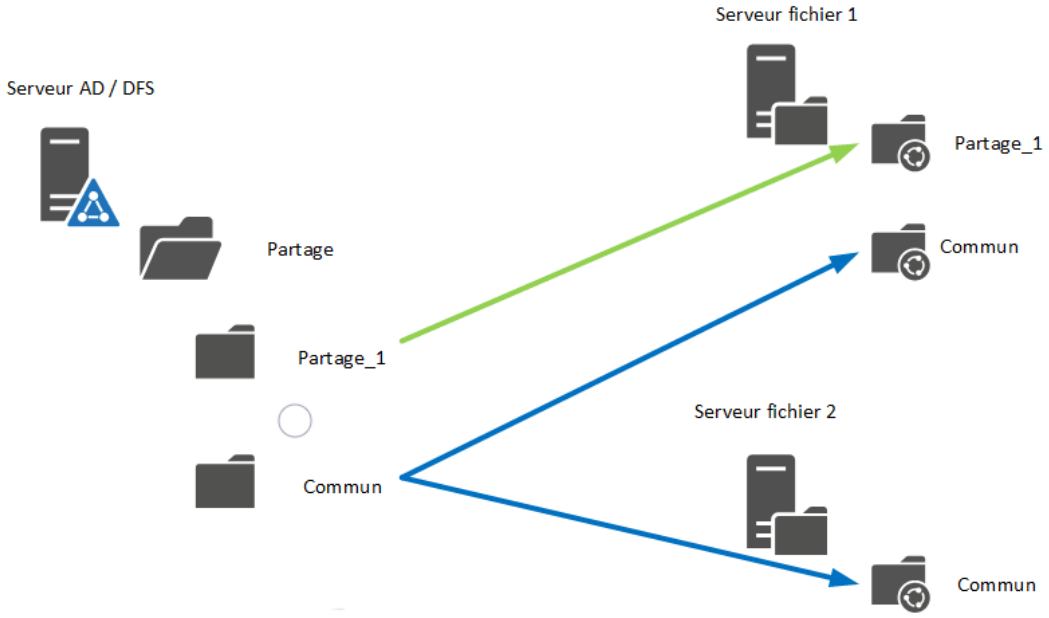
Si un des serveurs est hors service ou bien a un disque dur cassé, il n'y aura pas de pertes de données puisque l'on va pouvoir y accéder sur le serveur en état de fonctionner.

Pour réaliser ceci nous allons utiliser le DFS.

Qu'est-ce que le DFS et comment le configurer

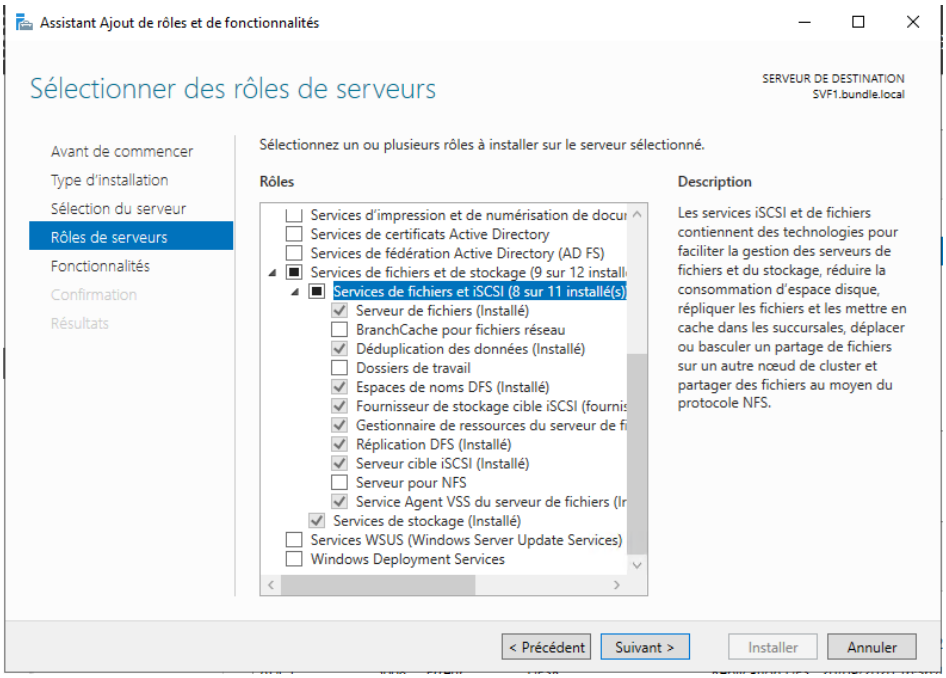
La technologie Distributed File System (DFS) de Microsoft, en français «Système de fichiers distribués » est un ensemble de services client et serveur permettant de fournir une arborescence logique aux données partagées depuis des emplacements différents, de rassembler différents partages de fichiers à un endroit unique de façon transparente et d'assurer la redondance et la disponibilité des données grâce à la réplication.

Avec cette technologie, il est possible de monter un seul même lecteur sur le poste de tous les utilisateurs, les partages existants se présenteront sous forme de dossiers et fonctionneront comme des raccourcis. L'affichage ou non des dossiers se configure ensuite en fonction de l'appartenance aux groupes Active Directory.



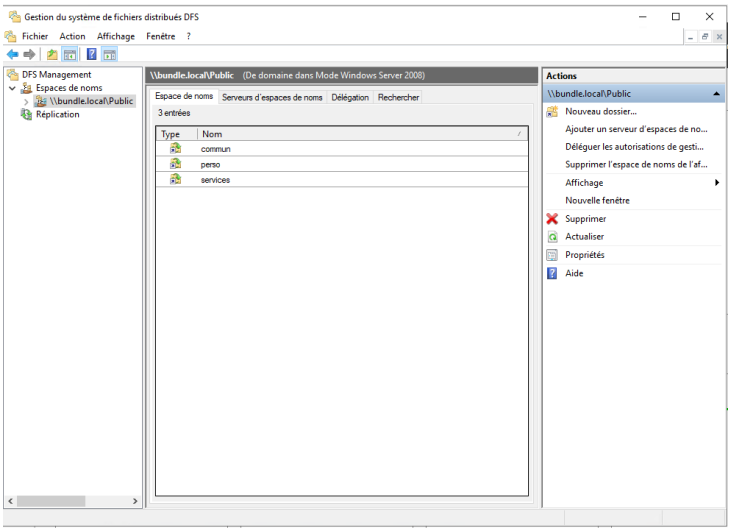
Installation du service DFS

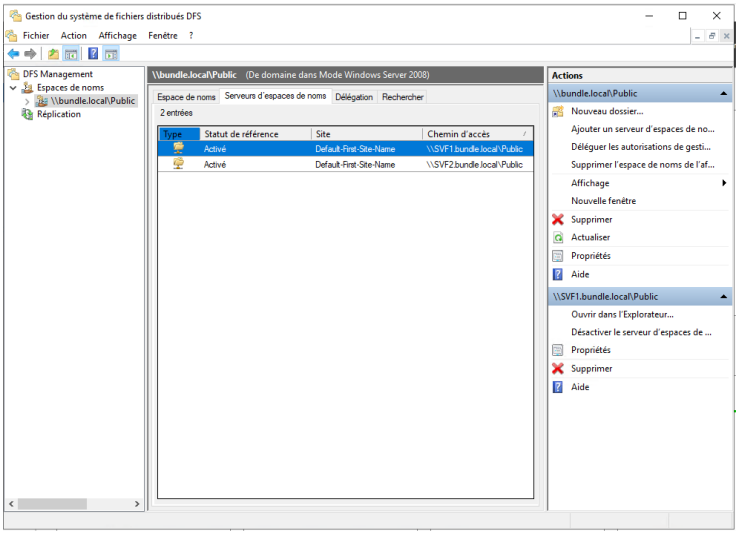
Il faut installer et sélectionner « Espaces de noms DFS » et « Réplication DFS »



Configuration du service DFS

Il faut donc créer les dossiers ainsi que les partages





◢ SVF1 (4)			
Commun	F:\partage\Commun	SMB	Non-cluster
Perso	F:\partage\Perso	SMB	Non-cluster
Public	C:\DFSRoots\Public	SMB	Non-cluster
services	F:\partage\services	SMB	Non-cluster
◢ SVF2 (4)			
commun	F:\commun	SMB	Non-cluster
perso	F:\perso	SMB	Non-cluster
Public	C:\DFSRoots\Public	SMB	Non-cluster
services	F:\services	SMB	Non-cluster

Serveur LINUX

DISTRIBUTION LINUX COMPARATIF

Nous avons pour ce projet choisi d'utiliser 2 distributions Linux différentes.

Tout d'abord il y a CentOS, afin d'assurer une stabilité des applications métiers. En effet, les versions de CentOS sont maintenues pendant 10 ans, ce qui signifie que les applications d'entreprise sont parfaitement prises en charge.ppt

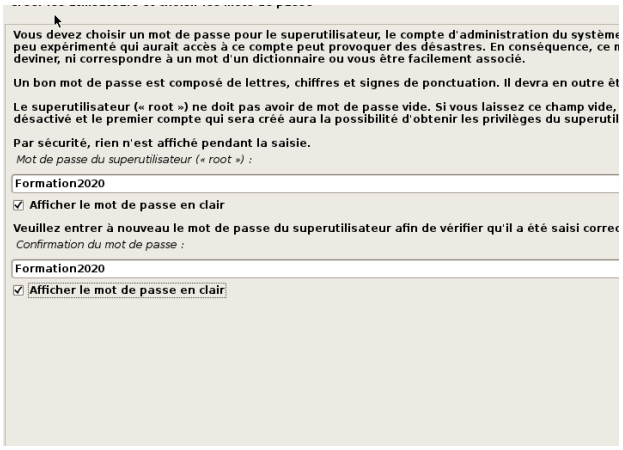
Puis, nous utilisons aussi DEBIAN. Le serveur SAMBA. Ici on choisit cette distribution car il est important d'avoir un minimum de maintenance lorsque l'on utilise un serveur, pour ne pas avoir de gros trous de sécurité, et DEBIAN est mis à jour tous les 2 ans environ.

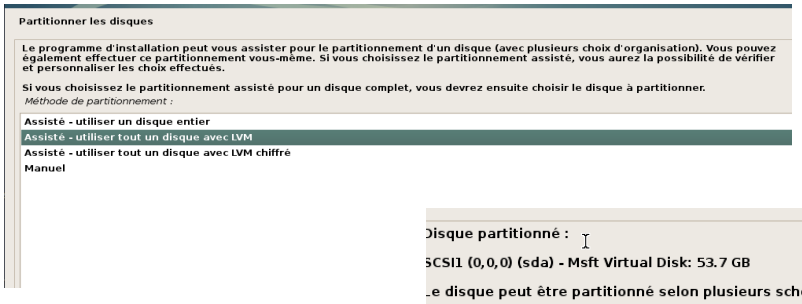
De plus les mises à jour de CENTOS, basées sur le modèle de RHEL, sont bien plus difficiles à mettre en place sans désinstaller la version ultérieure.

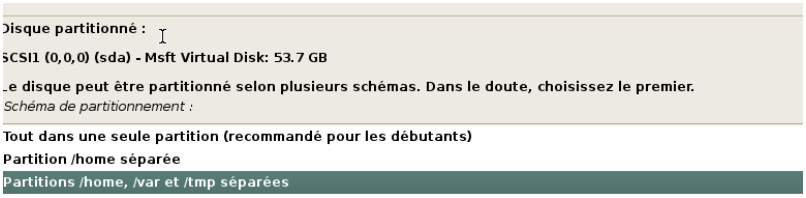
INSTALLATION DEBIAN

Debian ne nous sert ici que pour le serveur SAMBA. Son installation est assez simple puisque sur Hyper-V, la seule contrainte reste de choisir la génération adaptée. Nous sommes ici sur debian 9 donc nous choisirons la génération 2.

L'installation se fait très rapidement. Nous allons y définir le nom de la machine, sa configuration réseau, choix de partition (cryptée ou non)

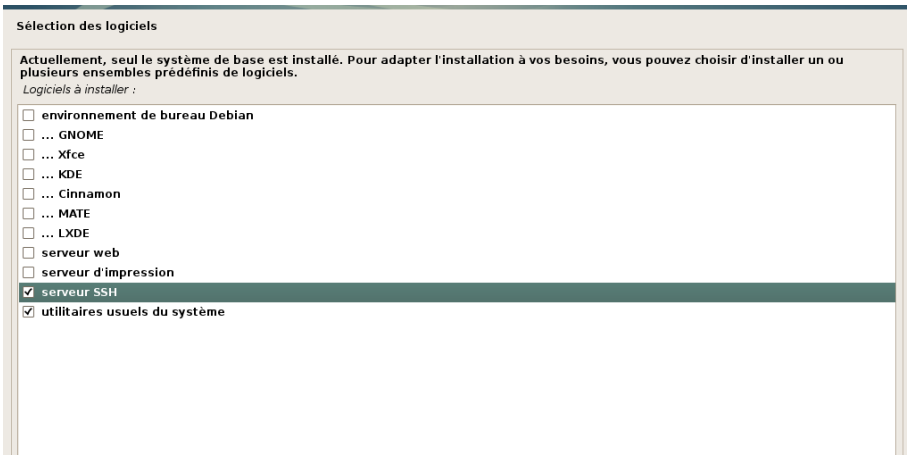






Si la machine est connectée au réseau il est tout à fait possible d'y effectuer une mise à jour des paquets en choisissant une des sources proposées au cours de l'installation.

L'installation est très guidée, mais attention tout de même à bien changer les logiciels comme ci-dessous.

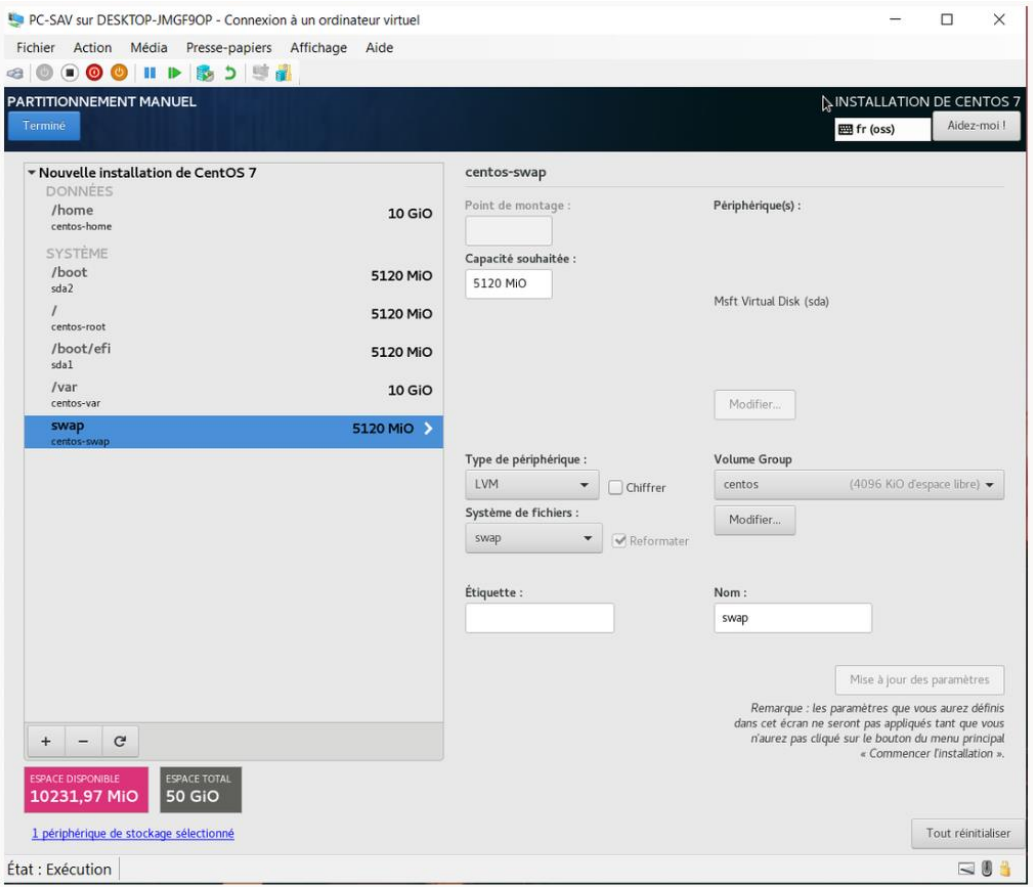


INSTALLATION CENTOS

L'installation de CentOS n'est pas beaucoup plus compliquée que celle de Debian.

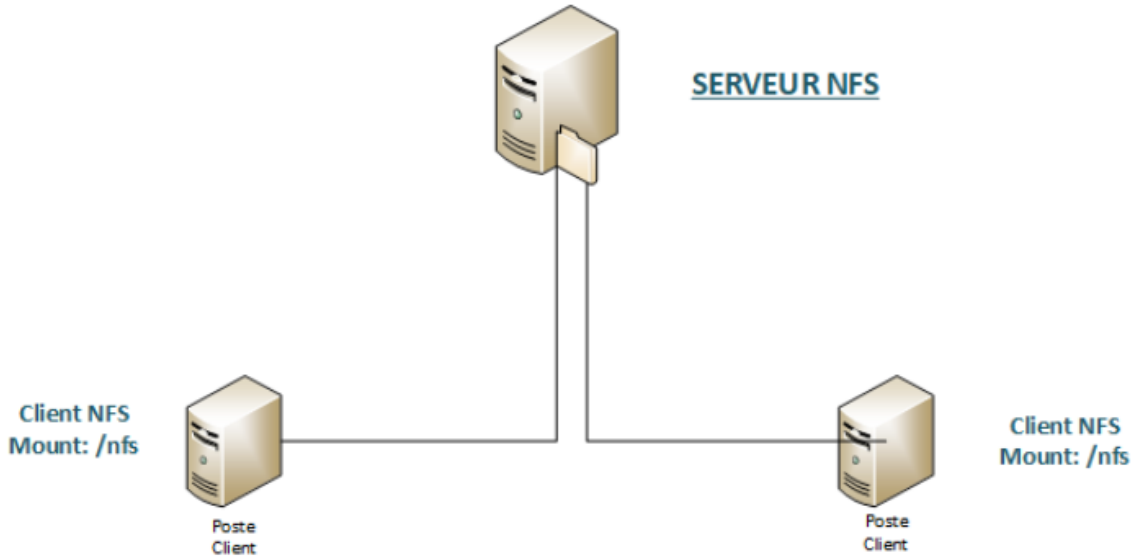
En effet, i suffit de lancer l'installation dans Hyper-V de la même manière que Debian (emplacement, génération 2, etc. ...). Ce qui change se trouve lors de l'installation de l'OS à proprement parler. En effet la présentation des options au démarrage est un petit peu plus fournie, avec notamment la config réseau ipv4 et ipv6 possible dés le démarrage.

L'interface de gestion des disques change aussi, comme ci-dessous. L'installation reste quand même elle aussi très guidée.



SERVEUR NFS

Le serveur NFS (Network File System) est le protocole de partage de répertoires par réseau. Il permet d'accéder à des fichiers distants.



Pour cela il faut d'abord rajouter un DD de 10Go sur hyper-V et le partitionner/formater afin d'allouer ce DD à toute la partie NFS.

Il est important de le rendre automatique sinon au redémarrage le DD ne remontera pas.

Pour la suite nous allons l'installer grâce à la commande yum install nfs utilis -y, puisque nous sommes sous Centos. Il ne faut pas oublier le débloquer les ports nfs.

Pour finir il suffit de se connecter sur une autre machine CentOS pour vérifier que tout fonctionne.

Vient ensuite la partie de création d'un dossier qui va accueillir les dossier nfs. Il faut ensuite monter le partage et automatiser cette même tâche.

```
[lcoralie@SRV-TESTFTP ~]$ df -h
Sys. de fichiers        Taille Utilisé Dispo Uti% Monté sur
/dev/mapper/centos-root    20G    958M   20G   5% /
devtmpfs                  452M       0  452M   0% /dev
tmpfs                     464M       0  464M   0% /dev/shm
tmpfs                     464M    6,2M  457M   2% /run
tmpfs                     464M       0  464M   0% /sys/fs/cgroup
/dev/sda2                1014M    124M  891M  13% /boot
/dev/sda1                 200M     12M  189M   6% /boot/efi
/dev/mapper/centos-home   6,6G     33M  6,6G   1% /home
/dev/mapper/centos-var     10G    140M  9,9G   2% /var
tmpfs                      93M       0   93M   0% /run/user/1000
172.17.246.116:/nfs        50G     33M   50G   1% /mnt/partage
[lcoralie@SRV-TESTFTP ~]$
```

Le serveur nfs est aussi le serveur ftp. La seule différence étant que le serveur FTP sert à communiquer avec l'extérieur tandis que le nfs est utilisé pour les communications internes.

SERVEUR FTP

Qu'est-ce que le ftp ?

Le service FTP (File Transfer Protocol) est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.

Cela sert surtout à se connecter sur un serveur de fichiers distant sans passer par du mappage réseau (sous Windows)

On commence donc par installer les paquets pour le serveur avec la commande :

yum install vsftpd

Ensuite on vérifie si le serveur ftp a bien été créé

getent passwd ftp

On y ajoute les règles suivantes dans le firewall (pour ouvrir les ports en permanence).

firewall-cmd –permanent –add-port=21/tcp

firewall-cmd –permanent –add-port=40000-40100/tcp

firewall-cmd –permanent –add-service=ftp

Recharger la configuration.

firewall-cmd –reload

Lancer les services ysftpd au démarrage et le démarrer

systemctl enable ysftpd

systemctl start ysftpd

On ajoute les droits Selinux (permet de surveiller les processus en cours d'exécution)

vi /etc/vsftpd/vsftpd.conf

```
pasv_max_port=11000
user_sub_token=$USER
local_root=/home/$USER/ftp
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
rsa_cert_file=/etc/cert/vsftpd.pem
rsa_private_key_file=/etc/cert/vsftpd.pem
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH
```

A la suite de ces lignes ajouter les lignes suivante :

allow_writeable_chroot=YES

pasv_enable=YES

pasv_min_port=40000

pasv_max_port=40100

Création du dossier certificat

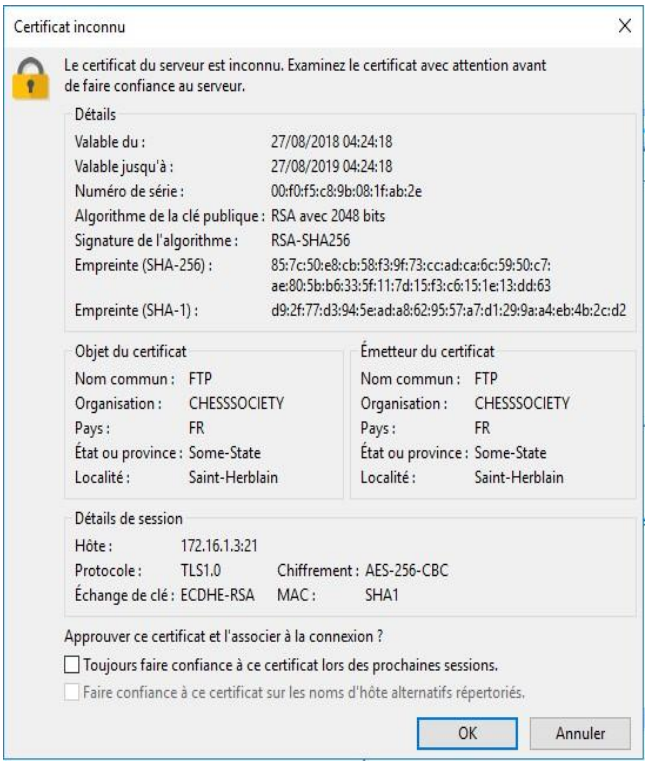
Mkdir /etc/ssl/private

Création du certificat pour sécuriser les connexions avec la commande :

```
root@serveurdebian:~# openssl req -new -x509 -days 365 -nodes -out /etc/proftpd/server.crt
-keyout /etc/proftpd/server.key
```

Lors de la création du certificat les lignes à remplir sont optionnelles (nom, prénom, ville…)

Lors de la connexion au serveur FTP, il sera demandé de valider le certificat :



SERVEUR SAMBA

Samba est un service qui permet à un serveur de Linux de communiquer avec notre AD Windows, de créer des dossiers partagés vers Windows et de pouvoir effectuer des sauvegardes, ce qui est important puisque c'est notre serveur de stockage.

L'installation de samba se fait sur une machine Debian 9, configurée au préalable.

On commence donc avec l'installation de ces 4 paquets avec le compte root.

```
apt-get install samba smbclient samba-common

apt-get install winbind libnss-winbind libpam-winbind

apt-get install ntp

apt-get install libpam-krb5 krb5-user
```

Ensuite on configure le DNS. Pour cela on commence par se mettre sur le commutateur interne, puis on parametre le DNS avec « nano /etc/resolv.conf », et ensuite il ne nous reste plus qu'à vérifier en tapant « dig + nom du domaine ».

On enchaine avec l'installation de Kerberos, qui est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes et l'utilisation de tickets, et non de mots de passe en clair, évitant donc le risque d'interception des mots de passe des utilisateurs, et qui permet donc surtout de se connecter à sa session sans forcément être sur le domaine.

```
root@SRV-SMB:~# nano /etc/krb5.conf
```

```
workgroup = FORMATION
realm = formation.local
security =ADS
password server = AD-DC1.formation.local
os level = 0
local master = No
domain master = No
template shell = /bin/bash
winbind enum users = yes
winbind enum groups = yes
winbind use default domain = yes
idmap config FORMATION:range = 10000000-19000000
idmap config FORMATION:backend = rid
idmap config * : range = 11000-20000
idmap config * : backend = tdb

[partage]
        comment = Partage de fichier
        path = /samba
        read only = no
        guest ok = yes
        public = yes
        valid users = "@FORMATION\utilisateur du domaine"
        browseables = yes
        writable = yes
```

Ensuite on se connecte sur putty afin d'y faire une sauvegarde de notre fichier d'origine. Puis on redémarre Samba afin d'y appliquer toutes les mises à jour effectuées. On intègre ensuite dans le domaine grâce à « net join -S DC1 -U admin ».

On redémarre à nouveau et on vérifie que tout s'est passé comme prévu avec « net ads testjoin » et « net ads info ». Pour finir, il faut modifier le « nsswitch » qui va nous permettre de switcher justement entre l'AD et Samba (nano /etc/nsswitch.conf).

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat winbind
group:          compat winbind
shadow:         compat winbind
gshadow:        files

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

Maintenant que la configuration DNS et l'accès à l'AD ont été configurés, on peut passer à la partie stockage de notre serveur en créant un espace afin d'accueillir les fichiers.

```
root@SRV-SMB:~# mkdir /samba
root@SRV-SMB:~# ^C
root@SRV-SMB:~# chmod 777 /samba/
```

```
33  fdisk /dev/sdb
34  lsblk
35  fdisk /dev/sdc
36  fdisk /dev/sdb
37  pcvreate /dev/sdb1
38  pvcreate /dev/sdb1
39  vgcreate vgsmb-samba /dev/sdb1
40  vgs
41  lsblk
42  lvcreate -n lvsmb -l 100%FREE vgsmb-samba
43  lsblk
44  history
45  mkfs.xfs /dev/vgsmb-samba/lvsmb
46  mkfs.ext4 /dev/vgsmb-samba/lvsmb
47  lsblk
48  fdisk -l
49  mount /dev/vgsmb-samba/lvsmb /samba
50  lsblk
51  nano /etc/fstab
```

```
55  lsblk
56  fdisk /dev/sdc
57  nano /etc/fstab
58  df -h
59  fdisk /dev/sdc
60  lsblk
61  pvcreate /dev/sdc1
62  pvdisplay
63  vgextend vgsmb-samba /dev/sdc1
64  history
```

On étend ensuite le VG, puis on modifie de fichier smb.conf pour y entrer les bonnes infos afin de continuer le partage avec DC1.

Même sans être du domaine on peut s'y connecter avec sa machine physique grâce à l'ip.

SERVEUR WEB

Nous allons devoir mettre en place un serveur Web afin de consulter et administrer le parc informatique de l'entreprise. Pour ce faire nous utiliserons APACHE qui est le serveur web le plus utilisé sur Linux.

Le but est que nos ordinateurs clients puissent se connecter sur cette interface Web, mais pas (encore) par une personne extérieure à l'entreprise.

Sur notre serveur Linux, ici CentOS, il faut d'abord mettre une IP fixe et s'assurer d'être à jour si on utilise DEBIAN.

L'installation de notre serveur web se fait simplement avec la commande « sudo yum update httpd » puis « sudo yum install httpd ».

Il faut aussi s'assurer que le port 80 est ouvert, grâce à la commande « sudo firewall-cmd --permanent --add-service=http »

On va ensuite check si le serveur est opérationnel, en le démarrant au préalable avec « sudo systemctl start httpd », puis « sudo systemctl status httpd ». Si le serveur est en route il y aura affiché un « active running » parmi les informations affichées.

Ensuite, pour finir de vérifier, il nous suffit de lancer une page web avec notre ip en tant qu'url, afin de tomber sur la page par défaut de Apache2.

Pour la suite, il suffit d'installer PhpMyAdmin ce qui permet de se connecter à l'interface graphique. Nous intégrons ensuite nos tables déjà définies grâce à un script dans phpMyAdmin.

Pour finir, il nous suffira de paramétrer les requêtes etcetera afin de rendre le tout plus lisible et surtout exploitable.

Aspect financier

Les investissements

Les investissements nécessaires vont regrouper du matériel ainsi que des licences.

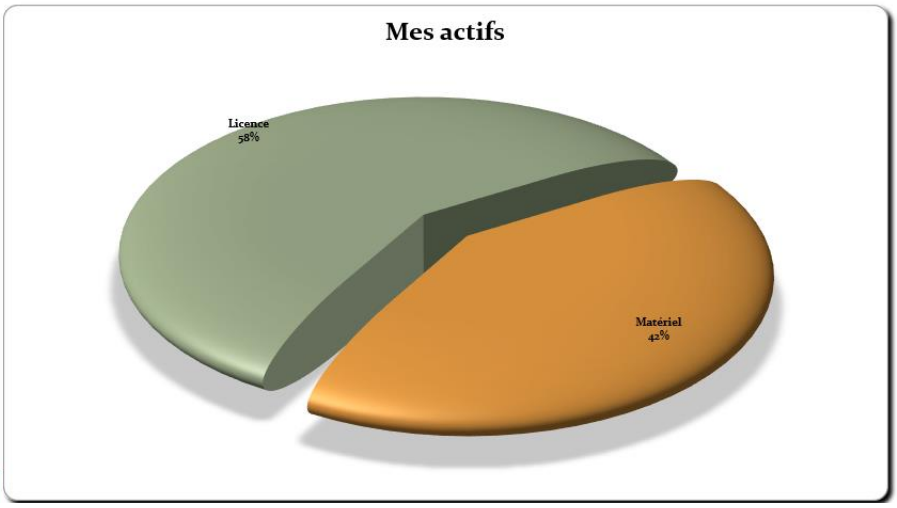
Description	Quantité	Unité	Prix unitaire HT	Total HT	TVA
Windows server data center 2019	2	1	4 103,23 €	8 206,46 €	20%
Disque dur seagate 8To Sata 6gbit/s	8	1	235,52 €	1 884,16 €	20%
Disque dur western digital 3To Sata 6gbit/s	12	1	213,98 €	2 565,76 €	20%
Synology RS2418+ Serveur NAS SATA 6Gb/s	1	1	2 244,99 €	2 244,99 €	20%
Onduleur Eaton, 3KW / 3000VA, 240V, 4 min @ 2500 W	1	1	3 028,00 €	3 028,00 €	20%
windows serveur 2019 license calx10	9	1	289,99 €	2 609,91 €	20%
Serveur DELL PoweEdge r630	2	1	1 271,81 €	2 543,62 €	20%
16Go de RAM DDR4	4	1	169,88 €	679,52 €	20%
Symantec End Point protection	100	1	70,91 €	7 091 €	20%
Total HT Total TVA			Total HT	30 853,42 €	
TVA 20 %			TVA 20 %	37 024,10 €	
			Total TTC	37 024,10 €	

Répartition des dépenses

La répartition des dépenses se fait de la manière suivante :

- Pour le matériel : 12 946,05€ HT
- Pour les licences : 17 907,37€ HT

Type d'actif	Montant
Licence	17 907 €
Matériel	12 946 €



Evolutions possible

Pour améliorer le projet dans un temps futur, nous pourrions intégrer un gestionnaire de parc informatique et de ticket avec **GLPI**

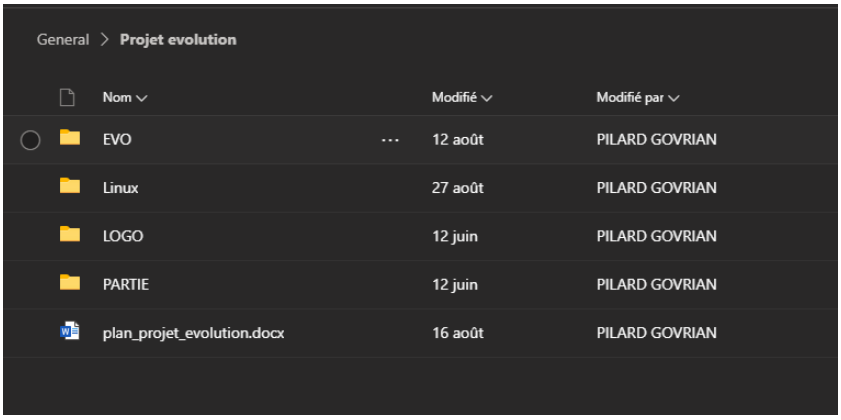
Nous pouvons aussi envisager l'intégration de WSUS, Windows Server Update Services est un service permettant de distribuer les mises à jour pour Windows et d'autres applications Microsoft sur les différents ordinateurs fonctionnant sous Windows au sein d'un parc informatique.

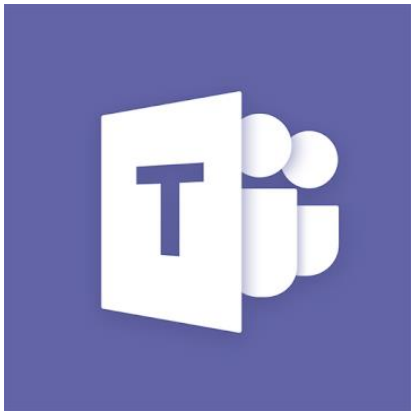
Nous pouvons aussi proposer la mise en place de borne wifi pour les utilisateurs qui ont des ordinateurs portables ou pour les personnes externes à l'entreprise.

La communication au sein de l'équipe

Pour communiquer nous avons utilisé différents outils, que ce soit pour partager des fichiers ou bien faire des réunions de groupe.

Microsoft Teams : Nous avons fait un groupe pour le projet et ainsi nous avons mis les différentes ressources nécessaires pour alimenter au fur et à mesure notre projet.





Discord : Une plateforme pour effectuer des réunions et discuter à distance.

Et le dernier outil était **Messenger**, pour envoyer un message lorsque c'était important et pour qu'il soit vu le plus vite possible grâce à son système de notifications sur smartphone.

PROJET EVOLUTION

Bundle

Responsable du projet

Date de début du projet : 20/04/2020

Incrément de défilement : 4

Marqueur de jalon : 1

Description du jalon	Affecté à	Avancement	Début	Nombre de jours
Windows serveur				
Domain controler	Govrian	100%	30/04/2020	15
ADDS / DNS	Govrian	100%	13/05/2020	6
DHCP	Govrian	100%	17/05/2020	3
Windows admin center (client)	Govrian	100%	18/05/2020	3
Création OU/Groupe	Govrian	100%	19/05/2020	4
Serveur Fichier	Govrian	100%	05/05/2020	10
Replication	Govrian	90%	15/07/2020	30
Serveur Impression	Govrian	100%	20/07/2020	4
GPO	Teguy	0%	07/06/2020	0
Sauvegarde	Govrian	60%	08/07/2020	6
WDS	Govrian	50%	09/08/2020	6
Introduction				
Page présentation (Société)	Govrian	100%	06/05/2020	13
Organigramme	Govrian	100%	07/05/2020	9
Charte Graphique	Govrian	100%	08/05/2020	11
Réseaux (info)	Govrian	90%	09/05/2020	11
Linux				
Samba server	Clement/Rafael	80%	14/09/2020	4
Server WEB	Clement/Rafael	80%	10/09/2020	14
Mise en place FTP	Clement/Rafael	80%	14/09/2020	6
Annexe				
Devis	Clement	70%	25/08/2020	3
Glossaire	Govrian / Clèment	80%	10/08/2020	3

Glossaire :

Active directory (AD) : fournit des services centralisés d'identification et d'authentification à un réseau d'ordinateurs, Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour.

Base de données (BDD) : c'est un lot d'informations stockées dans un dispositif informatique. Les technologies existantes permettent d'organiser et de structurer la base de données de manière à pouvoir facilement manipuler le contenu et stocker efficacement de très grandes quantités d'informations

CAL : Licence d'accès client (Client Access License) Une licence qui donne le droit à un utilisateur ou à un périphérique de consommer les services d'un logiciel serveur ; Il existe trois types de licences pour un logiciel serveur : par siège, par serveur ou par processeur.

Debian : C'est une organisation communautaire et démocratique, dont le but est le développement d'un système d'exploitation basé exclusivement sur des logiciels libres .On l'assimile généralement à sa version Debian GNU/Linux

DFS (Distributed File System): c'est une structure hiérarchique de volume logique indépendamment de l'emplacement physique de la ressource . Il permet de regrouper de façon logique tous les partages sur des serveurs différents sur un même espace. Ainsi les utilisateurs ne sont plus obligés de connaître l'emplacement de tous les partages sur le réseau. Par exemple les dossiers qui concernent la comptabilité sont sur différents serveurs avec DFS, tous ces répertoires sont regroupés sur un seul partage. Cette mise en place est transparente vis-à-vis de l'utilisateur. Un des points forts de DFS c'est la tolérance de panne, il est possible de basculer sur un autre serveur si les fichiers sont indisponibles. DFS est une solution qui répond aux besoins des entreprises en termes de disponibilité.

DHCP : Dynamic Host Configuration Protocol : C'est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau.

DNS : Le Domain Name System (système de noms de domaine) est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine.

FTP : Acronyme de File Transfer Protocol (protocole de transfert de fichiers) : Protocole utilisé pour la copie de fichiers vers et à partir de systèmes informatiques distants sur un réseau, tel que Internet, au moyen du protocole TCP/IP.

GPO : Les stratégies de groupe (GPO pour Group Policy Object) sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory pour restreindre les actions et les risques potentiels.

Intranet : C'est un ensemble de services internes à un réseau local, c'est-à-dire accessibles uniquement à partir des postes d'un réseau local, ou bien d'un ensemble de réseaux bien définis, et invisibles (ou inaccessibles) de l'extérieur.

Lecteur réseau : raccourci permettant de se connecter à un répertoire distant

Linux : Système d'exploitation fondé sur le noyau Linux.

MySQL : C'est un système de gestion de base de données (SGBD). Selon le type d'application, sa licence est libre ou propriétaire. Il fait partie des logiciels de gestion de base de données les plus utilisés au monde, autant par le grand public (applications web) que par des professionnels.

Partage de fichiers : Technique de transfert de fichier consistant à distribuer ou à donner accès à distance à des données dans un réseau informatique.

PHP : Un langage de scripts libre principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale, en exécutant les programmes en ligne de

PowerShell : Logiciel Microsoft d'interface de lignes de commande et langage de script.

commande.

RAID : désigne les techniques permettant de répartir des données sur plusieurs disques durs afin d'améliorer soit la tolérance de panne, la sécurité et les performances de l'ensemble. Aujourd'hui, le mot est devenu l'acronyme de Redundant Array of Independent (or inexpensive) Disks, ce qui signifie « regroupement redondant de disques indépendants »

Samba : Samba est un outil qui permet de partager des fichiers ou des dossiers entre différentes machines (ordinateur, tablettes...) qui peuvent tourner sous différents systèmes d'exploitation

Serveur d'impression : Serveur qui permet de partager une ou plusieurs imprimantes entre plusieurs utilisateurs d'un même réseau.

Windows Serveur : Système d'exploitation Microsoft pour serveur destiné à une entreprise.

Ressources utilisées

https://www.it-connect.fr/

https://labo-tech.fr/

https://www.toutwindows.com/

https://www.editions-eni.fr/

https://www.ldlc-pro.com/

https://www.veeam.com/

https://memo-linux.com/debian-9-installation-pas-a-pas/

https://docs.microsoft.com/fr-fr/windows-server/

https://docs.microsoft.com/fr-fr/windows-server/get-started-19/whats-new-19

https://topics-cdn.dell.com/pdf/microsoft-windows-server-2019_install-guide_fr-fr.pdf

https://github.com/