Windows Server 2016

Les bases pour administrer et configurer votre serveur (2e édition)

Ce livre sur Windows Server 2016 est destiné aux **administrateurs système** ou aux **techniciens en informatique** qui souhaitent se former sur cette version du système d'exploitation serveur de Microsoft ou mettre à jour leurs connaissances par rapport aux anciennes versions. Il est composé de parties théoriques toujours complétées de **parties pratiques** permettant de mettre en place les solutions étudiées.

Après avoir bien identifié les **différents rôles et les fonctionnalités** offertes par le système d'exploitation, l'auteur présente **Hyper-V** (la mémoire vive, les différents types de disques, les snapshots...) puis le **partage d'un fichier VHD** et son **redimensionnement**, et enfin les **switchs virtuels**. Cet apport théorique permet la **création d'une maquette** (ou bac à sable) composée de machines virtuelles exécutant Windows Server 2016 et Windows 10.

L'auteur présente ensuite les **services Active Directory** afin de permettre aux personnes débutantes d'appréhender le vocabulaire utilisé pour Active Directory. Les **sites AD**, la **réplication**, le **catalogue global** sont autant de paramètres étudiés. Le lecteur réalisera la promotion d'un serveur en tant que **contrôleur de domaine** et en tant que **RODC** (Read Only Domain Controller) et découvrira le **clonage d'un contrôleur de domaine virtuel** ou encore **Azure AD** et le fonctionnement de **Azure AD Join**. La console **Gestionnaire de serveur** et certaines de ses fonctionnalités, **Nano Server** ainsi que les objets Active Directory comme la **corbeille AD** sont également expliqués.

Dans les chapitres qui suivent, les **services DHCP** sont traités (haute disponibilité, administration à l'aide de PowerShell...), ainsi que les **services réseau**, l'implémentation d'un **serveur DNS** et d'un **serveur de fichiers** ou encore la mise en place d'un **espace de noms DFS.**

Enfin les derniers chapitres auront pour sujet la mise en place, la gestion et le dépannage des **stratégies de groupe**, la **sécurité** avec notamment la mise en place d'une **stratégie de mot de passe affinée**, la mise en place d'un **serveur de déploiement** (**capture des données d'une partition** ou création d'un **fichier de réponse**), l'installation d'un **serveur WSUS** ainsi que les outils permettant la **gestion et la surveillance du serveur** et la présentation du langage **PowerShell**.

Cette nouvelle édition du livre s'enrichit de quelques nouveautés comme la **mise en place de containers** ou la **récupération d'évènements** à l'aide de **WinRMS**.

Tout au long de ce livre sur Windows Server, l'auteur a mis l'accent sur **PowerShell** : plusieurs ateliers sont réalisés uniquement en PowerShell (migration d'un serveur de fichiers, migration du DHCP...).

Des éléments complémentaires sont en téléchargement sur cette page.

Les chapitres du livre :
Rôles et fonctionnalités – Hyper-V – Installation du bac à sable – Services de domaine Active Directory – Console Gestionnaire de serveur – Gestion des objets Active Directory – Implémentation d'un serveur DHCP – Les services réseau sous Windows Server 2016 – Implémentation d'un serveur DNS – Implémentation d'un serveur de fichiers – Gestion du système de fichiers DFS – Infrastructure de stratégies de groupe – Gestion de la politique de sécurité – Dépanner les stratégies de groupe – Implémentation du service de déploiement – Distribuer des mises à jour avec WSUS – Gestion et surveillance des serveurs – PowerShell

---

Nicolas BONNET

Nicolas BONNET est Consultant et Formateur sur les systèmes d'exploitation Microsoft depuis plusieurs années et possède une expérience de plus de 10 dans l'administration des systèmes informatiques. Il est certifié MCT (Microsoft Certified Trainer), MCSA (Windows 7, 8, 10, 2008, 2012 et Office 365), MCSE Cloud Infrastructure, MCSE Mobility et reconnu Microsoft MVP (Most Valuable Professional) Enterprise Mobility. Il est membre des communautés cmd (http://cmd.community) et aos (http://aos.community). À travers cet ouvrage, il transmet au lecteur toute son expérience sur les technologies serveur et leur évolution. Ses qualités pédagogiques aboutissent à un livre réellement efficace sur l'administration de Windows Server 2016.

Organisation du livre

Le livre est composé de 18 chapitres présentant les différentes fonctionnalités du système d'exploitation Windows Server 2016.

Afin de pouvoir effectuer la partie pratique dans de bonnes conditions, le chapitre Installation du bac à sable décrit la création d'une maquette. Cette dernière est équipée de 5 machines virtuelles :

- **AD1**, **AD2**, **SV1** et **SRVCore** exécutant Windows Server 2016.
- Une machine cliente **CL10-01** sous Windows 10.

Les chapitres, chacun traitant d'un sujet différent, peuvent être parcourus de façon indépendante. Chaque chapitre est construit afin de vous présenter la théorie mais également la mise en pratique sur une ou plusieurs VM (machine virtuelle). Le système d'exploitation de la machine hôte est Windows Server 2012 R2, les machines virtuelles fonctionnent sous Windows Server 2016 pour les serveurs et sous Windows 10 pour la machine cliente. AD1, AD2 et SV1 exécuteront leur système d'exploitation avec une interface graphique, SRVCore sera uniquement en mode ligne de commande.

Certains scripts ou modèles d'administration au format ADM peuvent être téléchargés depuis la page Informations générales.

Les rôles

Les rôles et fonctionnalités ci-dessous ne sont qu'une petite liste de ceux présents dans Windows Server 2016.

Depuis Windows Server 2008 R2, il est possible d'installer les différents rôles depuis la console **Gestionnaire de serveur**. Ces derniers apportent des fonctions supplémentaires aux serveurs. Ainsi l'équipe IT offre des services supplémentaires (adressage IP automatique des postes et autres équipements raccordés au réseau, serveur d'impression…) à ses utilisateurs. La plupart contiennent des services de rôle, permettant l'activation de certaines fonctionnalités. Ils s'installent généralement lors de l'installation d'un autre rôle ou d'une fonctionnalité. L'ajout peut également s'effectuer après l'installation.

1. Accès à distance

Le rôle **Accès à distance** permet de fournir un **service** VPN. La partie routage est également présente et offre la fonctionnalité qui permet le routage de paquets.

Les services de rôle disponibles sont :

- **DirectAccess** et **VPN** : DirectAccess permet la connexion au réseau de l'entreprise sans aucune intervention de l'utilisateur. La connexion est établie uniquement lorsque l'utilisateur est connecté en dehors du réseau local.
- **Routage** : ce service de rôle permet l'installation de plusieurs types de routeurs dont ceux exécutant RIP et les proxys IGMP.

2. Hyper-V

Depuis Windows Server 2008, l'hyperviseur de Microsoft, **Hyper-V**, peut être installé. Il permet de mettre en place une plateforme de virtualisation. Il a été enrichi avec Windows Server 2012 et 2012 R2. De nouvelles fonctionnalités ont été intégrées à Windows Server 2016. Il est désormais possible d'ajouter à chaud pour une VM une carte réseau virtuelle ainsi que de la mémoire. Cette fonctionnalité très intéressante permet de réduire le temps d'indisponibilité du service offert par la machine virtuelle concernée. D'autres fonctionnalités comme la distribution du service d'intégration ont été ajoutées à Hyper-V sous Windows Server 2016.

3. DHCP (Dynamic Host Configuration Protocol)

Le rôle permet la distribution de baux DHCP aux différents équipements qui en font la demande. Il peut être installé sur un serveur en mode installation complète ou en mode Core (installation sans interface graphique).

4. DNS (Domain Name System)

Obligatoire dans un domaine Active Directory, il permet la résolution de noms en adresse IP et inversement. Ce service permet également aux postes clients de trouver leurs contrôleurs de domaine. Il peut être installé sur un serveur ne possédant pas d'interface graphique.

5. IIS (Internet Information Services)

Serveur web, il permet l'affichage et le stockage de sites et d'applications web. De nos jours, il est de plus en plus fréquent qu'une application possède une interface web.

Ce rôle est celui qui possède le plus de services de rôle.

- **Fonctionnalités HTTP communes** : installe et gère les fonctionnalités HTTP basiques. Ce service de rôle permet de créer des messages d'erreurs personnalisés afin de gérer les réponses faites par le serveur.
- **Intégrité et diagnostics** : apporte les outils nécessaires à la surveillance et au diagnostic de l'intégrité des serveurs.
- **Performances** : permet d'effectuer de la compression de contenu.
- **Sécurité** : mise en place des outils permettant d'assurer la sécurité du serveur contre les utilisateurs mal intentionnés et les requêtes IIS.
- **Outils de gestion** : fournit les outils de gestion pour les versions précédentes de IIS.
- **Serveur FTP** : permet l'installation et la gestion d'un serveur FTP.

6. AD DS (Active Directory Domain Services)

Permet le stockage des informations d'identification des utilisateurs et ordinateurs du domaine. Ce rôle est exécuté par un serveur portant le nom de contrôleur de domaine. Ce dernier a pour fonction d'authentifier les utilisateurs et ordinateurs présents sur le domaine AD.

Ce rôle peut être installé sur un serveur ne possédant pas d'interface graphique.

7. AD FS (Active Directory Federation Services)

Le rôle fournit un service fédéré de gestion des identités. Il identifie et authentifie un utilisateur qui souhaite accéder à un extranet.

Ainsi, deux entreprises peuvent partager de manière sécurisée des informations d'identité d'Active Directory pour un utilisateur Office 365 uniquement.

Plusieurs services de rôle le composent :

- **Service de fédération** : l'infrastructure est installée afin de fournir l'accès à des ressources.
- **Agent Web AD FS** : permet de valider les jetons de sécurité délivrés et d'autoriser un accès authentifié à une ressource web.
- **Proxy FSP** (*Federation Service Proxy*) : permet d'effectuer la collecte d'informations d'authentification utilisateur depuis un navigateur ou une application web.

8. AD RMS (Active Directory Rights Management Services)

Protège une ressource contre une utilisation non autorisée. Les utilisateurs sont identifiés et une licence leur est attribuée pour les informations protégées.

Il est ainsi plus simple d'interdire à un utilisateur de copier un document sur une clé USB ou d'imprimer un fichier confidentiel.

Lors de l'installation du rôle, deux services peuvent être installés :

- **Active Directory Rights Management Server** : permet de protéger une ressource d'une utilisation non autorisée.

- **Prise en charge de la fédération des identités** : profite des relations fédérées entre deux organisations pour établir l'identité de l'utilisateur et lui fournir un accès à une ressource protégée.

9. AD CS (Active Directory Certificate Service)

Installe une autorité de certification afin d'effectuer des opérations d'émission et de gestion de certificats.

Six services de rôle peuvent être ajoutés à l'installation :

- **Autorité de certification** : fournit une infrastructure à clé publique.
- **Inscription de l'autorité de certification via le web** : une interface web est installée afin de permettre à un utilisateur d'effectuer des demandes et renouvellements de certificats. Il est également possible de récupérer des listes de révocation de certificats ou d'effectuer une inscription à des certificats de cartes à puce.
- **Répondeur en ligne** : permet la gestion et la distribution des informations de statut de révocation.
- **Service d'inscription de périphérique réseau** : émet et gère les certificats des routeurs et des autres périphériques réseaux.
- **Service web Inscription de certificats** : ce service de rôle donne la possibilité aux utilisateurs et ordinateurs d'effectuer l'inscription et le renouvellement de certificats.
- **Service web Stratégie d'inscription de certificats** : donne aux utilisateurs et ordinateurs des informations sur la stratégie d'inscription de certificats.

10. Service de déploiement Windows (WDS)

Ce rôle fournit un service de déploiement de systèmes d'exploitation à travers le réseau. Le serveur possède deux types d'images : les **images de démarrage** qui permettent l'accès à l'installation de Windows ou à un dossier partagé (MDT) et les **images d'installation** qui contiennent les métadonnées nécessaires à l'installation du système d'exploitation.

Avec l'installation de ce service, deux services de rôle peuvent être installés :

- **Serveur de déploiement** : fournit les fonctionnalités nécessaires au déploiement d'un système d'exploitation. Les fonctionnalités de capture sont également prises en compte par ce service.
- **Serveur de transport** : utilisé pour la transmission des données en multidiffusion.

11. Service de stratégie et d'accès réseau

Ce rôle permet la gestion des accès au réseau par le biais d'accès sans fil, de serveurs VPN ainsi que de commutateurs d'authentification 802.1x. L'installation de NPS (*Network Policy Server*) permet la mise en place de la protection d'accès réseau (NAP).

Les services de rôle disponibles sont :

- **Serveur NPS** : permet la mise en place des stratégies d'accès réseau pour les demandes de connexion.
- **Autorité HRA** : émission de certificats d'intégrité pour les postes de travail conformes aux exigences d'intégrité.
- **HCAP** (*Host Credential Authorization Protocol*) : la solution NAP est intégrée avec la solution de contrôle d'accès Cisco.

12. WSUS

Permet d'approuver les mises à jour avant l'installation sur un poste client, ce dernier étant rangé dans un groupe d'ordinateurs. Cette solution permet d'effectuer une approbation pour un groupe en particulier (exemple : groupe « test » en premier puis, si le correctif ne pose pas de problèmes, il est approuvé pour le deuxième).

Trois services de rôle sont disponibles :

- **WID Database** : installe la base de données utilisée par WSUS dans WID (*Windows Internal Database*). Ce type de base de données est utilisable par d'autres rôles (AD RMS, etc.).
- **WSUS Services** : installe le service WSUS ainsi que tous les composants nécessaires.
- **Base de données** : installe la base de données pour les services WSUS (un serveur SQL est nécessaire, contrairement à WID Database).

13. Services de fichiers et iSCSI

Le service de fichiers permet la mise en place de quotas sur le système de fichiers ainsi qu'un système de filtrage par extension afin d'interdire le stockage de certains fichiers. Un espace de noms DFS peut être installé par l'intermédiaire d'un service de rôle.

Les services suivants offrent la possibilité d'être installés en tant que service de rôle :

- **Serveur de fichiers** : gestion des dossiers partagés.
- **BranchCache pour fichier réseau** : prise en compte de BranchCache sur le serveur. Ce service permet la mise en cache de documents afin de réduire l'utilisation de la ligne reliant deux sites distants. L'utilisateur n'a par exemple plus besoin de venir chercher les documents à son siège social, ces derniers sont mis en cache sur un serveur ou un poste local.
- **Déduplication des données** : permet de libérer de l'espace disque en supprimant les données dupliquées, une copie unique des données identiques est stockée sur le volume.
- **Espace de noms DFS** : installe les outils nécessaires pour la création et la gestion de l'espace de noms.
- **Gestionnaire de ressources du serveur de fichiers** : outil permettant la gestion d'un système de fichiers en effectuant la création de quotas et le filtrage de fichiers.
- **Réplication DFS** : synchronise des dossiers sur plusieurs serveurs locaux ou sur un site distant.

Les fonctionnalités

Une fonctionnalité apporte des "outils" supplémentaires au système d'exploitation. Comme pour un rôle, une fonctionnalité peut s'installer soit de manière manuelle, soit de manière automatique.

1. Chiffrement de données BitLocker

BitLocker permet le chiffrement de chaque volume afin d'éviter une fuite des données en cas de perte ou de vol de la machine. Une vérification du système d'amorçage nécessite la présence d'une puce **TPM** sur la machine.

2. Clustering avec basculement

Permet à des serveurs de fonctionner ensemble, ceci afin d'offrir une haute disponibilité. En cas de panne de l'un des serveurs, la continuité de service est assurée par les autres.

3. Équilibrage de la charge réseau

Permet la distribution du trafic afin d'éviter une saturation d'un des serveurs.

4. Gestion de stratégies de groupe

Composant logiciel enfichable qui permet l'administration et la gestion des différentes stratégies de groupe.

5. Outils de migration de Windows Server

Ajoute des applets de commande PowerShell afin de faciliter la migration des rôles serveur.

6. Service de gestion des adresses IP

Installe une infrastructure permettant la gestion d'un espace d'adresses IP et des serveurs correspondants (DHCP…). IPAM prend en charge la découverte des serveurs dans la forêt Active Directory de manière automatique.

Introduction

Hyper-V est le système de virtualisation de Microsoft, présent dans les systèmes d'exploitation depuis Windows Server 2008, et Windows 8 sur les systèmes d'exploitation client.

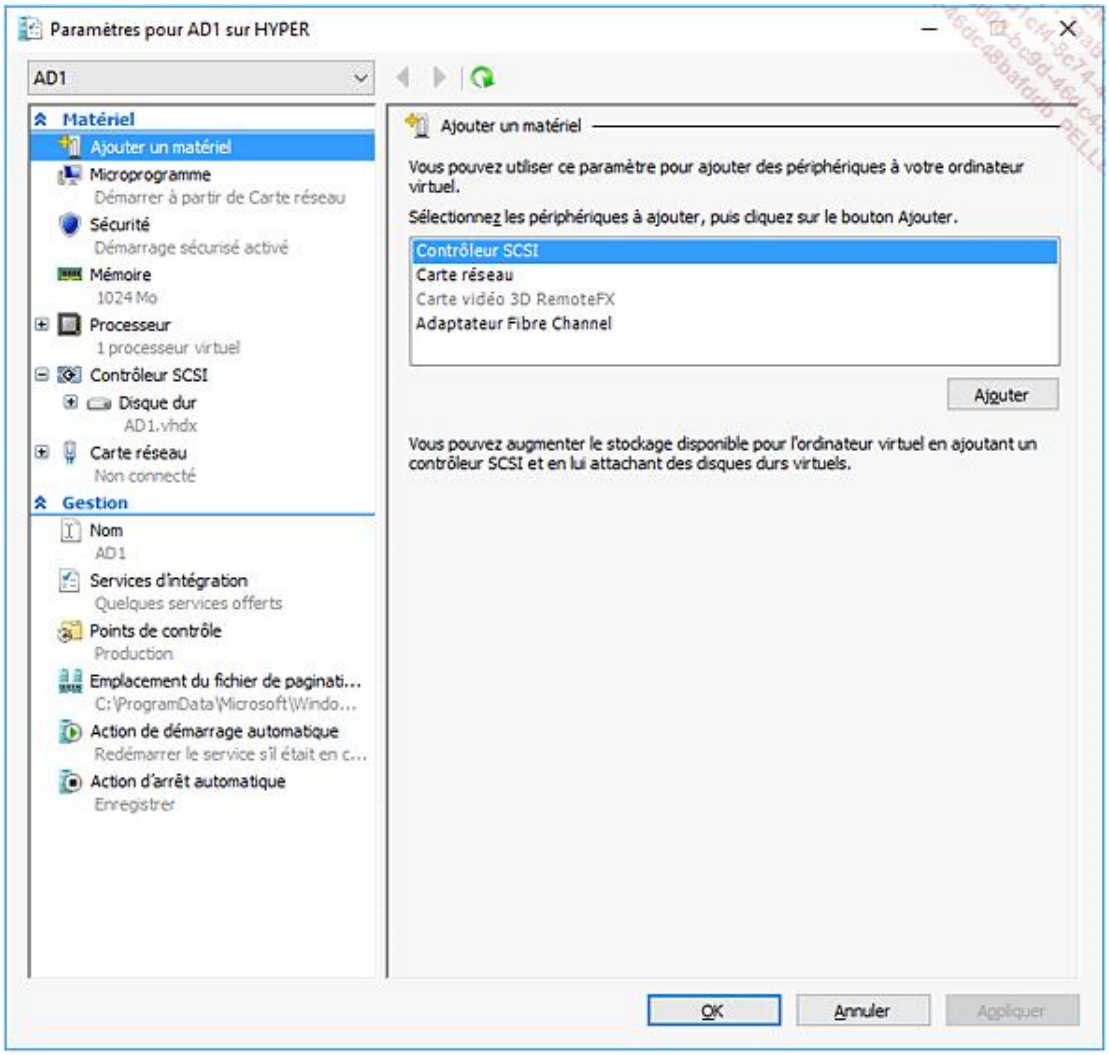
Implémentation d'Hyper-V

Cet hyperviseur offre l'avantage d'offrir un accès immédiat au matériel de la machine hôte, et donc de meilleurs temps de réponse. L'installation s'effectue par l'intermédiaire de la console **Gestionnaire de serveur** ou en PowerShell.

1. Les machines virtuelles sous Hyper-V

Par défaut, une machine virtuelle utilise les équipements suivants :

- BIOS : le BIOS d'un ordinateur physique est simulé, plusieurs facteurs peuvent être configurés :
  - L'ordre de boot pour la machine virtuelle (réseau, disque dur, DVD…).
  - Le démarrage sécurisé qui permet d'empêcher le code non autorisé de s'exécuter au démarrage de la machine virtuelle.
- Mémoire RAM : une quantité de mémoire vive est allouée à la machine virtuelle. Un maximum de 1 To de mémoire peut être alloué. Depuis Windows Server 2008 R2 SP1, il est possible de mettre en place la mémoire dynamique (traitée plus loin dans ce chapitre).
- Processeur : comme pour la mémoire, il est possible d'allouer un ou plusieurs processeurs (en fonction du nombre de processeurs et du nombre de cœurs de la machine physique). Un maximum de 64 processeurs peut être appliqué à une machine.
- Contrôleur SCSI : ajoute un contrôleur SCSI à la machine virtuelle. Il est ainsi possible d'ajouter des disques durs ou des lecteurs de DVD. En choisissant la création d'une machine virtuelle de génération 2, il est impossible d'ajouter un contrôleur IDE.
- Carte réseau : depuis Windows Server 2012 R2, la carte réseau de la machine virtuelle peut désormais effectuer un boot PXE (démarrage sur le réseau et chargement d'une image) sans être de type hérité.



Tous les composants ci-dessus peuvent être configurés lors de la création de la machine virtuelle (carte réseau, disque dur, lecteur DVD) ou en y accédant dans les paramètres de la machine virtuelle concernée.

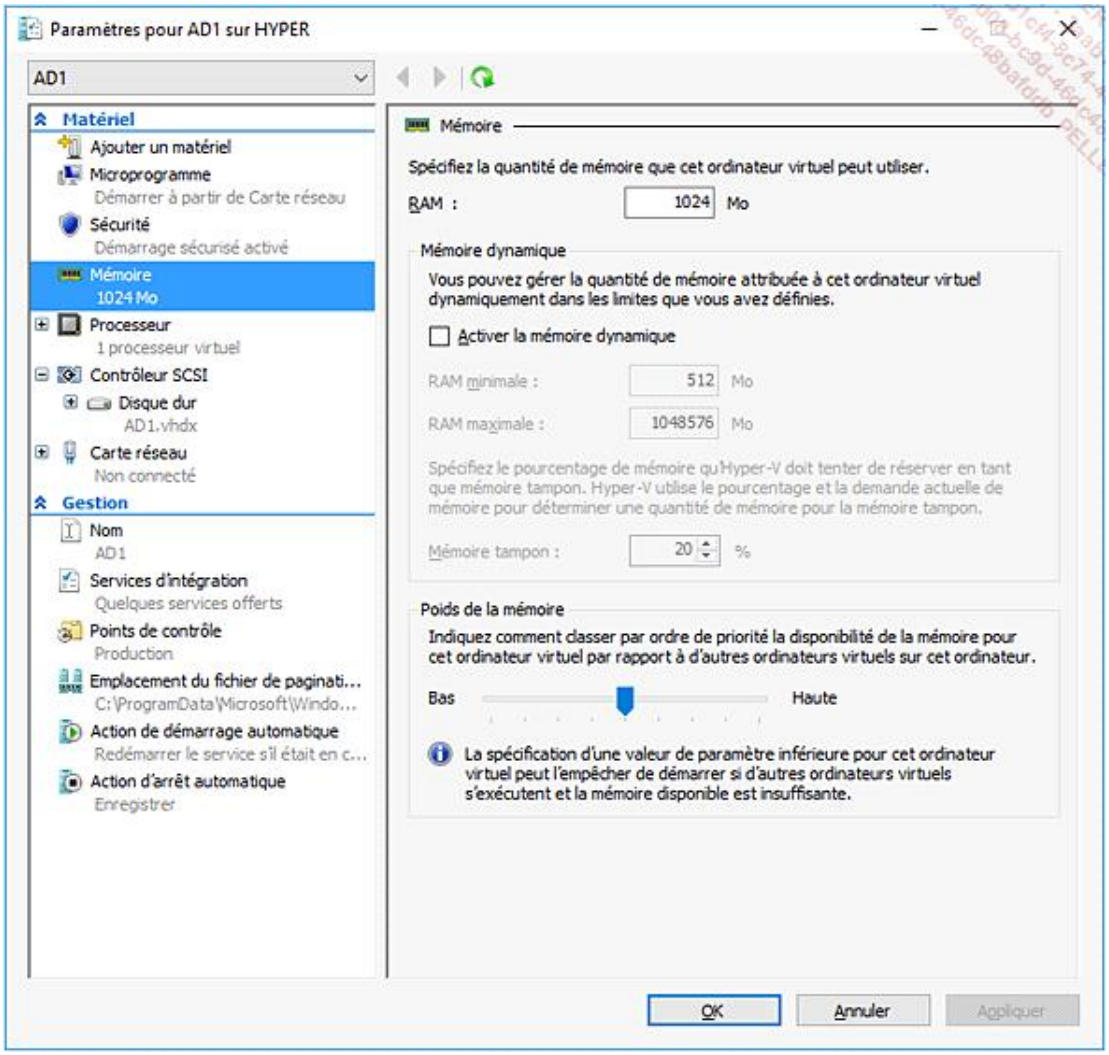
2. La mémoire dynamique avec Hyper-V

À la sortie de Windows Server 2008, le système de virtualisation Hyper-V permettait d'assigner une quantité de mémoire statique uniquement. Ainsi, le nombre de machines virtuelles s'en trouve réduit. Si un serveur se voit attribuer 4 Go de RAM, la quantité réservée est identique même s'il n'y a aucune activité sur la machine virtuelle.

La mémoire dynamique permet d'allouer une quantité minimum de mémoire. Néanmoins si la machine virtuelle a besoin de plus de mémoire, elle est autorisée à demander une quantité supplémentaire, grâce au pilote DMVSC. Cette dernière ne peut excéder la quantité maximale accordée. Cette fonctionnalité a été introduite dans les systèmes d'exploitation serveurs depuis Windows Server 2008 R2 SP1.

Il n'est pas recommandé d'utiliser cette fonctionnalité avec certains rôles et logiciels (Exchange par exemple).

Introduite avec Windows Server 2012, la mémoire tampon est une solution pour l'allocation de la mémoire minimum liée au démarrage de la machine virtuelle. De ce fait le manque de mémoire lors du démarrage d'une VM est comblé par l'utilisation de cette mémoire tampon (*Memory Buffer*). Celle-ci va permettre d'effectuer une allocation de mémoire de manière très rapide.



Le **Poids de la mémoire** permet la mise en place de priorité pour la disponibilité de la mémoire.

Le disque dur des machines virtuelles

Un disque dur virtuel est un fichier utilisé par hyper V pour représenter des disques durs physiques. Il est possible de stocker dans ces fichiers des systèmes d'exploitation ou des données. On peut créer un disque dur en utilisant :

- La console Gestionnaire Hyper-V.
- La console Gestion des disques.
- La commande DISKPART en invite de commandes.
- La commande PowerShell New-VHD.

Depuis Windows Server 2012, des disques virtuels au format VHDX sont utilisés.

Celui-ci offre plusieurs avantages par rapport à son prédécesseur, le format VHD (*Virtual Hard Disk*). Les tailles des fichiers ne sont plus limitées à 2 To, chaque disque dur virtuel peut ainsi avoir une taille maximale de 64 To. Le VHDX est moins sensible à la corruption du fichier suite à une coupure inattendue (due à une panne de courant par exemple) du serveur. Il est possible de convertir des fichiers VHD existants en VHDX (ce point est traité plus loin dans ce chapitre).

Il est possible de procéder au stockage des disques durs virtuels sur des partages de fichiers de type SMB 3. Pour cela, lors de la création d'une machine virtuelle avec Hyper-V, il est possible de spécifier un partage réseau.

1. Les différents types de disques

Lors de la création d'un nouveau disque dur virtuel, plusieurs choix nous sont proposés.

- Disque de taille fixe : lors de la création, la taille totale du fichier est réservée. La fragmentation sur le disque dur de la machine hôte est réduite et les performances améliorées. Le principal inconvénient concerne l'espace disque utilisé même si le VHD(X) est vide.
- Disque de taille dynamique : au moment de la création, une taille maximale du fichier est indiquée. La taille augmente en fonction du contenu jusqu'à la taille maximale. Lors de la création d'un fichier VHD de type dynamique, ce dernier a une taille de 260 kilo-octets contre 4 096 Ko pour un format VHDX. L'opération peut être effectuée en PowerShell à l'aide de la cmdlet **New-VHD** et avec le paramètre **-Dynamic**.
- Disque de type Pass-Through : permet à une machine virtuelle d'accéder directement au disque physique. Le disque est considéré comme lecteur interne pour le système d'exploitation. Cela peut être très utile pour connecter la VM à un LUN (*Logical Unit Number*) iSCSI. Néanmoins, cette solution nécessite un accès exclusif de la VM au disque physique concerné. Ce dernier doit être mis hors ligne par l'intermédiaire de la console Gestion des disques.

2. Gestion d'un disque virtuel

Certaines opérations peuvent être effectuées sur un fichier VHD. Il est par exemple possible de le compacter afin de réduire la taille utilisée ou de le convertir (format VHD en VHDX). Lors de la conversion du disque virtuel, le contenu est alors copié vers le nouveau fichier (par exemple lors de la conversion d'un fichier de type taille fixe en fichier de type taille dynamique). Une fois les données copiées et le nouveau disque mis en place, l'ancien fichier est supprimé.

D'autres opérations comme la réduction d'un fichier dynamique sont réalisables. Cette option permet de réduire la taille d'un disque si ce dernier n'utilise pas tout l'espace qui lui est affecté. Pour les disques de type taille fixe, il est nécessaire en amont de convertir le fichier VHD en fichier de type dynamique.

Ces actions peuvent être réalisées à l'aide de l'**Assistant Modification de disque dur virtuel**, option **Modifier le disque...** dans le bandeau **Actions**.

Il est également possible d'utiliser les cmdlets PowerShell **resize-partition** et **resize-vhd** pour effectuer le compactage d'un disque dur virtuel dynamique.

3. Les disques de différenciation

Un disque de différenciation permet de réduire la taille de stockage nécessaire. En effet, cela consiste à créer un disque parent commun à plusieurs machines et un disque qui contient les modifications (apportées au disque parent), le disque qui contient les modifications étant propre à chaque machine.

La taille nécessaire au stockage des machines virtuelles s'en trouve donc réduite. Attention, la modification d'un disque parent cause l'échec des liens du disque de différenciation. Il est donc nécessaire par la suite de reconnecter les disques de différenciation en utilisant l'option **Inspecter disque...** dans le bandeau **Actions**.

Il est possible de créer ce type de disque en utilisant la cmdlet PowerShell **New-VHD**.

La commande ci-dessous permet la création d'un disque nommé **Differentiel.vhd**, ce dernier utilise un disque parent nommé **Parent.vhd**.

```
New-VHD c:\Differentiel.vhd -ParentPath c:\Parent.vhd -differencing
```

4. Les checkpoints dans Hyper-V

Un checkpoint correspond à une "photo" de la machine virtuelle au moment où il est effectué. Ce dernier est contenu dans un fichier portant l'extension **avhd** ou **avhx** en fonction du type de fichier de disque dur choisi. Pour effectuer la création, il est nécessaire de sélectionner la machine puis de cliquer sur l'option **Checkpoint** dans le bandeau **Actions**.

Chaque machine peut posséder jusqu'à 50 checkpoints. Si ce dernier est créé lorsque la machine est démarrée, le contenu de la mémoire vive est également intégré dans le fichier. Lors de la restauration d'un checkpoint, il est possible que la machine virtuelle ne puisse plus se connecter au domaine. En effet son application peut avoir pour conséquence de rompre le canal sécurisé entre le contrôleur de domaine et la machine cliente. Il est possible de le réinitialiser en effectuant une nouvelle jonction au domaine ou en utilisant certaines commandes DOS.

Attention cette fonctionnalité ne remplace en aucun cas la sauvegarde, car les fichiers **avhd** ou **avhdx** sont stockés sur le même volume que la machine virtuelle. En cas de casse du disque, tous les fichiers sont perdus et il est impossible de les restaurer.

5. Partage d'un disque VHD

Depuis Windows Server 2012 R2 il est possible de partager des fichiers VHD entre plusieurs machines virtuelles. Très utile pour la mise en place d'infrastructures de haute disponibilité telle que l'installation d'un Cloud privé ou d'un Guest Cluster (cluster de machine virtuelle). Cette fonctionnalité permet à plusieurs machines virtuelles l'accès aux mêmes fichiers VHDX. Ces derniers peuvent être hébergés sur des volumes partagés de type cluster (CSV) ou simplement sur un partage SMB (*Server Message Block*) qui peut être basé sur un SOFS (*ScaleOut File Server*).

Néanmoins, il est nécessaire de respecter certains prérequis pour la mise en place d'un Guest cluster utilisant des disques virtuels partagés :

- Un cluster à basculement Hyper-V à 2 nœuds.

- Les serveurs exécutent obligatoirement Windows Server 2012 R2 ou version supérieure.
- Les serveurs sont membres du même domaine.
- Le VHDX partagé doit être positionné sur un volume partagée CSV (*Cluster Shared Volume* - Stockage en mode block) ou un SOFS avec SMB 3 (stockage en mode fichier).

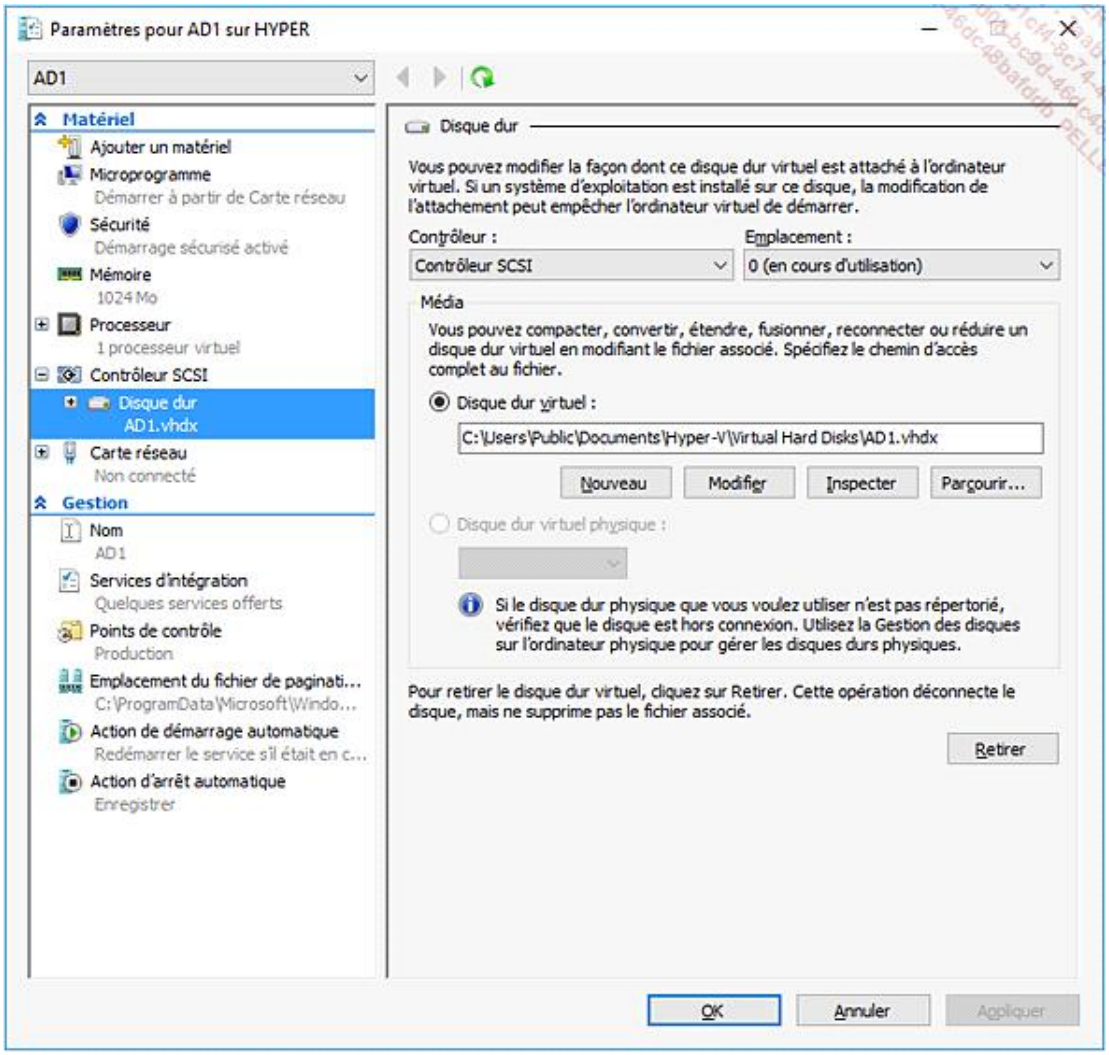
6. Redimensionner la taille d'un VHD à chaud

La fonctionnalité de redimensionnement d'un fichier VHD a été améliorée afin de pouvoir maintenant être effectuée lorsque la machine virtuelle est en fonctionnement.

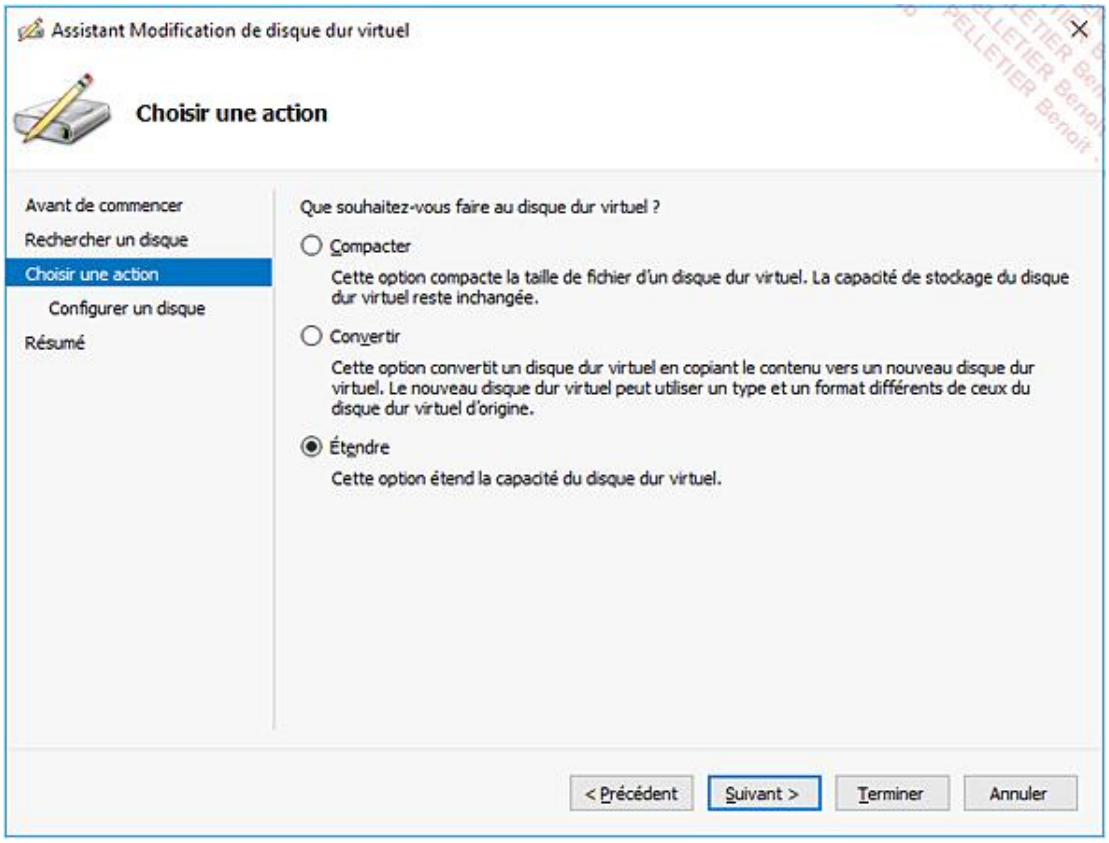
Les administrateurs ont maintenant la possibilité d'effectuer cette opération sans éteindre le serveur et donc sans couper l'accès à une fonctionnalité (Exchange, serveur de fichiers…). Néanmoins la fonctionnalité n'est opérationnelle que pour des fichiers VHDX connectés à un contrôleur SCSI. La taille peut être augmentée ou réduite.

Pour effectuer cette opération, il est nécessaire de procéder aux actions suivantes :

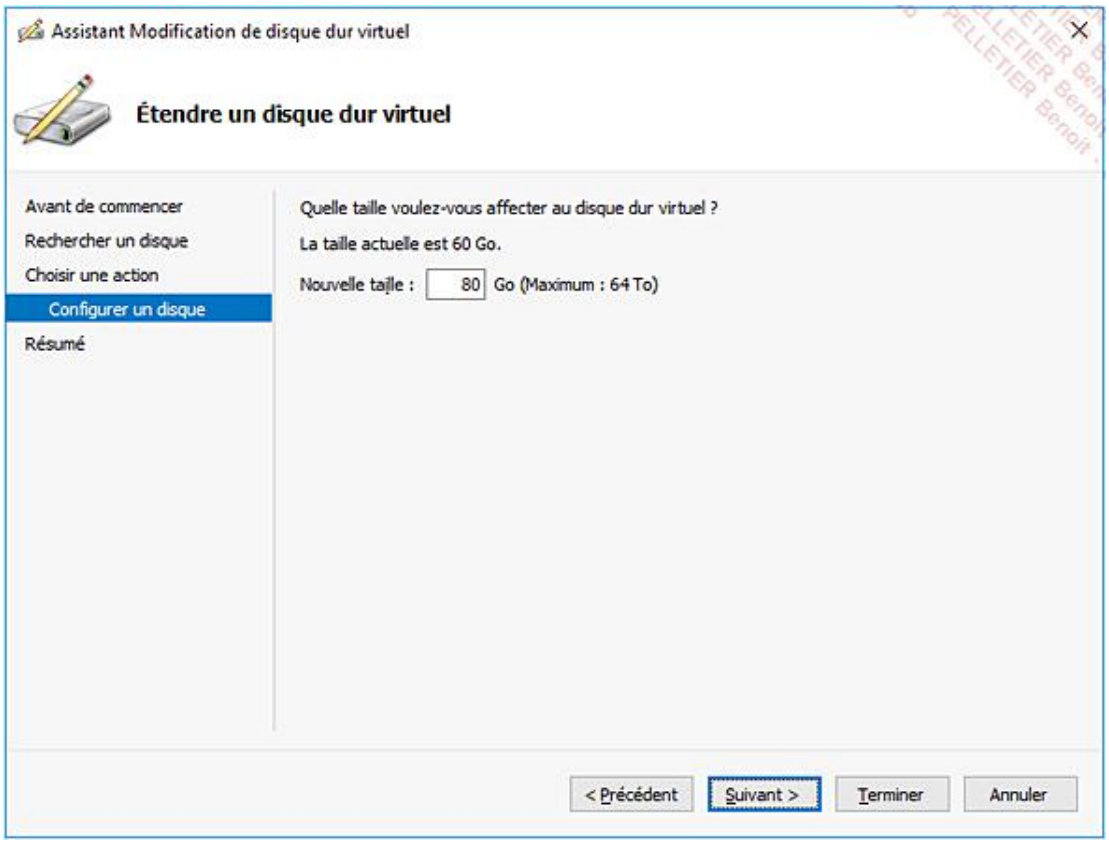
- Effectuez un clic droit sur une machine virtuelle puis sélectionnez l'option **Paramètres**.
- Sélectionnez le disque **.vhdx** de la machine puis cliquez sur **Modifier**.



- Dans la fenêtre **Rechercher un disque virtuel**, cliquez sur **Suivant**.
- Sélectionnez le bouton radio **Étendre** puis cliquez sur **Suivant**.



- Indiquez une taille supérieure à celle actuelle puis cliquez sur **Suivant**.



- Enfin, cliquez sur **Terminer** pour valider l'action.

La taille du disque dur virtuel a été étendue alors que la machine était en cours d'exécution.

Gestion des réseaux virtuels

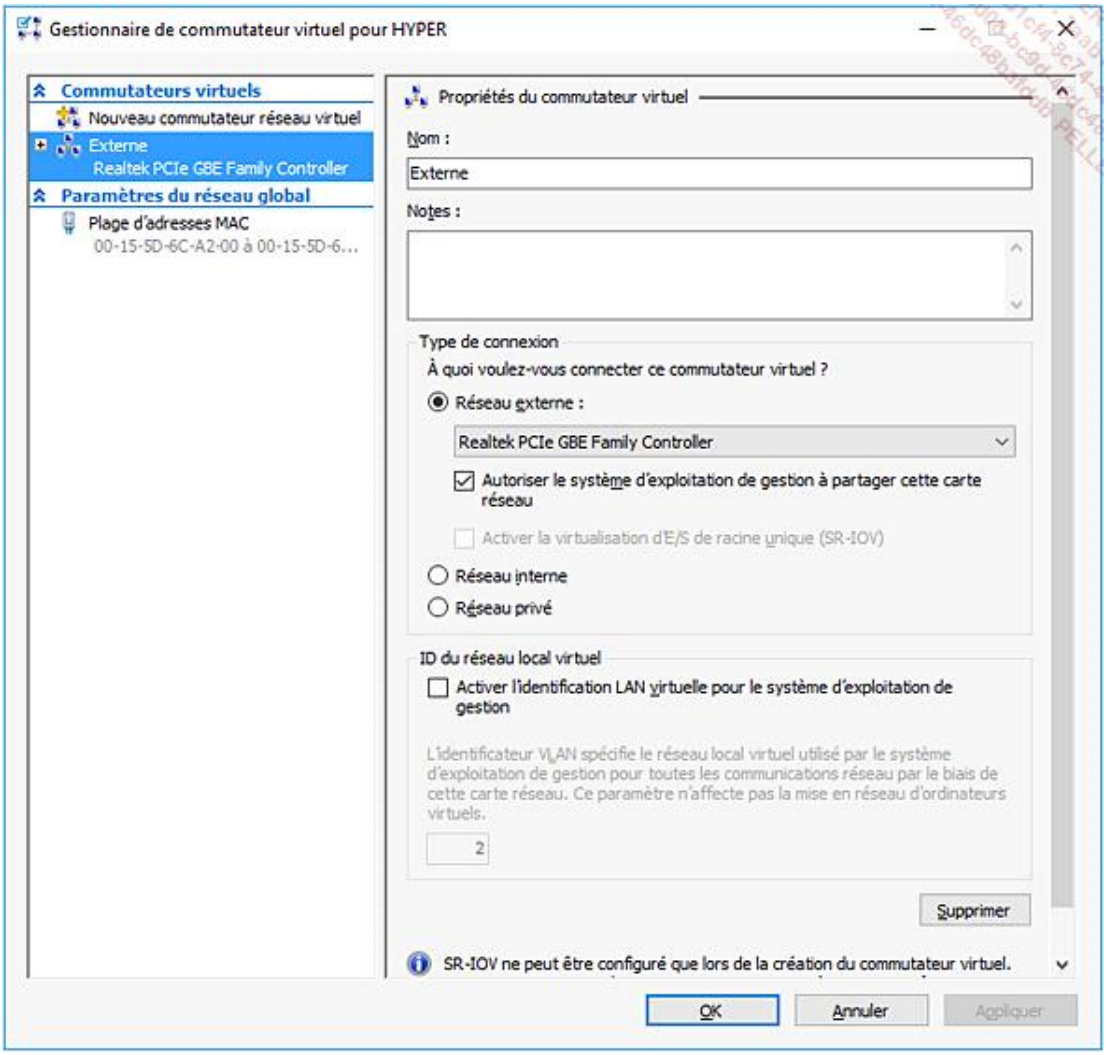
Plusieurs types de réseaux peuvent être créés et appliqués à une machine virtuelle. Ceci afin de permettre aux différentes stations de communiquer entre elles ou avec des équipements externes à la machine hôte (routeur, serveur…).

Les commutateurs virtuels

Le principe d'un commutateur virtuel est le même que celui d'un commutateur (switch) physique que l'on peut trouver sur n'importe quel réseau informatique. Connu sous le terme de réseau virtuel avec Windows Server 2008, on parle maintenant de commutateur virtuel. Il est possible de gérer ces derniers en utilisant l'option **Gestionnaire de commutateur virtuel** dans le bandeau **Actions**.

Trois types de switch peuvent être créés :

- **Externe** : avec ce type de commutateur virtuel, il est possible d'utiliser la carte réseau de la machine hôte dans la machine virtuelle. Ainsi, cette dernière obtient une connexion sur le réseau physique lui permettant d'accéder à un équipement ou un serveur du réseau de production.
- **Interne** : permet la création d'un réseau entre la machine physique et les machines virtuelles. Il permet la communication entre les machines virtuelles ainsi qu'avec l'hôte physique qui les héberge. Il n'est pas lié à carte réseau physique, il est donc impossible pour les machines virtuelles d'accéder au réseau local.
- **Privé** : la communication peut se faire uniquement entre les machines virtuelles, la machine hôte ne peut pas contacter une des VM.


Gestionnaire de commutateur virtuel pour HYPER
Commutateurs virtuels
Nouveau commutateur réseau virtuel
Externe
Realtek PCIe GBE Family Controller
Paramètres du réseau global
Plage d'adresses MAC
00-15-5D-6C-A2-00 à 00-15-5D-6...
Propriétés du commutateur virtuel
Nom :
Externe
Notes :
Type de connexion
À quoi voulez-vous connecter ce commutateur virtuel ?
Réseau externe :
Realtek PCIe GBE Family Controller
Autoriser le système d'exploitation de gestion à partager cette carte réseau
Activer la virtualisation d'E/S de racine unique (SR-IOV)
Réseau interne
Réseau privé
ID du réseau local virtuel
Activer l'identification LAN virtuelle pour le système d'exploitation de gestion
L'identificateur VLAN spécifie le réseau local virtuel utilisé par le système d'exploitation de gestion pour toutes les communications réseau par le biais de cette carte réseau. Ce paramètre n'affecte pas la mise en réseau d'ordinateurs virtuels.
2
Supprimer
SR-IOV ne peut être configuré que lors de la création du commutateur virtuel.
OK
Annuler
Appliquer

Gestion des machines virtuelles

De nouvelles fonctionnalités sont apparues avec Windows Server 2016. Certaines d'entre elles permettent d'améliorer la gestion quotidienne des machines virtuelles.

1. Mise à niveau de la version d'une VM

Les versions Hyper-V sous Windows Server 2012/2012 R2 et Windows Server 2016 utilisent une version des fichiers de configuration de la machine virtuelle différente. Ainsi certaines fonctionnalités offertes par le nouvel hyperviseur peuvent ne pas fonctionner sur la machine importée.

Les machines virtuelles possédant une version 5 sont compatibles avec des Hyper-V fonctionnant sous Windows Server 2012 R2 et Windows Server 2016. Ceux possédant une version 8 peuvent pour leur part fonctionner uniquement sur un hyperviseur Windows Server 2016.

Les cmdlets PowerShell permettent de connaître la version des machines hébergées. La commande ci-dessous affiche la version de chaque machine virtuelle.

```
Get-VM * | format-table Name,Version
```



Nous pouvons voir dans l'écran ci-dessus que la VM est en version 5. Il est donc possible d'utiliser la cmdlet suivante.

```
Update-Vm Version vmname
```



La version de la machine virtuelle est maintenant bien en 8.



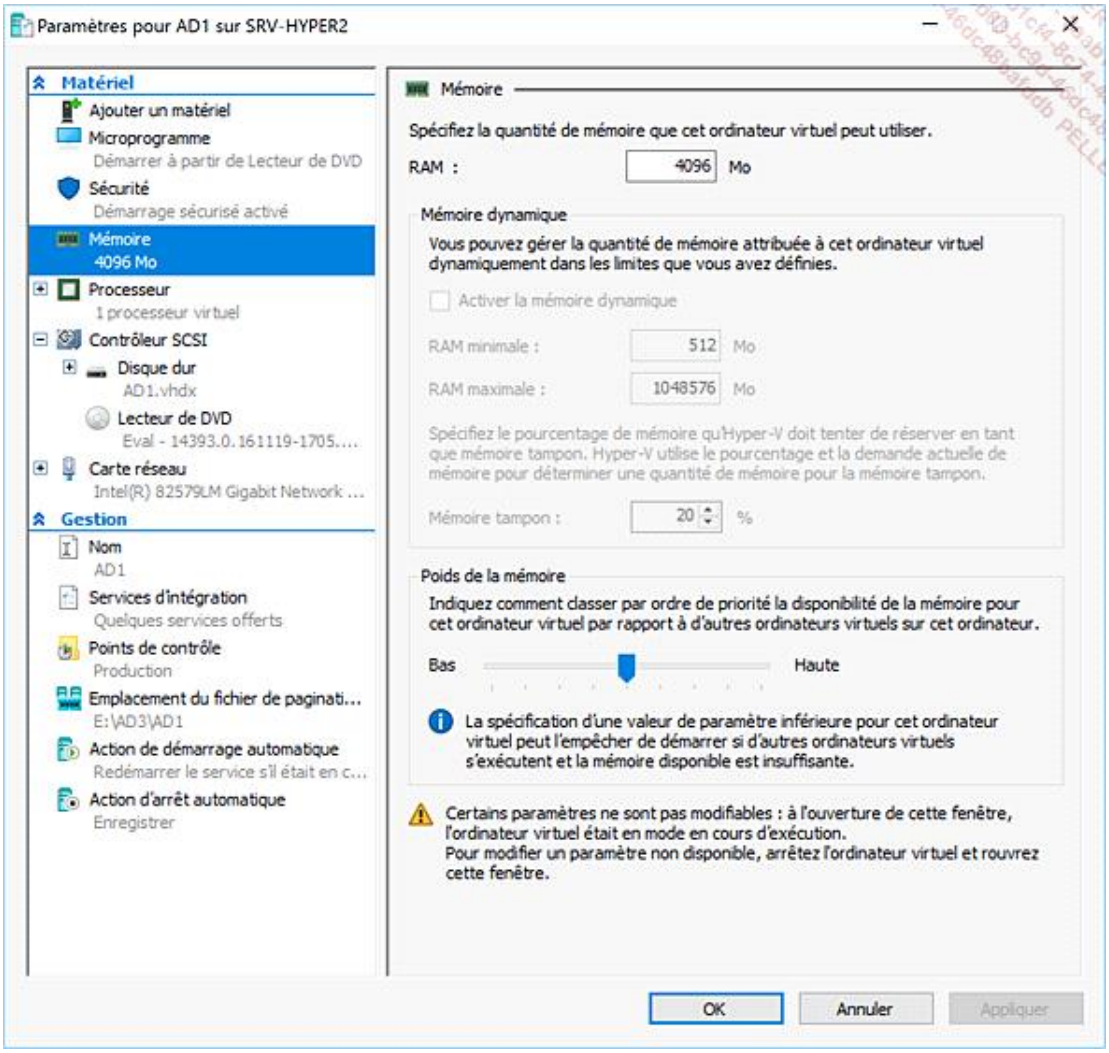
Il est intéressant de noter qu'il est impossible de passer d'une version 8 à une version 5.

2. Nouvelles fonctionnalités

Nous avons pu voir dans le point précédent une des fonctionnalités apportées à Hyper-V. Vous pouvez voir ci-dessous d'autres points.

3. Configuration des VM

Dans les anciennes versions d'Hyper-V, il était impossible de procéder à l'ajout de mémoire à chaud. En effet, cette opération ne pouvait être effectuée qu'après avoir éteint la machine. Dès lors, le service offert (Exchange, serveur de fichiers...) était inaccessible. Windows Server 2016 offre la possibilité de modifier la quantité de mémoire allouée à la machine virtuelle, et ce même si cette dernière est allumée. Les cartes réseau peuvent également être modifiées sans arrêt de la machine virtuelle. Néanmoins, seules les machines virtuelles de génération 2 sont concernées (Windows ou Linux). Dans le cas ci-dessous, la machine virtuelle est de génération 2 et en version 8.



Il est intéressant de noter qu'un nouveau format de fichier de configuration a vu le jour avec Windows Server 2016. Il améliore les performances de lecture et d'écriture des données de configuration de la machine. De plus le risque de corruption suite à une défaillance du système de stockage a été réduit.

Deux nouvelles extensions sont donc utilisées :

- VMCX : pour les fichiers de stockage.

- VMRS : pour les données de l'état d'exécution.

Services d'intégration

Les services d'intégration, qui permettent entre autres la synchronisation d'horloge avec l'hôte, sont désormais distribuables à l'aide de Windows Update.

Snapshot et PowerShell direct

Dans la version Hyper-V de Windows Server 2016, les snapshot ont été améliorés afin de prendre en compte ceux réalisés dans un contexte de production (avec VSS - *Volume Snapshots Service*). De plus il est maintenant possible de faire exécuter une commande ou script PowerShell sur la machine virtuelle depuis l'hôte de virtualisation.

```
Enter-pssession -vmname NomVM
Invoke-command -VMName NomVM -scriptBlock {commands}
```

Rolling Hyper-V Cluster Upgrade

En cas d'utilisation d'un cluster Hyper-V sous Windows Server 2012 R2, il est possible d'ajouter un nœud sous Windows Server 2016, ceci de manière transparente. Le cluster continuera de fonctionner avec le niveau de fonctionnement du cluster Windows Server 2012 R2.

Après avoir upgradé l'ensemble des nœuds vers Windows Server 2016, il sera possible d'augmenter le niveau fonctionnel du cluster. Pour cela la commande **Update-ClusterFunctionalLevel** pourra être utilisée. Comme pour l'Active Directory, il est impossible de faire un retour en arrière.

Linux Secure Boot

Cette version d'Hyper-V offre la possibilité de bénéficier du Secure Boot pour les VMs sous Linux. Cela nécessite néanmoins d'avoir une machine virtuelle de génération 2. Cette fonctionnalité nécessite d'exécuter la commande PowerShell suivante sur la machine hôte.

```
Set-VMFirmware NomVM -SecureBootTemplate
MicrosoftUEFICertificateAuthority
```

Connexion avec Hyper-V Manager

Il est désormais possible d'utiliser des *credentials* (nom d'utilisateur / mot de passe) différents afin de se connecter sur un autre serveur Hyper-V depuis la console.

Storage QoS

La création de règles QoS peut être effectuée sur un SOFS. Ces dernières pourront être appliquées aux disques durs virtuels des machines présentes dans Hyper-V. Cette fonctionnalité autorise une meilleure gestion du stockage en termes de charge.

Le bac à sable

Le bac à sable est un environnement virtuel ou physique de test qui permet de travailler sans perturber les machines ou serveurs en production.

La virtualisation permet de diminuer le nombre de machines physiques nécessaires. Ainsi un seul serveur est nécessaire pour faire fonctionner plusieurs machines virtuelles. Il sera néanmoins nécessaire d'avoir les ressources suffisantes (mémoire, espace disque suffisants...).

1. Configuration nécessaire

Un serveur ou machine robuste est nécessaire pour faire tourner les machines virtuelles. Le serveur utilisé pour cet ouvrage est équipé d'un Pentium Core i7 3,40 GHz et de 16 Go de RAM. Le système d'exploitation hôte installé est Windows Server 2012 R2.

Si votre configuration est inférieure à celle-ci, il suffira de démarrer seulement les machines virtuelles nécessaires. Il est utile de conserver un minimum de 1 Go pour la machine hôte.

La solution de virtualisation choisie est **Hyper-V** qui est intégré aux versions serveur de Windows depuis la version 2008. Il est possible d'installer Hyper-V sur Windows 8.1 et Windows 10, néanmoins une version Professionnel ou Entreprise est nécessaire.

2. Installation du système hôte

Le serveur Hyper-V utilisé pour cet ouvrage a été installé avec Windows Server 2012 R2. Il est néanmoins possible d'installer Windows Server 2016. Les opérations ci-dessous seront identiques quel que soit le système d'exploitation.

Avant de procéder à l'installation de Windows Server 2012 R2 sur le poste physique, il est nécessaire de s'assurer de respecter les prérequis du système d'exploitation.

- **Processeur** : 1,4 GHz minimum et architecture 64 bits.
- **Mémoire RAM** : 512 Mo minimum. Néanmoins, un serveur équipé de 1024 Mo s'avère être le strict minimum.
- **Espace disque** : une installation de base avec aucun rôle nécessite un espace disque de 15 Go. Il faut prévoir un espace plus ou moins conséquent en fonction du rôle du serveur.

Depuis Windows 2008, deux types d'installation sont proposés.

Une **installation complète** : une interface graphique est installée et permet l'administration du serveur de manière graphique ou en ligne de commande.

Une **installation minimale** : le système d'exploitation est installé mais aucune interface graphique n'est installée. Seule une invite de commandes est présente : les installations des rôles et fonctionnalités, ou l'administration quotidienne, se font en ligne de commande. Il est néanmoins possible d'administrer les différents rôles à distance en installant les fichiers **RSAT** (*Remote Server Administration Tools*) sur un poste distant.

Une fois l'installation du serveur terminée, il est nécessaire de configurer le nom du serveur et de définir sa configuration IP.

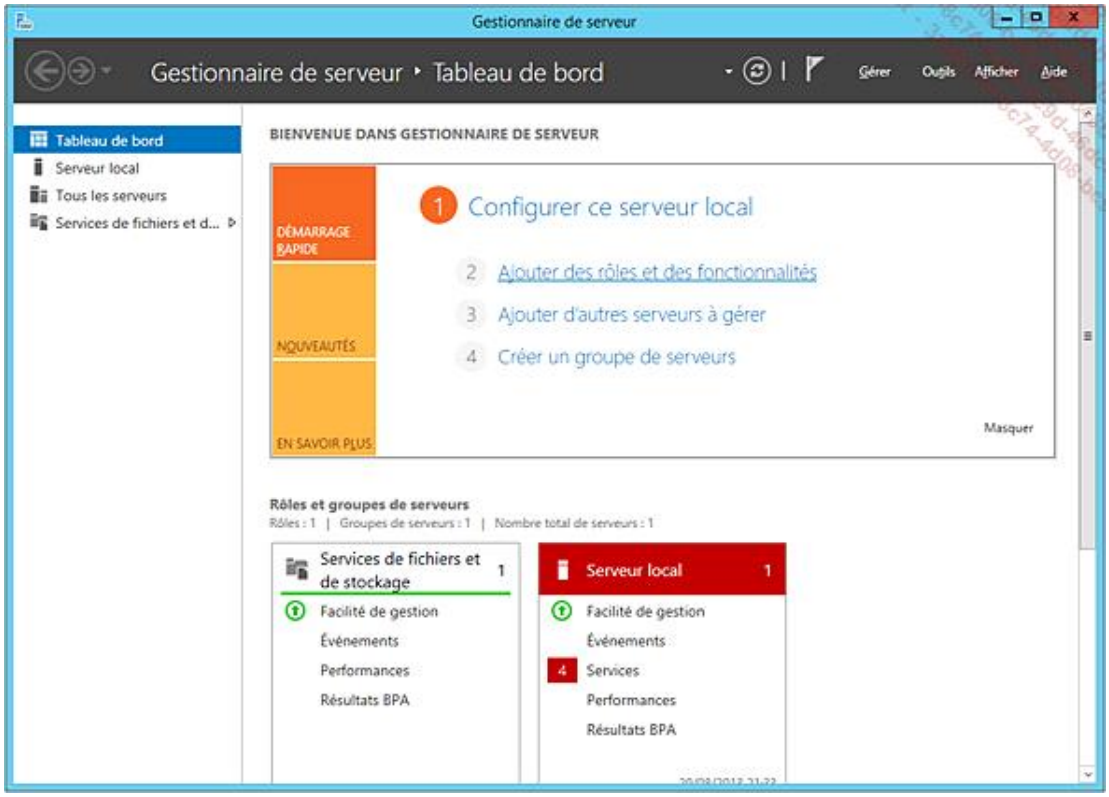
Création des machines virtuelles

L'étape suivante est l'installation du rôle **Hyper-V** puis la création, l'installation et la configuration des différentes machines virtuelles.

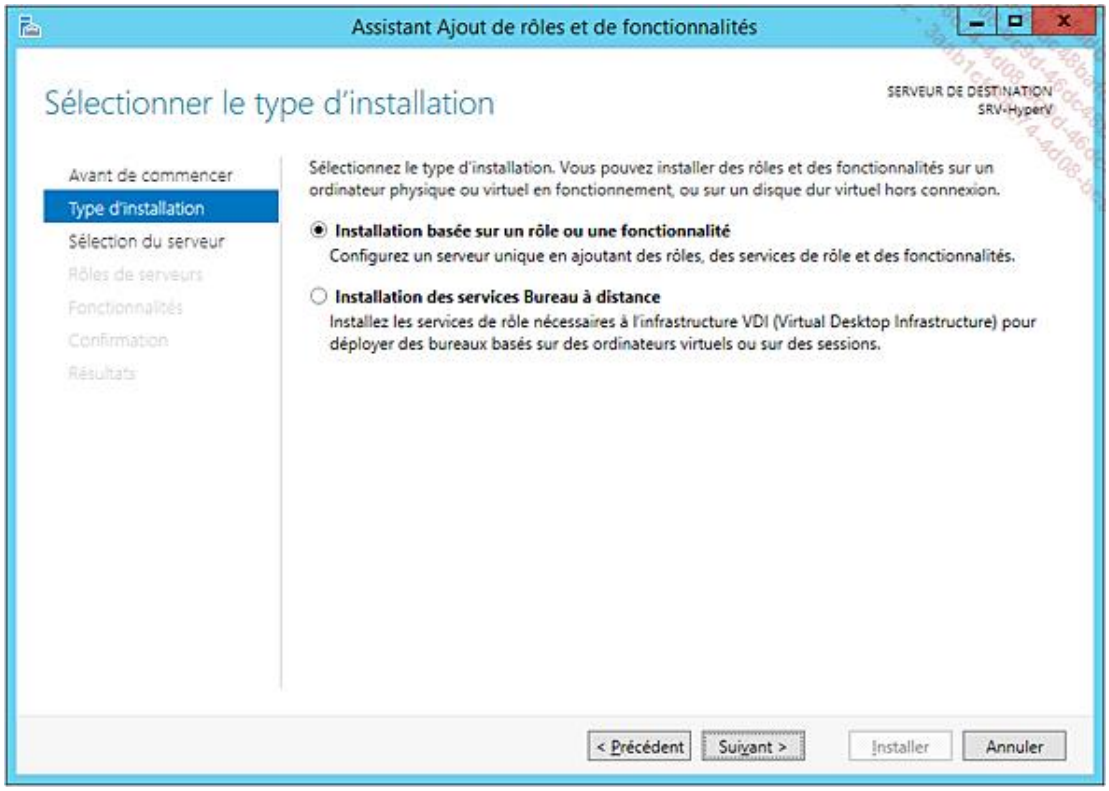
- Cliquez sur le **Gestionnaire de serveur** (première icône dans la zone de lancement rapide).



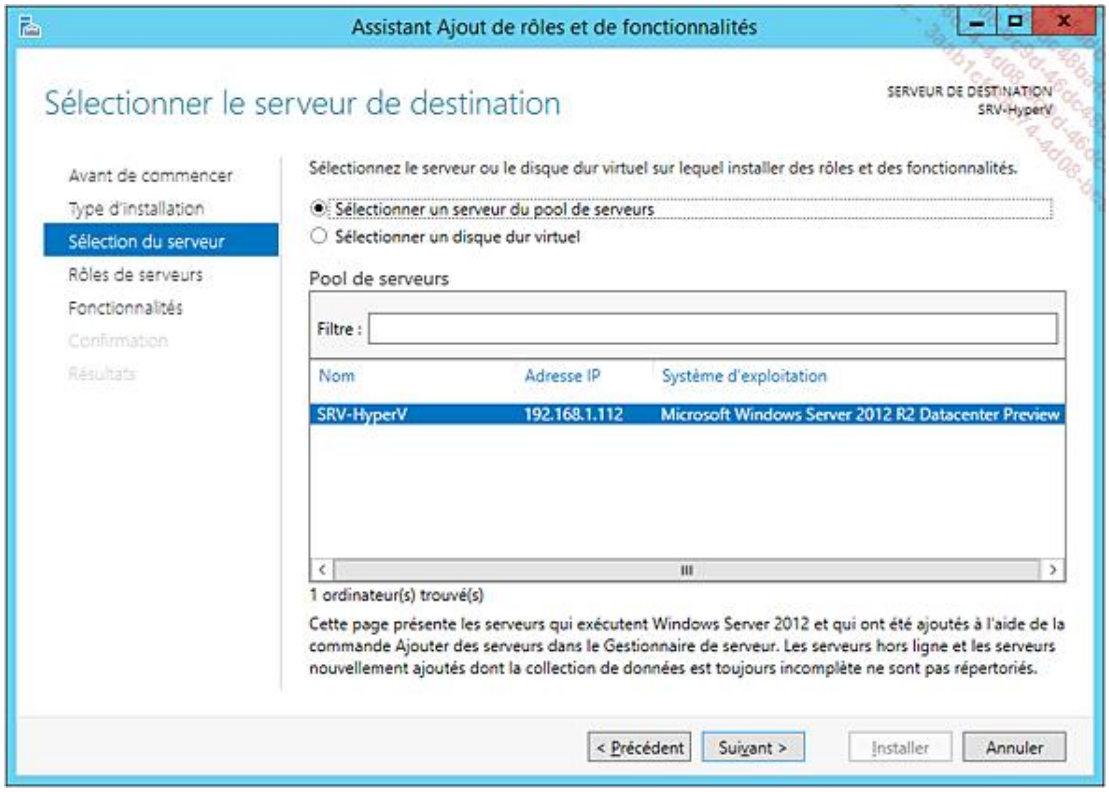
- Dans la console, cliquez sur **Ajouter des rôles et fonctionnalités**.



- L'assistant se lance. Cliquez sur **Suivant**.
- **Hyper-V** est un rôle, laissez le choix par défaut puis cliquez sur **Suivant**.

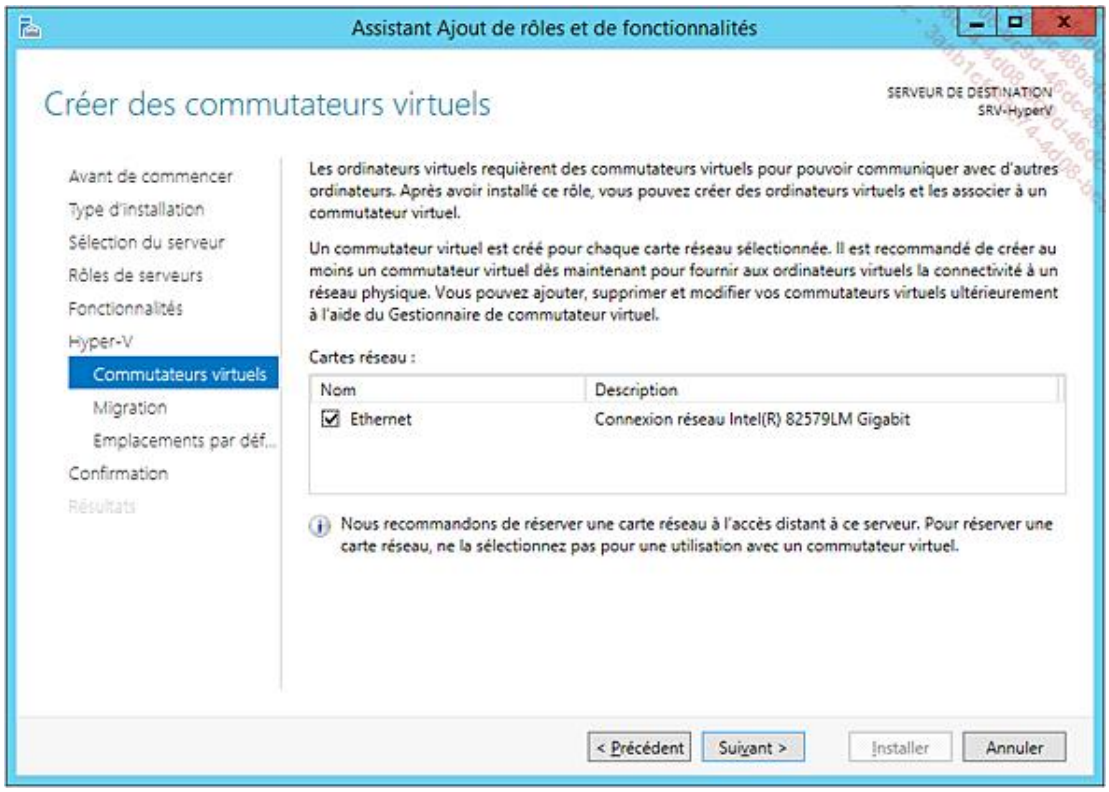


- Vérifiez que la machine de destination est bien la vôtre, puis cliquez sur **Suivant**.



- Cochez la case **Hyper-V**, puis cliquez sur **Ajouter des fonctionnalités** dans la fenêtre qui s'affiche.
- Cliquez sur **Suivant** dans la fenêtre d'installation des fonctionnalités.
- Il est nécessaire de créer un commutateur virtuel : cliquez sur la carte réseau afin de faire un pont entre le réseau physique et la machine virtuelle. Cette action peut être effectuée par la suite ; de même, il sera également possible de créer d'autres commutateurs virtuels.

- Cliquez sur **Suivant**.

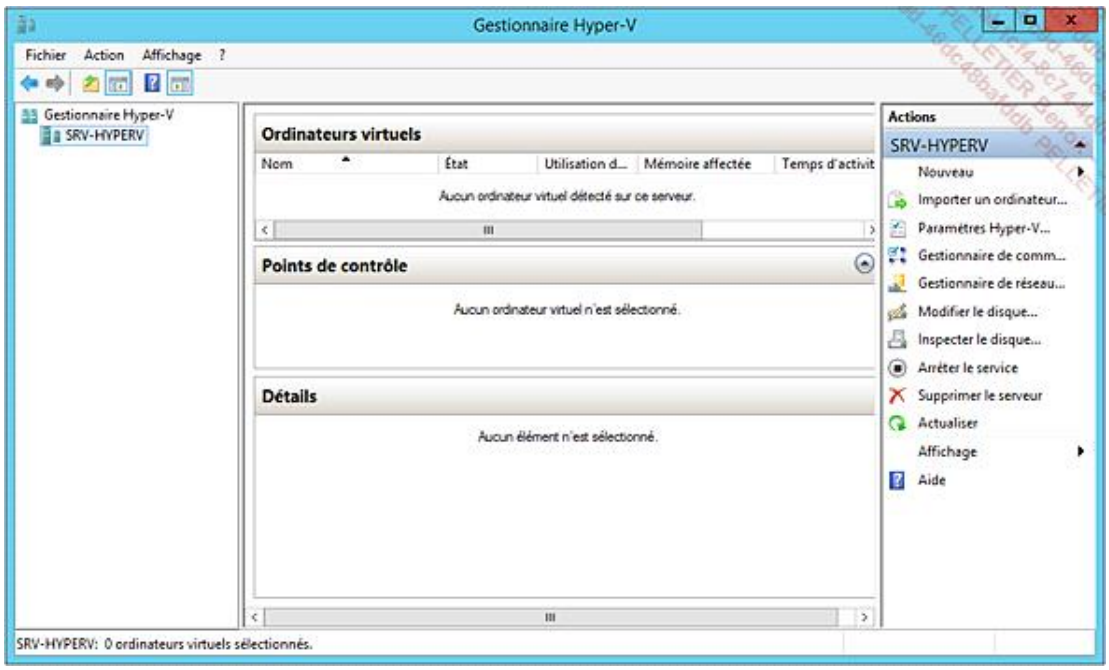


- Cliquez deux fois sur **Suivant**, puis sur **Installer** dans la fenêtre **Confirmer les sélections d'installation**.
- Redémarrez le serveur une fois l'installation terminée.
- Cliquez sur le menu **Démarrer**.

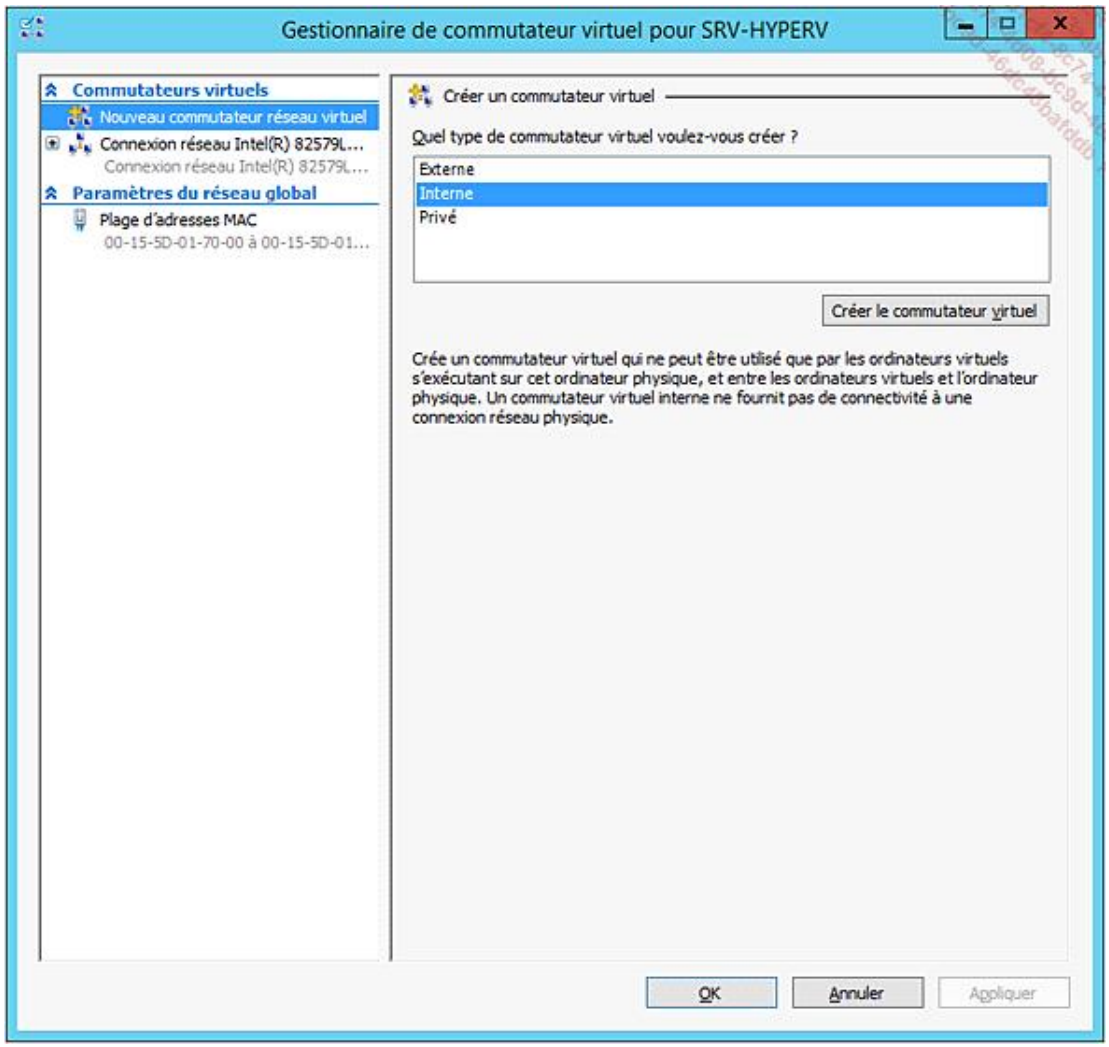
Une icône est présente pour le **Gestionnaire Hyper-V** dans les **Outils d'administration**.

Il est maintenant nécessaire de configurer l'interface réseau. Il est possible d'utiliser la carte physique ou de créer une carte interne. Pour cette dernière, deux options sont possibles :

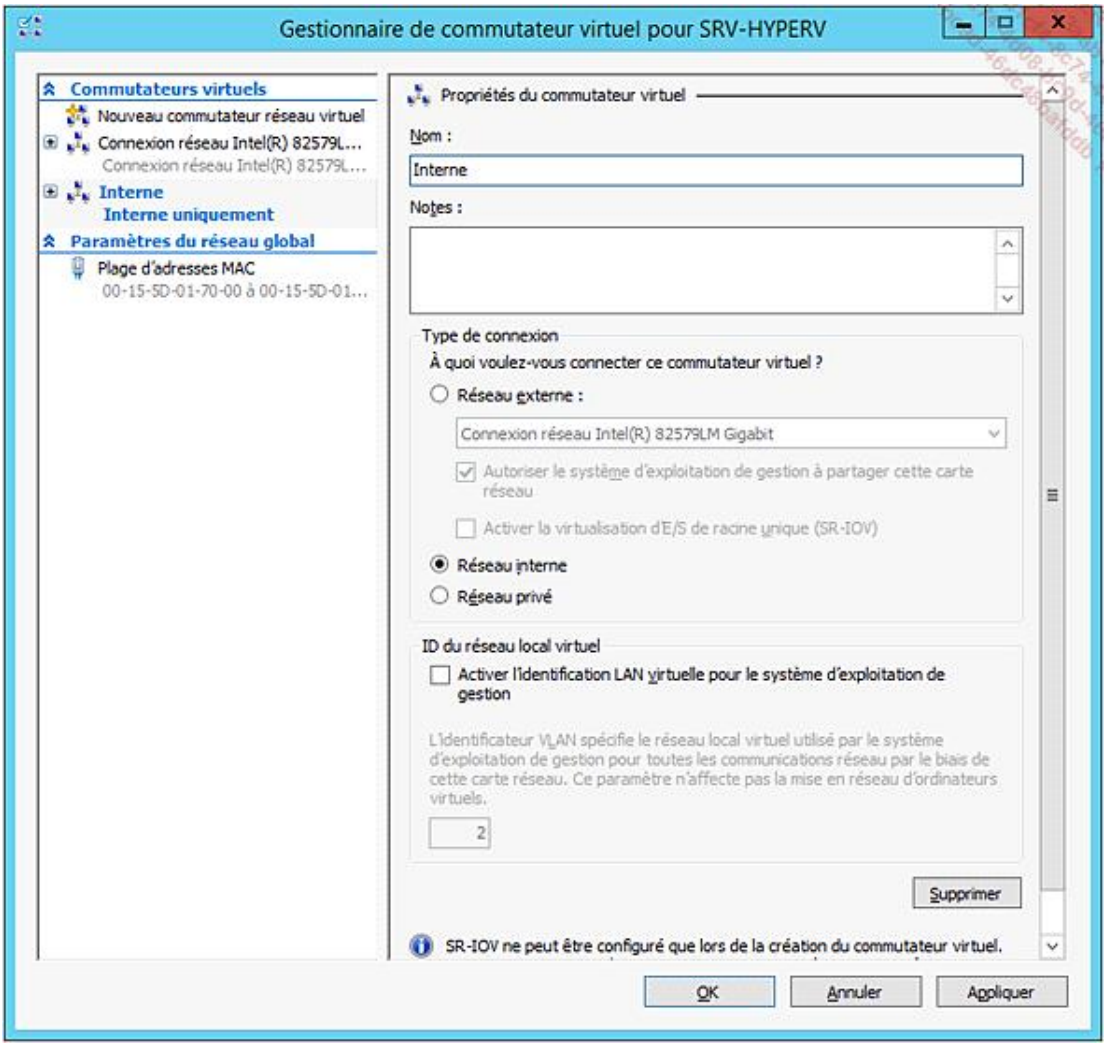
- **Réseau interne** : un réseau virtuel est créé entre la machine hôte et les machines virtuelles. Il est impossible de joindre une machine/périphérique sur le réseau physique (serveur, imprimante réseau…).
- **Réseau privé** : les machines virtuelles sont isolées de la machine hôte, les VM ne peuvent pas contacter la machine hôte ainsi que les machines sur le réseau physique.



- Cliquez sur **Gestionnaire de commutateur virtuel** dans la console **Hyper-V** (bandeau **Actions**).
- Cliquez sur **Interne** puis sur le bouton **Créer le commutateur virtuel**.



- Nommez la carte nouvellement créée **Interne**.



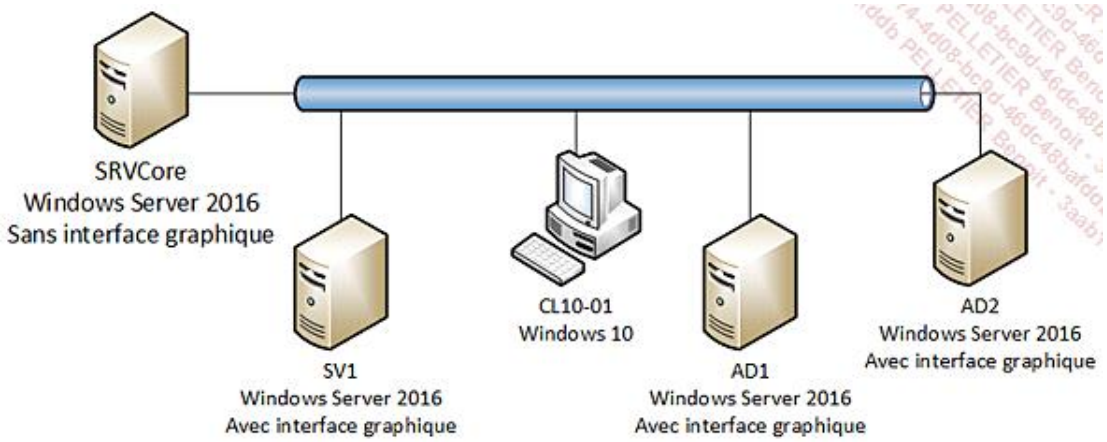
Cliquez sur **Appliquer** puis sur **OK**.

1. Schéma de la maquette

Cinq machines virtuelles vont être créées, les systèmes d'exploitation utilisés sont Windows Server 2016 ou Windows 10. De plus certains ateliers (migration d'un serveur de fichier, migration du DHCP…) nécessitent une machine virtuelle exécutant Windows Server 2012 R2. Il est également possible d'utiliser une VM sous Windows Server 2008 ou 2008 R2. Les commandes PowerShell devront néanmoins être adaptées à ce système. Il est important de noter que ces dernières ne fonctionnent pas sur Windows Server 2003.

La maquette contient quatre serveurs et un poste de travail virtuel :

- **AD1**, contrôleur de domaine du domaine formation.local.
- **AD2**, contrôleur de domaine du domaine formation.local.
- **SV1**, serveur membre du domaine formation.local.
- **SRVCore**, serveur en version core (installation minimale), non membre du domaine).
- **CL10-01**, poste client sous Windows 10 membre du domaine formation.local.



Rôles installés et configuration des serveurs et postes :

	Rôles installés	Configuration IP
AD1	Active Directory, DNS et DHCP	Adresse IP : 192.168.1.10 Masque de sous-réseau : 255.255.255.0 Serveur DNS primaire : 192.168.1.10 Serveur DNS auxiliaire : 192.168.1.11
AD2	Active Directory et DNS	Adresse IP : 192.168.1.11 Masque de sous-réseau : 255.255.255.0 Serveur DNS primaire : 192.168.1.10 Serveur DNS auxiliaire : 192.168.1.11
SV1	Aucun rôle	Adresse IP : 192.168.1.12 Masque de sous-réseau : 255.255.255.0 Serveur DNS primaire : 192.168.1.10 Serveur DNS auxiliaire : 192.168.1.11
SRVCore	Aucun rôle	Adresse IP : 192.168.1.13 Masque de sous-réseau : 255.255.255.0 Serveur DNS primaire : 192.168.1.10 Serveur DNS auxiliaire : 192.168.1.11
CL10-01	Aucun rôle	Configuration attribuée par le serveur DHCP.

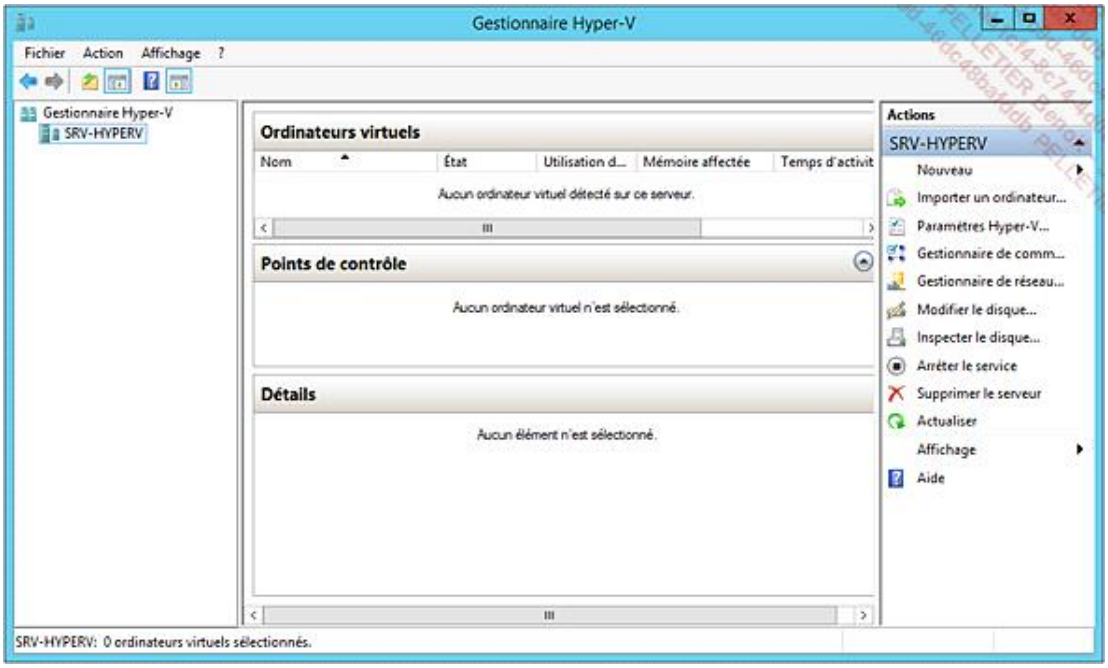
L'installation et la configuration des rôles sont détaillées dans les chapitres suivants.

2. Machine virtuelle AD1

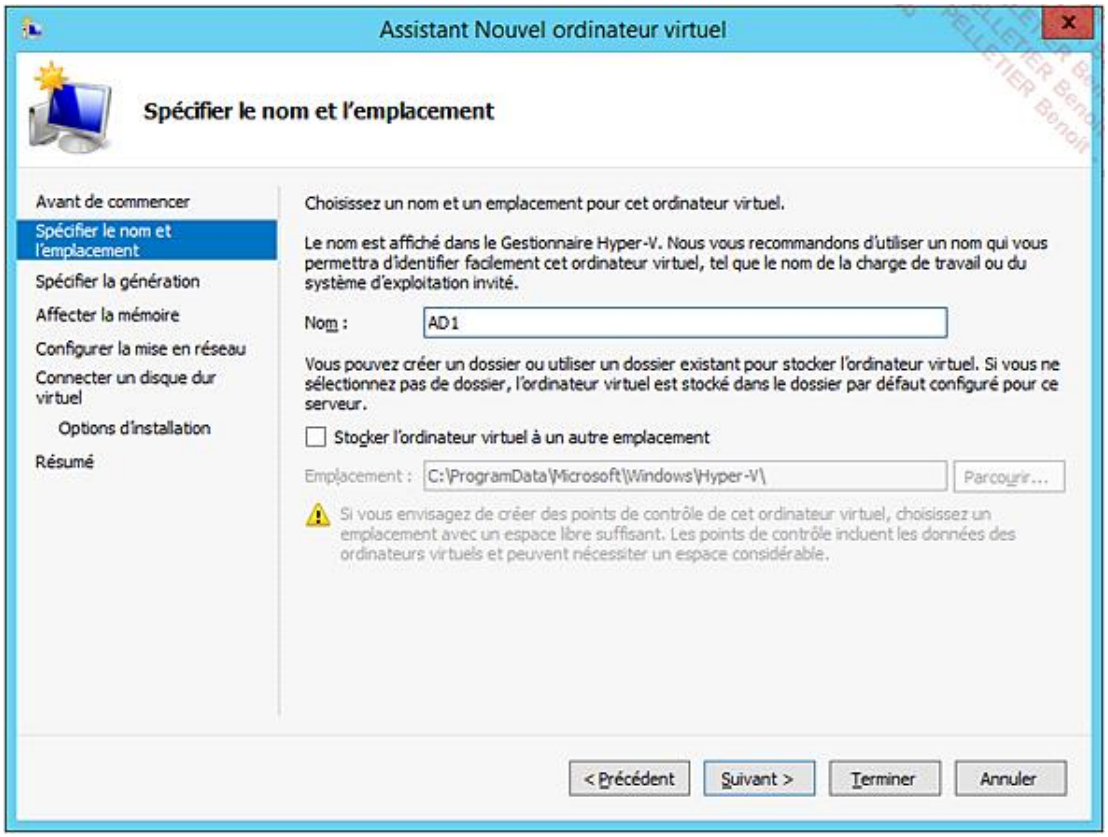
La procédure détaillée ci-dessous doit être reproduite pour les autres serveurs.

a. Création et paramétrage de la VM

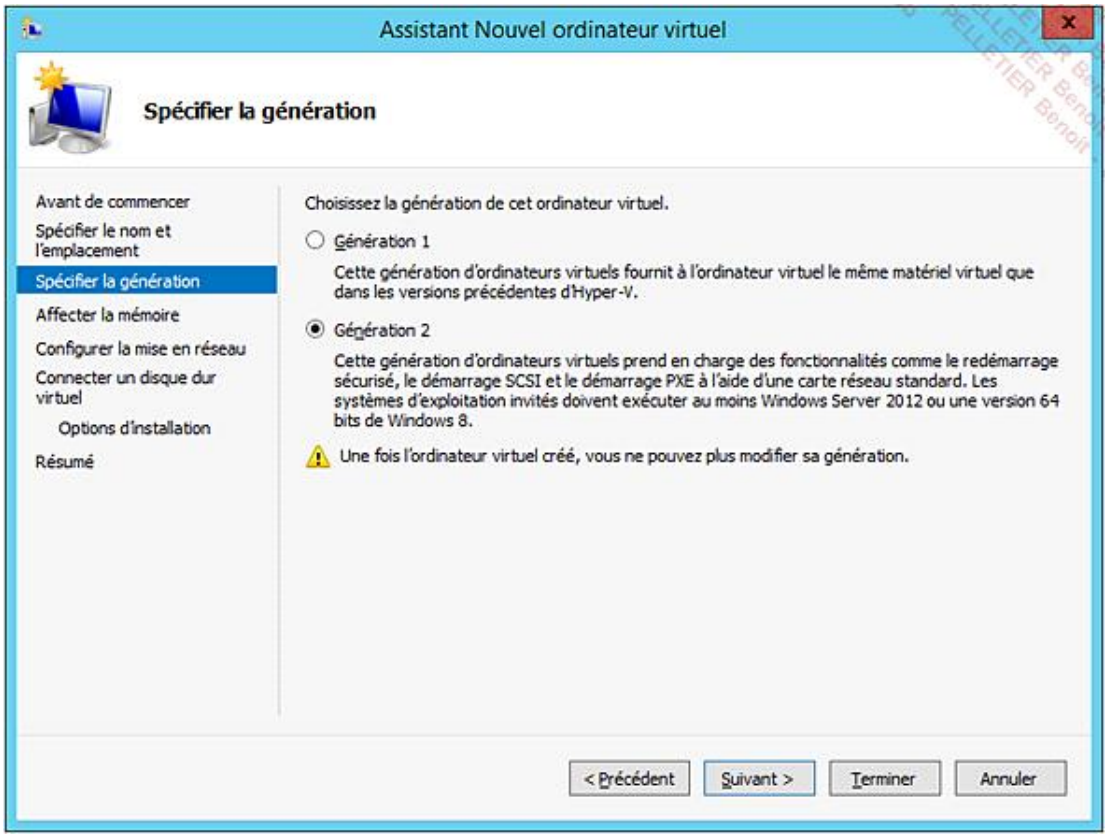
- Dans la console **Hyper-V**, cliquez sur **Nouveau** dans le volet **Actions** puis sur **Ordinateur virtuel**.



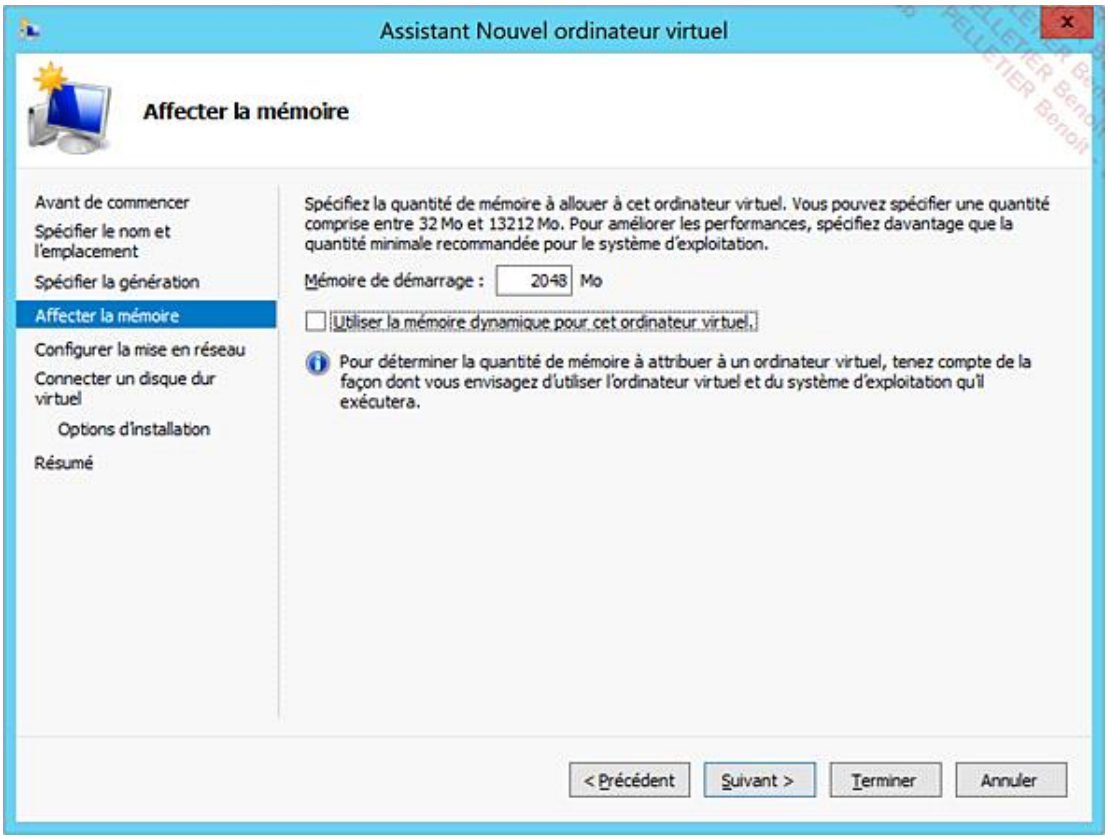
- Dans la fenêtre **Avant de commencer**, cliquez sur **Suivant**.
- Saisissez **AD1**, dans le champ **Nom**.



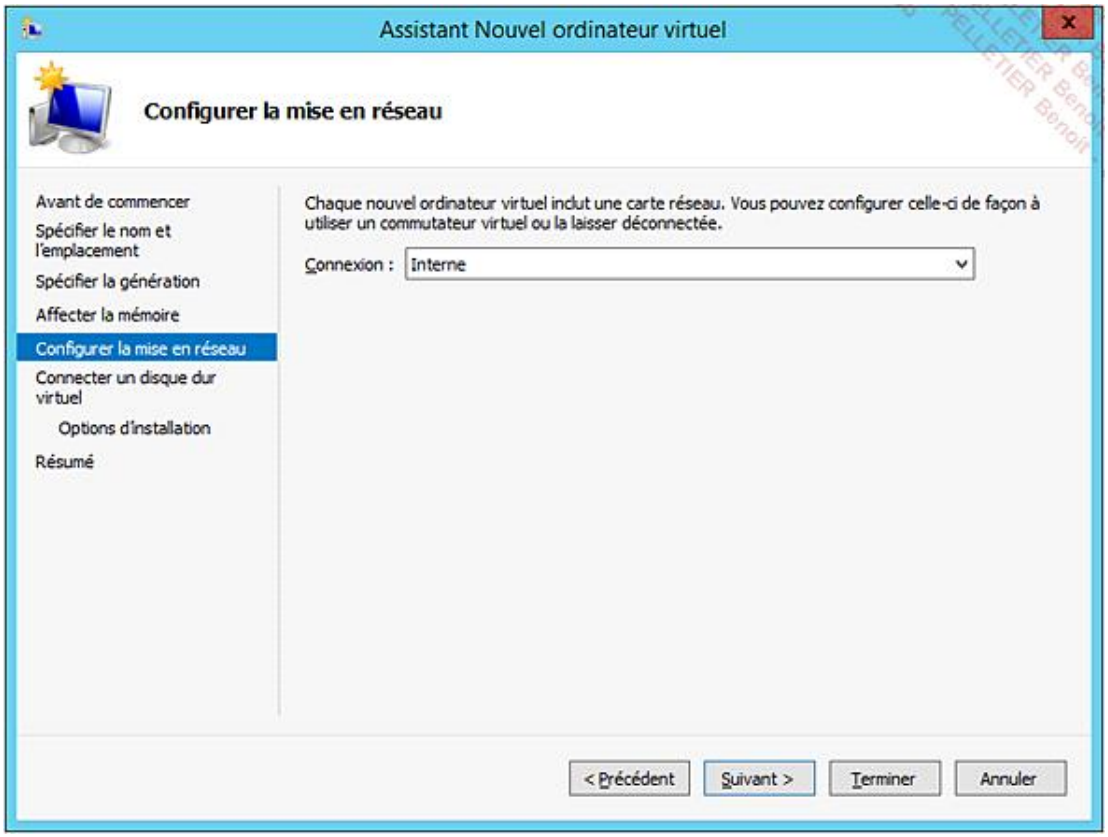
- Dans la fenêtre **Spécifier la génération**, cochez l'option **Génération 2** puis cliquez sur **Suivant**.



Saisissez **2048** dans le champ **Mémoire de démarrage**, ou plus si souhaité.



Dans la fenêtre **Configurer la mise en réseau**, sélectionnez la carte réseau souhaitée (interne ou carte réseau physique) puis cliquez sur **Suivant**.



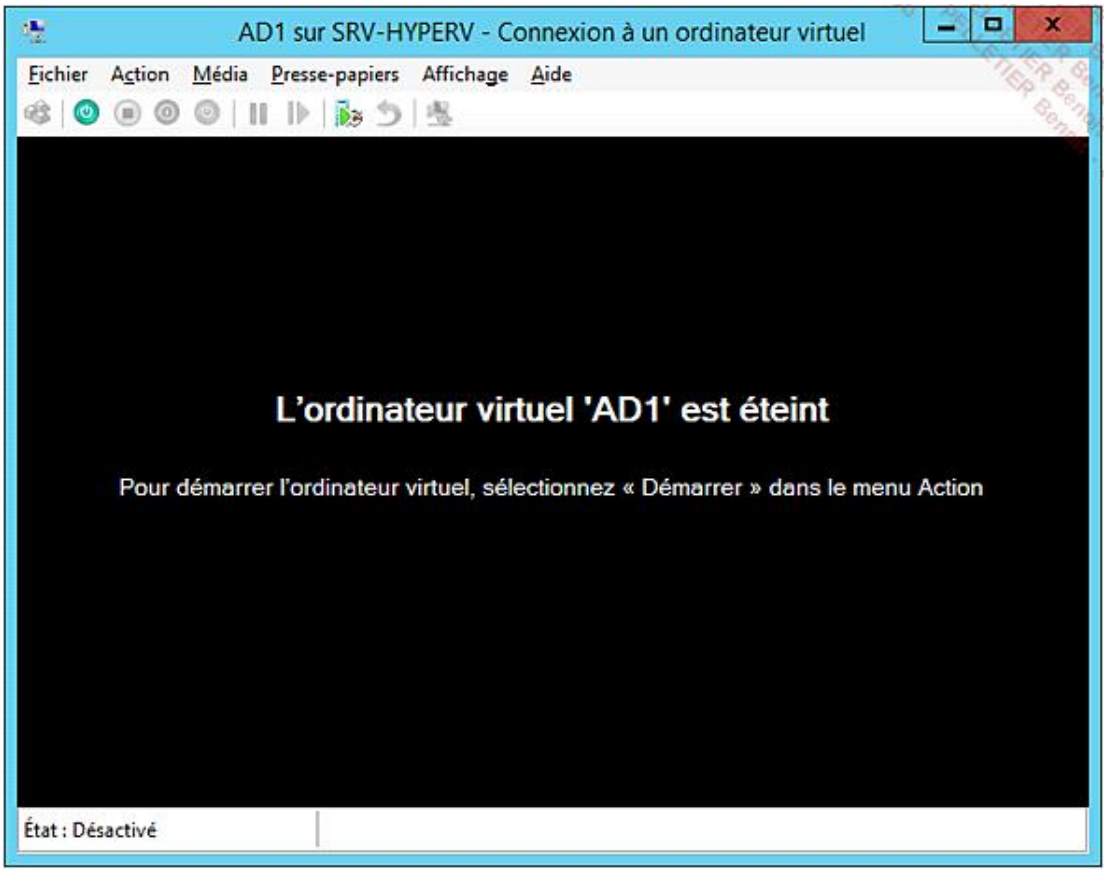
- Saisissez **60** dans le champ **Taille** du disque et validez à l'aide du bouton **Suivant**.
- Connectez à la machine virtuelle l'ISO ou le DVD de Windows Server 2016 et cliquez sur **Suivant**.
- Dans la fenêtre du résumé, cliquez sur **Terminer**.

La nouvelle machine apparaît dans la fenêtre centrale de la console.

Le disque dur de la machine est créé mais vierge. Il est nécessaire de le partitionner et d'installer un système d'exploitation.

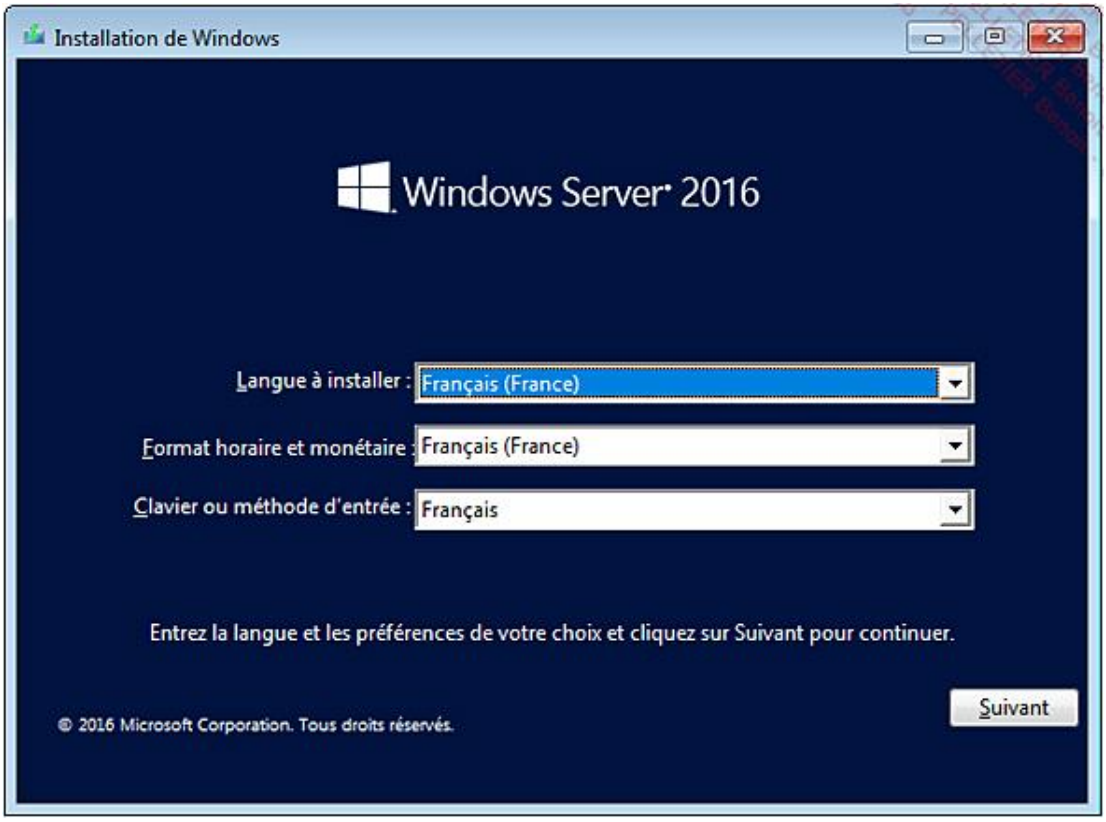
b. Installation du système d'exploitation

- Double cliquez sur l'ordinateur précédemment créé et visible dans la console. Cliquez sur le bouton **Démarrer** (bouton vert).

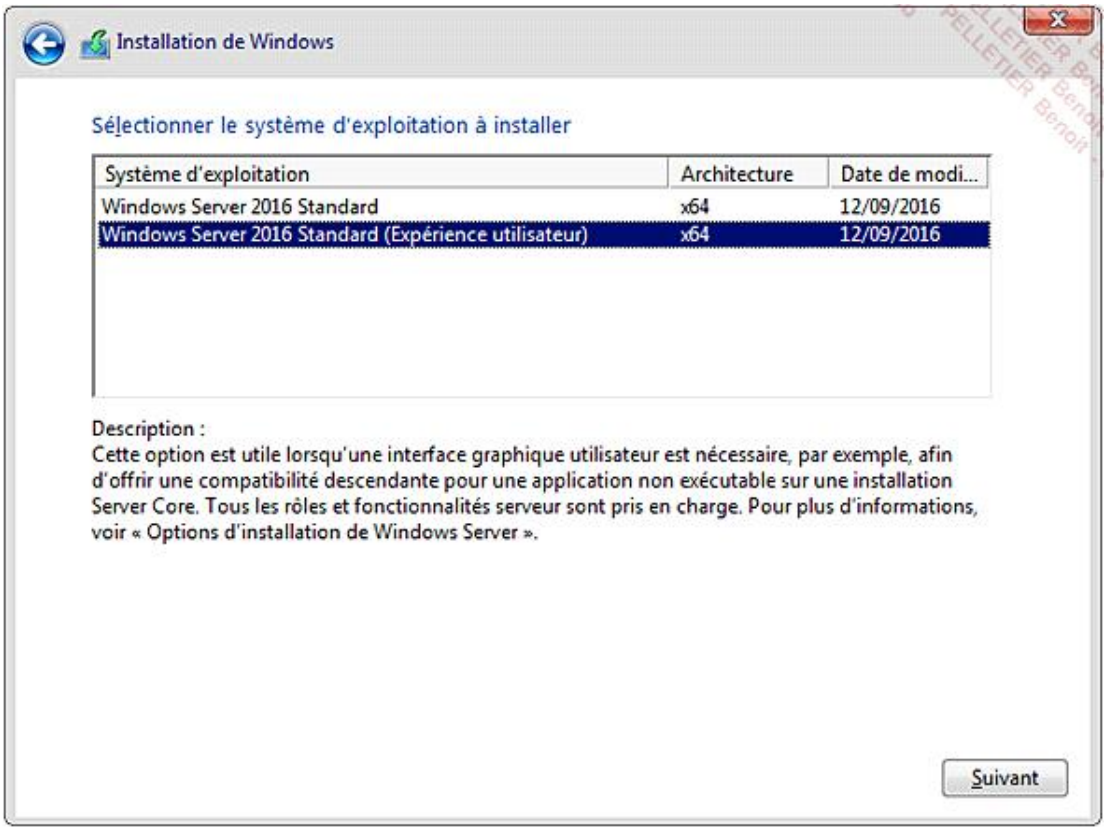


La machine démarre et l'installation de Windows Server 2016 débute.

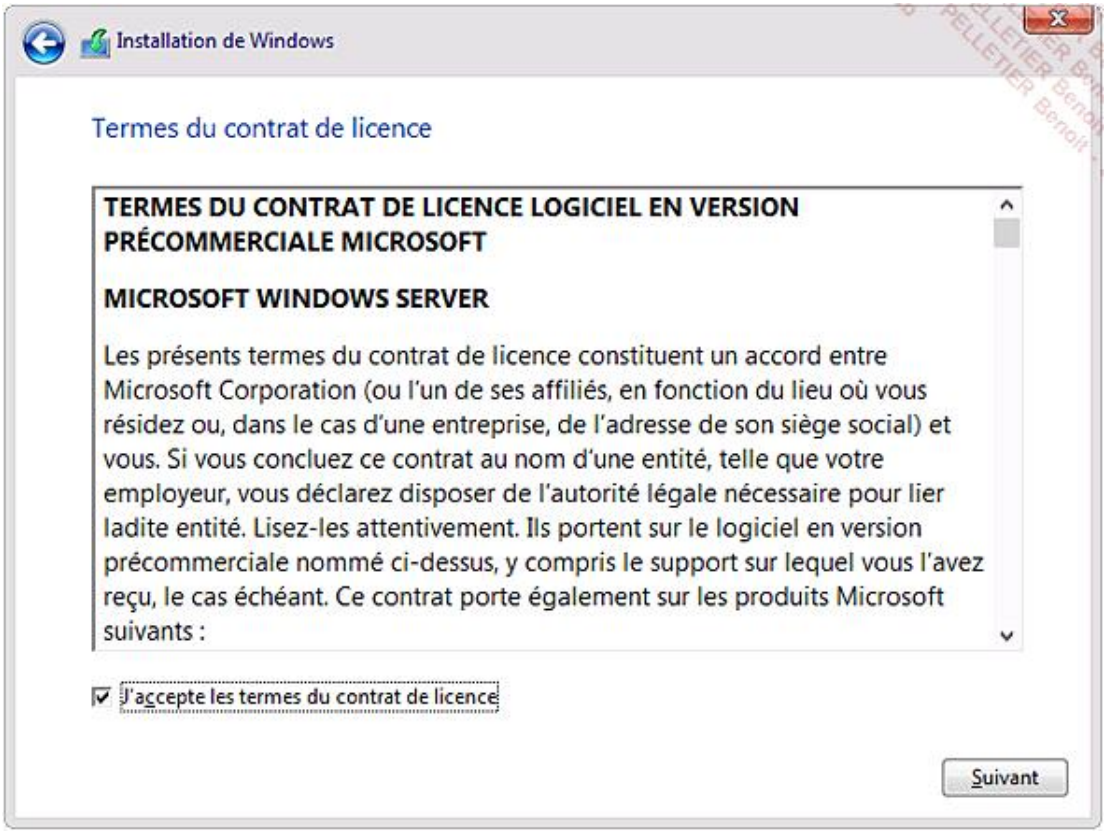
- Dans la fenêtre du choix des langues (la langue française est sélectionnée par défaut). Sélectionnez la langue souhaitée puis cliquez sur **Suivant**.



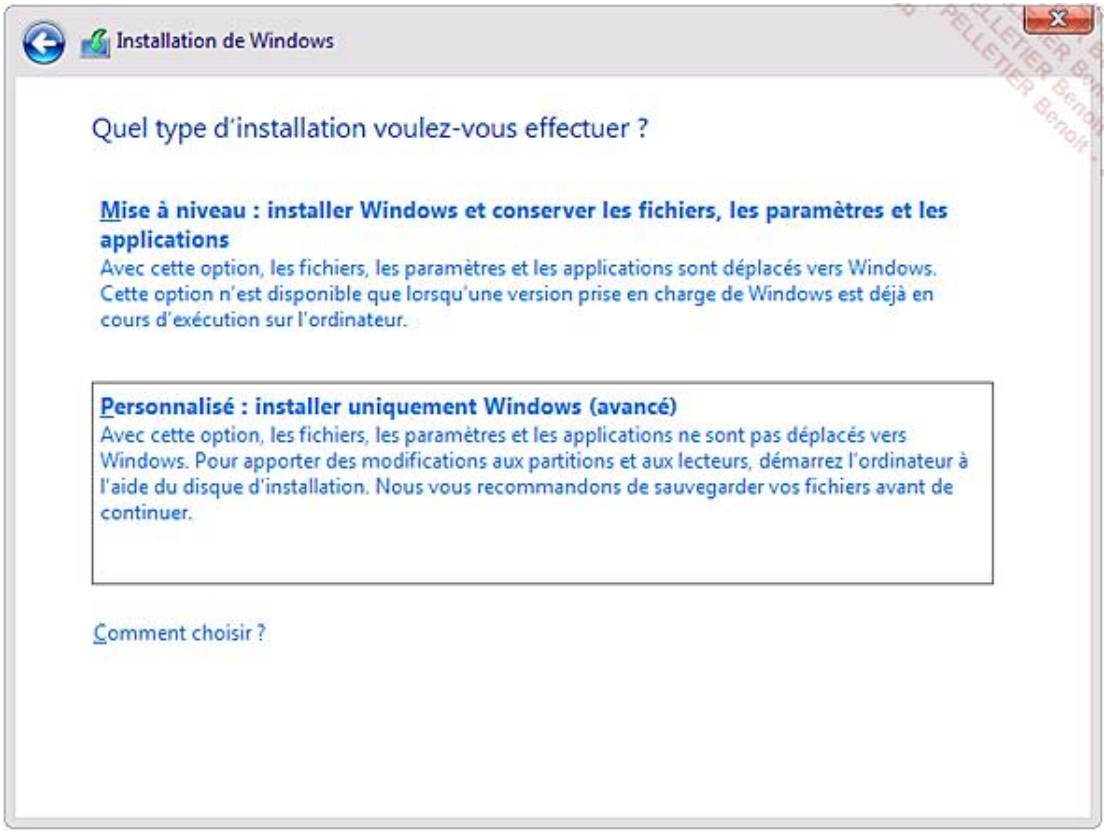
- Cliquez sur **Installer maintenant** pour lancer l'installation.
- Cliquez sur **Windows Server 2016 Standard (Expérience utilisateur)** puis cliquez sur **Suivant**.



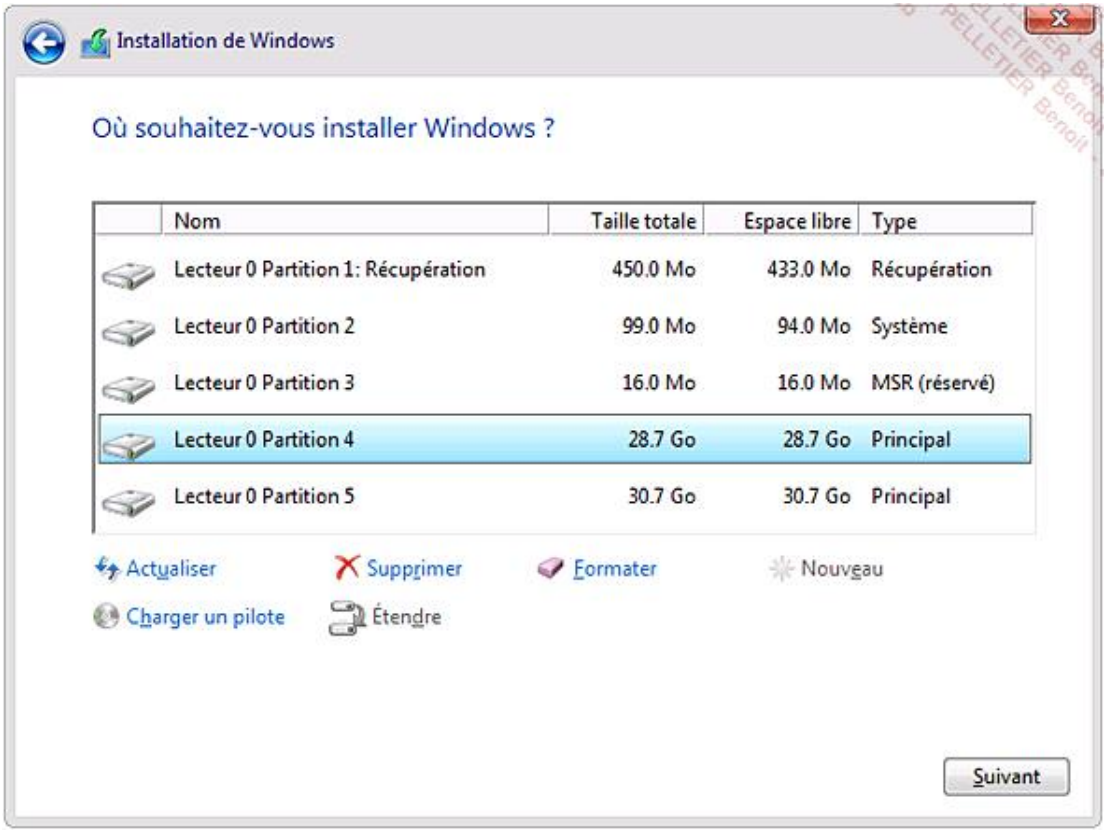
- Acceptez la licence puis cliquez sur **Suivant**.



Sélectionnez le type d'installation **Personnalisé : installer uniquement Windows (avancé)**.



À l'aide de l'option **Nouveau**, créez deux partitions de 30 Go.



Cliquez sur la première partition puis sur **Suivant**.

L'installation est en cours…

- Saisissez le mot de passe **Pa$$w0rd** puis confirmez-le.

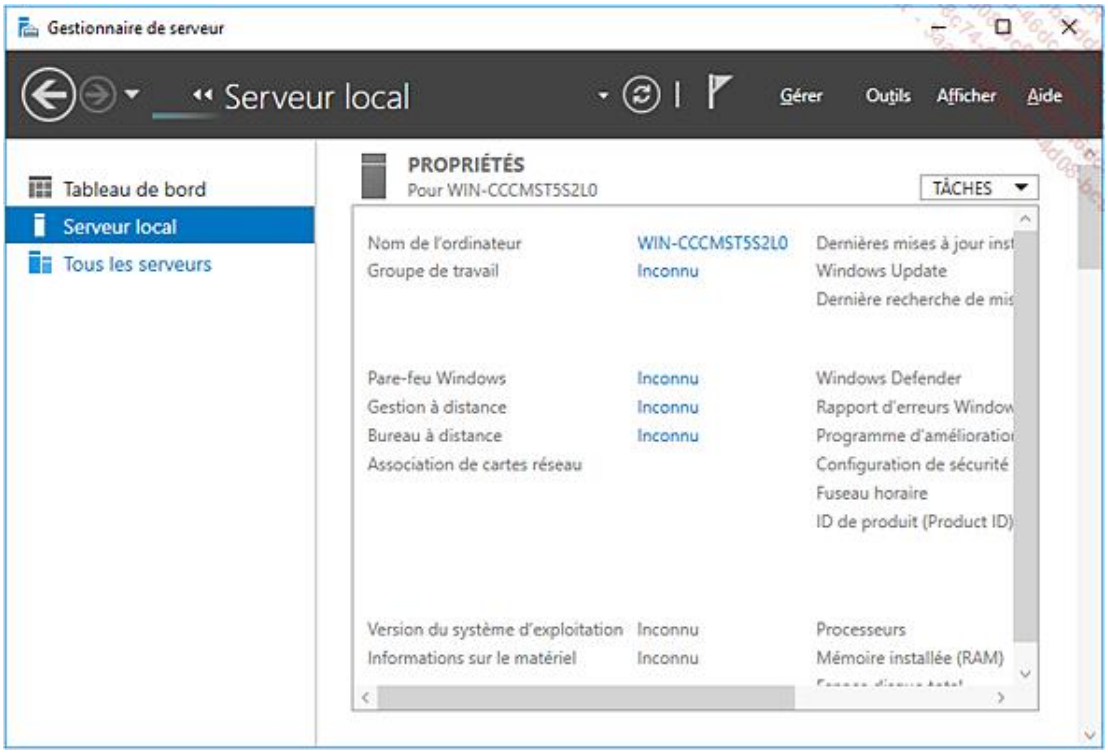
L'installation est maintenant terminée. L'étape suivante est la modification du nom du poste et la configuration IP de la machine.

c. Configuration post-installation

Afin d'effectuer un [Ctrl][Alt][Suppr] sur la machine virtuelle nouvellement installée, la séquence de touche [Ctrl][Alt][Fin] ou la première icône dans la barre d'outils doivent être utilisées.



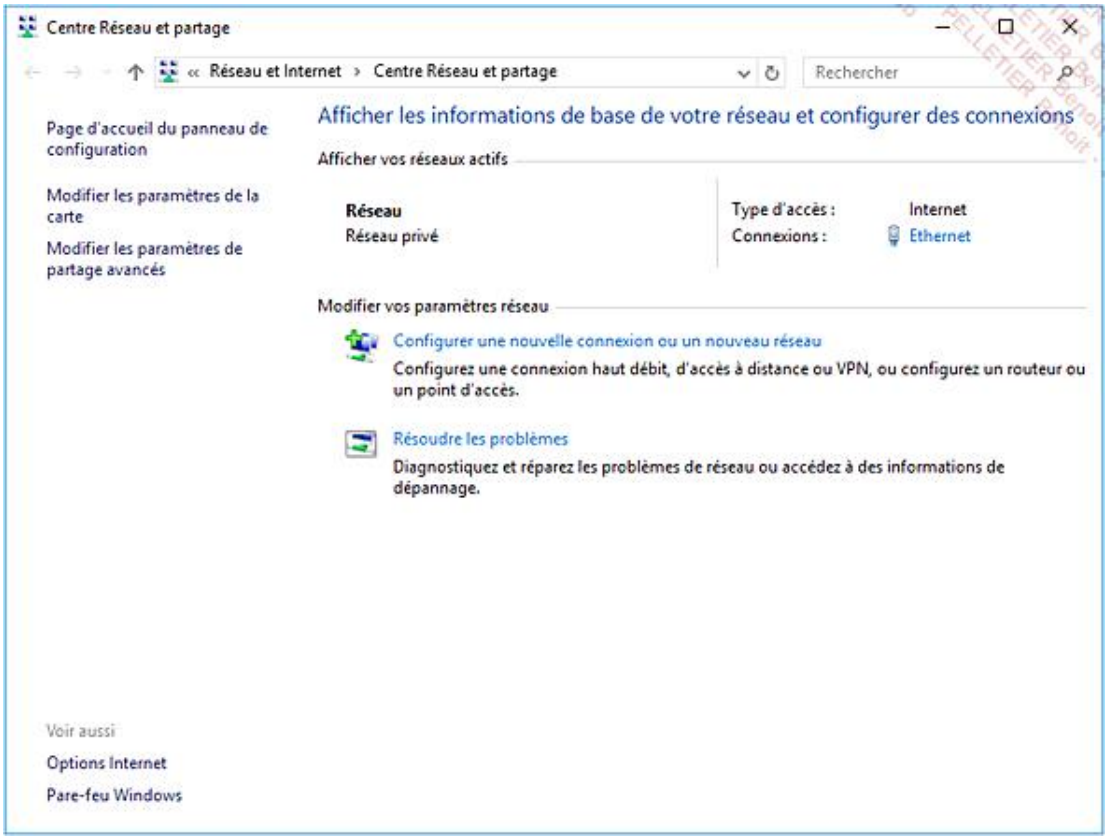
- Ouvrez une session en tant qu'**administrateur** en saisissant le mot de passe configuré à la section précédente.
- Dans la console **Gestionnaire de serveur**, cliquez sur **Serveur local**.



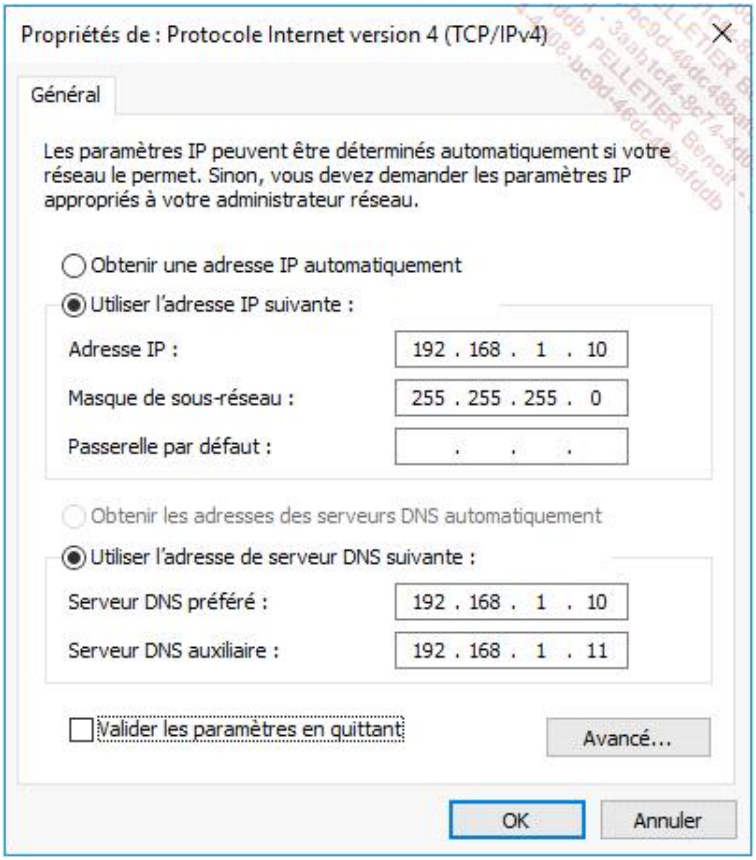
- Cliquez sur le **Nom de l'ordinateur** afin d'ouvrir les propriétés système.
- Dans la fenêtre **Propriétés système**, cliquez sur **Modifier** puis saisissez le nom du serveur (**AD1**).
- Cliquez deux fois sur **OK** puis sur **Fermer**.
- Redémarrez la machine virtuelle afin de rendre effectives les modifications.

Il est désormais nécessaire de configurer l'adressage IP de la carte réseau.

- Effectuez un clic droit sur le **Centre Réseau et partage** présent dans la zone de notification (icône à gauche de l'heure) puis cliquez sur **Ouvrir le Centre Réseau et partage**.
- Cliquez sur **Modifier les paramètres de la carte**.



- Double cliquez sur la carte réseau, puis sur **Propriétés**.
- Dans la fenêtre des propriétés, double cliquez sur **Protocole Internet Version 4 (TCP/IPv4)**.
- Configurez l'interface réseau comme ci-dessous.



Les manipulations à reproduire étant les mêmes, seuls les paramètres seront détaillés pour les machines virtuelles suivantes.

Les modifications à effectuer sont le nom du poste et sa configuration IP.

3. Machine virtuelle AD2

Ce serveur est le deuxième contrôleur de domaine de la maquette, il se nomme **AD2**. La quantité de mémoire allouée est de **2048 Mo** et le disque virtuel de **60 Go** est divisé en deux partitions.

- **Adresse IP** : 192.168.1.11
- **Masque de sous-réseau** : 255.255.255.0
- **Serveur DNS préféré** : 192.168.1.10
- **Serveur DNS auxiliaire** : 192.168.1.11
- **Mot de passe de l'administrateur local** : Pa$$w0rd

La machine ne doit pas être jointe au domaine, aucun rôle n'est à installer pour l'instant.

4. Machine virtuelle SV1

Ce serveur est membre du domaine. Différents rôles seront installés par la suite.

La quantité de mémoire allouée est de **2048 Mo** et le disque virtuel de **60 Go** est divisé en deux partitions.

- **Nom du poste** : SV1
- **Adresse IP** : 192.168.1.12
- **Masque de sous-réseau** : 255.255.255.0
- **Serveur DNS préféré** : 192.168.1.10
- **Serveur DNS auxiliaire** : 192.168.1.11
- **Mot de passe de l'administrateur local** : Pa$$w0rd

5. Machine virtuelle SRVCore

Ce serveur est installé en mode sans interface utilisateur (mode core). Toutes les configurations seront apportées dans les chapitres suivants.

La quantité de mémoire allouée est de **1024 Mo** et le disque virtuel de **30 Go** est partitionné avec une seule partition.

- **Mot de passe de l'administrateur local** : Pa$$w0rd

6. Machine virtuelle CL10-01

Poste client sous **Windows 10 1709**, cette machine est membre du domaine. La configuration IP se fera par

l'intermédiaire d'un **serveur DHCP**.

La quantité de mémoire allouée est de **2048 Mo** et le disque virtuel de **30 Go** est partitionné avec une seule partition.

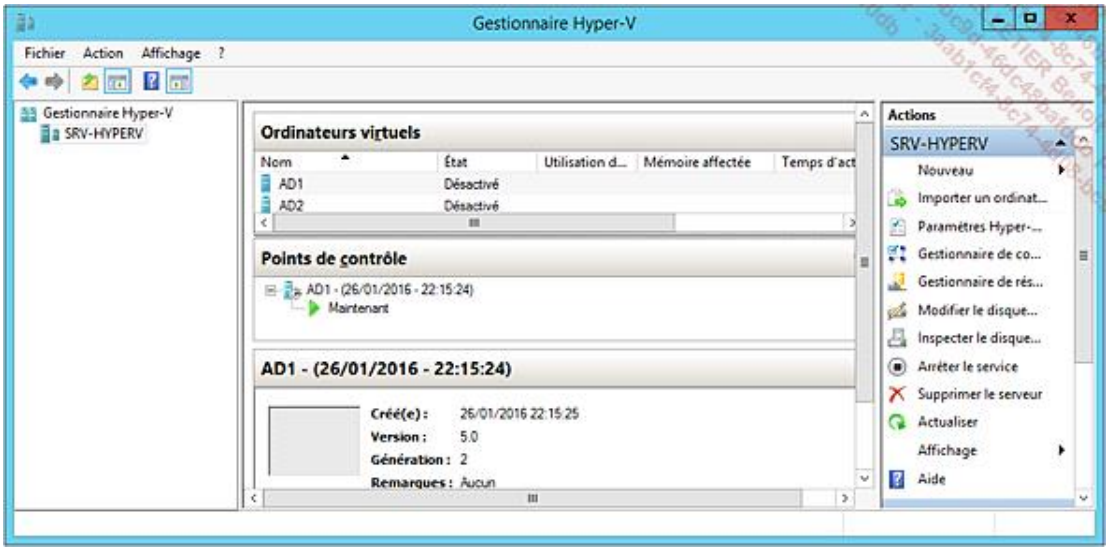
- **Nom du poste** : CL10-01
- **Mot de passe de l'administrateur local** : Pa$$w0rd

7. Les points de contrôle

Les points de contrôle (« snapshot ») permettent de sauvegarder l'état de la machine virtuelle. Il est ainsi possible, en rétablissant un point de contrôle, de retrouver très facilement un état précédent. Attention cette opération peut avoir un incident sur la production en fonction du rôle du serveur.

- Ouvrez la console **Gestionnaire Hyper-V**.
- Effectuez un clic droit sur la VM souhaitée puis sélectionnez **Point de contrôle**.

Il apparaît dans la console.



Présentation des services de l'Active Directory

Active Directory est un annuaire implémenté sur les systèmes d'exploitation depuis Windows 2000 Server. Depuis cette première version de l'annuaire, de nombreuses améliorations ont été apportées.

1. La forêt Active Directory

Une forêt est une collection d'un ou plusieurs domaines Active Directory, le premier installé étant appelé domaine racine. Son nom DNS (exemple : Formation.local) sera également donné à la forêt. Dans notre exemple, la forêt aura le nom Formation.local.

Dans une forêt, l'ensemble des domaines utilise la même partition configuration et schéma. Le système de partition est détaillé à la section Les partitions d'Active Directory.

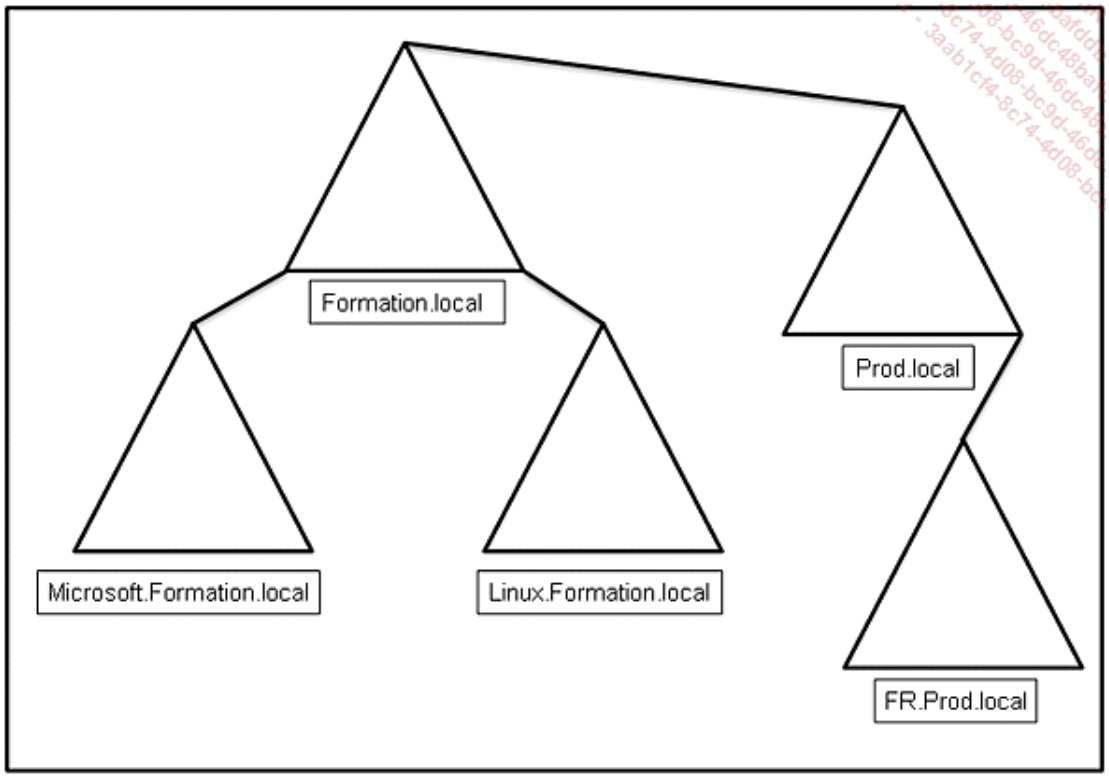
Aucune donnée (compte utilisateur, ordinateur…) n'est répliquée en dehors de la forêt, cette dernière sert donc de frontière de sécurité.

2. Le domaine et l'arborescence de domaines

Une arborescence de domaines est une suite de domaines qui partagent un espace de noms contigu. Ainsi dans l'exemple ci-après nous pouvons voir l'arborescence de domaines Formation.local. Cette dernière contient un domaine enfant nommé Microsoft.Formation.local. Le nom Formation.local est bien identique aux deux domaines.

La relation d'approbation entre **les domaines d'une même arborescence** est de type parent/enfant. Lors de l'ajout d'un domaine enfant, une relation d'approbation de type bidirectionnelle et transitive est créée automatiquement.

Si l'espace de noms est différent, nous parlerons dans ce cas d'une nouvelle arborescence. Les domaines Formation.local et Prod.local sont deux arborescences différentes dans la même forêt.



Le domaine représente une limite de sécurité où les utilisateurs sont définis.

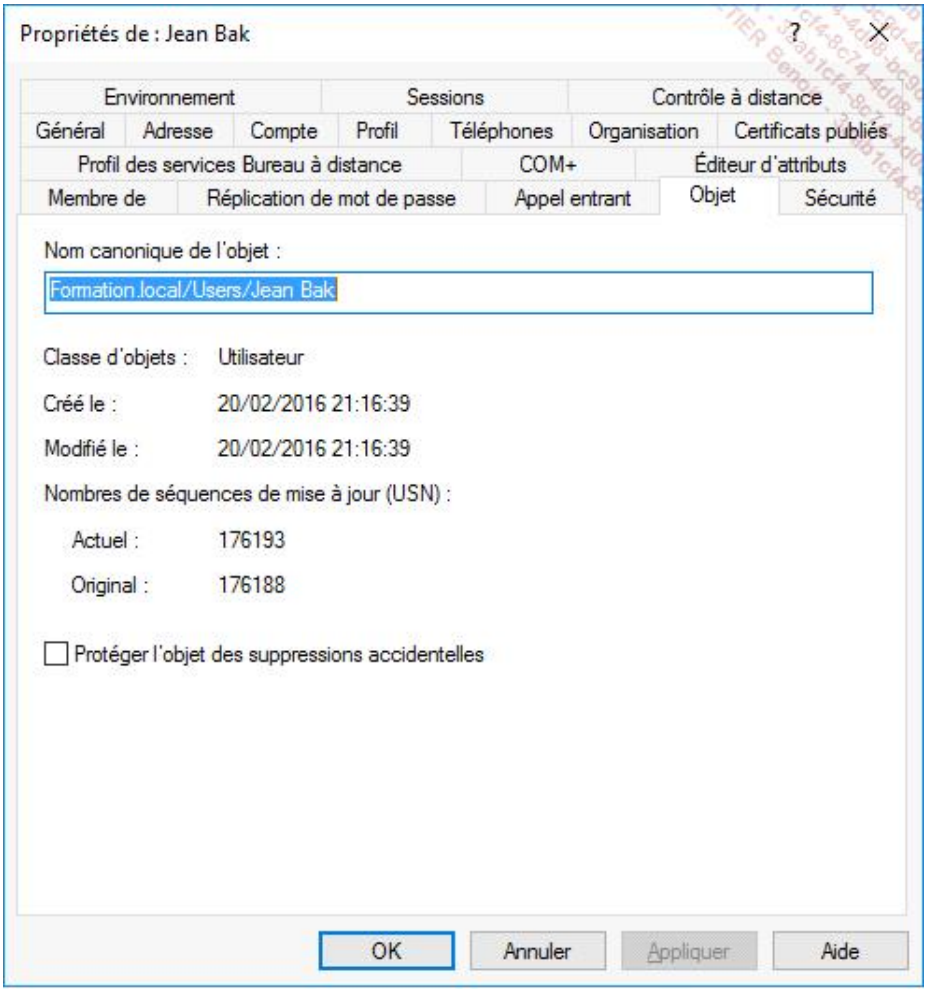
Un domaine contient au moins un contrôleur de domaine. Néanmoins il est recommandé d'en avoir deux afin d'assurer l'authentification en cas de maintenance ou de crash d'un des serveurs d'annuaire. Si plus aucun serveur n'est en ligne, l'authentification ne pourra plus être assurée, ce qui va impliquer une perte de production pour l'ensemble des utilisateurs.

Un serveur ayant le rôle de contrôleur de domaine a la responsabilité de l'authentification des comptes utilisateurs et ordinateurs.

3. L'unité d'organisation

Une **unité d'organisation** (**OU**, *Organizational Unit*) est un objet de type conteneur. Il permet d'effectuer une hiérarchisation dans l'annuaire Active Directory. Les objets (utilisateurs, ordinateurs) sont ainsi regroupés pour l'application d'une GPO (*Group Policy Object* - stratégie de groupe) ou pour faciliter l'administration. Il est possible également de déléguer l'administration des objets présents dans ce conteneur. Cette dernière action permet de donner à un utilisateur la possibilité d'effectuer une action (réinitialiser le mot de passe de l'utilisateur, ajouter des objets,…) sans nécessiter de droits d'administrateur du domaine.

Depuis Windows Server 2008, il est possible de se protéger contre la suppression accidentelle d'une unité d'organisation. Par défaut lors de la création d'une OU, cette protection est activée. Il faudra décocher la case **Protéger l'objet des suppressions accidentelles** dans l'onglet **Objet** des propriétés pour pouvoir supprimer une OU.



4. Les objets

Il est possible de trouver différents types d'objets Active Directory :

- **Utilisateur** : permet d'authentifier les utilisateurs physiques qui ouvrent une session sur le domaine. Des droits et permissions sont associés au compte afin de permettre l'accès à une ressource (dossier partagé, boîte aux lettres mail, imprimante…).
- **Groupe** : permet de rassembler différents objets (utilisateurs ou ordinateurs) qui doivent avoir un accès identique (lecture, modification…) sur une ressource (dossier partagé, etc.). L'administration des permissions est plus aisée en utilisant des groupes.
- **Ordinateur** : permet d'authentifier les postes physiques ou virtuels connectés au domaine. Il est possible de positionner le compte ordinateur dans une ACL, cela permettra l'accès à une ressource. Si l'authentification ne peut être effectuée, l'ouverture de session sur le domaine est impossible.
- **Unité d'organisation** : conteneur qui permet l'organisation des objets de façon hiérarchique. Il est possible de lui appliquer une ou plusieurs stratégies de groupe. De plus, cet objet offre la possibilité de mettre en place une délégation.
- **Imprimante** : une imprimante partagée peut être publiée dans Active Directory. Cette action simplifie les étapes de recherche et d'installation pour un utilisateur.

5. Les partitions d'Active Directory

Active Directory utilise quatre types de partitions d'annuaire, toutes partagées par les contrôleurs de domaine. La création est effectuée lors de l'étape de promotion. Les partitions de configuration et de schéma sont partagées par l'ensemble des contrôleurs de domaine.

- **Partition de domaine** : contient les informations sur les objets qui ont été créés dans un domaine (attributs de compte utilisateur et d'ordinateur…). Ces informations sont présentes uniquement sur l'ensemble des serveurs d'annuaire du domaine concerné.
- **Partition de configuration** : permet de décrire la topologie de l'annuaire (liste complète des domaines, arborescences et forêt). L'ensemble des contrôleurs de domaine de la forêt se partagent les informations contenues dans cette partition.
- **Partition de schéma** : contient tous les attributs et classes de tous les objets qui peuvent être créés. Lors de la création d'un compte utilisateur, l'objet et ses propriétés sont dupliqués depuis le schéma. Lors de l'ajout d'un nouveau service (Exchange, sccm,…), il est nécessaire de procéder à la mise à jour de cette partition. Il est intéressant de noter qu'un seul serveur dans la forêt contient le droit d'écriture sur le schéma, les autres étant uniquement en lecture seule.
- **Partition DNS** : contient la ou les bases de données DNS. Les informations de la base, les enregistrements y sont stockés.

Ces partitions sont stockées dans la base de données Active Directory, son emplacement physique sur le serveur d'annuaire est le répertoire **%sysemroot%\NTDS**.

6. Les maîtres d'opération FSMO

Cinq rôles **FSMO** (*Flexible Single Master Operation*) existent dans une forêt Active Directory. Ils possèdent chacun une fonction au sein de l'annuaire et la perte de certain de ces rôles peut être problématique.

Deux rôles sont présents uniquement sur un des contrôleurs de domaine de la forêt, ils sont généralement présents au niveau du domaine racine (premier domaine de la forêt).

- **Rôle maître de schéma** : comme nous l'avons vu, le schéma est en lecture seule sur les contrôleurs de domaine. Néanmoins il est parfois nécessaire de procéder à sa mise à jour. Pour cela, un contrôleur de domaine dans la forêt dispose du rôle Maître de schéma.
- **Maître de dénomination de domaine** : lors d'une opération au niveau du domaine (ajout/suppression,…), le serveur qui possède ce rôle permet d'assurer une cohérence des noms de domaine.

Les trois autres rôles sont présents sur chaque domaine de la forêt.

- **Maître RID** : ce rôle est donné à un des contrôleurs de domaine. Son rôle est l'attribution de **blocs d'identificateur relatifs (RID)** aux différents contrôleurs de domaine de son domaine qui en font la demande. Le RID est utilisé lors de la création d'un objet pour créer le **SID (identifiant de sécurité)**. Ce dernier est construit en associant le RID à l'identificateur de domaine (SID du domaine identique à l'ensemble des objets).
- **Maître infrastructure** : le serveur possédant ce rôle est responsable de la surveillance des objets des autres domaines de la forêt. Lors de la présence dans une ACL d'un objet étranger à son domaine, il a pour fonction la prise en charge de la vérification de l'état de ces objets (désactivé, renommé, supprimé…).
- **Maître émulateur PDC** : ce rôle a une importance capitale dans une forêt Active Directory. En effet il a pour rôle de synchroniser son horloge avec un serveur de temps. Par la suite les différents contrôleurs de domaine viendront effectuer la même opération en le prenant comme maître de temps. Ainsi l'ensemble des contrôleurs de domaine auront une horloge synchronisée. La gestion du temps est également importante pour les postes et serveurs. Ces derniers sont également synchronisés à l'aide des contrôleurs de domaine.

7. Le catalogue global

Un serveur catalogue global est un contrôleur de domaine qui possède une copie des attributs de tous les objets Active Directory de son domaine. Par défaut seuls certains attributs sont répliqués, il est néanmoins possible d'inclure d'autres attributs en fonction de votre besoin.

La console **Schéma Active Directory** permet de sélectionner les attributs à répliquer.

Lors de l'authentification de l'utilisateur, le serveur catalogue global est interrogé, ceci afin de récupérer la liste des groupes universels dont l'utilisateur est membre.

8. Les sites AD

Afin de réduire l'utilisation des lignes reliant les différentes entités physiques (siège et sites distants), les domaines sont découpés en sites AD. Ces derniers représentent généralement la topologie physique de l'entreprise. Dans un site AD, la connectivité réseau est considérée comme très bonne. On parlera de réplication intrasite (réplication entre les contrôleurs de domaine du site).

En créant ce découpage, avec les sites AD, l'administration des réplications entre les sites est facilitée. Ainsi on économise la bande passante des liaisons WAN. La réplication sera de type intersites.

Lors d'une ouverture de session, le contrôleur de domaine du site AD sur lequel l'utilisateur est présent sera préféré. Néanmoins dans le cas où aucun serveur d'authentification n'est présent, le contrôleur de domaines d'un autre site sera utilisé.

9. La réplication intrasite et la réplication intersites

La réplication permet de s'assurer qu'une modification effectuée sur un contrôleur de domaine est transmise à ses

paires. Cette opération s'effectue à l'aide d'objets de type « connexion ». Elles sont de type unidirectionnels (réplication entrante uniquement).

Ces chemins de réplication (objet connexion), vont permettre la création de la topologie de réplication. La vérification de la cohérence des données (**KCC**, *Knowledge Consistency Checker*) pourra être également assurée.

La topologie permet également d'avoir une continuité au niveau de la réplication et ce même en cas de défaillance d'un contrôleur de domaine. Il est donc **très important** de ne pas modifier les liens de connexion. L'ISTG effectue la création de la topologie et l'adapte en fonction des pannes des serveurs d'annuaire ou coupure réseau. Si les liens ont été modifiés manuellement, cette opération de mise à jour de la topologie ne s'effectue plus. Il est donc recommandé de laisser travailler l'ISTG sans intervenir.

Comme nous l'avons vu, il existe deux types de réplications :

- Intrasite
- intersites

La réplication intrasite permet une réplication des modifications pour les contrôleurs de domaine d'un même site.

À la suite d'une modification d'une des partitions Active Directory, une notification est effectuée au bout de 15 secondes par le contrôleur de domaine à son premier partenaire. Cette opération de notification a pour but de donner l'information du changement.

Trois secondes plus tard, une notification est envoyée aux autres contrôleurs de domaine. Ces délais dans les notifications permettent d'assurer une réduction du trafic réseau.

Suite à la notification, le serveur partenaire demande la modification. L'agent de réplication d'annuaire (**DRA**, *Directory Replication Agent*) peut par la suite opérer le transfert.

Dans le cas où aucune modification n'est effectuée, la méthode de scrutation est utilisée.

Cette méthode consiste à interroger un serveur afin de connaître une éventuelle modification sur une des partitions de l'Active Directory. L'intervalle de scrutation pour une réplication intrasite est d'une heure. Cette valeur est celle par défaut.

La réplication de type intersites consiste à effectuer des réplications sur des serveurs d'annuaire présent dans des sites AD différents.

L'**ISTG** (*Intersite Topology Generator*, générateur de topologie intersites) effectue la création d'objets de connexion entre les serveurs de chaque site. Cela permet la réplication intersites.

Pour les raisons évoquées plus haut, il est préférable de ne pas modifier ses liens de connexion.

Dans chaque site, un contrôleur de domaine est sélectionné afin d'obtenir le rôle de tête de pont. Ce dernier a la responsabilité de répliquer ou récupérer d'éventuelles modifications d'un autre serveur tête de pont. Par la suite une réplication de type intrasite s'opère. Cette élection est effectuée automatiquement. Pour les mêmes raisons que les liens de connexion, il est préférable de ne pas faire d'élection manuelle.

Pour effectuer la réplication intersites, deux protocoles sont utilisés :

- **IP** : utilisé pour toutes les réplications intrasites et intersites. Ce protocole est très souvent utilisé.
- **SMTP** : utilisé principalement en cas de connexions non fiables. Une CA (autorité de certification) est nécessaire, ce qui alourdit l'administration. Ce protocole est très peu utilisé pour la réplication.

10. Niveau fonctionnel du domaine et de la forêt

Un niveau fonctionnel permet l'activation d'une ou plusieurs fonctionnalités pour un domaine ou une forêt. Plusieurs niveaux sont disponibles, néanmoins toute modification de niveau est irréversible (il est par la suite impossible de descendre d'un niveau).

Ceci a un impact sur le domaine et/ou la forêt mais principalement sur les contrôleurs de domaine. Il est nécessaire d'avoir au minimum tous les contrôleurs de domaine qui exécutent le système d'exploitation correspondant à celui du niveau fonctionnel choisi. Si le niveau choisi est Windows Server 2008, les contrôleurs de domaine doivent au minimum exécuter Windows Server 2008.

Niveau fonctionnel Windows Server 2008

Le niveau fonctionnel Windows Server 2008 offre les fonctionnalités suivantes :

- Activation de la réplication du système de fichiers **DFS** (*Distributed File System*) pour le dossier **SYSVOL**.
- Protocole AES (*Advanced Encryption Services*) 128 et 256 bits pour l'authentification Kerberos.
- Mise en place de la stratégie de mot de passe affinée.

Au niveau de la forêt, aucune nouvelle fonctionnalité n'est apportée.

Niveau fonctionnel Windows Server 2008 R2

Le niveau fonctionnel permet l'utilisation de la **corbeille AD**. Cette dernière assure la restauration d'un objet Active Directory (unité d'organisation, compte utilisateur...). L'ensemble des propriétés sont restaurées.

Niveau fonctionnel Windows Server 2012

Une nouveauté est apportée avec le niveau fonctionnel du domaine, avec le protocole Kerberos Armoring. Aucune nouveauté n'est apportée avec le niveau fonctionnel de la forêt.

Niveau fonctionnel Windows Server 2012 R2

Aucune nouveauté apportée par le niveau fonctionnel de la forêt. Concernant celui du domaine la sélection du niveau fonctionnel 2012 R2 permet d'obtenir les fonctionnalités suivantes :

- **Silos de stratégies d'authentification** : cette fonctionnalité permet l'application de stratégie d'authentification pour certains comptes (utilisateurs, ordinateurs, servi-ces).
- **Stratégies d'authentification** : appliquées aux comptes utilisateur, elles permettent d'indiquer sur quelle machine un utilisateur peut ouvrir une session. Cette fonctionnalité utilise un contrôle d'accès basé sur des conditions.

Niveau fonctionnel Windows Server 2016

Aucune nouveauté offerte par le niveau fonctionnel.

Promotion d'un contrôleur de domaine

Un contrôleur de domaine est un serveur dont la fonction principale est l'authentification des utilisateurs et ordinateurs. Il a également la charge de permettre l'accès aux ressources partagées (boîtes aux lettres, dossiers partagés, imprimantes…).

1. Prérequis nécessaires à la promotion d'un serveur

La promotion d'un serveur en contrôleur de domaine nécessite certains prérequis. Si ces derniers ne sont pas respectés, l'opération est stoppée.

- **Système de fichiers NTFS** : les volumes et les partitions doivent être formatés avec un système de fichiers NTFS.
- **Nom du poste** : un nom de 15 caractères maximum est recommandé de plus il est préférable de ne pas utiliser de caractères spéciaux (#, é, è...), les chiffres et les caractères minuscules et majuscules peuvent eux être utilisés sans risques.
- **L'interface réseau** : elle doit être configurée avec une configuration IPv4/IPv6 correcte. L'adressage statique est recommandé pour tous les serveurs et si besoin, une exclusion doit être effectuée dans le DHCP.
- **Nom de domaine** : le nom de domaine utilisé doit être sous la forme d'un nom DNS (domaine.extension). Il est souhaitable d'utiliser des extensions qui ne soient pas utilisées sur Internet (.msft, …).
- **Serveur DNS** : un serveur DNS est nécessaire pour le fonctionnement de l'Active Directory. Néanmoins, si aucun serveur DNS n'est présent, l'installation de ce dernier peut s'effectuer pendant la promotion du serveur. Dans le cas contraire, vérifier la configuration IP afin d'utiliser le serveur DNS de production.

2. Installation d'un nouveau domaine dans une nouvelle forêt

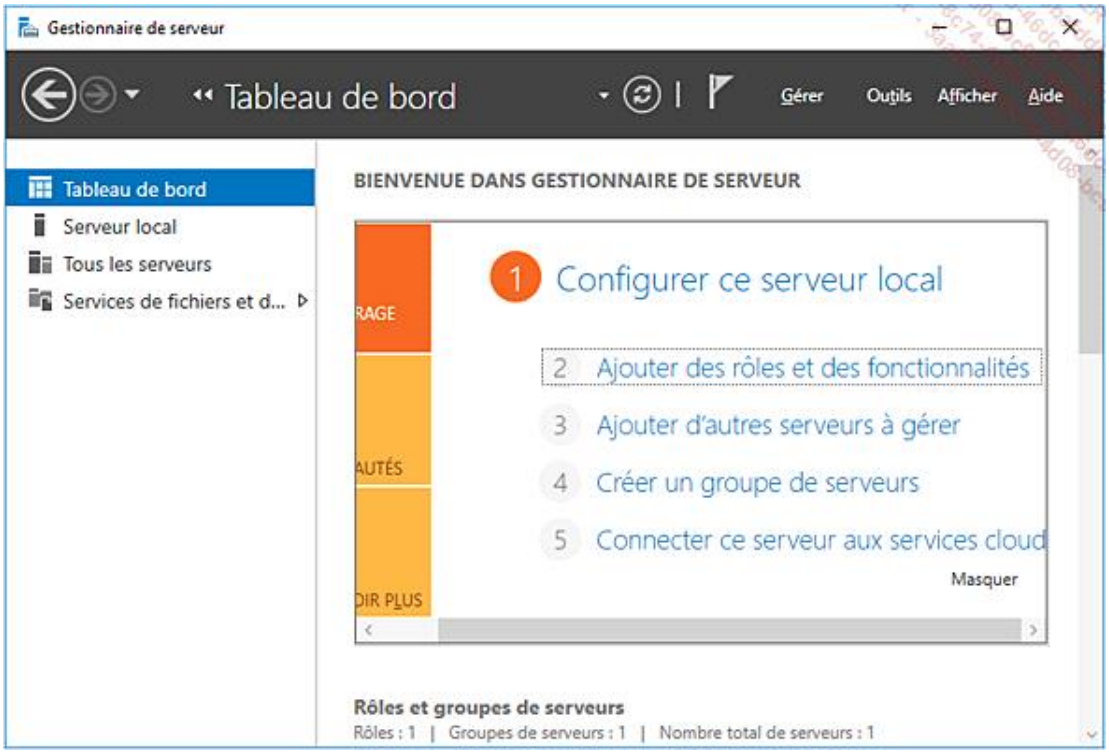
Les services AD sont considérés comme des rôles et sont présents dans la liste des rôles.

Démarrez la machine virtuelle **AD1**.

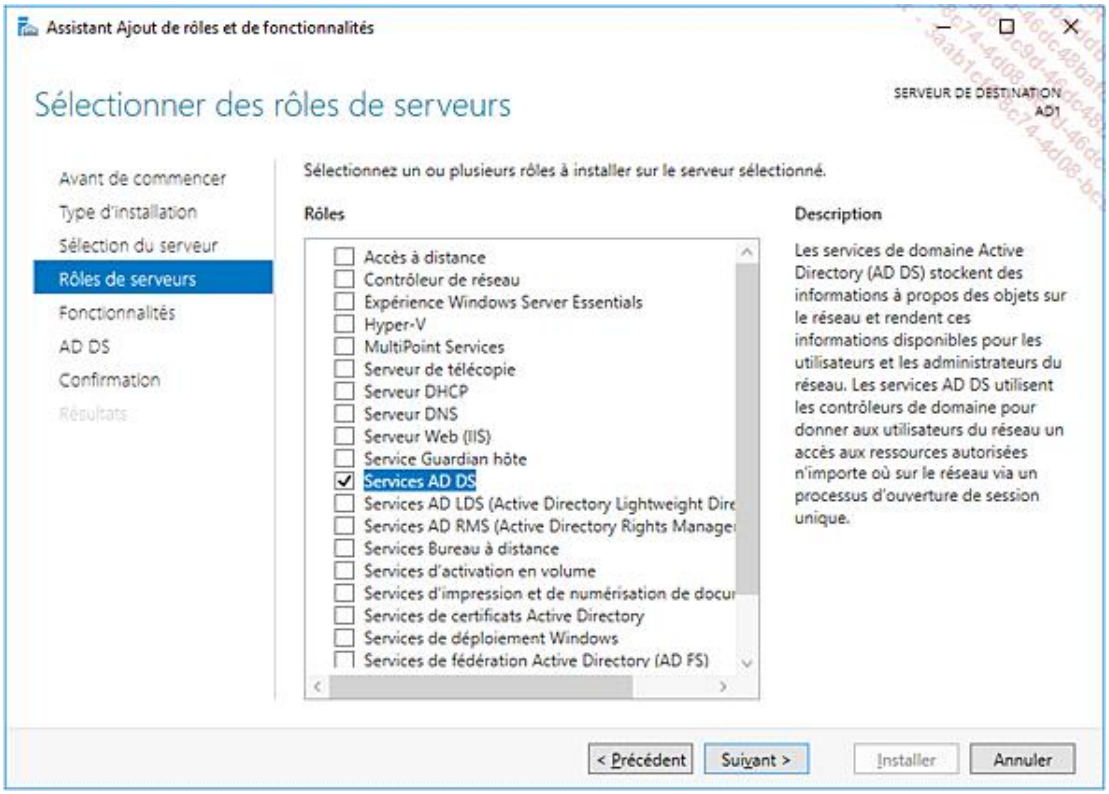


La configuration ayant déjà été faite, il suffit maintenant d'installer Active Directory.

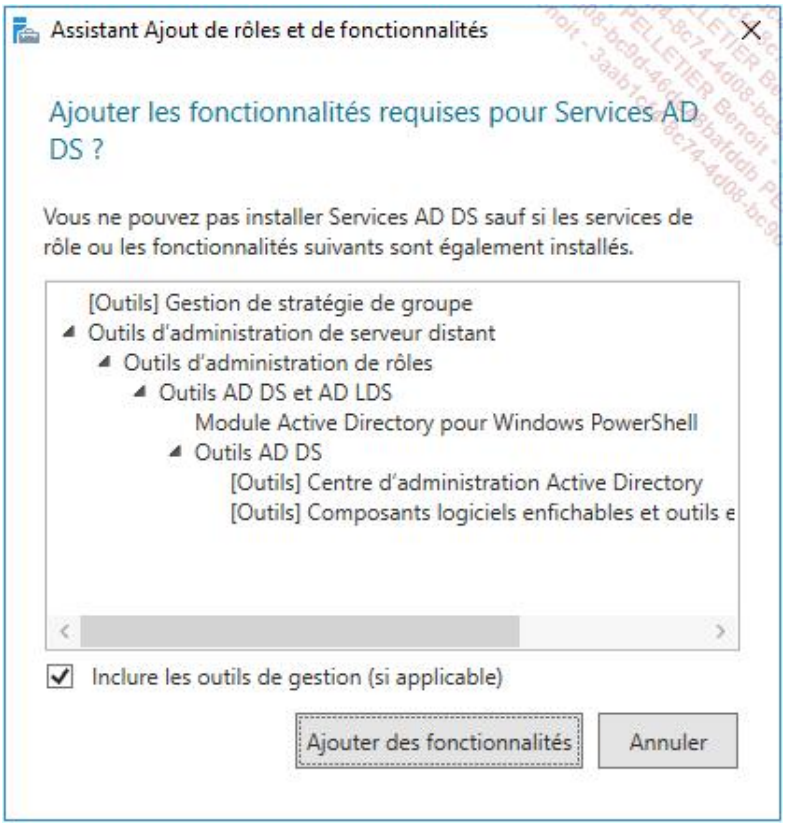
Dans la console **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et fonctionnalités**.



- L'assistant se lance. Cliquez sur **Suivant**.
- Dans les fenêtres **Type d'installation** et **Sélection du serveur**, laissez le paramètre par défaut puis cliquez sur **Suivant**.
- Activez la case à cocher **Services AD DS** pour effectuer l'installation.

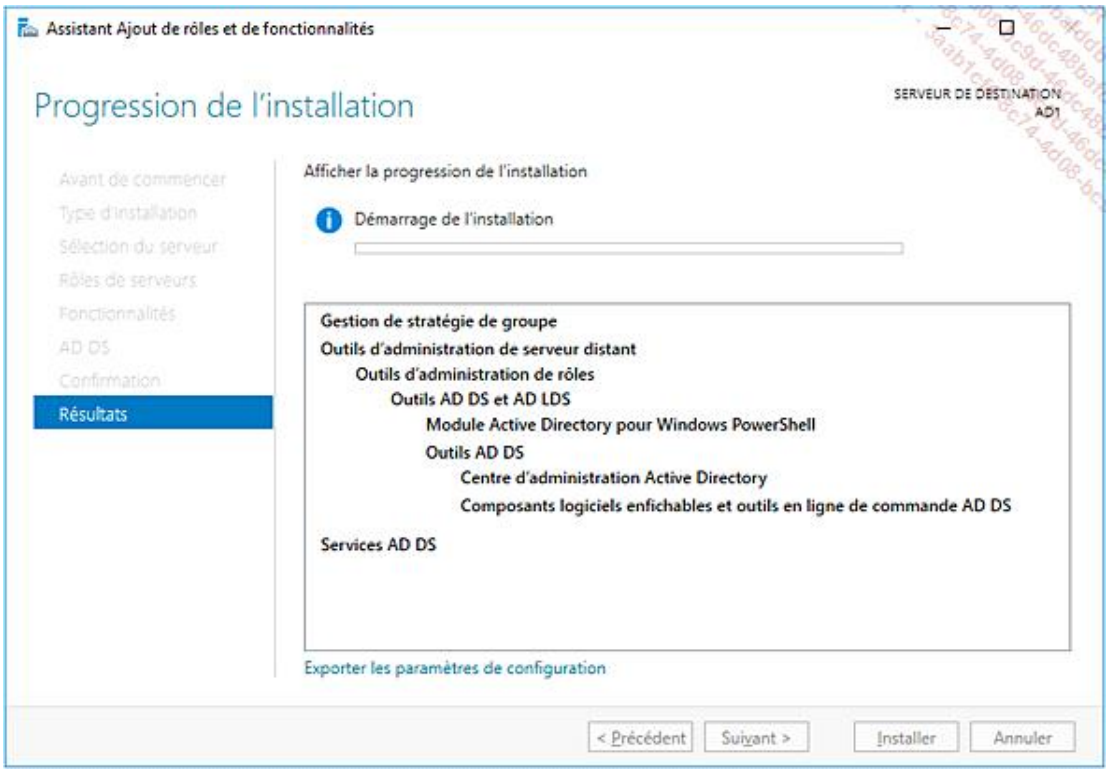


- Cliquez sur **Ajouter des fonctionnalités** dans la fenêtre qui s'affiche, afin d'installer les fonctionnalités nécessaires à Active Directory.



- Cliquez sur **Suivant** dans la fenêtre **Sélectionner des fonctionnalités** puis cliquez sur **Suivant**.
- Cliquez sur **Installer** pour lancer l'installation.

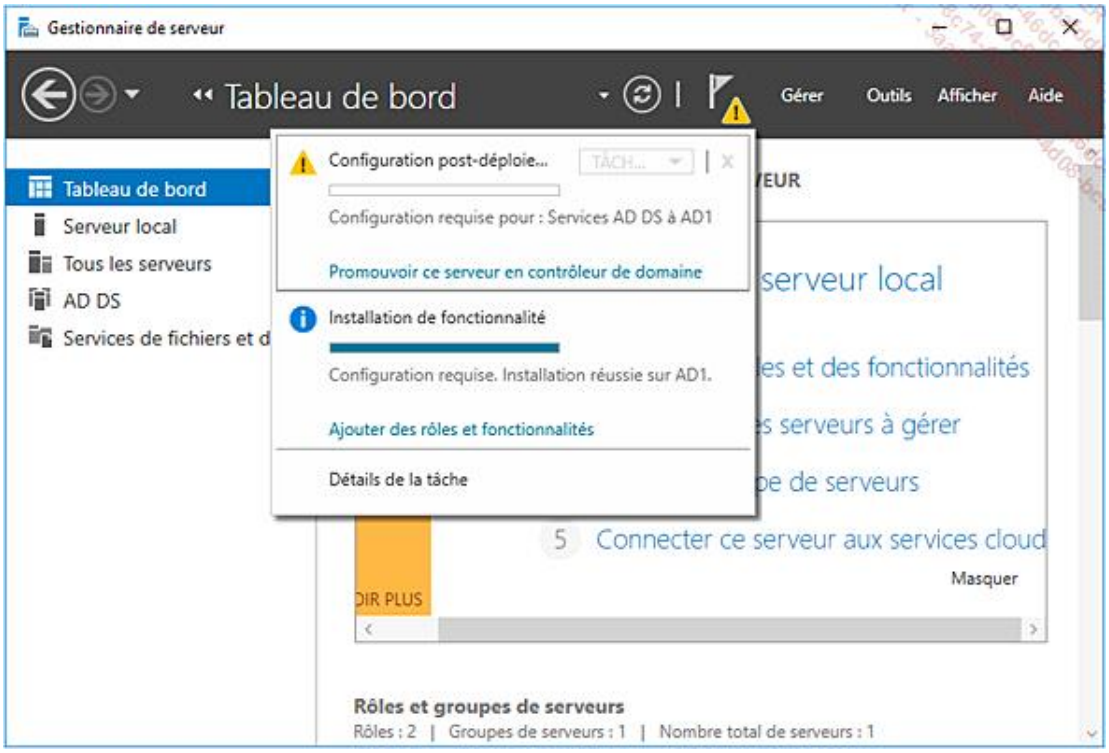
L'installation est en cours…



- Une fois l'installation terminée, cliquez sur **Fermer**.

Dans la console **Gestionnaire de serveur**, cliquez sur le drapeau contenant le point d'exclamation.

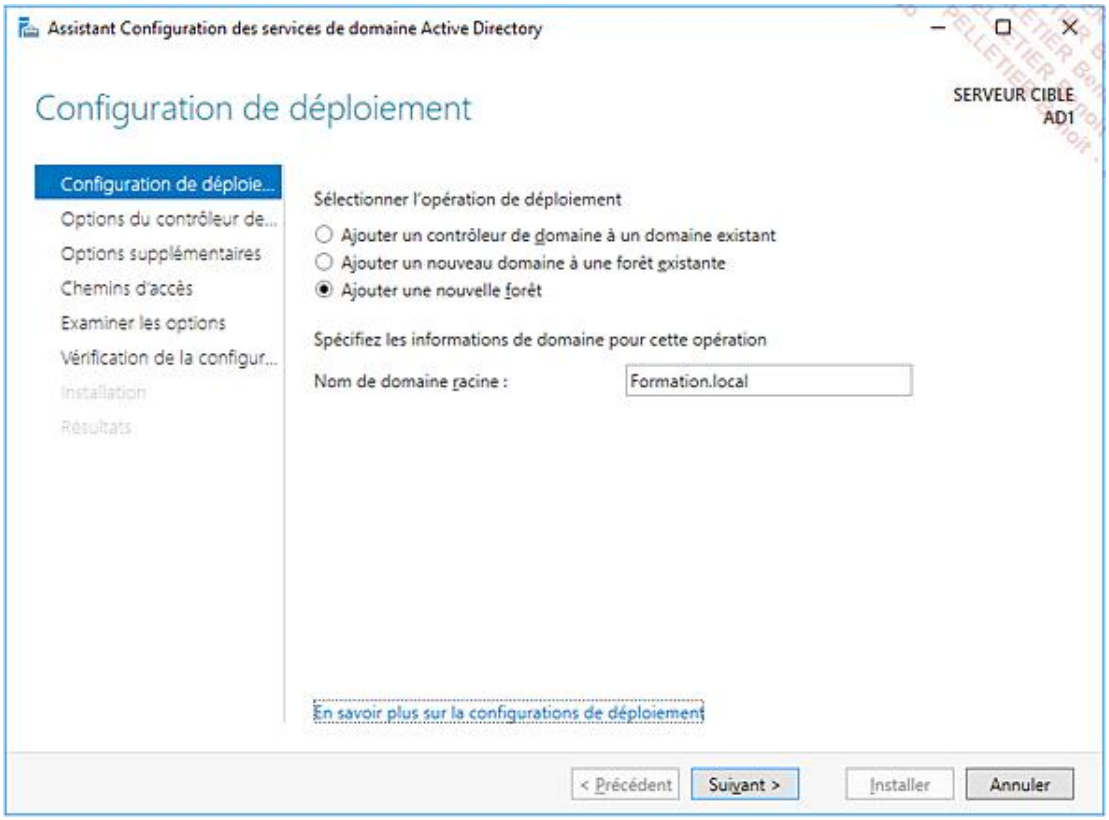
Cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.



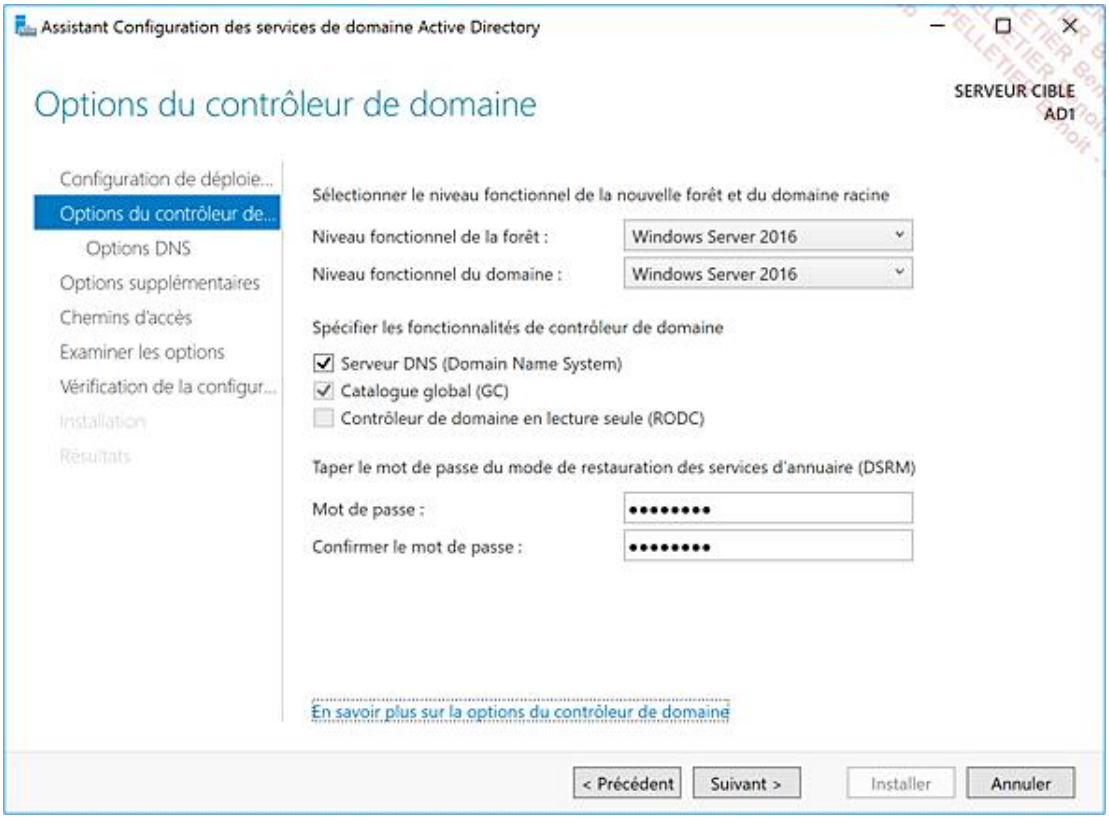
Trois options sont possibles :

- **Ajouter un contrôleur de domaine à un domaine existant** : un contrôleur de domaine est ajouté au domaine Active Directory afin d'assurer une tolérance de panne. Le deuxième serveur ajouté peut également assurer l'authentification des utilisateurs et postes de travail. Il est recommandé d'avoir deux contrôleurs de domaine dans un domaine dont un physique.
- **Ajouter un nouveau domaine à une forêt existante** : cette option permet d'effectuer la création d'une nouvelle arborescence ou l'ajout d'un domaine enfant.
- **Ajouter une nouvelle forêt** : une nouvelle forêt est créée et le domaine racine donne son nom à la forêt.

Cliquez sur **Ajouter une nouvelle forêt** et saisissez **Formation.local** dans le champ **Ajouter une nouvelle forêt**.



- Cliquez sur **Suivant** pour valider votre choix.
- Laissez la valeur par défaut dans les listes déroulantes **Niveau fonctionnel de la forêt** et **Niveau fonctionnel du domaine**. Laissez cochée la case **Serveur DNS** afin que le rôle soit installé et configuré.
- Saisissez **Pa$$w0rd** dans le champ **Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)**.



- Dans la fenêtre **Options DNS**, cliquez sur **Suivant**.
- Après quelques secondes, le nom de domaine NetBIOS apparaît. Vérifiez que le nom est FORMATION.
- Cliquez sur **Suivant** pour valider la fenêtre.
- Laissez les **Chemins d'accès** par défaut et cliquez sur **Suivant**.
- Cliquez sur **Suivant** après avoir vérifié les paramètres dans la fenêtre **Examiner les options**.
- Cliquez sur **Installer** pour lancer l'installation de l'Active Directory et la promotion du serveur. À la fin de l'installation, le serveur redémarre.
- Ouvrez la session en tant qu'administrateur.

Le mot de passe du compte administrateur du domaine est l'ancien mot de passe du compte administrateur local. Un contrôleur de domaine n'a pas de base SAM (*Security Account Manager*), donc pas de compte ou groupe locaux.

- Affichez le menu **Démarrer**, puis accédez aux **Outils d'administration**.

Suite à l'installation, de nouvelles consoles ont été ajoutées. Elles permettent l'administration de l'annuaire.

- **Utilisateurs et Ordinateurs Active Directory** : administration des différents objets de l'annuaire (OU, groupe, utilisateur…).
- **Sites et Services Active Directory** : administration des sites AD et de la réplication.
- **Domaine et approbation Active Directory** : création de relations d'approbation entre domaines ou entre forêts.
- **Gestion des stratégies de groupe** : création, administration et maintenance des différentes stratégies de groupe.
- **Modification ADSI** : modification des attributs LDAP.

Le serveur qui vient d'être installé peut effectuer des modifications sur la base de données AD et donc répliquer ces modifications. Cette réplication peut poser problème en cas d'altération de la base de données ou en cas de mauvaise modification.

Pour ces raisons, il est utile dans certains cas d'installer un **contrôleur de domaine en lecture seule (RODC)**.

3. Installation d'un serveur en mode RODC

Apparue avec Windows Server 2008, la fonctionnalité de contrôleur de domaine en lecture seule consiste à installer un contrôleur de domaine qui possède uniquement des droits de lecture sur la base de données AD. Il sera impossible d'effectuer des modifications : les différentes opérations (ajout/modification/suppression) sont apportées sur un contrôleur de domaine en lecture/écriture et par réplication au RODC.

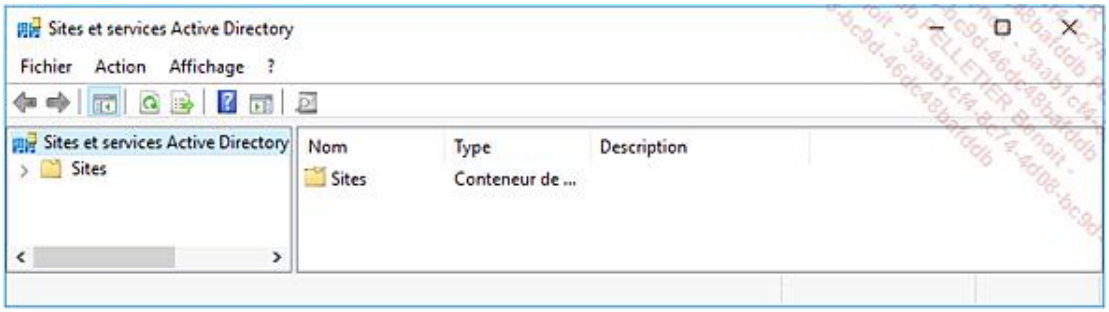
Il est également possible de se connecter en local à un RODC. Une délégation peut donc être donnée à un autre utilisateur pour l'administration du serveur (mise à jour Windows Update…) sans que celui-ci ne soit **administrateur du domaine**.

Néanmoins, certains prérequis sont à respecter :

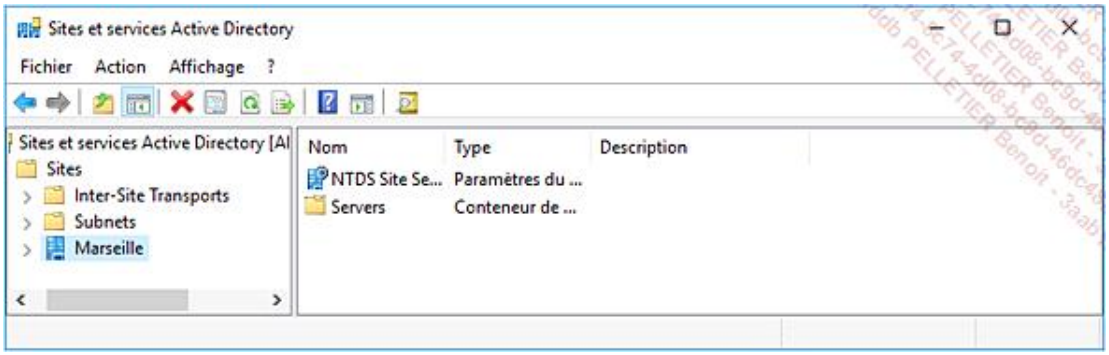
- **Niveau fonctionnel** : Windows Server 2003 ou supérieur pour la forêt et le domaine.
- **Schéma** : l'extension du schéma doit être effectuée afin d'accueillir la fonctionnalité RODC (adprep/rodcprep).
- **Contrôleur de domaine** : un contrôleur de domaine en lecture/écriture sous Windows Server 2008 ou supérieur doit être présent sur le domaine.

L'installation d'un RODC (*Read Only Domain Controller*, contrôleur de domaine en lecture seule) s'effectue souvent sur des sites distants. Nous allons donc dans un premier temps effectuer la création d'un deuxième site AD. Ce dernier contiendra uniquement le serveur RODC. Par la suite, la promotion du serveur pourra être effectuée.

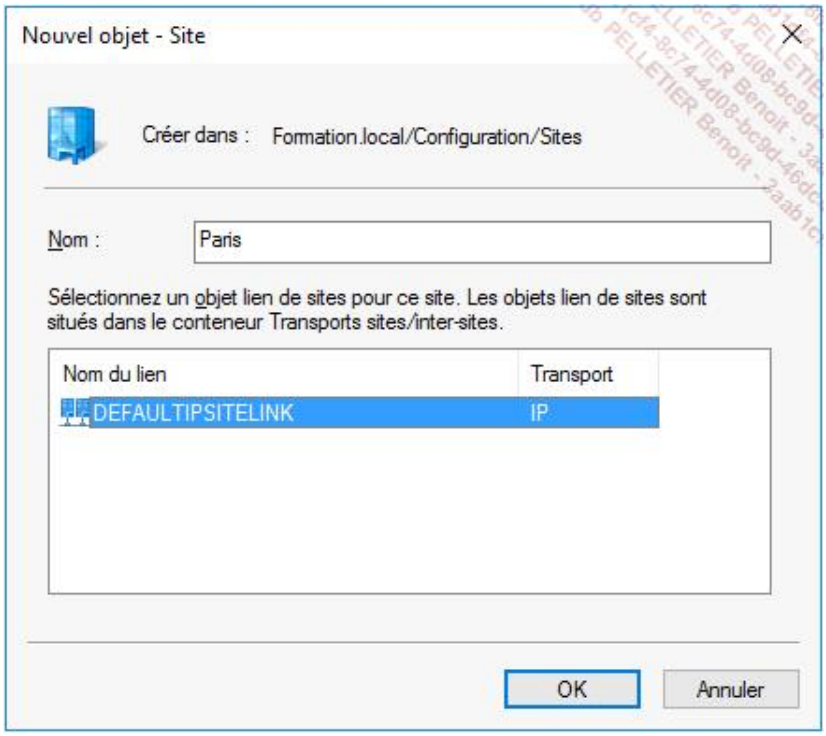
- Sur **AD1**, accédez à la console Sites et services Active Directory.



- Déroulez le dossier **Sites** afin d'afficher les sites présents dans AD.
- Effectuez un clic droit sur **Default-First-Site-Name** puis sélectionnez l'option **Renommer**.
- Remplacez le nom par défaut par **Marseille**.

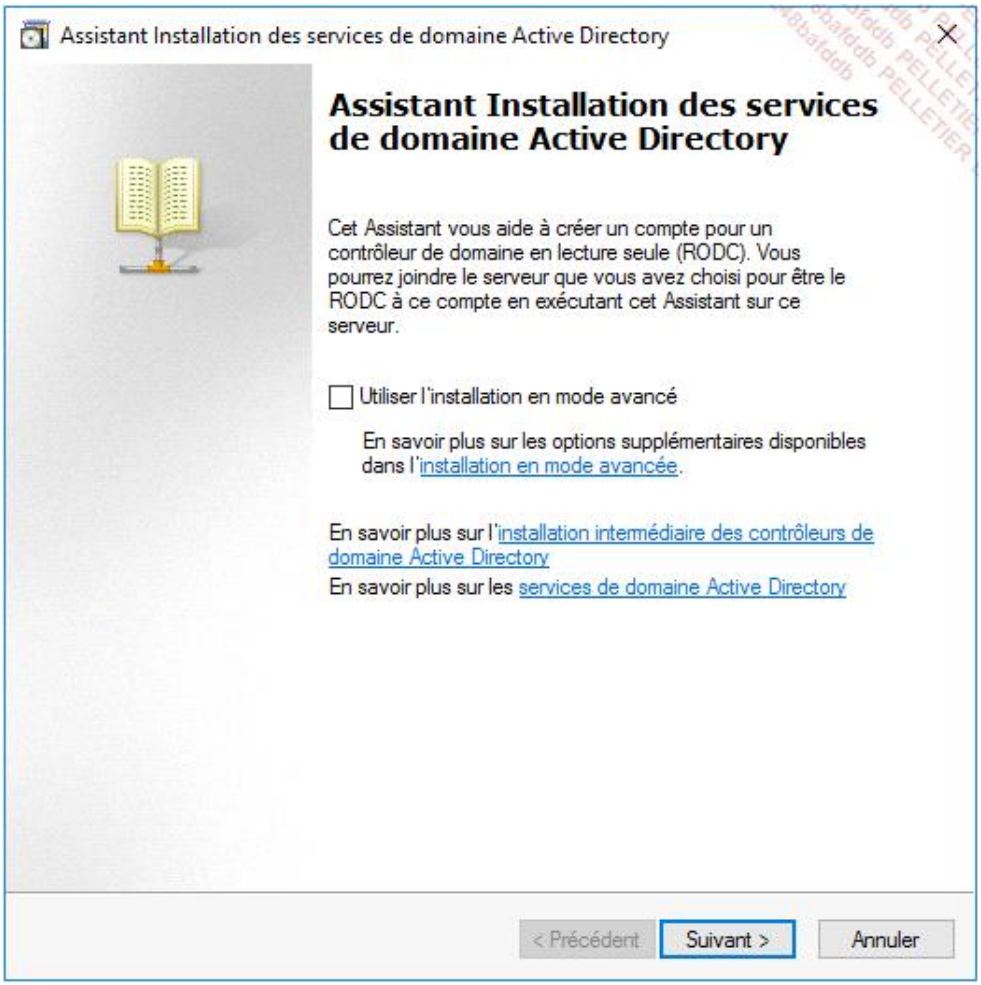


- Effectuez un clic droit sur le dossier **Sites** et sélectionnez **Nouveau Site**.
- Dans le champ **Nom**, saisissez **Paris** et sélectionnez **DEFAULTIPSITELINK**.

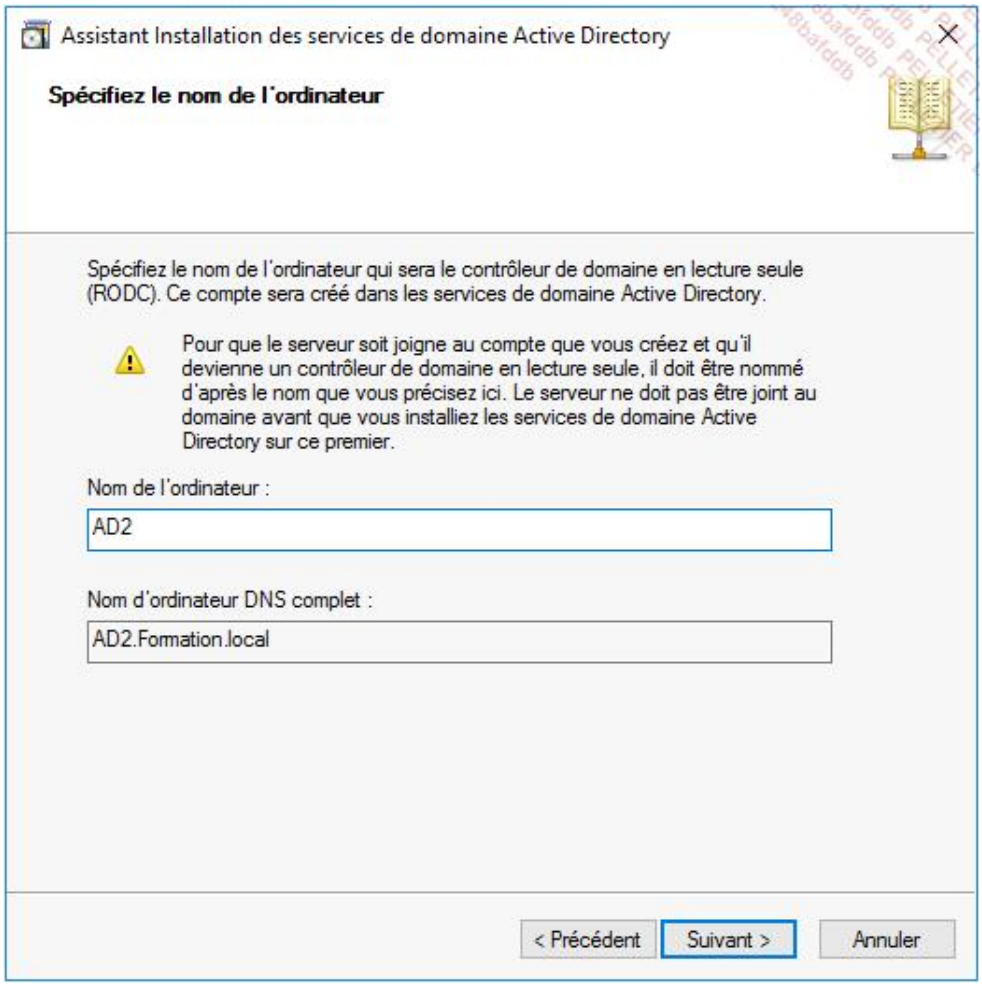


Le RODC est placé sur le site de Paris. Ce dernier doit être créé en amont de la promotion.

- Cliquez sur **OK** au message d'information.
- Depuis les outils d'administration, ouvrez la console **Utilisateurs et Ordinateurs Active Directory**.
- Effectuez un clic droit sur l'OU **Contrôleur de domaine** puis sélectionnez l'option **Créer au préalable un compte de contrôleur de domaine en lecture seule...**.
- Cliquez sur **Suivant** dans la fenêtre d'accueil de l'assistant.

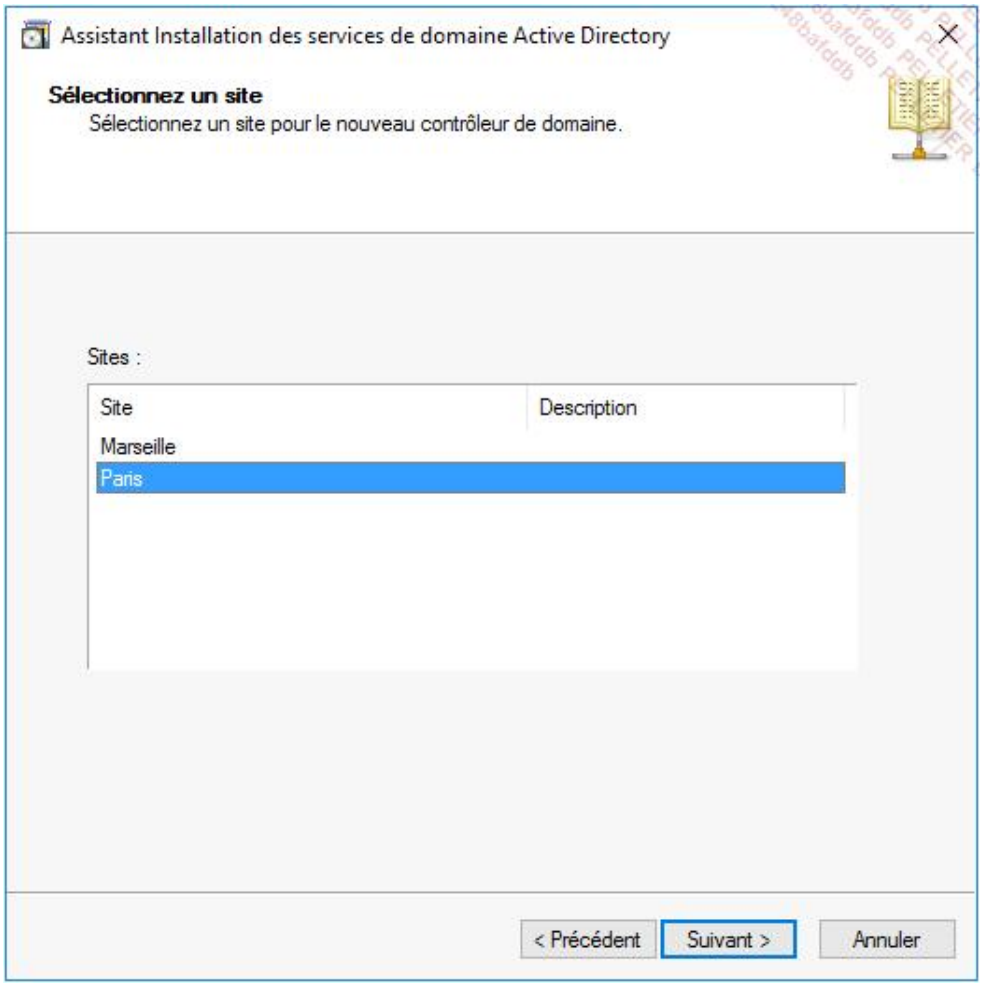


- Dans la fenêtre **Informations d'identification réseau**, laissez le choix par défaut. Le compte **Administrateur** est utilisé pour l'installation.
- Saisissez le nom du serveur (AD2) dans le champ **Nom de l'ordinateur** puis cliquez sur **Suivant**. AD2 ne doit pas être membre du domaine, et si le compte ordinateur existe, ce dernier doit être supprimé. Dans le cas contraire, un message vous avertit qu'un compte existe déjà.

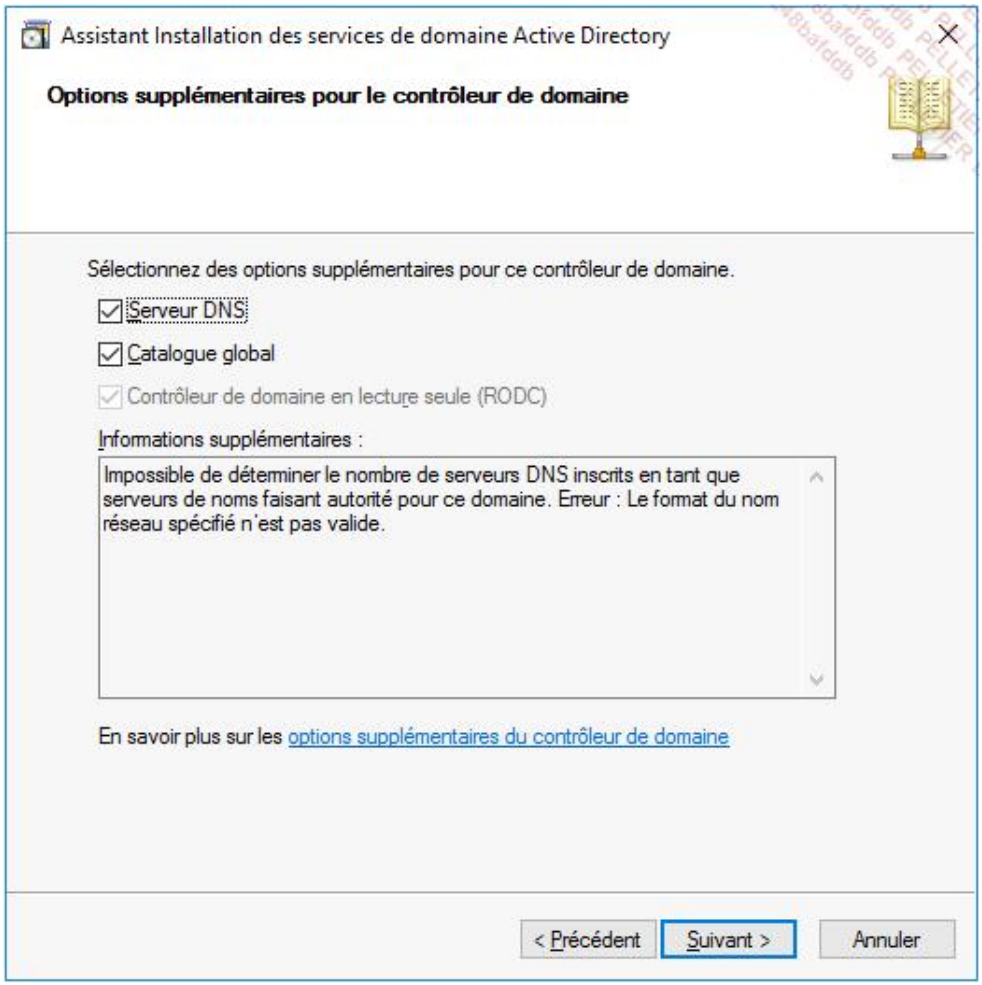


Il est très important de mettre le nom exact du futur RODC.

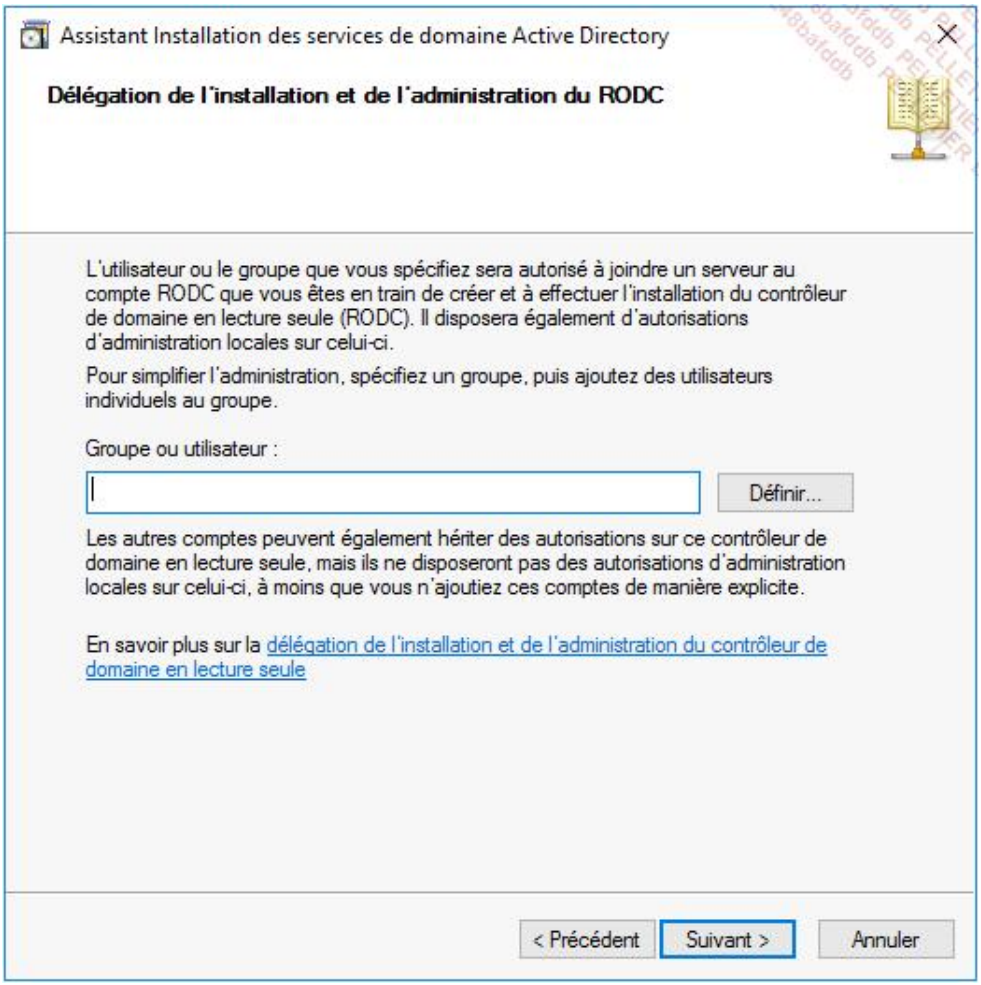
Le choix du site doit être fait, sélectionnez **Paris** et cliquez sur **Suivant**.



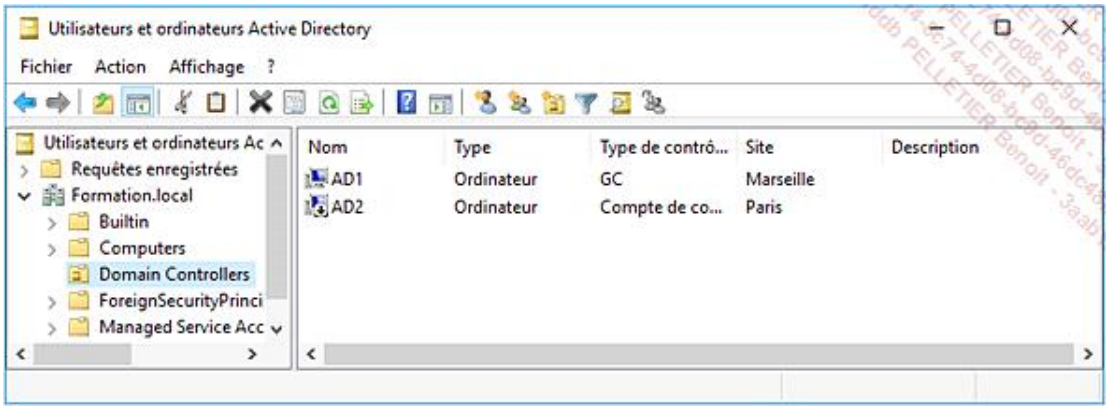
- Attendez la fin de l'analyse de la configuration DNS. À l'aide de la fenêtre suivante, il est possible d'effectuer plusieurs choix :
  - **Serveur DNS** : installation d'un serveur DNS en mode lecture seule.
  - **Catalogue global** : le serveur installé aura le rôle de catalogue global.
  - **Contrôleur de domaine en lecture seule (RODC)** : le contrôleur de domaine installé est un RODC et non un serveur avec des droits de lecture/écriture dans Active Directory.



Il n'est pas envisagé de déléguer l'administration du serveur sur le site de Paris, l'installation est donc faite avec le compte **administrateur du domaine**. Cliquez sur **Suivant** dans la fenêtre **Délégation de l'installation et de l'administration du RODC**.



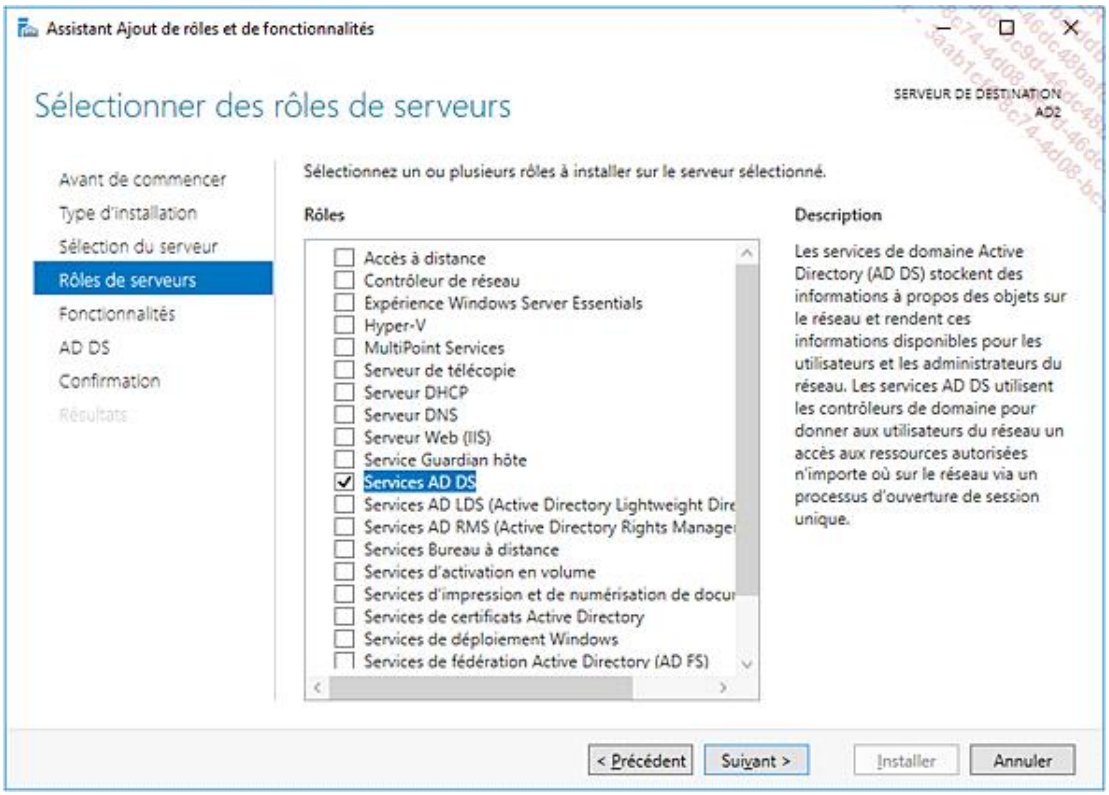
- Dans la fenêtre de résumé, cliquez sur **Suivant** puis sur **Terminer**. Le compte de la machine apparaît avec l'état désactivé.



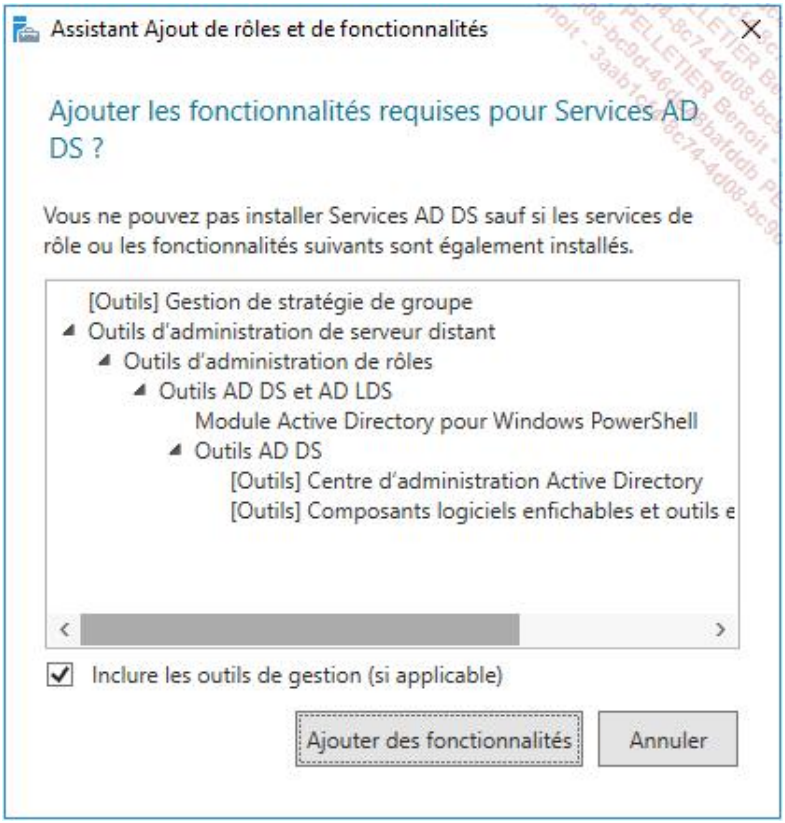
Le compte ayant été créé au préalable, la promotion peut maintenant être effectuée. Cette étape peut évidemment être évitée, dans ce cas le compte ordinateur du RODC est créé lors de la promotion. Néanmoins, dans ce cas précis, la mise en place d'une délégation est impossible, il sera nécessaire de le faire à la suite de la promotion.

- Connectez-vous à la machine virtuelle AD2 puis ouvrez une session en tant qu'administrateur.
- Dans la console **Gestionnaire de serveur**, cliquez sur **Ajouter des Rôles et des fonctionnalités**.
- L'assistant se lance, cliquez sur **Suivant**.
- Cliquez sur **Installation basée sur un rôle ou une fonctionnalité** dans la fenêtre **Sélectionner le type d'installation**.

- Dans la fenêtre du choix de serveur de destination, laissez le paramètre par défaut.
- Cochez la case **Services AD DS**.



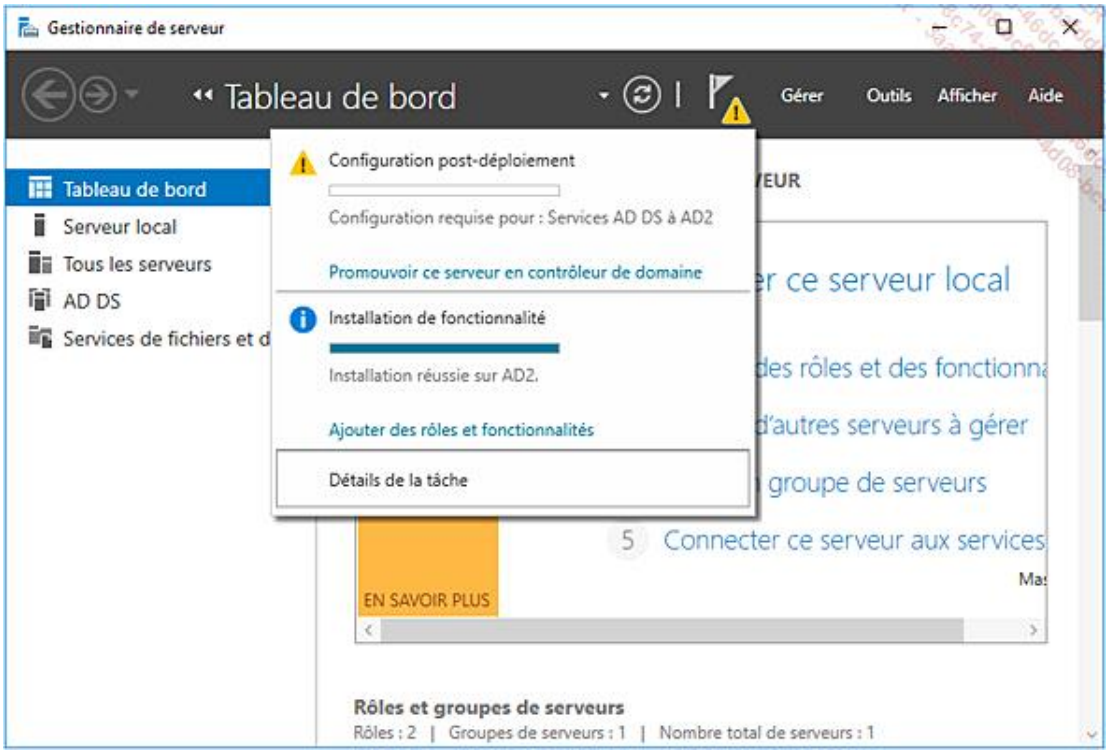
- Cliquez sur **Ajouter des fonctionnalités** dans la fenêtre qui s'affiche afin d'installer les fonctionnalités nécessaires à Active Directory.



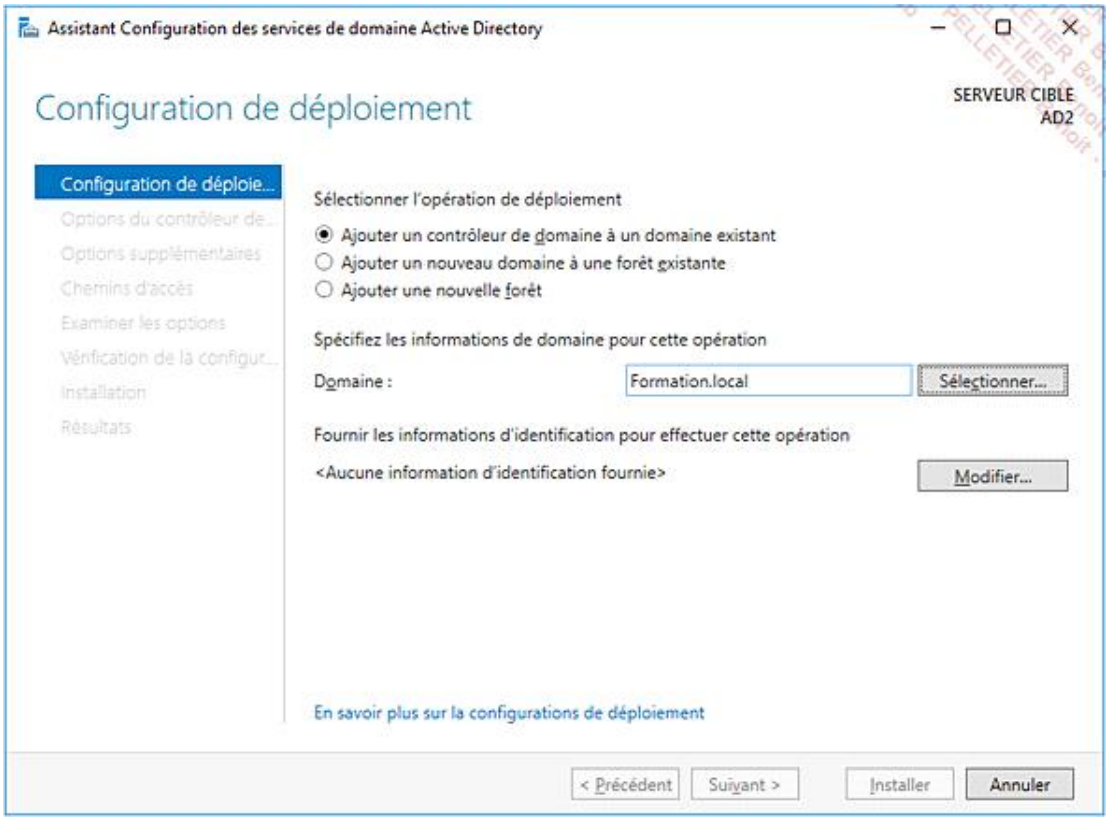
- Cliquez sur **Suivant** dans la fenêtre **Sélectionner des fonctionnalités**.
- Cliquez sur **Installer** pour lancer l'installation.

L'installation est en cours…

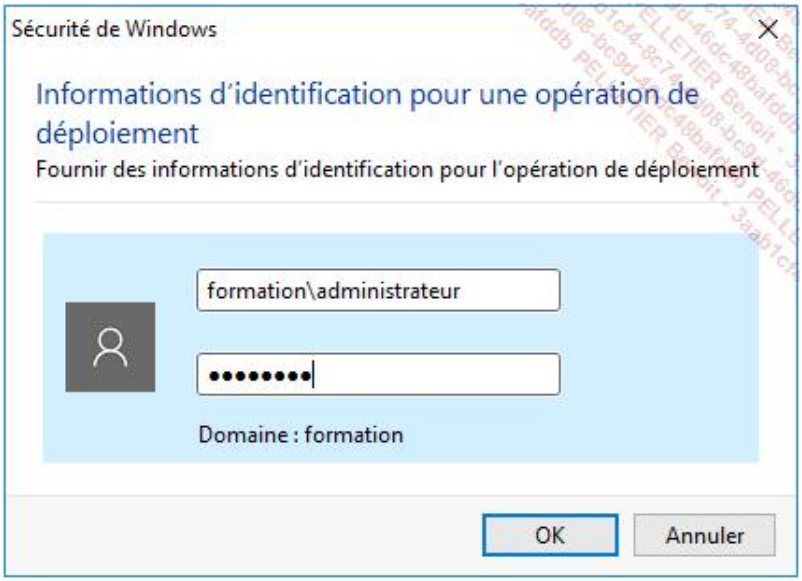
- Une fois l'installation terminée, cliquez sur **Fermer**.
- Dans la console **Gestionnaire de serveur**, cliquez sur le drapeau présent dans la zone de notification.
- Cliquez sur **Promouvoir ce serveur en contrôleur de domaine**.



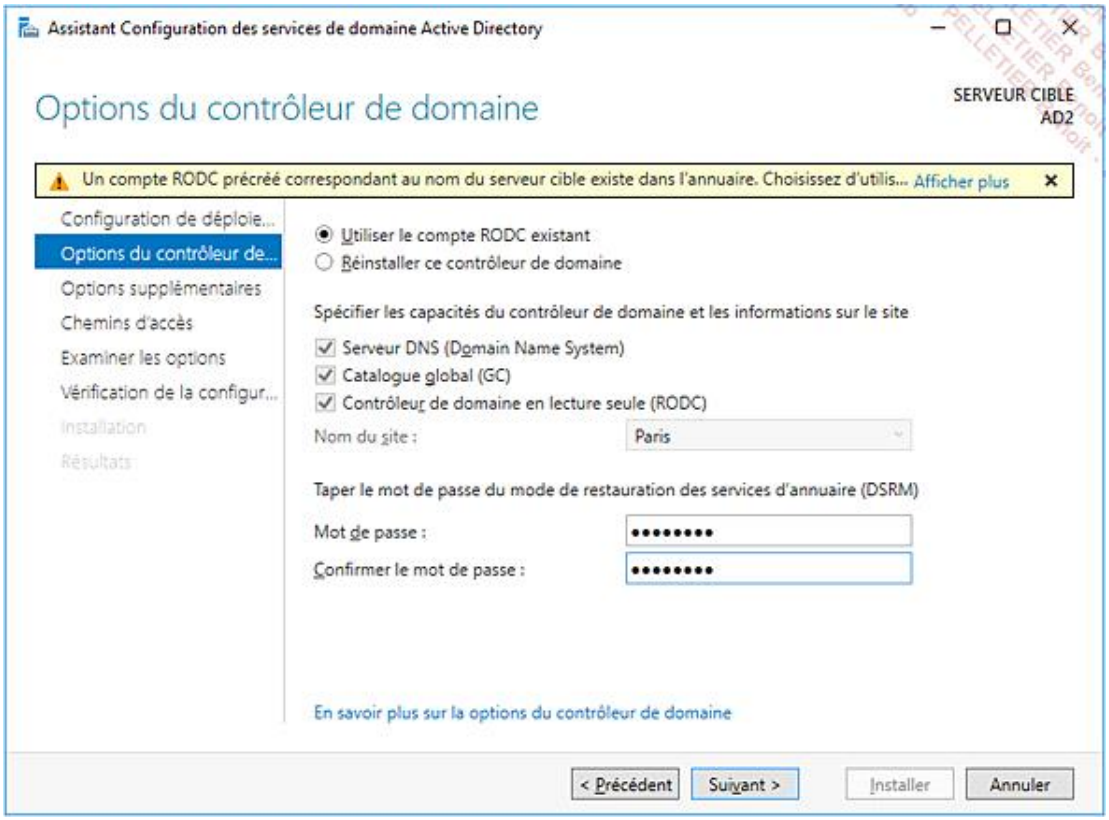
- Cliquez sur **Ajouter un contrôleur de domaine à un domaine existant** et saisis-sez dans le champ **Domaine** le nom du domaine **Formation.local**.



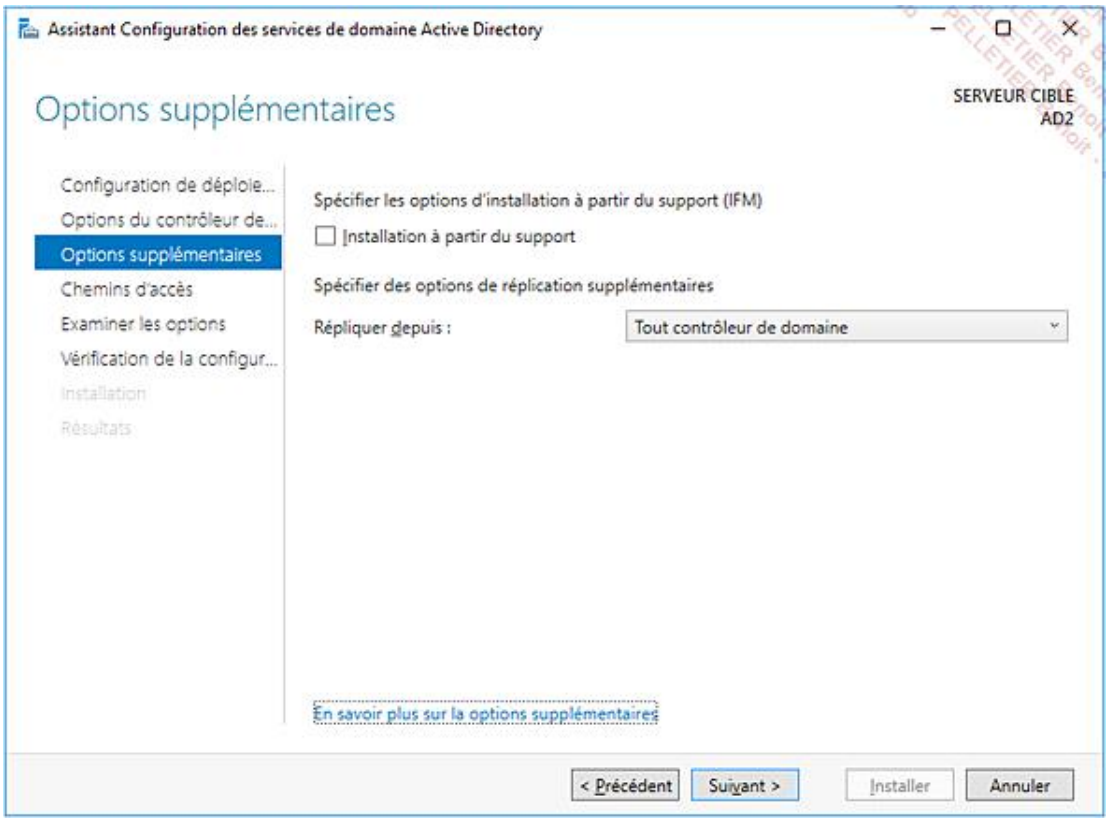
- Cliquez sur le bouton **Modifier** afin de saisir les informations d'identification.
- Saisissez **formation\administrateur** dans le champ du nom d'utilisateur ainsi que le mot de passe dans le champ adéquat.



- Saisissez **Pa$$w0rd** dans le champ **Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)** puis cliquez sur **Suivant**.



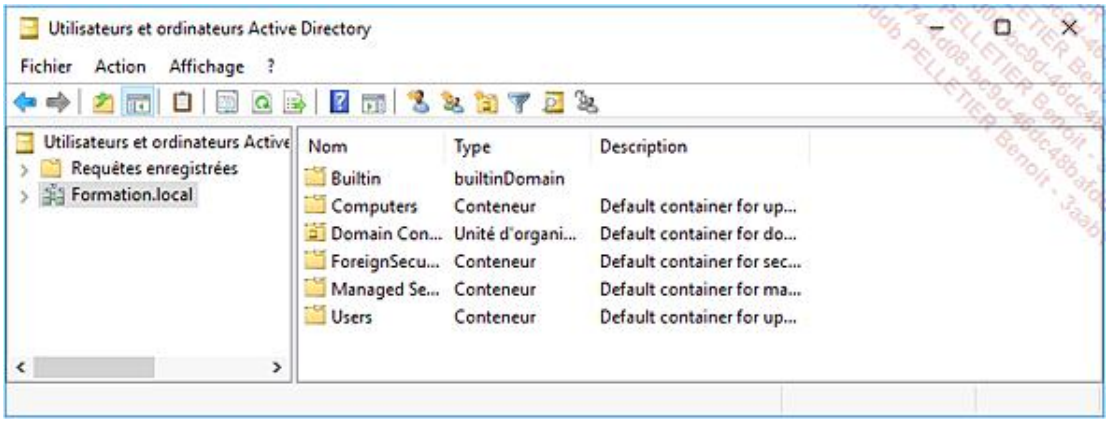
- Un seul contrôleur de domaine est présent, laissez les choix par défaut dans la fenêtre **Options supplémentaires** et cliquez sur **Suivant**.



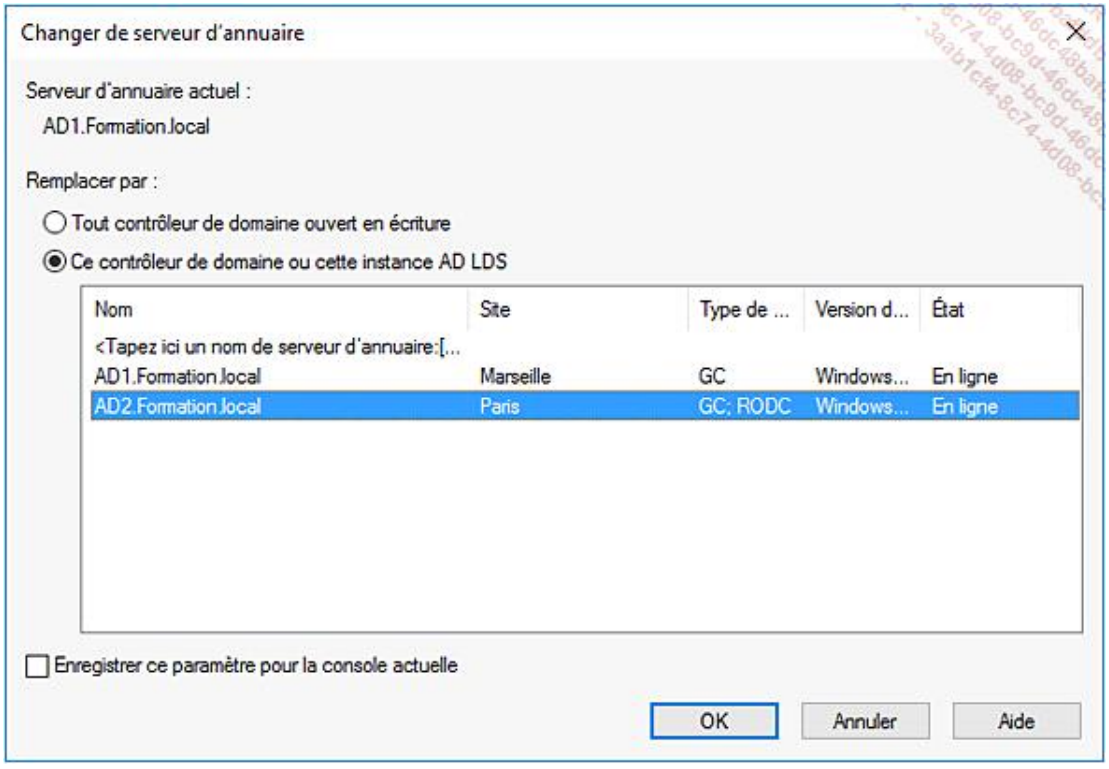
- Dans la fenêtre des chemins d'accès, cliquez sur **Suivant**.
- Dans la fenêtre du résumé, cliquez sur **Suivant**.
- Cliquez sur **Installer** dans la fenêtre de vérification de la configuration.

À la fin de l'installation, le serveur redémarre afin de finaliser l'installation. Le RODC est maintenant installé correctement.

- Démarrez une session en tant qu'**administrateur du domaine**.
- Ouvrez la console **Utilisateurs et ordinateurs Active Directory**.

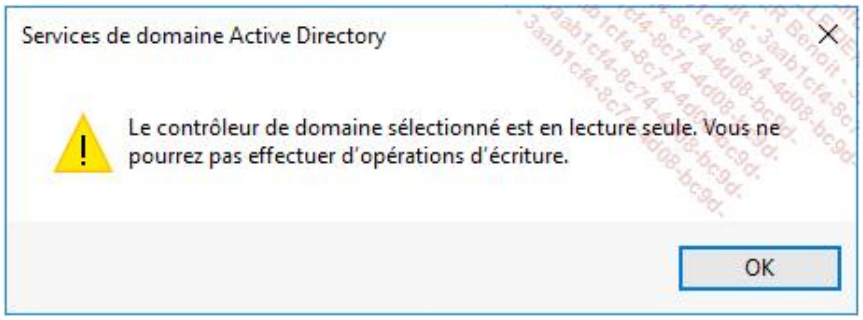


- Effectuez un clic droit sur le domaine puis un clic gauche sur **Changer de contrôleur de domaine**.
- Sélectionnez **AD2** puis cliquez sur **OK**.



Un message vous avertit que la connexion a été faite sur un RODC.

- Cliquez sur **OK**.

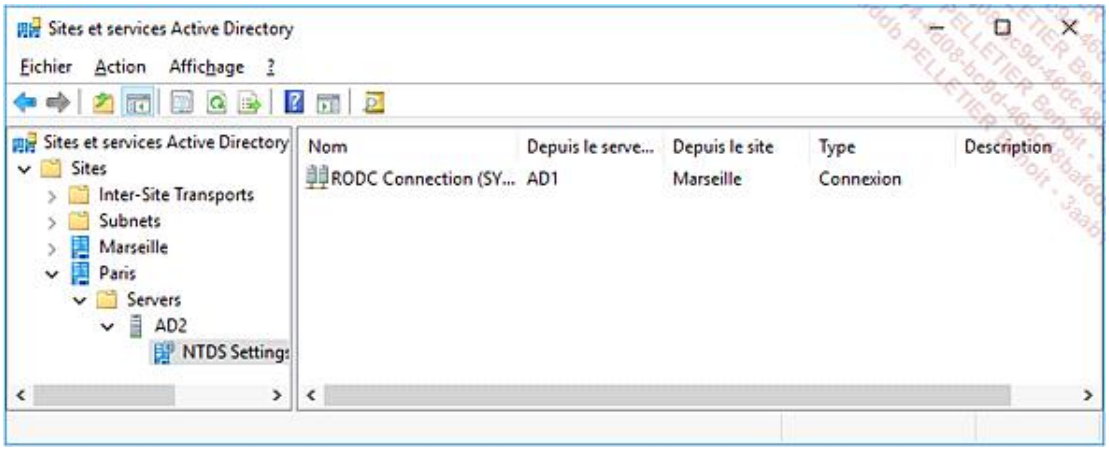


Il est impossible de créer un nouvel objet sur **AD2**.

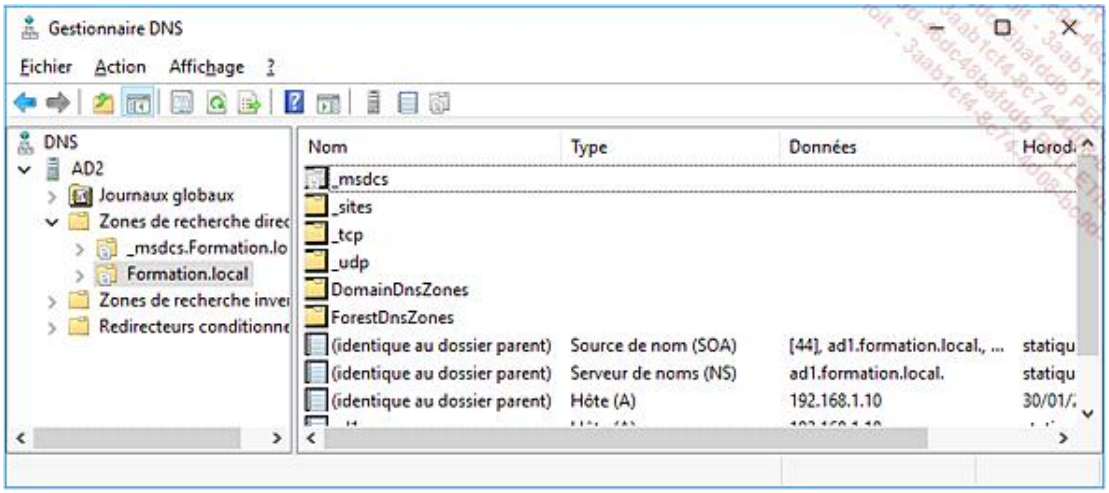
4. Vérifications à réaliser après l'installation d'un contrôleur de domaine

L'installation d'un contrôleur de domaine terminée, il peut être utile de vérifier les points suivants :

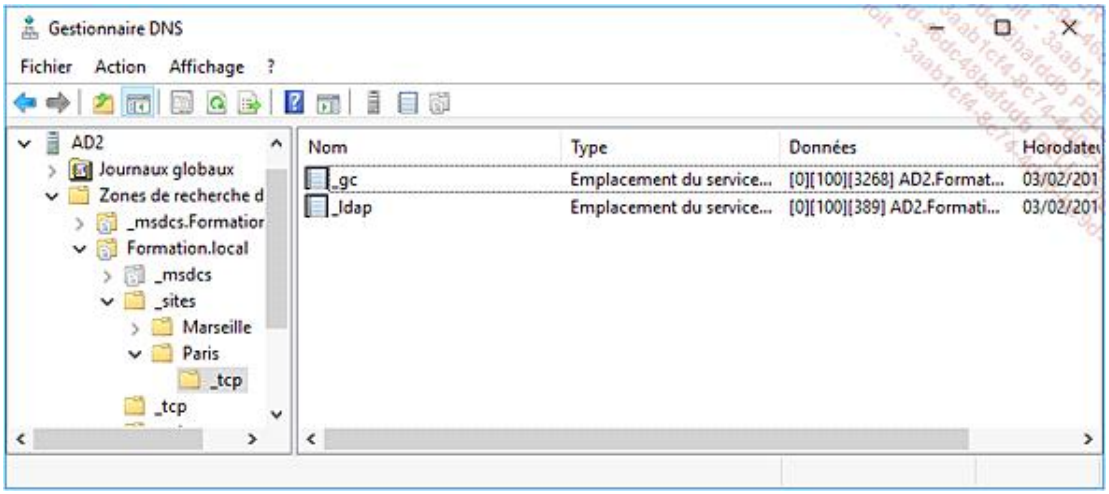
- La bonne configuration des sites AD.
- La configuration de la réplication intersites.
- L'association des sous-réseaux IP avec les bons sites.



- La bonne configuration de la zone DNS. Cette vérification peut être effectuée par l'intermédiaire de la console DNS.



- La présence des enregistrements de type SRV dans le DNS doit également être vérifiée.



- Exécutez la commande `dcdiag /test:replications` qui permet de s'assurer d'une bonne réplication entre AD1 et AD2.

Il est possible d'effectuer d'autres vérifications en fonction de l'architecture de votre réseau (plusieurs forêts avec des relations d'approbation entre elles, plusieurs domaines dans la forêt…).

Redémarrage de l'AD

Active Directory s'appuie sur une base de données. Il est donc nécessaire dans certains cas de défragmenter la base, d'effectuer une restauration à la suite d'un crash, ou toute autre opération de maintenance.

Pour effectuer toutes ces manipulations, il est nécessaire d'avoir un accès complet à la base de données. Lors de l'utilisation quotidienne de l'Active Directory, l'accès est limité aux fonctionnalités offertes par les différents outils (Sites et services AD, Utilisateurs et ordinateurs AD…).

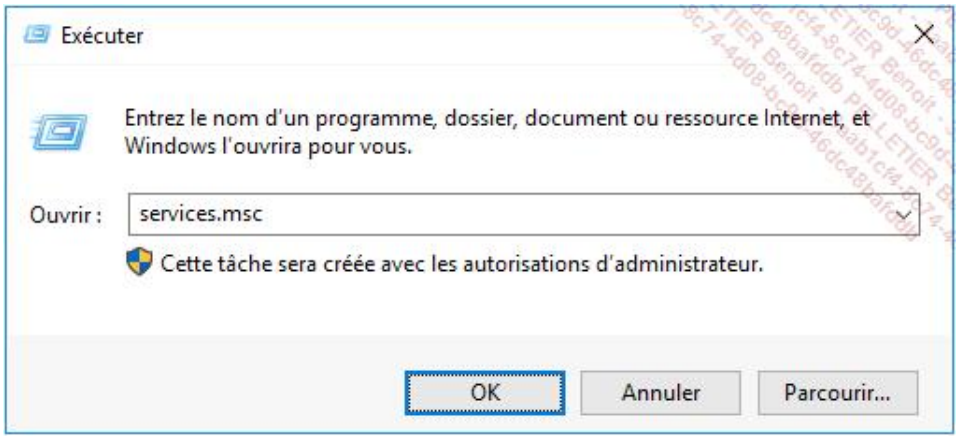
Depuis Windows Server 2008, un nouveau service Windows permet d'arrêter l'annuaire AD afin d'obtenir un accès complet à la base de données.

1. Démarrage/arrêt des services Active Directory avec la console MMC Services

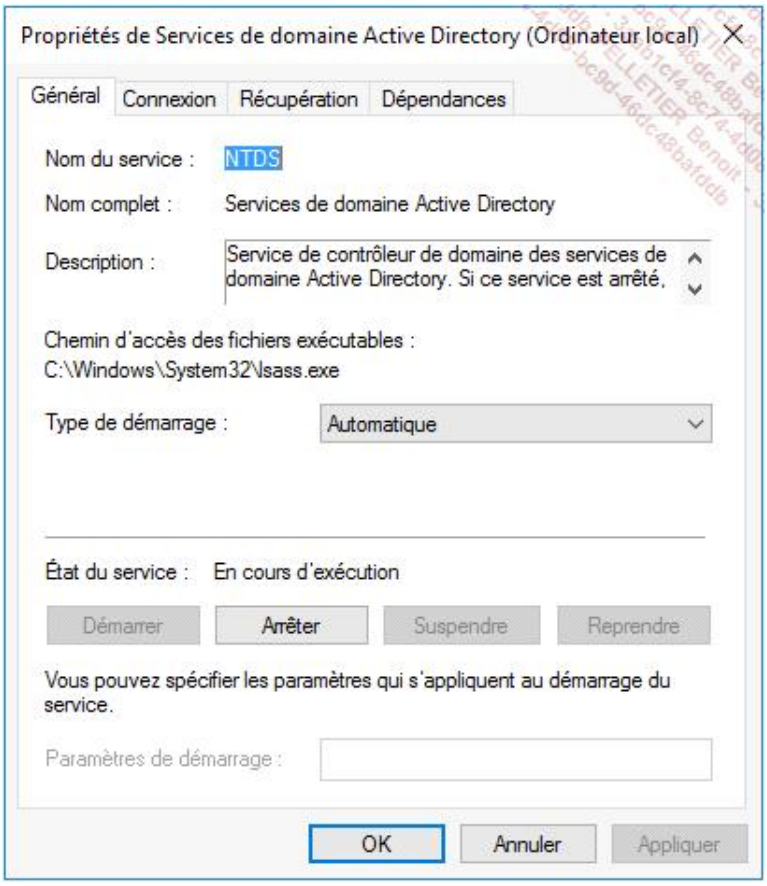
Il existe deux manières d'arrêter ou de démarrer le service Active Directory, la première, vue dans le présent point, est la gestion du service depuis la console MMC Services.msc.

L'arrêt de ce service permet d'effectuer une maintenance (défragmentation…) sur la base de données du rôle AD DS.

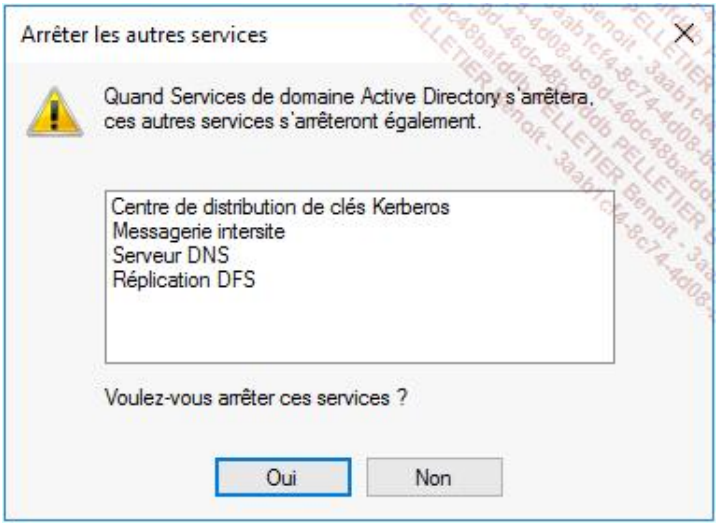
- Effectuez un clic droit sur le bouton **Démarrer** puis un clic gauche sur **Exécuter**. La deuxième est vue dans le point suivant.
- Saisissez dans le champ **services.msc**.



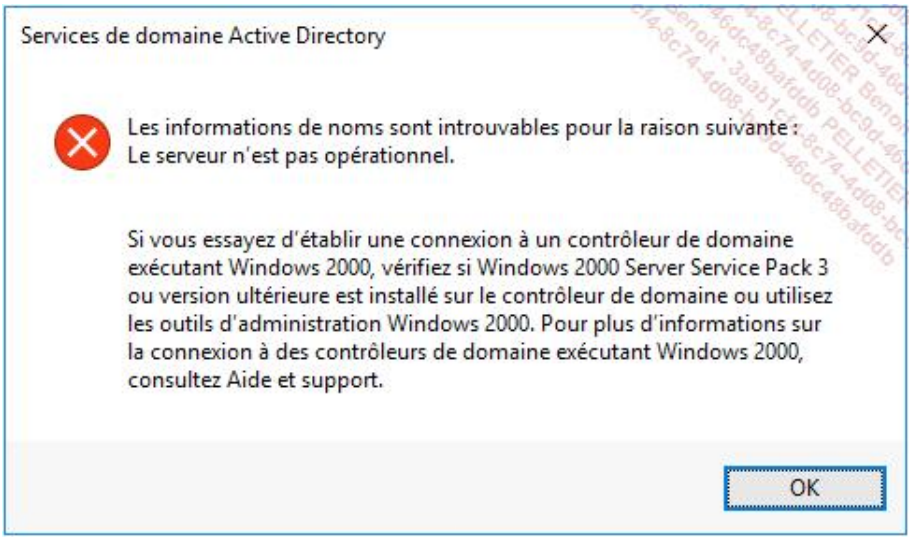
- Double cliquez sur **Services de domaine Active Directory**, puis cliquez sur **Stop**.



- D'autres services doivent être également arrêtés. Cliquez sur **Oui**.



Après l'arrêt des services, il est impossible d'accéder à la console **Utilisateurs et ordinateurs Active Directory**.

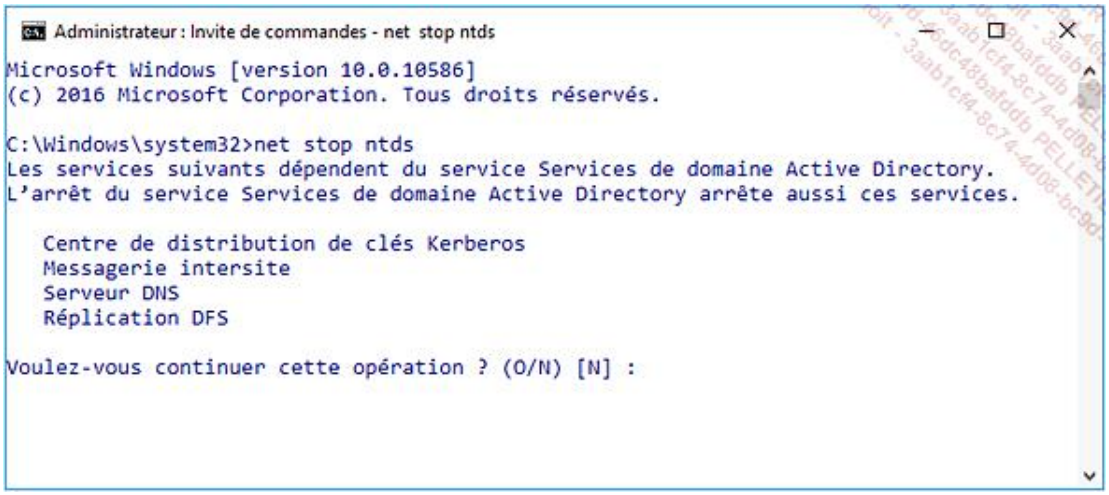


- Redémarrez le service de **Services de domaine Active Directory**.

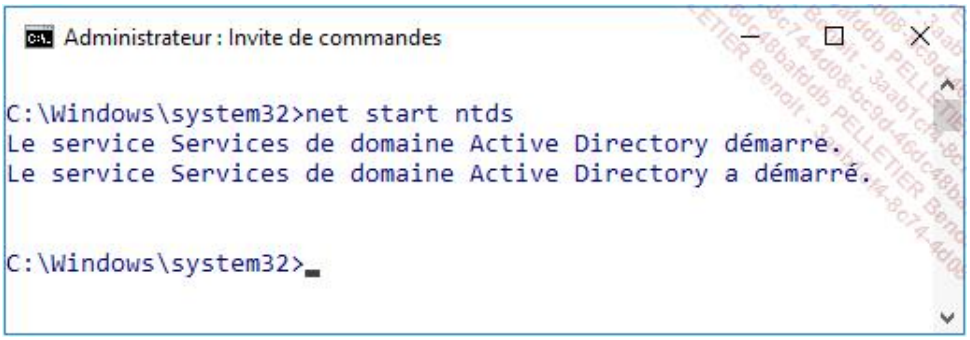
2. Démarrage/arrêt des services Active Directory avec l'invite de commandes

Comme pour tous les services, il est possible d'arrêter ou de redémarrer les services Active Directory en ligne de commande. L'instruction à utiliser est `net stop` pour l'arrêt du service et `net start` pour le démarrage.

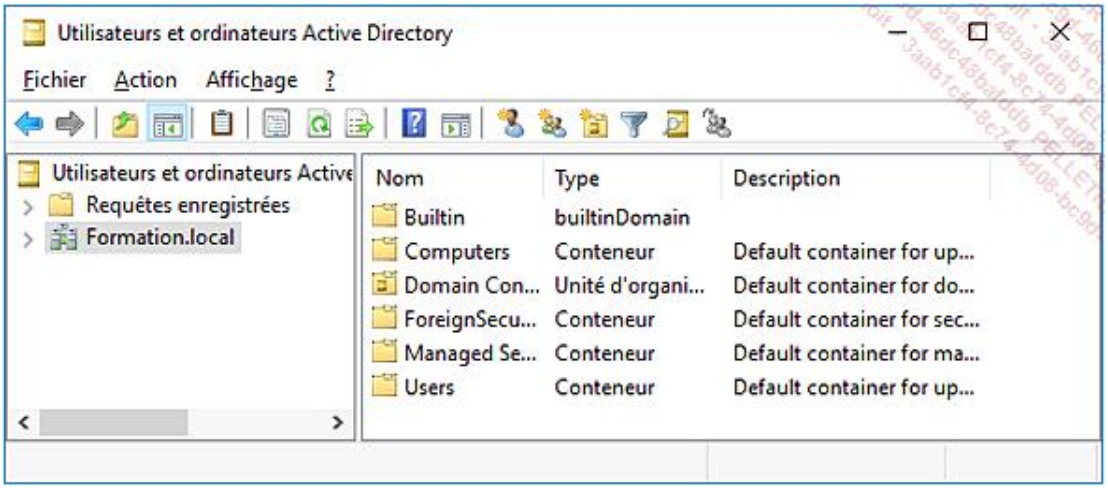
- Ouvrez une invite de commandes DOS.
- Saisissez dans la fenêtre `net stop ntds`. Validez l'arrêt des autres services par un **O**.



- Tentez d'ouvrir la console **Utilisateurs et ordinateurs Active Directory**. Un message d'erreur apparaît.
- Saisissez dans la fenêtre `net start ntds`.



Il est de nouveau possible d'accéder à la console.



Suppression d’un contrôleur de domaine

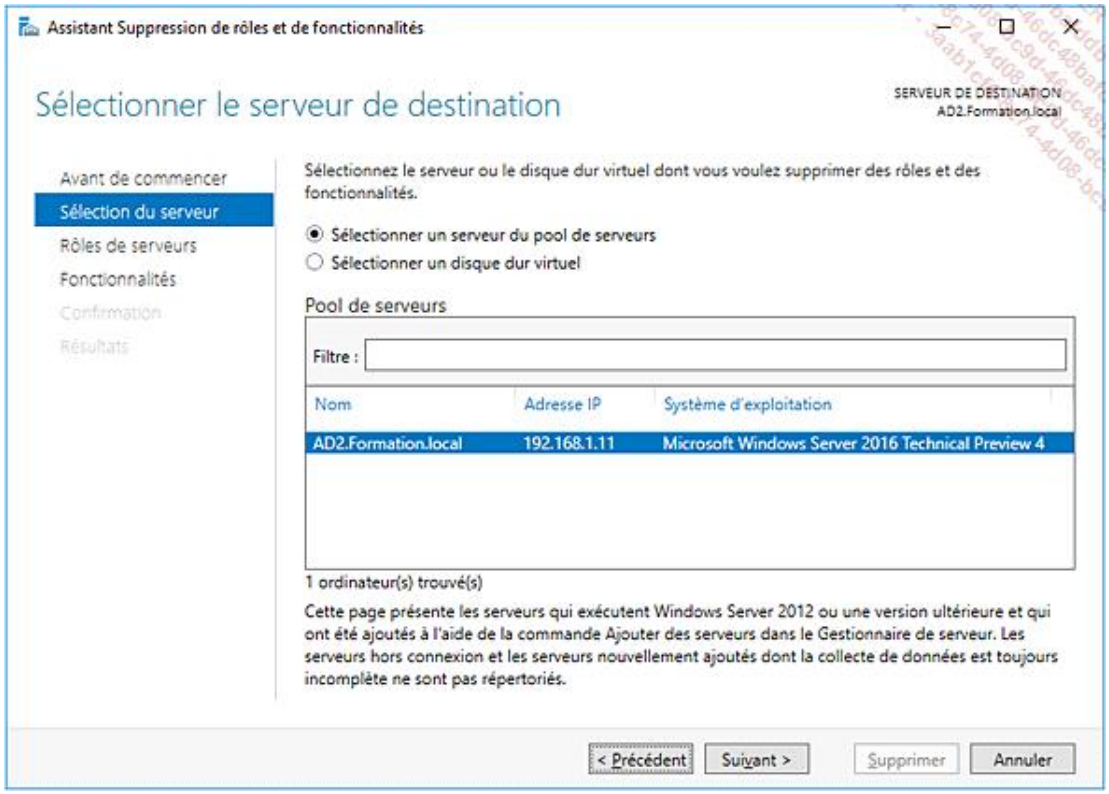
Un contrôleur de domaine peut être amené à être rétrogradé en simple serveur membre pour des raisons de changement de serveur ou autres.

La manipulation consiste à enlever le rôle de contrôleur de domaine au serveur.

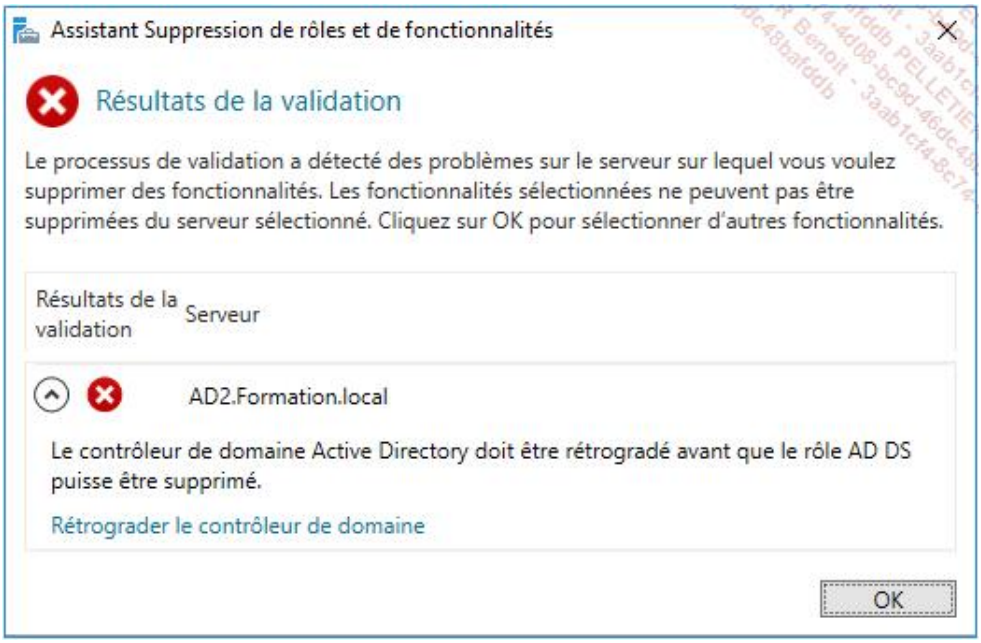
Supprimer un contrôleur de domaine d’un domaine

Le domaine **Formation.local** est constitué d’un contrôleur de domaine en lecture/écriture et d’un contrôleur de domaine uniquement en lecture. L’opération consiste à supprimer le rôle **AD DS** sur le RODC. On parlera donc de rétrogradation du serveur.

- Ouvrez une session sur **AD2** en tant qu’administrateur du domaine.
- Lancez la console **Gestionnaire de serveur**.
- Cliquez sur **Gérer** puis sur **Supprimer des rôles et fonctionnalités**.
- Cliquez sur **Suivant** dans la page d’accueil de l’assistant.
- Dans la fenêtre **Sélectionner le serveur de destination**, cliquez sur **Suivant**.

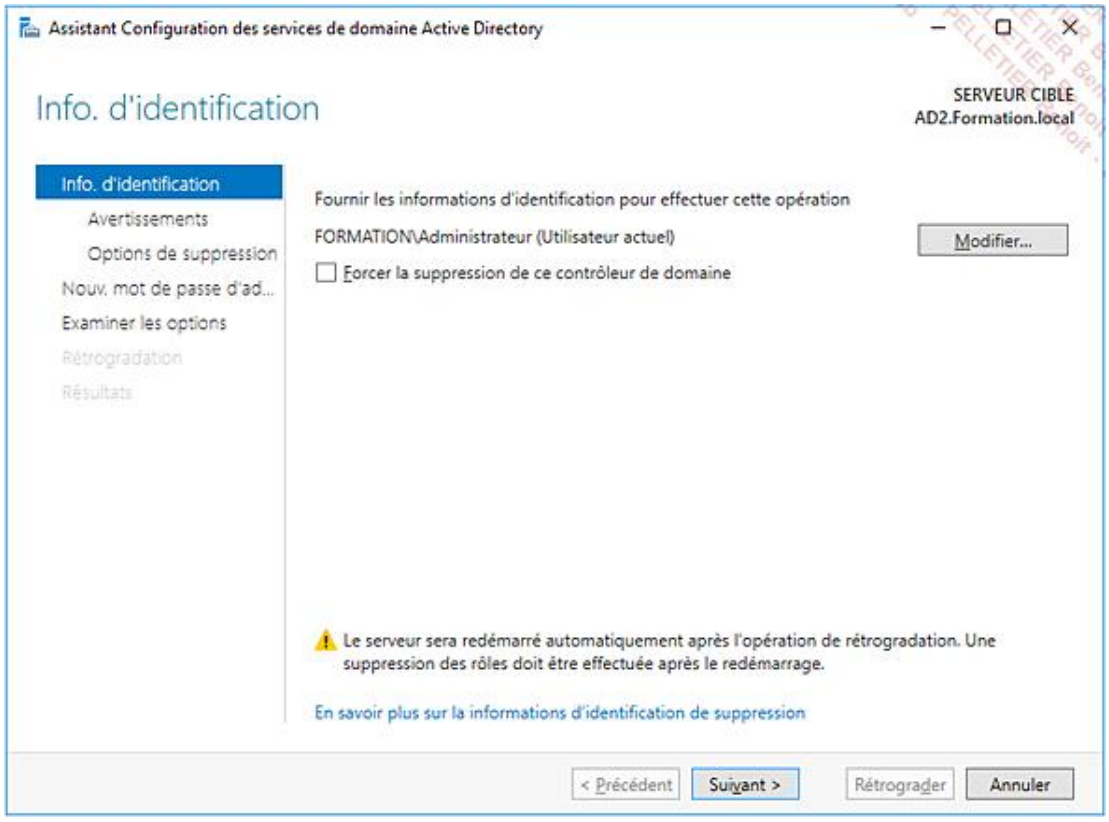


- Décochez le rôle **Services AD DS**. Les fonctionnalités sont également à supprimer. Un message d’erreur apparaît. Cliquez sur **Rétrograder le contrôleur de domaine**.

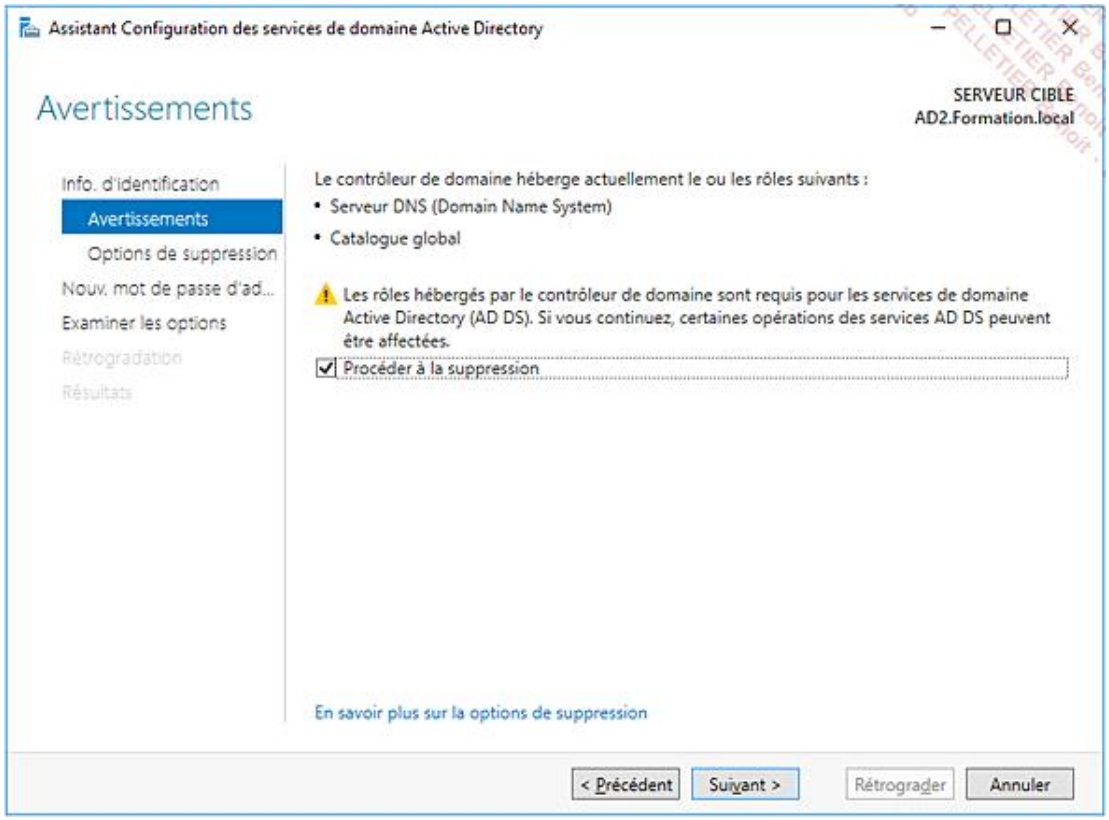


- Dans la fenêtre d'identification, cliquez sur **Suivant**.

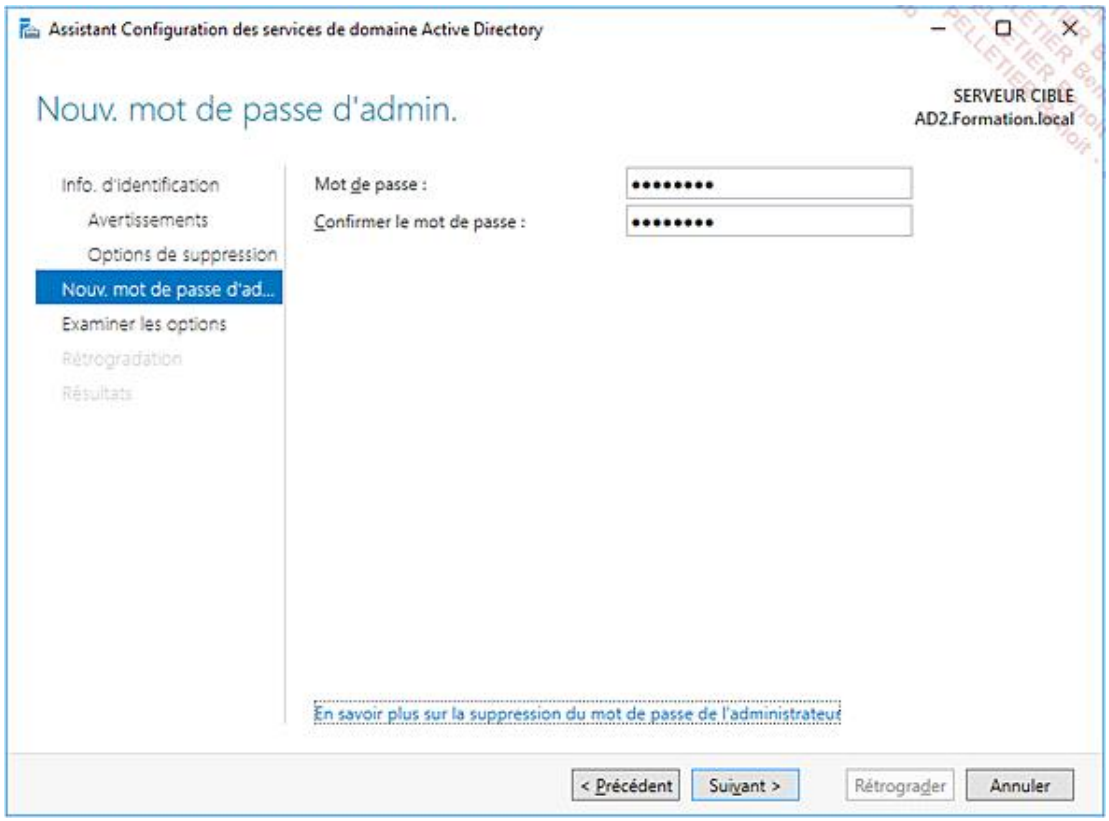
Le compte à utiliser pour la rétrogradation du serveur peut être changé à l'aide du bouton **Change**. En cas de contrôleur de domaine isolé, il est utile de cocher la case **Forcer la suppression de ce contrôleur de domaine**.



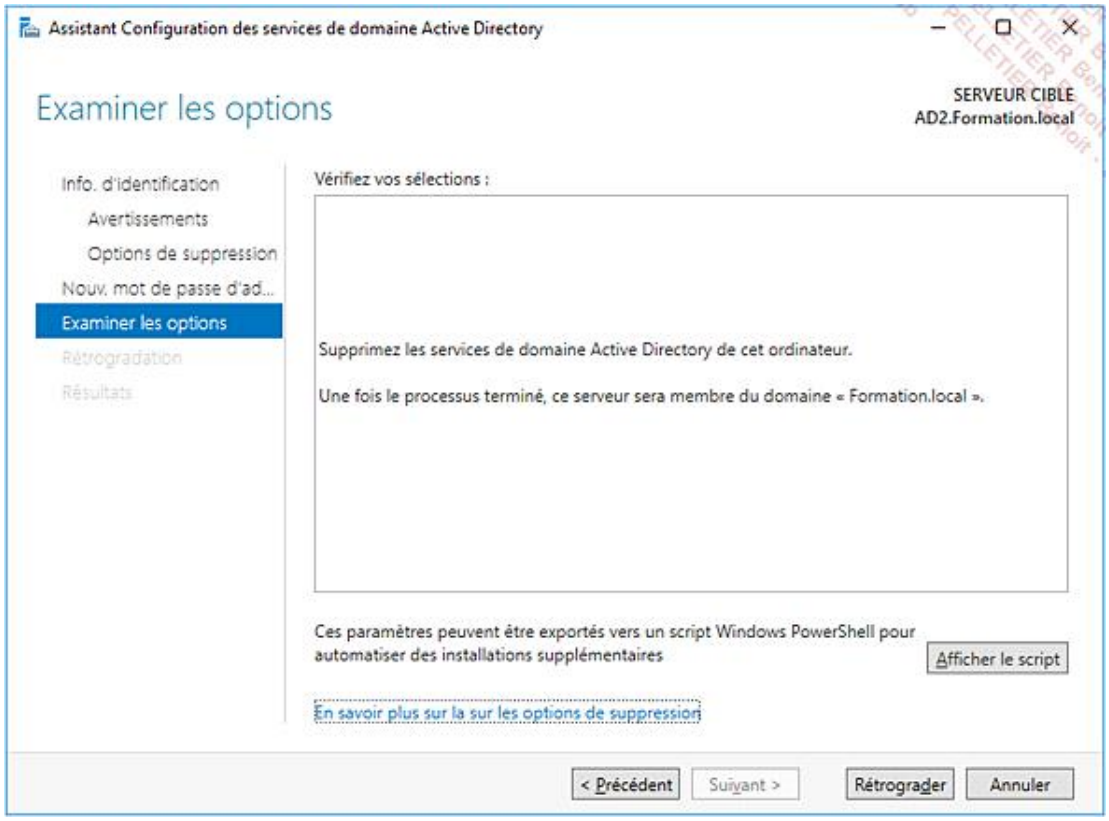
- Cochez la case **Procéder à la suppression** puis cliquez sur **Suivant**.



- Laissez décochée la case **Conserver les métadonnées de contrôleurs de domaine** puis cliquez sur **Suivant**.
- Saisissez, à la fin de la rétrogradation, le mot de passe qui sera utilisé pour le compte administrateur local du serveur (mot de passe : **Pa$$w0rd**).



- Dans la page du résumé, cliquez sur **Rétrograder**.



À la fin de la rétrogradation, le serveur redémarre.

- Ouvrez une session sur AD2 en tant qu'administrateur.

Le serveur ne possède plus le rôle **Contrôleurs de domaine**.

Clonage d'un contrôleur de domaine virtualisé

Le clonage d'un contrôleur de domaine consiste à effectuer une copie du disque dur virtuel (fichier VHD) d'un contrôleur de domaine existant. Il est nécessaire de créer un fichier de configuration clone. Le nombre d'étapes et le temps nécessaire pour le déploiement d'un contrôleur de domaine sont réduits à l'aide de cette fonctionnalité.

Le clone utilise les critères suivants pour détecter qu'il s'agit d'une copie d'un autre contrôleur de domaine.

Présence du fichier **DCCloneConfig.xml** dans un des emplacements suivants :

- Le répertoire où réside ntds.dit (%windir%\NTDS).
- La racine d'un lecteur de média amovible.

Le contexte de sécurité du serveur source est utilisé par le contrôleur de domaine cloné afin de communiquer avec le serveur ayant le rôle **Emulateur PDC**. Ce dernier doit exécuter nécessairement Windows Server 2012 ou version ultérieure.

Après la vérification que le serveur qui effectue la demande est bien autorisé pour l'opération de clonage, l'émulateur PDC crée une nouvelle identité machine, un nouveau compte et un nouvel SID ainsi que le mot de passe permettant d'identifier cette machine en tant que DC réplica. Une fois les informations reçues, le serveur clone prépare les fichiers de base de données afin de servir de réplique.

1. Les différents composants du clonage

De nouvelles instructions PowerShell sont contenues dans le module Active Directory :

New-ADDCCloneConfigFile : permet la mise en place du fichier **DCCloneConfig.xml** au bon endroit, étape indispensable pour déclencher le clonage. Des contrôles préalables sont effectués afin de permettre le bon fonctionnement de l'opération. L'exécution peut être locale sur un contrôleur de domaine virtualisé en cours de clonage, ou à distance en utilisant l'option **offline**.

Les vérifications préalables effectuées sont les suivantes :

- Le contrôleur de domaine qui est en train d'être préparé est autorisé pour le clonage (utilisation du groupe Contrôleur de domaine clonable).
- Le serveur ayant le rôle d'émulateur PDC doit exécuter Windows Server 2012 ou version ultérieure.
- Les programmes ou services listés par l'exécution de la commande **Get-ADDCCloningExcludedApplicationList** sont inclus dans le fichier **CustomDCCloneAllowList.xml**.

DCCloneConfig.xml : il est nécessaire de s'assurer de la présence du fichier dans le dossier **%windir%\NTDS** ou à la racine d'un lecteur de média amovible. Il permet le lancement du clonage ainsi que la fourniture des paramètres de configuration du DC cloné. Il est recommandé d'utiliser **New-ADDCCloneConfigFile** pour la création du fichier afin d'éviter tout risque d'erreur.

Get-ADDCCloningExcludedApplicationList : ce cmdlet doit être exécutée en amont du processus de clonage sur le contrôleur de domaine source. Elle permet de déterminer les services ou programmes installés qui ne sont pas compatibles avec la fonctionnalité. La recherche est effectuée en utilisant la console Gestionnaire de services et la base de registre (HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall).

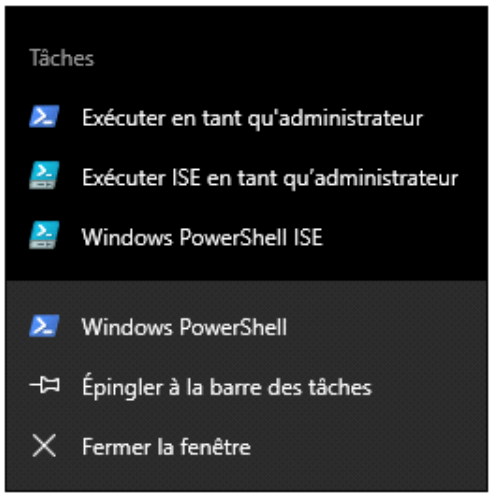
CustomDCCloneAllowList.xml : ce fichier permet de créer des exceptions pour des applications non compatibles avec le clonage. Cette opération est obligatoire sans quoi les opérations suivantes sont impossibles. Exécutez **Get-**

ADDCCloningExcludedApplicationList afin de trouver les différents services et programmes non présents dans le fichier **DefaultDCCloneAllowList.xml**. Le commutateur **GenerateXml** doit être utilisé afin de permettre la génération du fichier XML d'exception. Ce dernier permettra de créer des exceptions pour un ou plusieurs services/applications non compatibles avec le clonage.

2. Prérequis au clonage

- Le compte utilisé doit être membre du groupe **Administrateurs du domaine** et la console PowerShell doit, elle, être exécutée avec l'élévation de privilège.

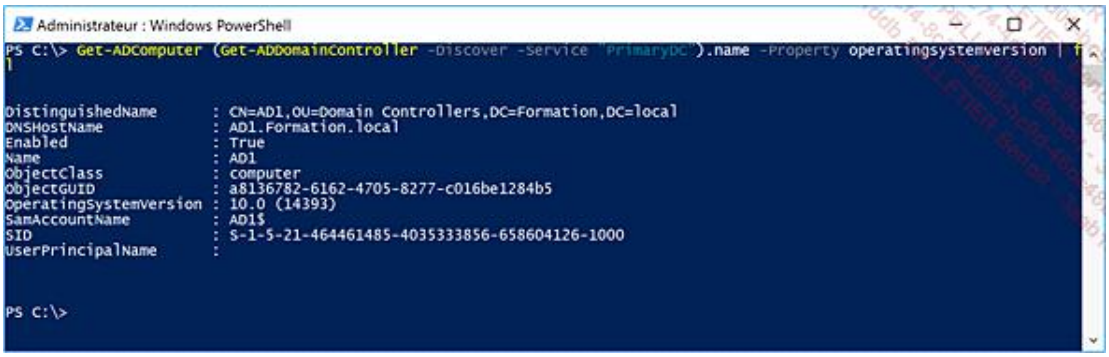
Effectuez un clic droit sur **PowerShell** et sélectionnez **Exécuter en tant qu'administrateur**.



- Il est possible d'utiliser un seul serveur Hyper-V, attention néanmoins les fichiers VHD des deux machines (le clone et la machine clonée) ont le même nom. Il est donc préférable d'effectuer l'exportation dans un répertoire différent de celui où est stockée la machine source.
- Pour connaître le serveur qui a ce rôle, il est possible d'utiliser la commande PowerShell ci-dessous :

```
Get-ADComputer (Get-ADDomainController -Discover -Service
"PrimaryDC").name -Property operatingsystemversion | fl
```

Le script peut être téléchargé depuis la page Informations générales.



- Il est recommandé de s'assurer de l'état de santé du contrôleur de domaine afin de dupliquer un serveur sain. Pour cela, utilisez la commande **dcdiag**. Consultez le lien ci-dessous pour avoir plus d'informations sur cette commande :http://blogs.technet.com/b/askds/archive/2011/03/22/what-does-dcdiag-actually-do.aspx
- Si le contrôleur de domaine source est également serveur DNS, le clone a également le rôle de serveur DNS. Les

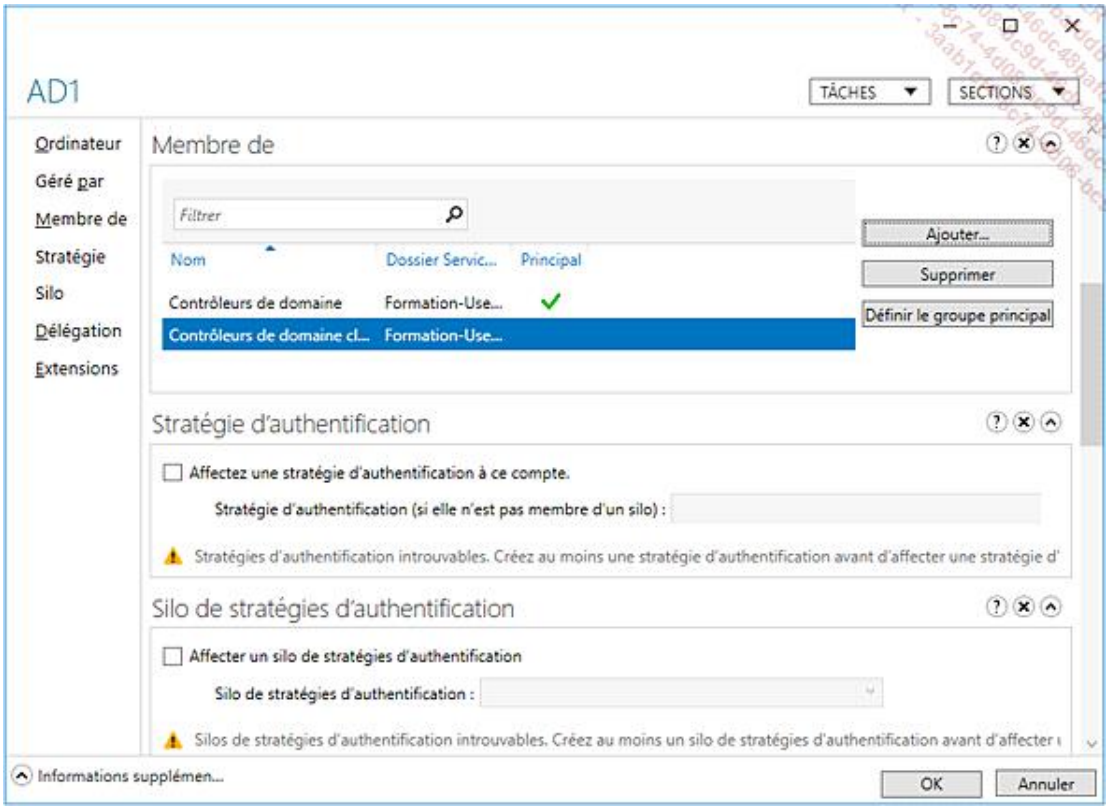
zones DNS **doivent être intégrées à Active Directory**.

- Lors du clonage, l'adresse configurée dans le client DNS du serveur n'est pas dupliquée vers la destination ; elle est spécifiée dans le fichier **DCCloneConfig.xml**. Si ce dernier ne contient pas l'information, le client DNS pointera sur lui-même en tant que serveur préféré par défaut. Si besoin, il est nécessaire de mettre à jour les délégations DNS pour le contrôleur domaine cloné.
- Les serveurs ayant les rôles suivants ne peuvent pas être clonés :
  - DHCP (Dynamic Host Configuration Protocol)
  - Active Directory Certificate Services (AD CS)
  - Active Directory Lightweight Directory Services (AD LDS)

Il est donc nécessaire de procéder à la migration de ces rôles.

3. Mise en place de la solution de clonage

- Sur le contrôleurs de domaine AD1, ouvrez la console **Centre d'administration Active Directory**.
- Dans l'OU **Contrôleurs de domaine**, double cliquez sur **AD1** puis, à l'aide de l'onglet **Membre de**, ajoutez le compte au groupe **Contrôleur de domaine clonables**.



- Cliquez sur **OK** afin de valider l'ajout.

La réplication sur le serveur ayant le rôle d'émulateur PDC doit être effectuée afin de s'assurer de la réussite des opérations de clonage.

La commande PowerShell ci-dessous peut également être utilisée.

```
Add-ADGroupMember -Identity "CN=Contrôleurs de domaine
clonables,CN=Users,DC=formation,DC=local" -Member
"CN=AD1,OU=Domain Controllers,DC=formation,DC=local"
```

Le script peut être téléchargé depuis la page Informations générales.

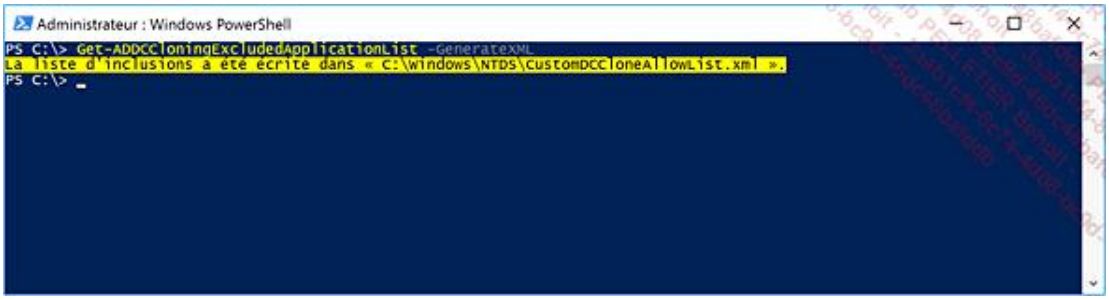
Redémarrer le serveur afin de prendre en compte l'ajout dans le groupe.

L'exécution de la cmdlet `Get-ADDCCloningExcludedApplicationList` est maintenant nécessaire afin de permettre l'identification de tous les programmes ou services qui ne sont pas compatibles pour l'opération de clonage. Cette manipulation est à faire sur le contrôleur de domaine source virtualisé.

La commande doit être exécutée avant le lancement de la commande PowerShell `New-ADDCCloneConfigFile`. Si ce dernier détecte des applications exclues (non compatibles), le fichier **DCCloneConfig.xml** n'est pas créé.

Saisissez dans la console PowerShell :

```
Get-ADDCCloningExcludedApplicationList -GenerateXML
```



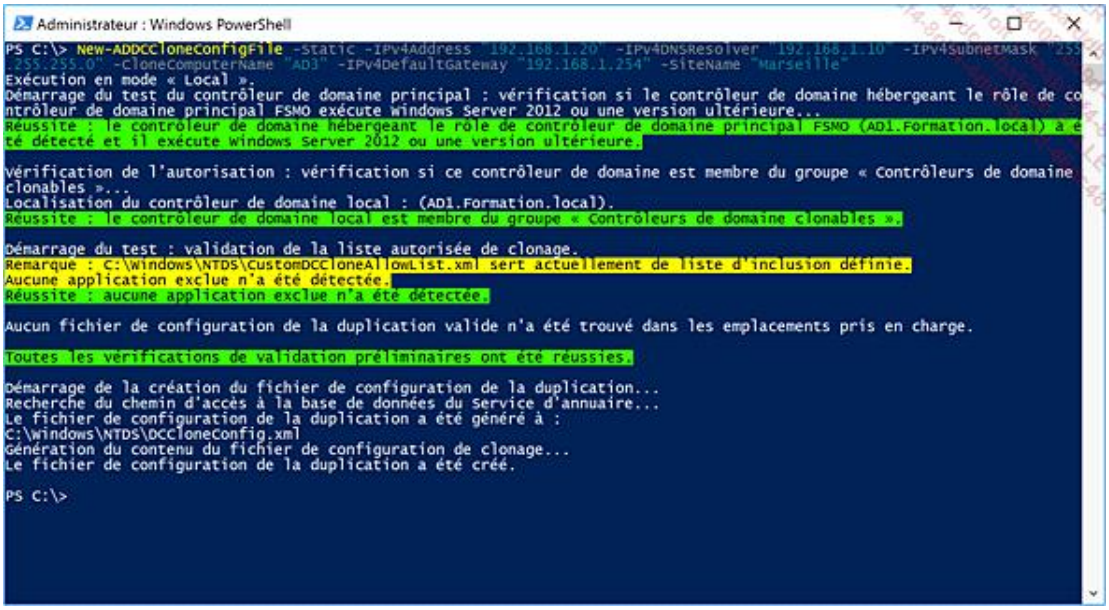
En version d'évaluation, un service non approuvé est détecté. L'utilisation du commutateur **-Generate XML** permet la création du fichier d'exception.

Le script peut être téléchargé depuis la page Informations générales.

Vérifiez qu'aucun programme ou service ne pose problème. Si un logiciel a été détecté, il est nécessaire de vérifier avec l'éditeur les risques encourus par le clonage du contrôleur de domaine. Pour les incompatibilités au niveau des rôles, il est nécessaire de migrer les rôles vers un autre serveur.

Saisissez dans la console PowerShell la commande :

```
New-ADDCCloneConfigFile -Static -IPv4Address "192.168.1.20"
-IPv4DNSResolver "192.168.1.10" -IPv4SubnetMask "255.255.255.0"
-CloneComputerName "AD3" -IPv4DefaultGateway "192.168.1.254"
-SiteName "Marseille"
```



Le fichier est créé. Il permet de configurer le serveur qui portera le nom **AD3** dont la configuration IP est la suivante :

- **Adresse IP** : 192.168.1.20
- **Masque de sous-réseau** : 255.255.255.0
- **Passerelle par défaut** : 192.168.1.254
- **Serveur DNS préféré** : 192.168.1.10

Si un contrôleur de domaine déjà existant n'est pas inscrit en tant que serveur DNS préféré, le clonage échoue.

Le contrôleur de domaine fera partie du même site Active Directory.

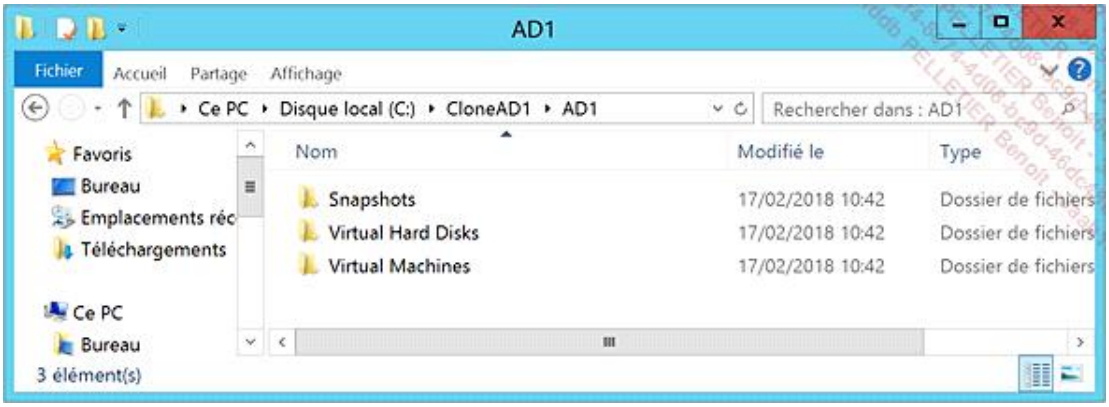
4. Exportation et importation du contrôleur de domaine source avec Hyper-V 2012 R2

Le contrôleur de domaine source virtualisé doit maintenant être exporté afin d'être importé.

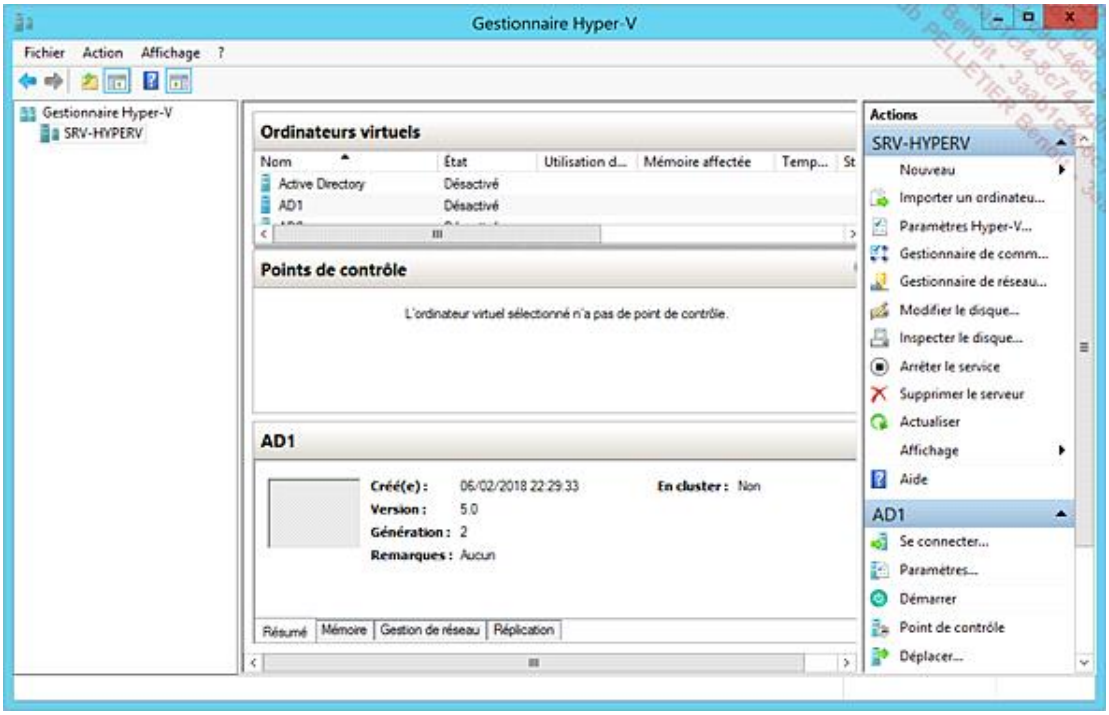
Il est nécessaire d'être au minimum membre du groupe Administrateur local du serveur Hyper-V.

Si la machine virtuelle possède des snapshots, ils doivent être supprimés avant d'effectuer l'exportation.

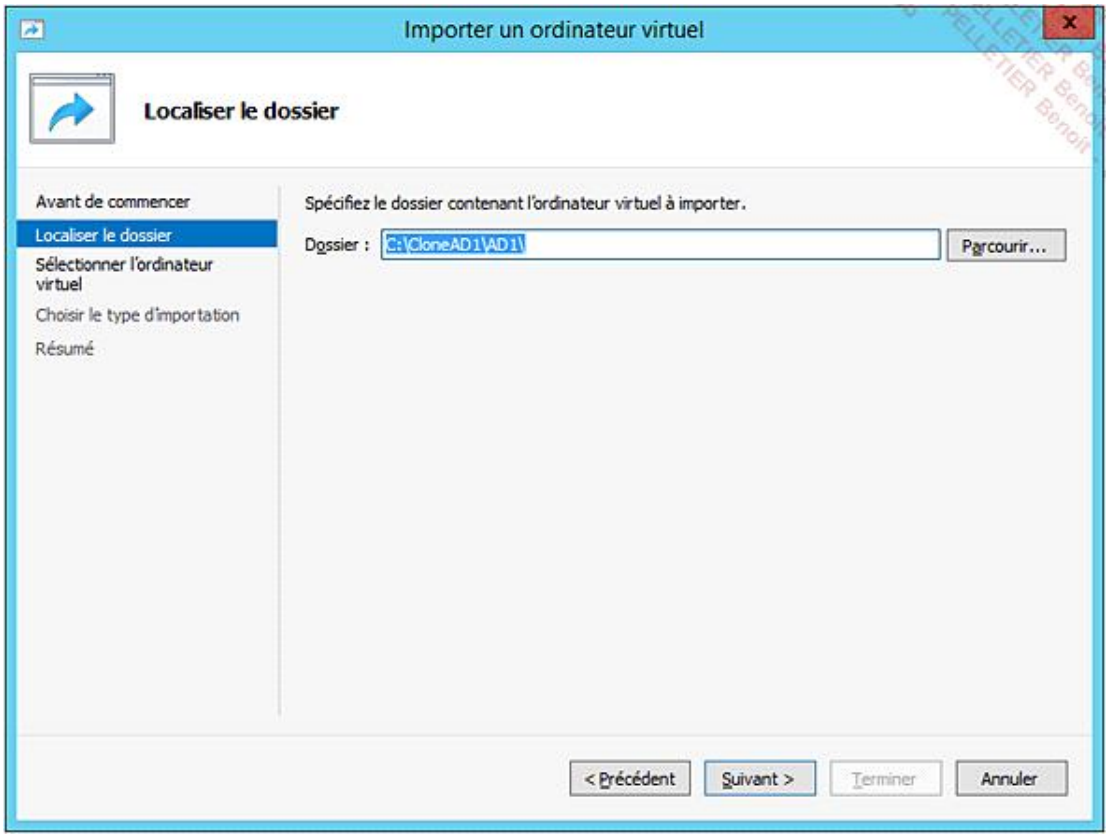
- Arrêtez le serveur **AD1** afin de pouvoir l'exporter.
- Il est désormais possible depuis Hyper-V sous Windows Server 2012 R2 d'effectuer une exportation de la VM sans avoir à l'éteindre, néanmoins dans le cas d'un clonage, un arrêt est préférable.
- Exportez **AD1** dans le dossier **C:\CloneAD1** en effectuant un clic droit sur la machine virtuelle puis en sélectionnant **Exporter**.



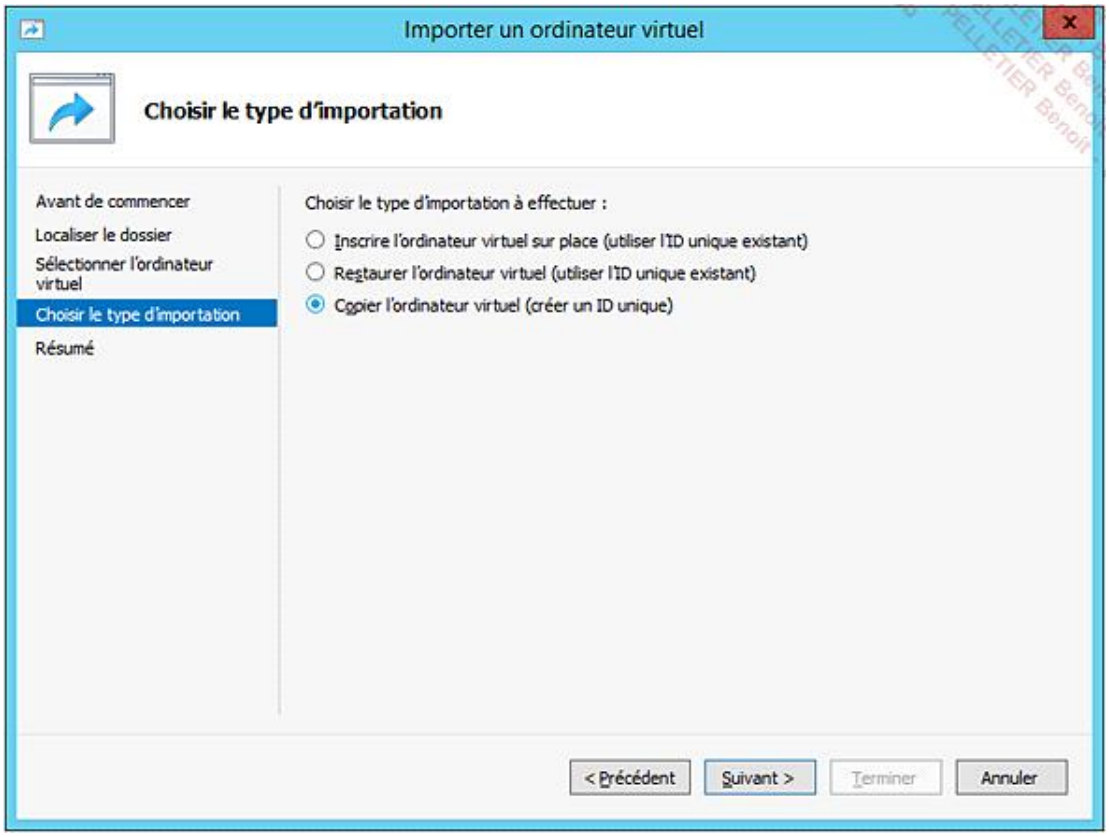
- Dans le bandeau **Actions** de la console **Gestionnaire Hyper-V**, cliquez sur **Importer un ordinateur virtuel**.



- Cliquez sur **Suivant** dans la fenêtre **Avant de commencer**.
- À l'aide du bouton, sélectionnez le dossier **AD1** présent dans **C:\clonead1** puis cliquez sur **Suivant**.

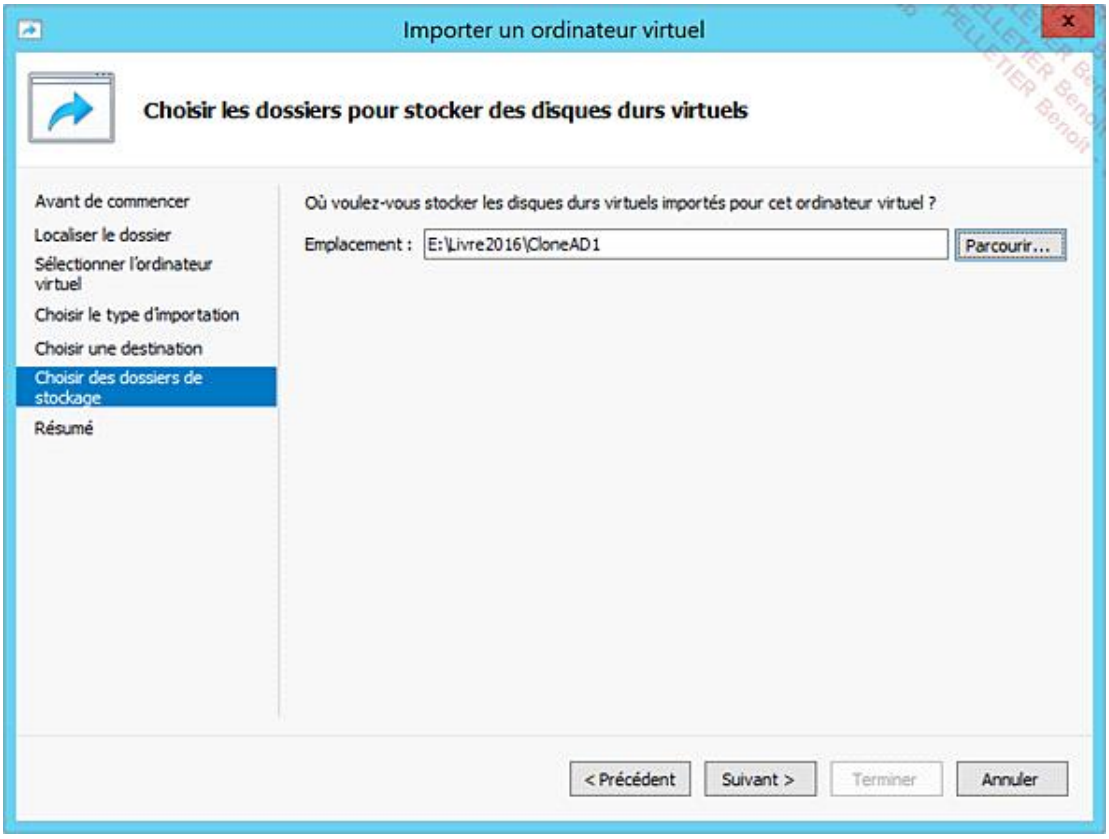


- Dans la fenêtre **Sélectionner l'ordinateur virtuel**, cliquez sur **Suivant**.
- Dans le choix du type d'importation, sélectionnez **Copier l'ordinateur virtuel (créer un ID unique)**, puis cliquez sur **Suivant**.



- Cliquez sur **Suivant**.

Stockez le fichier VHDX clone d'AD1 à un endroit différent du chemin par défaut afin d'éviter d'éventuels conflits liés au nom en double.



- Lancez l'importation en cliquant sur **Terminer**.
- Dans Hyper-V, renommez la machine virtuelle nouvellement importée et donnez-lui le nom d'AD3.

Il s'agit du nom dans Hyper-V et non du nom dans Windows.

- Démarrez en premier la machine source.
- Une fois la machine démarrée, la VM cible peut à son tour être mise sous tension.

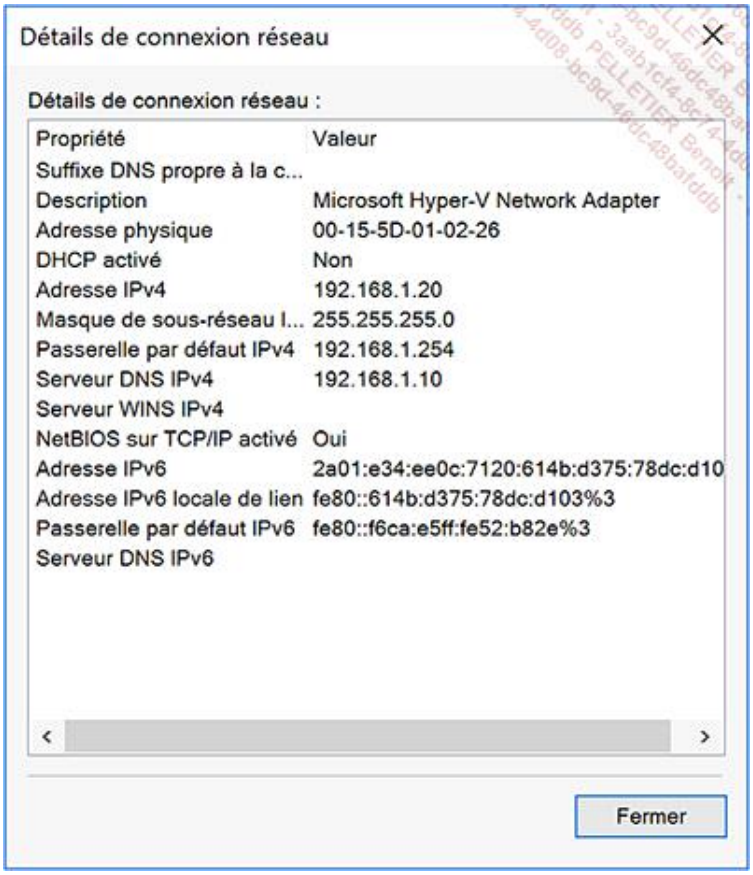
Lors du démarrage, le système détecte la présence du fichier et effectue le clonage.



À la fin de l'opération, on peut vérifier que le nom du poste a bien été configuré.

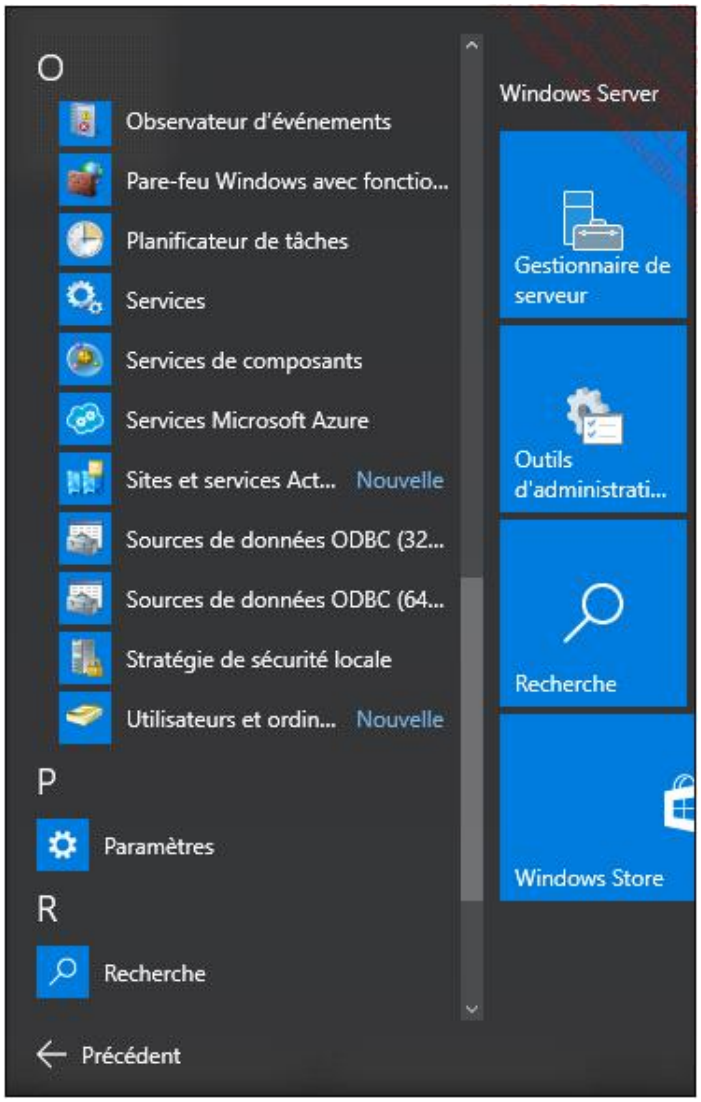


La configuration de la carte réseau est bien celle qui a été spécifiée lors de la création du fichier.



L’adresse du serveur DNS peut maintenant être modifiée afin de mettre AD3 en tant que serveur préféré et AD1 en serveur auxiliaire.

Les rôles DNS et AD DS sont bien présents sur le nouveau contrôleur de domaine.



Enfin, le contrôleur de domaine AD3 a les mêmes propriétés que le serveur AD1 (membre des mêmes groupes de sécurité, catalogue global…).

Gestion des accès privilégiés

Nouvelle fonctionnalité apportée au rôle Active Directory Domain Services dans Windows Server 2016, PAM (*Privileged Access Management* - Gestion des accès privilégiés) permet la gestion des comptes dit « privilégiés ».

Dans un domaine AD, certaines tâches nécessitent de posséder des droits d'administration (Admins du domaine, Administrateur du schéma...). Il n'est pas rare de trouver ces droits affectés directement au compte de l'utilisateur.

Ce type d'autorisation peut causer de gros problèmes de sécurité, les processus et applications utilisant les droits de l'utilisateur. Ainsi un malware ou autre virus a la possibilité de se déployer beaucoup plus simplement sur l'ensemble du réseau.

Cette nouvelle fonctionnalité ajoutée à Windows Server 2016 offre à l'équipe IT la possibilité de gérer plus simplement cette problématique de droit. Par défaut, aucun compte utilisateur ne possède de droits d'administrateur.

De plus, elle donne la possibilité de faire la demande d'un droit d'administration (lors de la création de compte, par exemple). L'approbation pourra être effectuée de manière manuelle ou automatique, la personne ayant initié la demande se verra octroyer le droit pour une durée limitée.

Il est intéressant de noter qu'une granularité au niveau des droits sera mise en place. L'utilisateur ne recevra donc pas les droits complets d'administrateur mais plutôt l'autorisation d'effectuer certaines tâches.

Mise à niveau d'un contrôleur de domaine 2012 R2

L'Active Directory est très souvent un point central pour l'accès aux applications et autres services mis en place. Ainsi, lors de la mise à niveau des contrôleurs de domaine, il est important de valider certaines tâches.

1. Audit de l'état de santé

L'audit de l'état de santé est un des points les plus importants car il va permettre de valider la mise à niveau des contrôleurs de domaine. En effet, il n'est pas recommandé d'effectuer ce type d'opération si un composant Active Directory ou la réplication subit des dysfonctionnements.

La première étape va être de valider le fonctionnement de différentes applications utilisant l'annuaire avec le nouveau système d'exploitation.

Prenons comme exemple Exchange 2016 : il est nécessaire d'installer la Rollup Update 3 ou supérieure pour un bon fonctionnement en AD Windows Server 2016.

Un inventaire logiciel à jour permet de valider rapidement cette étape.

Une fois l'étape de compatibilité validée, il est nécessaire de prendre en compte l'état de santé des contrôleurs de domaine. Pour cela, plusieurs commandes doivent être exécutées :

- Repadmin
- Gpotool
- W32tm
- Dcdiag

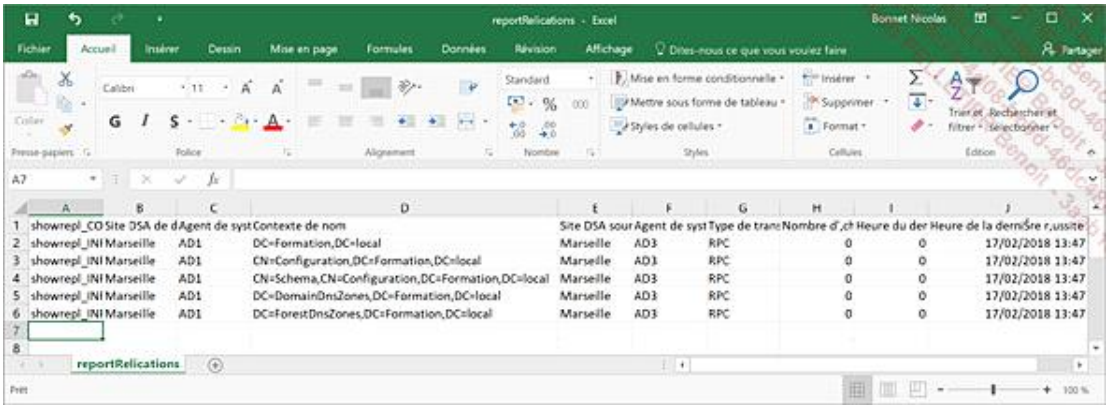
Repadmin

À l'aide de cette commande, il est possible de s'assurer du bon fonctionnement des réplications AD. Comme nous l'avons vu plus haut dans ce chapitre, deux types de réplication s'opèrent dans un domaine AD.

La commande ci-dessous permet donc d'obtenir un fichier csv qui va nous permettre de voir très rapidement l'état des réplications.

```
Repadmin /showrepl * /csv > C:\reportRelications.txt
```

Ouvrez le fichier txt avec Excel puis dans l'assistant sélectionnez une séparation à l'aide de la virgule. Le résultat est le suivant.



	A	B	C	D	E	F	G	H	I	J
1	showrepl_CO	Site DSA de d	Agent de syst	Contexte de nom	Site DSA sour	Agent de syst	Type de trans	Nombre d'ch	Heure du der	Heure de la dernière r,ussite
2	showrepl_INI	Marseille	AD1	DC=Formation,DC=local	Marseille	AD3	RPC	0	0	17/02/2018 13:47
3	showrepl_INI	Marseille	AD1	CN=Configuration,DC=Formation,DC=local	Marseille	AD3	RPC	0	0	17/02/2018 13:47
4	showrepl_INI	Marseille	AD1	CN=Schema,CN=Configuration,DC=Formation,DC=local	Marseille	AD3	RPC	0	0	17/02/2018 13:47
5	showrepl_INI	Marseille	AD1	DC=DomainDnsZones,DC=Formation,DC=local	Marseille	AD3	RPC	0	0	17/02/2018 13:47
6	showrepl_INI	Marseille	AD1	DC=ForestDnsZones,DC=Formation,DC=local	Marseille	AD3	RPC	0	0	17/02/2018 13:47
7										
8										

Si un problème de réplication est présent, il est nécessaire d'investiguer et de le corriger. Dans le cas contraire, les autres tests peuvent être exécutés.

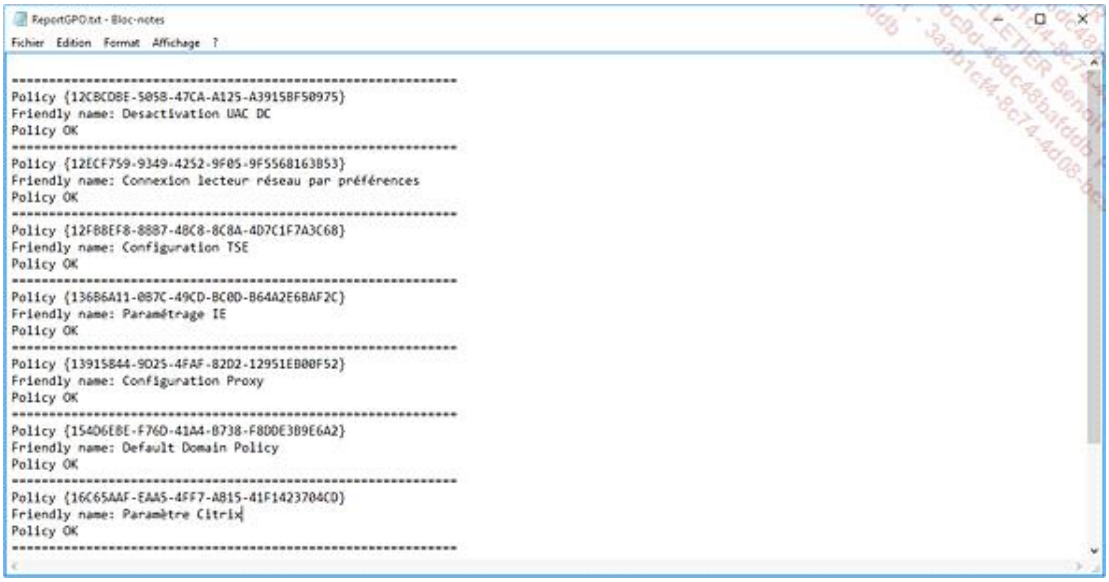
Gpotool

Une fois la réplication validée, il est nécessaire de valider la partie sysvol (réplication FRS ou DFSR). Également importante, elle peut contenir une partie des stratégies de groupe. Une mauvaise réplication peut causer des incohérences au niveau d'une ou plusieurs stratégies de groupe.

L'outil gpotool peut être utilisé, ce dernier est disponible en téléchargement sur le blog de l'auteur http://www.nibonnet.fr/?p=272. Il permet de valider en comparant les informations présentes dans l'annuaire Active Directory et celles dans Sysvol. Ce point sera abordé dans le chapitre traitant de la stratégie de groupe.

Après avoir exécuté la commande ci-dessous, un fichier log est créé.

```
gpotool > c:\reportgpo.txt
```



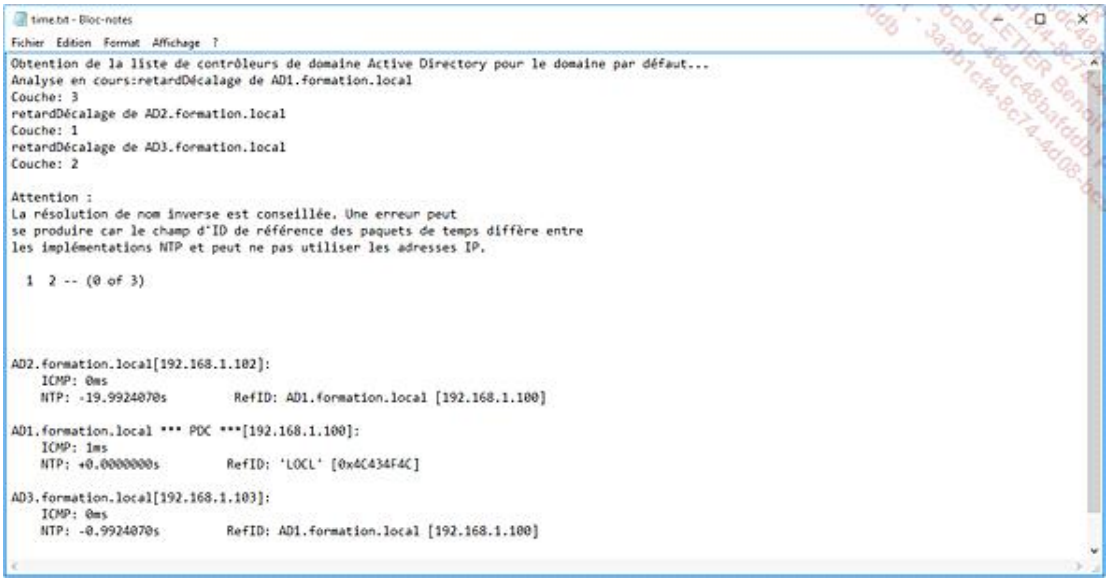
```
ReportGPO.txt - Bloc-notes
Fichier  Edition  Format  Affichage  ?

----------------------------------------------------------------
Policy {12CBCDBE-5058-47CA-A125-A39158F50975}
Friendly name: Desactivation UAC DC
Policy OK
----------------------------------------------------------------
Policy {12ECF759-9349-4252-9F05-9F5568163B53}
Friendly name: Connexion lecteur réseau par préférences
Policy OK
----------------------------------------------------------------
Policy {12FB8EF8-8887-48C8-8C8A-4D7C1F7A3C68}
Friendly name: Configuration TSE
Policy OK
----------------------------------------------------------------
Policy {136B6A11-0B7C-49CD-BC0D-B64A2E6BAF2C}
Friendly name: Paramétrage IE
Policy OK
----------------------------------------------------------------
Policy {13915844-9D25-4FAF-82D2-12951EB0BF52}
Friendly name: Configuration Proxy
Policy OK
----------------------------------------------------------------
Policy {154D6E8E-F76D-41A4-B738-F8DDE3B9E6A2}
Friendly name: Default Domain Policy
Policy OK
----------------------------------------------------------------
Policy {16C65AAF-EAA5-4FF7-A815-41F1423704CD}
Friendly name: Paramètre Citrix
Policy OK
----------------------------------------------------------------
```

W32tm

La synchronisation de l'horloge peut désormais être abordée. En effet, il est très important de s'assurer du bon fonctionnement de ce composant. Pour cela, la commande `w32tm /monitor` peut être utilisée.

Le résultat sera le suivant :



Dcdiag

Le dernier test va consister à vérifier l'état de tous les composants de l'annuaire. Pour cela, la commande dcdiag doit être utilisée. Cette dernière va soumettre l'ensemble des contrôleurs de domaines à une batterie de test.

Pour s'assurer du bon fonctionnement de vos contrôleurs de domaine, utilisez la commande ci-dessous :

```
Dcdiag /V /C /D /E > c:\dcdiag.txt
```

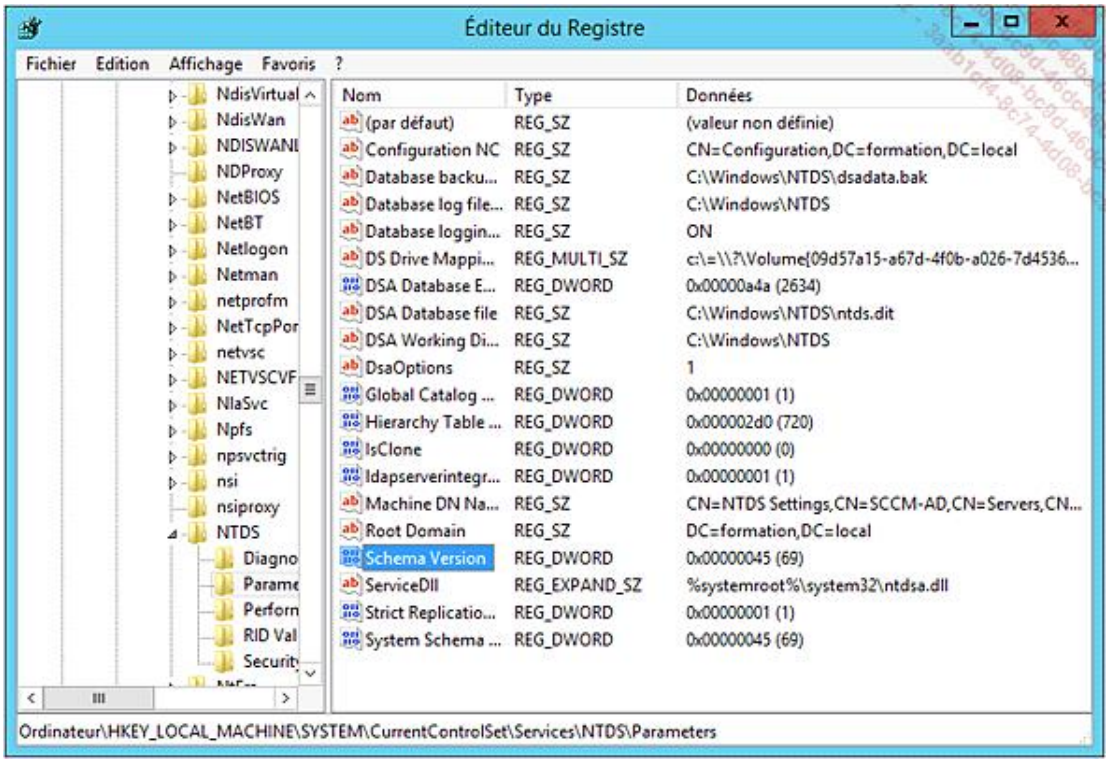
Une fois l'exécution terminée, analyser finement le résultat de tous les tests. En cas d'échec, il est important de comprendre la cause de celui-ci et d'identifier la gravité. Il est conseillé de traiter les problèmes de gravités importantes avant toute mise à niveau.

Attention certaines applications (Exchange par exemple) peuvent nécessiter un certain niveau de Service Pack pour être compatibles avec le nouvel annuaire. En cas de mise à niveau depuis Windows Server 2008 R2, il est nécessaire de s'assurer que la compression de SID (apparu avec Windows Server 2012) soit compatible avec votre baie SAN, votre NAS ou autre équipement.

2. Mise à jour du schéma

Après avoir passé la phase d'audit, le schéma Active Directory peut être mis à jour. Il est conseillé d'effectuer cette étape à la main afin d'obtenir un retour de la commande (il est également possible de le faire de manière automatique en utilisant l'assistant de promotion). Ainsi, en cas d'échec, l'opération d'analyse du problème sera plus aisée.

En accédant à la valeur Dword Schema Version, on peut visualiser la version du schéma. Si la valeur est égale à 69, le schéma est en version 2012 R2.

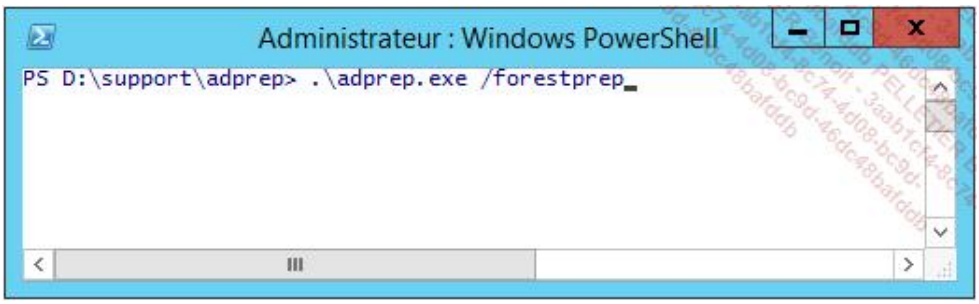


Sur le contrôleur de domaine possédant le rôle **FSMO Maître de schéma**, ouvrez une session avec un compte administrateur possédant le droit **administrateur du schéma ou administrateur de l'entreprise**.

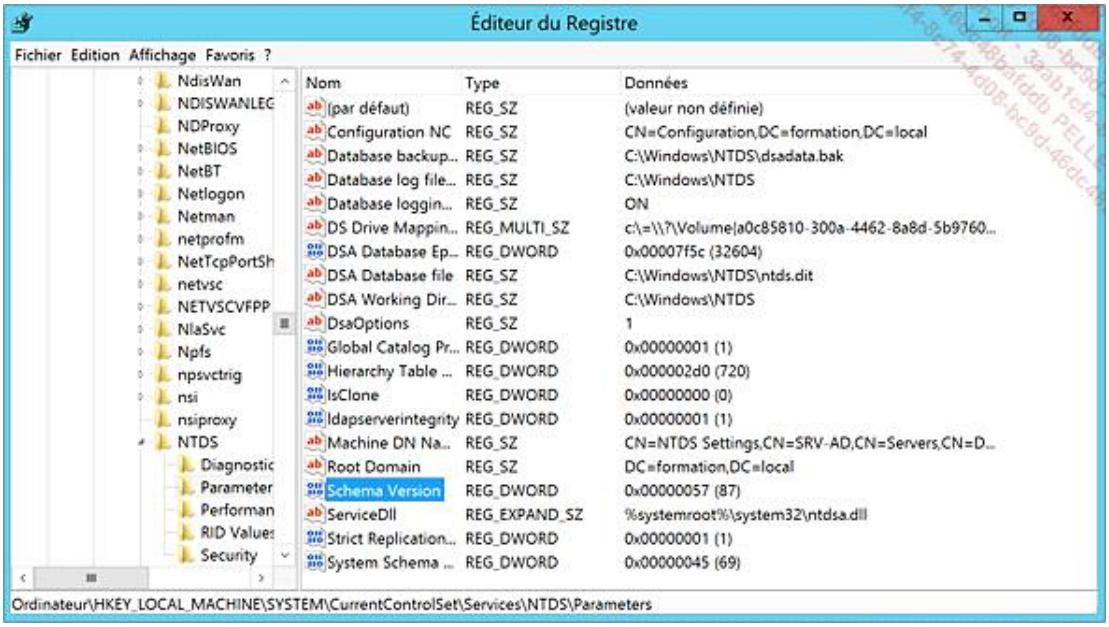
Par défaut le compte administrateur est membre de ces deux groupes. Après avoir connecté l'ISO (ou inséré le DVD pour un serveur physique) de Windows Server 2016, lancez une invite de commandes puis accédez au dossier d:\support\adprep

Remplacer d: par la lettre du lecteur de DVD.

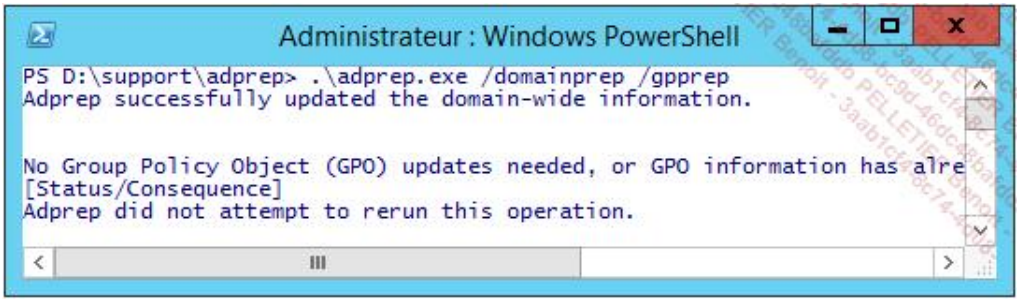
Exécutez la commande `adprep.exe /forestprep`, afin de mettre à jour le schéma.



La valeur DWORD possède désormais la valeur 87.



Sur le contrôleur de domaine possédant le rôle de maître d'infrastructure, exécutez la commande `adprep /domainprep /gpprep`.



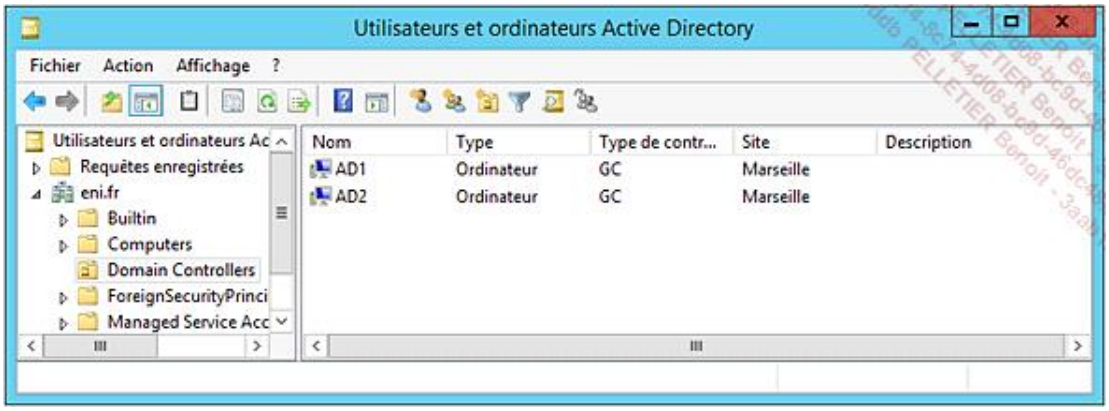
3. Mise à niveau des contrôleurs de domaine

L'opération de mise à niveau peut maintenant être effectuée. Cette dernière va consister à ajouter de nouveaux serveurs dans la forêt en remplacement des anciens. Une fois ces derniers supprimés, la répartition des rôles FMSO ainsi que la configuration du serveur de temps pourra être opérée.

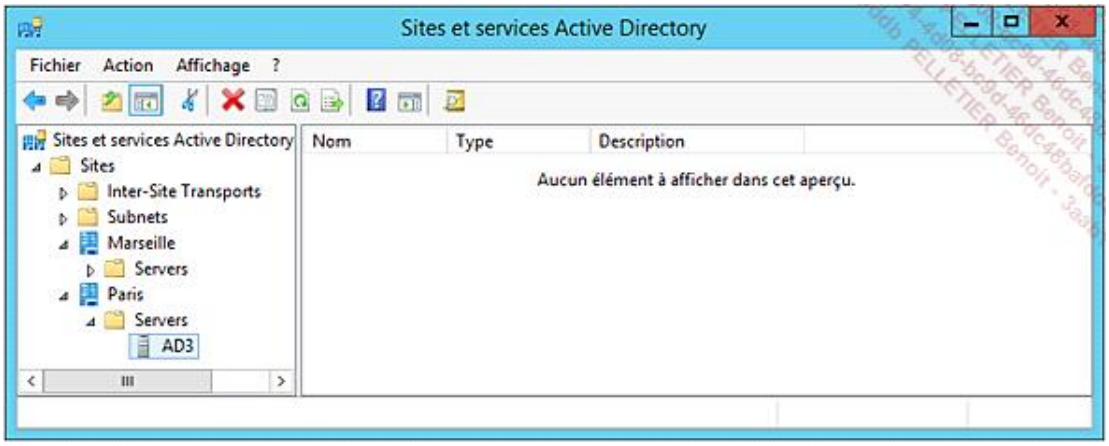
Afin de pouvoir récupérer le nom et l'adresse IP des anciens serveurs, nous allons dans un premier temps positionner l'ensemble des rôles FSMO sur un des contrôleurs de domaine. Ce dernier sera rétrogradé en dernier.

Effectuez la rétrogradation du premier serveur puis sortez-le du domaine et supprimez son compte d'ordinateur.

L'unité d'organisation Domain Controllers ne contient désormais plus que deux contrôleurs de domaine.



Dans la console **Sites et services Active Directory**, supprimez **AD3**.



Après avoir donné l'IP et le nom de l'ancien serveur AD3 au serveur exécutant Windows Server 2016, effectuez la promotion de ce dernier. Depuis l'assistant de promotion, positionnez-le directement dans le site AD adéquat.

Effectuez la même opération pour le serveur AD2 afin qu'il ne reste plus qu'un contrôleur de domaine sous Windows Server 2012 R2 dans la forêt.

Avant la rétrogradation du serveur AD1, il est nécessaire de distribuer les rôles FSMO. Pour cela, vous pouvez utiliser la KB Microsoft ci-dessous : https://support.microsoft.com/fr-fr/kb/223346

Ainsi les bonnes pratiques seront respectées. La rétrogradation du contrôleur de domaine peut être effectuée, néanmoins il est conseillé de ne pas procéder à l'élévation du niveau fonctionnel. Il est préférable d'attendre un délai de 10 heures minimum, ceci afin de s'assurer qu'aucun dysfonctionnement applicatif n'a lieu lors de l'utilisation des tickets kerberos fournit par les nouveaux serveurs d'annuaires.

Si aucun dysfonctionnement n'est détecté, la promotion du troisième et dernier serveur peut être effectuée. Par la suite, l'élévation du niveau fonctionnel du domaine et de la forêt peut être opérée.

La mise à niveau est maintenant terminée, l'ensemble des serveurs d'annuaire exécutent Windows Server 2016.

Utilisation de Azure Active Directory

Cette section du chapitre traitant d'Active Directory présente la partie Azure Active Directory. Pour les lecteurs souhaitant mettre en place cette fonctionnalité, il est nécessaire de créer un compte démo sur le portail d'Azure puis d'activer la version d'évaluation d'Azure AD Premium.

La plateforme Azure offre de nombreuses fonctionnalités dont la possibilité d'utiliser un annuaire Active Directory. Il permet ainsi la gestion des identités pour toutes les activités dans le cloud (accès aux applications SAAS…). Généralement synchronisé avec un annuaire *on-premises* (présent dans le réseau local de l'entreprise), il offre également la possibilité de procéder à la création de comptes utilisateurs et groupes depuis l'interface. Trois éditions sont disponibles :

- Free (gratuite)
- De base
- Premium

La version Premium est celle qui offre le plus de services.

Documentation des différentes versions :

https://azure.microsoft.com/fr-fr/documentation/articles/active-directory-editions/

1. Fonctionnalités offertes par Azure AD

Azure AD est utilisé par des services en ligne tels que Office 365 ou Intune pour l'autorisation d'accès au service. La fonctionnalité d'authentification forte vient compléter la gestion des identités. Il est en effet possible d'activer pour certains utilisateurs l'obligation d'utiliser une authentification à deux facteurs (authentification forte).

En plus de leur couple login/mot de passe, une partie ou l'ensemble des utilisateurs devront utiliser un deuxième mécanisme d'authentification. Ce dernier peut être une application installée sur un smartphone qui fournit un code. Celui-ci possède une durée de vie très courte. Il est également possible de recevoir un SMS contenant un code à saisir. La troisième solution va consister à valider son identité par la réception d'un appel téléphonique et la pression d'une touche du téléphone.

L'édition Premium offre un portail web permettant la mise en place de délégation. Il est ainsi possible de permettre aux utilisateurs d'effectuer le changement de mot de passe ou la création de groupes d'utilisateurs.

Avec Windows 10, une entreprise peut intégrer les postes directement dans l'annuaire Azure AD. Dans ce cas, il n'est pas possible de l'intégrer au domaine AD de l'entreprise.

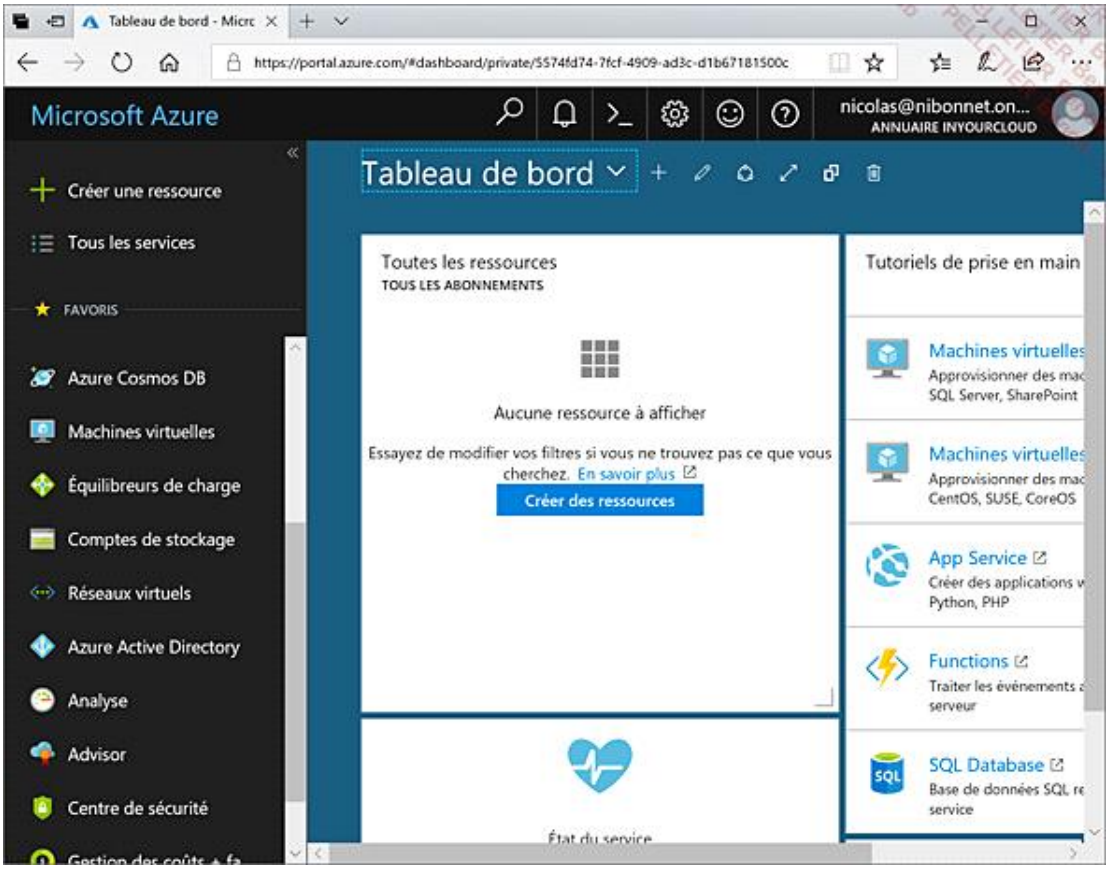
Les étapes permettant d'intégrer des postes Windows 10 à Azure AD sont détaillées plus loin dans ce chapitre. Le sujet est également traité sur le blog de l'auteur : http://www.nibonnet.fr/?p=1169.

2. Synchronisation d'un annuaire local

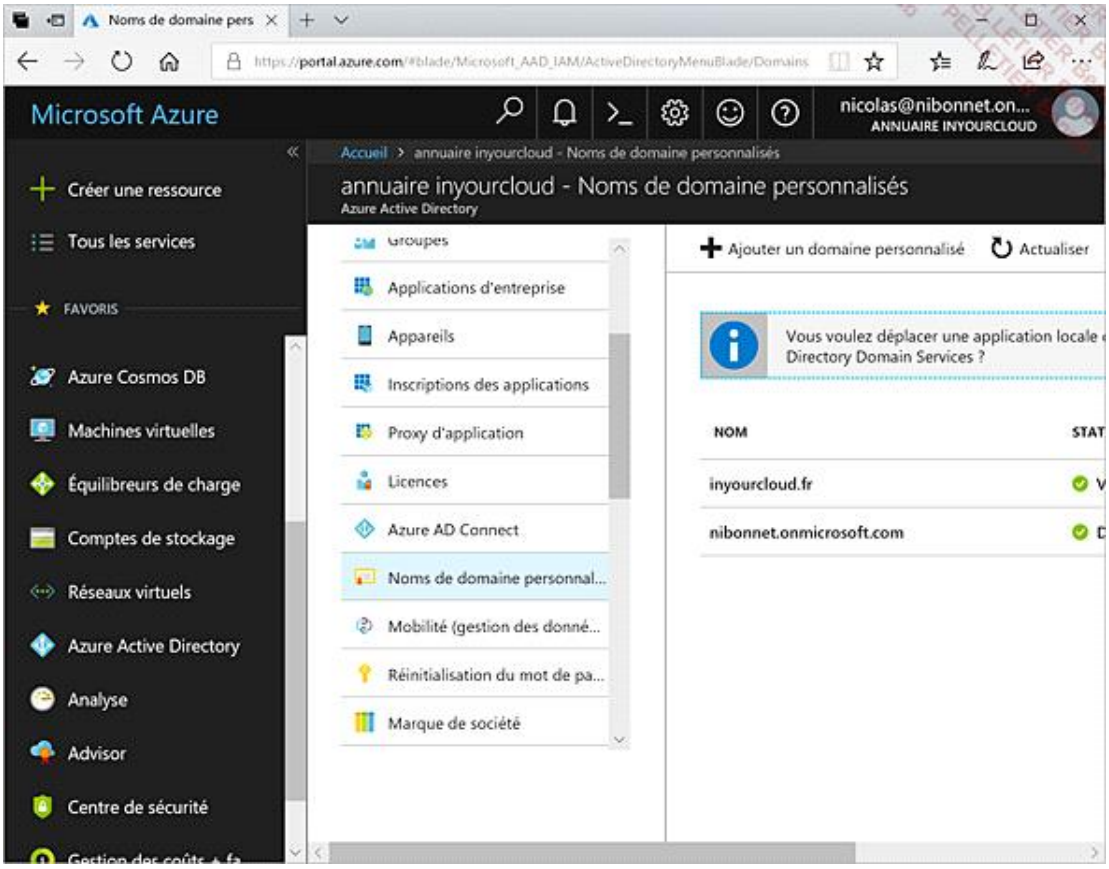
Il est intéressant de synchroniser un annuaire AD avec celui dans Azure. Ceci permet d'assurer l'authentification unique dans le réseau local ou depuis un équipement mobile (ordinateur portable, smartphone). Ainsi l'utilisateur utilisera son login/mot de passe pour accéder aux ressources présentes dans Azure.

Avant de pouvoir synchroniser l'annuaire Active Directory, il est nécessaire d'ajouter le nom de domaine à utiliser.

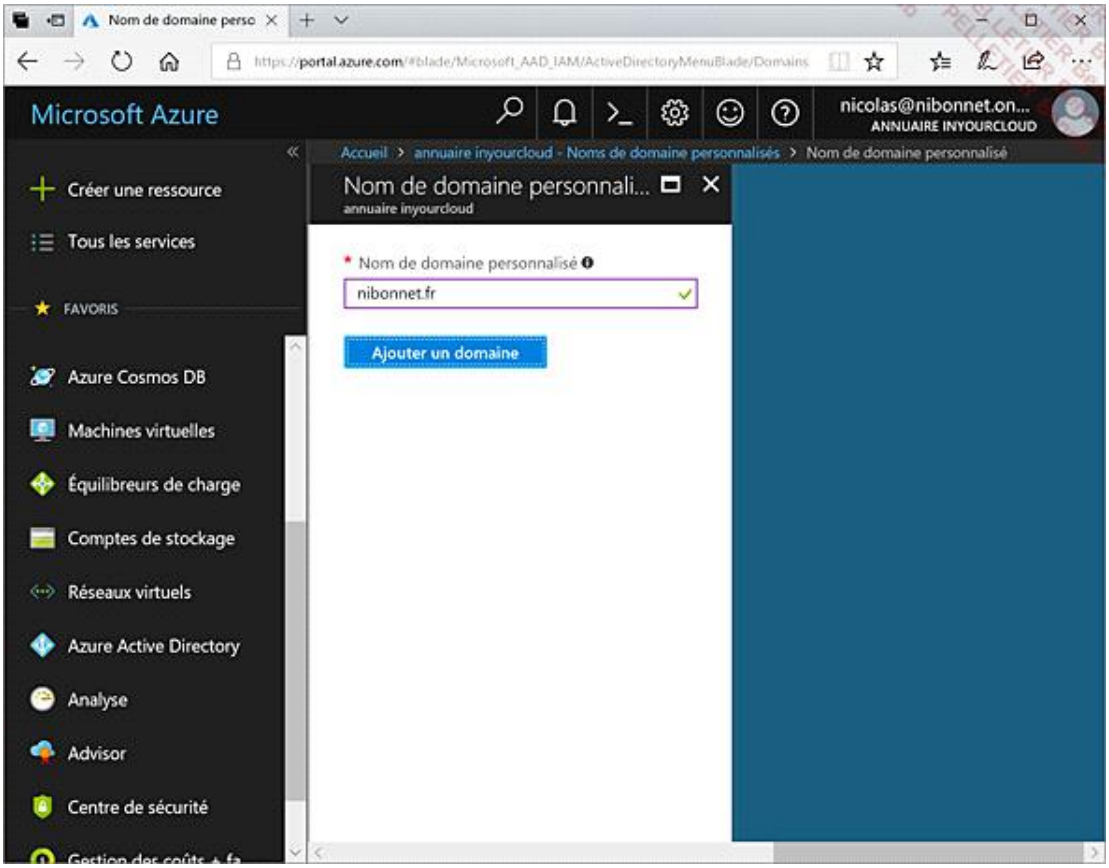
- Depuis la console Azure (azure.microsoft.com), accédez à la fonctionnalité Azure Active Directory en cliquant dessus sur le bandeau de gauche.



- Un menu s'affiche, cliquez sur **Noms de domaine personnalisés**.



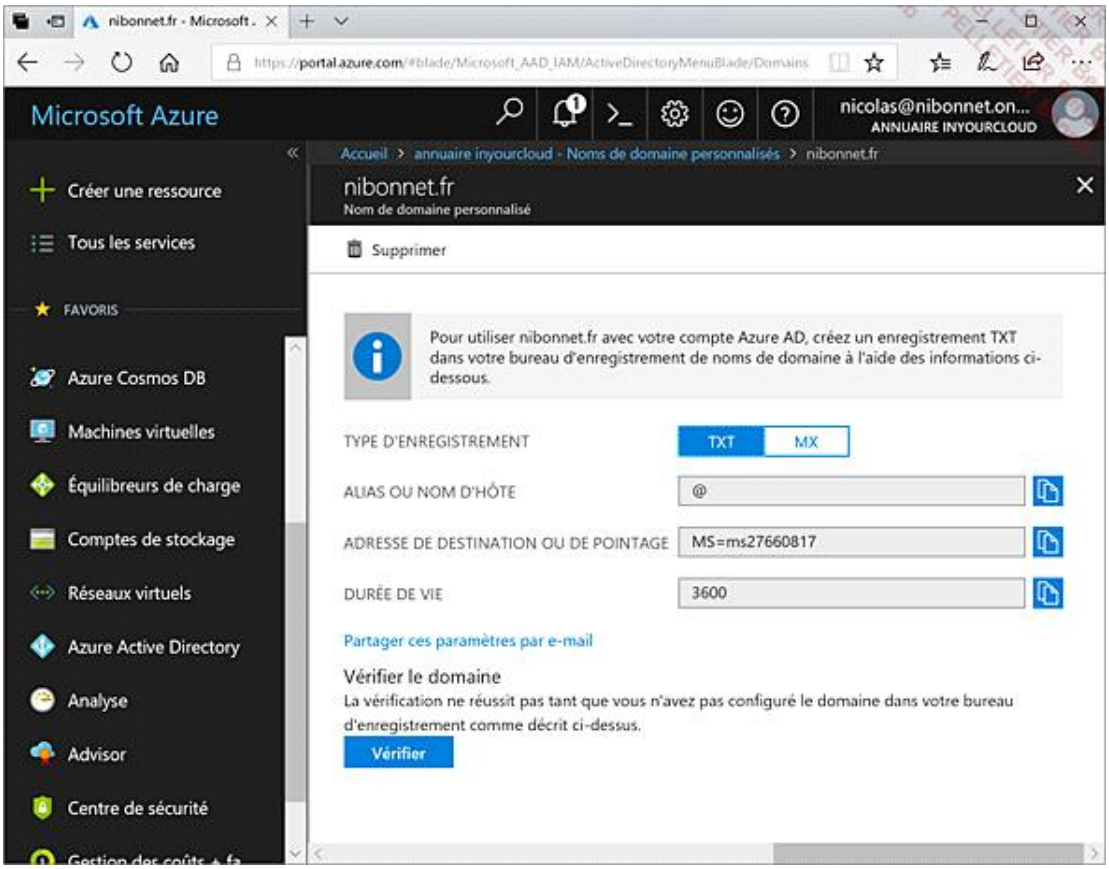
Cliquez sur **Ajouter un domaine personnalisé** puis ajoutez le nom de domaine. Cliquez ensuite sur le bouton **Ajouter un domaine**.



Il est nécessaire de procéder à l'ajout d'un enregistrement dans le DNS de la zone afin d'effectuer à la vérification

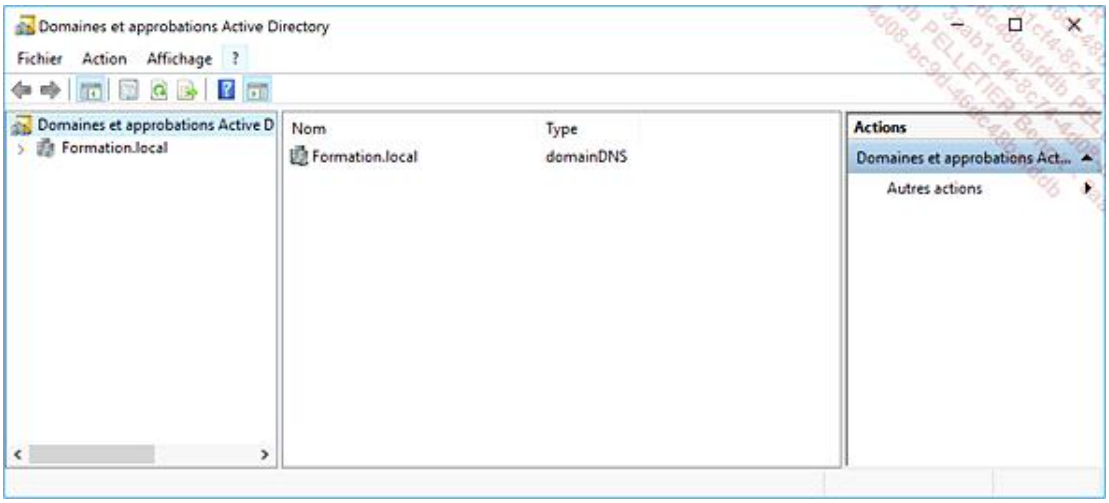
du nom de domaine. Suite à l'ajout, la valeur de l'enregistrement TXT est donnée, l'opération d'ajout s'effectuera dans le DNS de votre register.

- Après avoir ajouté l'enregistrement, cliquez sur le bouton **Vérifier**.

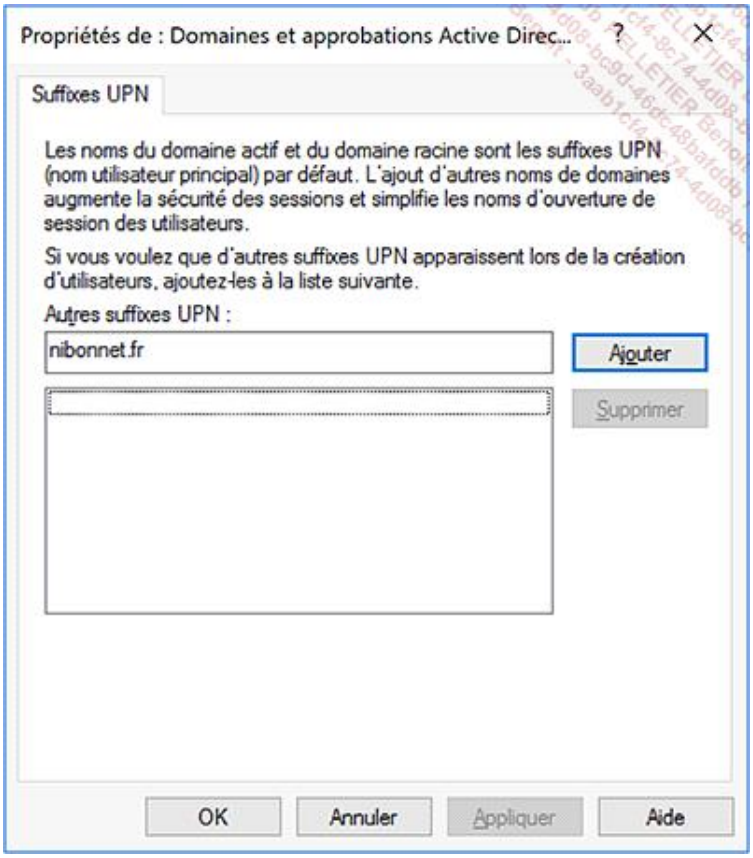


L'UPN (*User Principal Name*) des comptes utilisateurs à synchroniser peut maintenant être modifié. Il est nécessaire dans un premier temps de procéder à l'ajout du nom de domaine précédemment ajouté à Azure.

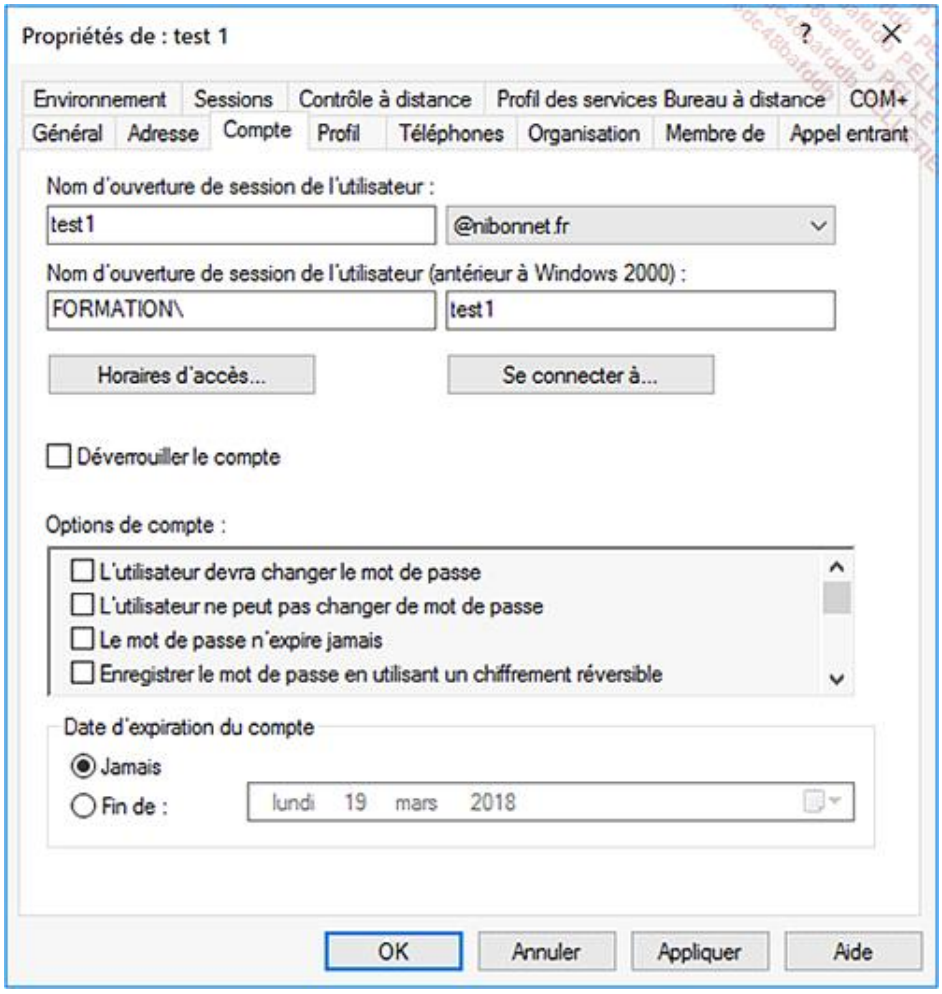
Depuis le contrôleur de domaine, accédez à la console **Domaines et approbations Active Directory**.



- Effectuez un clic droit sur **Domaines et approbations Active Directory** puis cliquez sur **Propriétés**. Ajoutez le nom de domaine puis cliquez sur **Ajouter**. Validez la modification à l'aide du bouton **OK**.

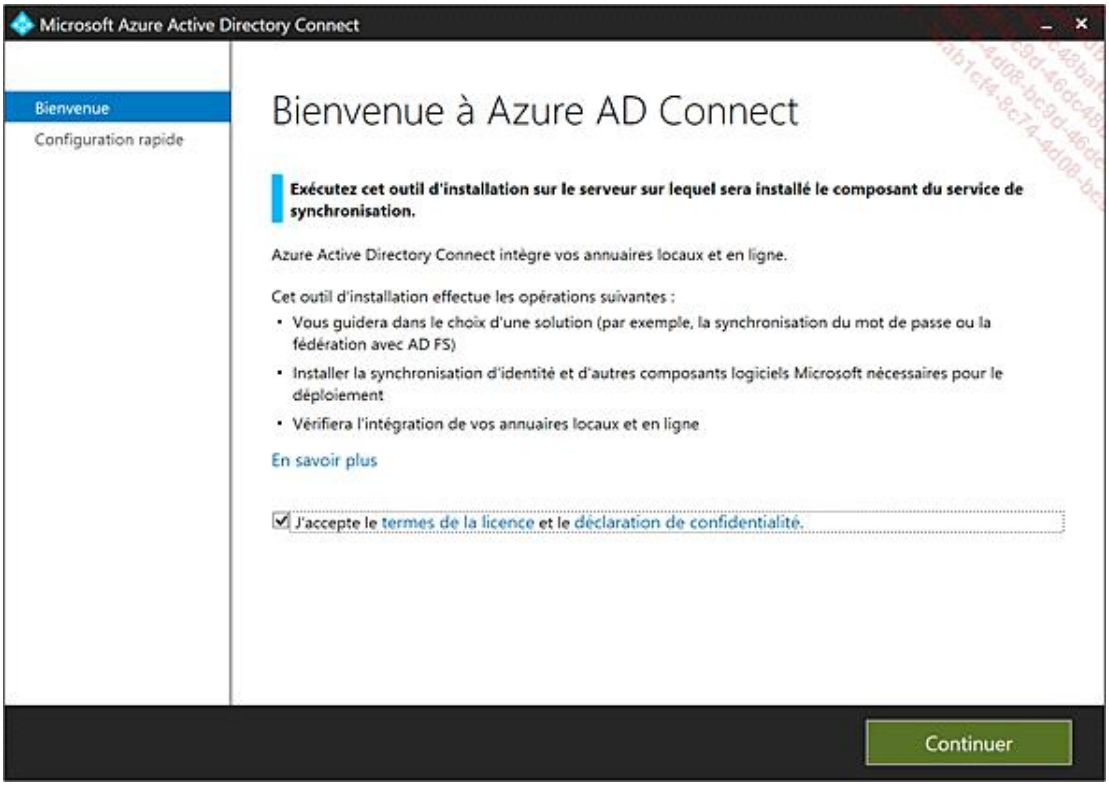


L'UPN peut maintenant être attribué aux utilisateurs qui doivent être synchronisés. Procédez à la création d'un groupe de sécurité puis ajoutez les comptes utilisateurs à synchroniser. Ce groupe sera utilisé pour limiter la synchronisation AD / Azure AD.

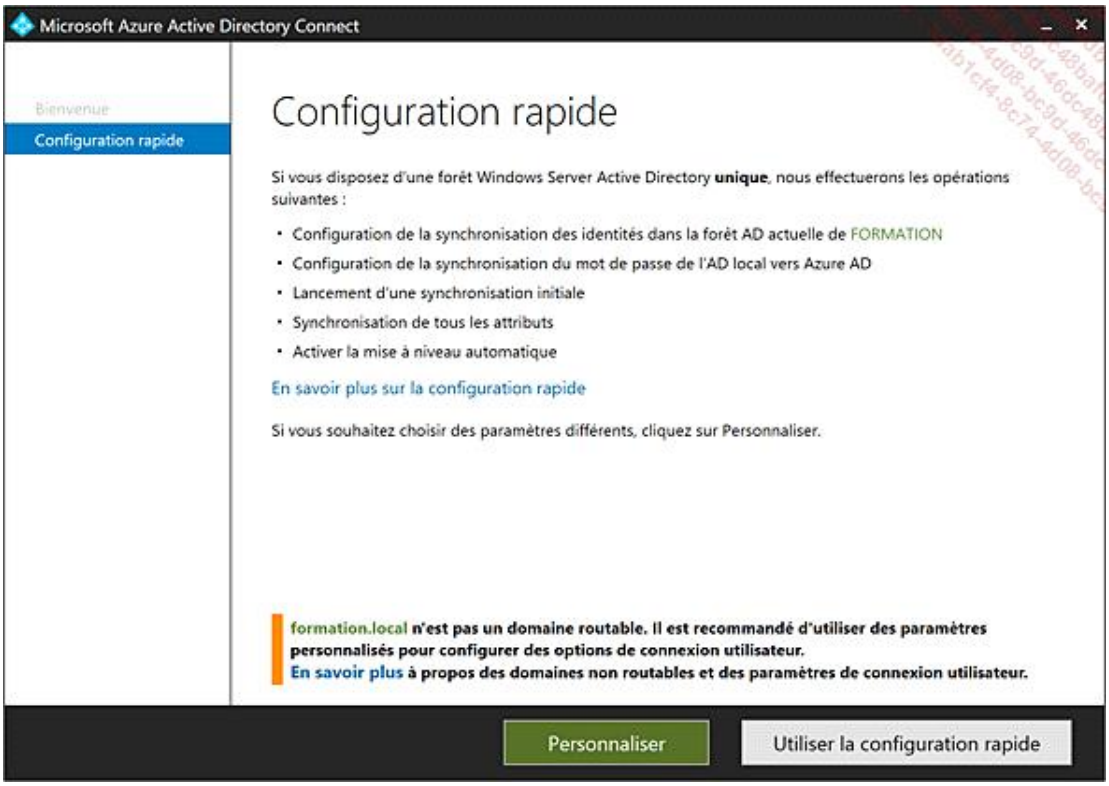


La synchronisation peut maintenant être effectuée. Cette opération se réalise à l'aide de l'outil Azure AD Connect présent à l'adresse ci-dessous : https://www.microsoft.com/en-us/download/details.aspx?id=47594

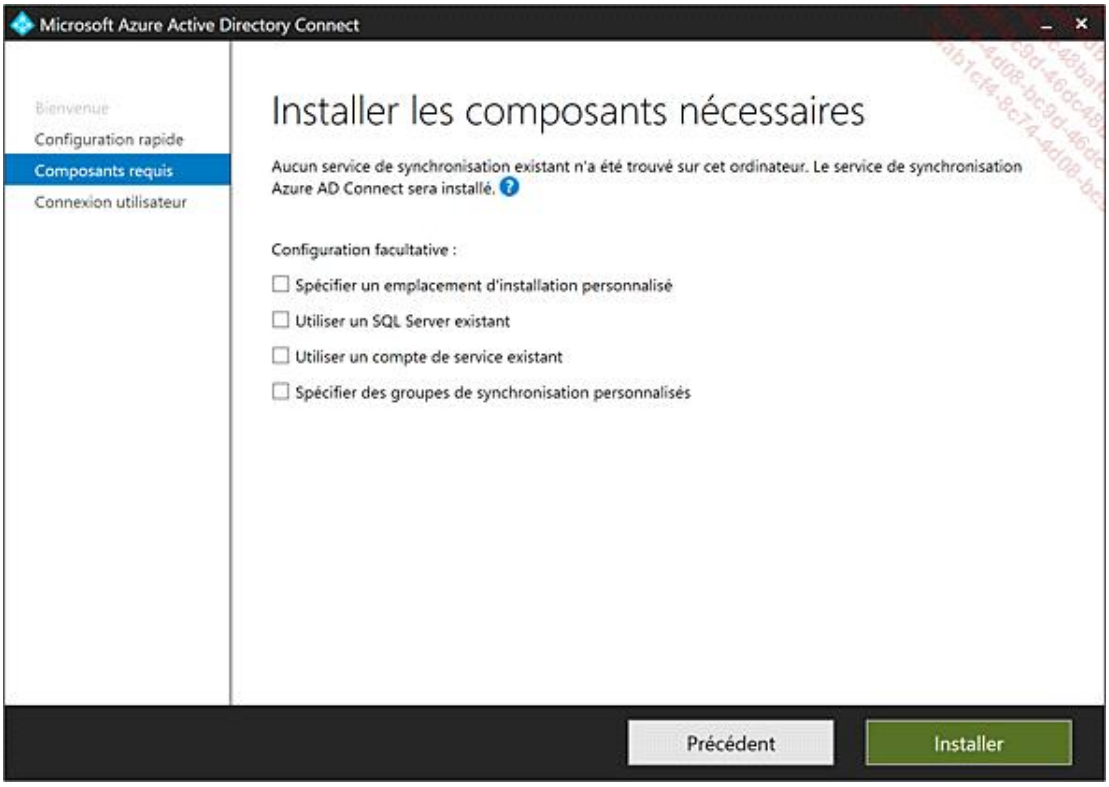
Une fois installé sur le contrôleur de domaine, un assistant se lance. Acceptez la licence puis cliquez sur **Continuer**.



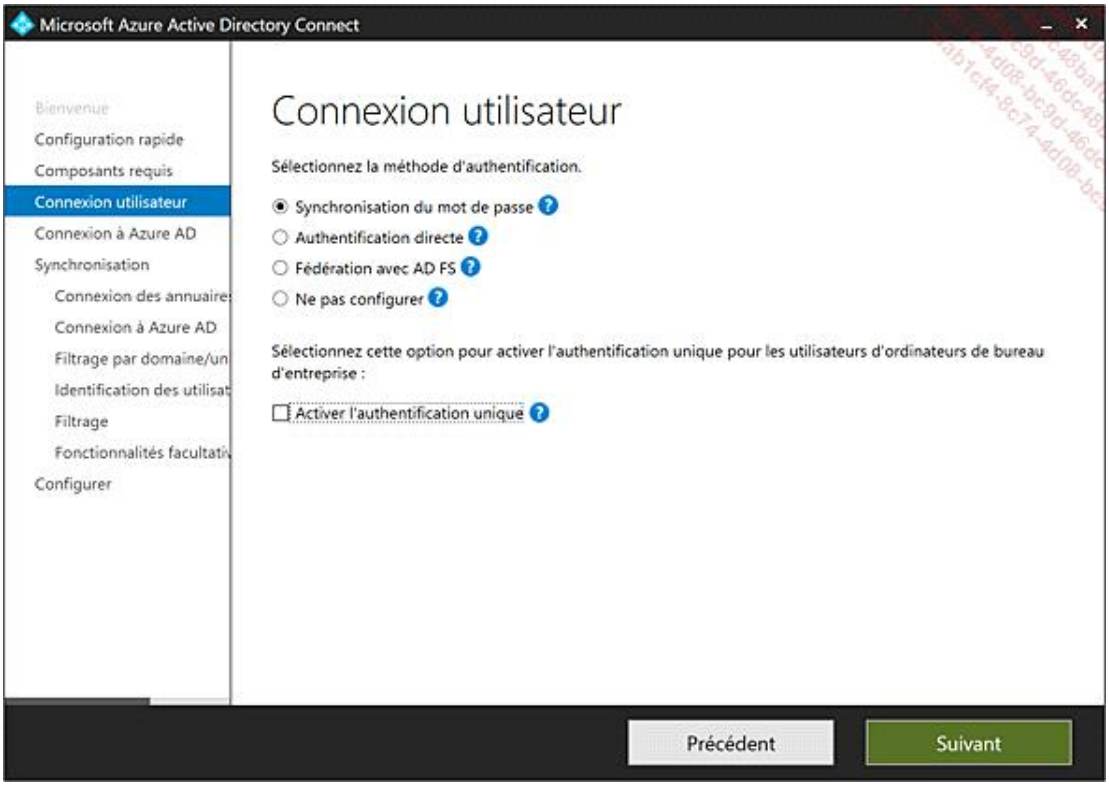
Le bouton **Personnaliser** va permettre de personnaliser l'installation, il est donc intéressant d'utiliser ce type d'installation.



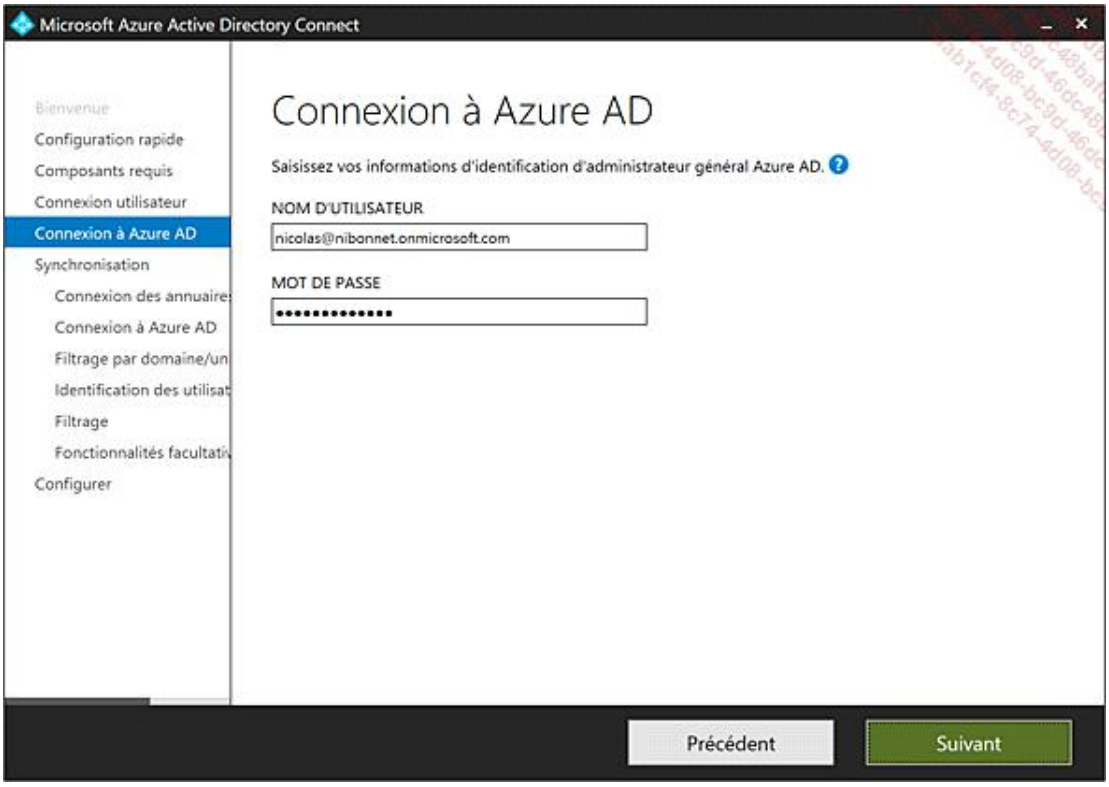
La fenêtre suivante permet l'utilisation d'une base de données SQL particulière ainsi que d'autres options d'installation. Le bouton **Installer** permet de procéder à l'installation des différents composants.



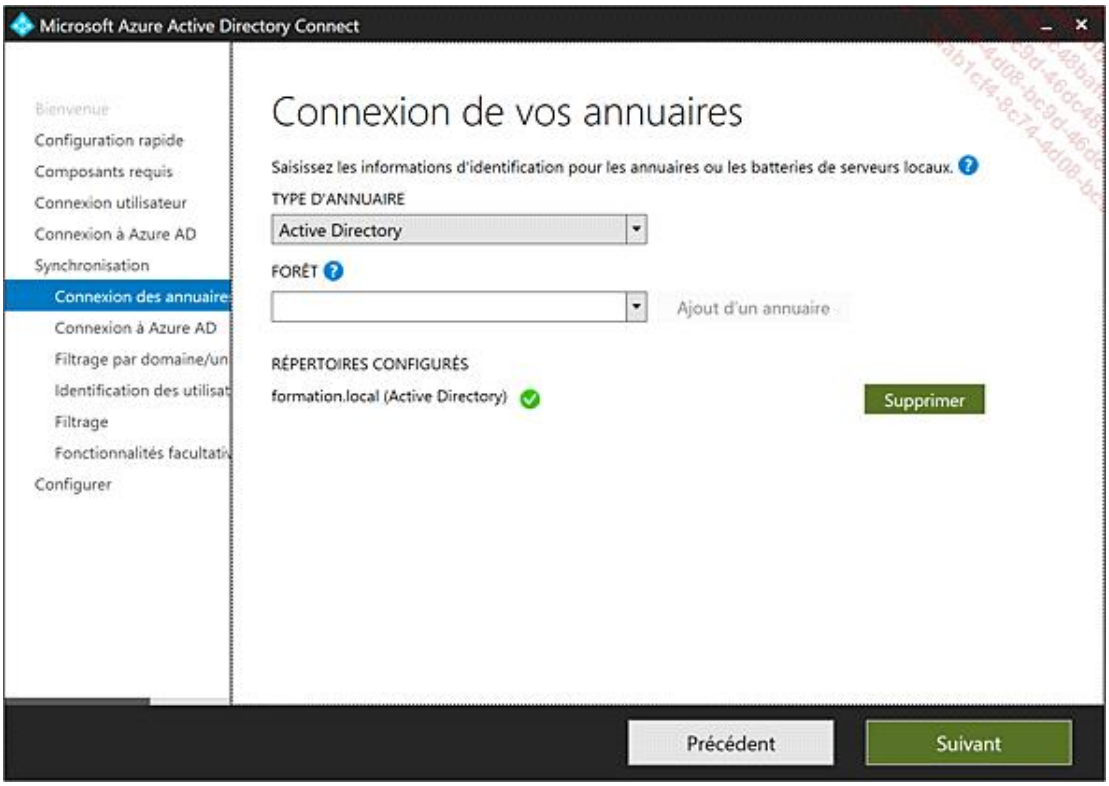
Un système AD FS peut être utilisé pour authentifier les utilisateurs. Il offre la particularité de ne pas stocker les mots de passe dans Azure AD. Dans notre exemple, la deuxième solution, qui consiste à synchroniser les mots de passe, va être utilisée.



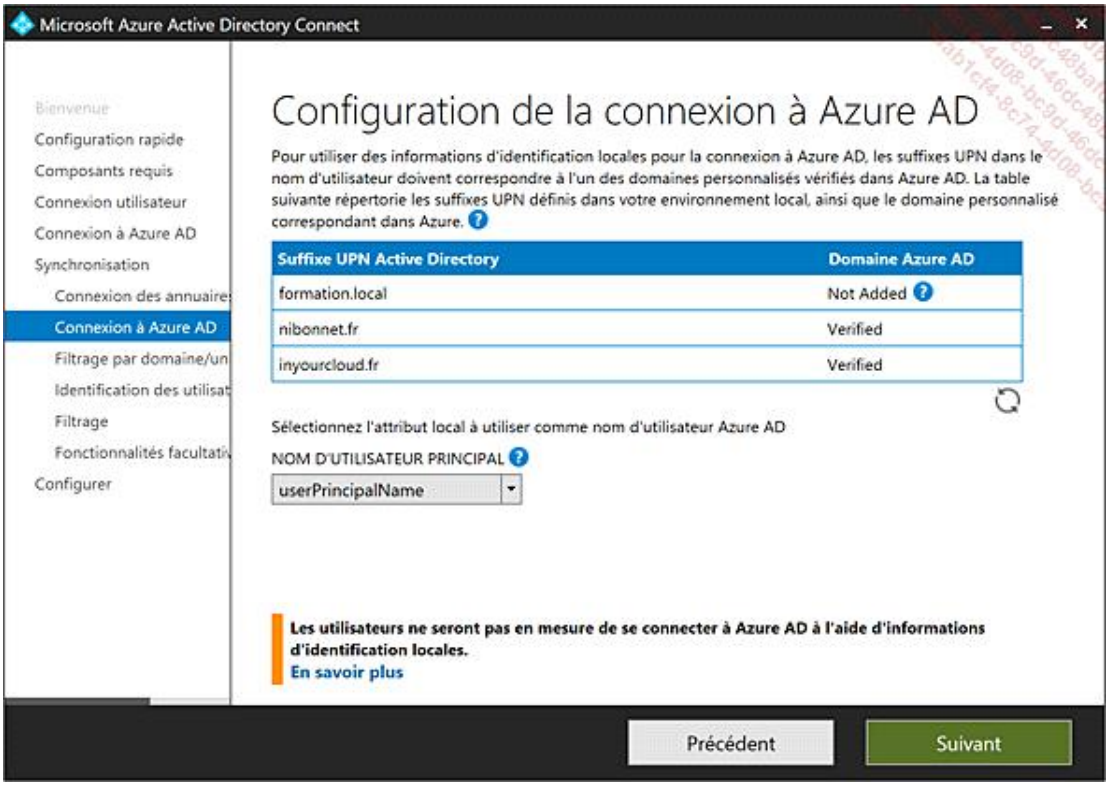
Il est nécessaire de saisir les identifiants d'un compte possédant des droits d'administrateur sur la base de données Azure AD.



Après la validation des identifiants Azure AD, il est nécessaire de cliquer sur **Ajout d'un annuaire** puis, dans la fenêtre qui s'affiche, de saisir les identifiants de l'annuaire local (sous la forme domaine\compte).

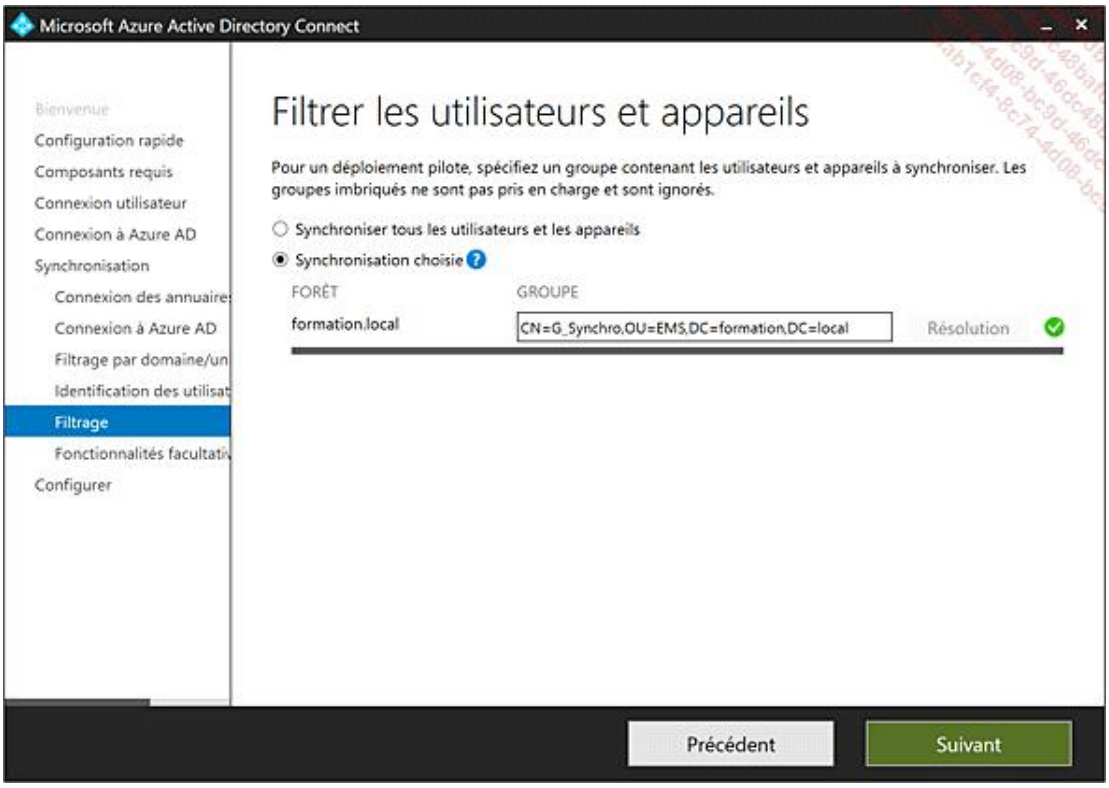


L'attribut local à utiliser est l'UPN (*User Principal Name*). La fenêtre suivante peut donc être validée sans être modifiée.



Les fenêtres **Filtrage par domaine** et **Identification des utilisateurs** n'ont pas besoin d'être modifiées, cliquez sur **Suivant** sans opérer de modification.

Dans le cas où seuls quelques utilisateurs doivent être migrés, il peut être intéressant de synchroniser un groupe d'utilisateur. Ainsi seuls les membres du groupe seront synchronisés.



Il n'est pas nécessaire de saisir le chemin LDAP du groupe. Saisissez le nom du groupe puis cliquez sur **Résolution**.

Les fenêtres suivantes peuvent être validées sans apporter de modifications.

3. Mise en place du Single Sign-on (SSO)

Le Single Sign-on offre aux utilisateurs la possibilité d'être connectés automatiquement aux différents portails cloud de Microsoft (SharePoint Online, Exchange Online…).

Cette fonctionnalité offre l'avantage de ne plus avoir à saisir de mot de passe pour un utilisateur déjà authentifié par les contrôleurs de domaine interne de l'entreprise.

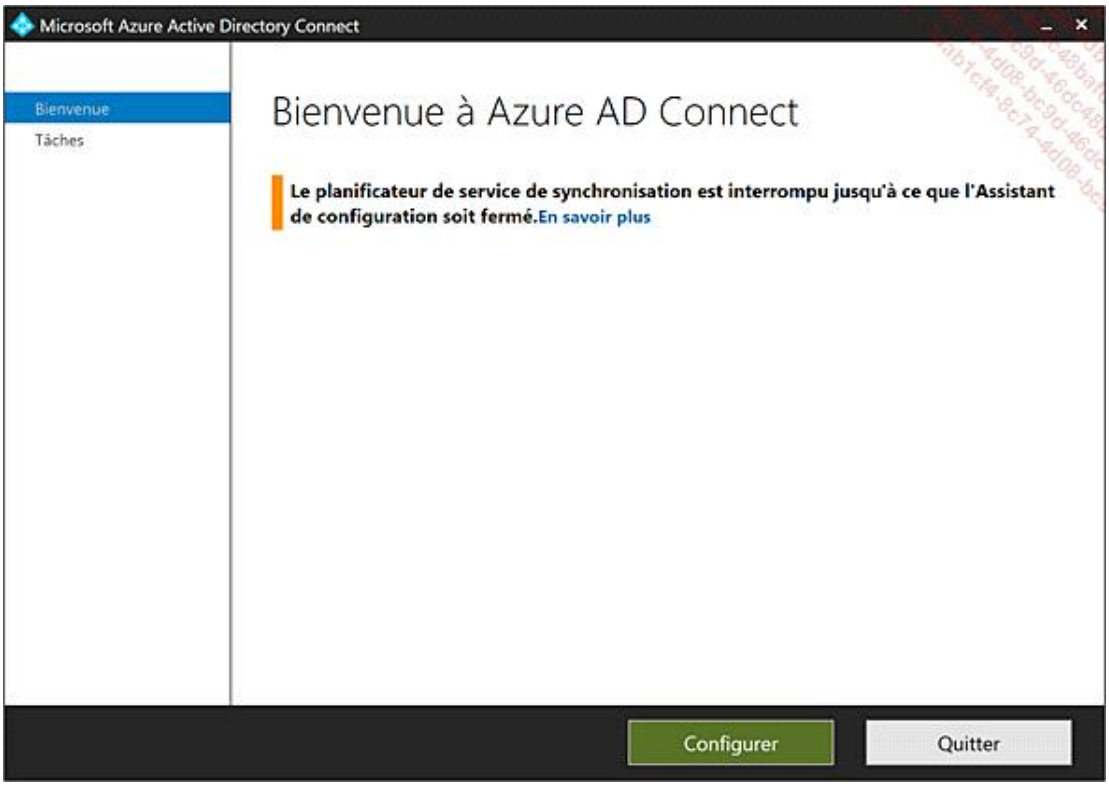
Il est important de noter que cette fonctionnalité n'est pas disponible avec les services de fédération.

La fonctionnalité s'active par l'intermédiaire de Azure AD Connect et ne nécessite pas de version payante de Azure AD.

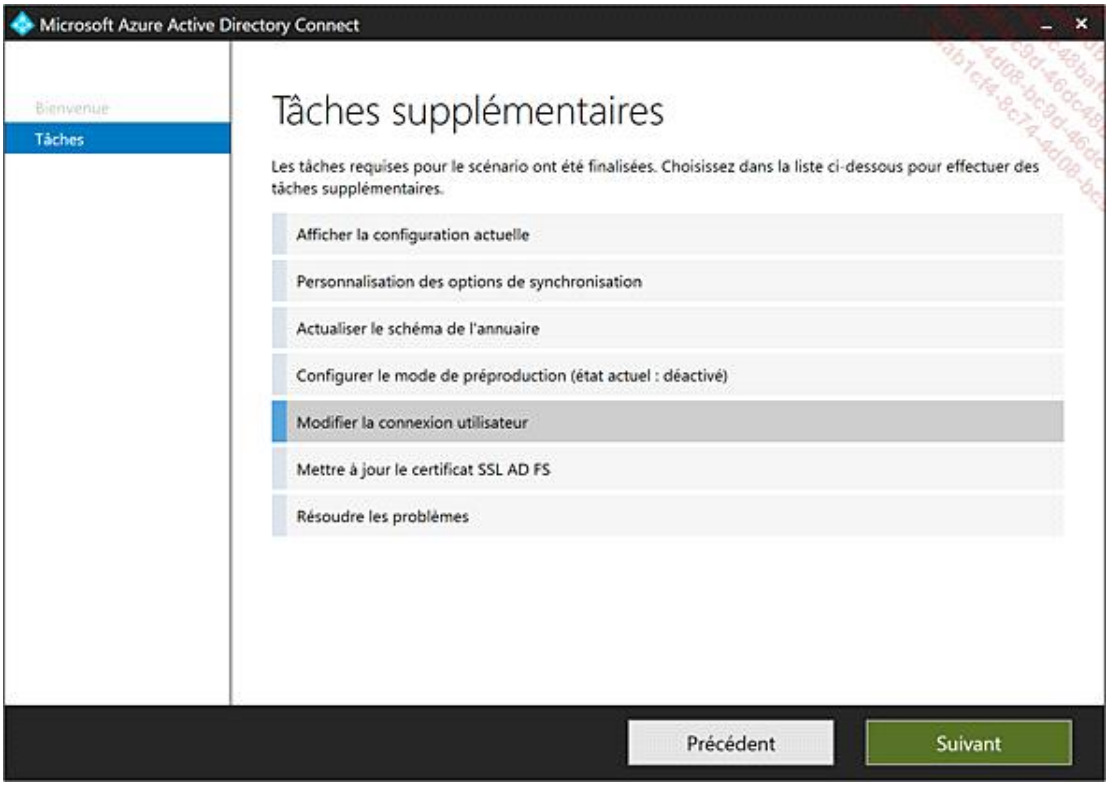
À l'heure où sont écrites ces lignes, tous les navigateurs Internet ne sont pas compatibles avec cette fonctionnalité.

Notez que suite à l'activation de la fonctionnalité, un compte ordinateur est créé. Ce dernier porte le nom AZUREADSSOACC. Il est important de ne pas désactiver ce compte ni de le supprimer.

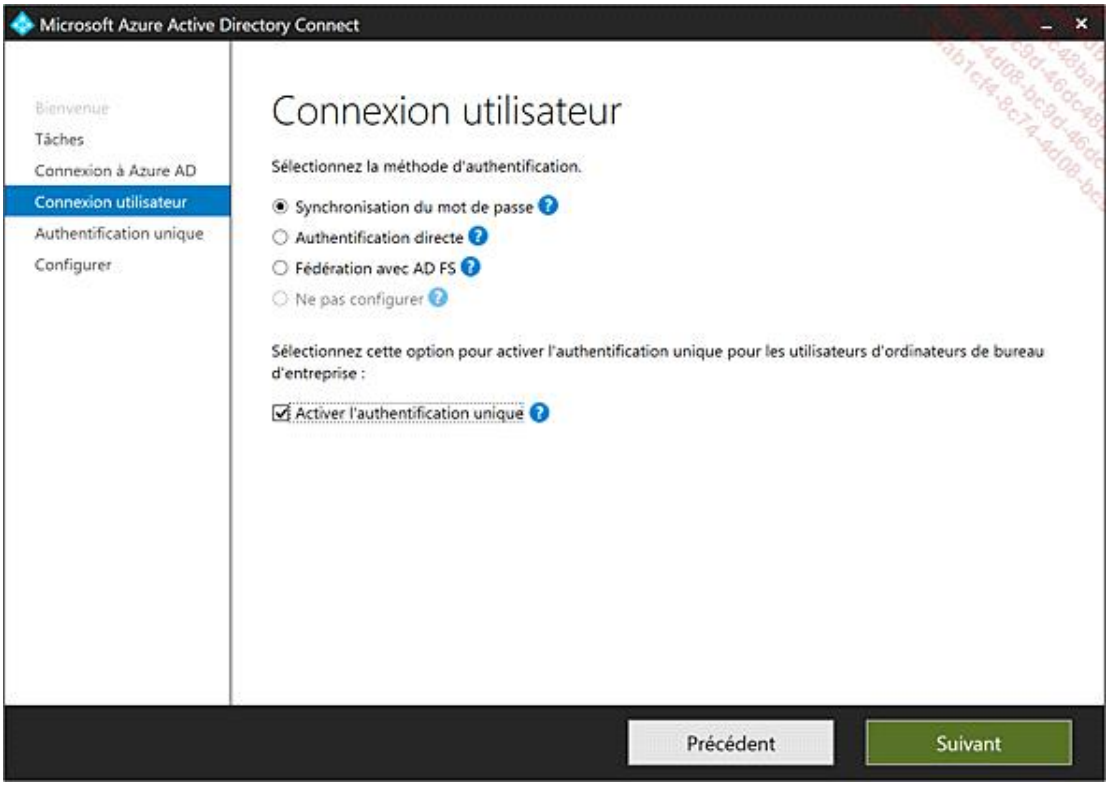
- Depuis le serveur où est installé Azure AD Connect, exécutez l'assistant en double cliquant sur l'icône **Azure AD Connect** présente sur le bureau.
- Un assistant s'affiche, cliquez sur **Configurer**.



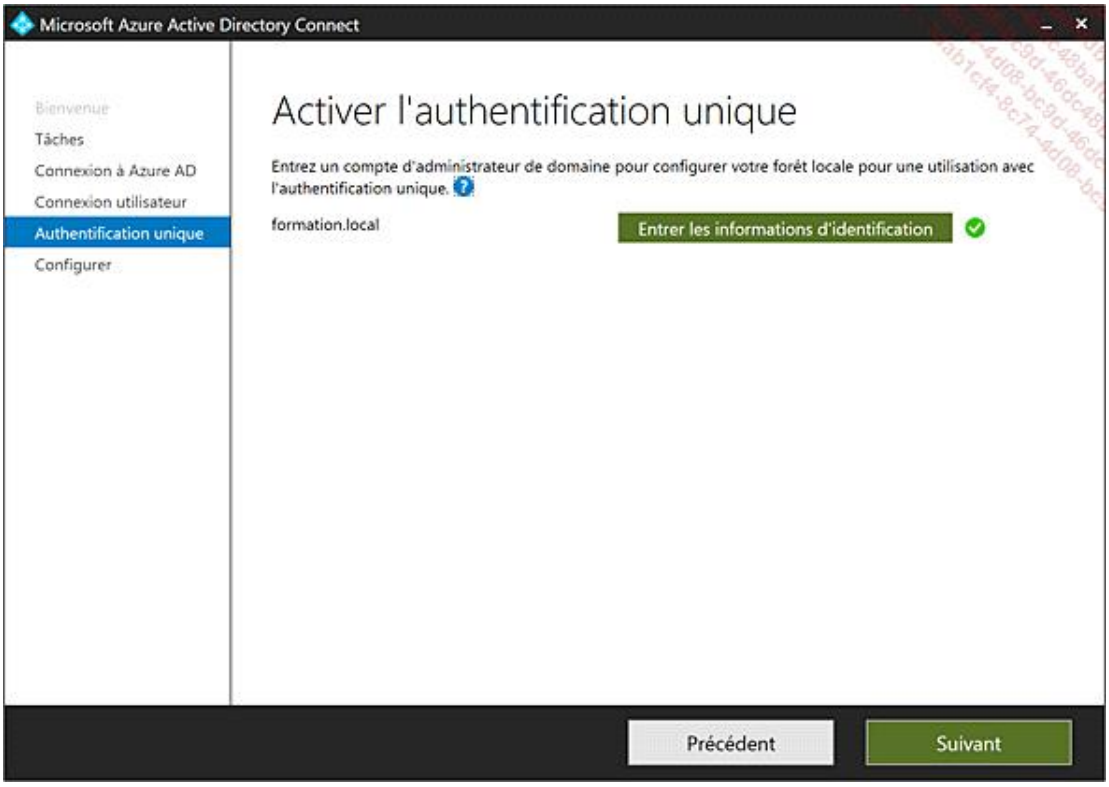
- Cliquez sur **Modifier la connexion utilisateur** puis cliquez sur **Suivant**.



- Après avoir saisi les identifiants pour se connecter au service cloud, cochez la case **Activer l'authentification unique** puis cliquez sur **Suivant**.



- Il est maintenant nécessaire de saisir les identifiants de connexion. Pour cela, cliquez sur le bouton **Entrer les informations d'identification**.

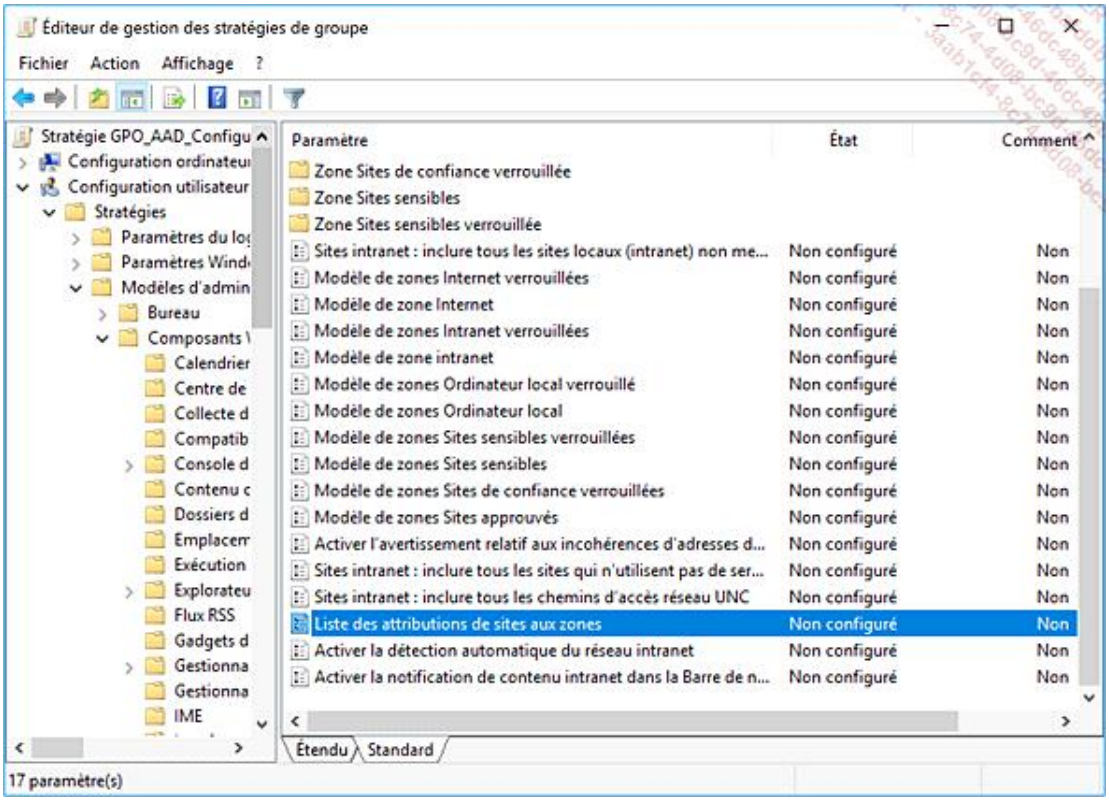


- La synchronisation peut maintenant être lancée. Dans la fenêtre **Configurer**, cliquez sur le bouton **Configurer**.

Pour que le SSO fonctionne, il est nécessaire que le poste de travail soit membre du domaine AD et de configurer Internet Explorer. Pour cette dernière opération, une stratégie de groupe a été créée. Elle est déployée à l'ensemble des utilisateurs.



- Éditez la stratégie de groupe puis accédez au paramètre **Liste des attributions de sites aux zones** présent dans **Configuration utilisateur** - **Composants Windows** - **Internet Explorer** - **Panneau de configuration Internet** - onglet **Sécurité**.

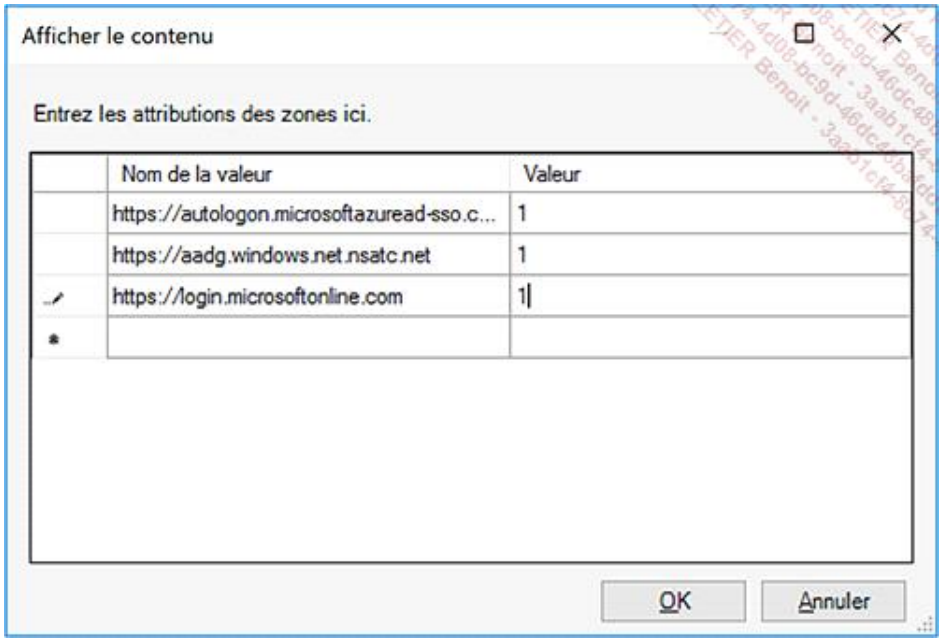


- Ajoutez les URL suivantes et la valeur 1.

  https://autologon.microsoftazuread-sso.com/

  https://aadg.windows.net.nsatc.net

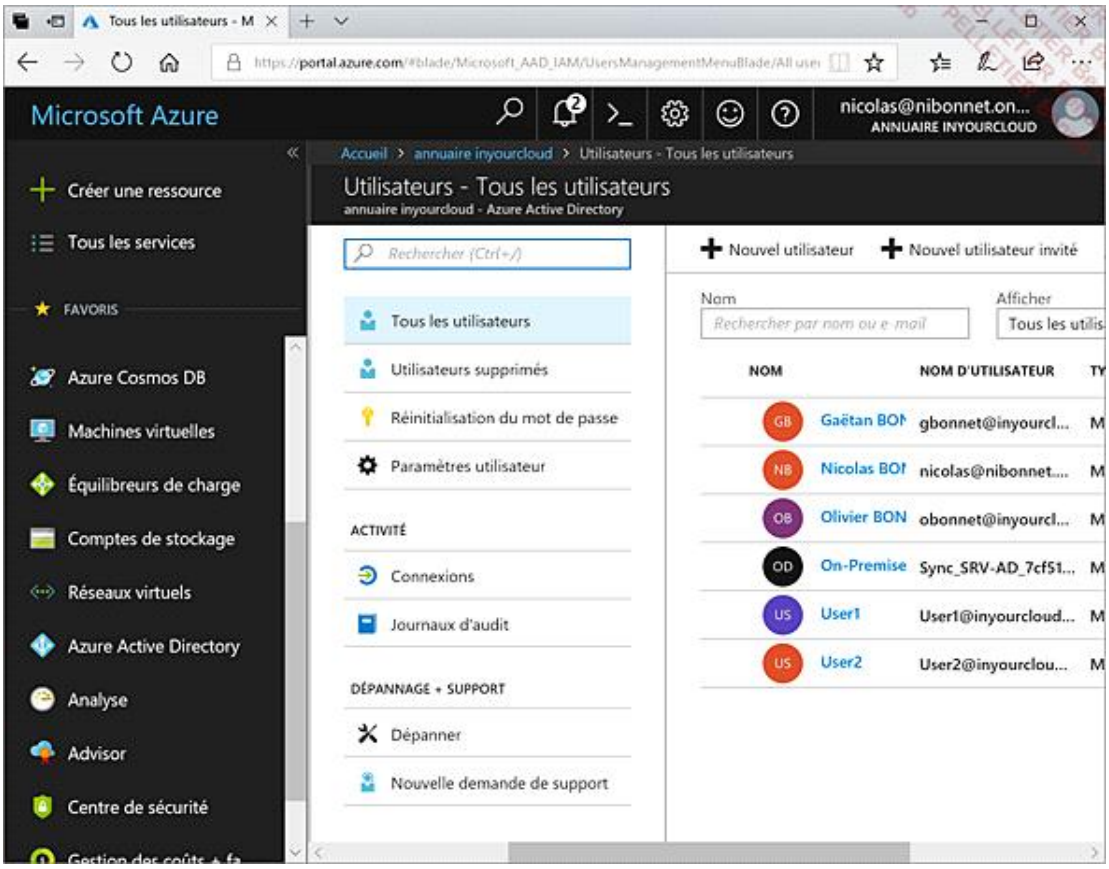
  https://login.microsoftonline.com



- Sur le poste client, vérifiez que la stratégie de groupe est bien appliquée. Avec le compte de l'utilisateur, accédez aux portail cloud (myapps.microsoft.com, etc.), saisissez le nom de l'utilisateur si besoin. La connexion est effectuée sans que l'utilisateur ait à saisir son mot de passe (attention, verifiez la compatibilité de votre navigateur Internet si cela ne fonctionne pas).

4. Gestion des utilisateurs dans Azure

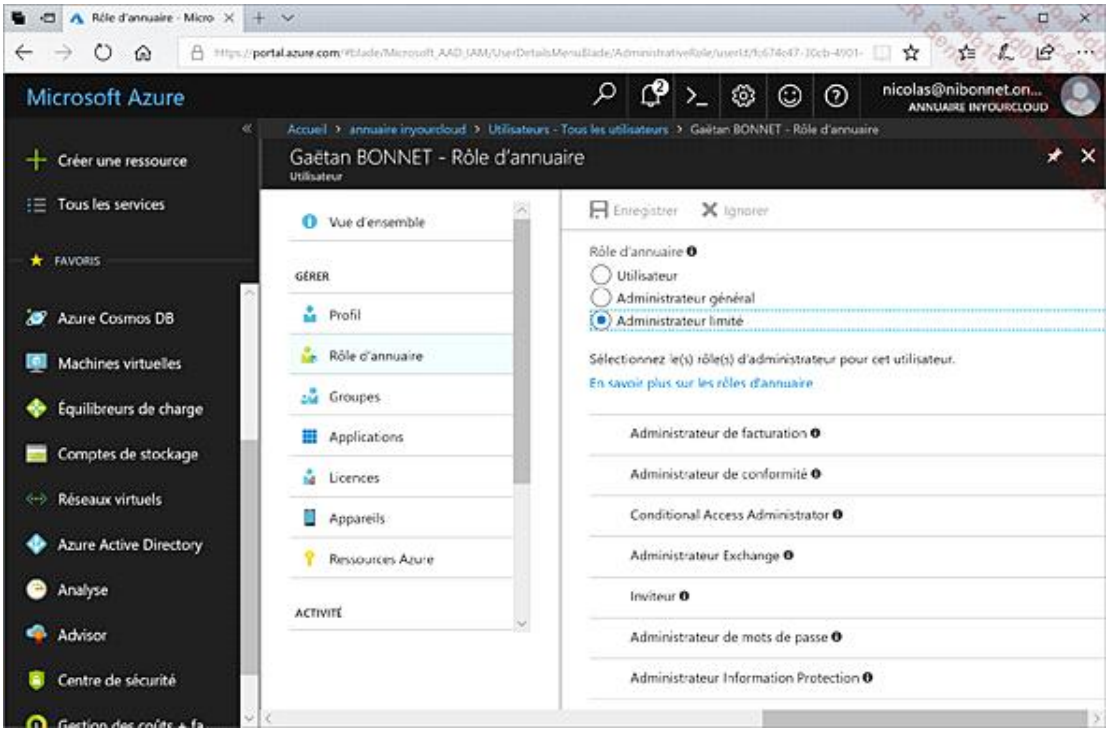
Comme dans un annuaire Active Directory, Azure AD peut contenir des utilisateurs.



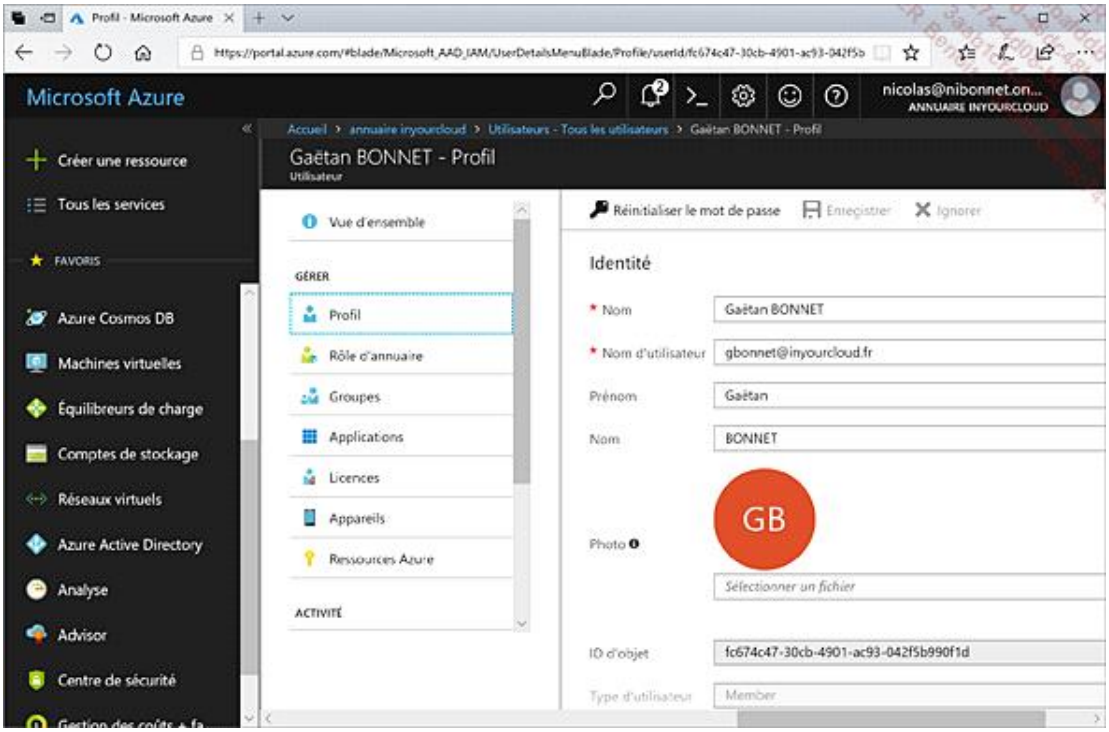
En sélectionnant un utilisateur, il est possible d'accéder à ses attributs. Son nom, son prénom et son nom d'utilisateur s'affichent.

Dans le cas de comptes synchronisés depuis un annuaire interne, la modification des champs est impossible.

Depuis cette même fenêtre, il est possible de configurer le rôle de l'utilisateur. Ainsi on peut voir que notre utilisateur possède le rôle d'administrateur limité.

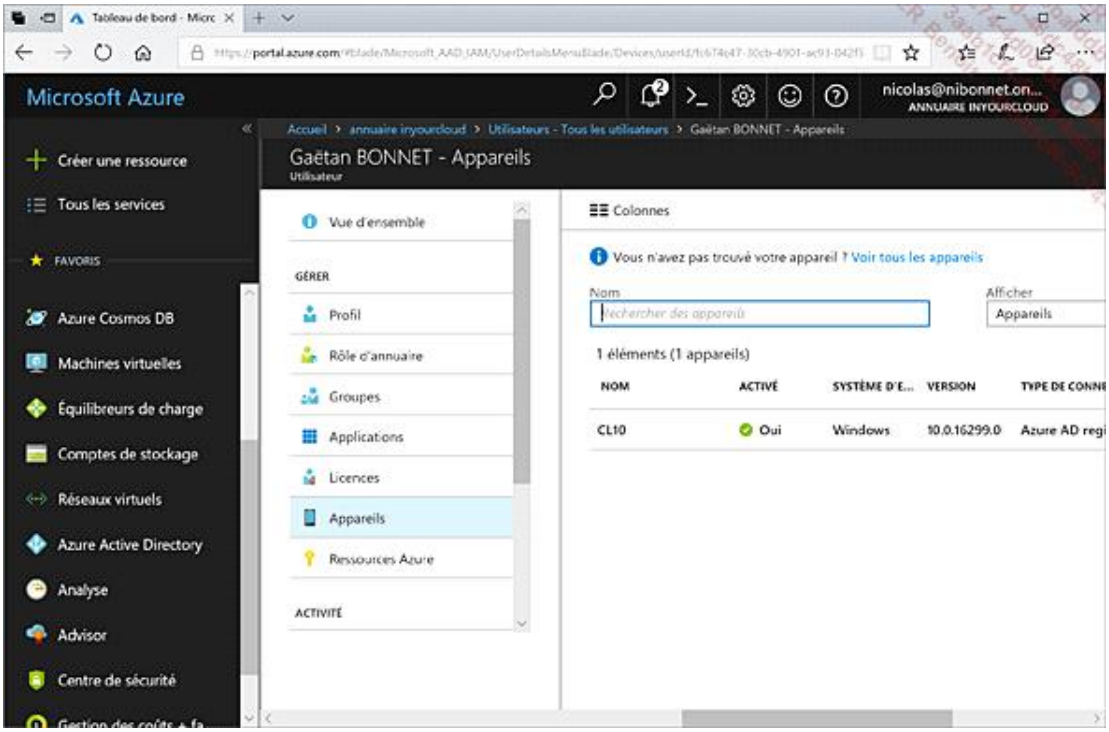


L'onglet **Profil** permet, lui, de visualiser les informations propres à l'utilisateur (service, numéro de téléphone…).



Depuis Windows 10, il est possible de joindre un poste de travail à un annuaire Azure AD. Ceci évidemment en lieu et place d'un annuaire AD.

L'onglet **Appareils** permet de visualiser les ordinateurs ajoutés par l'utilisateur.



Enfin, le dernier onglet **ACTIVITÉ** permet d'établir des rapports sur l'activité de l'utilisateur.

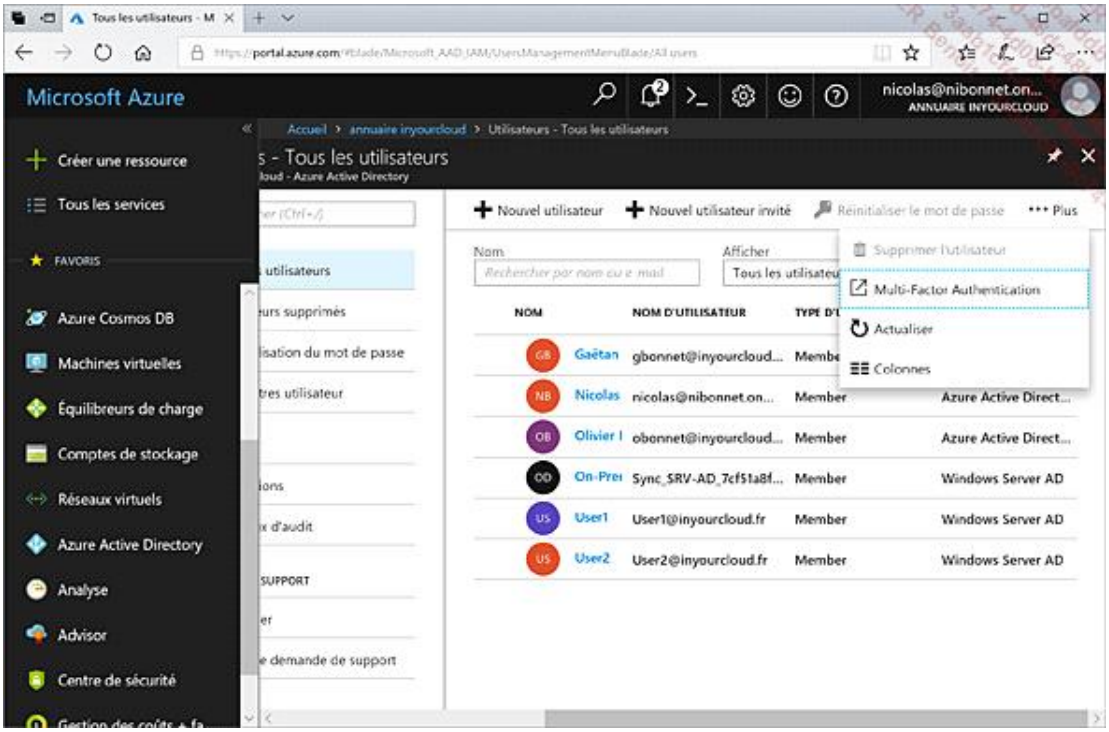
5. Authentification forte dans Azure

Certaines applications peuvent contenir des informations confidentielles (CRM…), d'autres sont "la vitrine" de l'entreprise (Twitter…). Il est donc important d'activer l'authentification forte en fonction du degré de confidentialité des données contenues dans l'application. Cette opération nécessite néanmoins de posséder l'édition Premium.

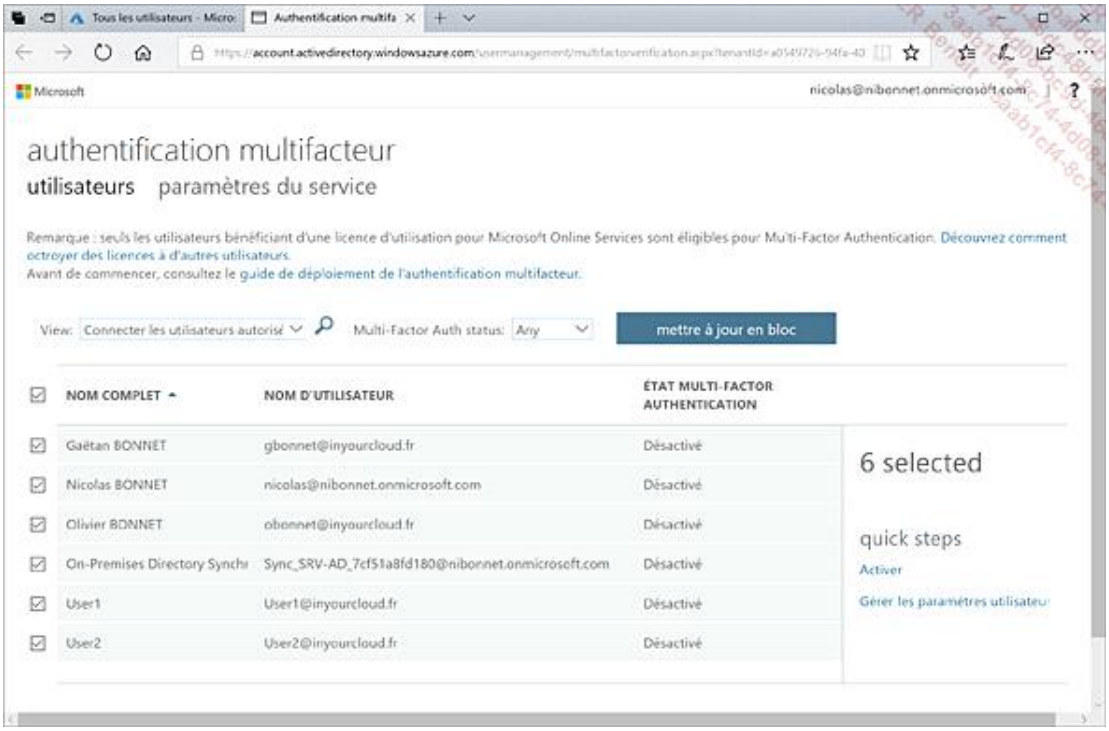
Le lien ci-dessous présente un récapitulatif des éditions de Azure AD.

https://msdn.microsoft.com/en-us/library/azure/dn532272.aspx

- L'activation de l'authentification forte s'effectue depuis l'interface web azure.microsoft.com. Sélectionnez Active Directory puis cliquez sur **Tous les utilisateurs**. Dans le bandeau supérieur, cliquez sur **Plus** puis sur **Multi-Factor Authentication**.

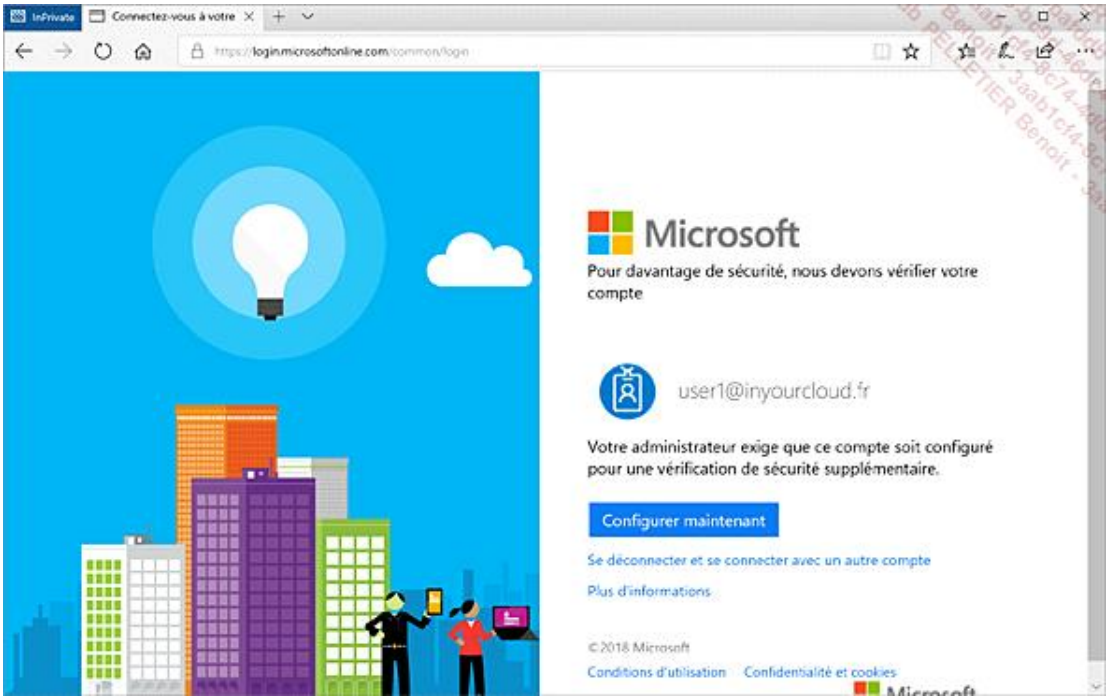


- Sélectionnez les utilisateurs souhaités puis cliquez sur **Activer**.

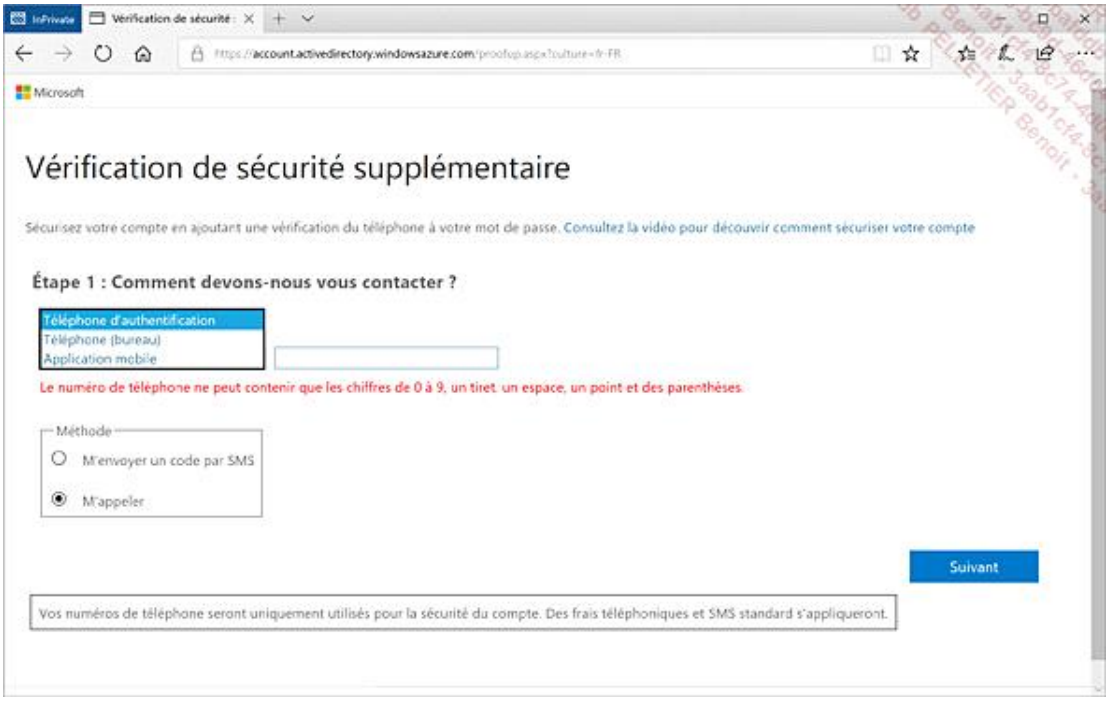


- Une fenêtre s'affiche. Il est nécessaire de cliquer sur **Activer multi-factor authentication** pour procéder à l'activation du MFA.

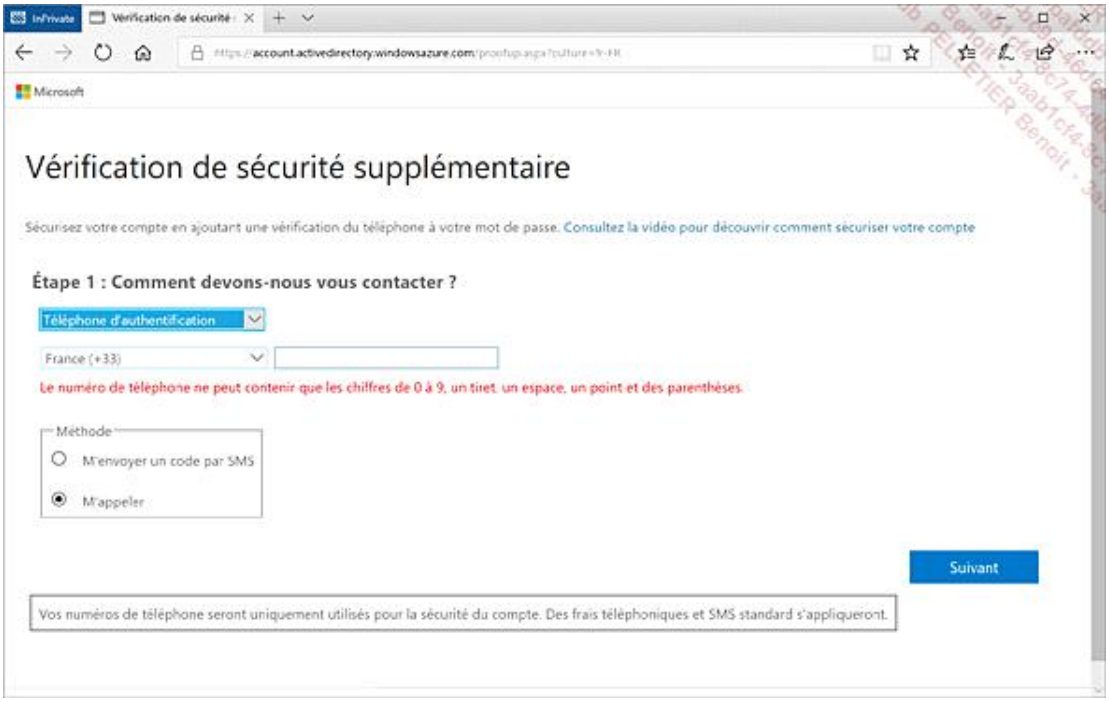
Lors de la prochaine connexion de l'utilisateur (au portail applicatif, par exemple : http://myapps.microsoft.com/), ce dernier devra sélectionner le type d'authentification souhaité.



Les trois possibilités d'authentification sont offertes à l'utilisateur.



En cas de sélection du premier choix, l'utilisateur devra saisir son numéro de téléphone.

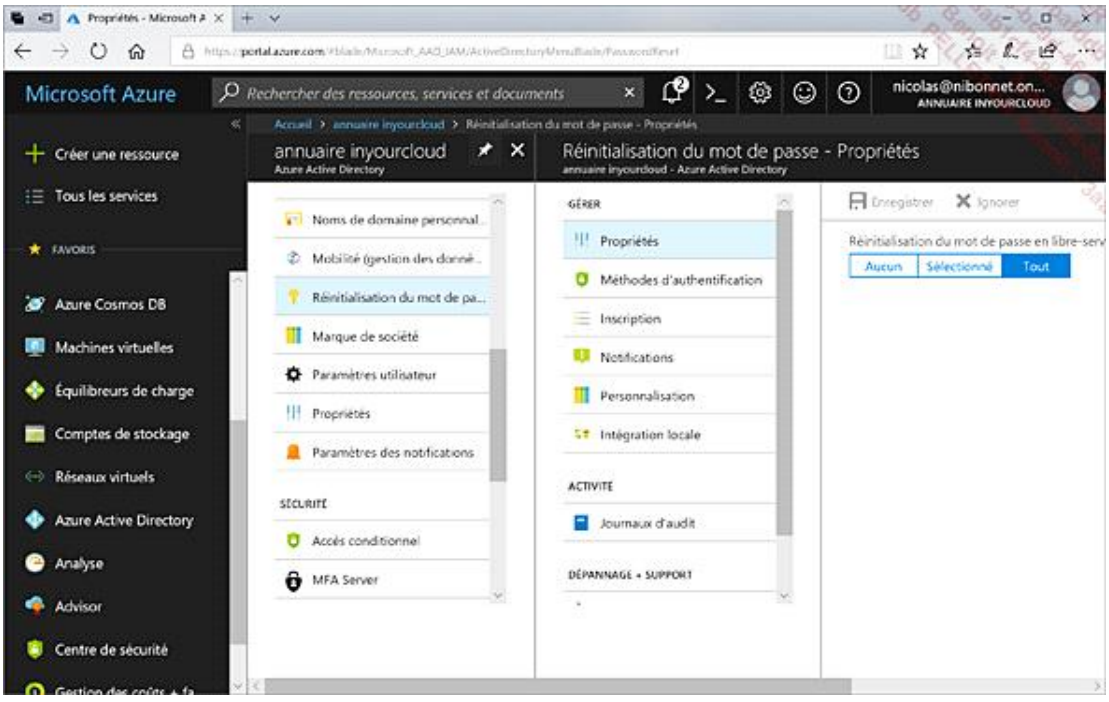


Après la validation du numéro, l'authentification forte est configurée.

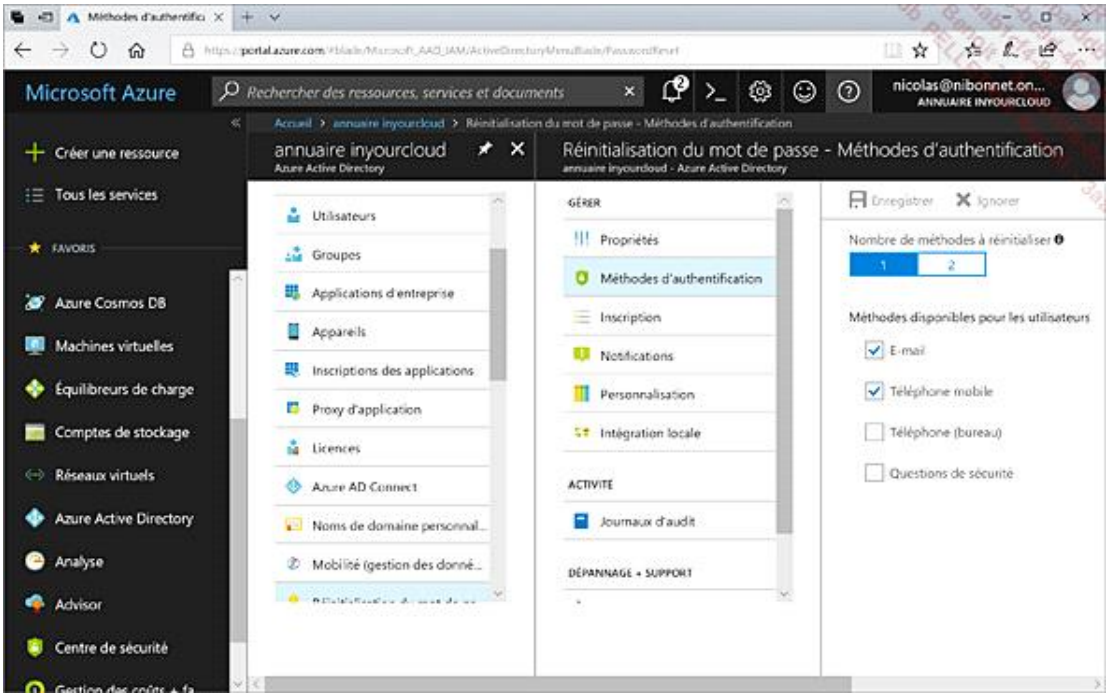
6. Le portail web Self-Service

Ce portail web offre la possibilité aux utilisateurs Azure AD de réinitialiser leur mot de passe sans intervention de l'équipe IT.

De plus, il offre l'avantage d'être disponible sur les trois éditions d'Azure AD (Free, Basic, Premium). Avant de pouvoir accéder au portail web, il est nécessaire de procéder à la configuration de la politique de réinitialisation du mot de passe utilisateur. Cette opération consiste à activer le paramètre présent dans l'onglet **Réinitialisation du mot de passe**. Il est possible d'autoriser la fonctionnalité pour tout le monde ou pour un groupe d'utilisateurs.



L'administrateur a la possibilité de définir le nombre de méthodes d'identification nécessaires pour procéder à la réinitialisation. Les méthodes disponibles doivent également être sélectionnées.



La personnalisation peut maintenant être effectuée à l'aide des autres onglets.

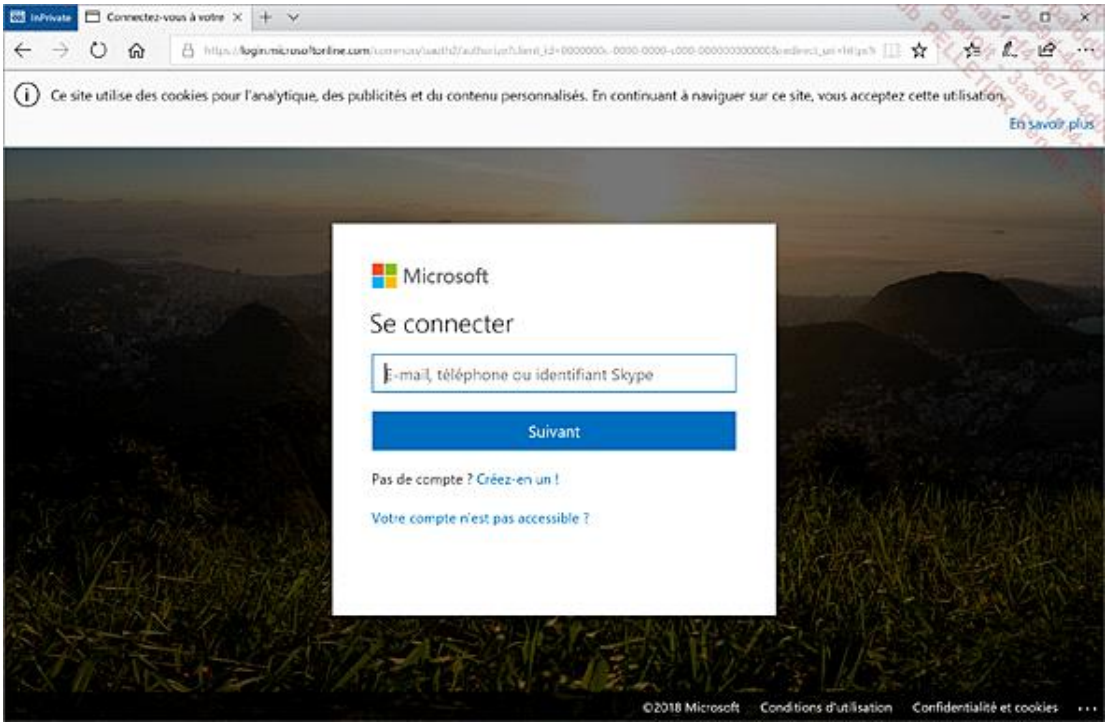
Notez qu'une licence Azure AD Premium est nécessaire pour procéder à la réinitialisation du mot de passe pour les comptes synchronisés avec un Active Directory.

a. Réinitialisation du mot de passe

Cette étape consiste à se connecter à l'interface web avec son compte. Pour une réinitialisation du mot de passe due à un oubli, il est nécessaire d'accéder à l'URL suivante :

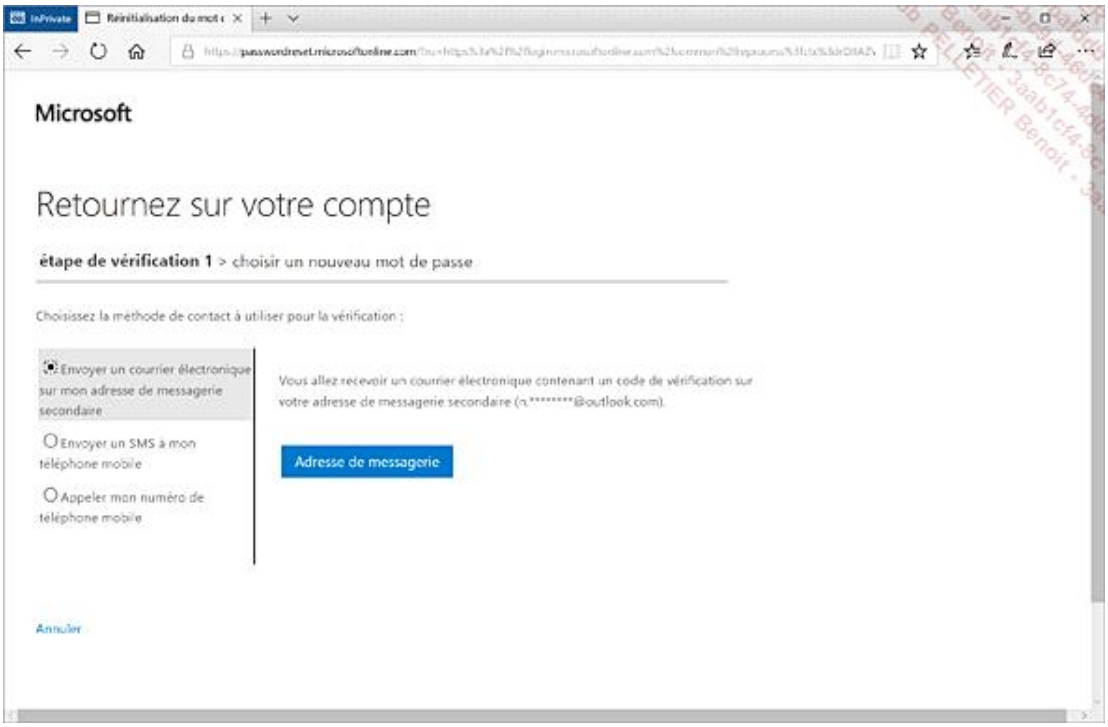
https://account.activedirectory.windowsazure.com/PasswordReset/Register.aspx

- Cliquez sur le lien **Votre compte n'est pas accessible ?** afin d'accéder au portail web de réinitialisation du mot de passe.



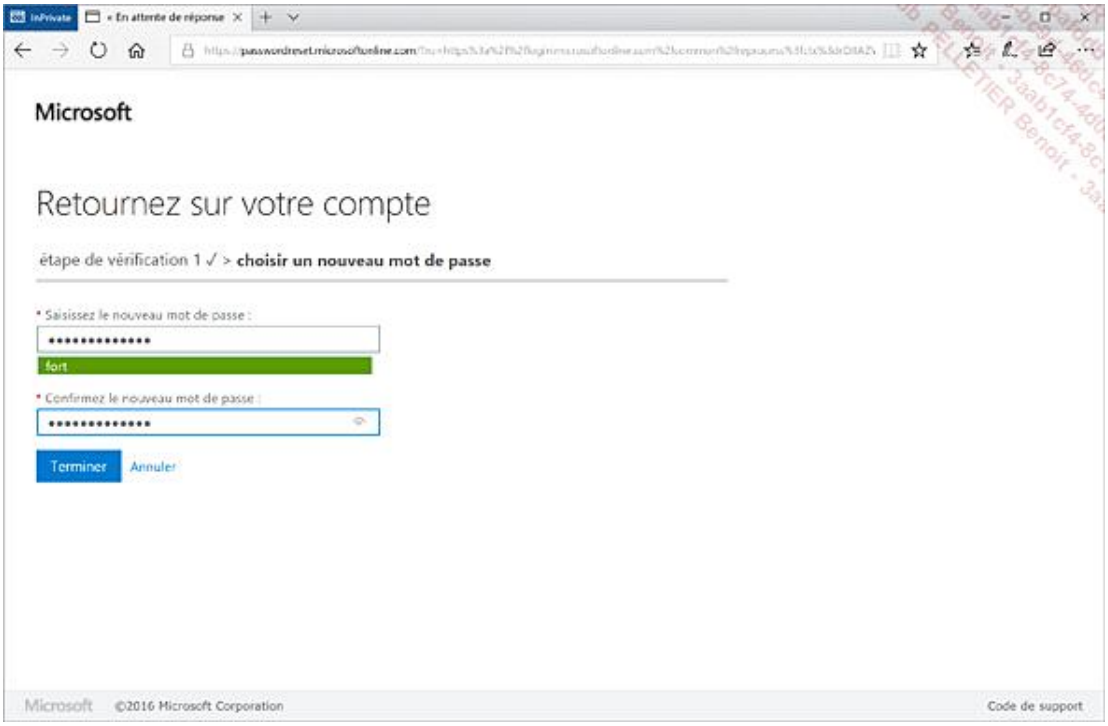
- Sélectionnez **compte professionnel ou scolaire** puis, dans la fenêtre qui s'affiche, saisissez l'identifiant utilisateur. Après avoir saisi les caractères de l'image, cliquez sur **Suivant**.

Il est maintenant nécessaire de sélectionner la méthode de contact à utiliser pour effectuer la vérification.



L'authentification forte étant activée pour l'utilisateur, ce dernier doit prouver son identité (SMS reçu, appel téléphonique…) et recevra un code de vérification.

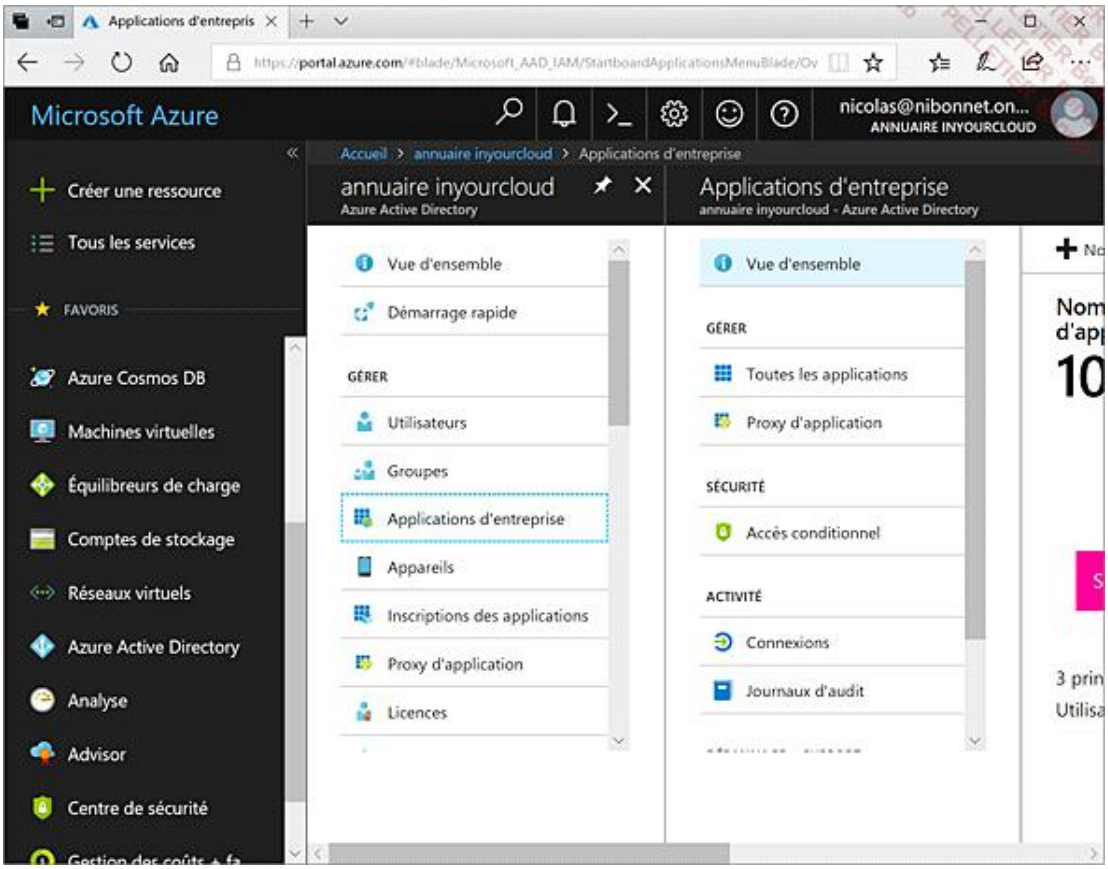
Une fois l'utilisateur vérifié, le mot de passe peut être modifié.



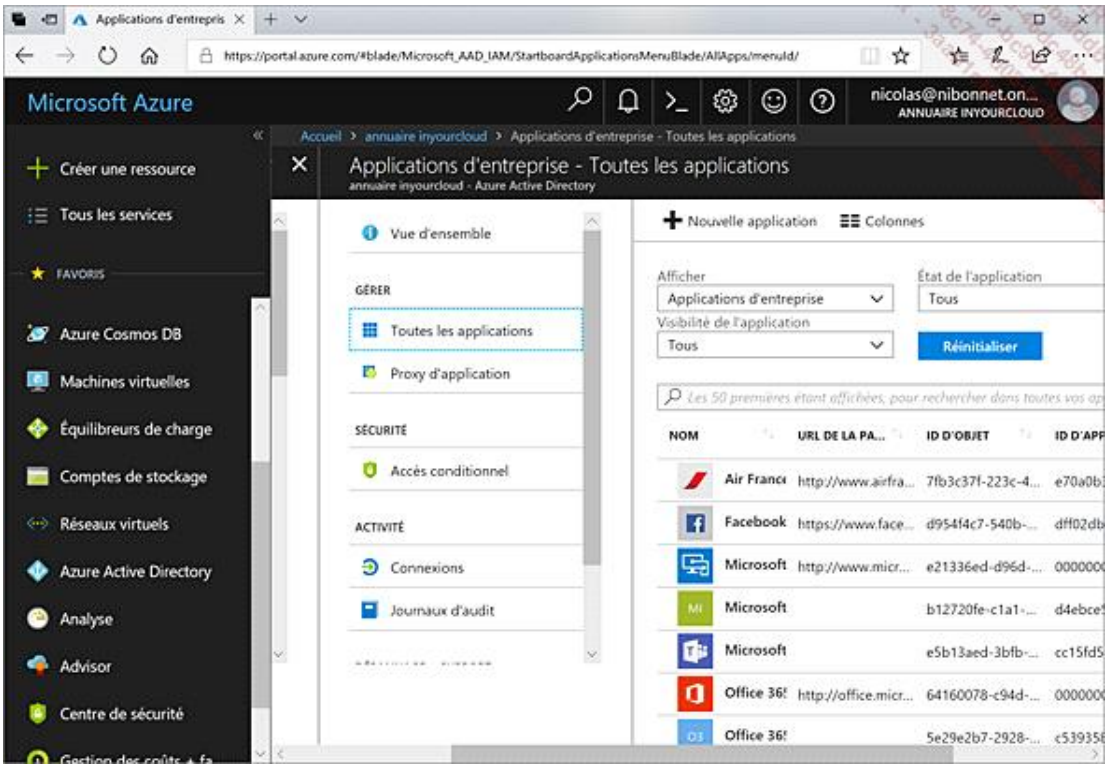
b. Mise à disposition d'applications

Azure Active Directory permet la mise à disposition d'applications, l'accès est octroyé à un utilisateur ou un groupe d'utilisateur.

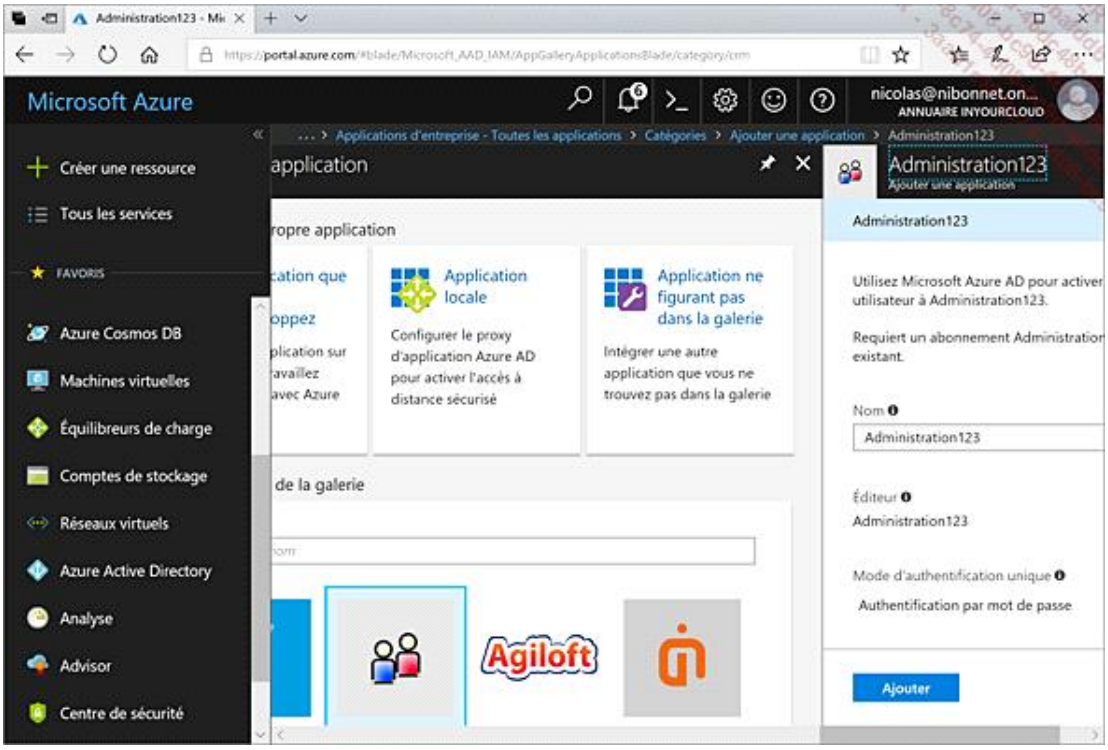
L'opération s'effectue par l'intermédiaire de l'onglet **Applications d'entreprise** présent dans l'annuaire Azure AD.



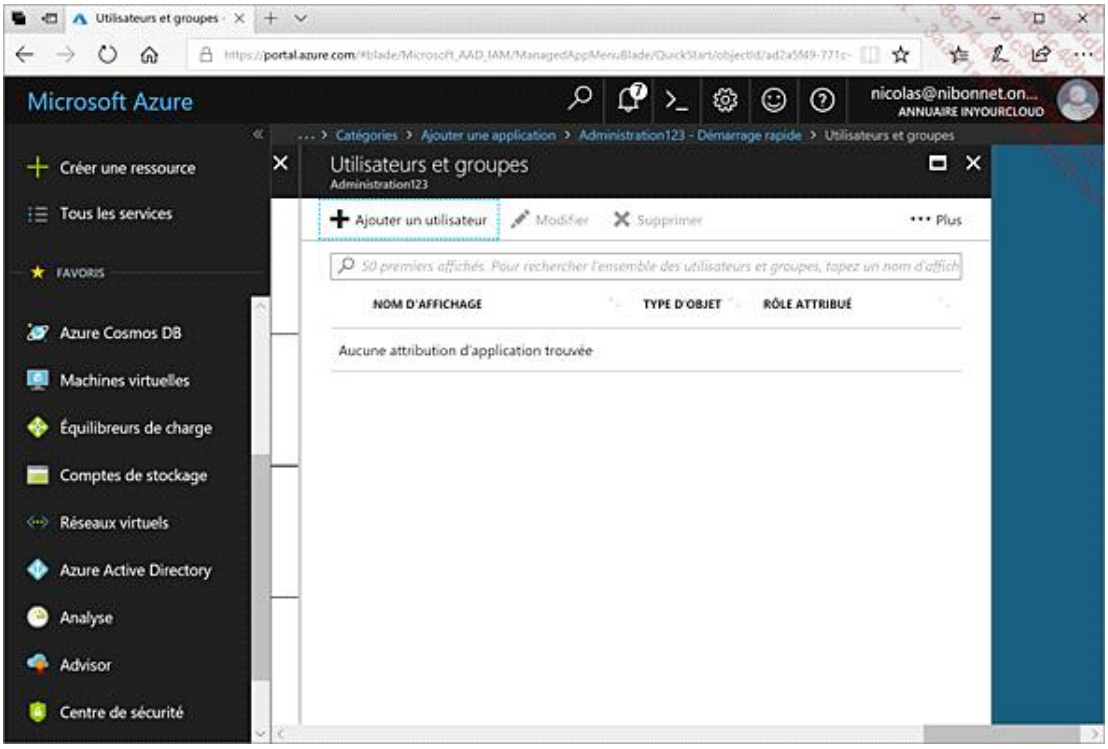
Cliquez sur **Toutes les applications** puis sur **Nouvelle application**.



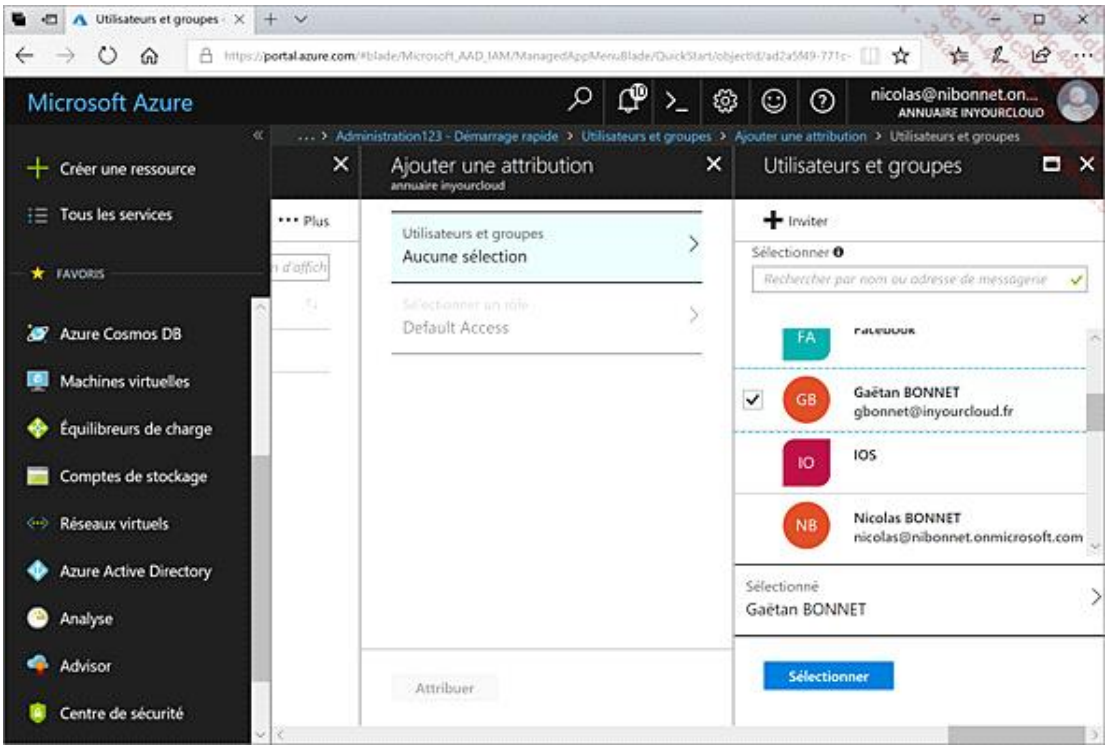
De nombreuses applications sont présentes. Sélectionnez celle souhaitée puis cliquez sur **Ajouter**.



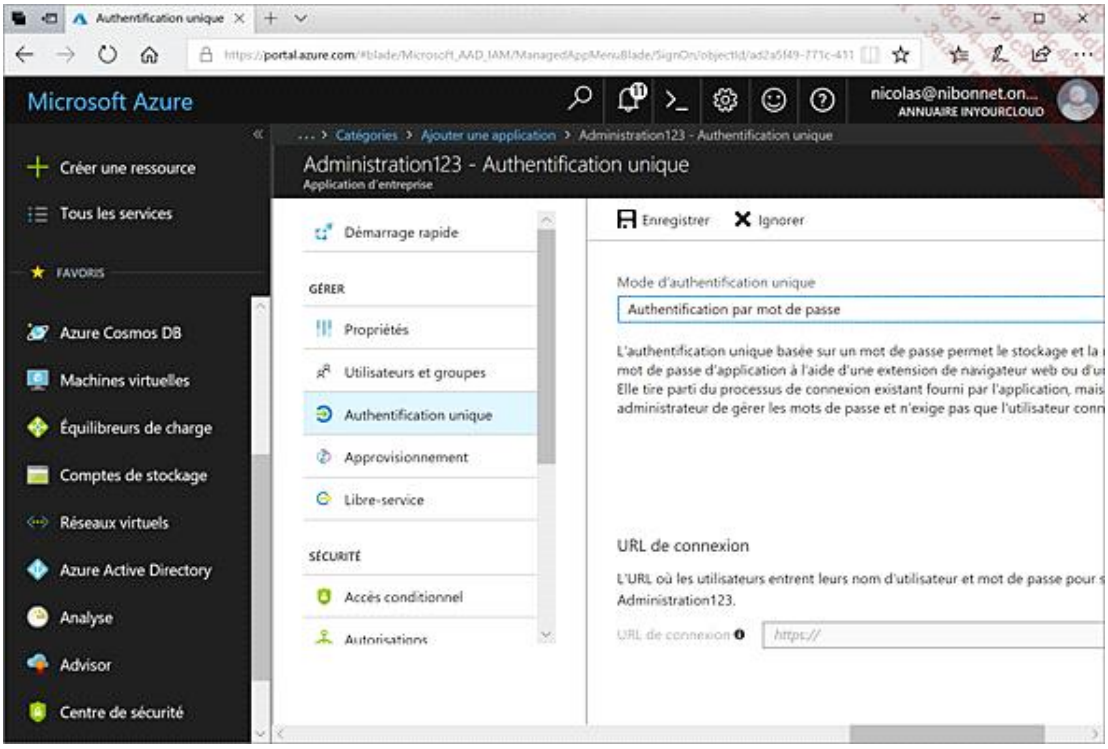
L'affectation de l'application à un ou plusieurs utilisateurs est effectuée au niveau de l'application. Dans les propriétés de celle-ci, cliquez sur **Utilisateurs et groupes**.



Sélectionnez l'utilisateur ou le groupe d'utilisateurs souhaité.

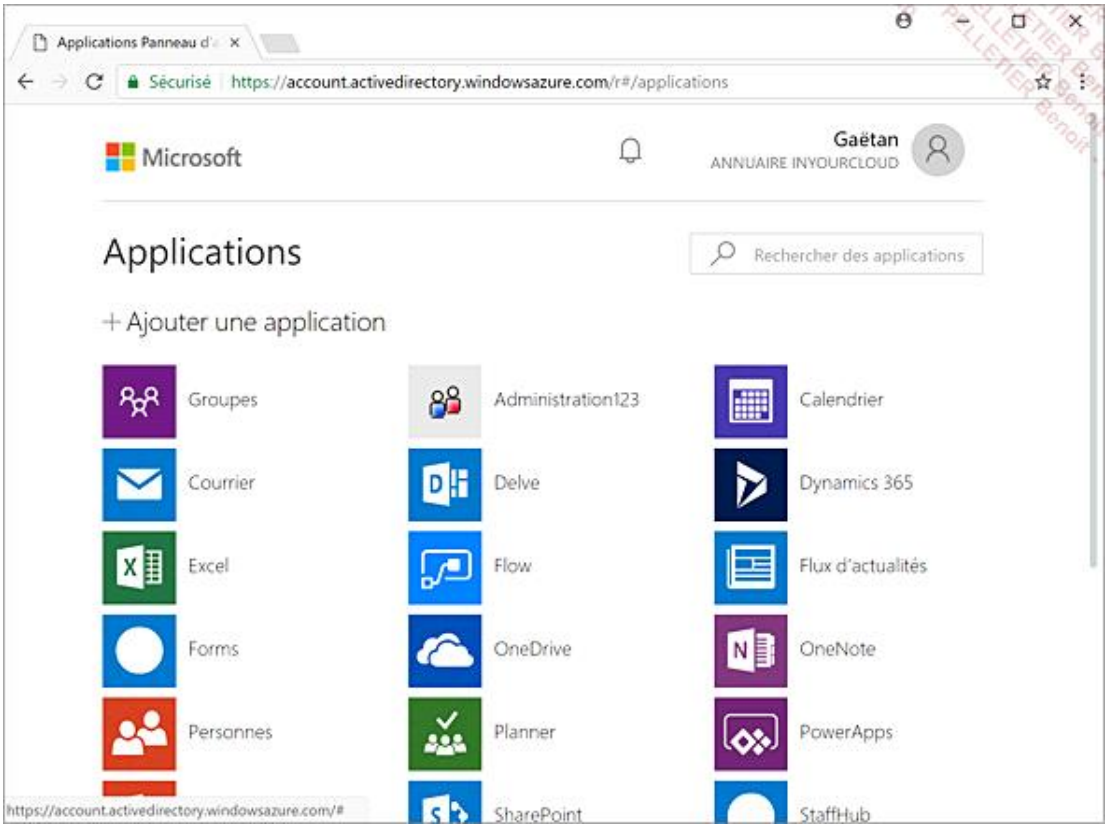


Depuis le menu, cliquez sur **Authentification unique** puis sélectionnez **Authentification par mot de passe**. Cliquez sur **Enregistrer** pour enregistrer la modification.



Lors de la première connexion, les identifiants seront demandés puis enregistrés dans l'annuaire. Néanmoins, il est possible de les préenregistrer, ainsi ils ne seront pas demandés à l'utilisateur ou aux utilisateurs.

En se rendant à l'URL http://myapps.microsoft.com/ puis en se connectant avec le compte utilisateur adéquat, on peut accéder à l'application mise à disposition.



L'utilisateur doit saisir ses identifiants lors de la première connexion. Le couple login/mot de passe sera enregistré

dans l'annuaire, l'utilisateur n'aura plus à les saisir.

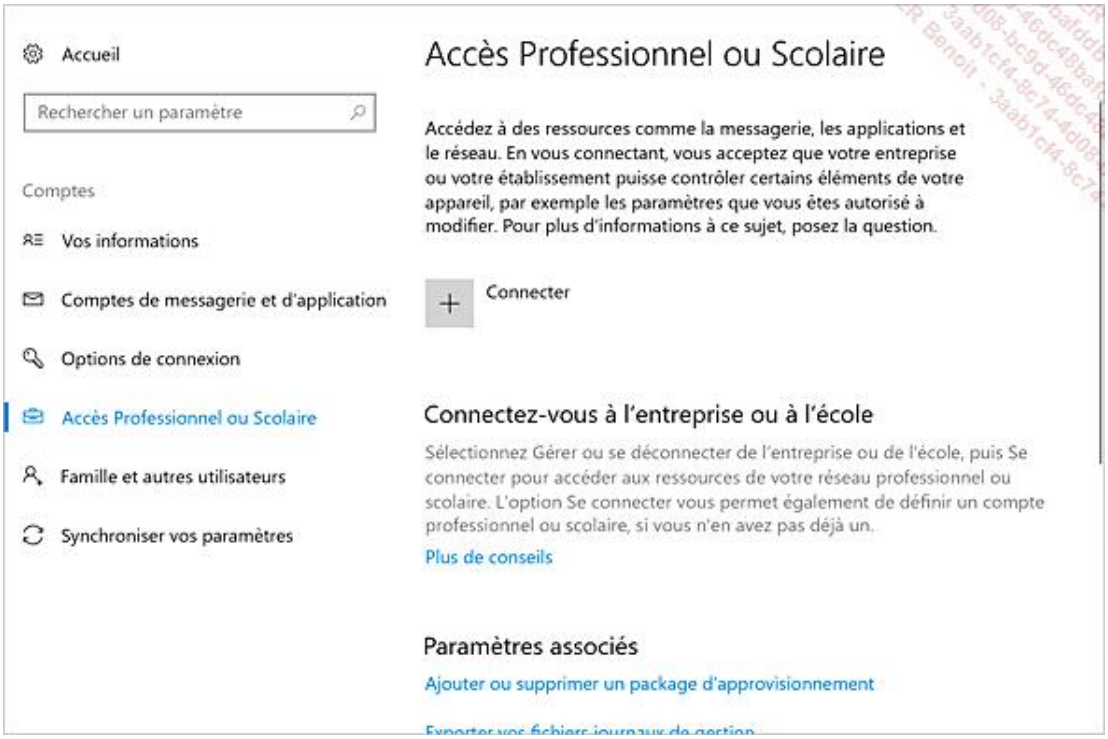
7. Azure AD Join avec Windows 10

Nous avons l'habitude depuis des années de joindre une machine à un domaine Active Directory. Néanmoins, certains postes de travail à forte mobilité sont difficilement administrables. Windows 10 permet la jonction à un annuaire Azure AD et une meilleure gestion de ces équipements dits « mobiles ». Notez que depuis la version 1709 de Windows 10, il est possible de joindre un annuaire Active Directory ainsi qu'un annuaire Azure Active Directory.

La jonction à un annuaire Azure AD permet d'obtenir un SSO (*Single Sign-On*) avec toute les applications et services s'appuyant sur Azure AD. La configuration très aisée pour joindre ce type d'annuaire permet à un utilisateur d'effectuer lui-même la jonction. Ainsi, il peut retrouver facilement ses documents et paramètres.

a. Fonctionnement de l'Azure AD Join

La jonction à un annuaire Azure AD peut être faite par le biais des écrans OOBE (*Out Of Box Experience*, écran d'accueil Windows présent à la suite de l'installation) ou par l'intermédiaire du nouveau panneau de configuration.



Par la suite, il est nécessaire de saisir son nom d'utilisateur et son mot de passe. En amont, les comptes utilisateurs doivent être synchronisés (synchronisation du mot de passe ou utilisation de serveur AD FS). En cas d'utilisation d'un serveur AD FS, une redirection vers les serveurs AD FS est effectuée. Suite à l'authentification, l'équipement localise un locataire correspondant dans Azure AD. En cas d'utilisation de la fonctionnalité multifacteur, une double authentification est effectuée.

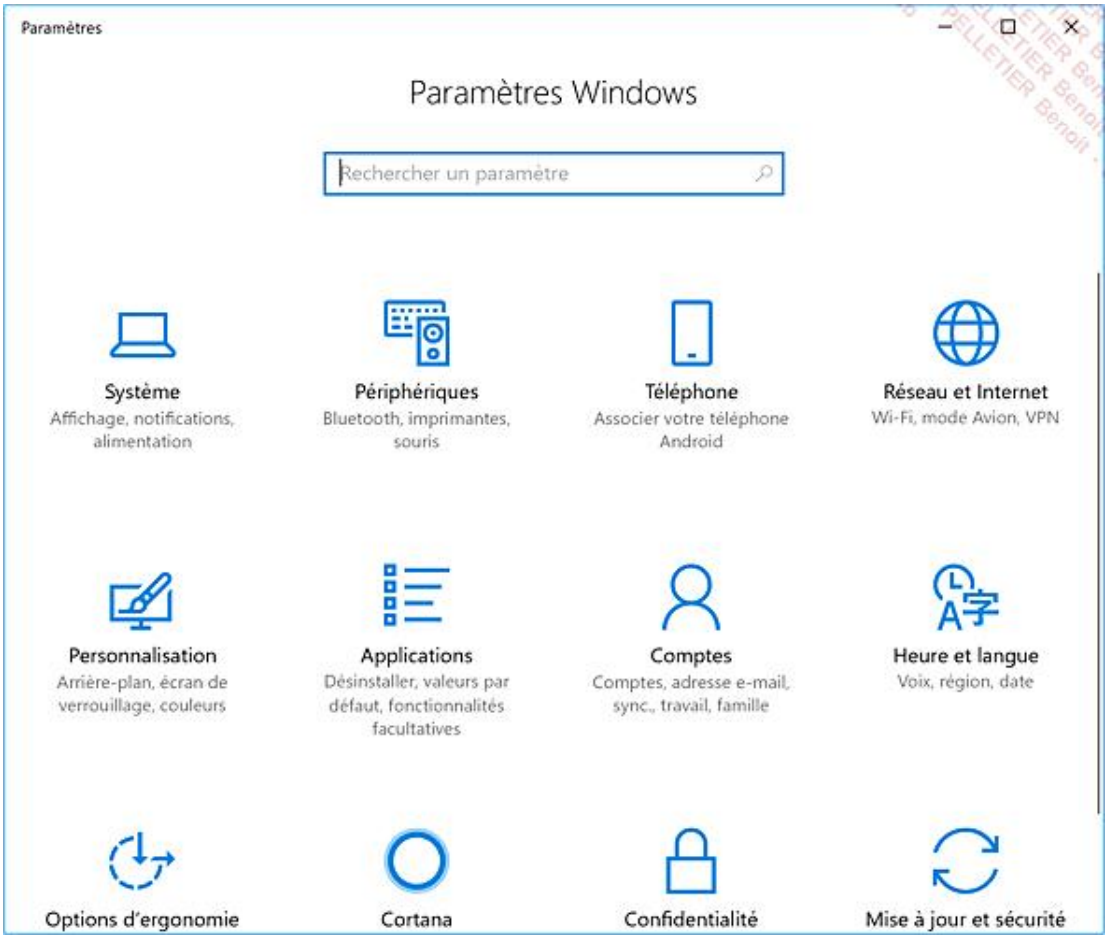
Une fois ces opérations réalisées, Azure AD vérifie si une inscription dans la gestion des appareils mobiles est exigée. Si tel est le cas, l'inscription de l'appareil à la base Azure AD puis à la gestion des appareils mobiles est effectuée. Dans le cas où cette dernière n'est pas requise, seule l'inscription à la base Azure AD est effectuée.

Par la suite, l'utilisateur a la possibilité de se connecter aux différents services cloud. Il est intéressant de noter que depuis Windows 10, il est possible de stocker la clé BitLocker dans un annuaire Azure AD.

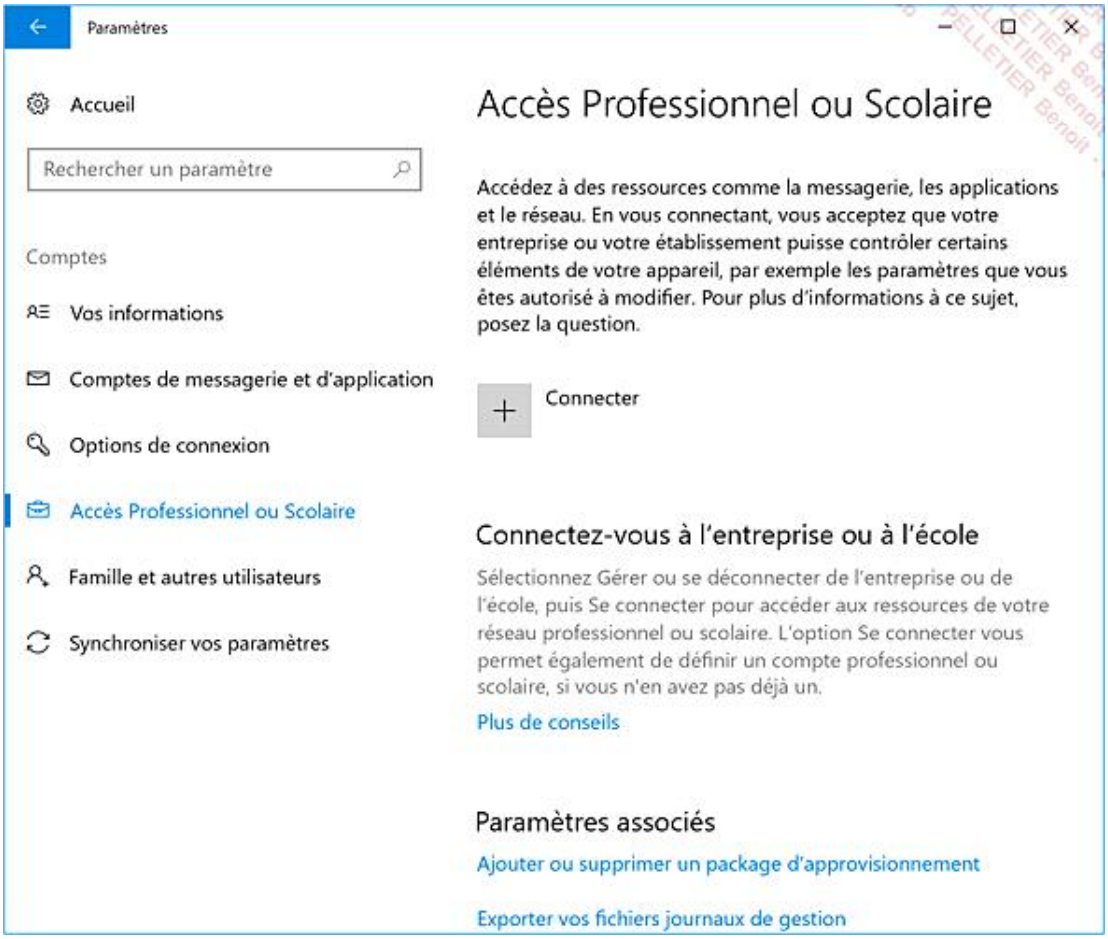
b. Jonction d'une machine à Azure AD Join

Dans l'exemple suivant, la machine Windows 10 va être jointe à une base Azure AD. Le domaine est managé (synchronisation des mots de passe dans Azure AD). De plus, la gestion des équipements mobiles n'est pas exigée. Les opérations ci-dessous nécessite une base Azure AD ; sans cette dernière, vous ne pourrez pas effectuer l'opération.

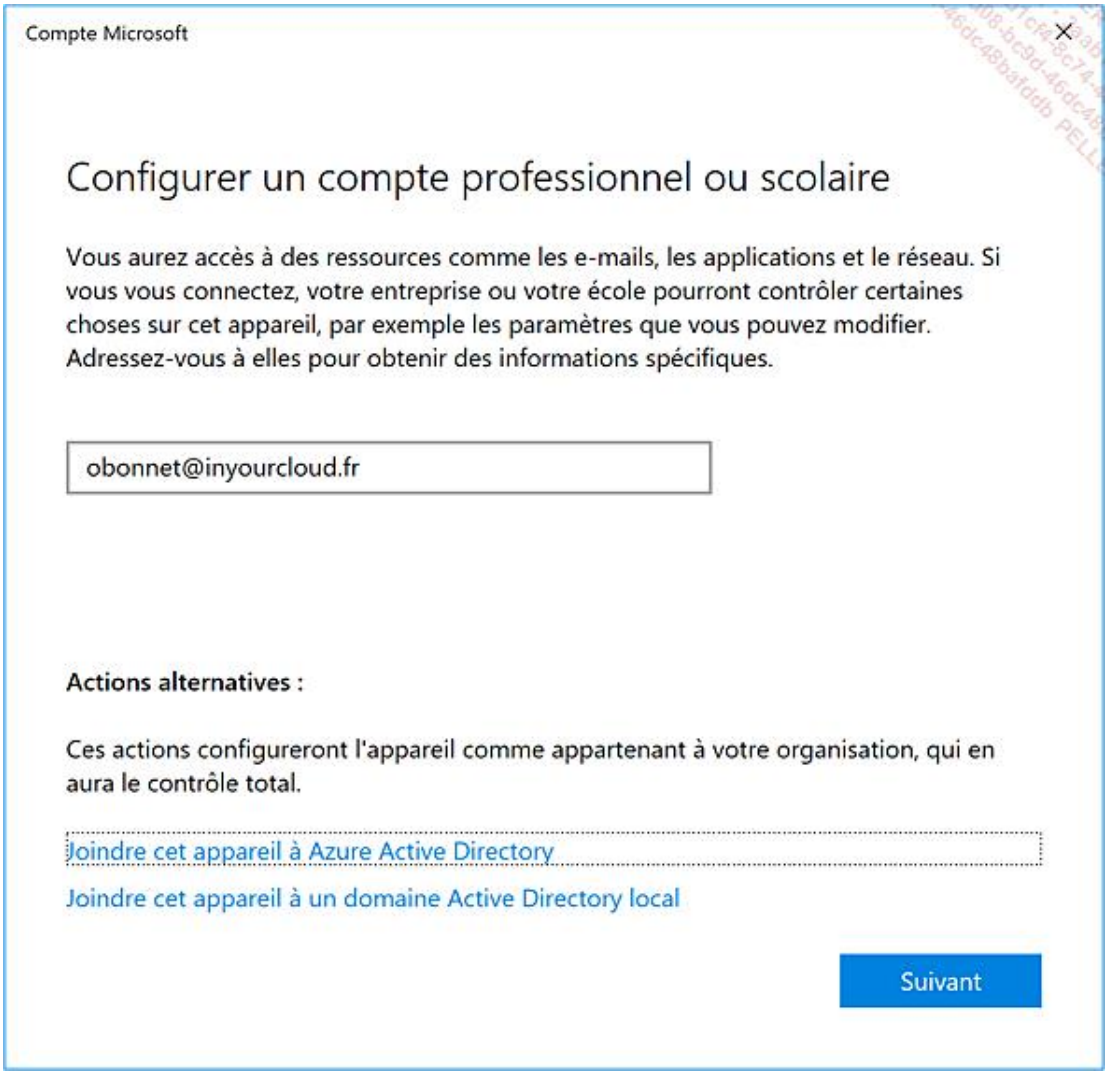
- Depuis le poste Windows 10, accédez aux paramètres Windows.



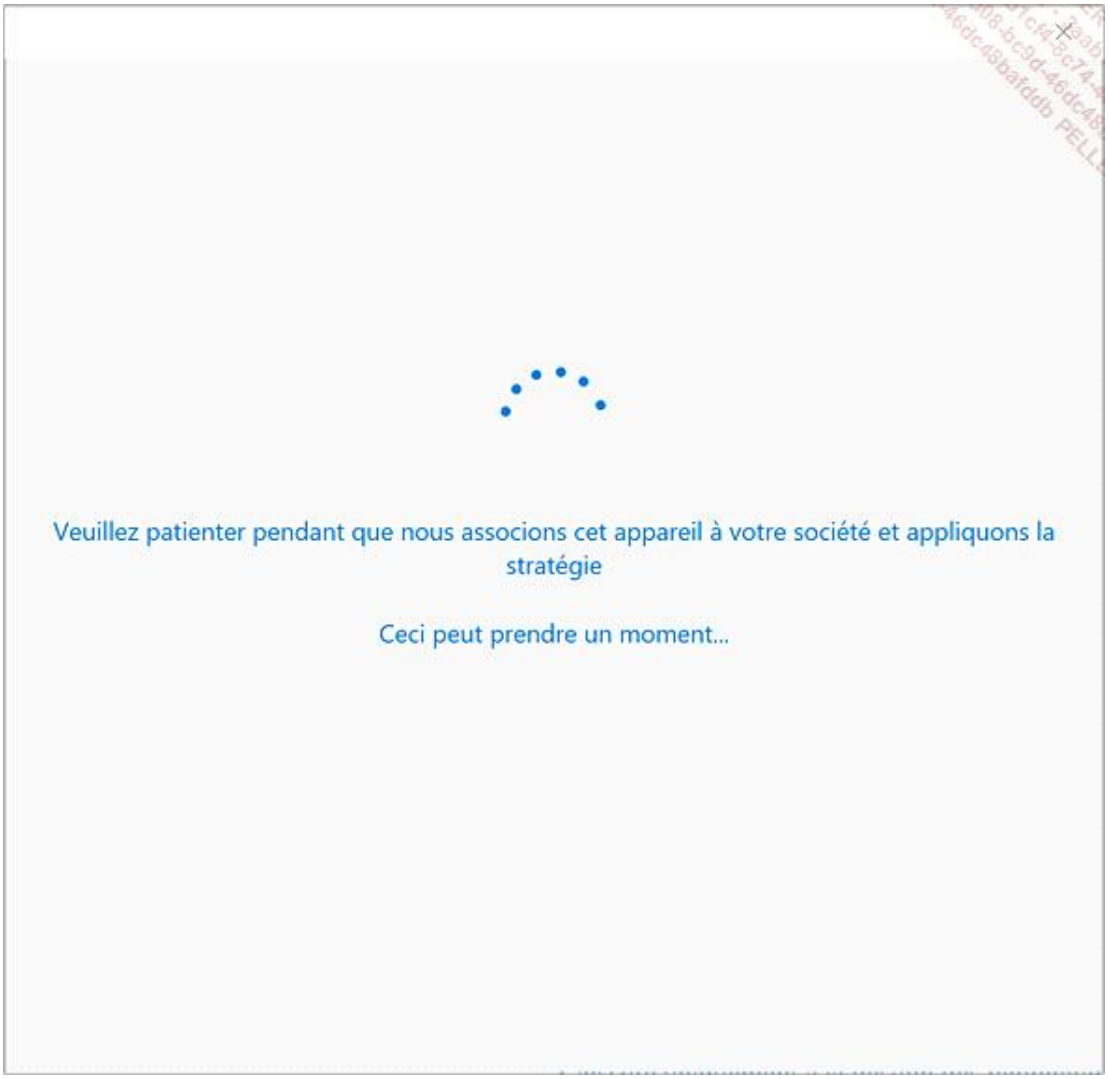
- Cliquez sur **Comptes** puis sur **Accès Professionnel ou Scolaire**.



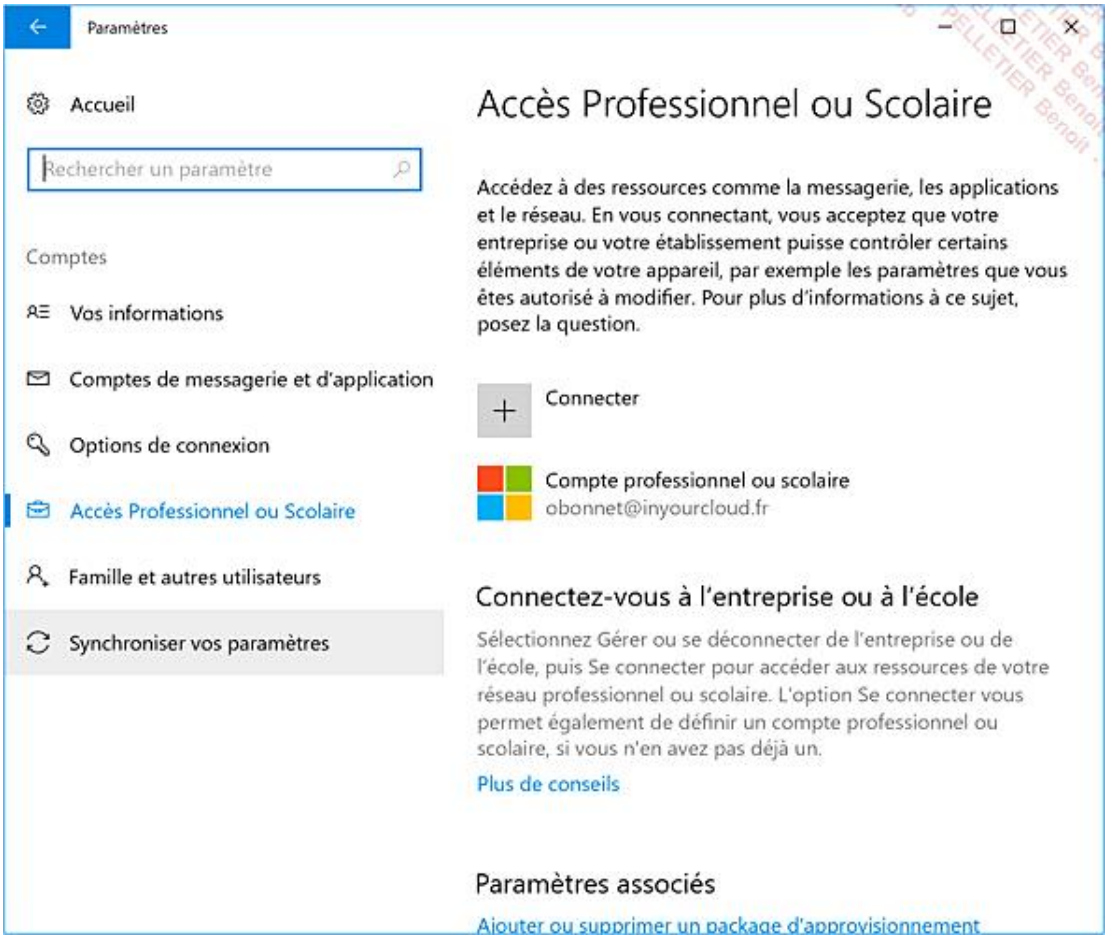
Cliquez sur **Connecter** puis saisissez les identifiants de l'utilisateur.



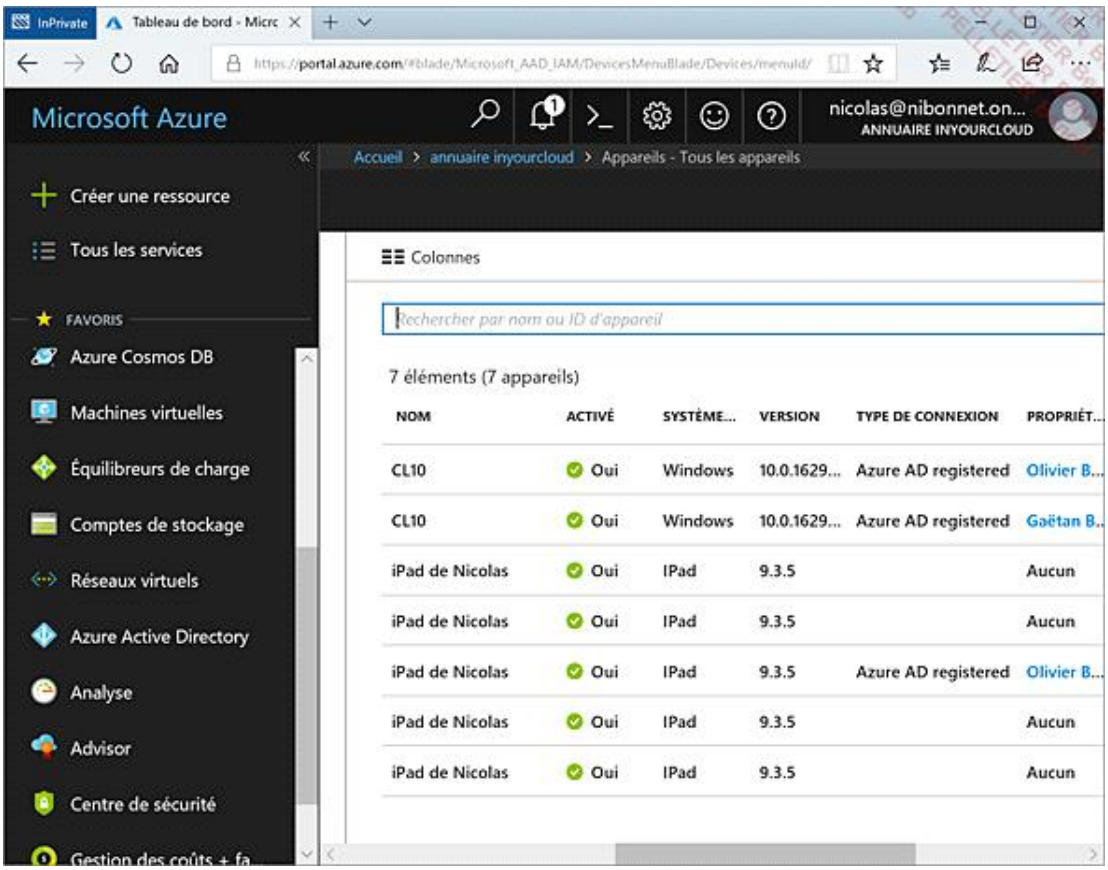
Après avoir saisi le mot de passe, la jonction est effectuée.



Suite à l'ajout, le compte est bien présent au niveau de l'équipement Windows 10.



La machine apparaît dans le portail Azure.



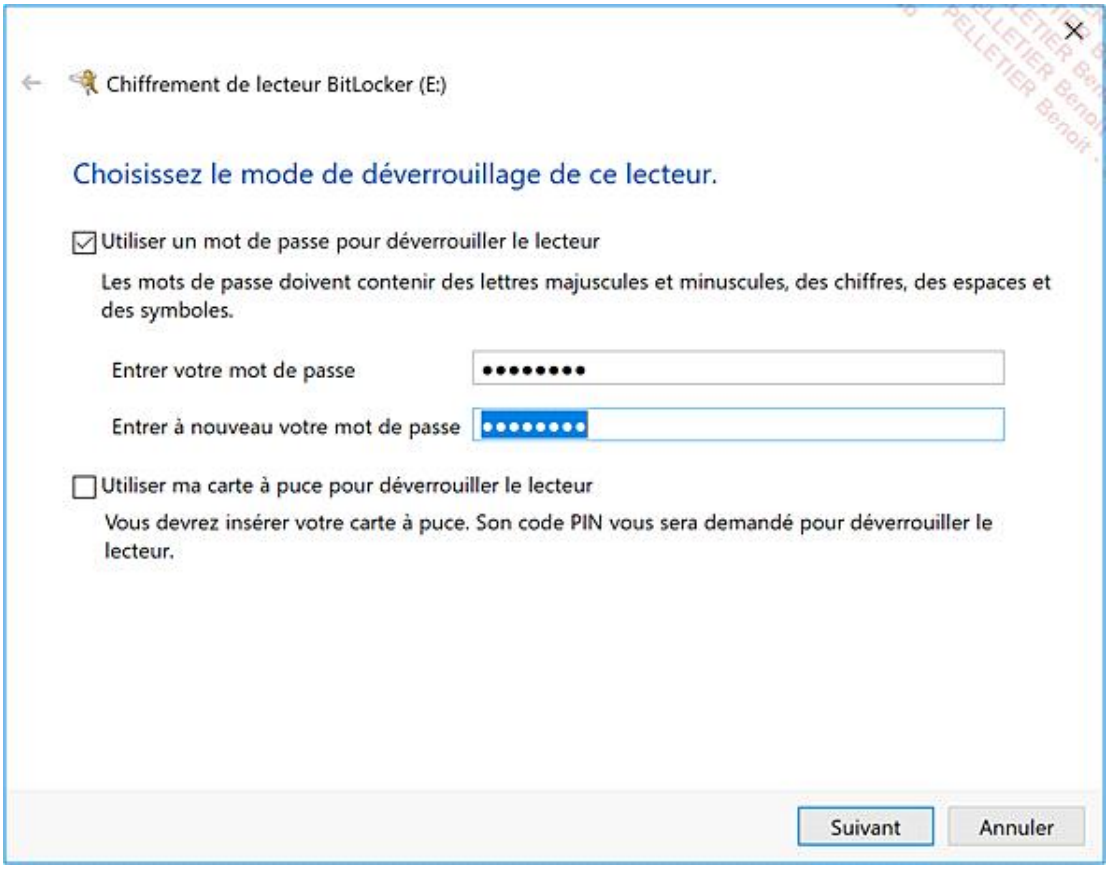
Il est maintenant possible de gérer les postes depuis la console Azure AD.

8. Remontée de la clé BitLocker dans la base Azure AD

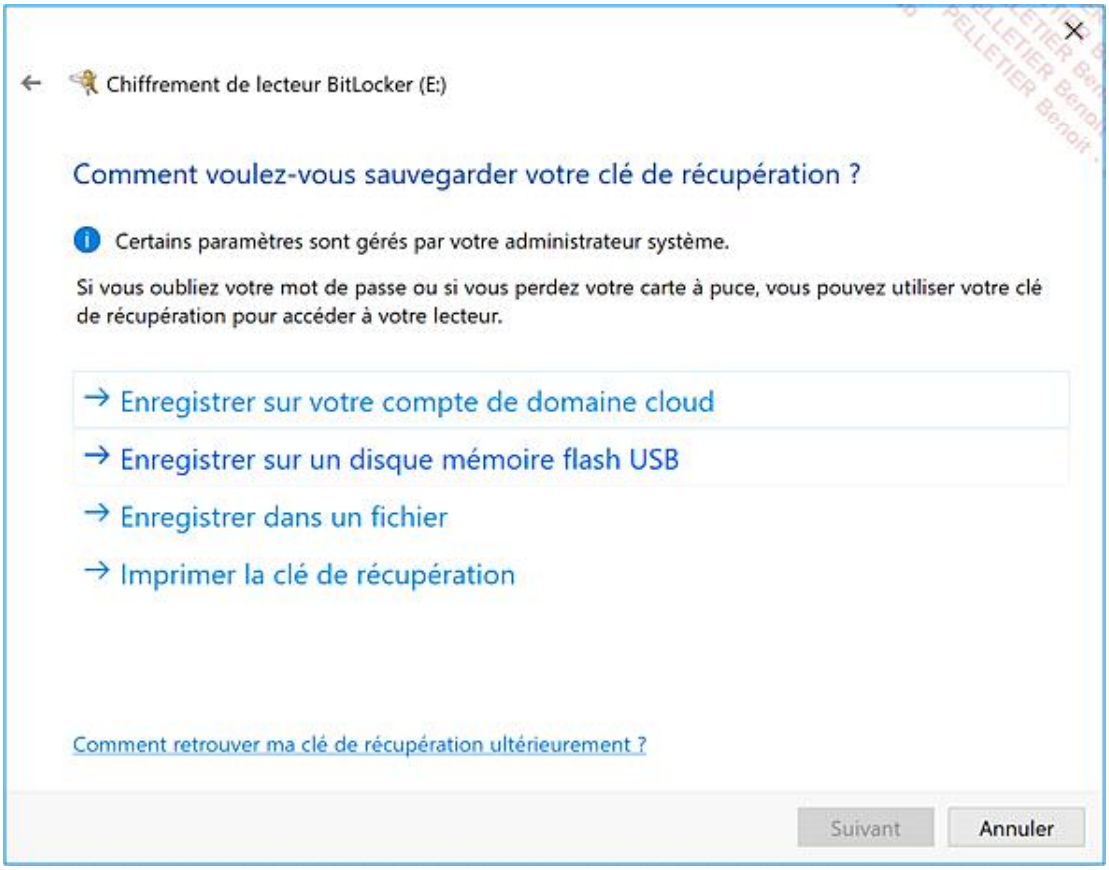
La sécurisation des postes à forte mobilité est un problème récurrent. L'activation de BitLocker est possible mais peut, dans le cas d'un poste en workgroup, être risquée. En effet, en cas de perte des clés de déverrouillage et de récupération, il peut être impossible de déverrouiller une partition.

Il est possible, depuis Windows 10, de stocker la clé de récupération BitLocker dans Azure AD. Il est évidemment nécessaire que la machine soit jointe à l'annuaire Azure AD.

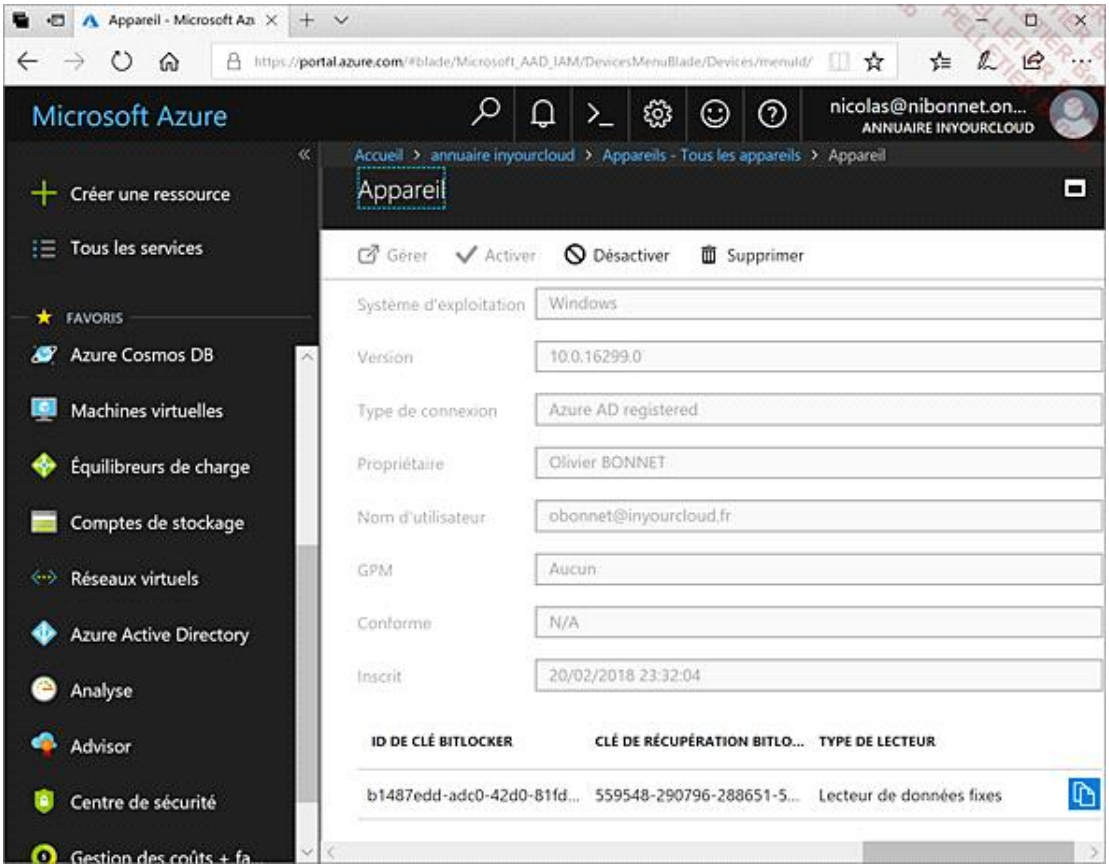
Par la suite, BitLocker peut être activé sur la partition système ou la partition de données. Lors de l'activation sur une partition de données, il est dans un premier temps nécessaire de définir le mode de déverrouillage.



Il est par la suite possible de procéder à l'ajout de la clé de récupération dans une base Azure AD. Pour cela, il est nécessaire de sélectionner l'option **Enregistrer sur votre compte de domaine cloud**.



Après avoir effectué le chiffrement de la partition, la clé de récupération est stockée dans l'annuaire Azure AD.



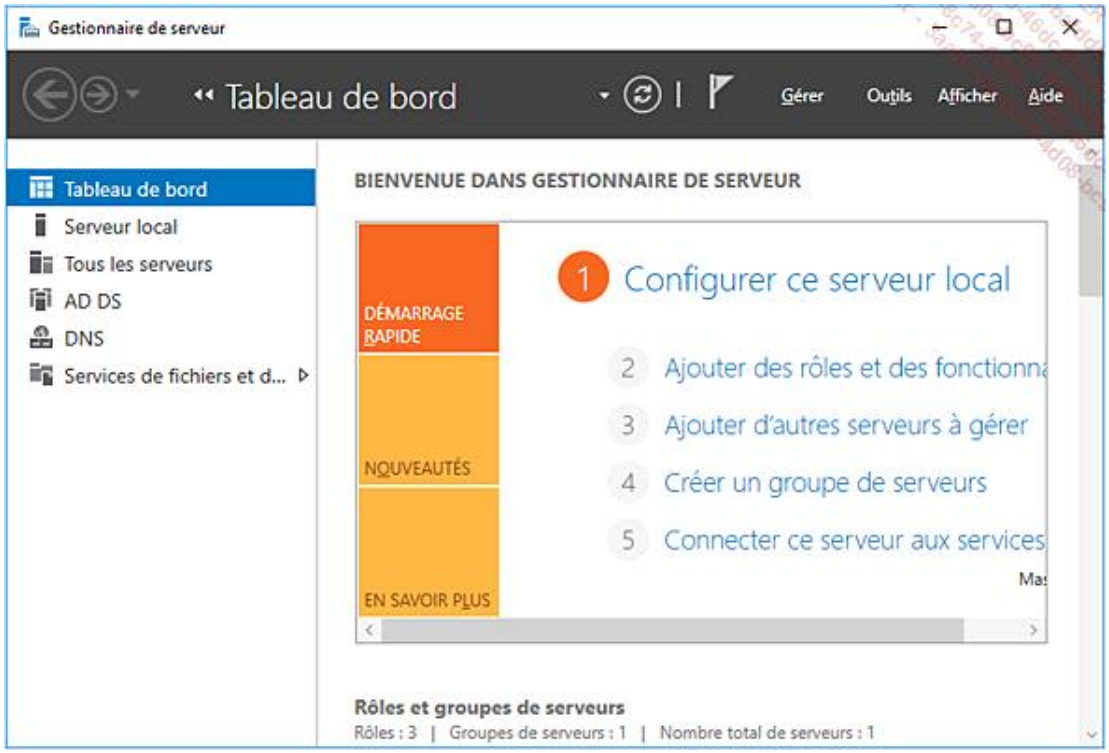
La clé de récupération pourra être utilisée pour déverrouiller de manière temporaire la partition.

Le gestionnaire de serveur

La console **Gestionnaire de serveur** permet la gestion de l'ensemble du serveur (configuration locale, rôle…). On peut y effectuer des opérations de configuration du serveur (adressage IP, nom du serveur…) mais également installer et accéder aux différents rôles (DNS, DHCP…).

Présente depuis Windows Server 2008 et Windows Server 2008 R2, elle a été améliorée avec Windows Server 2012/2012 R2 afin d'offrir une meilleure ergonomie.

Elle permet l'ajout et la suppression de rôles mais également la gestion de serveurs distants. Un groupe de serveurs qui sera géré par le biais de cette console peut être configuré.



Afin de pouvoir gérer les serveurs exécutant un système d'exploitation antérieur à Windows Server 2016, il est nécessaire d'installer les prérequis suivants :

Windows Server 2012 / 2012 R2

.NET Framework 4.6

Windows Management Framework 5.0

Windows Server 2008 R2

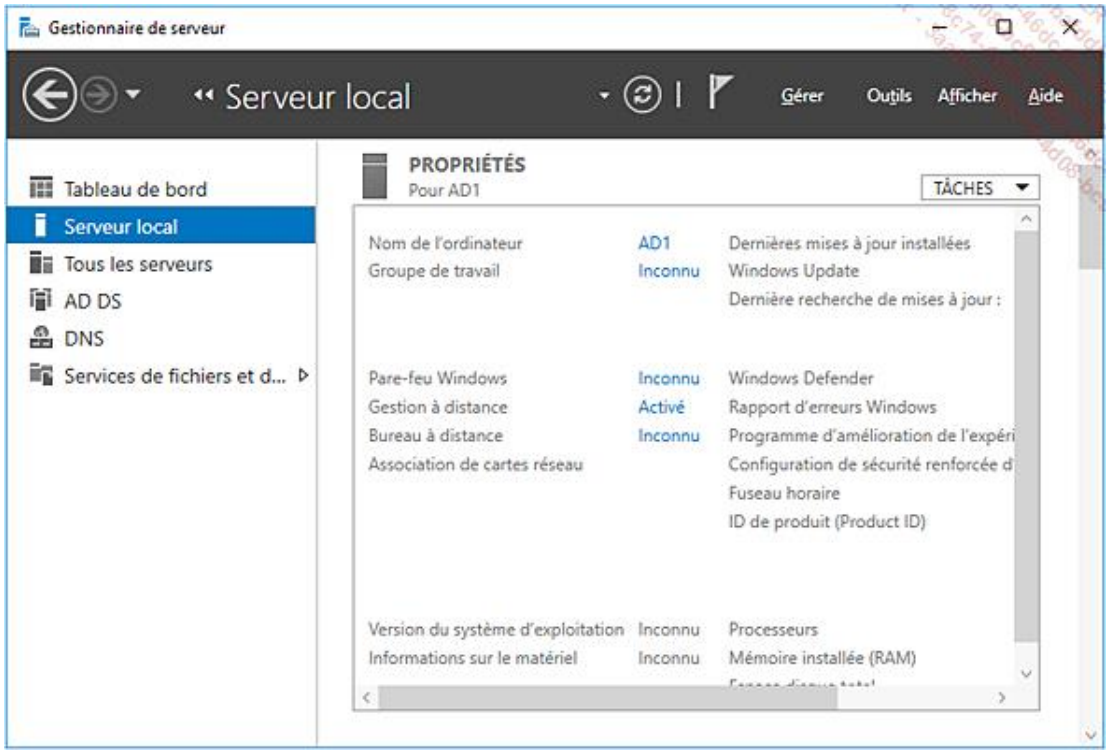
.NET Framework 4.5

Windows Management Framework 4.0

Windows Server 2008

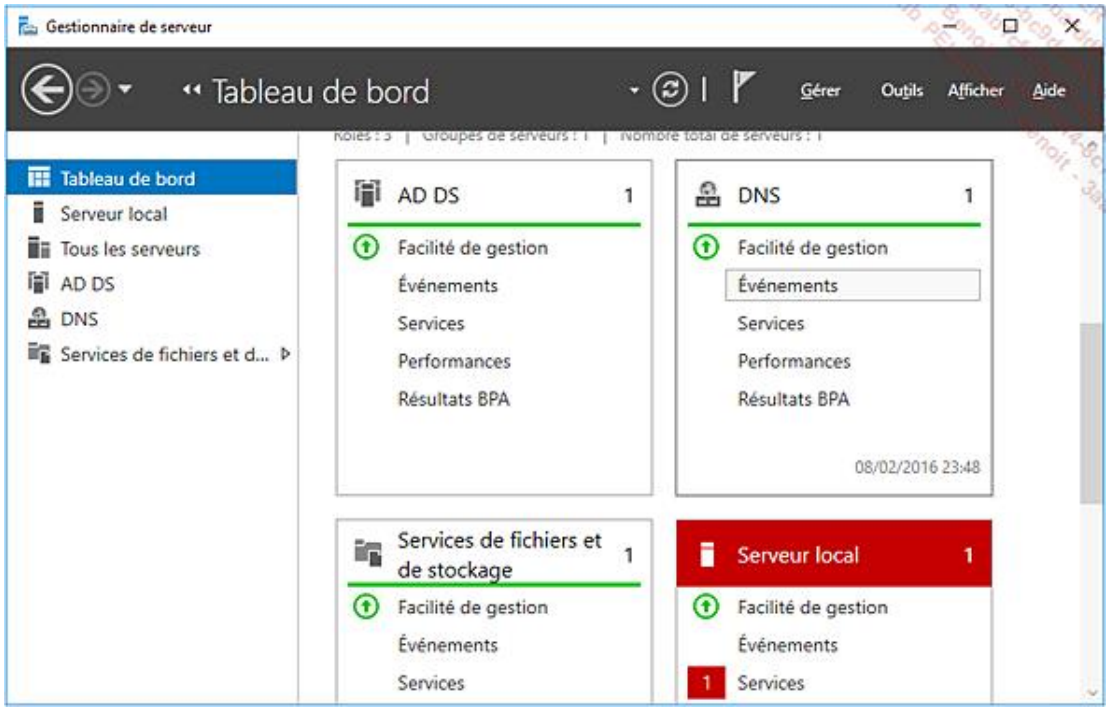
.NET Framework 4

La gestion du serveur local se fait également par le biais de cette console. Certaines informations peuvent être modifiées très rapidement. On retrouve le nom de l'ordinateur, le groupe de travail ou le domaine dont la machine est membre. Le bureau à distance ou la gestion à distance sont également configurables.



La propriété **Configuration de sécurité renforcée d'Internet Explorer** permet d'activer ou désactiver la sécurité renforcée d'Internet Explorer. Par défaut, l'option est activée.

Le **Tableau de bord** permet pour sa part de s'assurer très rapidement du bon état de santé des services. En cas de services arrêté, l'information s'affiche directement dans la console.



Ainsi, on peut voir sur l'écran précédent que les rôles **Services de fichiers et de stockage**, **AD DS** et **DNS** fonctionnent correctement. **Serveur local** a, quant à lui, un service arrêté.

Plusieurs points sont audités : les événements, les services, les performances et les BPA. Si un chiffre précède une catégorie, cela indique à l'administrateur qu'un ou plusieurs éléments sont à visualiser.

En cliquant sur **Événements**, une fenêtre présentant les détails de cet événement s'affiche.

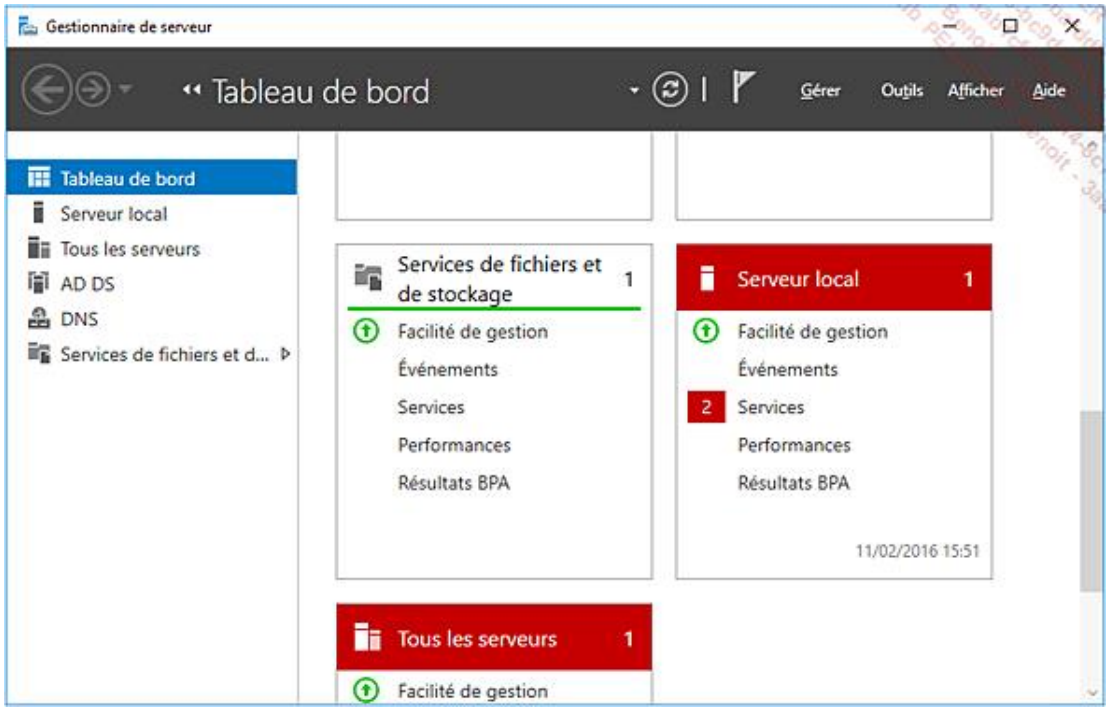
- Sur le serveur local, exécutez la commande `net stop spooler`.

Arrêter le service « spooler » provoque la création d'un nouvel événement. La commande ci-dessus permet d'effectuer l'arrêt de ce service.

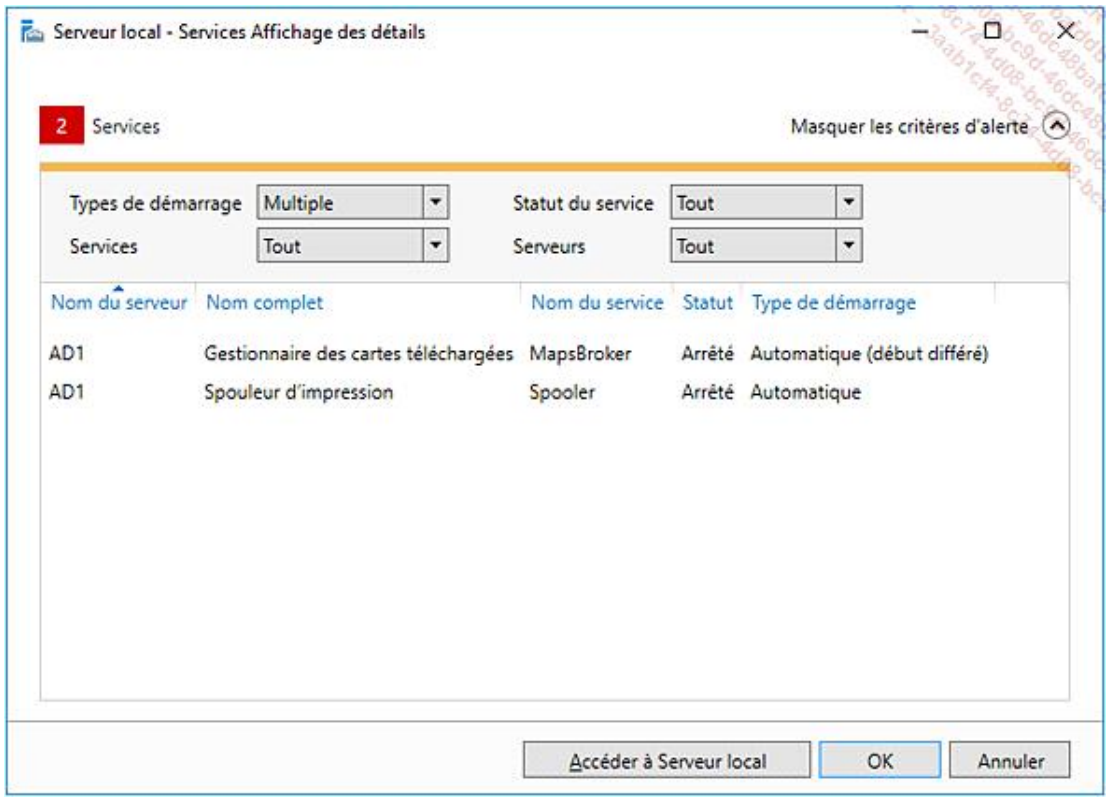


- Relancez la console **Gestionnaire de serveur**, une nouvelle analyse est exécutée.

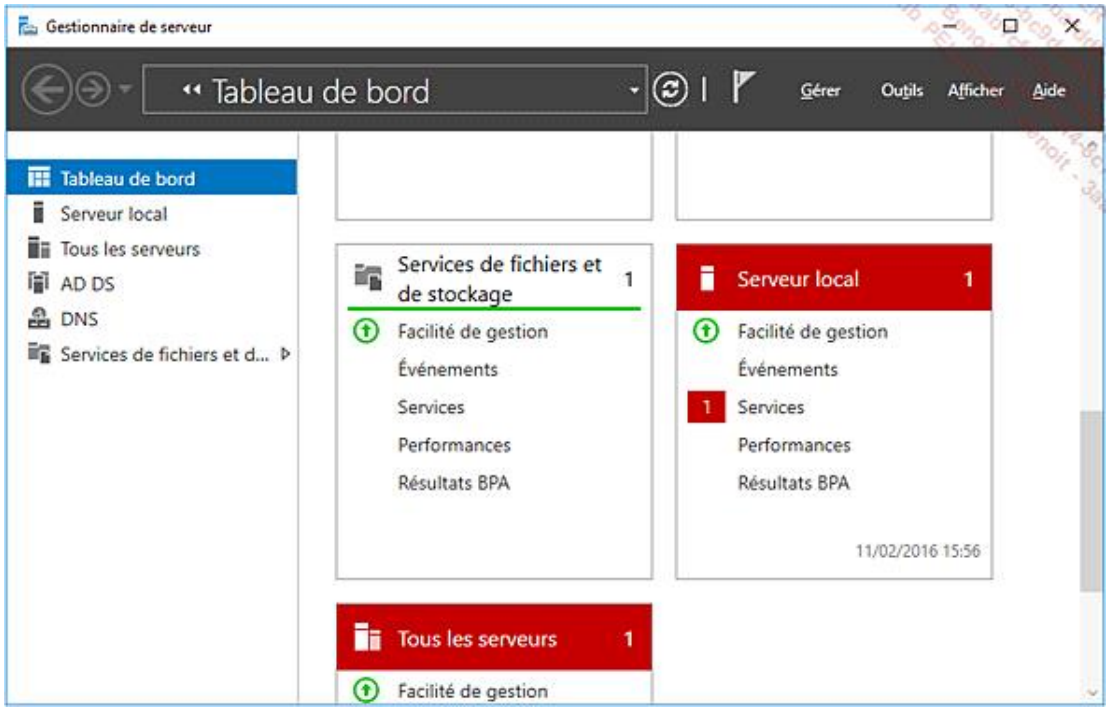
La console nous indique cette fois un problème sur deux services.



- Cliquez sur le lien **Services** afin d'afficher une nouvelle fenêtre présentant le ou les services qui posent problème.



- Effectuez un clic droit sur la ligne du service posant problème puis sélectionnez **Démarrer les services**.
- Cliquez sur **OK** puis cliquez sur le bouton **Actualiser** à droite de **Tableau de bord**.

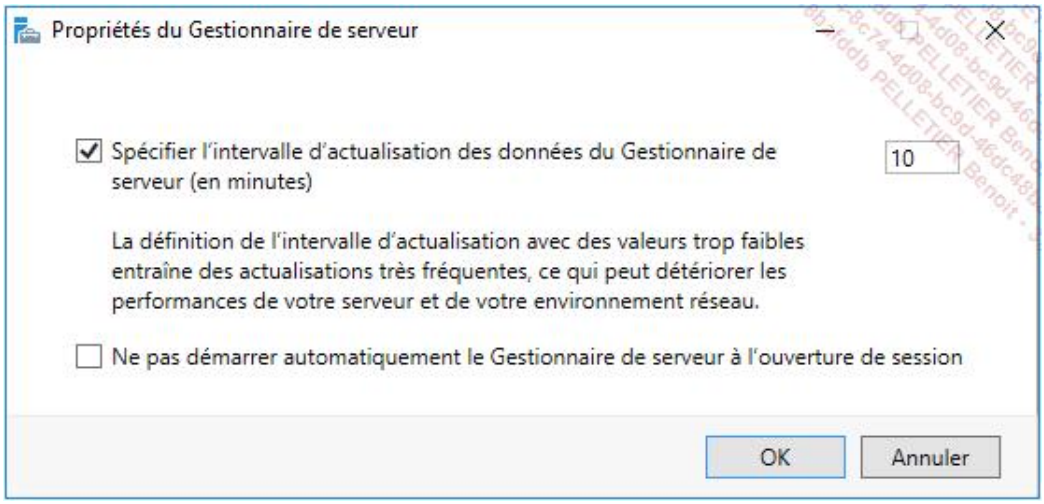


Le problème du service n'apparaît plus. La même opération peut être réalisée pour les serveurs distants. Il est néanmoins obligatoire de créer un groupe comprenant ces serveurs (ce point est traité plus loin dans le chapitre).

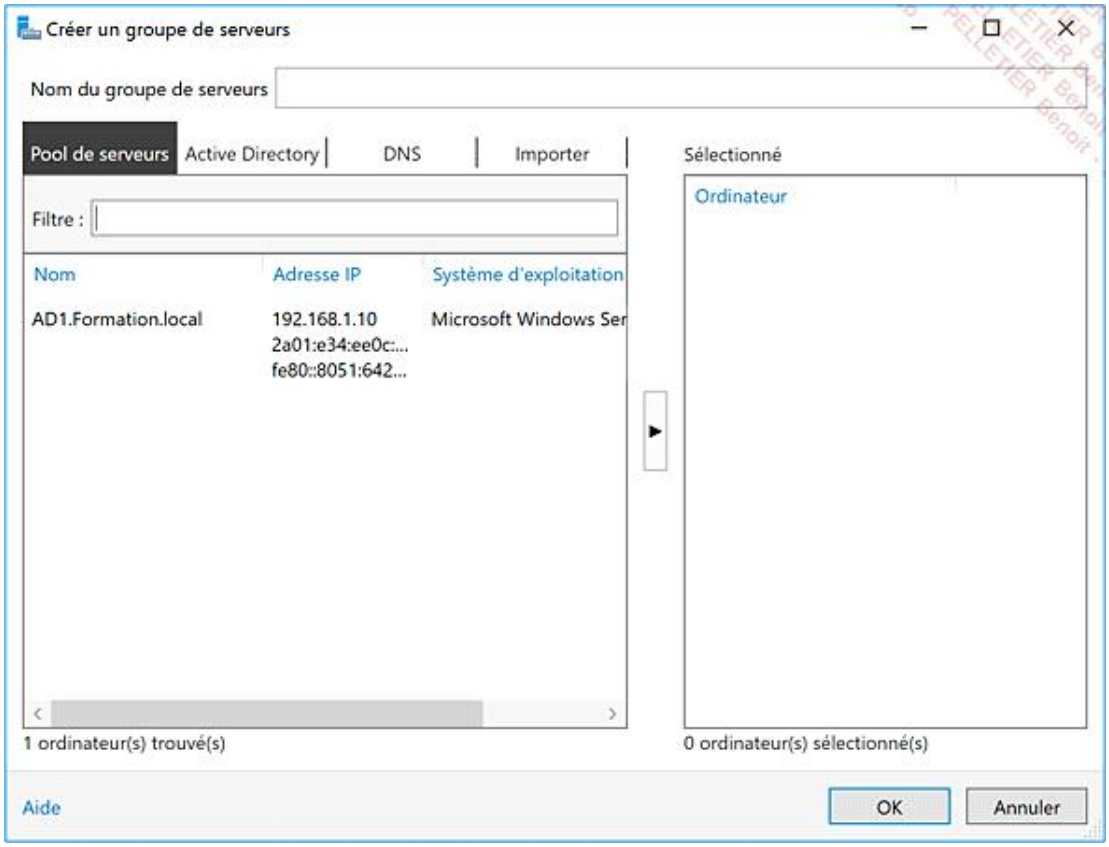
Le menu **Outils** permet d'accéder à un ensemble de consoles (**Gestion de l'ordinateur**, **Services**, **Pare-feu Windows avec fonctionnalités avancées de sécurité**…) et d'outils (**Diagnostic de mémoire Windows**, **Windows PowerShell**…).

Lors du clic sur le lien **Gérer**, un menu contextuel s'affiche donnant accès à un ensemble d'options :

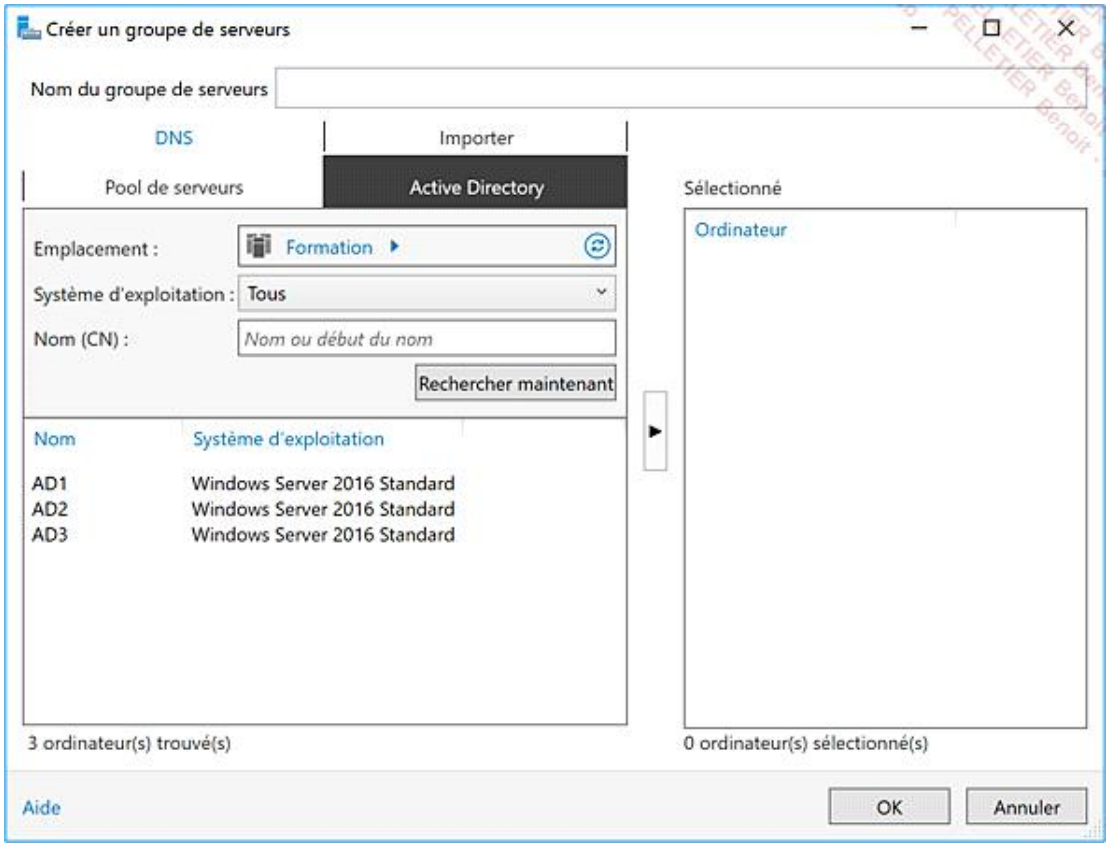
- **Propriétés du Gestionnaire de serveur** : il est possible de spécifier un délai d'actualisation des données de la console **Gestionnaire de serveur**. Par défaut, la valeur est configurée à 10 minutes. Le Gestionnaire peut être configuré afin de ne pas se lancer automatiquement lors de l'ouverture de session.



- **Créer un groupe de serveurs** : afin de pouvoir gérer plusieurs serveurs depuis cette machine, il convient de créer un groupe de serveurs. Par la suite, il est possible d'installer/supprimer des rôles ou simplement d'en effectuer la surveillance. L'ajout peut se faire par la saisie d'un nom ou d'une adresse IP dans l'onglet **DNS**.



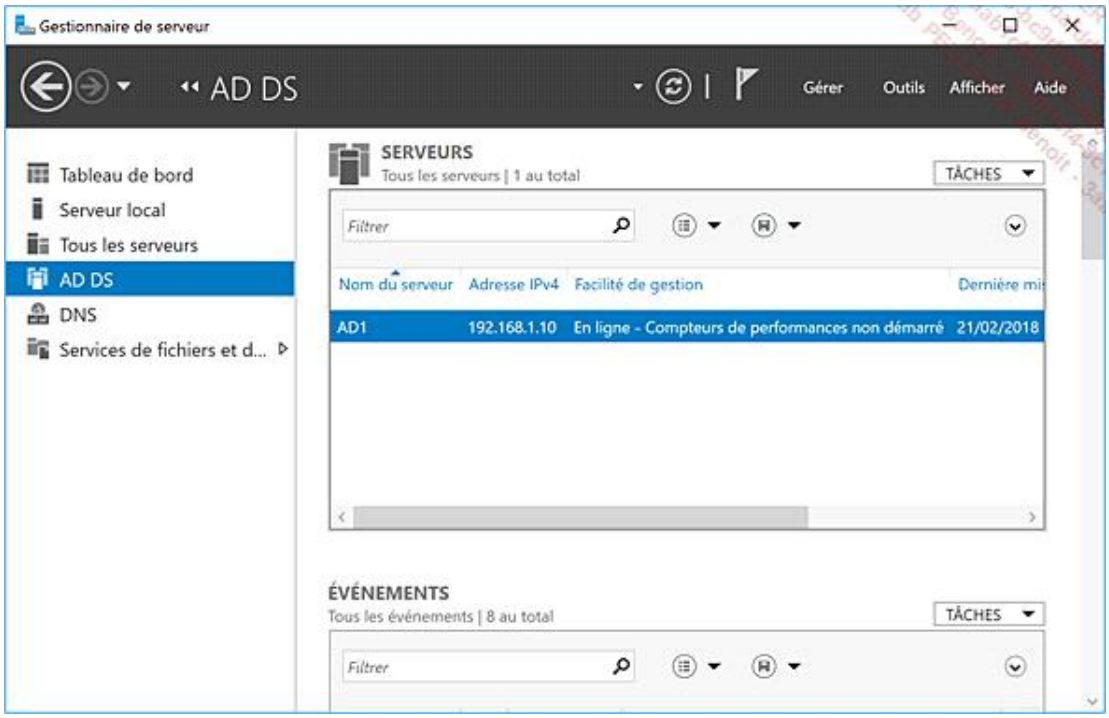
La recherche du poste peut également être effectuée à l'aide d'Active Directory, en sélectionnant l'emplacement (racine du domaine, unité d'organisation…) ou en saisissant le nom de la machine.



- **Ajouter/supprimer des rôles et fonctionnalités** : les opérations d'ajout ou de suppression peuvent être effectuées

sur le serveur local ou sur une machine distante.

Lors de l'ajout d'un nouveau rôle, un nouveau nœud apparaît dans la colonne de gauche de la console **Gestionnaire de serveur**. En cliquant dessus, le panneau central donne accès aux événements du rôle, BPA...

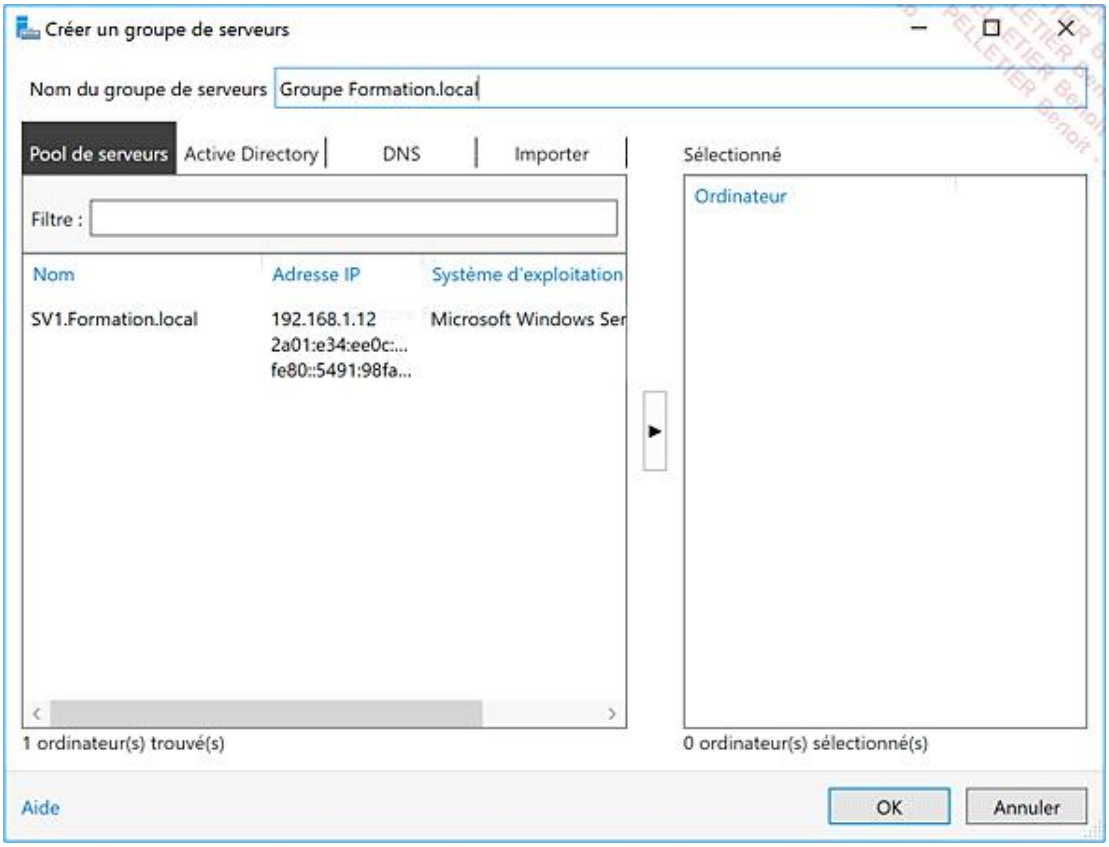


1. Création d'un groupe sur les serveurs

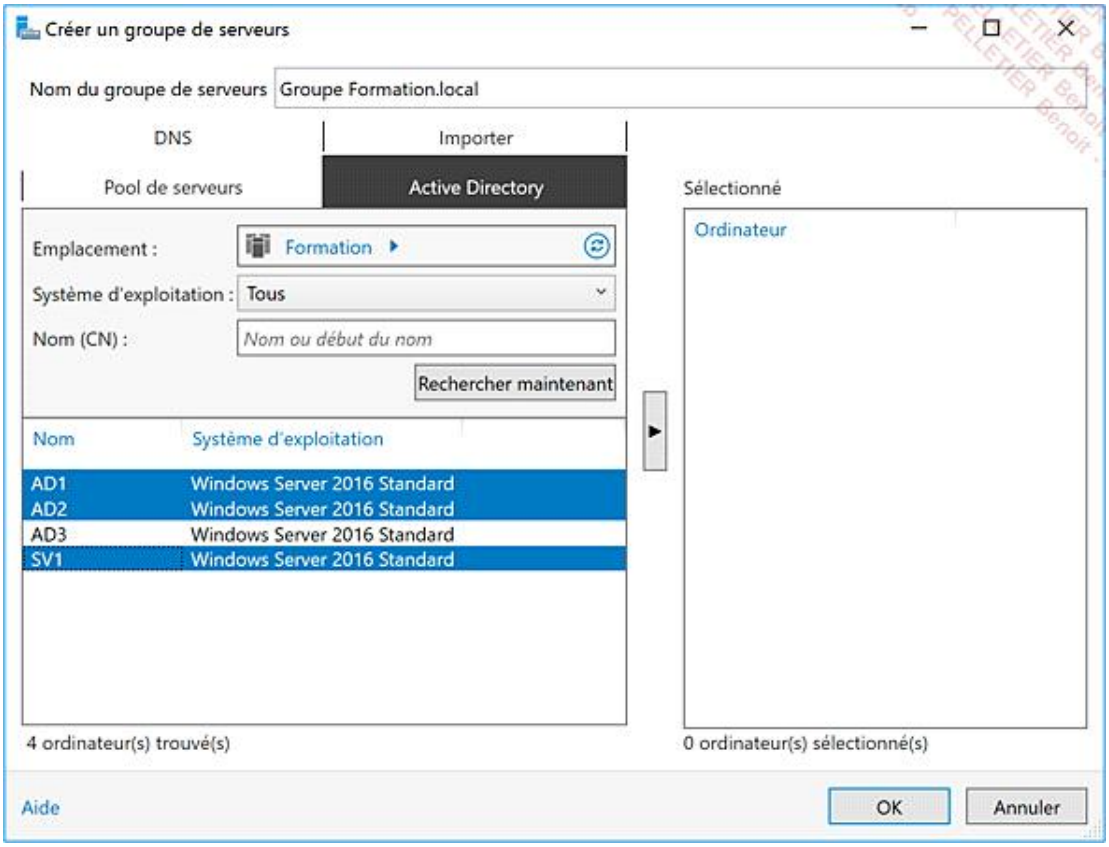
Comme nous avons pu le voir, la création d'un groupe nous permet d'effectuer l'administration à distance.

Pour effectuer les opérations ci-dessous, il est nécessaire de s'assurer que AD2 et SV1 sont membres du domaine.

- Joignez la machine **SV1** au domaine. Au redémarrage, lancez la console **Gestionnaire de serveur** si celle-ci ne s'affiche pas toute seule. Cliquez sur **Gérer** puis sélectionnez **Créer un groupe de serveur**.
- Dans le champ **Nom du groupe de serveurs**, saisissez **Groupe Formation.local**.

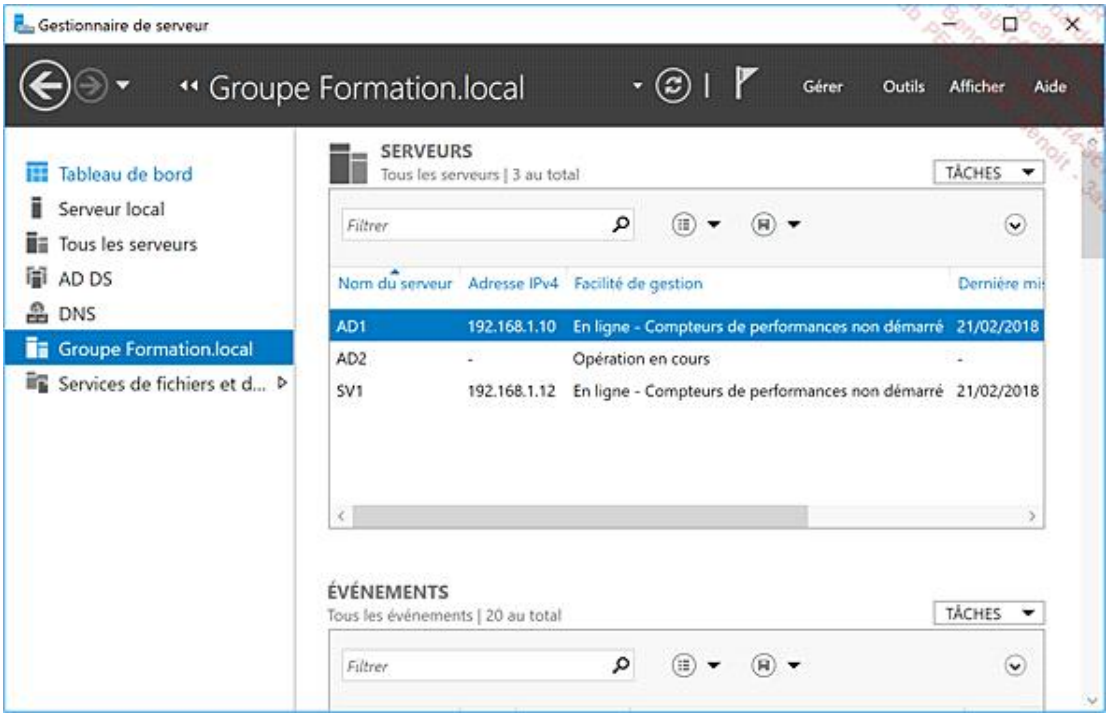


- Cliquez sur l'onglet **Active Directory**.
- Cliquez sur le bouton **Rechercher maintenant**.
- Sélectionnez **AD1**, **AD2** puis **SV1** et cliquez sur le bouton présent entre les champs de sélection et la liste **Selectionné** dans le but de les insérer dans le groupe.



- Cliquez sur **OK** afin de valider la création du groupe.

Le nouveau groupe est présent dans la console **Gestionnaire de serveur**.

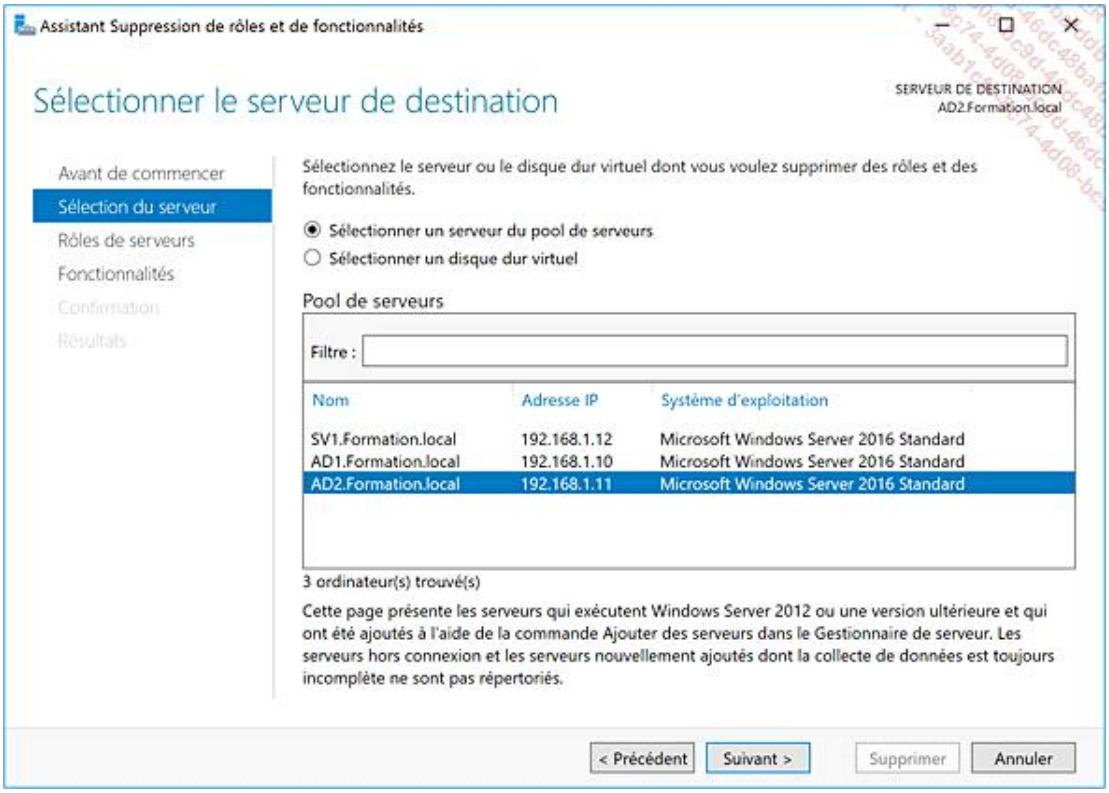


Ce groupe permet de récupérer l'état de santé des serveurs et d'effectuer des tâches à distance.

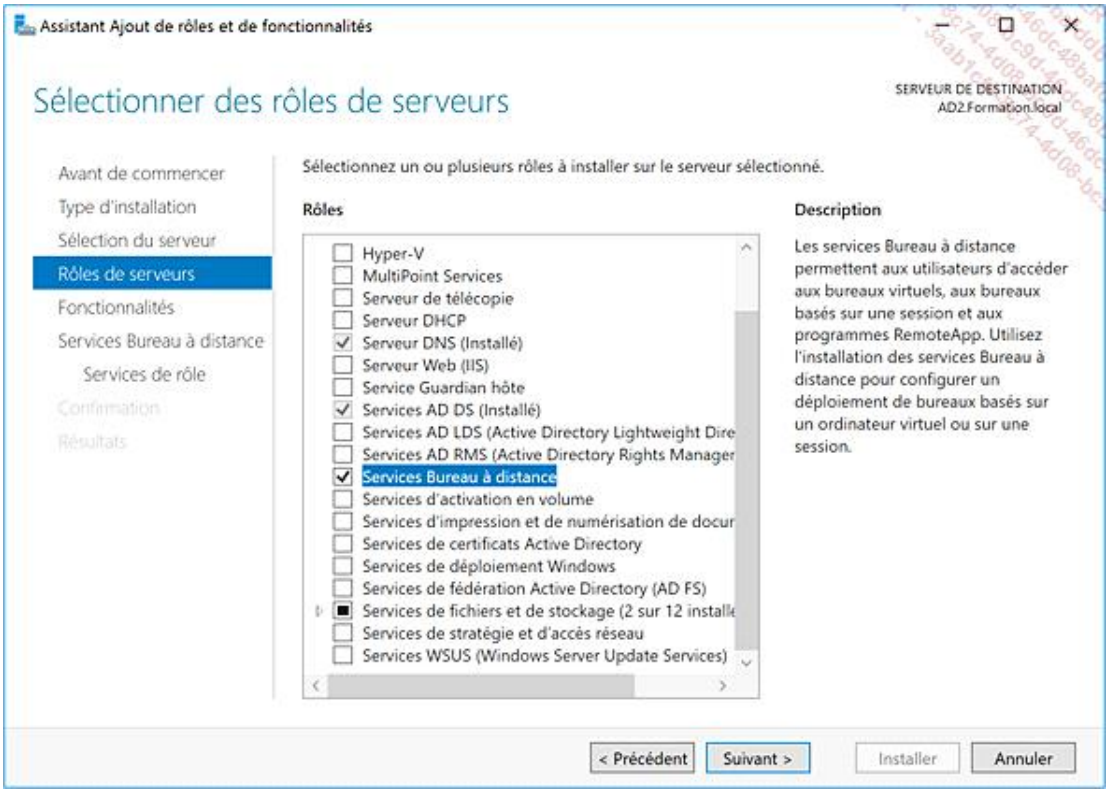
2. Installation d'un rôle à distance

Le groupe a été créé sur **SV1**. Nous allons donc nous servir de ce serveur pour installer le rôle Fax Server sur **AD2**.

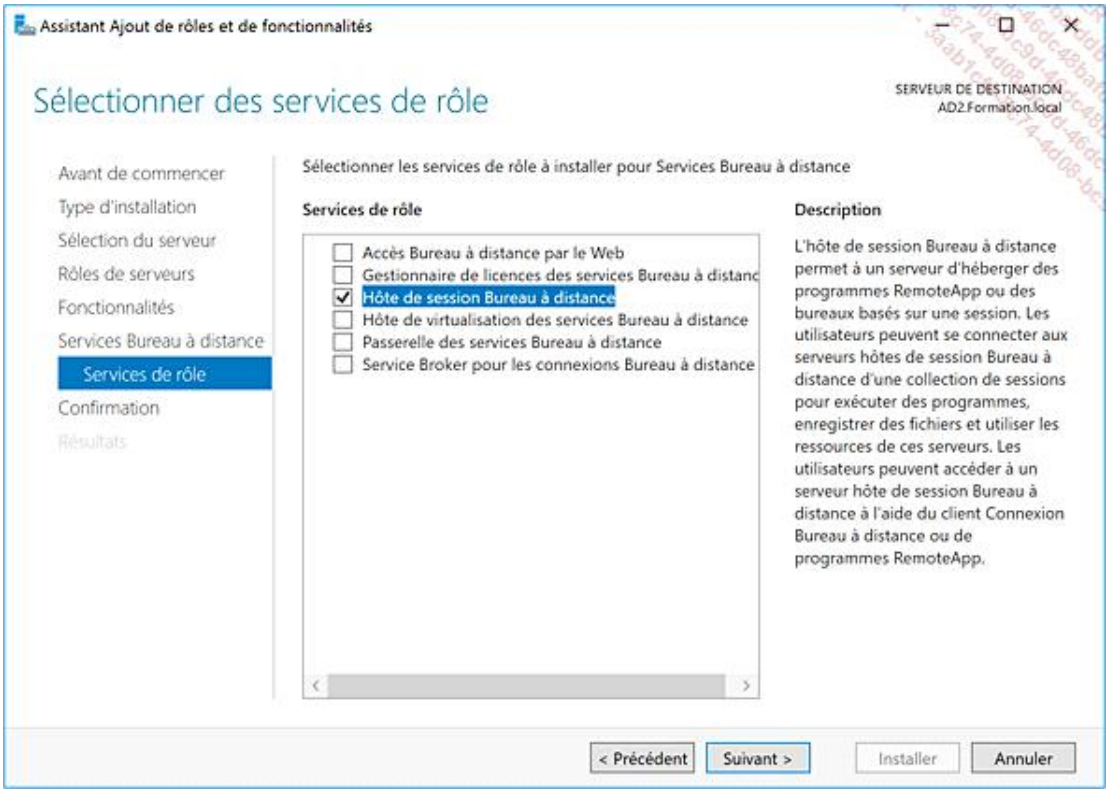
- Dans la console **Gestionnaire de serveur**, cliquez sur **Gérer** puis sur **Ajouter des rôles et des fonctionnalités**.
- Dans la fenêtre **Selectionner le type d'installation**, laissez le choix par défaut et cliquez sur **Suivant**.
- Sélectionnez **AD2.Formation.local** puis cliquez sur **Suivant**.



- Cochez **Services Bureau à distance**.

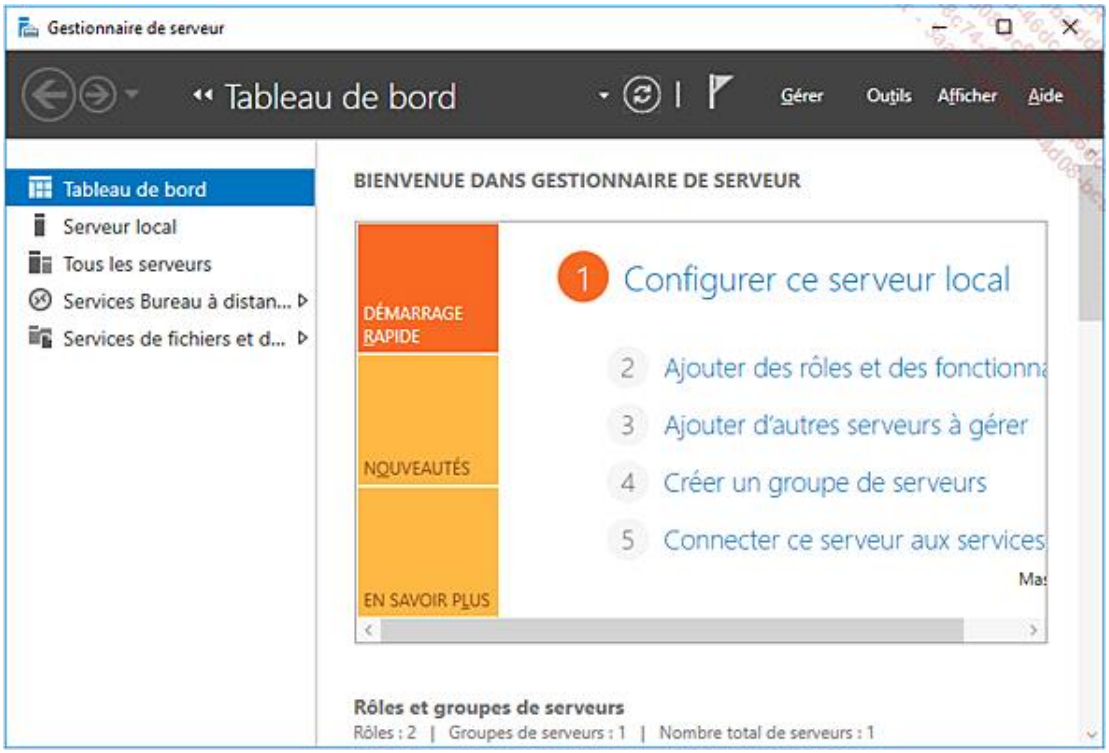


- Cliquez sur **Suivant** dans les fenêtres **Sélectionner les fonctionnalités** puis cochez **Hôte de session Bureau à distance**. Cliquez sur **Ajouter des fonctionnalités**.



Confirmez l'installation en cliquant sur le bouton **Installer**.

Le rôle est bien installé sur le serveur **AD2**.



Il est également possible de demander au poste distant de redémarrer depuis la console **Gestionnaire de serveur**.

Outils d'administration de serveur distant

Depuis de nombreuses années, il est possible de télécharger les outils RSAT afin d'effectuer l'administration à distance. Très pratiques, ils permettent d'administrer les différents rôles installés sur les serveurs. Les manipulations s'effectueront depuis le poste client ou un serveur d'administration sans avoir à se connecter en bureau à distance à la machine concernée.

L'outil ajoute simplement les composants logiciels enfichables utilisés par la console MMC.

1. Téléchargement des fichiers RSAT

Anciennement appelés Adminpack, les fichiers utilisés portent depuis Windows Server 2008 le nom de RSAT (*Remote Server Administration Tools*). À chaque changement majeur (changement de système d'exploitation, ...), il convient de réinstaller les bonnes versions.

Afin d'administrer Windows Server 2016, il est nécessaire de télécharger l'outil sur le site web de Microsoft. Les outils RSAT pour Windows 10 sont disponibles en accédant à l'URL suivante : https://www.microsoft.com/en-us/download/details.aspx?id=45520

Le fichier téléchargé peut être installé sur Windows 10.

2. Installation des outils d'administration

Il est nécessaire que le système d'exploitation utilise la même langue que les outils RSAT.

- Ouvrez une session sur CL10-01 en tant qu'administrateur puis configurez la carte réseau de la machine comme ci-dessous :

  Adresse IP : 192.168.1.14

  Masque de sous-réseau : 255.255.255.0

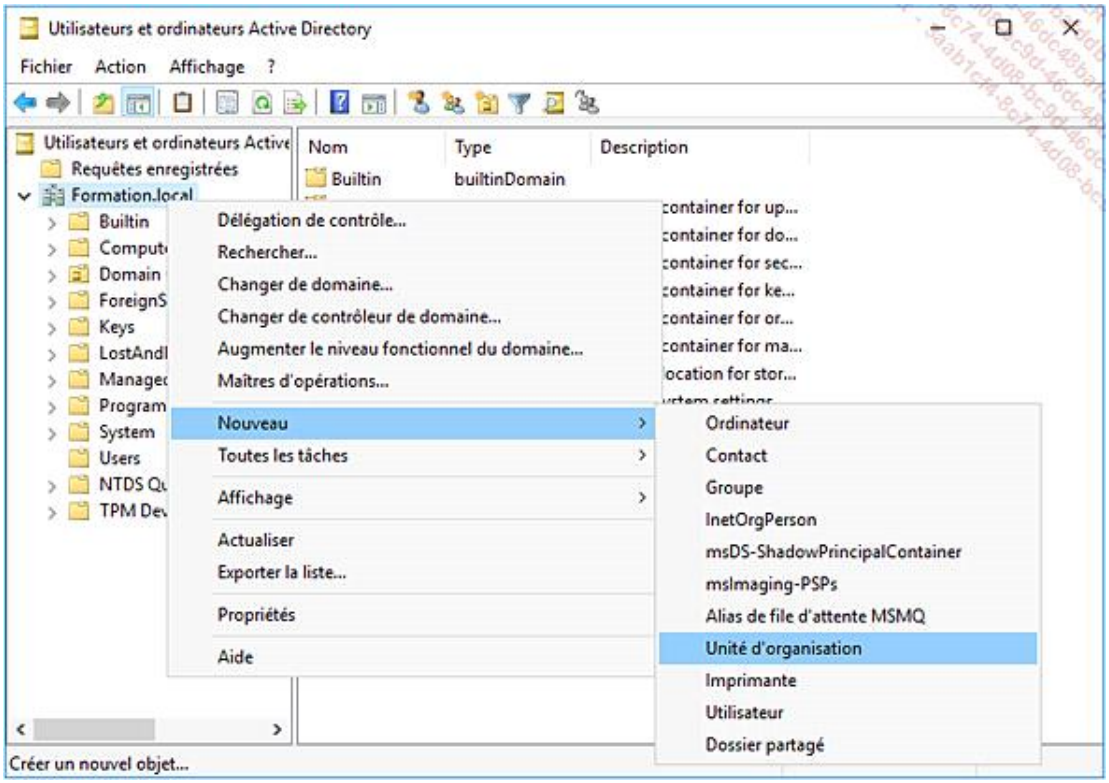
  Passerelle par défaut : 192.168.1.254

  Serveur DNS Préféré : 192.168.1.10

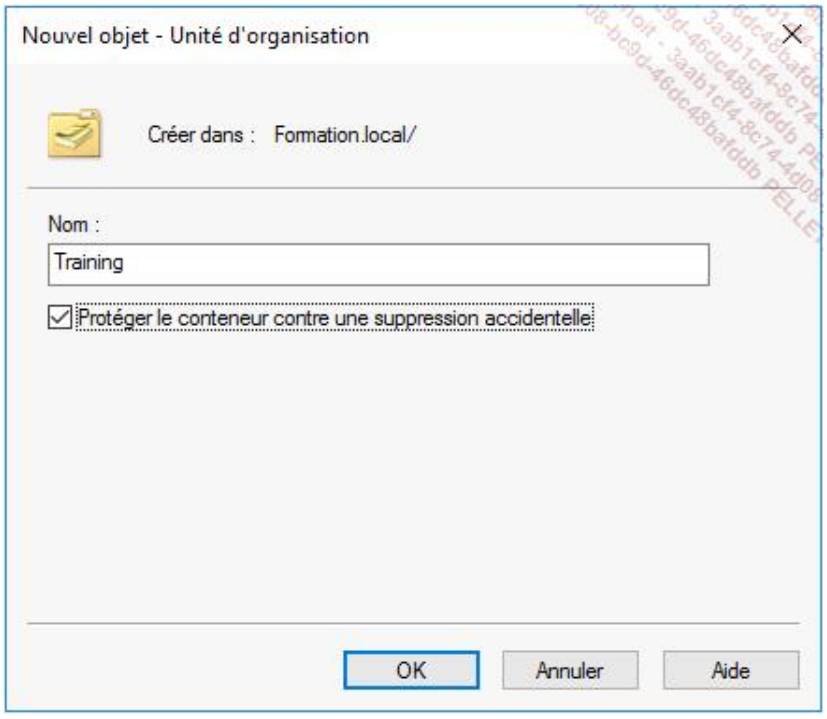
  Joignez la machine au domaine Formation.local

  Sur **AD1**, lancez la console **Utilisateurs et ordinateurs Active Directory**.

- Effectuez un clic droit sur la racine du domaine, dans le menu contextuel cliquez sur **Nouveau** et **Unité d'organisation**.

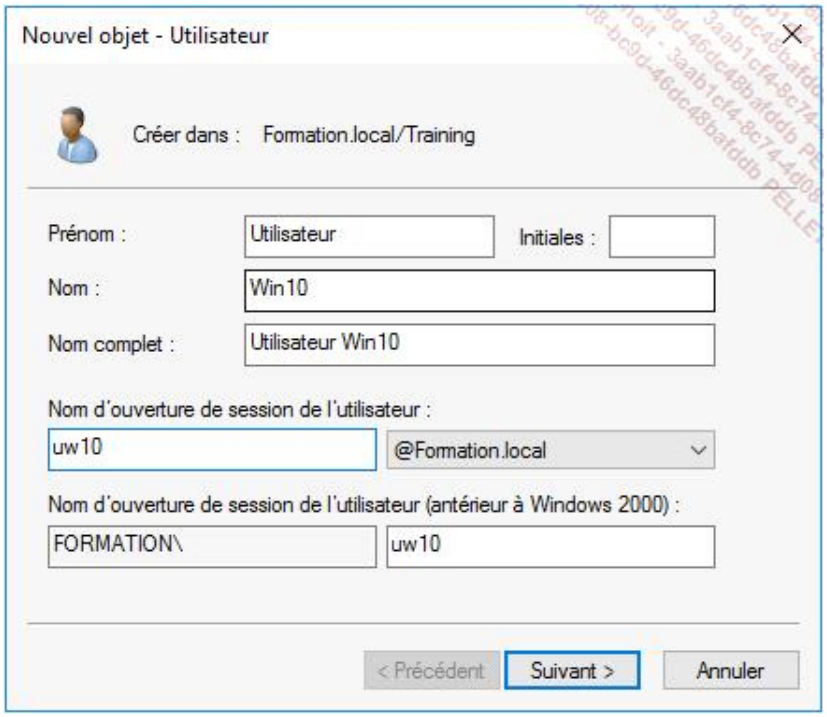


- Nommez l'OU **Training** puis cliquez sur **OK**.

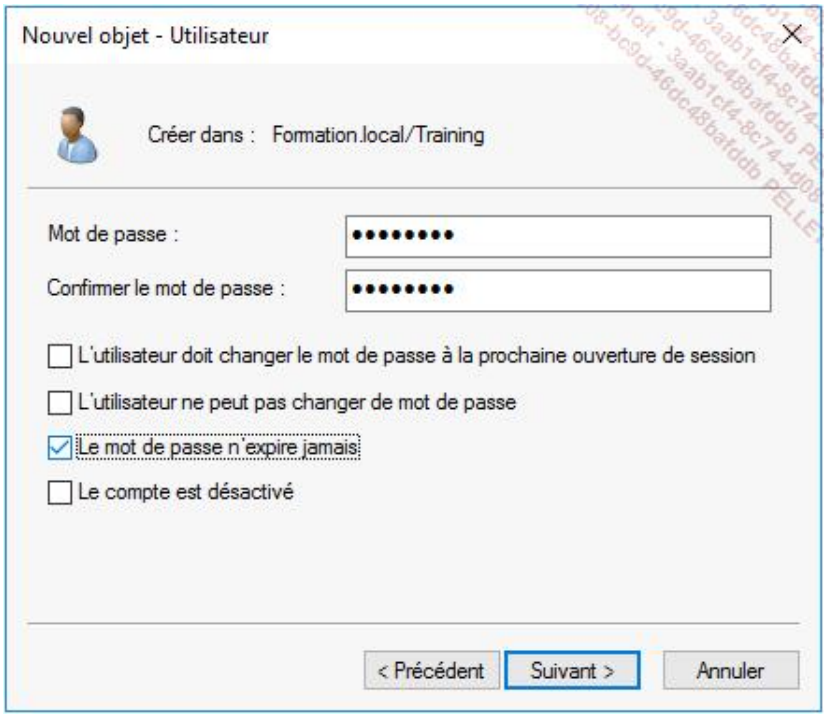


Dans le conteneur précédemment créé, effectuez la création d'un utilisateur.

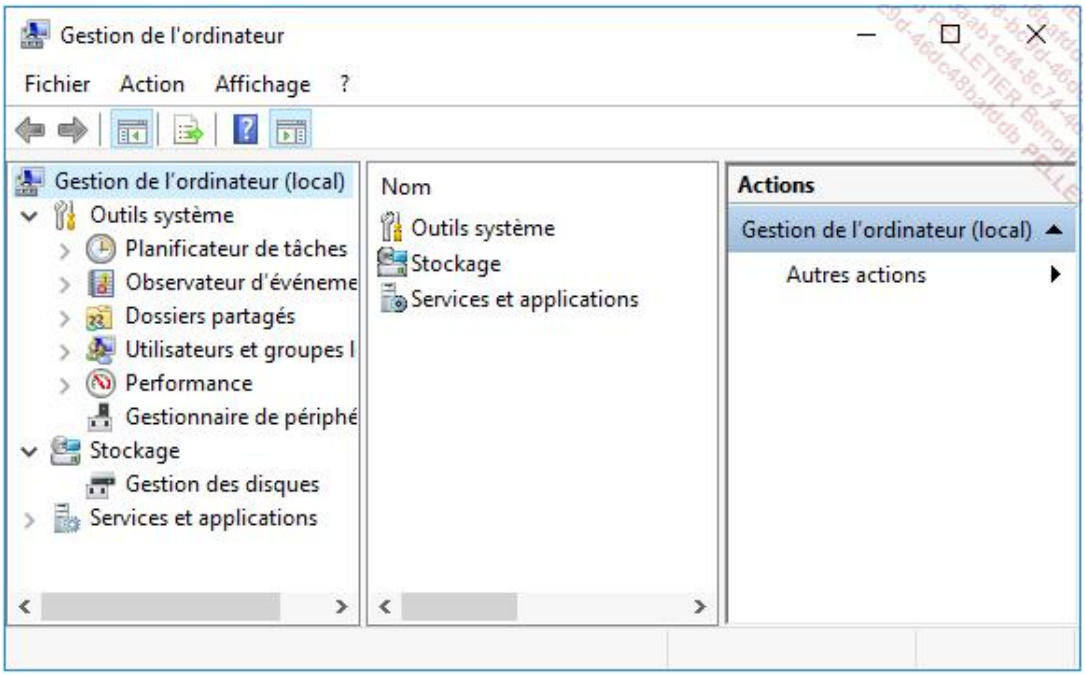
- Effectuez un clic droit sur l'OU **Training** puis dans le menu contextuel, sélectionnez **Nouveau** puis **Utilisateur**.
- Configurez l'utilisateur comme ci-dessous.



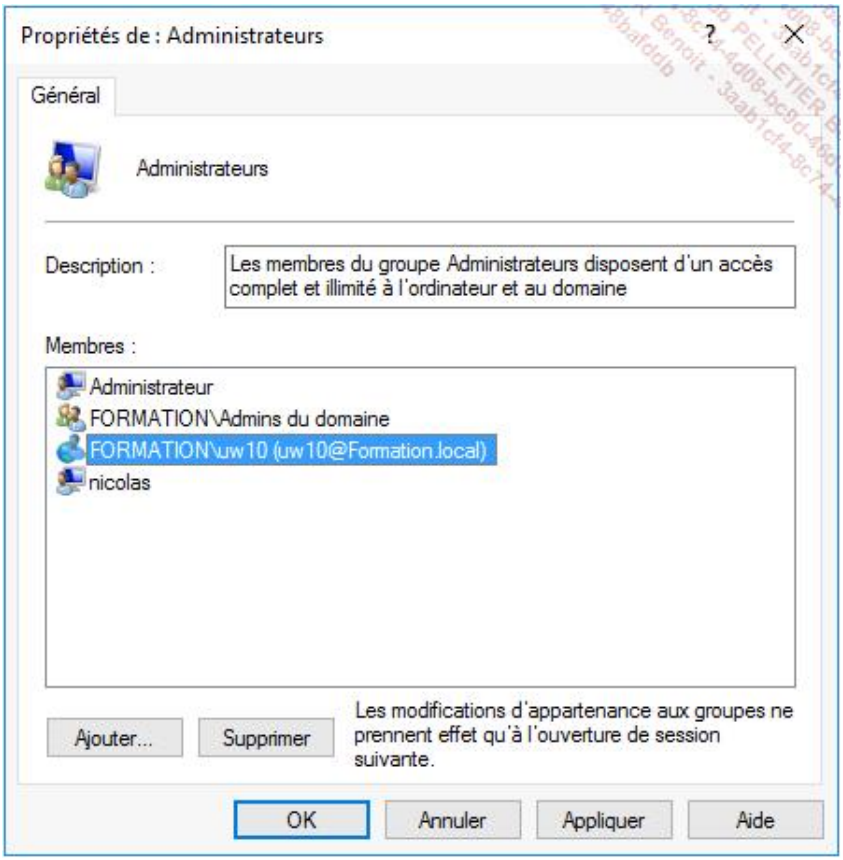
- Saisissez **Password** dans les champs mot de passe puis cliquez sur **Le mot de passe n'expire jamais**.



- Sur le poste CL10-01 ouvrez une session en tant que Formation\administrateur puis lancez la console **Gestion de l'ordinateur** (clic droit sur **Ce PC** dans l'Explorateur Windows puis **Gérer**).



- Sélectionnez **Utilisateurs ou groupes** puis double cliquez sur **Administrateurs**.
- Ajoutez le compte précédemment créé à l'aide du bouton **Ajouter**.



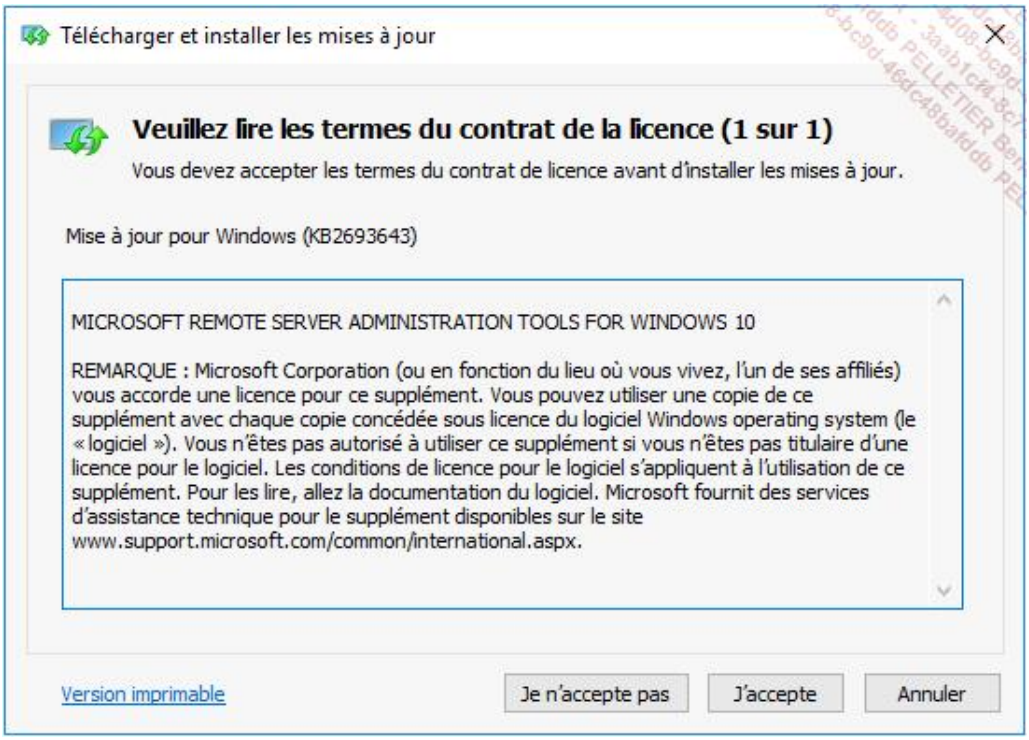
- Cliquez sur **OK** puis ouvrez une session avec cet utilisateur.
- Téléchargez le fichier RSAT pour Windows 10 :

  https://www.microsoft.com/fr-FR/download/details.aspx?id=45520

- Cliquez sur **Oui** afin de lancer l'installation.

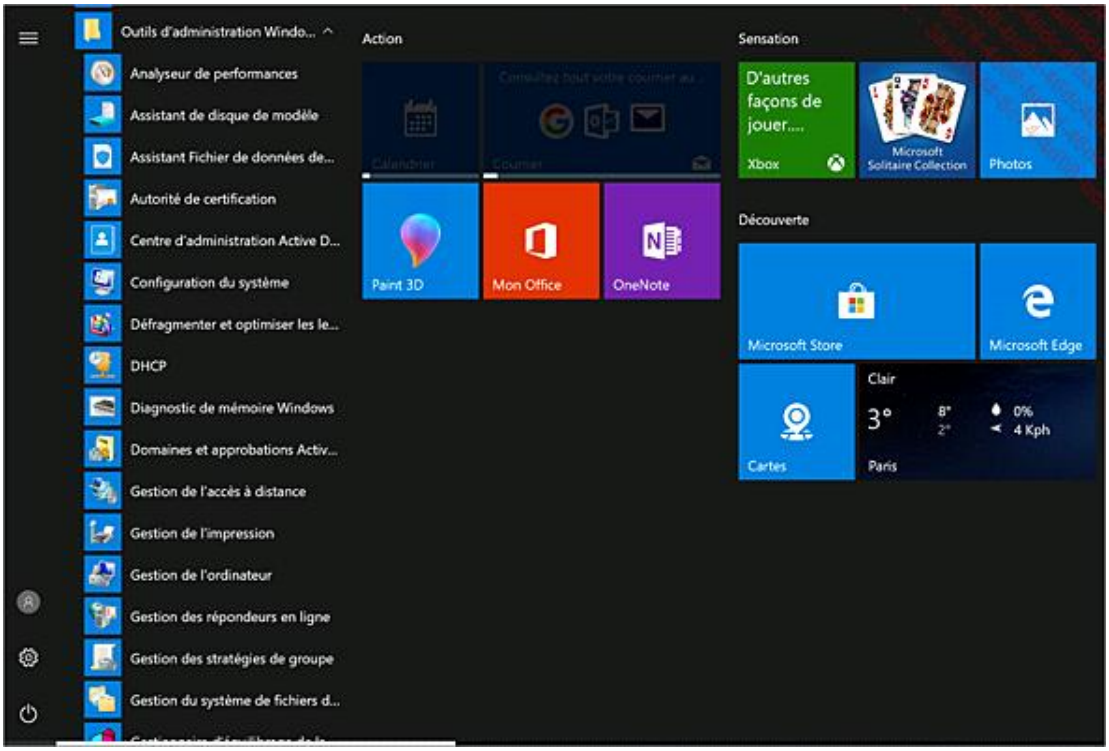
Acceptez la licence afin de poursuivre l'installation.

L'installation est en cours…



Cliquez sur **Fermer** à la fin de l'installation.

Le **Gestionnaire de serveur** et les outils d'administration sont ajoutés dans le menu Démarrer.



L'administration peut s'effectuer depuis ce poste de travail. L'utilisateur doit avoir les droits d'administration adéquats.

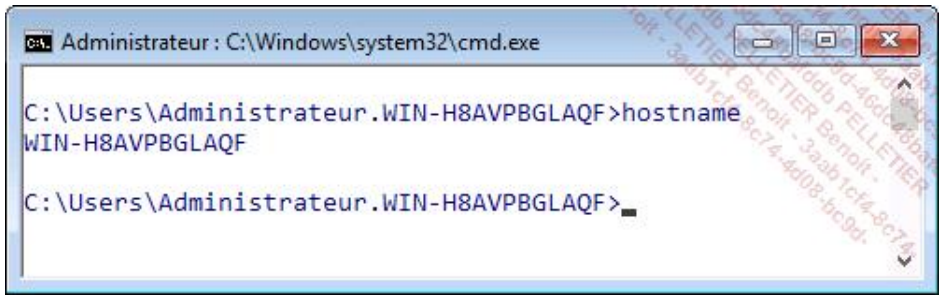
Serveur en mode installation minimale

Lorsqu'un serveur est installé en mode **Installation minimale**, le programme **explorer.exe** n'est pas installé. Seule l'invite de commandes est présente.

- Démarrez la machine virtuelle **SRVCore** puis ouvrez une session en tant qu'**administrateur**.

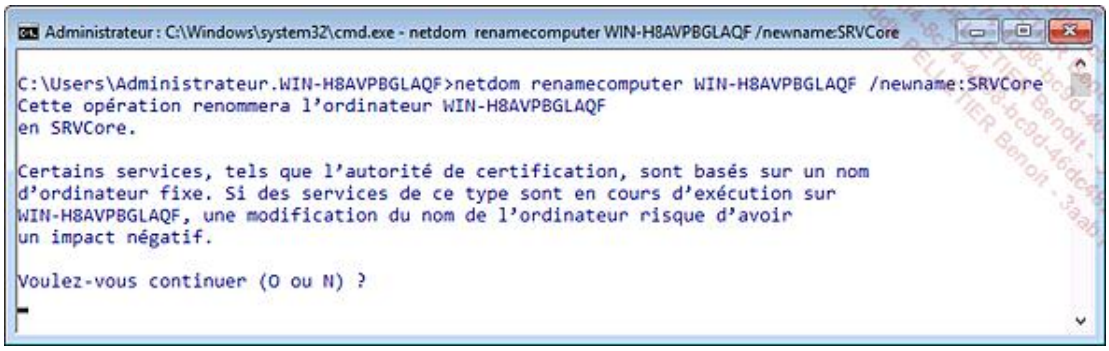
Si cela n'a pas été fait auparavant, définissez le mot de passe de l'administrateur local.

- Saisissez dans l'invite de commandes DOS la commande `hostname`.



- Tapez dans l'invite de commandes DOS `netdom renamecomputer NomActuel /NewName:SRVCore` puis appuyez sur [Entrée].

NomActuel peut être remplacé par la variable **%computername%**.

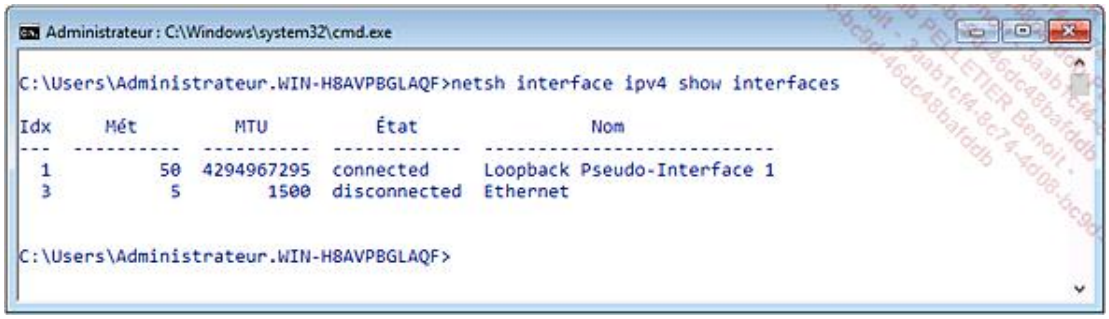


- Saisissez **O** puis appuyez sur la touche [Entrée].
- Redémarrez le serveur à l'aide de la commande `shutdown -r -t 0`.

Le commutateur **-r** permet d'effectuer un redémarrage du serveur, **-t 0** indique un redémarrage immédiat.

Avant de configurer la carte réseau, il est nécessaire de récupérer son nom.

- Saisissez la commande `netsh interface ipv4 show interfaces` puis appuyez sur la touche [Entrée].



Le nom de la carte réseau est **Ethernet**.

- Configurez la carte réseau à l'aide de la commande : `netsh interface ipv4 set address name="NomCarte" source=static address=192.168.1.13 mask=255.255.255.0 gateway=192.168.1.254`

  Puis validez à l'aide de la touche [Entrée].

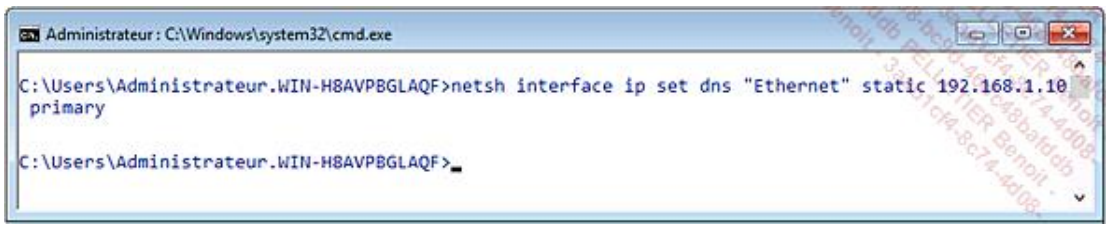
Remplacez **NomCarte** par le véritable nom de la carte réseau, **Ethernet** dans notre cas.



La carte a été configurée mais l'adresse du serveur DNS n'a pas été renseignée.

- Utilisez la commande `netsh interface ip set dns "NomCarte" static 192.168.1.10 primary` puis validez à l'aide de la touche [Entrée].

Remplacez **NomCarte** par le véritable nom de la carte réseau, **Ethernet** dans notre cas.



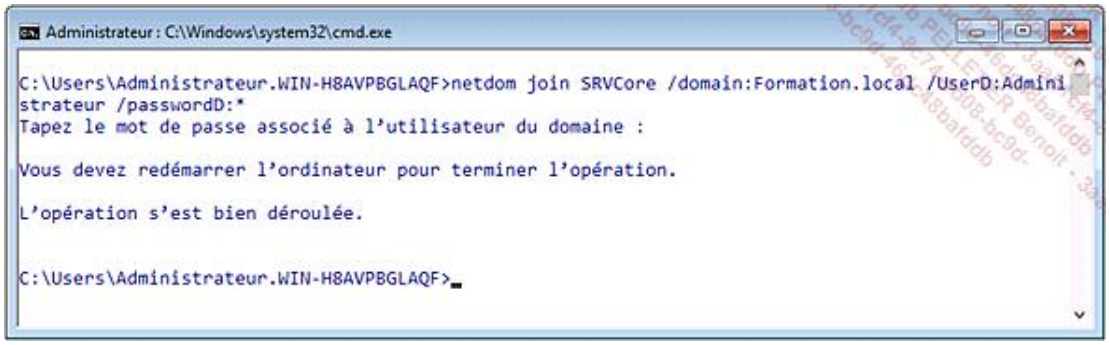
- Vérifiez la configuration de la carte à l'aide de la commande `ipconfig /all`.

Il est maintenant possible de joindre le serveur au domaine.

- Saisissez la commande : `netdom join SRVCore /domain:Formation.local /UserD:Administrateur /passwordD:*`

  Puis appuyez sur la touche [Entrée].

Le mot de passe doit être saisi car l'étoile a été insérée dans le commutateur /**passwordD**. Lors de la saisie, aucun caractère ne s'affiche.



La dernière étape est donc le redémarrage afin de prendre en compte la jonction au domaine.

- Saisissez la commande `shutdown -r -t 0`.
- Désactivez le firewall en saisissant la commande `netsh firewall set opmode disable`.

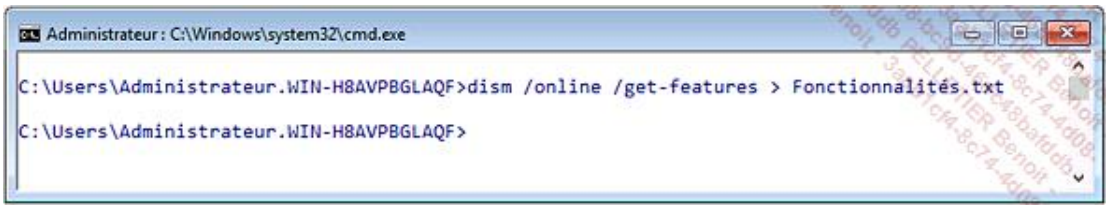
Installation de rôles avec une installation en mode Core

Le serveur ne possède pas d'interface graphique, l'installation doit donc s'effectuer en ligne de commande. Nous allons utiliser la commande `dism` pour lister, activer ou supprimer une fonctionnalité du système d'exploitation.

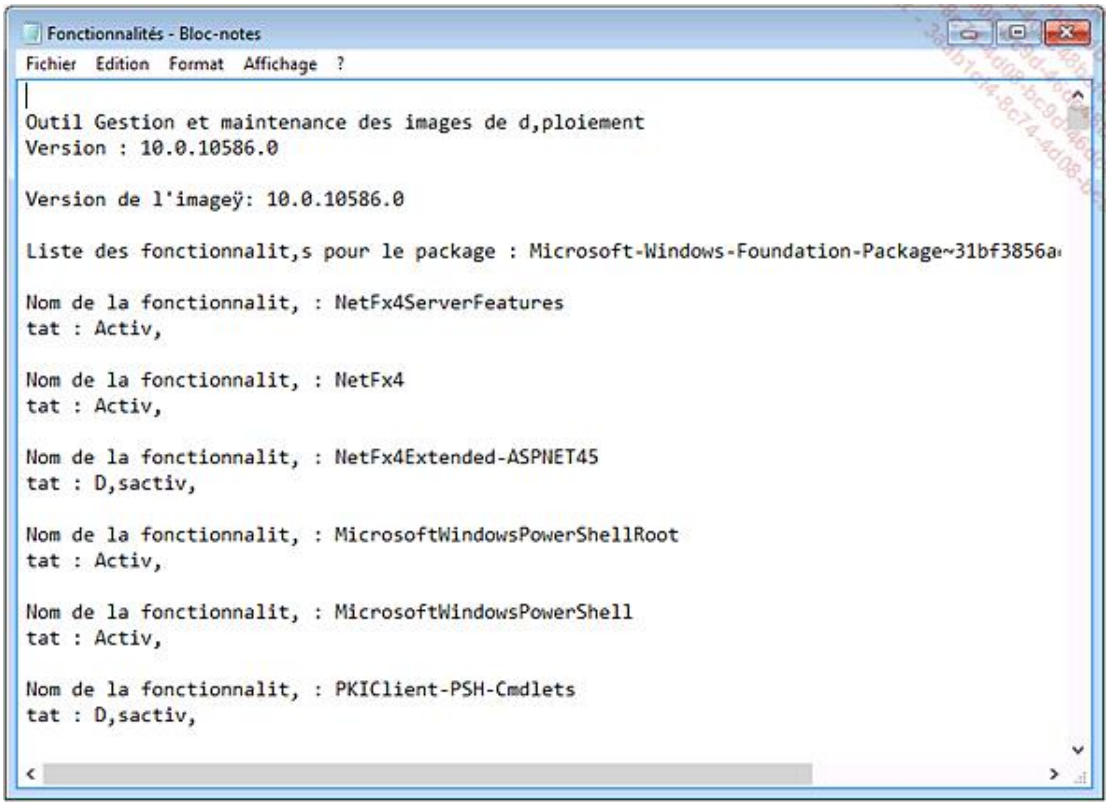
1. Afficher la liste des rôles et fonctionnalités

- Saisissez dans l'invite de commandes `dism /online /get-features > Fonctionnalités.txt` puis appuyez sur la touche [Entrée].

Les fonctionnalités disponibles dans le système d'exploitation en cours d'exécution (commutateur `/online`) sont répertoriées (`/get-features`). Le résultat est écrit dans le fichier Fonctionnalités.txt.



- Saisissez `Notepad Fonctionnalités.txt` afin d'ouvrir le fichier contenant le résultat.



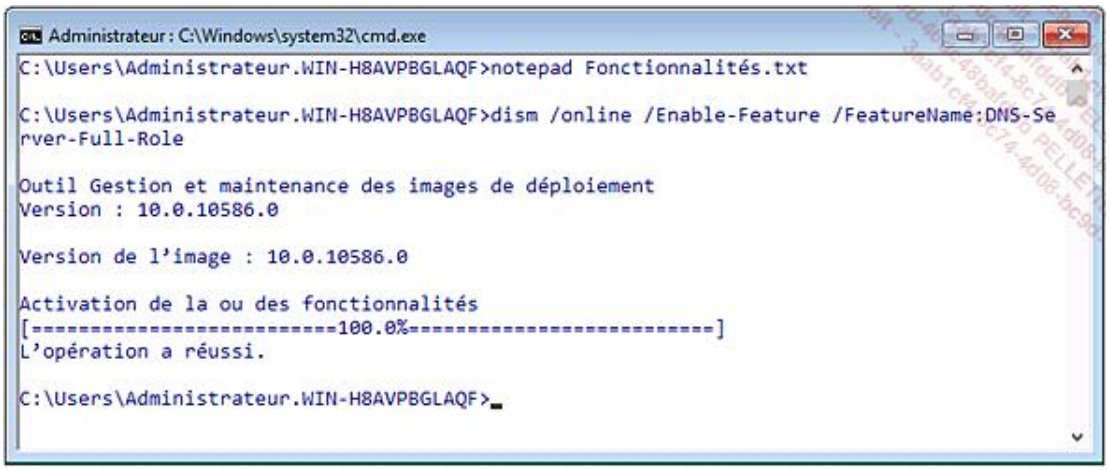
Le fichier donne le nom de la fonctionnalité et son état.

2. Ajouter un rôle ou une fonctionnalité

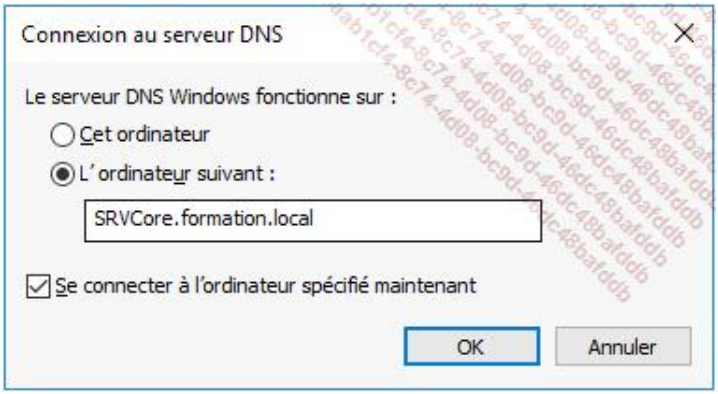
L'ajout d'une fonctionnalité s'effectue également avec la commande `dism`. La première étape est de récupérer le nom de la fonctionnalité qu'il est nécessaire d'installer.

Le nom du rôle pour serveur DNS est : **DNS-Server-Full-Role**.

- Dans l'invite de commandes, saisissez `dism /online /Enable-Feature /FeatureName:DNS-Server-Full-Role` puis appuyez sur la touche [Entrée].

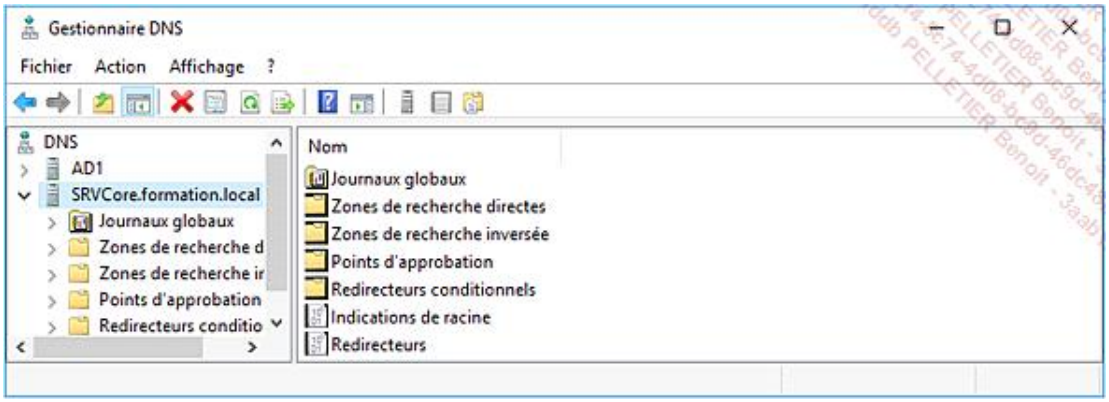


- Lancez la console DNS sur **AD1**.
- Effectuez un clic droit sur **DNS** puis sélectionnez **Établir une connexion au serveur DNS...** dans le menu contextuel.
- Sélectionnez le bouton radio **L'ordinateur suivant :** puis dans le champ saisissez **SRVCore.formation.local**.



- Cliquez sur **OK**.

Le serveur s'affiche dans la console, il est maintenant possible de le gérer depuis AD1.



La gestion du serveur DNS installé sur SRVCore peut être réalisée à distance.

3. Supprimer un rôle ou une fonctionnalité

Comme pour l'ajout, la suppression s'effectue à l'aide de la commande `dism`.

- Sur SRVCore, saisissez la commande `dism /online /Disable-Feature /FeatureName:DNS-Server-Full-Role` puis appuyez sur la touche [Entrée].



Le rôle est maintenant supprimé du serveur.

- Saisissez **Y** puis appuyez sur la touche [Entrée] pour redémarrer le serveur.

Ajouter/supprimer l’interface graphique

Depuis Windows Server 2008, il est possible d’installer des serveurs ne possédant pas d’interface graphique. Néanmoins, une fois le serveur installé, le retour en arrière était impossible. Il était possible avec Windows Server 2012 R2 d’ajouter/supprimer l’interface graphique à volonté. Cette fonctionnalité n’est malheureusement plus présente dans Windows Server 2016.

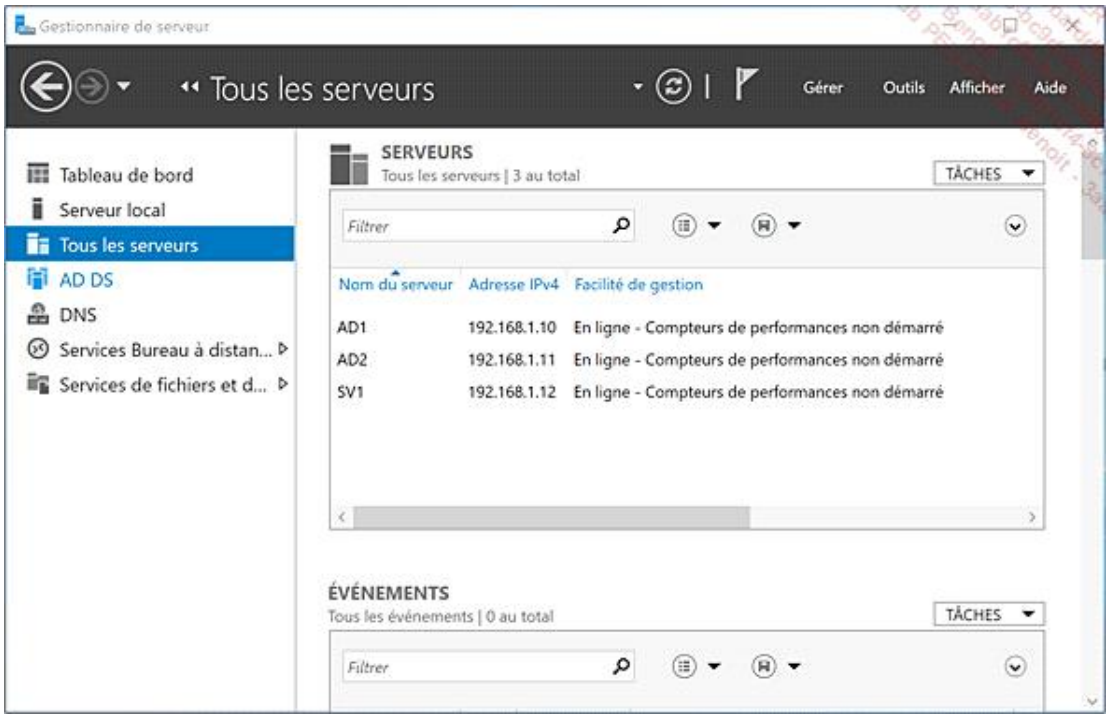
Suppression du groupe de serveurs

- Sur SV1, lancez la console **Gestionnaire de serveur**.
- Effectuez un clic droit sur **Groupe Formation.local** puis, dans le menu contextuel, sélectionnez **Supprimer un groupe de serveurs**.



- Cliquez sur **OK** dans la fenêtre d'avertissement.

Malgré la suppression du groupe, les postes restent présents dans **Tous les serveurs**.



Il est nécessaire de les supprimer à la main en effectuant un clic droit sur la ligne du serveur souhaitée.

Présentation de Nano Server

Contrairement aux versions précédentes, Windows Server 2016 permet l'installation de trois versions différentes.

- Desktop Experience : la version graphique.
- Server Core : la version ligne de commande.
- Nano Server : sans interface graphique.

Chaque installation possède ses avantages et inconvénients. Néanmoins, il est important de noter qu'il n'est plus possible de passer d'une version Core à une version graphique. Cette fonctionnalité, utilisée avec la version précédente et qui consistait à ajouter/supprimer l'interface graphique à souhait, a été supprimée.

Nano Server est une fonctionnalité apparue avec Windows Server 2016. Assez similaire au mode Core, il ne permet pas pour sa part de connexion locale. Il faut noter également une modification au niveau du support applicatif. En effet, Nano Server ne supporte que des applications, agents, etc. 64 bits. La gestion des mises à jour s'en trouve également facilitée. En effet, le nombre de correctifs nécessaires est largement réduit. À l'heure ou sont écrites ces lignes, Nano Server est supporté uniquement dans le modèle CBB (*Current Branch for Business*). Il n'existe pas de version LTSB.

Il n'est pas possible de télécharger le DVD de Nano Server, la création de l'image doit être effectuée en ligne de commande ou par l'intermédiaire d'un outil graphique (Nano Server Image Builder).

Le lien suivant vers le blog de l'auteur présente les différentes étapes pour la création de l'image par l'intermédiaire de Nano Server Image Builder : https://www.nibonnet.fr/nano-server-image-builder/.

Notez qu'il n'est pas possible d'implémenter cette fonctionnalité pour tous les rôles. Seuls les scénarios suivants sont compatibles :

- Serveur Hyper-V
- Serveur DNS
- Serveur web…

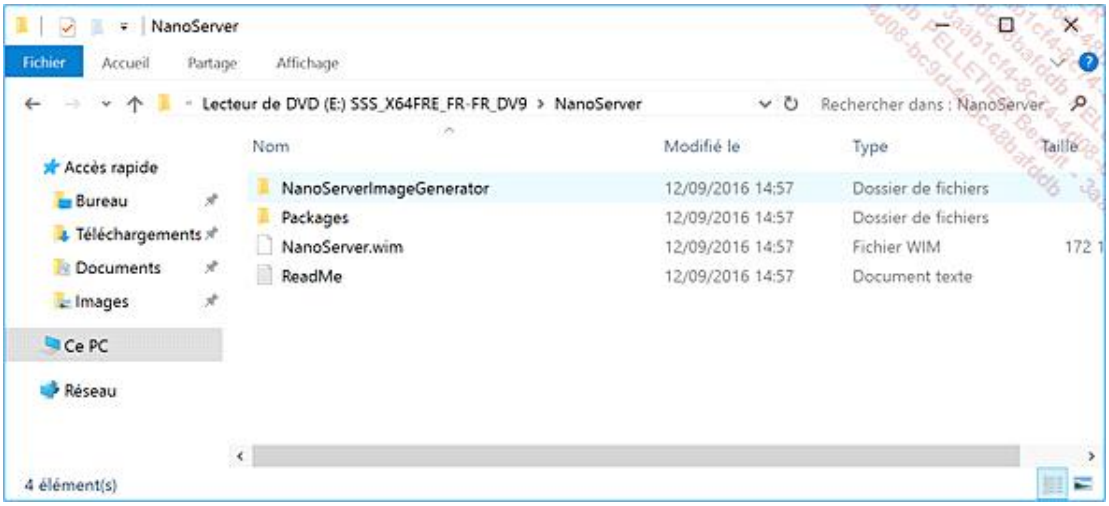
1. Création de l'image Nano Server

Nous l'avons vu dans le point précédent, l'utilisation de Nano Server nécessite la création d'une image. L'ensemble des fichiers nécessaires à la création sont présents dans le dossier NanoServer du DVD Windows Server 2016.

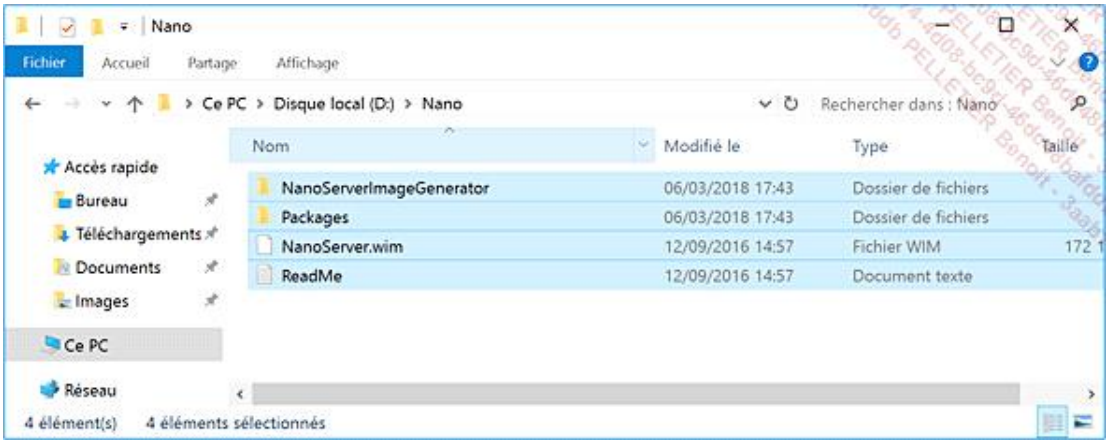
Par la suite, la création peut avoir trois utilisations :

- Utilisation d'une image VHD avec un serveur Hyper-V.
- Utilisation d'une image VHD avec un poste physique (boot sur VHD).
- Déploiement par l'intermédiaire d'une image WIM.

L'installation est composée de plusieurs étapes. Dans un premier temps, il est nécessaire de récupérer les fichiers sources présents sur le DVD.

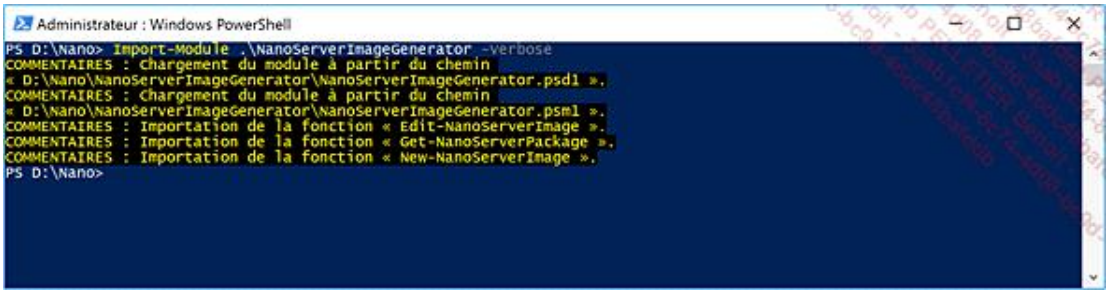


L'ensemble des fichiers présents dans le dossier NanoServer doivent être copiés dans une partition locale (poste de travail Windows 10, serveur…).



Après avoir lancé la console PowerShell, il est nécessaire d'accéder au répertoire précédemment copié. La commande permettant l'importation du module NanoServer peut maintenant être exécutée.

```
Import-Module .\NanoServerImageGenerator -Verbose
```



La création du fichier VHD peut maintenant être effectuée. La commande suivante peut être exécutée. Dans un premier temps, l'ISO de Windows Server 2016 peut être monté dans l'explorateur.

```
New-NanoServerImage -Edition <edition> -DeploymentType <deployment type>
-MediaPath <media path> -BasePath <base path> -TargetPath <target path>
-ComputerName <computer name> -Package <packages> -<other package switches>
```

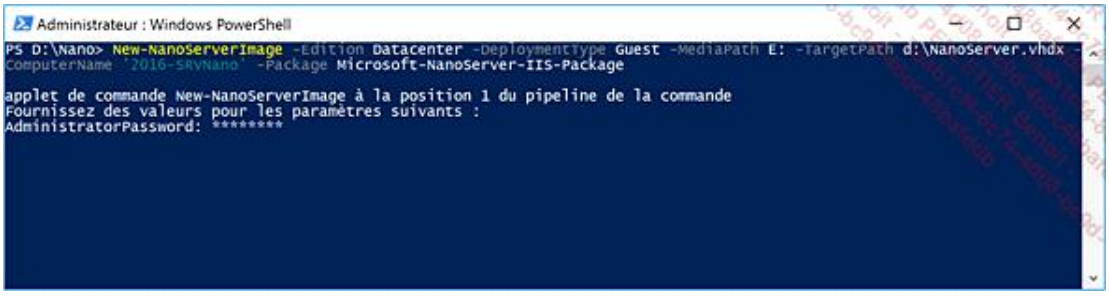
Définition des différents arguments :

- -Edition : édition de l'image Nano Server (Standard ou Datacenter).
- -DeploymentType : définit le type de déploiement souhaité (WIM, image VHD pour du boot sur VHD ou image VHD pour un hôte Hyper-V).
- -MediaPath : chemin de l'image ISO de Windows Server 2016.
- -BasePath : commutateur optionnel, il est utilisé lors de la création d'un fichier WIM. Les sources nécessaires à la création d'une image WIM sont copiées dans ce répertoire. La cmdlet New-NanoServerWim peut être utilisée sans spécifier le commutateur -MediaPath.
- -TargetPath : ce commutateur permet d'indiquer le chemin du répertoire de destination ainsi que le nom de l'image. Cette dernière est de plus composée de son extension.
- -ComputerName : nom de l'ordinateur Nano Server.
- -Package : utilisé pour l'installation de rôles ou fonctionnalités. Il est évidemment possible de combiner plusieurs packages (séparés par une virgule).
- -Other : utilisé par certains packages (pilotes, etc.). Il est nécessaire d'utiliser -OEMDrivers pour une utilisation sur un serveur physique. Le commutateur sera complété par le chemin où sont présents les pilotes.

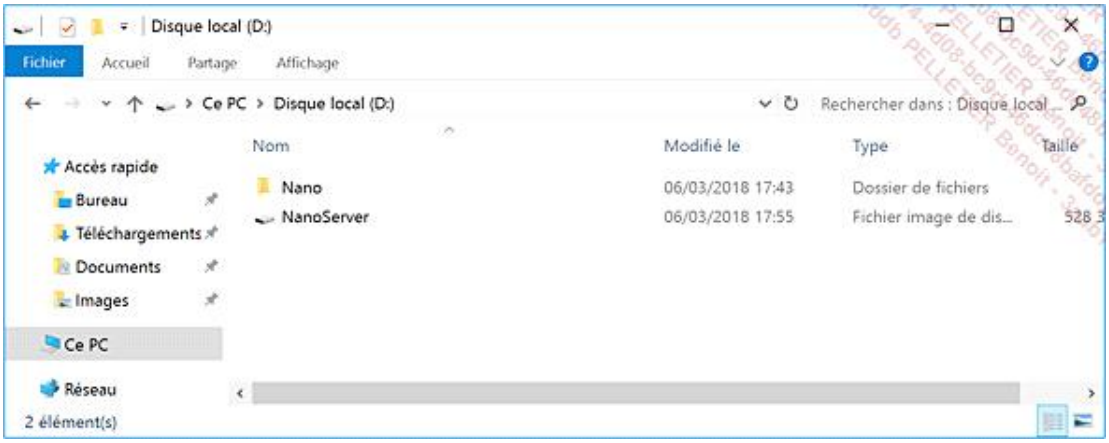
Exécutez la commande ci-dessous afin d'effectuer la création du fichier VHD.

```
New-NanoServerImage -Edition Datacenter -DeploymentType Guest -MediaPath
E: -TargetPath d:\NanoServer.vhdx -ComputerName '2016-SRVNano' -Package
Microsoft-NanoServer-IIS-Package
```

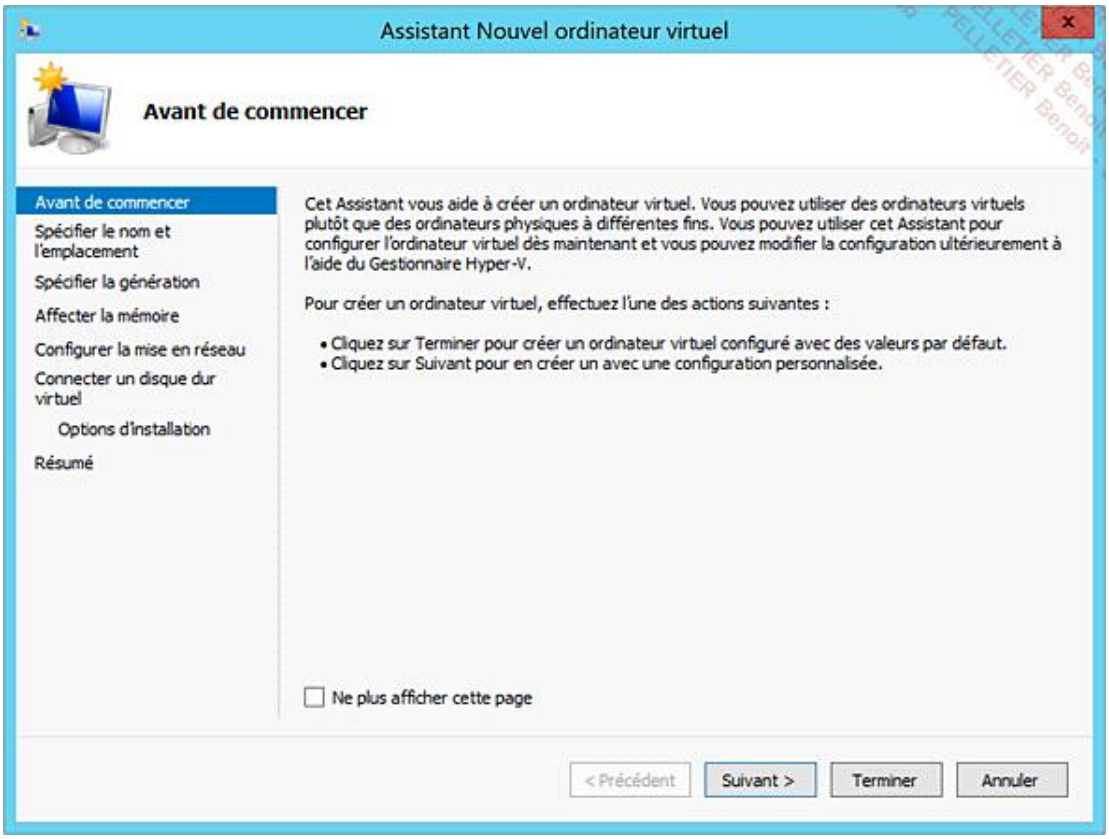
Saisissez le mot de passe de l'administrateur local puis validez la saisie à l'aide de la touche [Entrée]. La création du fichier est en cours.



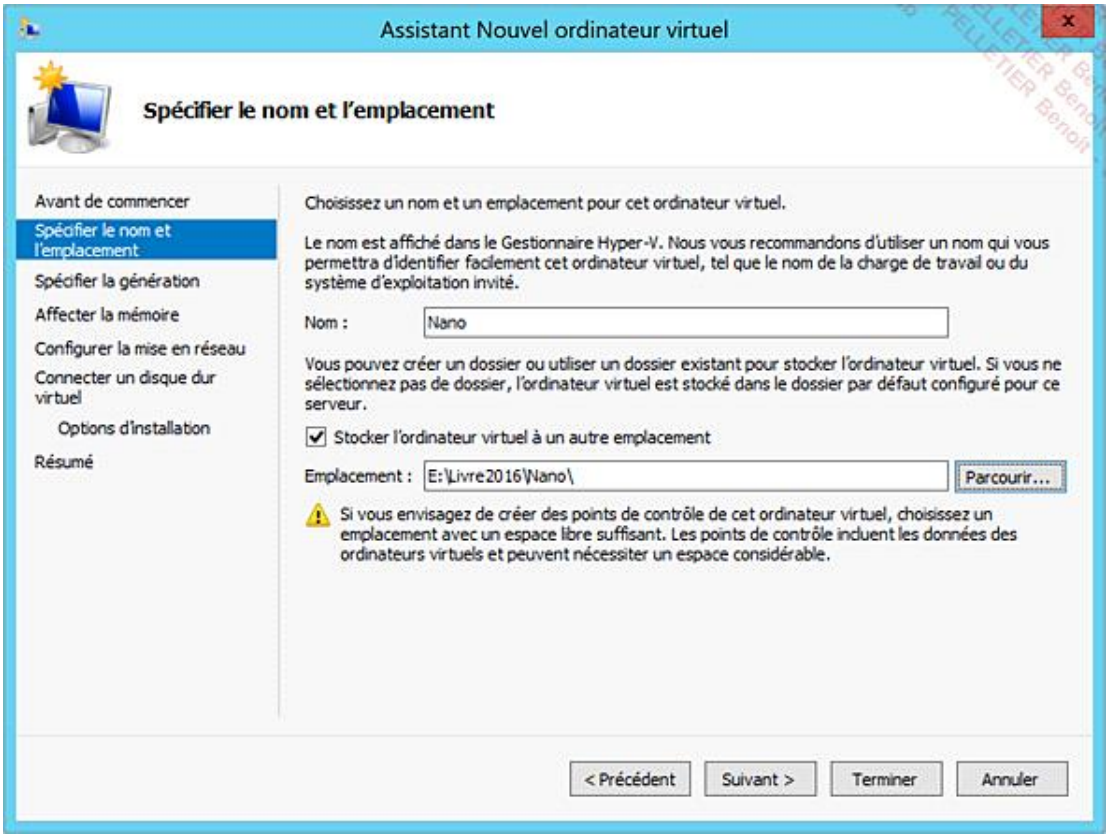
L'image est maintenant créée et présente. La machine virtuelle doit maintenant être créée dans Hyper-V.



Depuis la console Gestionnaire Hyper-V, cliquez sur **Nouveau** puis **Ordinateur virtuel**.

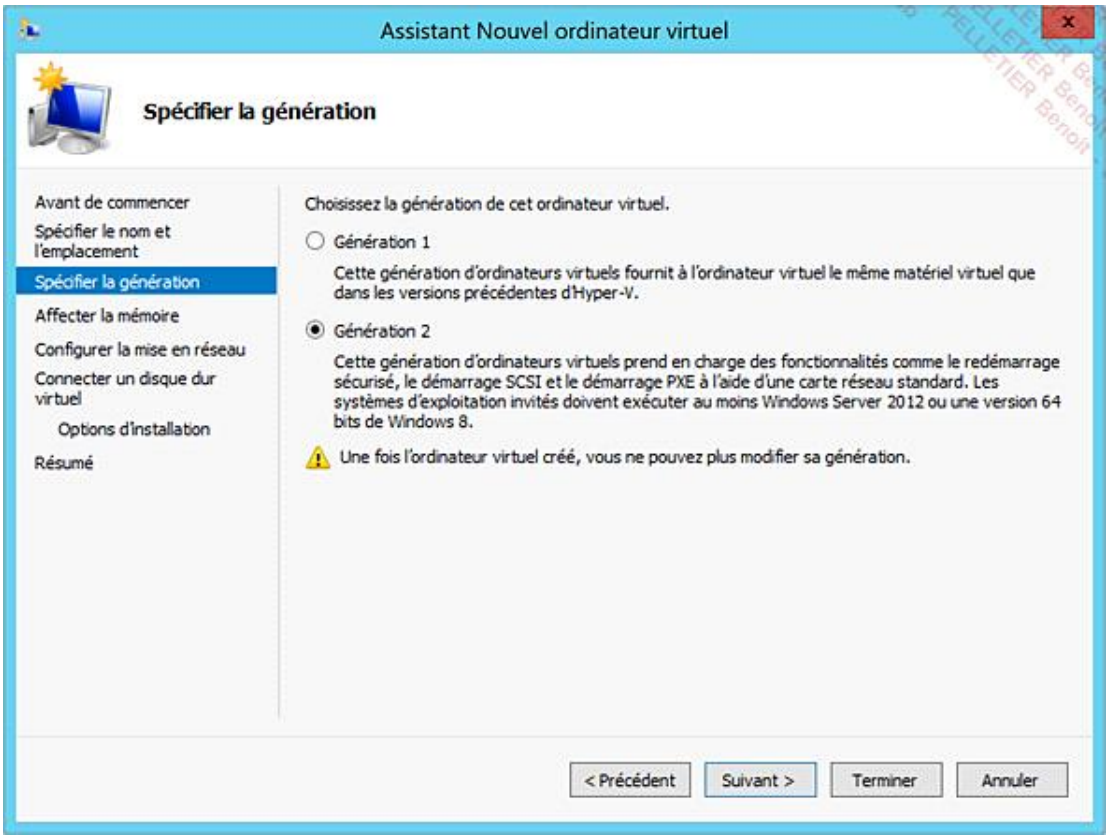


Dans l'assistant, saisissez le nom souhaité puis sélectionnez le répertoire de destination.

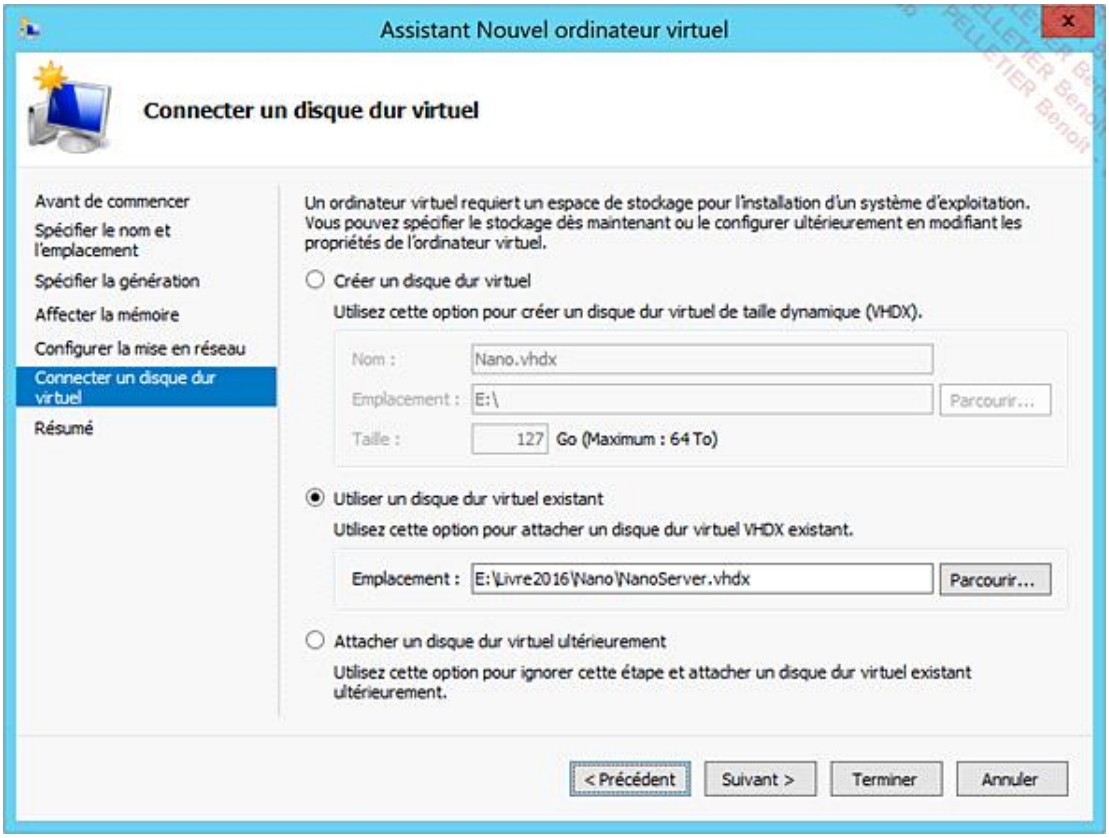


Le choix de la génération est important. Si le fichier précédemment créé est de type VHD, il est nécessaire de créer

une VM de génération 1. Dans le cas d'un fichier de type VHDX, une VM de génération 2 peut être utilisée.



Après avoir alloué une quantité de mémoire RAM et sélectionné le commutateur réseau souhaité, il est nécessaire de sélectionner le disque dur virtuel précédemment créé.



La machine virtuelle peut maintenant être démarrée. Pour être utilisée, une configuration (adresse IP, etc.) doit être effectuée.

2. Configuration de Nano Server

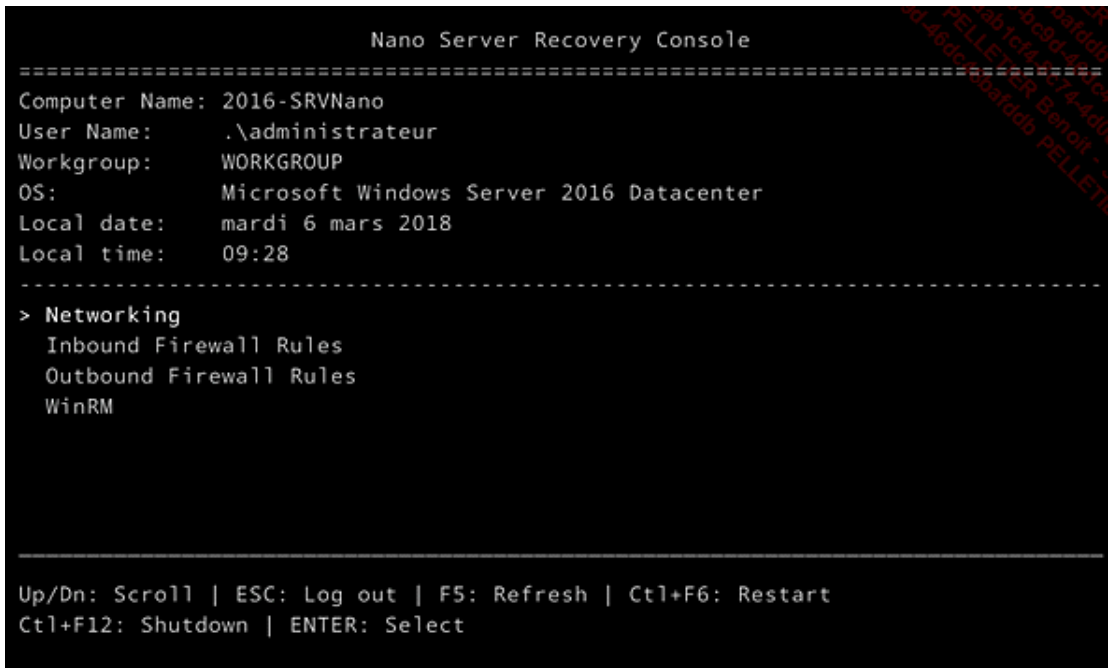
Nano Server ne possède pas d'interface graphique. Il est donc nécessaire de procéder à la configuration du serveur (nom, configuration IP) par l'intermédiaire de l'interface simplifiée qui s'affiche après l'ouverture de session. Les actions possibles sont limitées aux premières configurations effectuées sur un serveur :

- Configuration réseau.
- Configuration du pare-feu.
- WinRM.

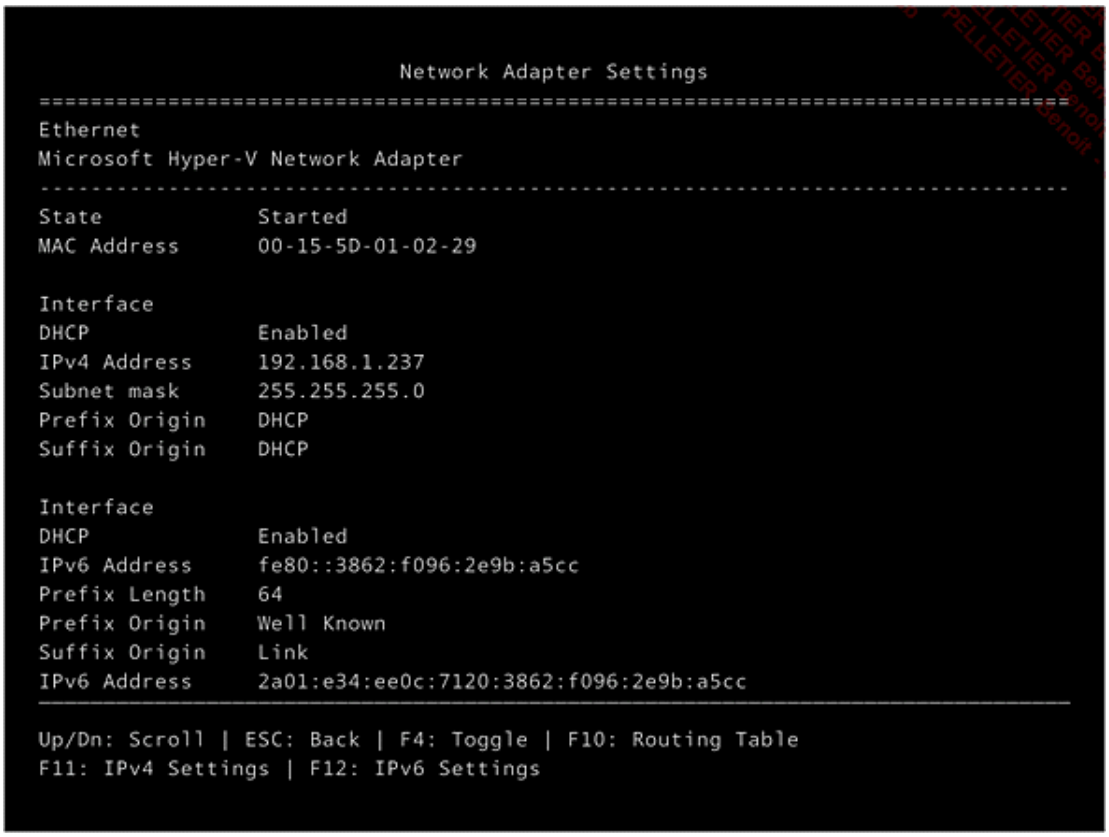
Avant de pouvoir procéder à la configuration du serveur, il est nécessaire de s'authentifier.



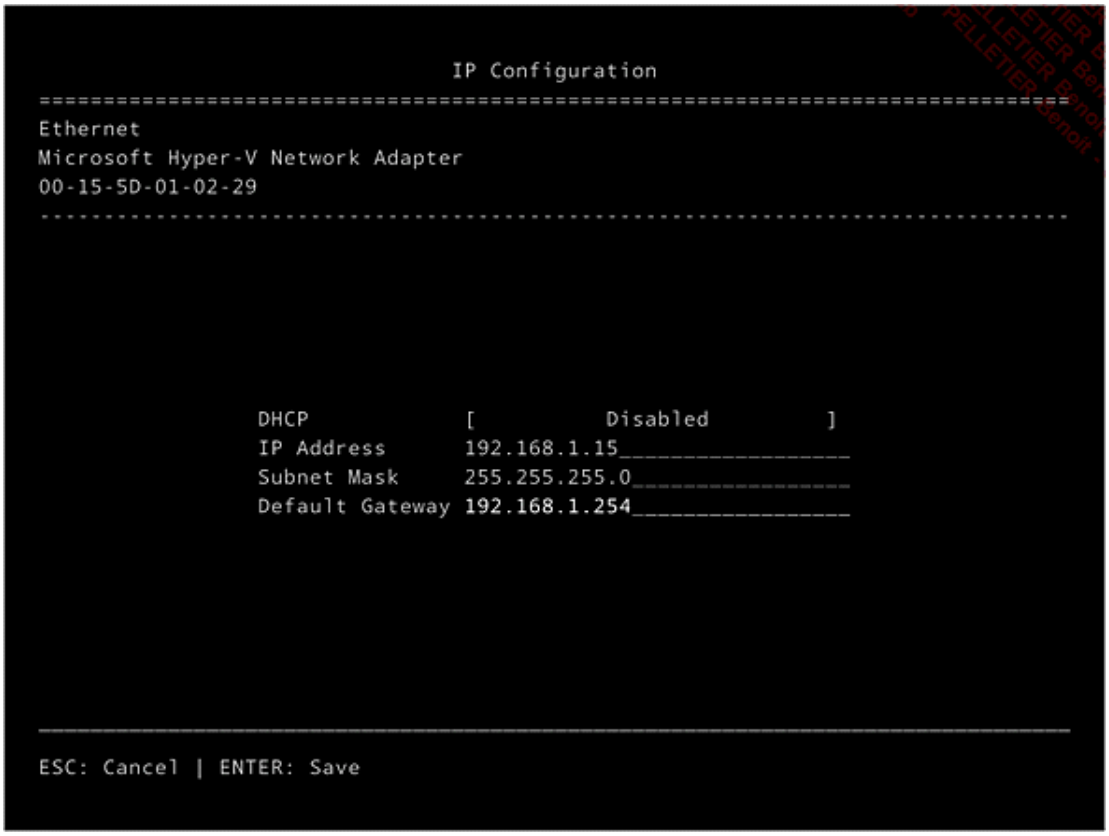
Sélectionnez **Networking** à l'aide des touches du clavier puis appuyez sur la touche [Entrée].



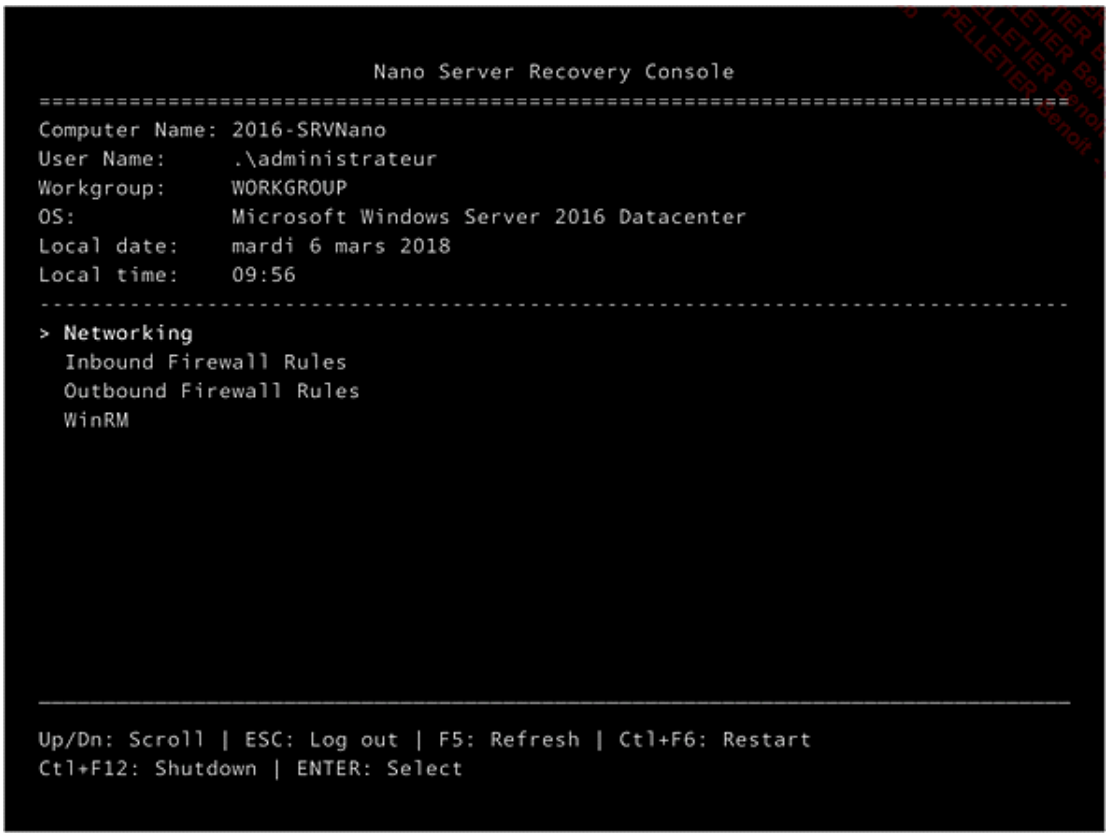
- Appuyez sur [Entrée] pour sélectionnez la carte Ethernet. La fenêtre qui s'affiche présente la configuration de la carte.
- Appuyez sur la touche [F11] pour modifier la configuration IPv4.



- Appuyez sur la touche [F4] pour désactiver le mode DHCP. À l'aide de la touche [Tab], configurez les différents champs comme ci-dessous.

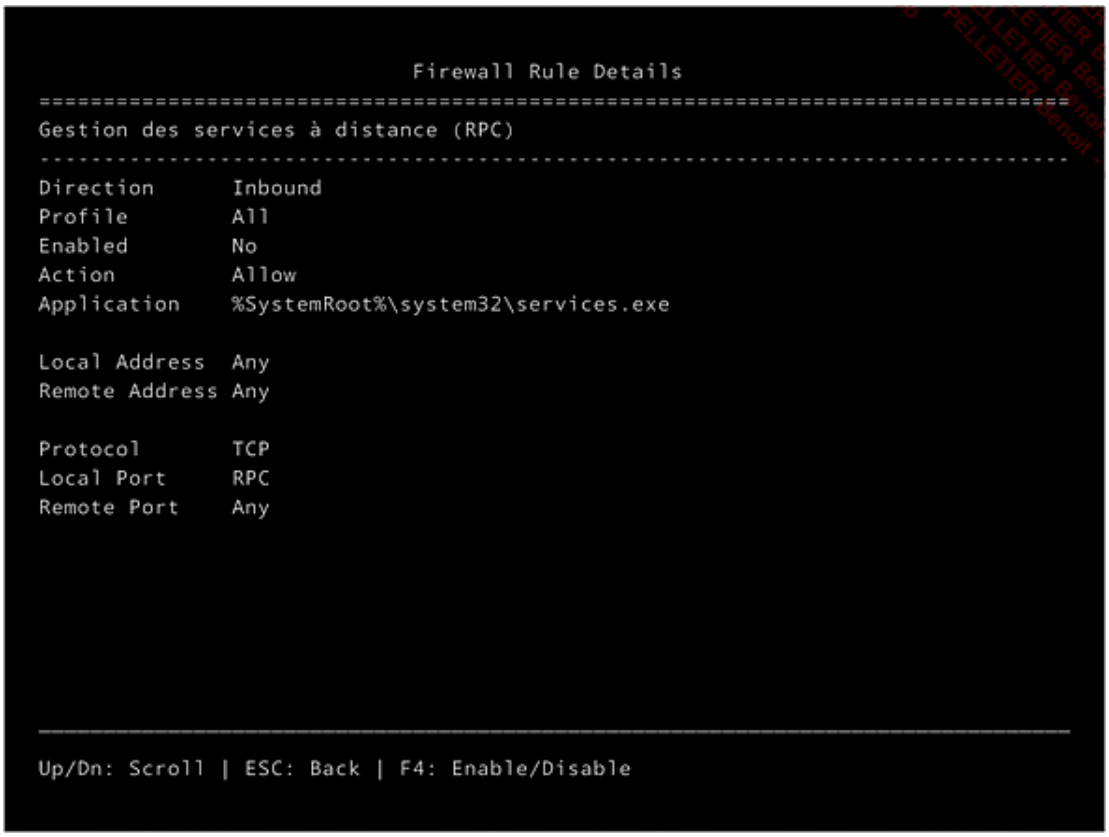


- Appuyez sur la touche [Entrée] pour valider la modification. Appuyez sur la touche [Echap] afin de revenir à la fenêtre **Nano Server Recovery Console**.



Le pare-feu doit maintenant être configuré. Par l'intermédiaire des flèches sur le clavier, accédez à **Inbound Firewall Rules** puis appuyez sur la touche [Entrée].

Accédez à la règle **Gestion des services à distances (RPC)** puis appuyez sur [Entrée].

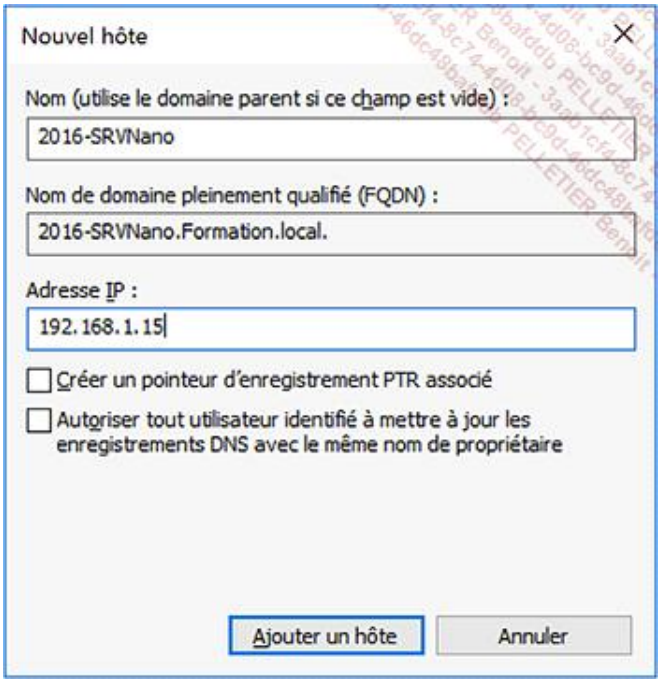


Appuyez sur [F4] pour activer la règle.

Effectuez la même opération pour les règles suivantes :

- Partage de fichiers et d'imprimantes (SMB-Entrée)
- Gestion à distance des journaux des événements (RPC)

La jonction au domaine nécessite d'effectuer la configuration du client DNS sur le serveur Nano. Afin de permettre la résolution de noms, il est nécessaire de créer un enregistrement dans le DNS.

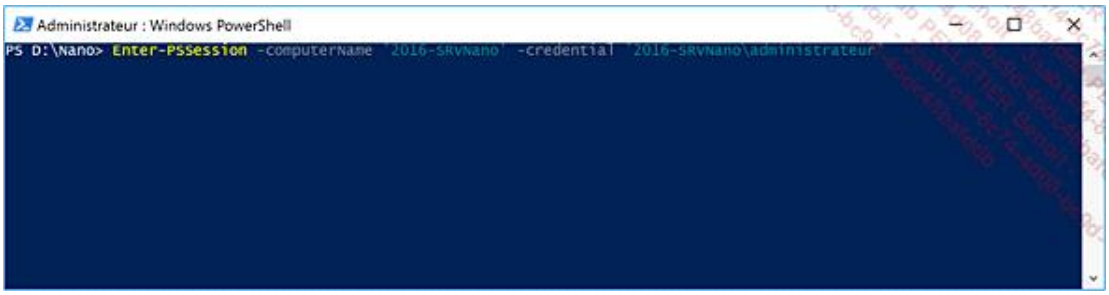


- Depuis le serveur AD1, lancez une invite de commandes PowerShell. Saisissez la commande `set-item WSMan:\localhost\Client\TrustedHosts "2016-SRVNano"`.
- Saisissez **O** pour valider l'opération puis appuyez sur la touche [Entrée].



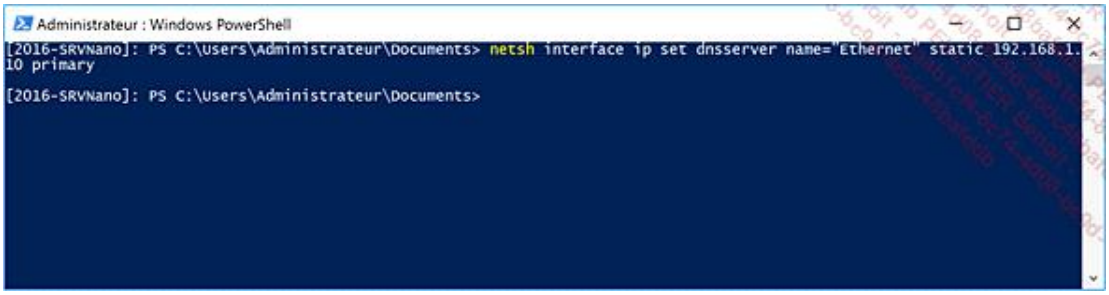
- Saisissez la commande `Enter-PSSession -computerName '2016-SRVNano' -credential '2016-SRVNano\administrateur'`.

Cette commande permet de se connecter à distance au serveur.



- Saisissez le mot de passe de l'administrateur puis cliquer sur **OK**. Par la suite, saisissez la commande ci-dessous afin de configurer le client DNS du serveur.

```
netsh interface ip set dnsserver name="Ethernet" static 192.168.1.10
primary
```

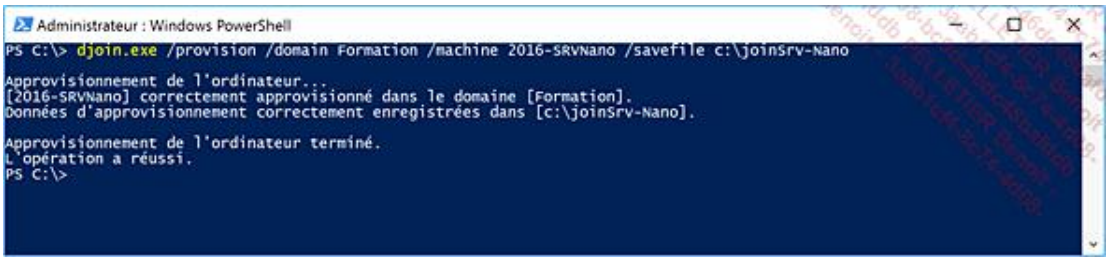


La jonction au domaine peut être effectuée à l'aide de la commande `djoin`. Cette dernière permet de réaliser la jonction même si le contrôleur de domaine n'est pas accessible. Elle nécessite d'exécuter une commande sur le contrôleur de domaine et une autre sur le serveur/poste qui doit joindre le domaine.

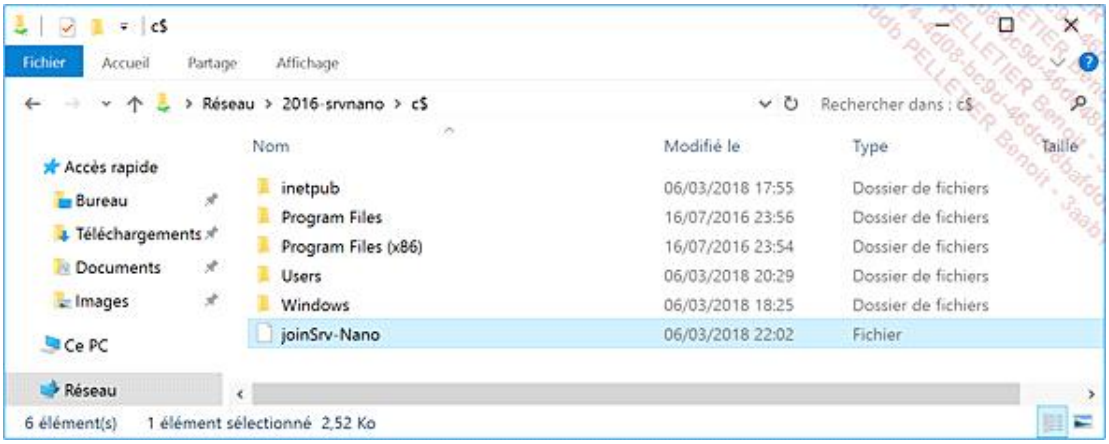
- Ouvrez une deuxième invite de commandes PowerShell sans fermer celle qui a permis de se connecter au serveur.

Commande djoin sur le contrôleur de domaine

```
djoin.exe /provision /domain Formation /machine 2016-SRVNano /savefile
c:\joinSrv-Nano
```



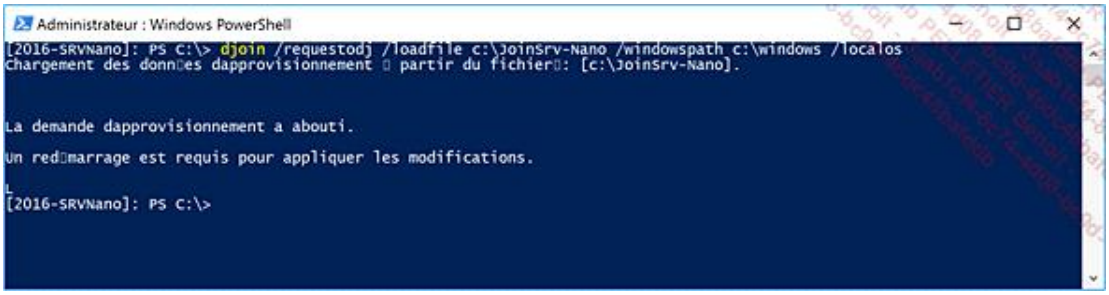
Copiez le fichier à la racine de la partition C: du serveur. Lors de l'exécution de la commande pour joindre le domaine, ce fichier sera chargé.



Commande djoin sur le serveur Nano Server

Depuis l'invite de commandes PowerShell qui a permis la connexion au serveur Nano (commande enter-pssession), exécutez la commande ci-dessous.

```
djoin /requestodj /loadfile c:\JoinSrv-Nano /windowspath
c:\windows /localos
```



Après le redémarrage, le serveur est membre du domaine. Il est possible de gérer en ligne de commande le serveur ou d'accéder à la console MMC pour visualiser les journaux d'événements, etc. Lors de l'installation, le package IIS a été installé. Depuis le contrôleur de domaine, accédez à l'URL http://2016-SRVNano. La page web par défaut s'affiche correctement.

Les conteneurs

1. Présentation

Les conteneurs sont une nouvelle fonctionnalité apportée par Windows Server 2016 TP3. Avec cette fonctionnalité, le système d'exploitation est virtualisé.

Lors de l'exécution d'une application présente dans un conteneur, cette dernière pense s'exécuter sur son propre système. Elle est réellement présente sur le même serveur que les autres applications.

Les conteneurs sont donc différents de la virtualisation de machine. Dans ce dernier cas, il n'est pas possible d'isoler une application. Si la machine virtuelle héberge trois applications, elles utilisent toutes le même système d'exploitation.

Avec les conteneurs, l'exécution d'une application s'effectue maintenant sans impacter le système d'exploitation, et inversement.

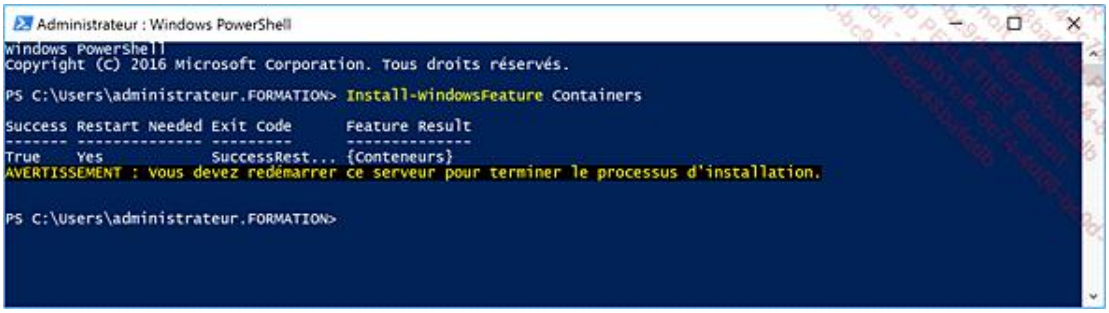
Les concepts clés ci-dessous sont important à prendre en compte :

- **Container Host** : serveur de type physique ou virtuel sur lequel la fonctionnalité **Windows Server Container** est installée. Il a pour fonction d'exécuter un ou plusieurs conteneurs Windows Server.
- **Container OS Image** : ce type d'image fournit un système d'exploitation. Il n'est pas possible de procéder à des modifications.
- **Container Image** : une image Container contient des modifications apportées et non présentes dans l'image OS (Container Image OS). Cela peut être l'installation d'un logiciel, la modification de clés de registre… Une image est créée en convertissant une Sandbox en Container Image.
- **Sandbox** : toutes les actions d'écriture telles que l'ajout d'une application, la modification d'une clé de registre, etc., sont présentes dans la Sandbox. Une fois le conteneur arrêté, il est possible de procéder à la suppression de ces modifications ou à la conversion d'une Sandbox en Container Image.
- **Container Repository** : les images Container sont stockées dans un référentiel local. L'hôte a la possibilité d'utiliser ces images une multitude de fois.
- **Container Management Technology** : la gestion des conteneurs peut s'effectuer par l'intermédiaire de PowerShell ou de Docker.

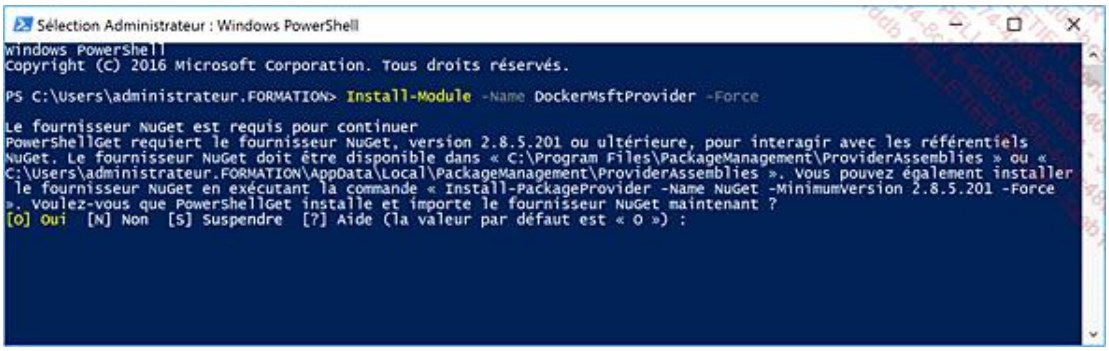
L'administration s'effectue par l'intermédiaire du client Docker ou tout simplement en PowerShell. Le déploiement des applications dans le cloud va s'en trouver facilité.

2. Mise en place

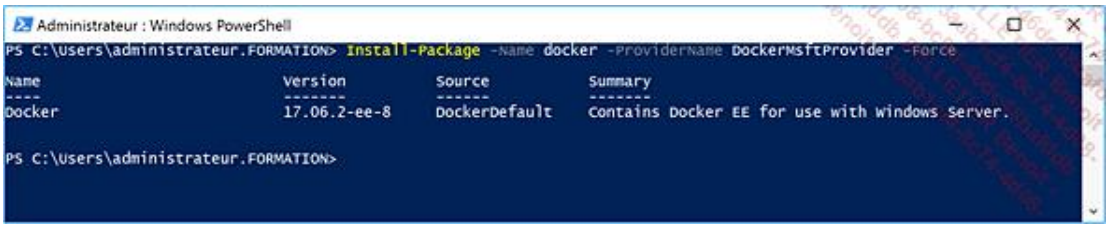
Sur le serveur **SV1**, lancez une console PowerShell puis exécutez la commande `Install-WindowsFeature Containers`. La fonctionnalité Conteneur est maintenant installée.



- Redémarrez le serveur à l'aide de la commande `shutdown -r -t 0`.
- Le module PowerShell nommé **DockerMsftProvider** peut maintenant être installé. Exécutez la commande `Install-Module -Name DockerMsftProvider -Force`. Saisissez **O** puis appuyez sur la touche [Entrée].

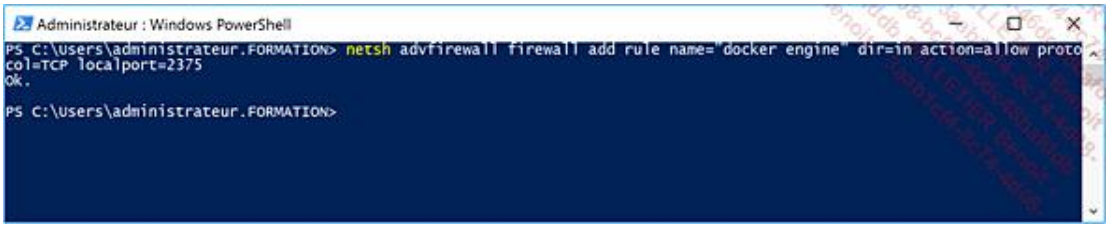


- Il est nécessaire de procéder à l'installation du package. Pour cela, exécutez la commande suivante : `Install-Package -Name docker -ProviderName DockerMsftProvider -Force`. Si ce n'est pas déjà fait, la KB3176939 doit être installée (effectuez la mise à jour du serveur par l'intermédiaire de Windows Update pour récupérer les dernières mises à jour).



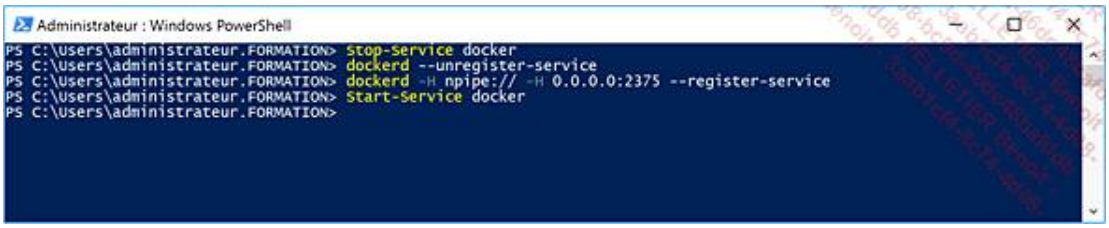
Une configuration du pare-feu est nécessaire. Utilisez la commande `Netsh` pour procédez à la configuration.

```
netsh advfirewall firewall add rule name="docker engine" dir=in
action=allow protocol=TCP localport=2375
```

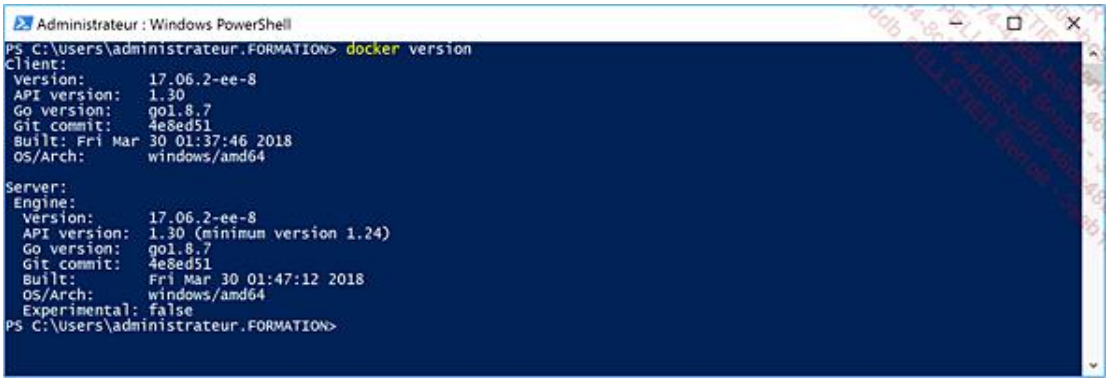


La configuration du service Docker (démon) peut maintenant être effectuée. Cette opération s'effectue à l'aide des commandes ci-dessous. Il est nécessaire de stopper le service puis de configurer le démon pour une écoute sur Pipe et TCP. Enfin, le service est par la suite redémarré.

```
Stop-Service docker
dockerd --unregister-service
dockerd -H npipe:// -H 0.0.0.0:2375 --register-service
Start-Service docker
```

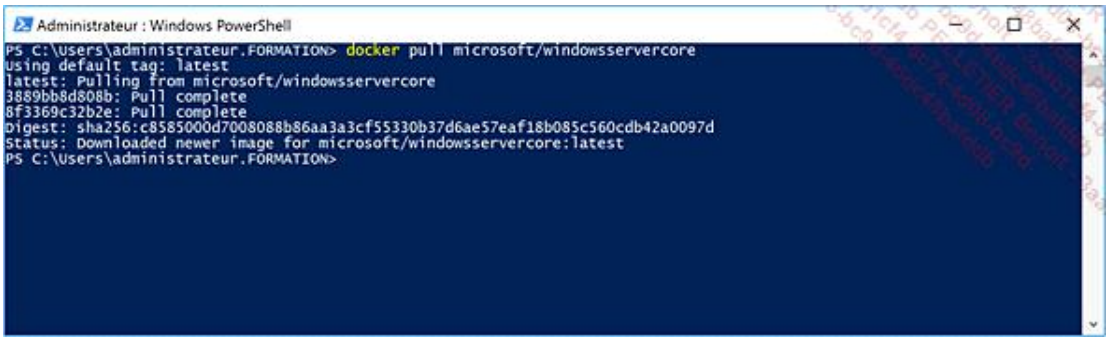


Docker est maintenant installé. Pour vérifier les propriétés du client et du serveur, il est nécessaire d'exécuter la commande `docker version`.

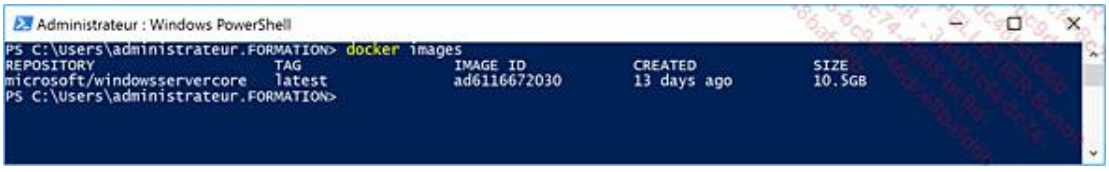


Les images de base peuvent désormais être récupérées à l'aide des commandes `docker pull microsoft/nanoserver` et `docker pull microsoft/windowsservercore`. En exécutant ces commandes, on s'assure de récupérer les dernières versions.

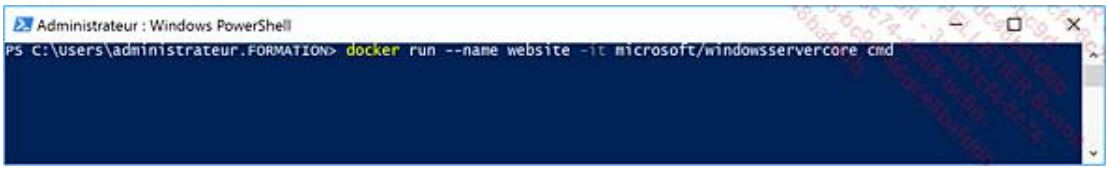
- Exécutez la commande `docker pull microsoft/windowsservercore`.



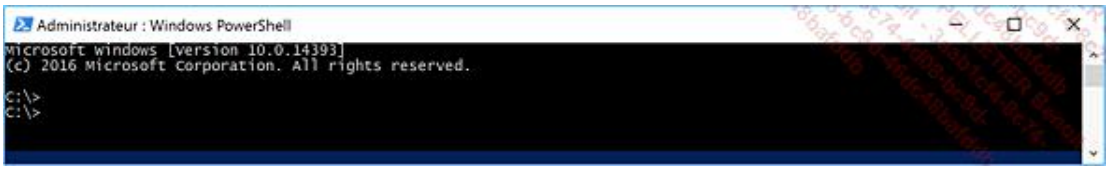
Les images peuvent être visualisées à l'aide de la commande `docker images`.



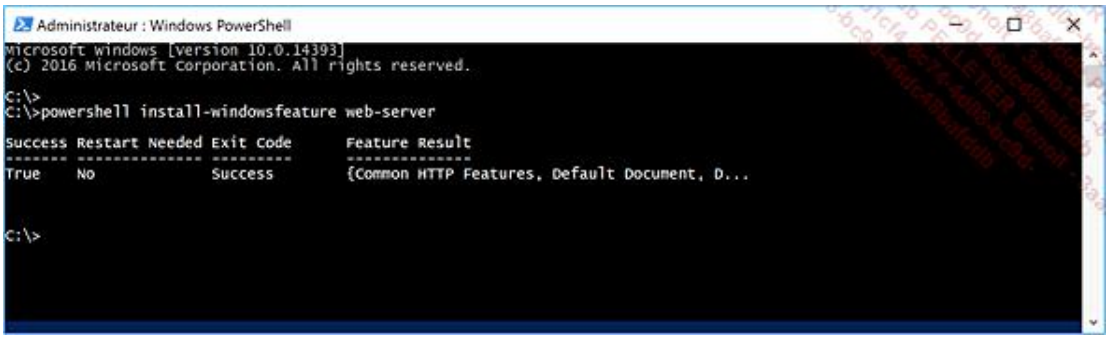
- Le conteneur peut maintenant être créé. Exécutez la commande :`docker run --name website -it microsoft/windowsservercore cmd`.



Une console DOS s'affiche.



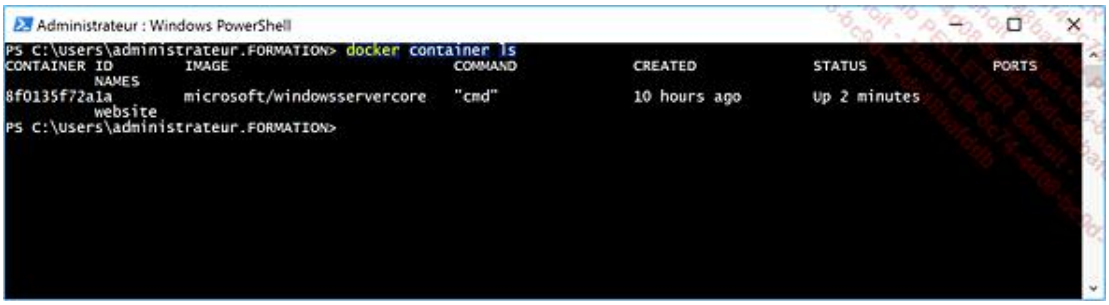
- L'installation d'un serveur web peut être effectuée. Exécutez la commande `powershell install-windowsfeature web-server`.



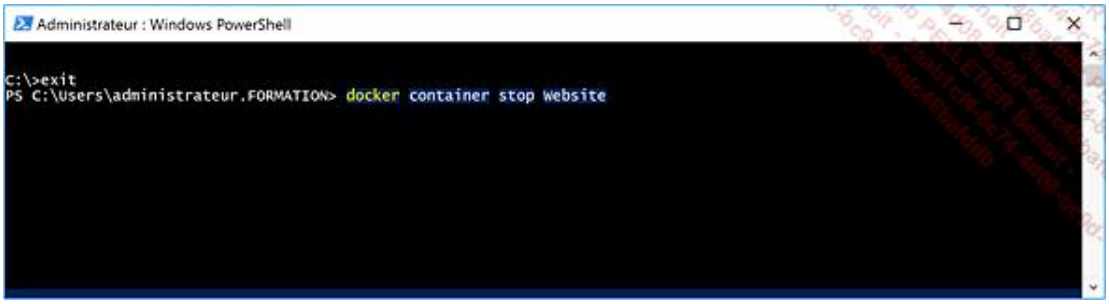
IIS est maintenant installé ; l'image peut être créée depuis ce conteneur. Ceci permettra de créer des conteneurs avec IIS préinstallé.

- Saisissez la commande `Exit` pour revenir à la console DOS.

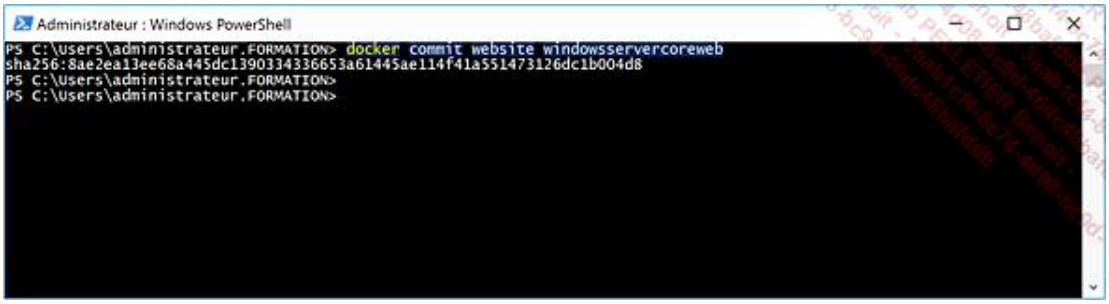
Vérifiez que le conteneur est toujours démarré en saisissant la commande `docker container ls`. Si aucun conteneur n'est présent, exécutez la commande `docker container start website`.



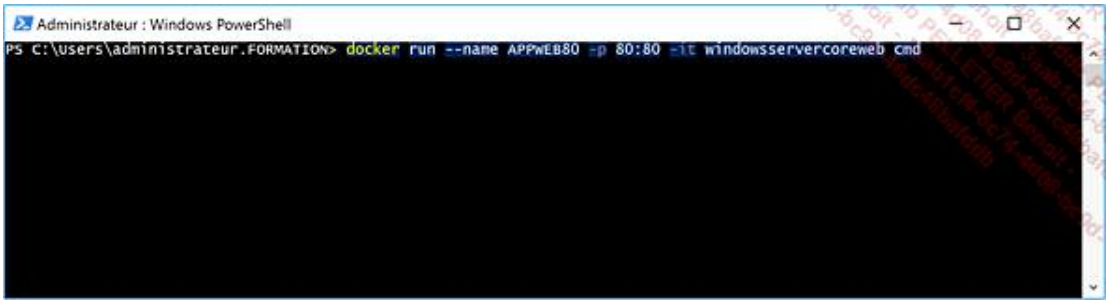
- Exécutez la commande `docker container stop website`, ceci permet de procéder à l'arrêt du conteneur.



- Exécutez `docker commit website windowsservercoreweb` pour effectuer la création de l'image.

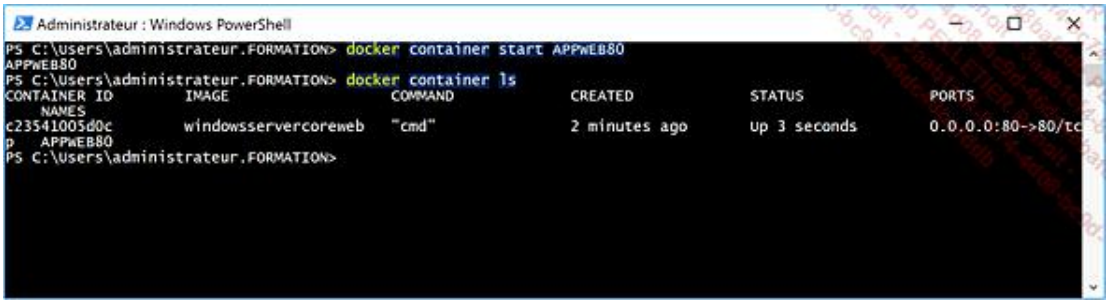


La création du conteneur utilisant la nouvelle image peut être effectuée. Pour cela, exécutez la commande `docker run --name APPWEB80 -p 80:80 -it windowsservercoreweb cmd`.

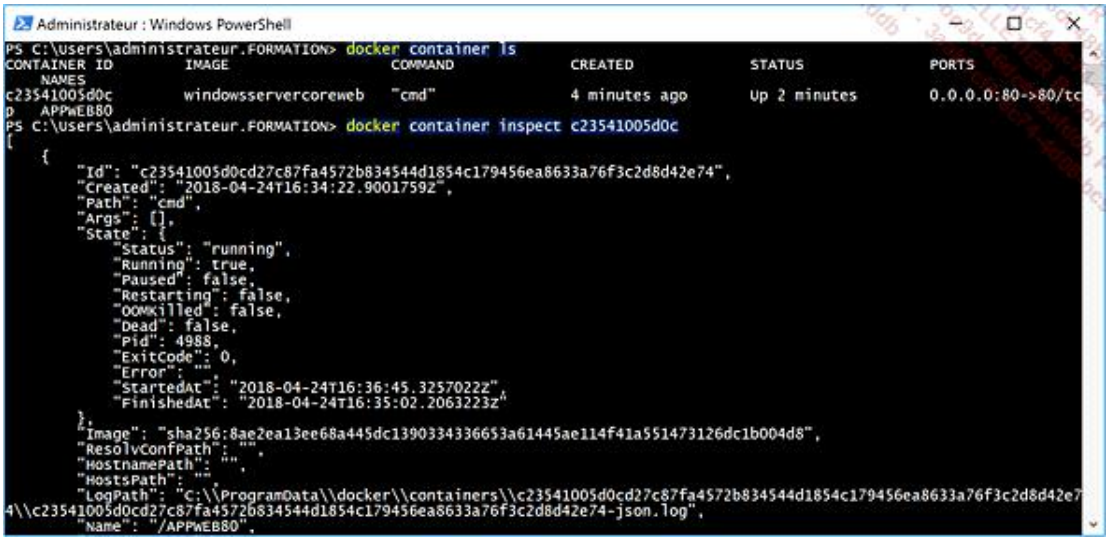


Le nouveau conteneur est maintenant en place et peut être utilisé.

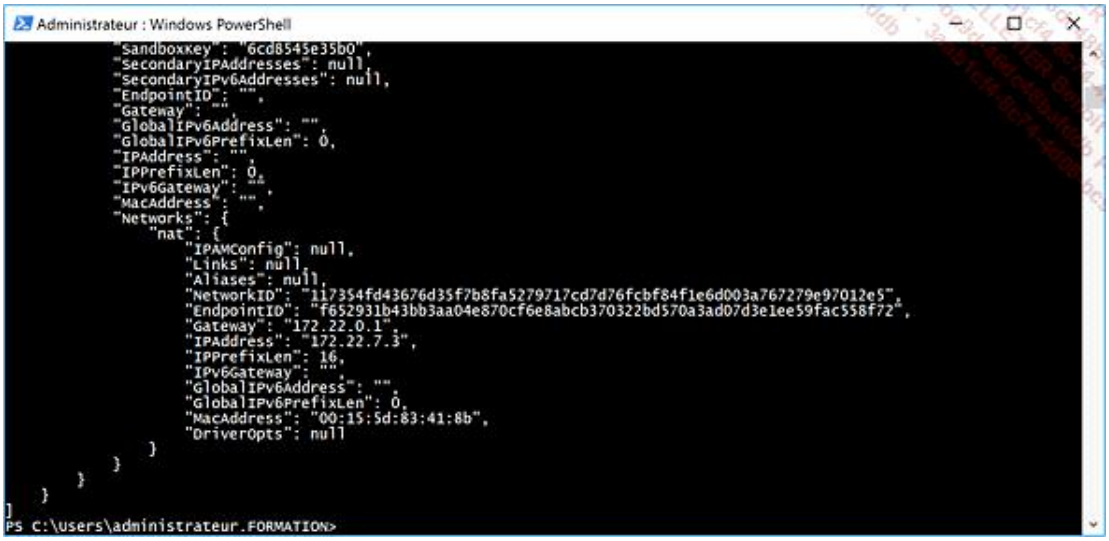
- Exécutez la commande `Exit` puis `docker container start APPWEB80`. Récupérez l'ID du conteneur à l'aide de la commande `docker container ls`.



- Une fois récupéré l'ID du conteneur utilisant l'image Windowsservercoreweb, exécutez la commande `docker container inspect IDContainer`.



La catégorie Networks contient l'adresse IP du conteneur.



Il est possible de créer d'autres conteneurs sur la même machine.

Le compte utilisateur

Active Directory contient différents types d'objets, dont le compte utilisateur. Généralement rattaché à une personne physique, ce type d'objet permet d'être authentifié par un contrôleur de domaine. L'utilisateur doit pour cela saisir un login et mot de passe afin de prouver son identité.

Ainsi, si la saisie de l'utilisateur est valide l'authentification est réussie, un jeton est attribué à la personne, qui contient notamment le SID (*Security IDentifier*) du compte utilisateur, unique dans le domaine AD, ainsi que l'ensemble des SID des groupes dont il est membre.

Les comptes utilisateur peuvent être locaux à un poste de travail ou un serveur (ils sont dans ce cas stockés dans une base SAM - *Security Account Manager*) ou de domaine (stockés dans Active Directory).

1. Création d'un utilisateur

Cet objet étant référencé dans le schéma, il est possible d'en créer à souhait (dans la limite du nombre d'objets maximum autorisé par l'annuaire Active Directory). Cette opération s'effectue à l'aide de la console **Utilisateurs et ordinateurs Active Directory**. La création peut être automatisée à l'aide de scripts PowerShell.

- Sur AD1, lancez la console **Utilisateurs et ordinateurs Active Directory**.
- Effectuez un clic droit sur le dossier système **Users** puis, dans le menu contextuel, sélectionnez **Nouveau** - **Utilisateur**.

Un assistant se lance. Il permet la création de l'objet utilisateur.

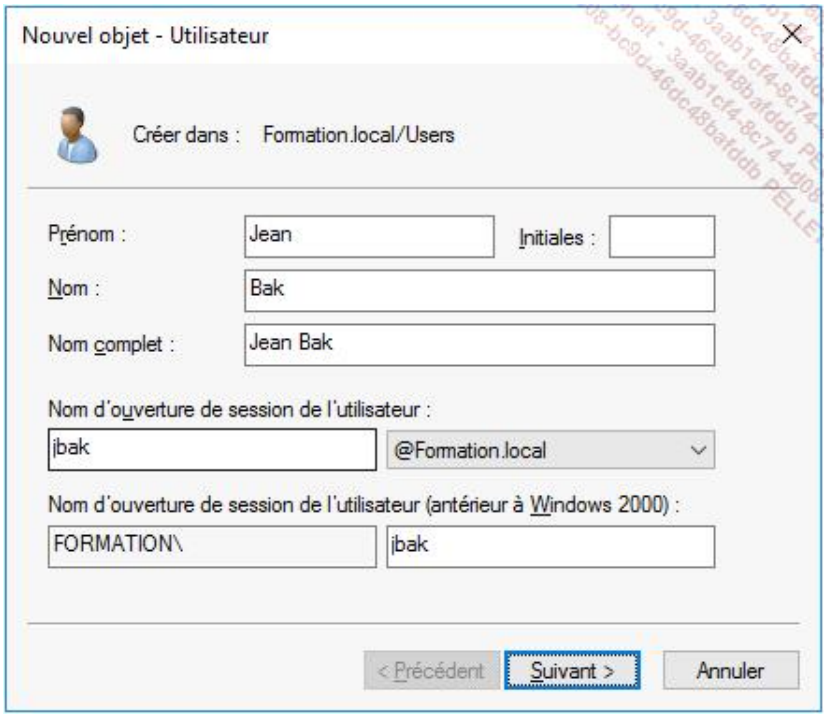
- Saisissez **Jean** dans le champ **Prénom**, puis **BAK** dans le champ **Nom**.

Le champ **Nom Complet** se remplit à partir des deux champs ainsi renseignés.

Les champs **Nom d'ouverture de session de l'utilisateur** et **Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000)** contiennent le nom d'ouverture de session utilisé pour ouvrir une session.

- Saisissez **jbak** dans le champ **Nom d'ouverture de session de l'utilisateur**.

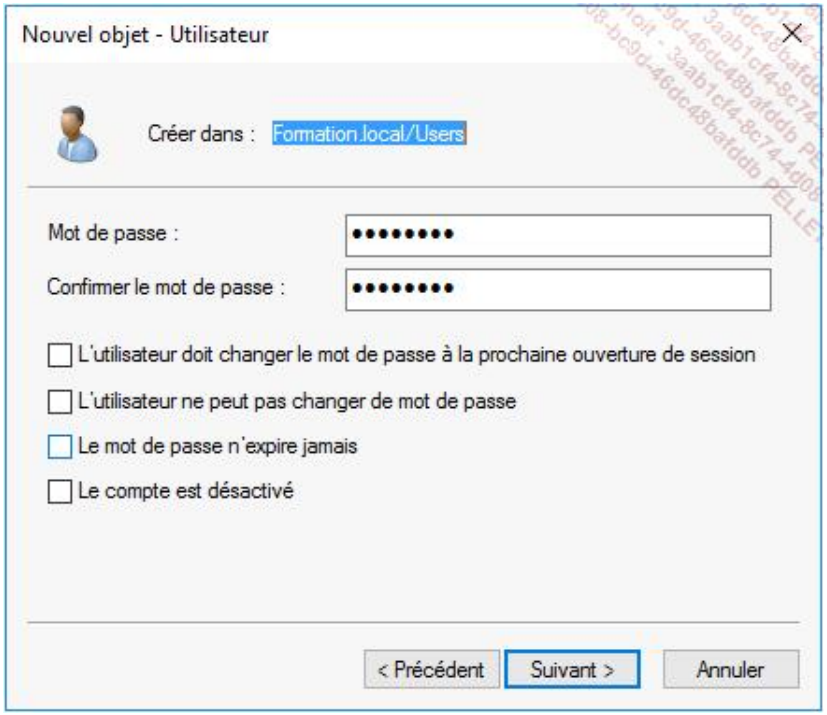
Le deuxième champ se remplit seul, ne le modifiez pas.



- Cliquez sur **Suivant**.
- Saisissez **Pa$$w0rd** dans le champ **Mot de passe** puis confirmez-le.

Ce mot de passe a l'avantage de respecter la politique de complexité du mot de passe qui est mise en vigueur pour les utilisateurs du domaine **Formation.local**.

- Décochez l'option **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session** puis cliquez sur **Suivant**.



- Cliquez sur **Terminer** pour lancer la création de l'objet.

2. Propriétés de l'objet utilisateur

Après l'étape de création de l'utilisateur, il convient de paramétrer ses propriétés.

Effectuez un clic droit sur l'utilisateur **Jean BAK** puis sélectionnez **Propriétés**.

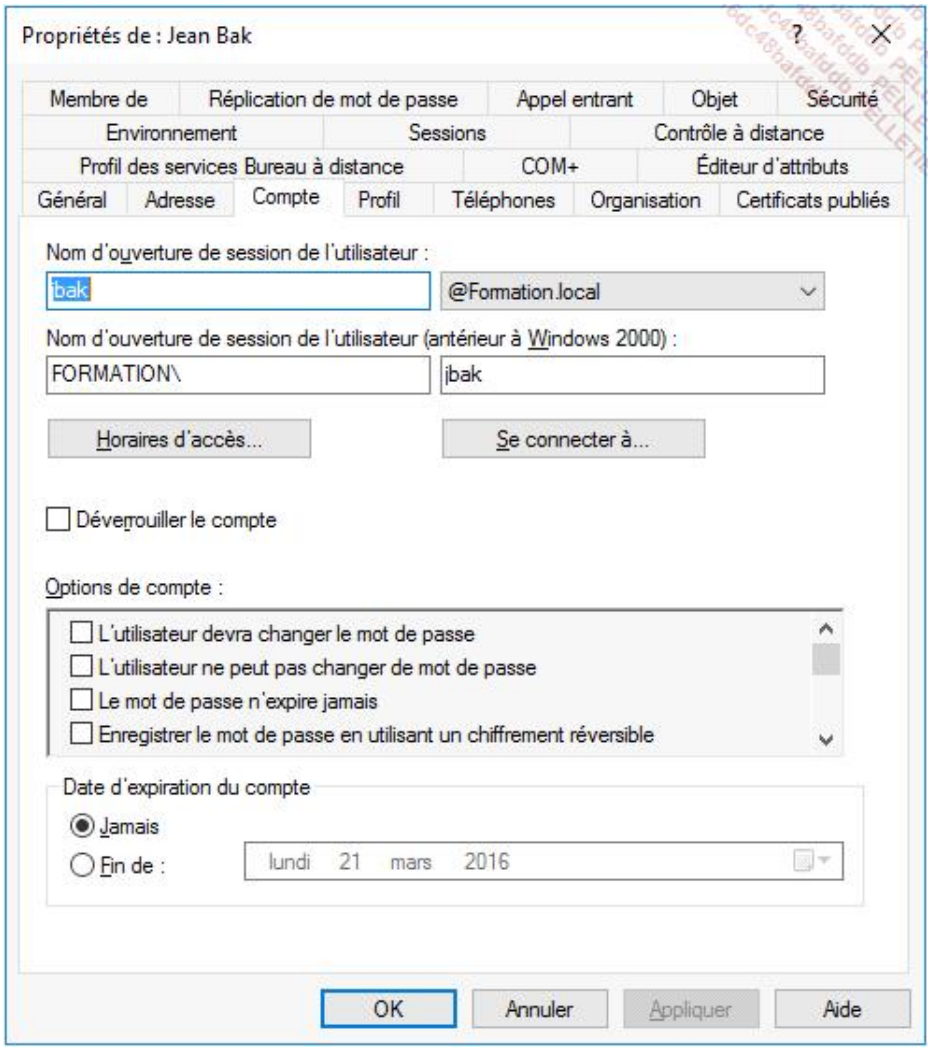
Certains onglets nécessitent l'affichage des fonctionnalités avancées. Dans la console Utilisateurs et ordinateurs Active Directory, cliquez sur le menu **Affichage** puis sur **Fonctionnalités avancées**. Seuls les onglets et propriétés les plus utilisés sont détaillés ci-dessous.

- L'onglet **Général** reprend les informations saisies lors de la création de l'objet. Il est possible de les compléter en saisissant la page web, le numéro de téléphone…
- L'onglet **Compte** permet de modifier le nom d'utilisateur mais également les différentes options de compte telles que :
  - l'utilisateur doit changer le mot de passe,
  - le mot de passe n'expire jamais.

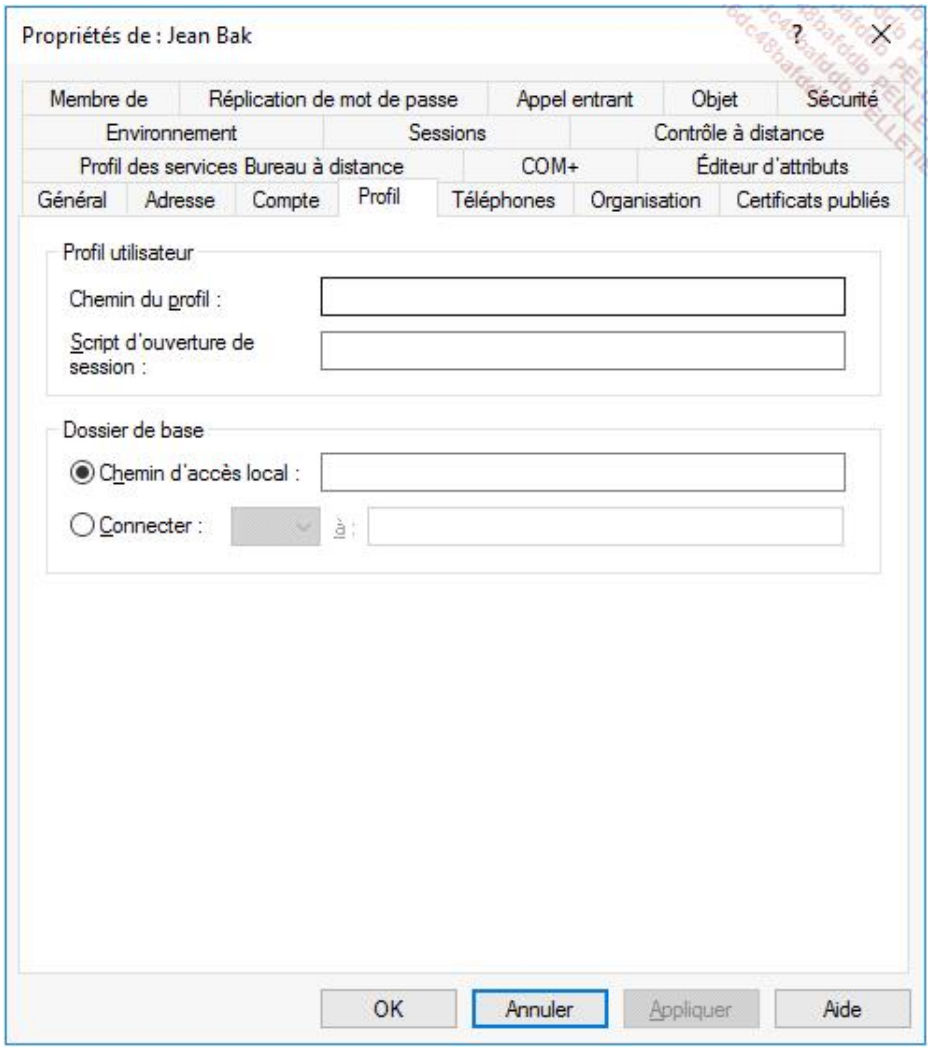
Il est également possible de choisir une date d'expiration pour le compte (très utile pour des personnes en CDD ou des stagiaires) ; lorsque la date est passée, le compte est automatiquement désactivé.

Le déverrouillage du compte peut également être effectué suite à un nombre de tentatives de connexion infructueuses égal à celui configuré dans la stratégie de mot de passe.

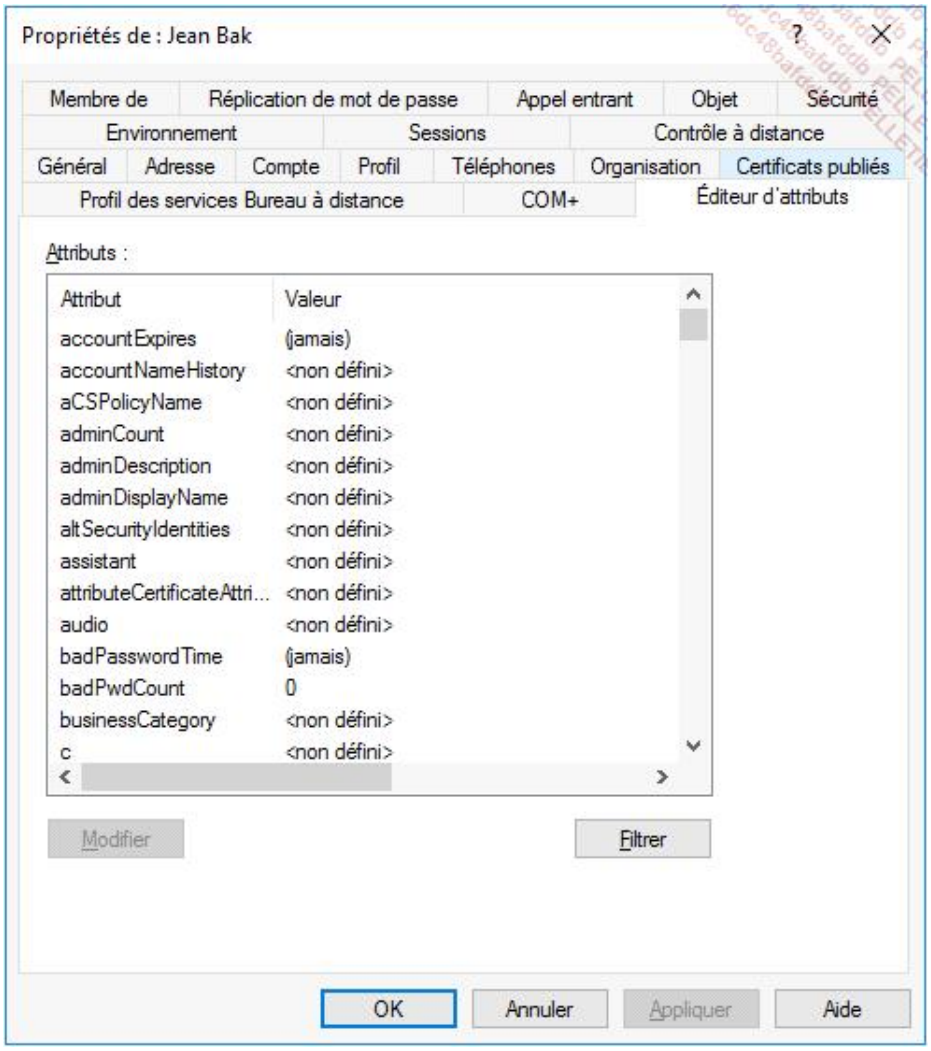
Enfin, la configuration des horaires d'accès, qui permet d'autoriser l'ouverture de session sur le domaine dans une fourchette de temps (par exemple, 9h - 18h), et la limitation des postes sur lesquels l'utilisateur a le droit de se connecter sont également deux propriétés configurables dans cet onglet.



- L'onglet **Profil** permet de configurer le chemin du profil de l'utilisateur. Lors de l'ouverture de session, le système d'exploitation vient récupérer le profil stocké dans le partage réseau. Par la suite, il est copié sur le poste sur lequel l'utilisateur a ouvert une session. Les modifications sont copiées dans le profil stocké sur le serveur lors de la fermeture de session. Le champ **Script d'ouverture de session** permet l'exécution d'un script lors d'une ouverture de session sur un poste de travail ou un serveur. Il est possible de réaliser la même opération lorsqu'un poste démarre ou s'arrête. Dans ce cas, l'exécution du script doit être configurée par une stratégie de groupe.

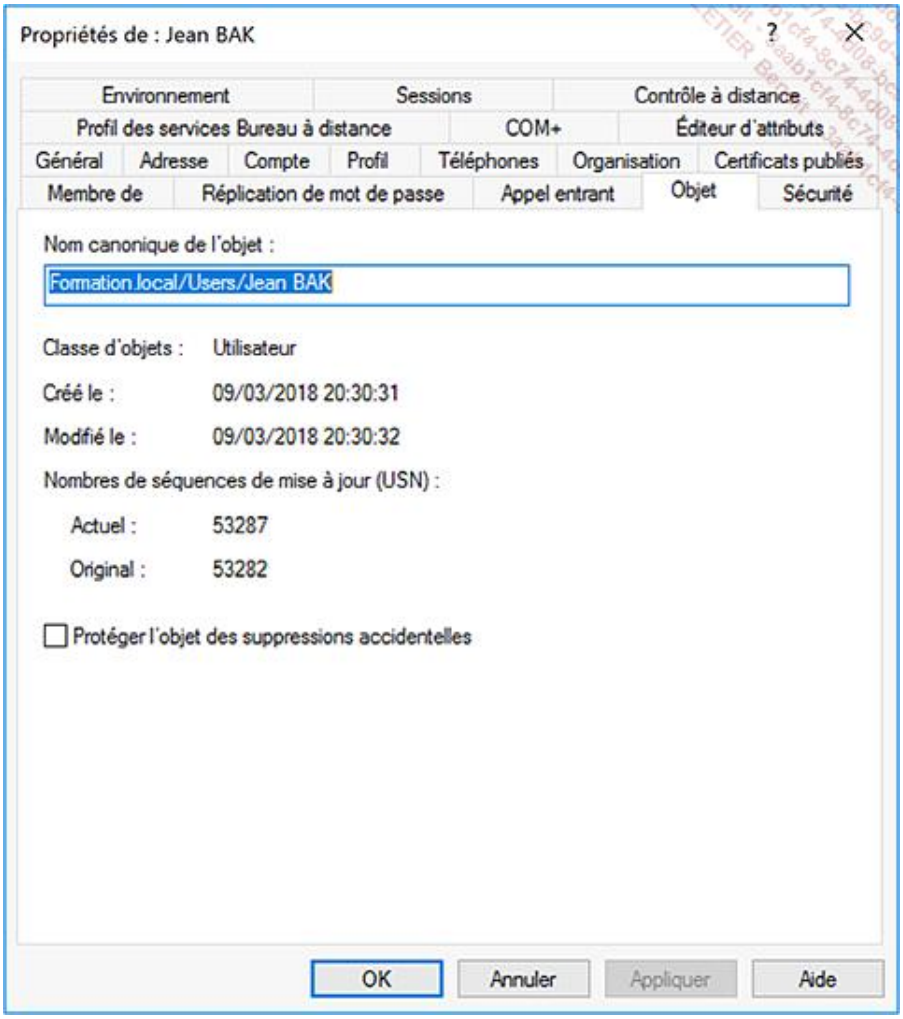


- L'onglet **Éditeur d'attributs** permet la visualisation et/ou la modification des attributs LDAP de l'objet.



Les fonctionnalités avancées doivent être activées pour accéder à cet onglet.

- L'onglet **Membre de** permet de visualiser les groupes dont l'objet est membre. Il est de même possible d'ajouter de nouveaux groupes.
- L'onglet **Réplication de mot de passe** est utilisé avec un serveur RODC (*Read Only Domain Controller*), il permet de s'assurer que le mot de passe du compte utilisateur a bien été mis en cache sur le serveur en lecture seule. Et ainsi permettre à l'utilisateur de se connecter même en cas de coupure de la ligne Wan. Par défaut, la fonctionnalité de mise en cache est désactivée.
- L'onglet **Objet** permet d'obtenir le nom canonique de l'objet. Ce dernier est composé du nom complet de l'objet précédé par son conteneur. Si ce dernier est enfant d'un autre conteneur, celui-ci apparaîtra et ainsi de suite jusqu'à la racine du domaine. On peut également visualiser la classe de l'objet ainsi que les date et heure de création et dernière modification. Le nombre de séquences de mise à jour (*Update Sequence Numbers* - USNs), qui s'incrémente à chaque modification, est également présent. Enfin la protection contre la suppression accidentelle peut également être activée. Par défaut, cette fonctionnalité est désactivée.



Comme pour tout objet Active Directory, une liste ACL est présente et donne des droits de modification, de suppression ou autres à des groupes ou utilisateurs.

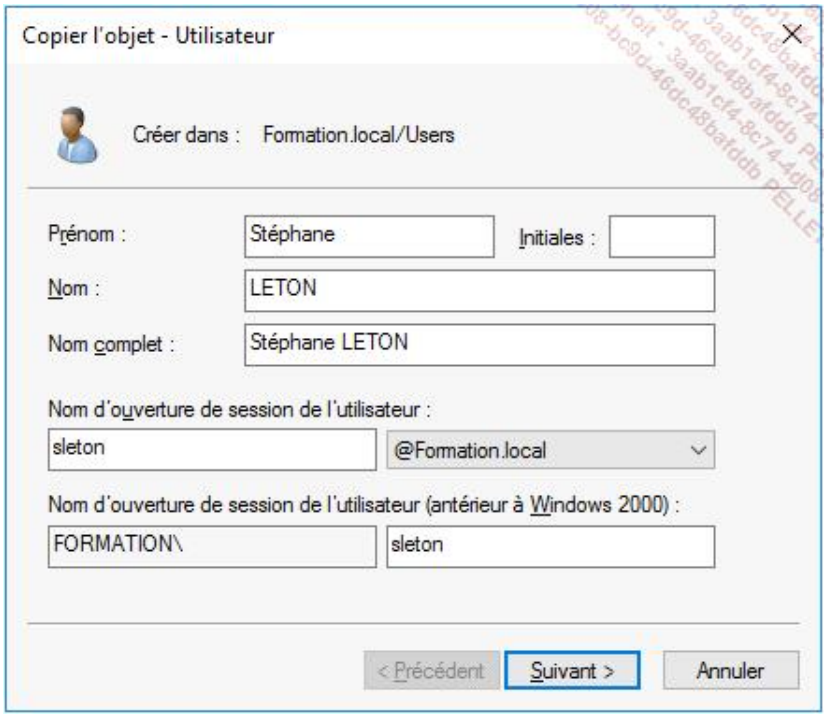
3. Création d'un modèle d'utilisateur

Il est fréquent dans une entreprise que plusieurs personnes faisant partie d'un même service aient accès aux mêmes ressources partagées. La liste des groupes dont ils sont membres est donc la même. Afin de faciliter la création d'utilisateurs possédant des propriétés communes, il est possible de créer un utilisateur modèle qui peut être copié. L'utilisateur qui sert de modèle peut être un compte modèle désactivé ou tout simplement un compte activé.

- Configurez les champs des onglets **Général**, **Adresse**, **Compte**, **Profil** et **Organisation** sur l'utilisateur **Jean BAK**.

Seuls les champs communs à tous sont copiés. Les autres devront être saisis pendant ou après la création.

- Effectuez un clic droit sur l'utilisateur puis, dans le menu contextuel, sélectionnez **Copier**.
- Un assistant de création se lance. Remplissez les champs **Prénom**, **Nom** puis **Nom d'ouverture de session de l'utilisateur** et **Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000)** puis cliquez sur **Suivant**.

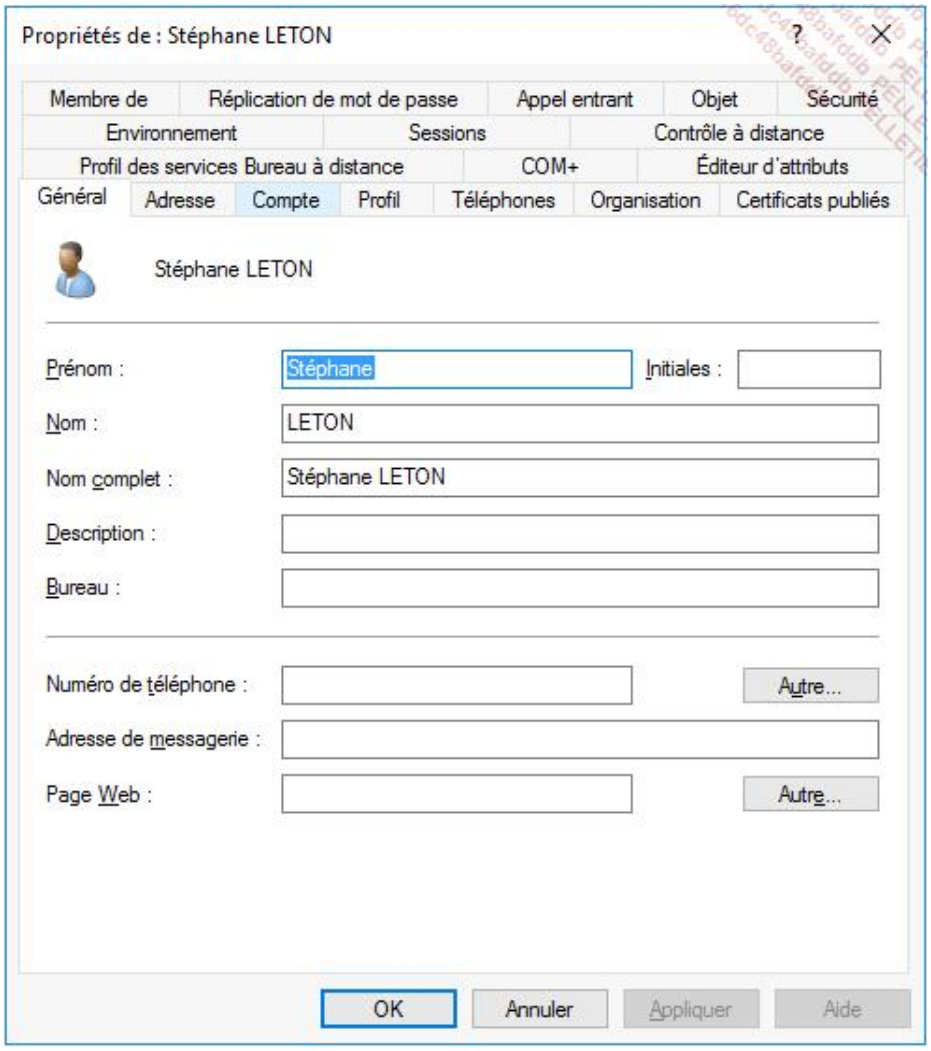


- Saisissez **Pa$$w0rd** dans le champ **Mot de passe**, puis confirmez-le et cliquez sur **Suivant**.

Les options de compte sont par défaut les mêmes que celles du compte modèle.

- Validez la création à l'aide du bouton **Terminer**.

Dans l'onglet **Général**, aucun champ n'a été copié depuis le compte modèle.



Les propriétés qui sont copiées sont :

- **Ville** et **Code postal** dans l'onglet **Adresse**.
- Toutes les propriétés à l'exception des noms d'ouverture de session.
- Le chemin du profil et le script d'ouverture de session.
- **Service** et **Société** dans l'onglet **Organisation**.
- La liste des groupes dans l'onglet **Membre de**.

4. Le jeton d'accès

Lors de l'ouverture d'une session, Active Directory se charge de l'authentification des utilisateurs et ordinateurs. L'autorité de sécurité locale (LSA, *Local Security Authority*) traite les requêtes d'authentification effectuées, pour cela Kerberos v5 est utilisée. Le protocole NTLM / NTLMv2 peut également être utilisé.

Après avoir authentifié un utilisateur, le contrôleur de domaine qui a effectué l'opération génère un jeton d'accès. Ce dernier contient le SID (*Security Identifier*) de l'utilisateur, ainsi que le SID des groupes dont l'utilisateur est membre. Lors de l'ajout dans un nouveau groupe (après la création du jeton), il est nécessaire de fermer puis rouvrir la session. Ceci permet d'effectuer une nouvelle fois l'étape de génération du jeton et de posséder le SID du nouveau groupe. Si la régénération n'est pas effectuée, l'utilisateur ne pourra pas accéder à la ressource partagée.

Lors de la tentative d'accès à une ressource, les SID contenus dans le jeton de l'utilisateur sont comparés à ceux présents dans la DACL (*Discretionary Access Control List*). Si un SID est trouvé, l'utilisateur se voit accorder l'accès avec les droits configurés dans la liste de contrôle d'accès, sinon l'accès est refusé.

5. Création d'un utilisateur en PowerShell

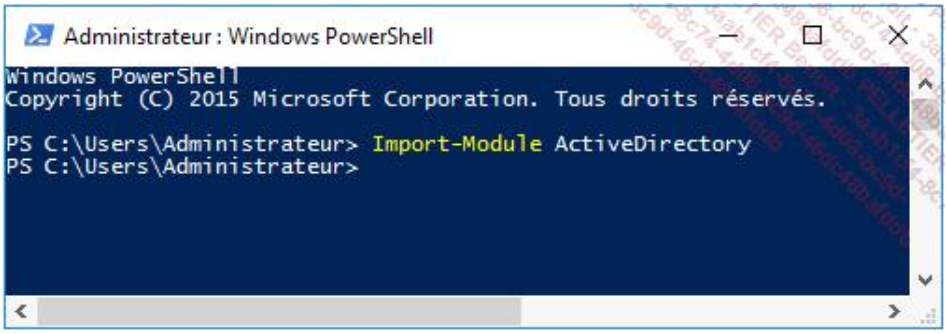
La création d'utilisateurs Active Directory en PowerShell permet d'automatiser la création de un ou plusieurs objets. Il est possible d'utiliser un fichier CSV avec un script PowerShell afin de créer un grand nombre d'utilisateur.

La cmdlet permettant la création d'un objet utilisateur dans un annuaire AD est **NewADUser**.

Les syntaxes ci-dessous peuvent être utilisées afin de créer un utilisateur.

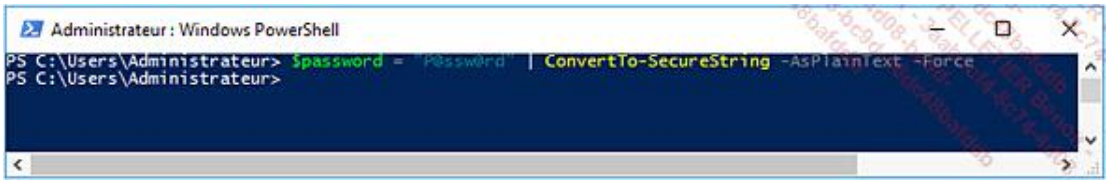
Dans un premier temps, le module Active Directory doit être importé, cela permet l'utilisation de commandes liées à l'annuaire AD (récupération des attributs LDAP d'un compte, création d'un utilisateur…). Ce module est présent sur les contrôleurs de domaine.

```
Import-module ActiveDirectory.
```



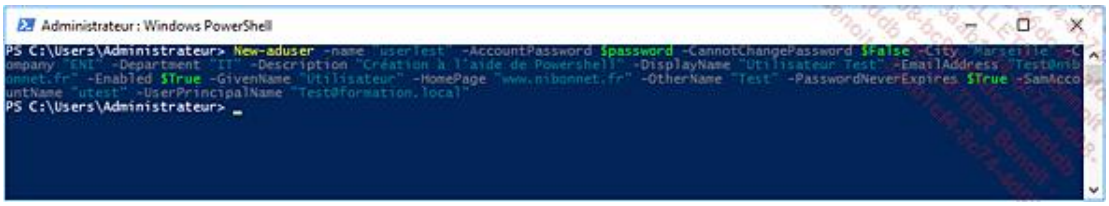
Nous allons maintenant utiliser une variable nommée password, qui nous servira à stocker le mot de passe de l'utilisateur. Néanmoins avant d'être stocké dans la variable, le mot de passe est converti en chaîne de caractère sécurisée.

```
$password = "P@ssw@rd" | ConvertTo-SecureString -AsPlainText -Force
```



L'instruction `New-aduser` peut maintenant être utilisée afin de procéder à la création du compte utilisateur. Le paramètre **CannotChangePassword** positionné à `False` autorise l'utilisateur à changer le mot de passe.

```
New-aduser -name "userTest" -AccountPassword $password
-CannotChangePassword $False -City "Marseille" -Company "ENI" -Department "IT"
-Description "Création à l'aide de Powershell" -DisplayName "Utilisateur Test"
-EmailAddress "Test@nibonnet.fr" -Enabled $True -GivenName "Utilisateur"
-HomePage "www.nibonnet.fr" -PasswordNeverExpires $True -SamAccountName "utest"
-UserPrincipalName "Test@Formation.local"
```



Le script peut être téléchargé depuis la page Informations générales.

L'utilisateur est correctement créé.

Les groupes dans Active Directory

Afin de faciliter l'administration, il est recommandé d'utiliser des groupes (comprenant des utilisateurs ou des ordinateurs). L'administration des accès à des ressources partagées au travers de groupes de sécurité est plus aisée. Une fois le groupe positionné, l'administration s'effectue depuis la console **Utilisateurs et ordinateurs Active Directory** et quasiment plus sur la ressource. Pour donner une autorisation, il suffit de rajouter l'utilisateur dans le groupe, pour lui ôter l'autorisation, il suffit d'enlever l'utilisateur du groupe.

De plus, un groupe peut être positionné sur la liste de contrôle d'accès de plusieurs ressources. La création des groupes peut être réalisée de deux manières :

- Par profil (un groupe Compta par exemple) ce qui permet de regrouper les personnes du service comptabilité.
- Par ressources (Compta, IT…), ce qui permet de regrouper toutes les personnes souhaitant accéder à une ressource.

Le nom du groupe doit, dans la mesure du possible, être le plus parlant possible. Prenons un exemple de nomenclature, cette dernière doit englober les composants suivants :

- **L'étendue**, ce point est traité plus loin dans le chapitre (**G** pour globale, **U** pour universel ou **DL** pour domaine local).
- **Le nom de la ressource** (Compta, Fax, BALNicolas, RH…).
- **Le droit NTFS** qui va être attribué au groupe (**w** pour écriture, **m** pour modifier, **r** pour lecture...).

Ainsi, si le groupe se nomme **G_Compta_w**, on peut très vite en déduire que c'est un groupe global positionné sur le dossier partagé Compta et qui donne des droits d'écriture à ses membres.

1. Types de groupes

Il existe dans Active Directory deux types de groupes : les **groupes de sécurité** et les **groupes de distribution**. Concernant le premier type, il consiste en une entité de sécurité et possède un SID. Il peut donc être positionné sur une liste de contrôle d'accès ou être utilisé comme groupe de diffusion par le serveur Exchange. Ce type de groupe possédant un SID, il est présent dans le jeton d'accès de l'utilisateur. Pour cette raison, il est conseillé, si le groupe est utilisé uniquement pour l'envoi de mail, de choisir un groupe de distribution.

Ce dernier type de groupes est utilisé par les applications de messagerie comme groupe de diffusion. Ne possédant pas de SID, les groupes concernés ne peuvent pas être positionnés dans une liste de contrôle d'accès. Un mail envoyé à ce groupe est transféré à l'ensemble de ses membres.

2. Étendues des groupes

Un groupe peut contenir des utilisateurs, des ordinateurs ou d'autres groupes en fonction de son étendue. En effet, cette dernière a un impact sur les membres et sur la ressource sur laquelle il est positionné. Il existe quatre étendues de groupe :

- **Local** : ce type de groupe se trouve dans la base locale (base SAM) de chaque machine ou serveur (à l'exception des contrôleurs de domaine qui n'en possèdent pas). Il peut contenir les utilisateurs ou les groupes locaux à la machine. Ces groupes locaux peuvent également contenir des objets Active Directory de type utilisateurs, ordinateurs ou groupes. Il est utilisé uniquement dans des ACL locales.

Lors de la jonction au domaine d'une station de travail ou d'un serveur, les groupes admins du domaine et utilisateurs du domaine sont respectivement membres des groupes locaux Administrateurs et Utilisateurs de la machine.

- **Domaine local** : utilisé pour gérer les autorisations d'accès aux ressources du domaine, il peut compter comme membres des utilisateurs, ordinateurs ou groupes globaux et universels de la forêt. Les groupes de type domaine local membres de ce groupe doivent appartenir au même domaine. Ce type de groupe peut être positionné uniquement sur des ressources (répertoire partagé, imprimante,…) de son domaine.
- **Globale** : contrairement à l'étendue **Domaine local**, les groupes globaux peuvent contenir des utilisateurs, des ordinateurs ou d'autres groupes globaux du même domaine. Ils peuvent être positionnés sur n'importe quelle ressource de la forêt.
- **Universelle** : les groupes universels peuvent contenir les utilisateurs, ordinateurs et groupes globaux et universels de n'importe quel domaine de la forêt. Il peut être membre d'un groupe de type **Universelle** ou **Domaine local**. Le groupe peut être positionné sur les ACL de toutes les ressources de la forêt. Il est préférable d'utiliser un nombre restreint de groupes universels.

La stratégie de gestion des groupes (**IGDLA**) définie par Microsoft permet de comprendre le système d'imbrication. Cette stratégie consiste à ajouter des **I**dentités (utilisateurs et ordinateurs) dans un groupe **G**lobal. Ce dernier est membre d'un groupe **D**omaine **L**ocal. Celui-ci sera positionné dans une **A**CL.

Ainsi, si un nouveau groupe appelé **G_Tech_w** doit avoir accès à la ressource partagée nommée Informatique, il n'est plus nécessaire d'accéder à l'ACL. Un ajout dans le groupe **DL_IT_w** (celui-ci est bien sûr positionné sur la ressource) doit être effectué afin de procurer l'accès souhaité.

3. Identités spéciales dans AD

Active Directory prend en charge les identités spéciales. Les membres de ces groupes sont gérés par le système d'exploitation.

L'affichage ou la modification de ces identités spéciales ne peut pas être effectué par l'intermédiaire de la console **Utilisateurs et Ordinateurs Active Directory**.

Voici une petite liste de ces groupes :

- **Ouverture de session anonyme** : utilisé pour les connexions à une ressource sans avoir fourni un nom d'utilisateur et un mot de passe. Avant Windows Server 2003, ce groupe était membre du groupe Tout le monde par défaut. Ce n'est plus le cas aujourd'hui.
- **Utilisateurs authentifiés** : contrairement aux utilisateurs anonymes, les membres de ce groupe sont les objets authentifiés par un contrôleur de domaine. Le compte invité n'est pas contenu dans ce groupe, même s'il dispose d'un mot de passe.
- **Tout le monde** : ce groupe contient l'ensemble des utilisateurs authentifiés ainsi que le groupe Invité.
- **Interactif** : lorsqu'un utilisateur accède à une ressource sur un ordinateur sur lequel il a ouvert une session localement, il est ajouté à ce groupe. Ce dernier contient également les utilisateurs qui ont ouvert une session via le bureau à distance.
- **Réseau** : contrairement au groupe précédent, celui-ci concerne les utilisateurs qui accèdent à une ressource sur le réseau.

Comme nous avons pu le voir, la gestion de ces groupes ne peut pas être effectuée par l'administrateur mais ce dernier a la possibilité de les rajouter dans une ACL.

4. Création d'un groupe

Sur AD1, ouvrez une session en tant qu'administrateur puis lancez la console **Utilisateurs et ordinateurs**

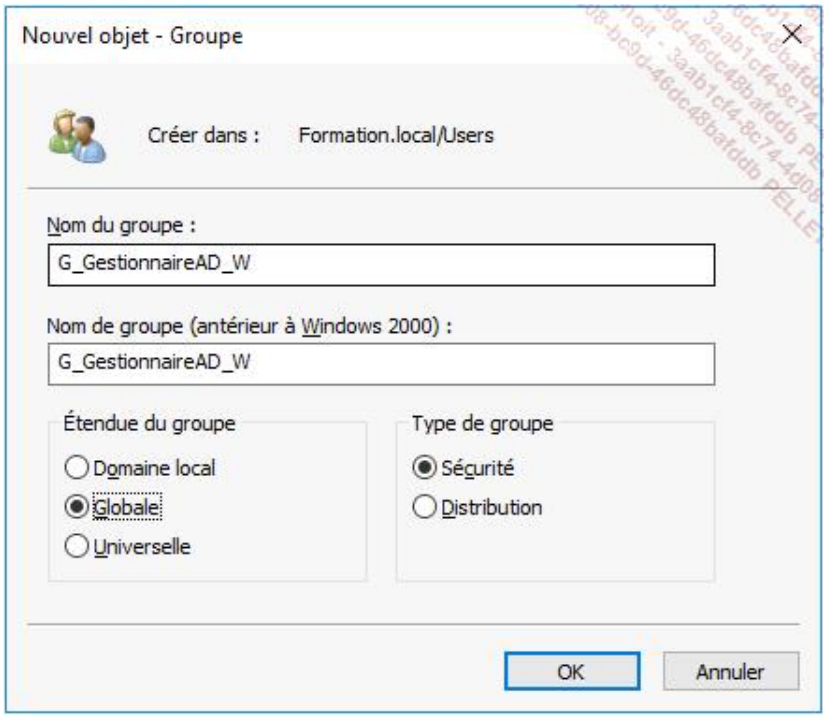
Active Directory.

- Sélectionnez le dossier système **Users**.
- Dans la barre d'outils, cliquez sur l'icône permettant l'ajout d'un groupe.

L'icône située à droite de celle permettant la création d'un groupe est grisée, ceci est le cas lorsque nous sommes dans un conteneur système. La création d'une unité d'organisation est impossible dans ce type de conteneur.



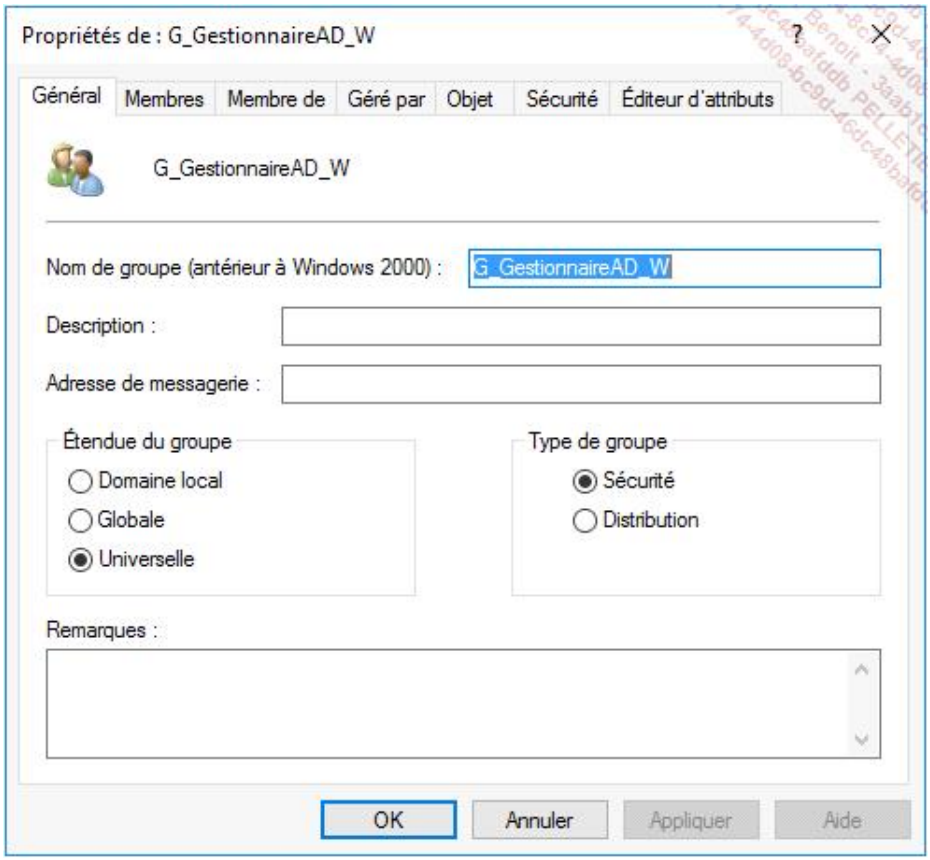
- Dans le champ **Nom du groupe** saisissez **G_GestionnaireAD_W** puis cliquez sur **OK**.



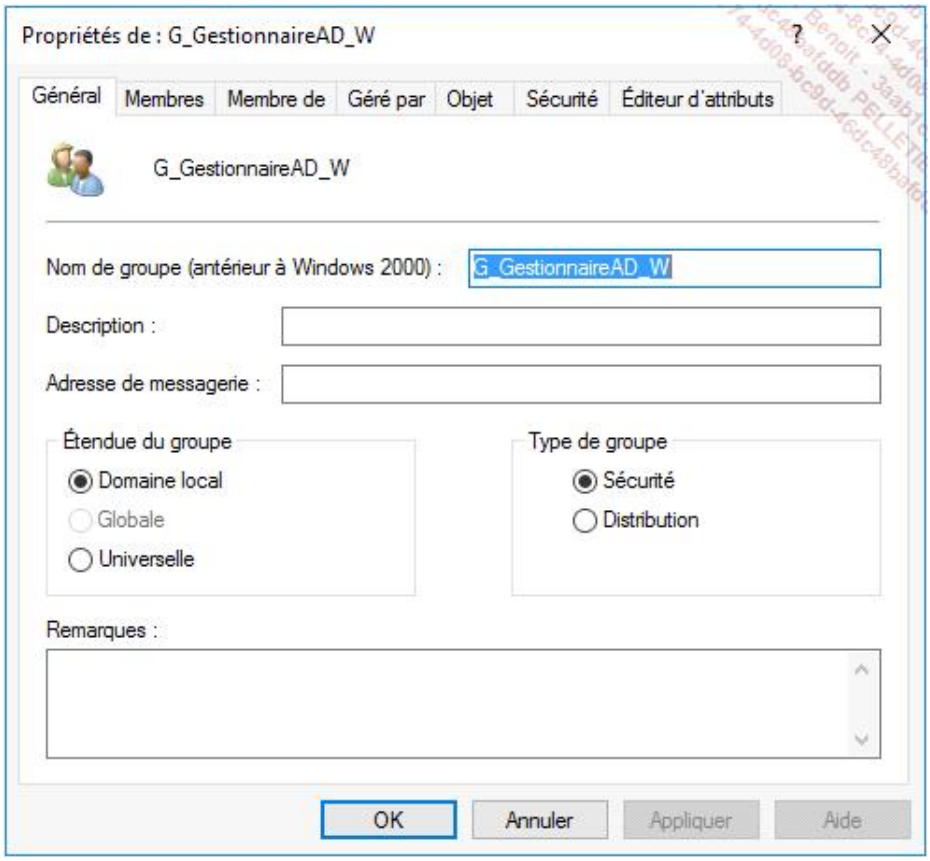
- Double cliquez sur le groupe qui vient d'être créé.

L'onglet **Général** reprend les informations que nous avons saisies. Le changement de l'étendue peut être fait (en fonction des membres du groupe…) depuis cet onglet. Pour mettre l'étendue en **Domaine local**, il est nécessaire dans un premier temps de la passer en **Universelle**.

- Cliquez sur **Universelle** puis sur **Appliquer**.

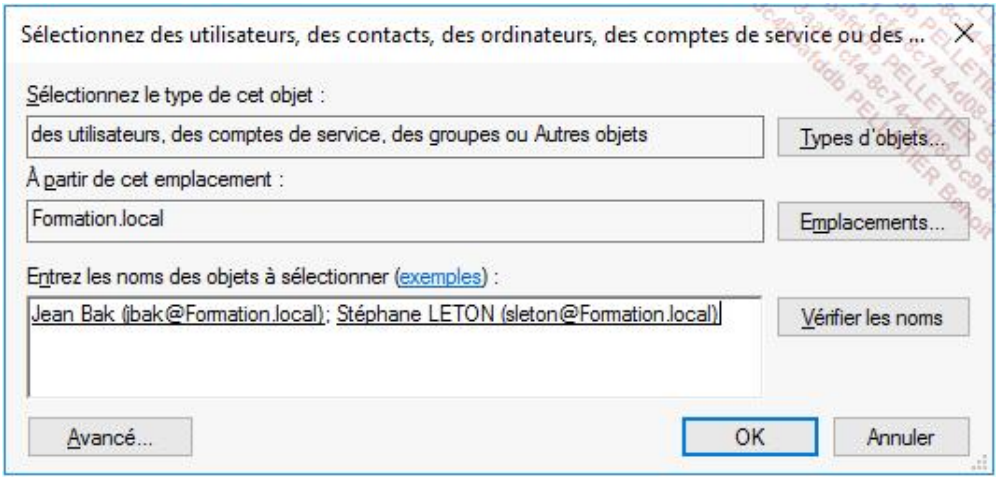


- Sélectionnez **Domaine local** et validez le choix en cliquant sur **Appliquer**.

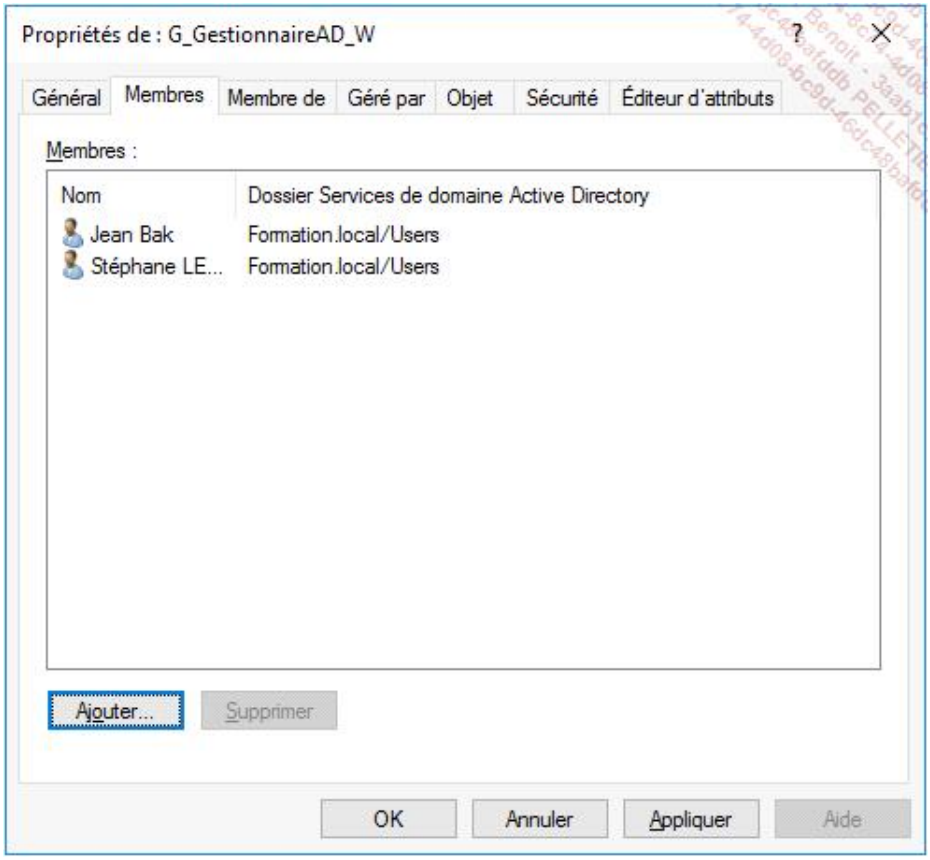


Les onglets **Membres** et **Membre de** permettent de rajouter des objets dans le groupe ou de rendre ce dernier membre d'un autre groupe.

- Cliquez sur l'onglet **Membres** puis sur le bouton **Ajouter**.
- Dans le champ **Entrez les noms des objets à sélectionner**, saisissez **Jbak;Sleton** et cliquez sur **Vérifier les noms**.



- Cliquez sur **OK**.



Comme pour tous les objets AD (unité d'organisation, compte utilisateur, compte ordinateur et groupe), la protection contre la suppression peut être activée. Certaine opération nécessite de sélectionner l'option **Fonctionnalité Avancée** dans le menu **Affichage**.

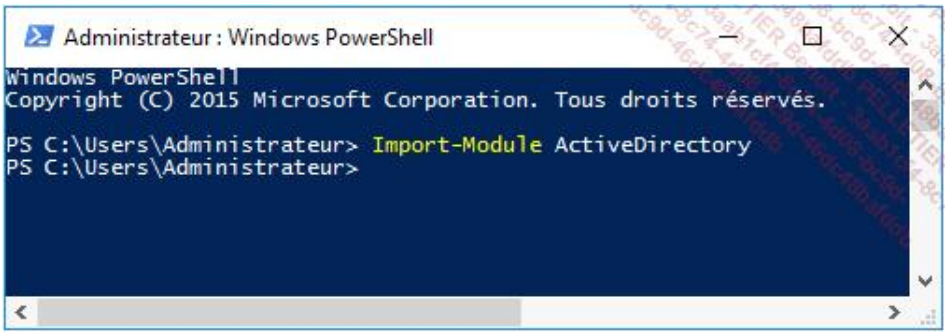
5. Création d'un groupe en PowerShell

Comme pour les utilisateurs, il est possible de créer des groupes Active Directory à l'aide de PowerShell.

La cmdlet **New-ADGroup** permet d'effectuer l'opération. La syntaxe à utiliser est la suivante :

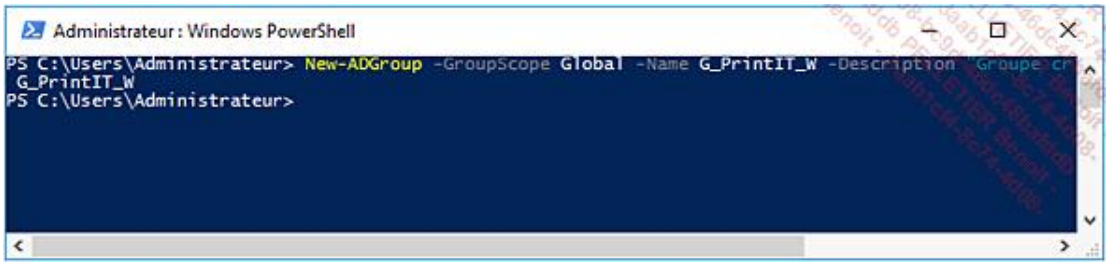
- Dans un premier temps, l'importation du module Active Directory doit être effectuée. Ceci permettra l'utilisation des cmdlets nécessaires pour effectuer des opérations sur l'annuaire.

```
Import-Module ActiveDirectory
```



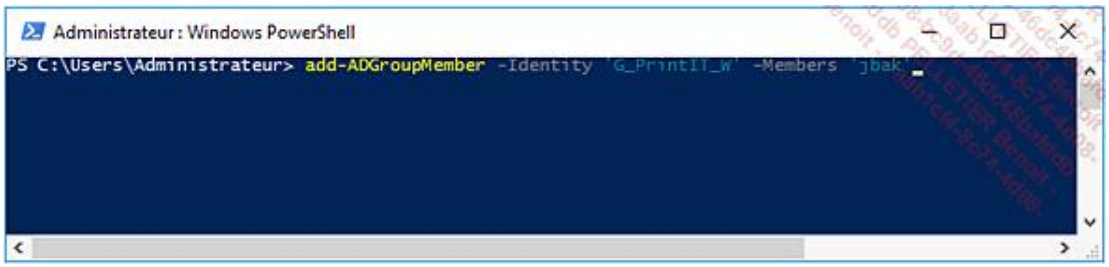
- L'opération de création peut maintenant être lancée.

```
New-ADGroup -GroupScope Global -Name G_PrintIT_W -Description
"Groupe créé avec Powershell" -DisplayName G_PrintIT_W
```



- Le groupe est bien créé, néanmoins l'ajout d'utilisateur s'effectue à l'aide de la cmdlet `Add-ADGroupMember`. Le module Active Directory doit avoir été importé avant d'exécuter la commande suivante :

```
add-ADGroupMember -Identity 'G_PrintIT_W' -Members 'jbak'
```

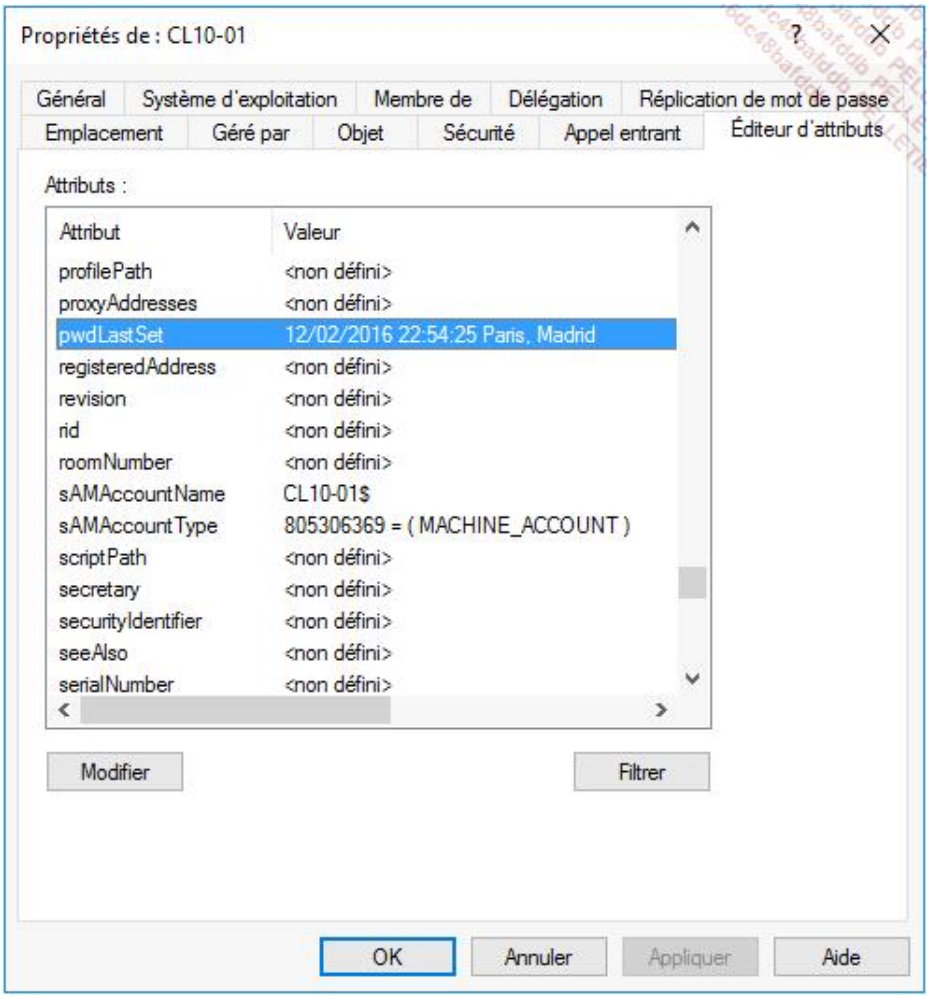


Après avoir exécuté l'ensemble des opérations ci-dessus, le groupe est bien créé et l'utilisateur ajouté.

Le compte ordinateur

Par défaut, un ordinateur appartient à un groupe de travail. Pour pouvoir ouvrir une session sur le domaine, l'ordinateur doit appartenir au domaine. Comme pour le compte utilisateur, l'ordinateur possède un nom d'ouverture de session (attribut **sAMAccountName**), un mot de passe et un SID. Ces informations d'identification permettent au compte ordinateur d'être authentifié sur le domaine. Si l'authentification réussit, une relation sécurisée est établie entre le contrôleur de domaine et le poste. Il est intéressant de noter que le changement de mot de passe d'un compte ordinateur est opéré tous les 30 jours par défaut.

Attribut date de changement de mot de passe



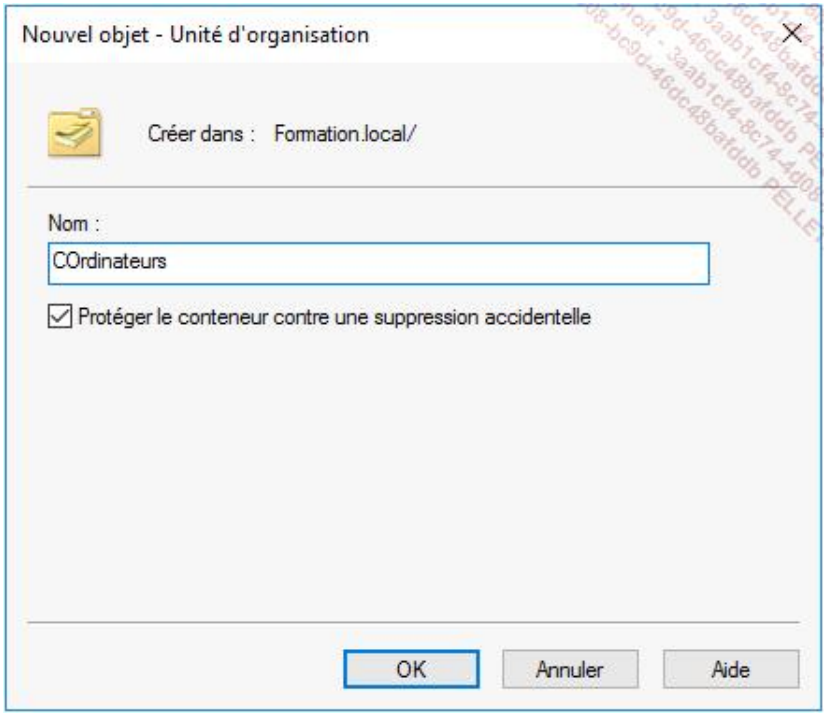
1. Le conteneur Computers

Lorsque l'ordinateur est joint au domaine et si le compte n'existe pas, un compte ordinateur est automatiquement créé dans le conteneur **Computers**. Ce dernier est un dossier système, aucune stratégie de groupe ne peut lui être appliquée (hors héritage évidemment). Il est donc nécessaire de déplacer le compte de l'ordinateur vers l'unité d'organisation souhaitée.

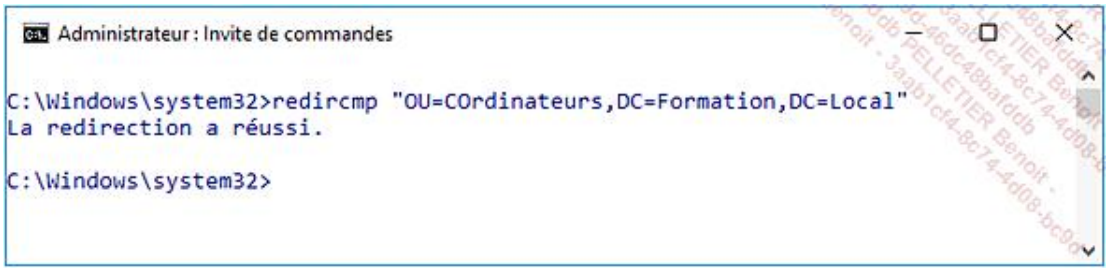
Néanmoins, il est possible d'effectuer la création des nouveaux comptes ordinateurs vers un autre conteneur. En effectuant cette opération, le conteneur par défaut peut être une unité d'organisation sur laquelle est positionnée une stratégie de groupe.

Pour effectuer cette opération, la commande `redircmp` est utilisée.

- Sur AD1, lancez la console **Utilisateurs et ordinateurs Active Directory**.
- Cliquez sur la racine du domaine puis, dans la barre d'outils, cliquez sur l'icône permettant la création d'une unité d'organisation.
- Dans le champ **Nom**, saisissez **COrdinateurs** puis cliquez sur **OK**.



- Lancez une invite de commandes DOS puis saisissez la commande `redircmp "OU=COrdinateurs,DC=Formation,DC=Local"` puis appuyez sur la touche [Entrée] du clavier.



Lors des prochaines jonctions, les comptes ordinateurs seront créés dans l'OU COrdinateurs.

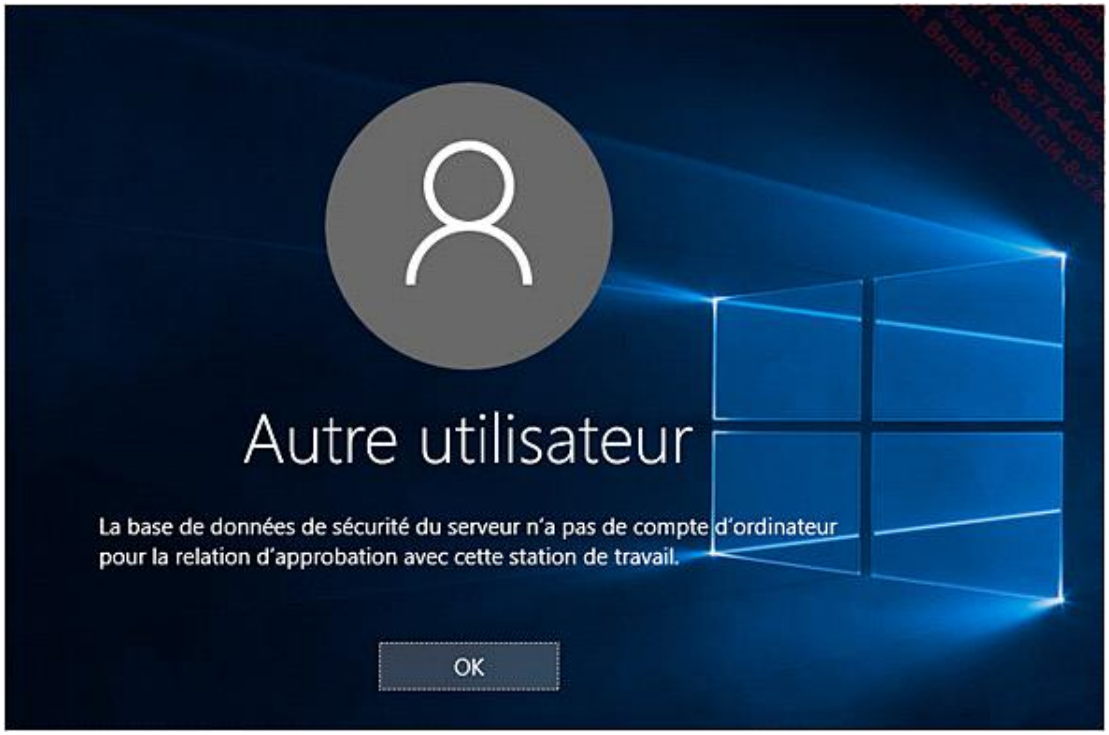
2. Canal sécurisé entre le contrôleur de domaine et le poste

Comme nous l'avons vu plus haut, lors de la jonction au domaine un compte ordinateur est créé. Ce dernier possède un nom d'utilisateur (**sAMAccountName**) et un mot de passe stocké sous forme de secret **LSA** (autorité de sécurité locale). Un changement de mot de passe est effectué tous les 30 jours. Lors de la connexion au domaine, les informations d'identification sont utilisées par le service **Netlogon** afin de créer un canal sécurisé avec le contrôleur de domaine.

Dans certains cas, il peut arriver qu'un canal sécurisé soit rompu. Le compte ordinateur n'étant alors plus authentifié, il est impossible d'ouvrir une session sur le domaine. Plusieurs actions peuvent causer cette rupture du canal :

- Restauration d'un contrôleur de domaine.
- Restauration du poste.
- Suppression et recréation du compte ordinateur.

Dans ces cas-là, un message d'erreur s'affiche, informant l'utilisateur qu'il est impossible de trouver un compte ordinateur.



La recréation du canal sécurisé est nécessaire pour ouvrir la session sur le domaine.

Pour réinitialiser le canal sécurisé rompu il est nécessaire de placer la machine concernée dans un workgroup puis de la remettre dans le domaine.

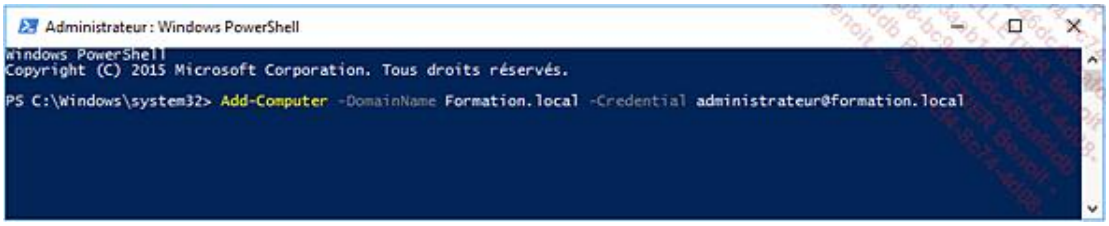
Une autre méthode consiste à régénérer le canal à l'aide des outils netdom ou nltest.

3. Jonction d'un ordinateur en ligne de commande

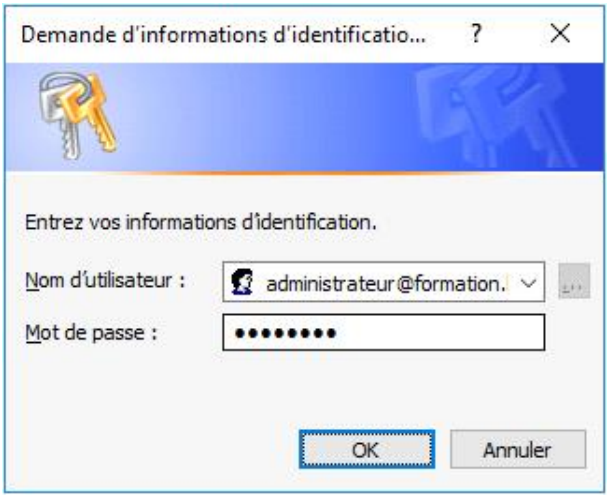
La jonction peut être réalisée à l'aide de l'interface graphique ou automatisée à l'aide de PowerShell.

Pour cela, la cmdlet Add-Computer doit être utilisée. Comme pour les deux précédents, il est nécessaire d'importer le module Active-Directory.

```
Add-Computer -DomainName Formation.local -Credential
administrateur@formation.local
```



Lors de l'exécution de la commande, une boîte de dialogue apparaît afin de pouvoir saisir le mot de passe du compte administrateur@formation.local.



Après le redémarrage, le poste est bien joint au domaine.

La corbeille AD

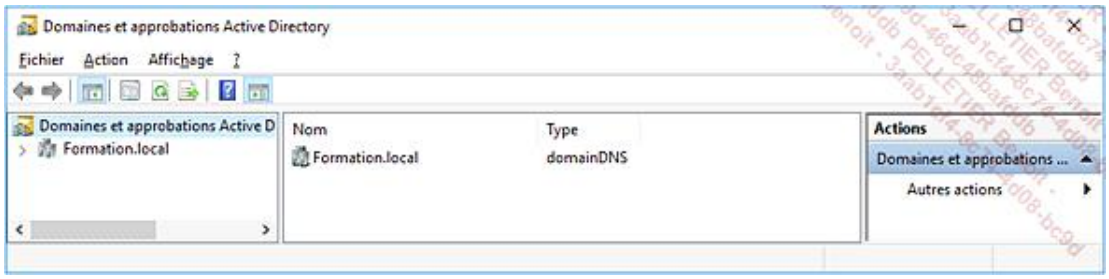
La suppression accidentelle d'un objet Active Directory peut avoir un impact plus ou moins important sur la production. Apparues avec Windows Server 2008 R2, l'activation de la corbeille AD et des objets supprimés étaient effectuées en PowerShell.

Lorsque la corbeille est activée, les attributs des objets Active Directory supprimés sont préservés. Il est donc possible d'effectuer la restauration de l'objet dans son intégralité.

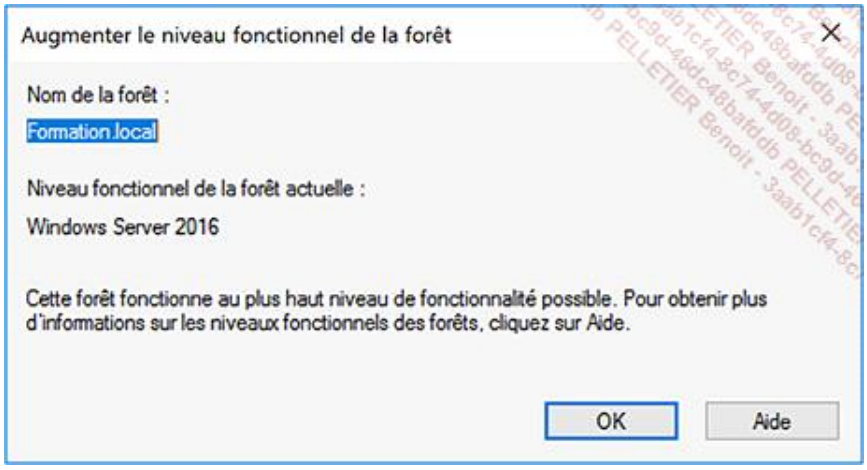
Depuis Windows Server 2012, la fonctionnalité a été améliorée par l'ajout d'une interface graphique qui permet la restauration d'un objet supprimé. Une liste de tous les objets ayant été supprimés s'affiche. L'administrateur peut ainsi sélectionner ceux dont il souhaite la récupération.

Comme beaucoup de fonctionnalités, la corbeille AD possède ses prérequis. Afin de pouvoir l'activer et l'utiliser, il est nécessaire d'avoir un niveau fonctionnel de la forêt configuré sur le niveau Windows Server 2008 R2 au minimum (tous les contrôleurs de domaine doivent donc être au minimum sous Windows Server 2008 R2). Comme pour les versions précédentes, l'activation de la corbeille est irréversible. La désactivation est donc impossible.

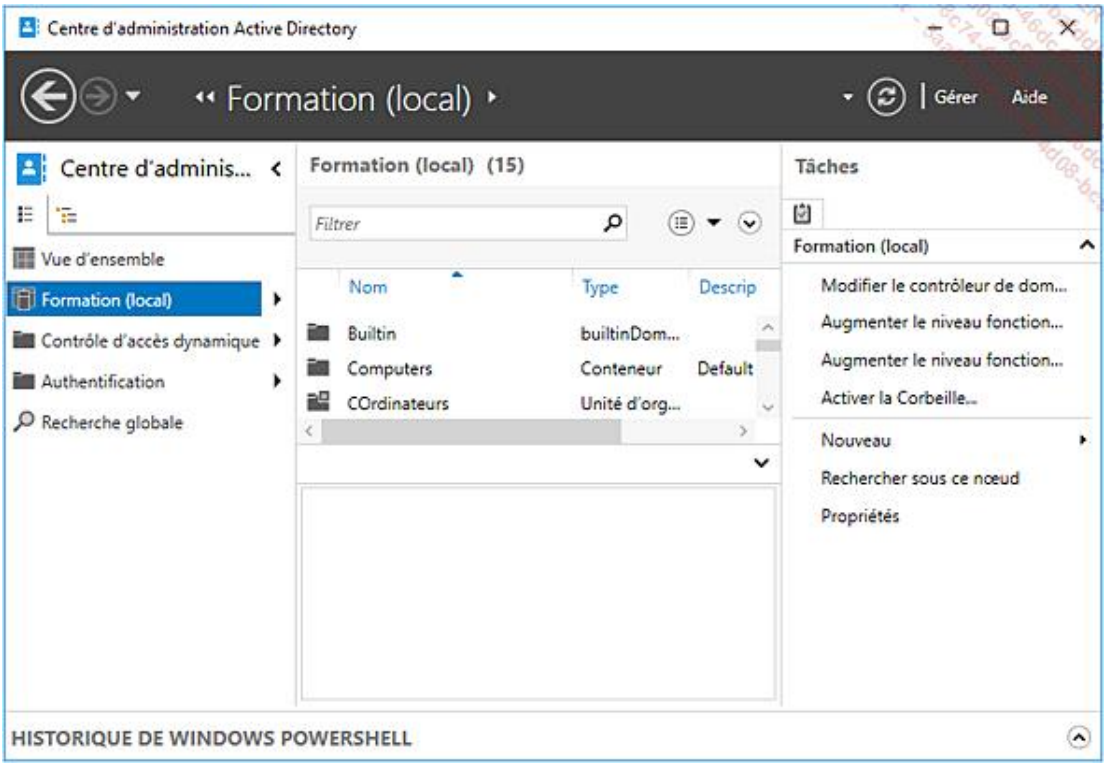
- Sur AD1, ouvrez la console **Domaines et approbations Active Directory**.



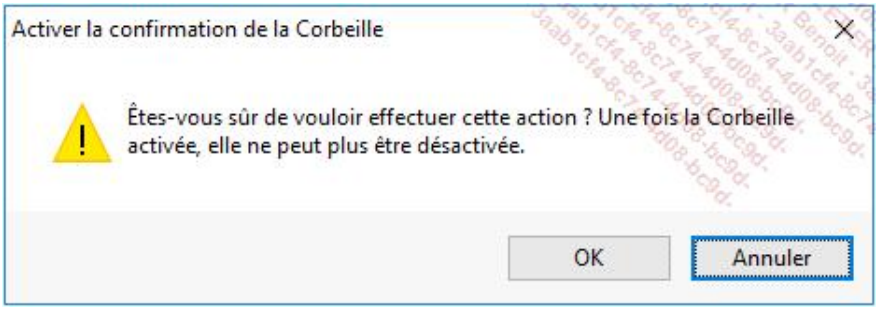
- Effectuez un clic droit sur **Domaines et approbations Active Directory** puis dans le menu contextuel, sélectionnez **Augmenter le niveau fonctionnel de la forêt**.
- Vérifiez qu'il est bien sur un niveau fonctionnel **Windows Server 2008 R2** ou version ultérieure.



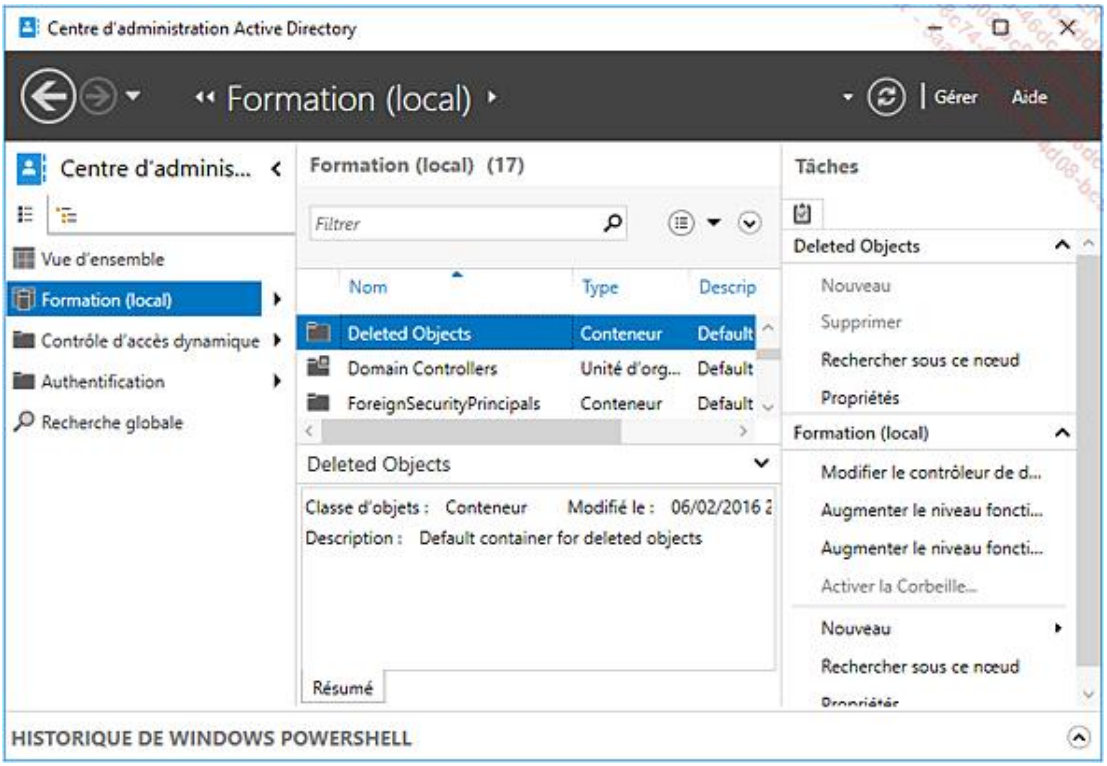
- Lancez la console **Centre d'administration Active Directory** depuis les outils d'administration.
- Dans le menu de gauche, double cliquez sur **Formation (local)**.



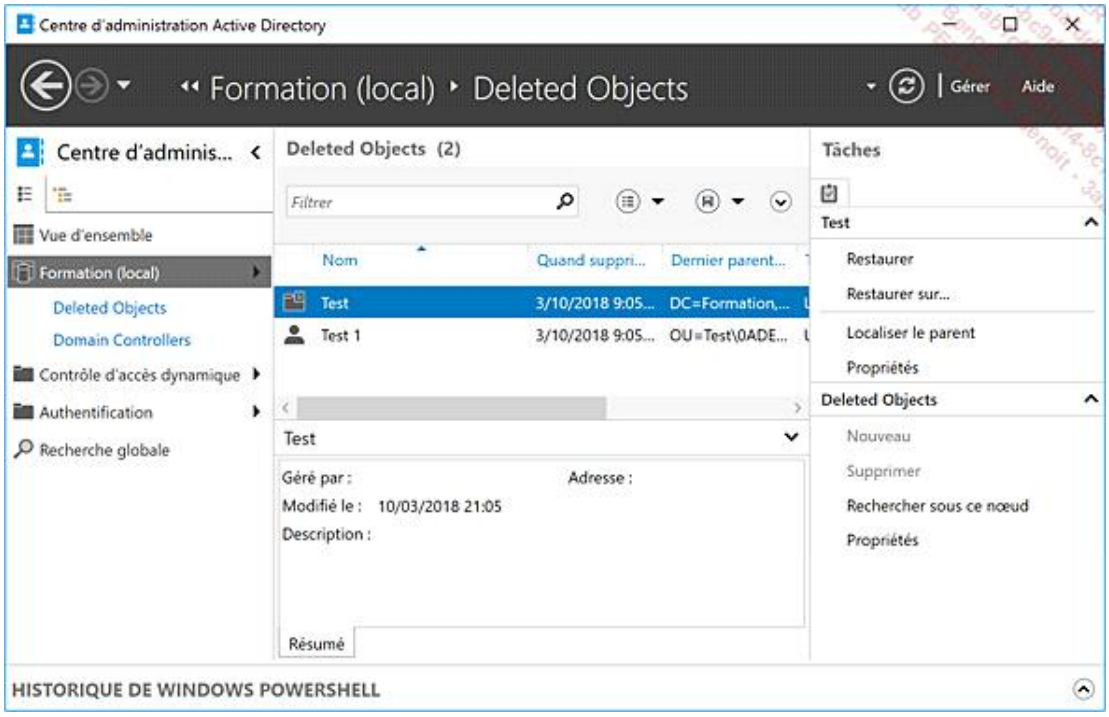
- Cliquez sur **Activer la corbeille** dans le bandeau **Tâches**.
- Cliquez sur **OK** afin de lancer l'activation.



- Créez des unités d'organisation, des groupes et des utilisateurs de test puis supprimez-les afin de les placer dans la corbeille.
- Dans la console **Centre d'administration Active Directory**, double cliquez sur **Deleted Objects**.



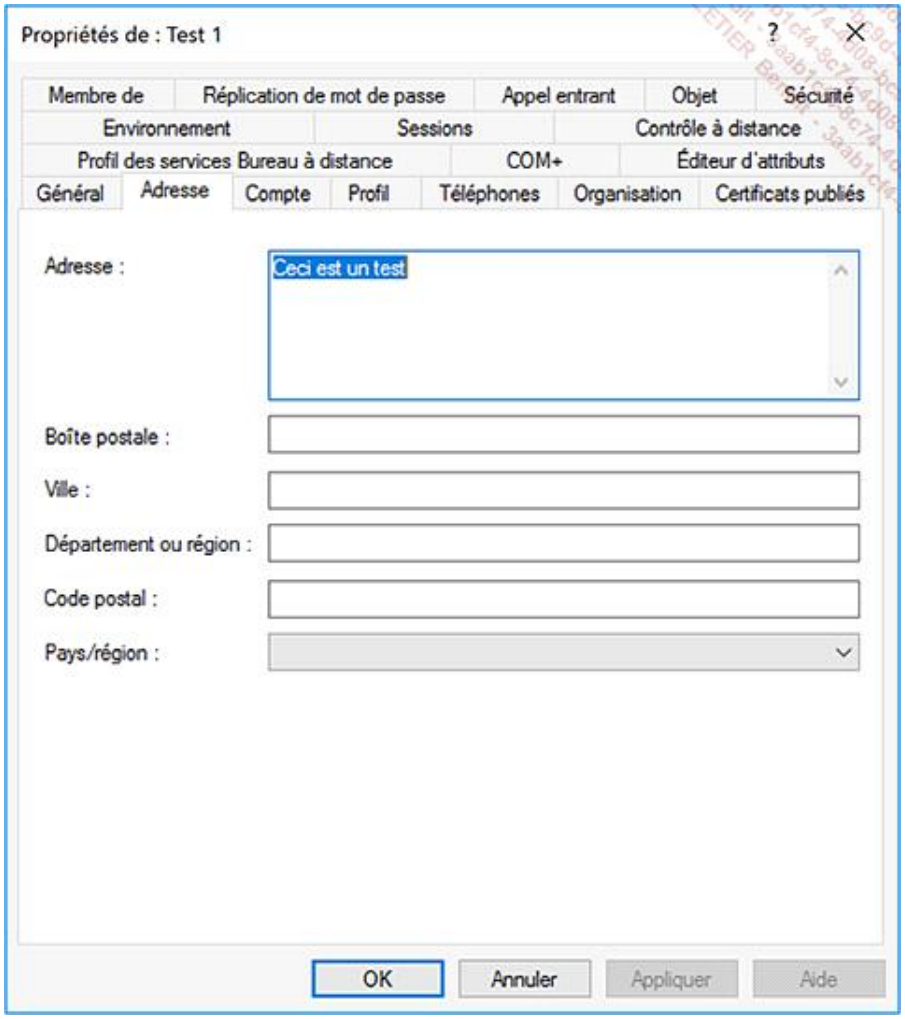
Les objets supprimés précédemment apparaissent.



Sélectionnez les objets supprimés puis cliquez sur **Restaurer**.

Restaurer sur dans le bandeau **Tâches** permet d'effectuer la restauration dans un endroit différent de celui d'origine.

Les attributs des comptes ont bien été restaurés.



Les opérations qui ont été réalisées ci-dessus peuvent être effectuées en PowerShell.

Rôle et fonctionnement du service DHCP

DHCP (*Dynamic Host Configuration Protocol*) est un protocole qui permet d'assurer la configuration automatique des interfaces réseaux. Cette configuration comprend une adresse IP, un masque de sous-réseau mais également une passerelle et des serveurs DNS. D'autres paramètres supplémentaires peuvent être distribués (serveur WINS…).

Au vue de la taille des réseaux actuels, il est souvent nécessaire de remplacer l'adressage statique saisi par un administrateur sur chaque machine par un adressage dynamique effectué par le biais du serveur DHCP. Ce dernier offre l'avantage d'offrir une configuration à chaque machine qui en fait la demande, de plus il est impossible de distribuer deux adresses IP identiques. Le conflit IP est donc évité. L'administration s'en trouve également facilitée.

Le serveur est capable d'effectuer une distribution de configuration IPv4 ou IPv6.

L'opération d'affectation d'une adresse IP passe par l'échange de plusieurs trames entre le client et le serveur.

La machine envoie à l'aide d'une diffusion (envoi d'un *broadcast*), un datagramme (**DHCP Discover**) sur le port **67**.

Tout serveur qui reçoit ce datagramme diffuse une offre DHCP au client (**DHCP Offer**). Le port utilisé pour l'offre est le **68**.

Le client retient la première offre qu'il reçoit et diffuse sur le réseau un datagramme (**DHCP Request**), il contient l'adresse IP du serveur et celle qui vient d'être proposée au client. Le serveur retenu reçoit une demande d'assignation de l'adresse alors que les autres serveurs sont avertis qu'ils n'ont pas été retenus.

Le serveur envoie un datagramme d'accusé de réception (**DHCP ACK** - *Acknowledgement*) qui assigne au client l'adresse IP et son masque de sous-réseau ainsi que la durée du bail et éventuellement d'autres paramètres (passerelle, DNS…).

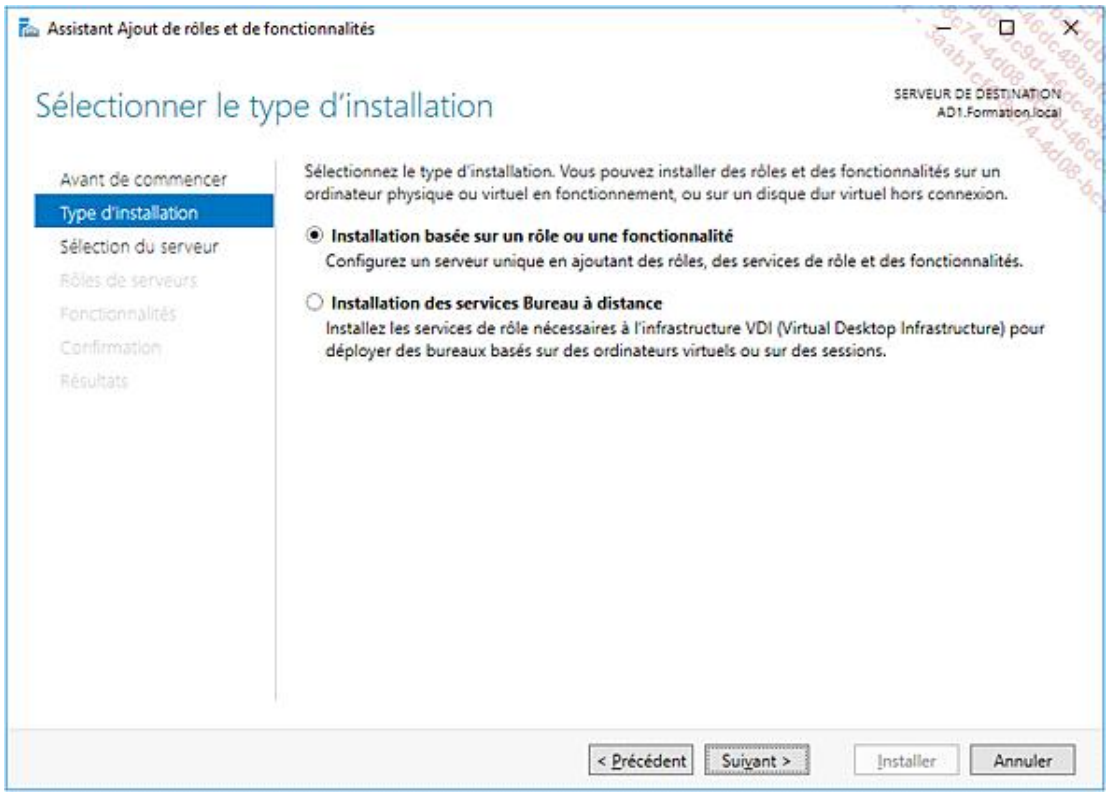
La liste des options que le serveur DHCP peut accepter est définie dans la **RFC 2134**.

Un bail DHCP (configuration attribuée à un poste) a une durée de validité définie par l'administrateur. À 50 % de la durée du bail, le client commence à demander son renouvellement. Cette demande est faite uniquement au serveur qui a attribué le bail. Si ce dernier n'a pas été renouvelé, la prochaine demande s'effectuera à 87,5 % de la durée. Arrivée à son terme, et si le client n'a pas pu obtenir de renouvellement ou une nouvelle allocation, l'adresse est désactivée. Ainsi la faculté d'utiliser le réseau local est perdue.

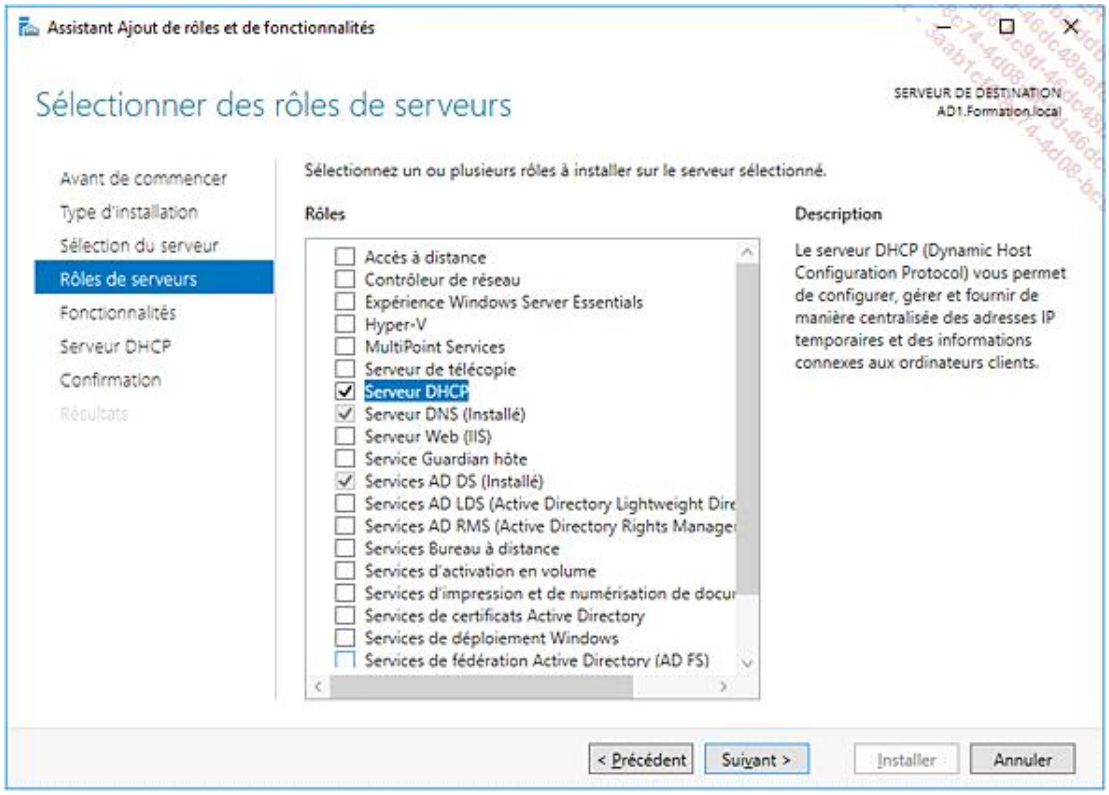
Installation et configuration du rôle DHCP

Comme pour les autres rôles, DHCP s'installe depuis la console **Gestionnaire de serveur**.

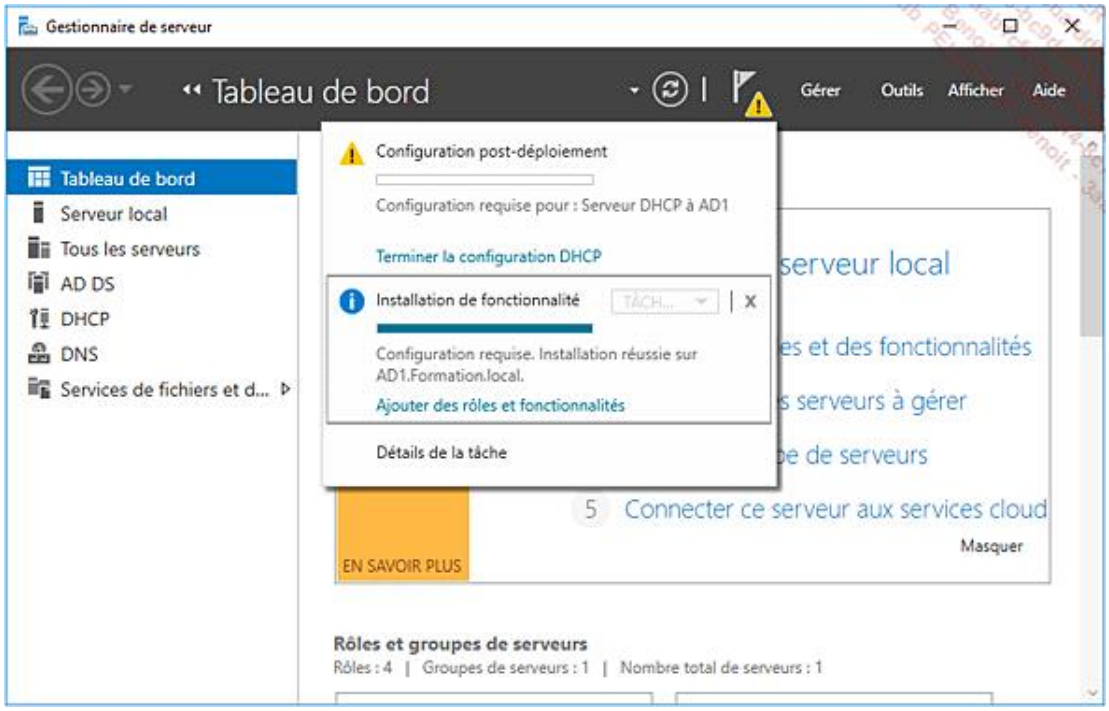
- Sur AD1, ouvrez la console **Gestionnaire de serveur** et cliquez sur **Ajouter des rôles et des fonctionnalités**.
- Dans la fenêtre **Sélectionner le type d'installation**, laissez le choix par défaut.



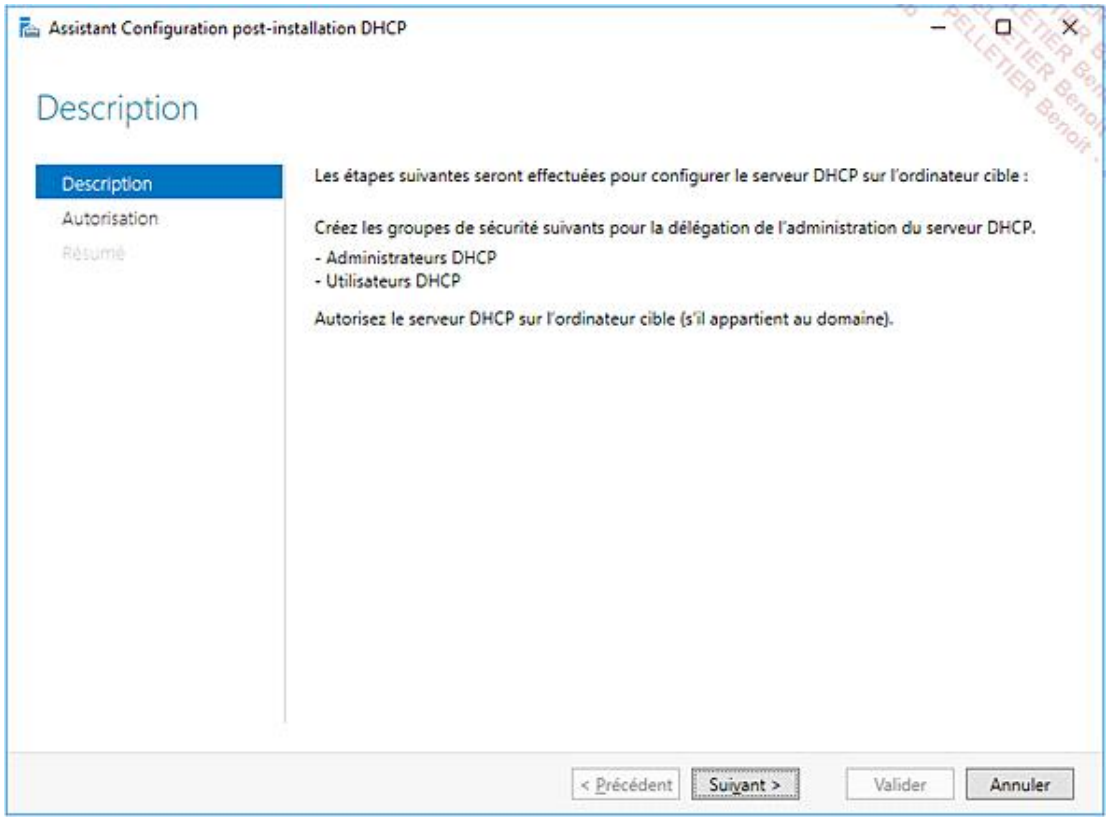
- Le serveur de destination est AD1. Laissez le choix par défaut puis cliquez sur **Suivant**.
- Sélectionnez le rôle **Serveur DHCP**. Les fonctionnalités doivent être installées, cliquez sur **Ajouter des fonctionnalités** dans la fenêtre qui s'affiche.



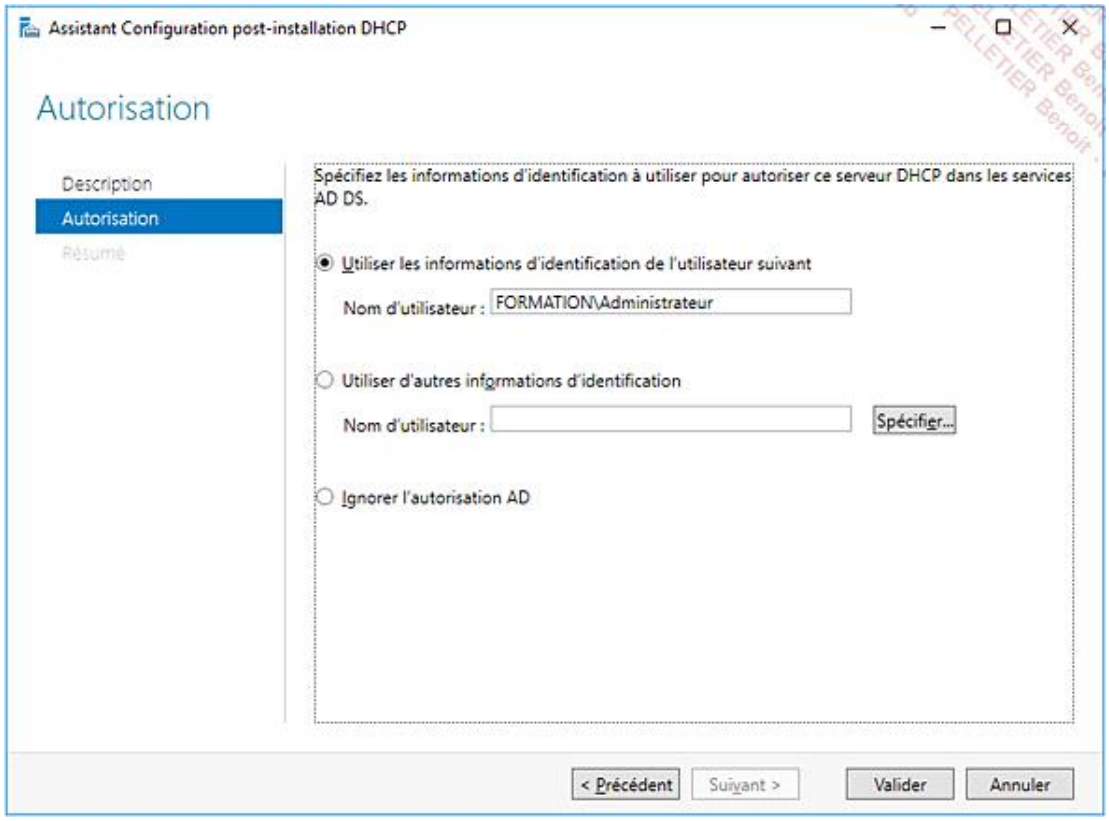
- Cliquez sur **Suivant** dans la fenêtre **Sélectionner des fonctionnalités**.
- Dans la fenêtre de confirmation, cliquez sur **Installer**.
- Dans le **Gestionnaire de serveur**, cliquez sur **Notifications** (drapeau), puis sur **Terminer la configuration DHCP**.



- Un assistant se lance, cliquez sur **Suivant**.



- Cliquez sur **Valider** puis sur **Fermer**.



- Dans le menu Démarrer, cliquez sur **Outils d'administration**.
- Double cliquez sur **DHCP**.

Le rôle est bien installé mais il n'est pas configuré.

1. Ajout d'une nouvelle étendue

Une **étendue DHCP** est constituée d'un pool d'adresses IP (par exemple, 192.168.1.100 à 192.168.1.200). Lorsqu'un client effectue une demande, le serveur DHCP lui attribue une des adresses du pool.

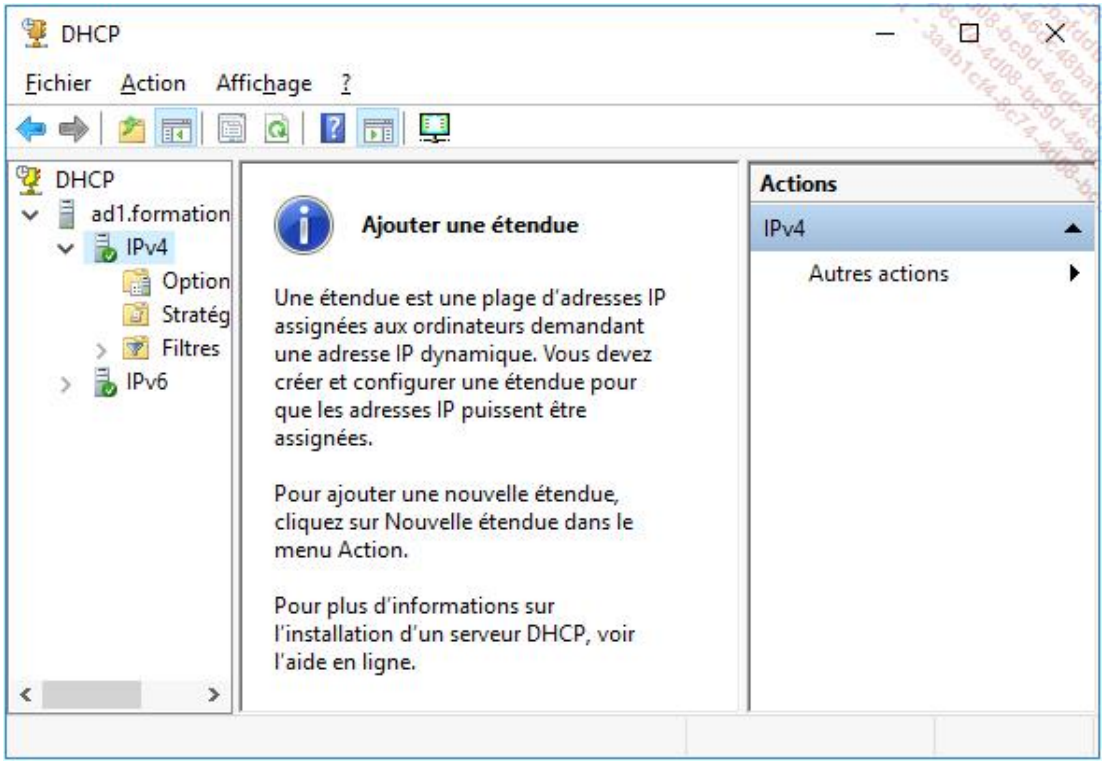
La plage d'adresses IP distribuables par l'étendue est nécessairement contiguë. Pour éviter la distribution de certaines adresses, il est possible de mettre en place des exclusions d'une adresse ou d'une plage contiguë. Ces dernières peuvent être assignées à un poste de façon manuelle sans risquer un conflit d'IP puisque le serveur ne distribuera pas ces adresses.

Utilisation de la règle 80/20 pour les étendues

Il est possible d'avoir deux serveurs DHCP actifs sur le réseau en découpant le pool d'adresses en deux. La règle du 80/20 permet dans un premier temps d'équilibrer l'utilisation des serveurs DHCP mais surtout de pouvoir avoir deux serveurs sans risque de conflit IP. Le serveur 1 distribue 80 % du pool d'adresses alors que le serveur 2 est configuré pour distribuer les adresses restantes (20 %). Ces pourcentages sont évidemment des cas généraux et peuvent être changés afin de répondre à votre besoin.

Configuration de l'étendue

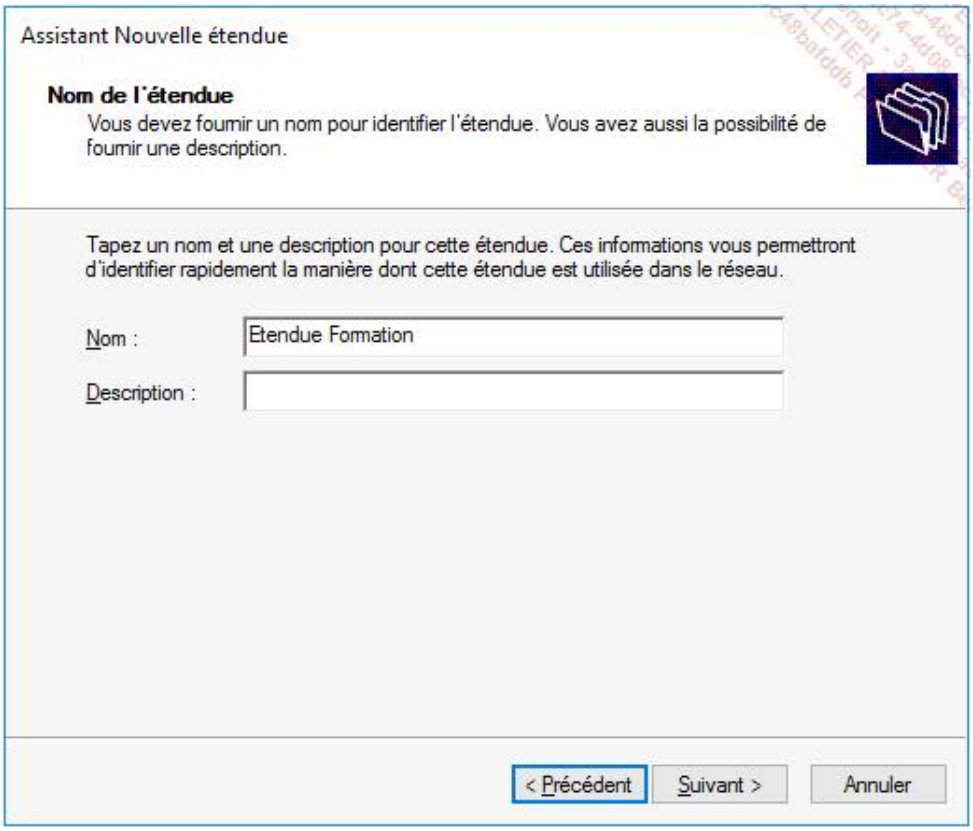
- Développez les nœuds **ad1.formation.local** puis **IPv4**.



- Effectuez un clic droit sur **IPv4** puis sélectionnez **Nouvelle étendue**.

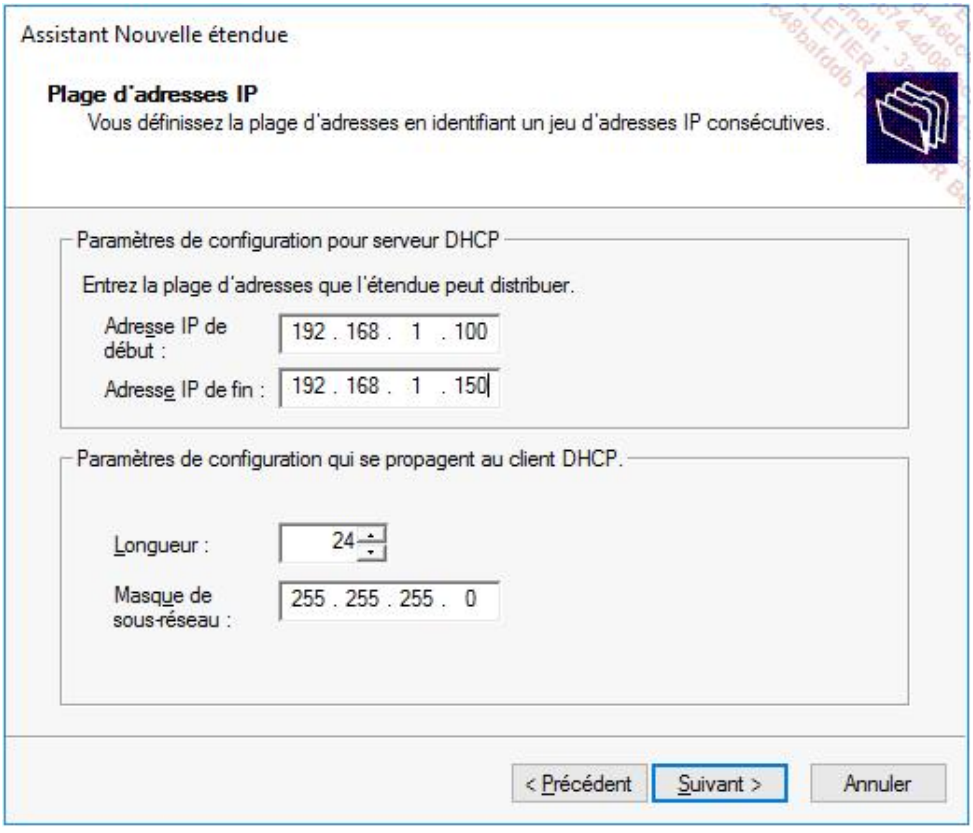
  L'assistant de création de la nouvelle étendue se lance.

- Saisissez **Etendue Formation** dans le champ **Nom**.



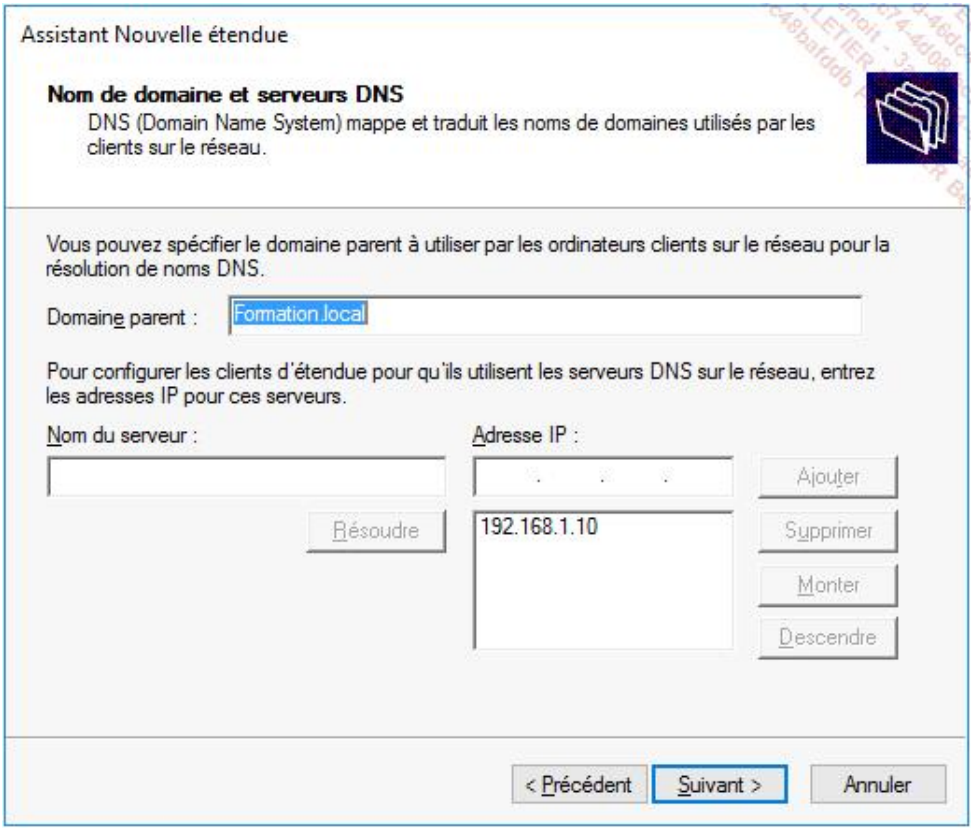
La plage d'adresses distribuable va de 192.168.1.100 à 192.168.1.150.

- Saisissez **192.168.1.100** dans **Adresse IP de début** et **192.168.1.150** dans **Adresse IP de fin**.



- Dans la fenêtre des exclusions, cliquez sur **Suivant**.

- Laissez la **Durée de bail** par défaut.
- Dans la fenêtre **Configuration des paramètres DHCP**, cliquez sur **Suivant**.
- Laissez le champ **Routeur** vide et cliquez sur **Suivant**.
- Si ce n'est pas déjà configuré, saisissez l'**Adresse IP** du serveur DNS (**192.168.1.10**) puis cliquez sur **Ajouter**.



- Dans la fenêtre des **Serveurs Wins**, cliquez sur **Suivant**.
- L'étendue est activée à la fin de l'assistant, laissez le choix par défaut.
- Cliquez sur **Terminer** pour fermer l'assistant.

2. Configuration des options dans le DHCP

Les options permettent de distribuer des « paramètres » supplémentaires dans le bail, tels que le nom de domaine DNS et l'adresse du serveur DNS. Trois types d'options existent :

- les options serveur,
- les options de l'étendue,
- les options de réservation.

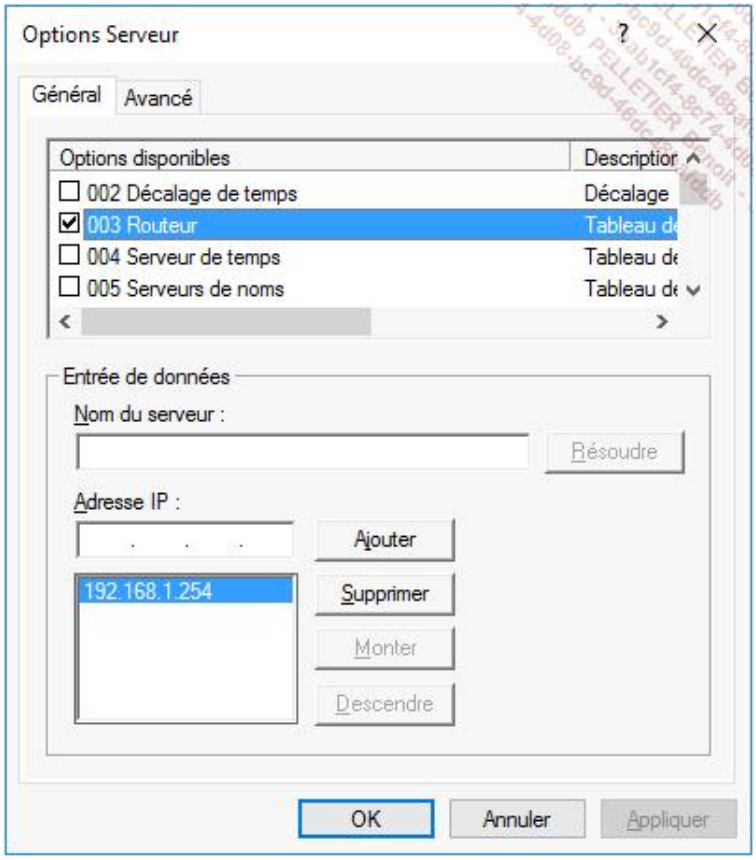
Les options serveur

Elles s'appliquent à toutes les étendues du serveur ainsi qu'aux réservations. **Si la même option est configurée dans les options d'étendue, c'est cette dernière qui l'emporte, l'option serveur est donc ignorée**.

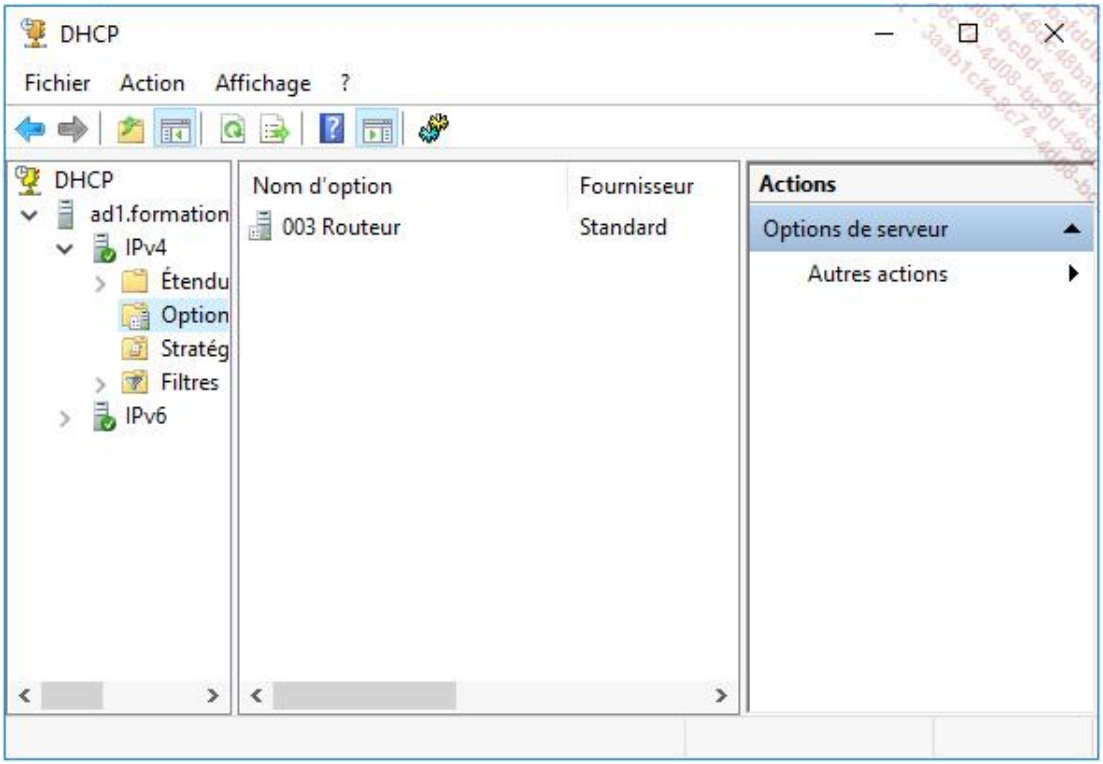
- Dans la console DHCP, effectuez un clic droit sur **Options de serveurs** puis cliquez sur **Configurer les**

options.

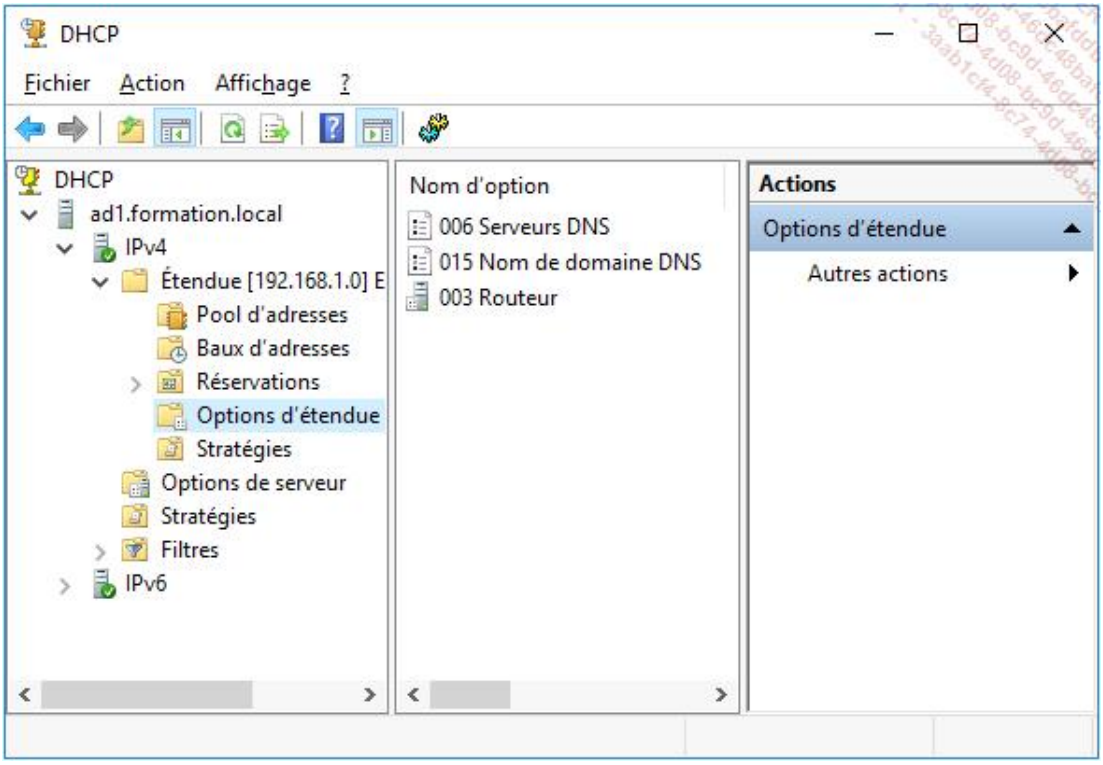
- Cochez la case **003 Routeur** et saisissez **192.168.1.254** dans le champ **Addresse IP**.
- Cliquez sur **Ajouter** puis sur **OK** pour créer l'option.



L'option est bien présente dans la console DHCP.



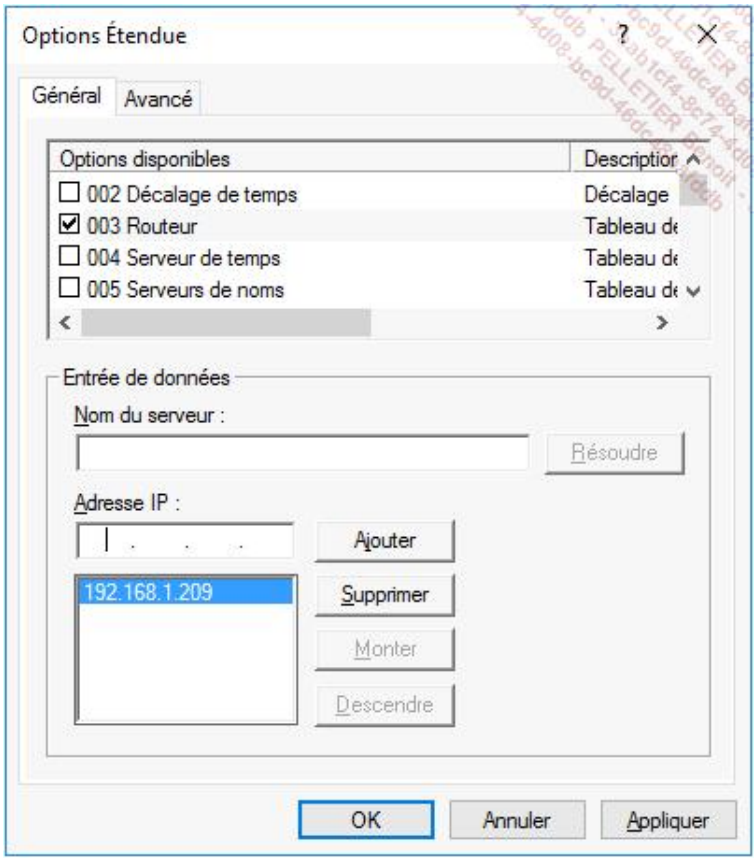
Les options apparaissent également dans les **Options d'étendue** et dans les options de **Réservations**.



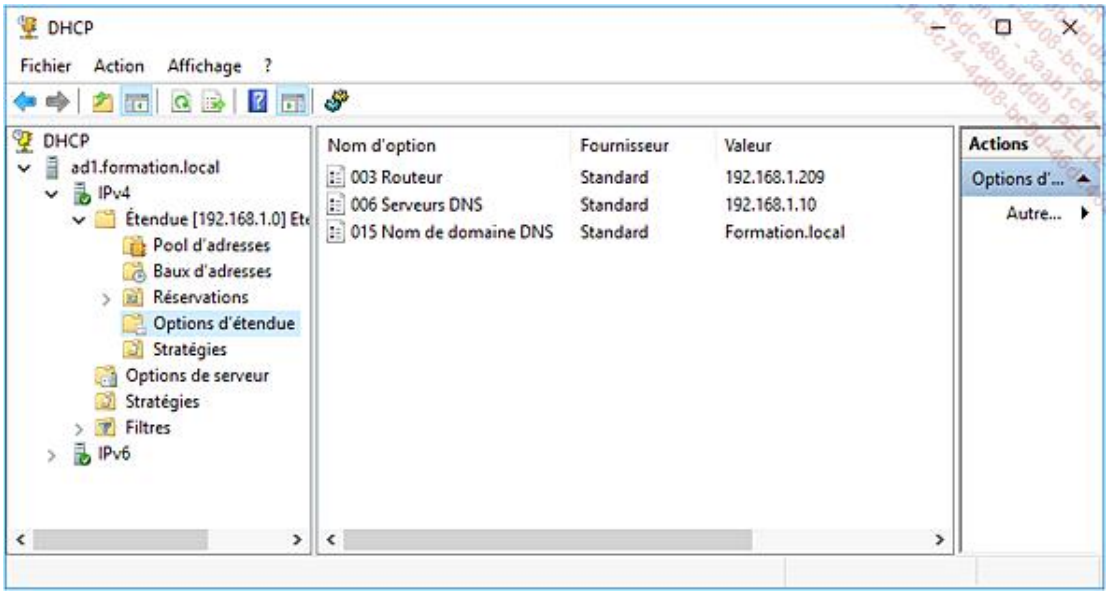
Les options de l'étendue

Elles s'appliquent uniquement à l'étendue concernée. Si le serveur possède plusieurs étendues, chacune possède ses options, pouvant être différentes d'une étendue à l'autre.

- Dans la console DHCP, effectuez un clic droit sur **Options d'étendue** puis cliquez sur **Configurer les options**.
- Cochez la case **003 Routeur** et saisissez **192.168.1.209** dans le champ **Adresse IP**.



Cliquez sur **Ajouter** puis sur **OK** pour créer l'option.



L'option d'étendue est bien prioritaire sur celles du serveur. L'option **Routeur** a donc bien été remplacée.

Les options de réservation

Elles s'appliquent uniquement aux réservations. Chaque réservation peut avoir des options différentes.

Les réservations sont étudiées après l'étude des options DHCP.

3. Réservation de bail DHCP

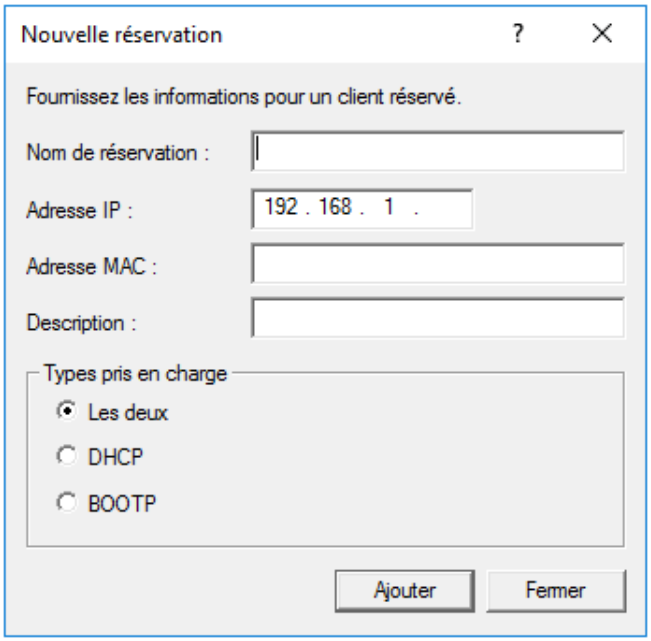
Les **réservations DHCP** permettent de s'assurer qu'un client configuré pour recevoir un bail DHCP aura systématiquement la même configuration ; très utile pour les imprimantes réseau que l'on souhaite garder en adressage dynamique.

La création d'une réservation nécessite la saisie de plusieurs informations :

- **Le nom de la réservation** : ce champ contient généralement le nom du poste ou de l'imprimante concerné par cette réservation.
- **L'adresse IP** : indique l'adresse qui doit être distribuée au client.
- **L'adresse MAC** : adresse MAC de l'interface réseau qui fait la demande.

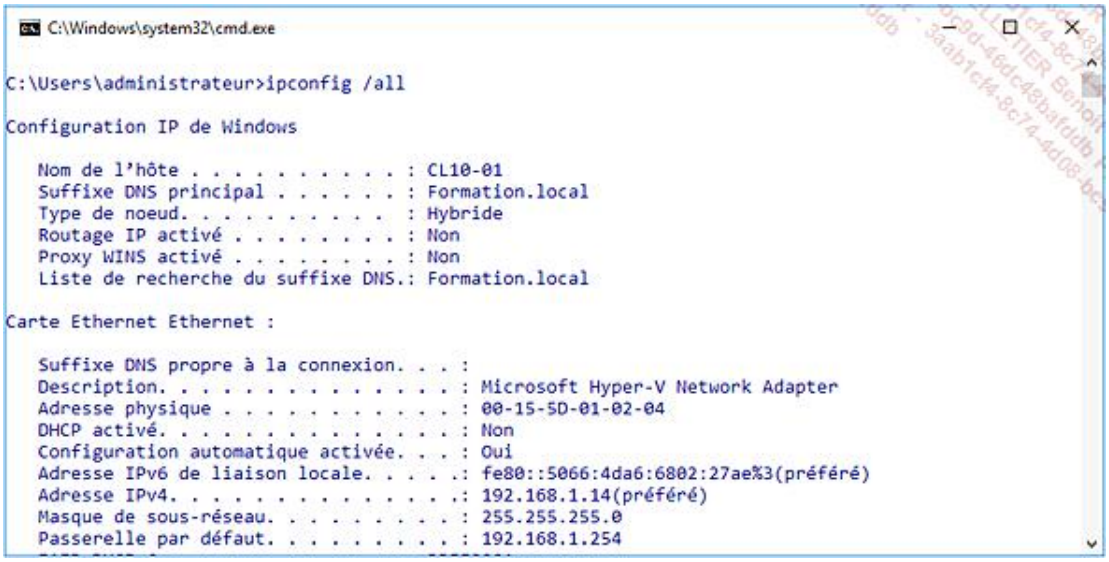
Si un poste possède deux interfaces réseau, il est impossible d'appliquer la même réservation aux deux interfaces.

Dans la console DHCP, effectuez un clic droit sur **Réservations** puis sélectionnez **Nouvelle réservation**.

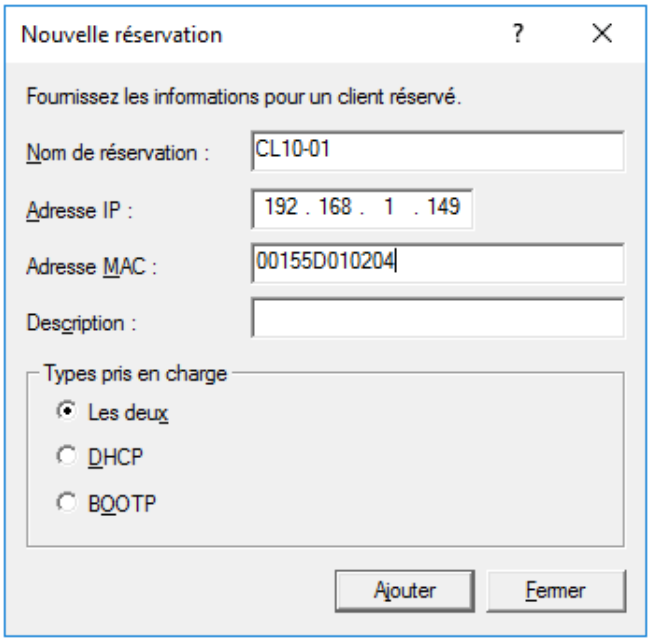


Configurez la fenêtre **Nouvelle réservation** comme ci-dessous :

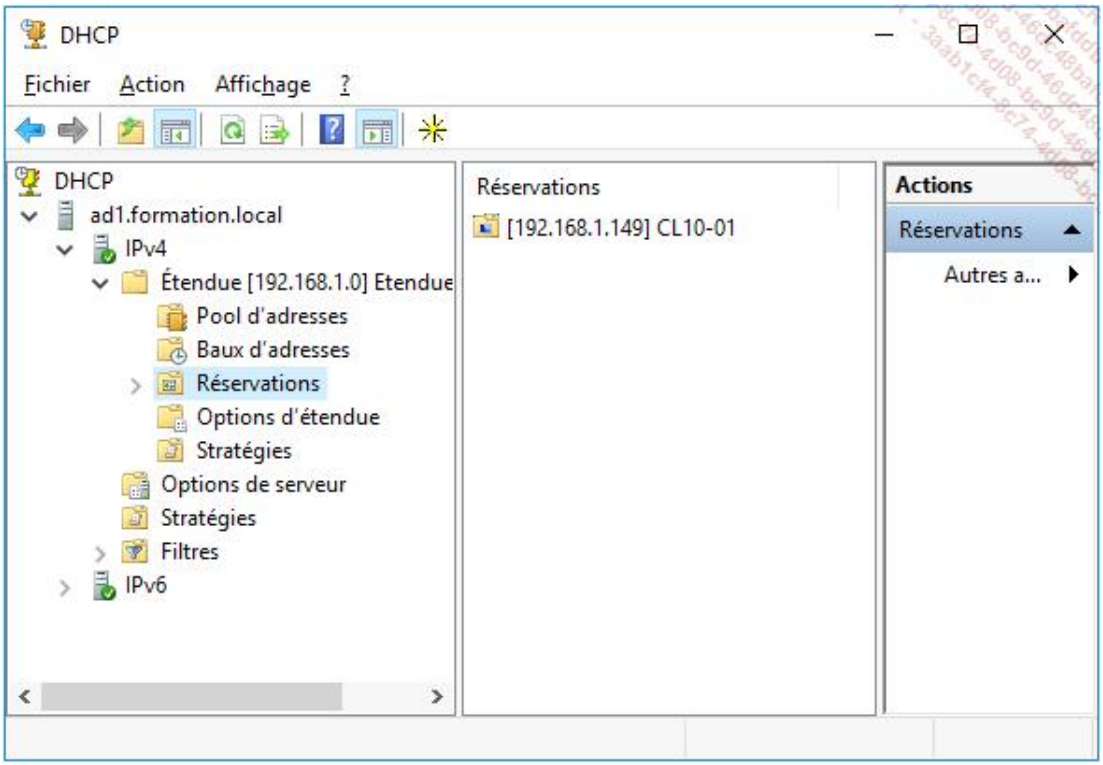
- **Nom de la réservation** : CL10-01
- **Adresse IP** : 192.168.1.149
- **Adresse MAC** : saisissez l'adresse MAC de la machine **CL10-01** (commande `ipconfig /all` à effectuer sur le poste client).



La description est un champ facultatif. Elle permet d'ajouter une indication supplémentaire.



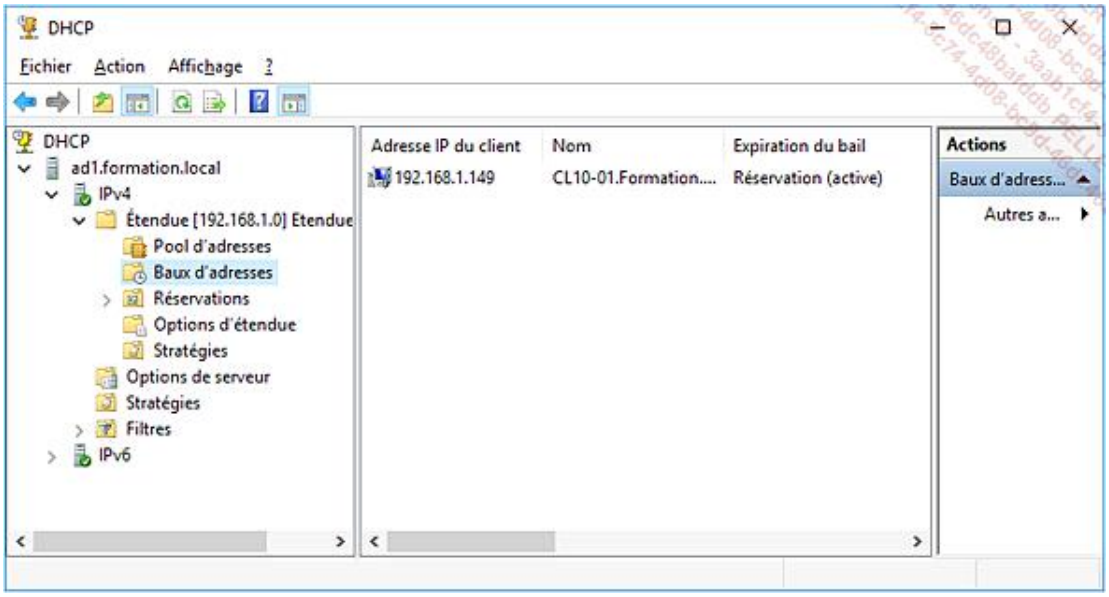
Cliquez sur **OK** pour valider la nouvelle réservation.



Sur le poste client, saisissez dans une invite de commandes DOS la commande `ipconfig /release` (pour libérer le bail), puis `ipconfig /renew` (pour effectuer une demande de configuration IP au serveur).

L'adresse IP est bien celle réservée.

La réservation apparaît en tant qu'**active** dans la console DHCP.



La réservation est maintenant en place. Depuis plusieurs années, il est possible d'implémenter des filtres dans le service DHCP.

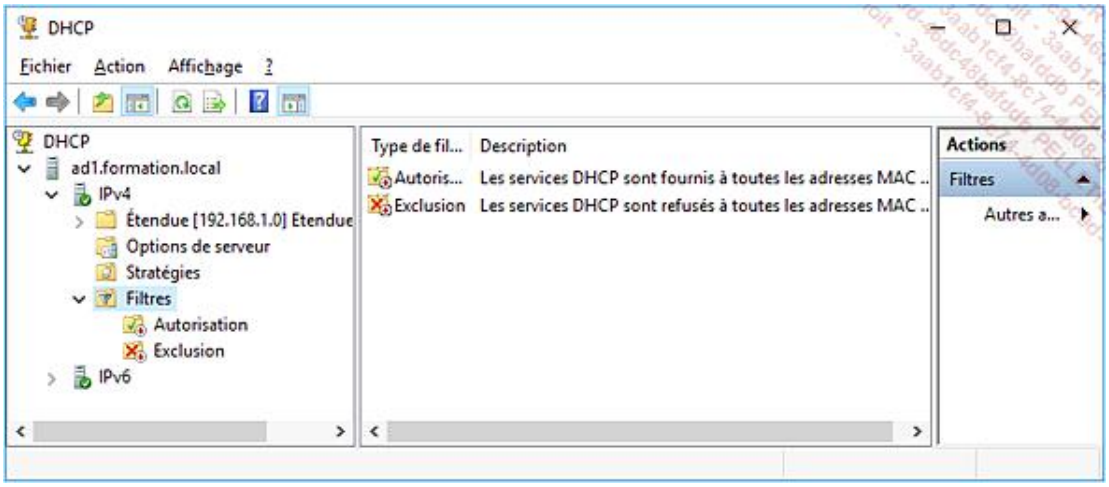
4. Mise en place des filtres

Les filtres permettent de créer des **listes vertes** et des **listes d'exclusion**. La liste verte permet à toutes les interfaces réseau dont les adresses MAC sont listées d'obtenir un bail DHCP. Elle est représentée par le dossier **Autorisation** dans le nœud **Filtres**. La liste d'exclusion, contrairement à la liste verte, interdit l'accès au service à toutes les adresses MAC référencées. Elle est représentée par le dossier **Exclusion**.

Cette fonctionnalité alourdit les tâches d'administration car il est nécessaire de saisir l'adresse MAC d'une nouvelle machine pour qu'elle puisse recevoir un bail.

Il est recommandé de créer les filtres avant d'activer la fonctionnalité. Dans le cas contraire, plus aucune machine de votre réseau ne pourra demander de bail.

Les filtres doivent être activés sur les deux serveurs dans le cas où la fonctionnalité de basculement est configurée.



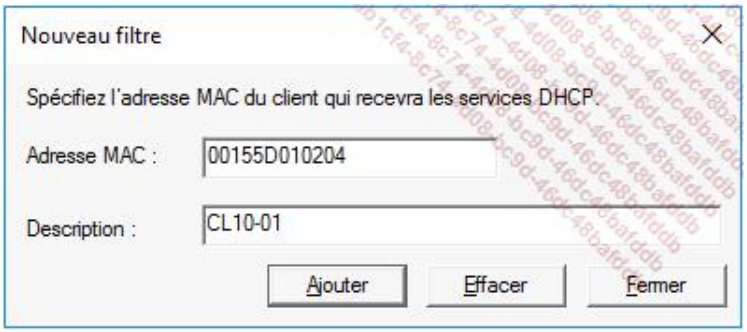
Par défaut, les deux listes sont désactivées.

- Effectuez un clic droit sur la liste **Autorisation** puis sélectionnez **Activer**. Recommencez la même opération pour **Exclusion**.
- Sur le poste client, libérez le bail (`ipconfig /release`) puis demandez-en un nouveau (commande `ipconfig /renew`).

Une erreur apparaît sur le poste, le serveur DHCP n'ayant pas répondu.



- Effectuez un clic droit sur **Autorisation** puis sélectionnez **Nouveau filtre**.
- Saisissez l'**Adresse MAC** de CL10-01 ainsi qu'une **Description**.



- Cliquez sur **Ajouter** pour valider le filtre.
- Sur CL10-01, relancez la demande d'un bail (`ipconfig /renew`).

  La demande est acceptée et le poste reçoit une configuration.



- Dans le dossier **Autoriser**, effectuez un clic droit sur le filtre qui vient d'être créé puis sélectionnez **Déplacer vers la liste d'exclusion**.

La même manipulation peut être effectuée pour déplacer un filtre de la liste d'exclusion vers la liste verte.

- Recommencez l'étape de libération/demande d'un nouveau bail sur le poste CL10-01.

Comme tout à l'heure, le serveur ne répond plus à la machine.



- Effectuez un clic droit sur le nœud **Autoriser** puis sélectionnez **Désactiver**. Recommencez la même opération pour le nœud **Exclusion**.

Base de données du service DHCP

1. Introduction

La base de données utilisée par le service DHCP peut stocker un nombre important d'enregistrements et le nombre de clients DHCP va influer sur la taille de la base.

Cette dernière fonctionne avec un moteur Exchange Server JET. Lors de l'installation du rôle, les fichiers ci-dessous nécessaires au fonctionnement du service sont stockés dans **Windows\System32\Dhcp**.

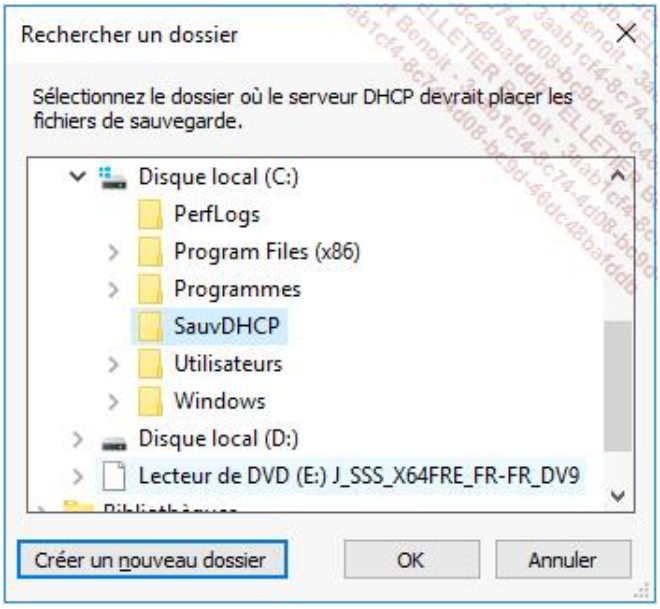
- **Dhcp.mdb** : base de données du service DHCP.
- **J50.log** : permet la journalisation des transactions.

Lors de l'attribution d'un bail, la base de données est mise à jour et une entrée est inscrite dans la base de registre.

2. Sauvegarde et restauration de la base de données

Les logiciels de sauvegarde du marché ont la possibilité de sauvegarder et de restaurer la base de données du service DHCP. Néanmoins, il est possible d'effectuer cette opération à la main.

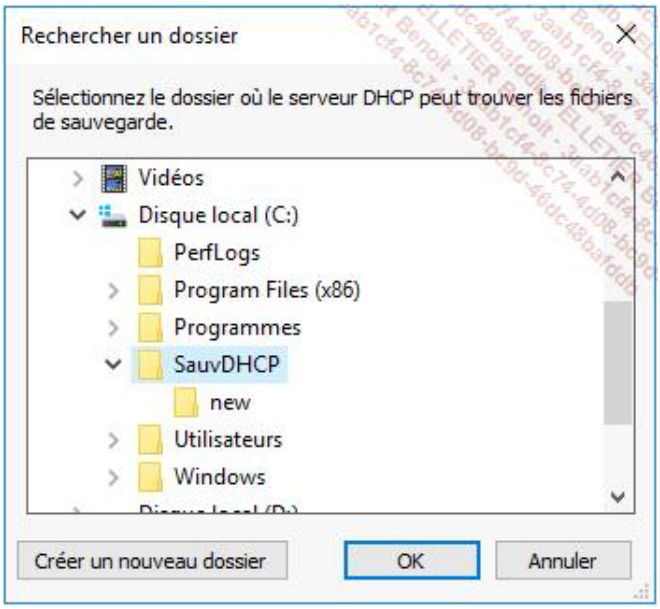
- Dans la console DHCP, effectuez un clic droit sur le serveur puis sélectionnez **Sauvegarder**.
- Créez un nouveau dossier appelé **SauvDHCP** dans **C:**.



- Ensuite, cliquez sur l'étendue présente dans le serveur DHCP et sélectionnez **Supprimer**.
- Validez les messages d'avertissement en cliquant deux fois sur **Oui**.

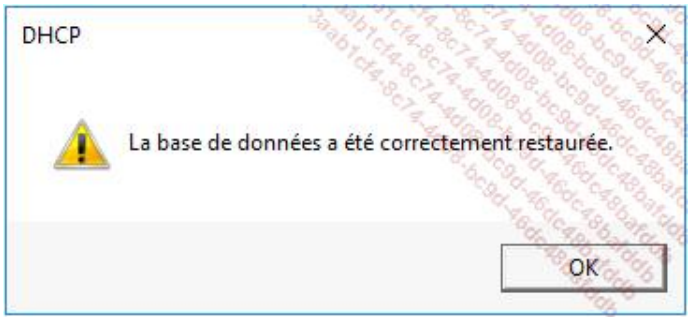
Il va maintenant être nécessaire d'effectuer une restauration.

- Dans la console DHCP, effectuez un clic droit sur le serveur puis sélectionnez **Restaurer**.
- Sélectionnez le répertoire créé pendant la sauvegarde puis cliquez sur **OK**.



Un message vous avertit que le service doit être redémarré. Cliquez sur **Oui**.

Le service est arrêté puis redémarré et un message vous avertit du bon fonctionnement de la restauration.



Vérifiez la présence de toutes les configurations (baux distribués, réservation…).

Haute disponibilité du service DHCP

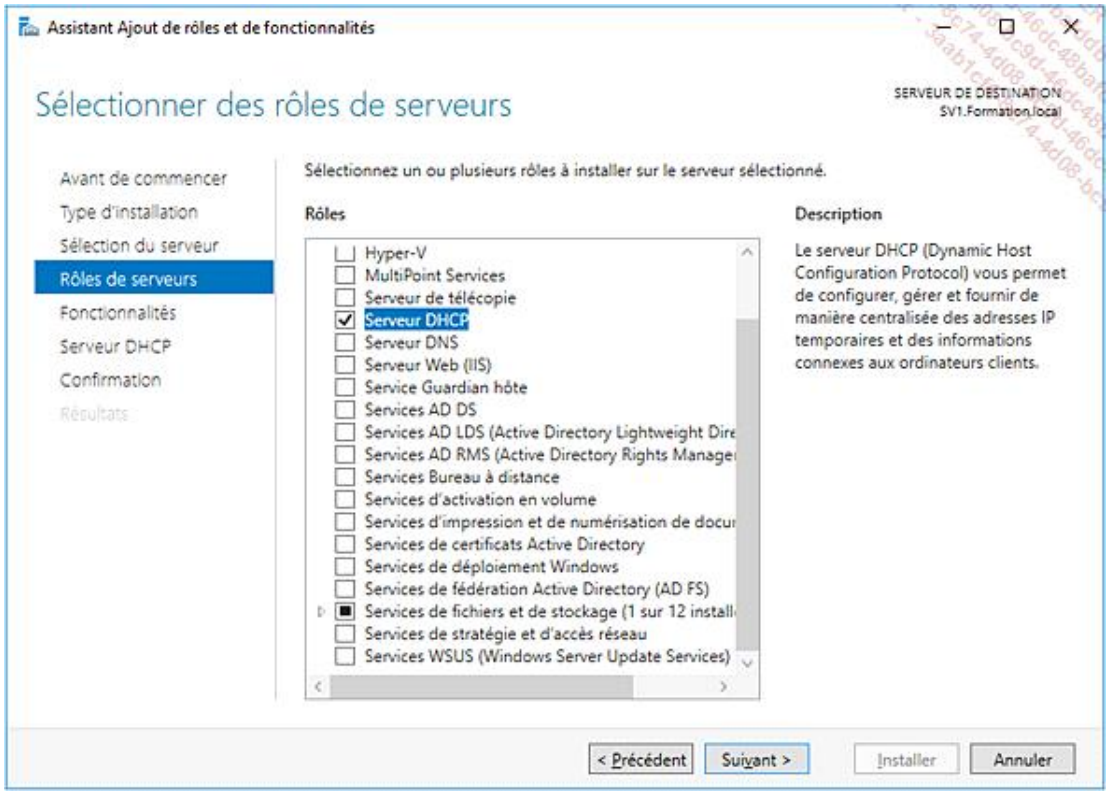
Le service DHCP est un service important dans un réseau informatique. En cas d'arrêt du service, plus aucun bail n'est attribué et les machines vont au fur et à mesure perdre l'accès au réseau. Pour éviter cela, il est possible d'installer un deuxième serveur DHCP et de partager la plage distribuée (généralement 80 % pour le premier serveur et 20 % pour l'autre). La deuxième solution consiste à installer un **cluster DHCP**, solution efficace mais qui nécessite quelques compétences.

Depuis Windows Server 2012, il est possible de faire travailler deux serveurs DHCP sans avoir à monter un cluster. Si un des serveurs n'est plus en ligne, les machines clientes peuvent continuer à recevoir des baux DHCP.

Lors de la configuration du mode équilibrage de charge, un découpage de la plage d'adresse est effectué en fonction du pourcentage configuré par l'administrateur. Chacun à la responsabilité de la partie de l'étendue qu'il gère. L'administration s'effectue par l'intermédiaire d'un des deux serveurs. Attention les réservations doivent être créées sur les deux serveurs.

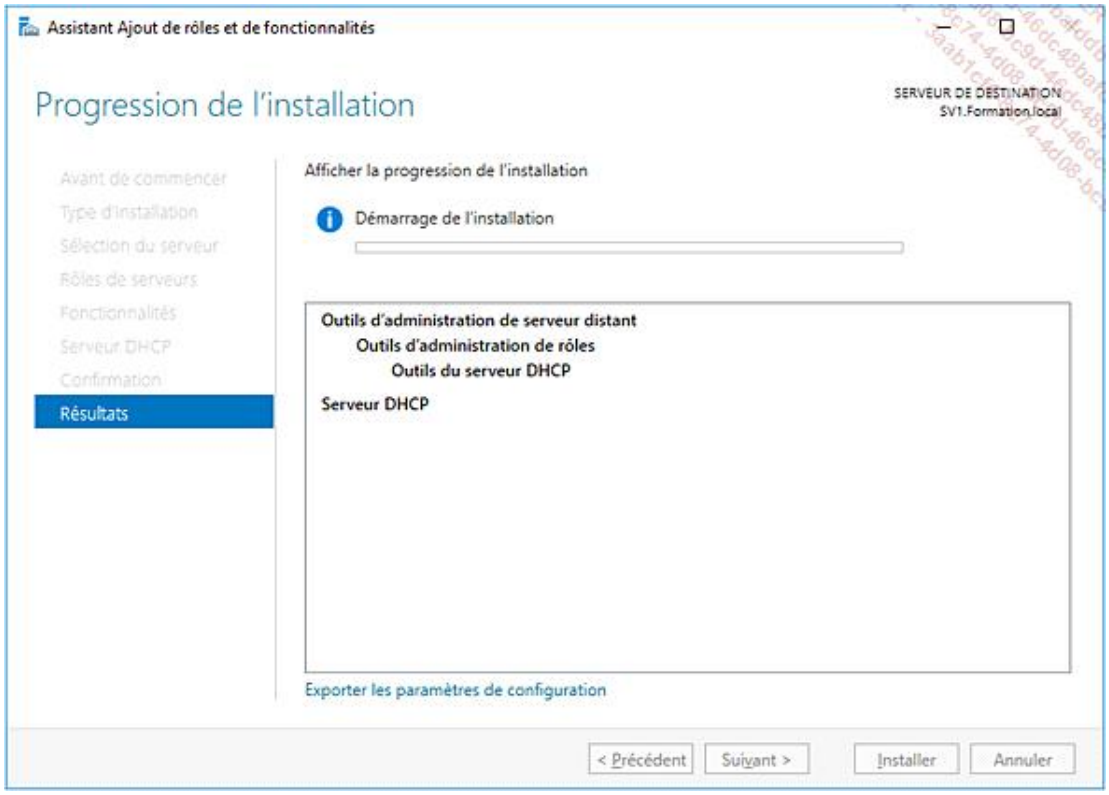
Le basculement DHCP ne peut contenir que deux serveurs. De plus, il peut être activé uniquement pour les étendues IPv4.

- Sur SV1, lancez la console **Gestionnaire de serveur** puis cliquez sur **Ajouter des rôles et des fonctionnalités**.
- Dans la fenêtre **Avant de commencer**, cliquez sur **Suivant**.
- Laissez le choix par défaut dans la fenêtre **Sélectionner le type d'installation** puis cliquez sur **Suivant**.
- Le serveur de destination est **SV1.formation.local**. Cliquez sur **Suivant**.
- Cochez la case **Serveur DHCP** puis cliquez sur le bouton **Ajouter des fonctionnalités** présent dans la fenêtre qui s'affiche.



- Cliquez trois fois sur **Suivant** puis sur **Installer**.

L'installation est en cours…



- À la fin de l'installation, cliquez sur **Fermer**.
- Dans la console **Gestionnaire de serveur**, cliquez sur le drapeau (zone de notification) puis sur **Terminer la configuration DHCP**.
- Cliquez sur **Suivant** dans la fenêtre **Description** puis sur **Valider** dans **Autorisation**.

La machine doit être membre du domaine, procédez à la jonction si ce n'est pas le cas et relancez l'étape d'Autorisation.

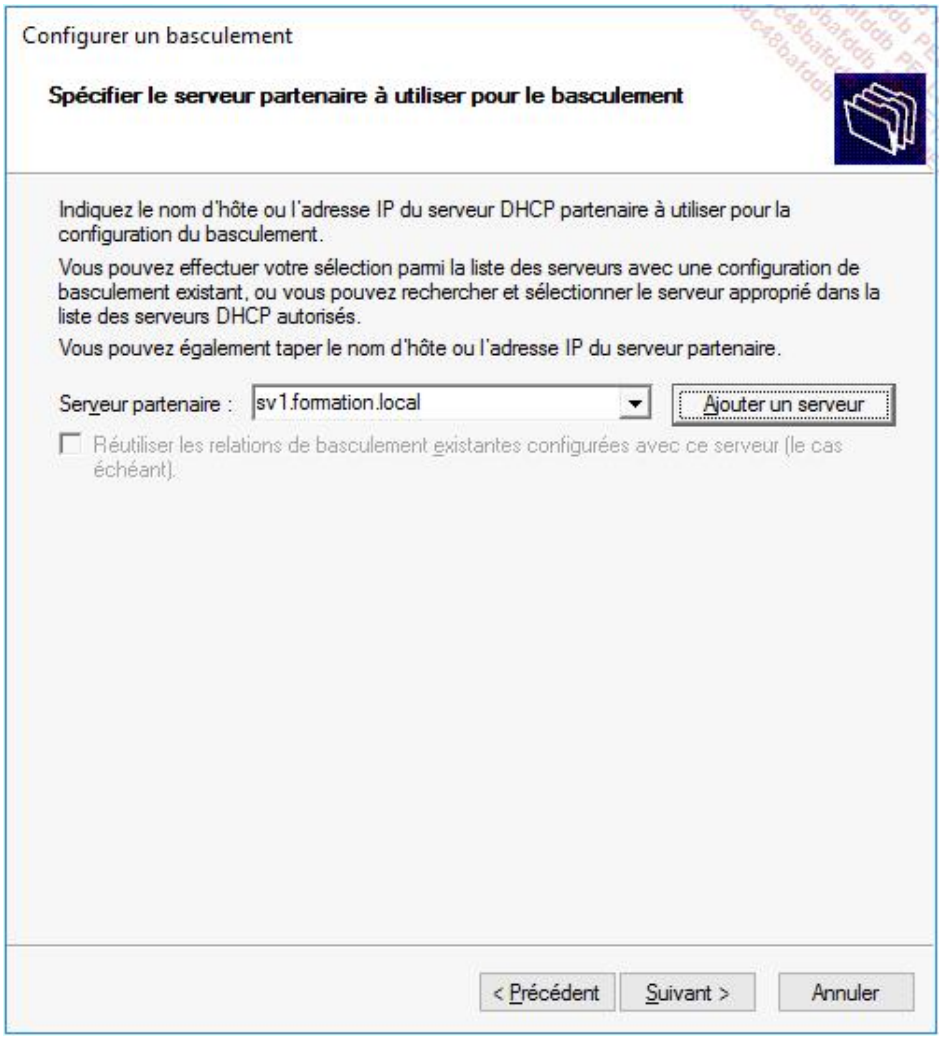
- Cliquez sur **Fermer**.
- Dans le menu Démarrer, cliquez sur **Outils d'administration** puis sur **DHCP**.
- Double cliquez sur **SV1.formation.local** puis sur **IPv4**.

Aucune étendue n'est présente.

- Sur AD1, ouvrez la console DHCP.
- Double cliquez sur **ad1.formation.local** puis sur **IPv4**.
- Effectuez un clic droit sur **IPv4** puis cliquez sur **Configurer un basculement**.
- Une seule étendue est présente dans le DHCP, cliquez sur **Suivant** dans la fenêtre **Introduction au basculement DHCP**.

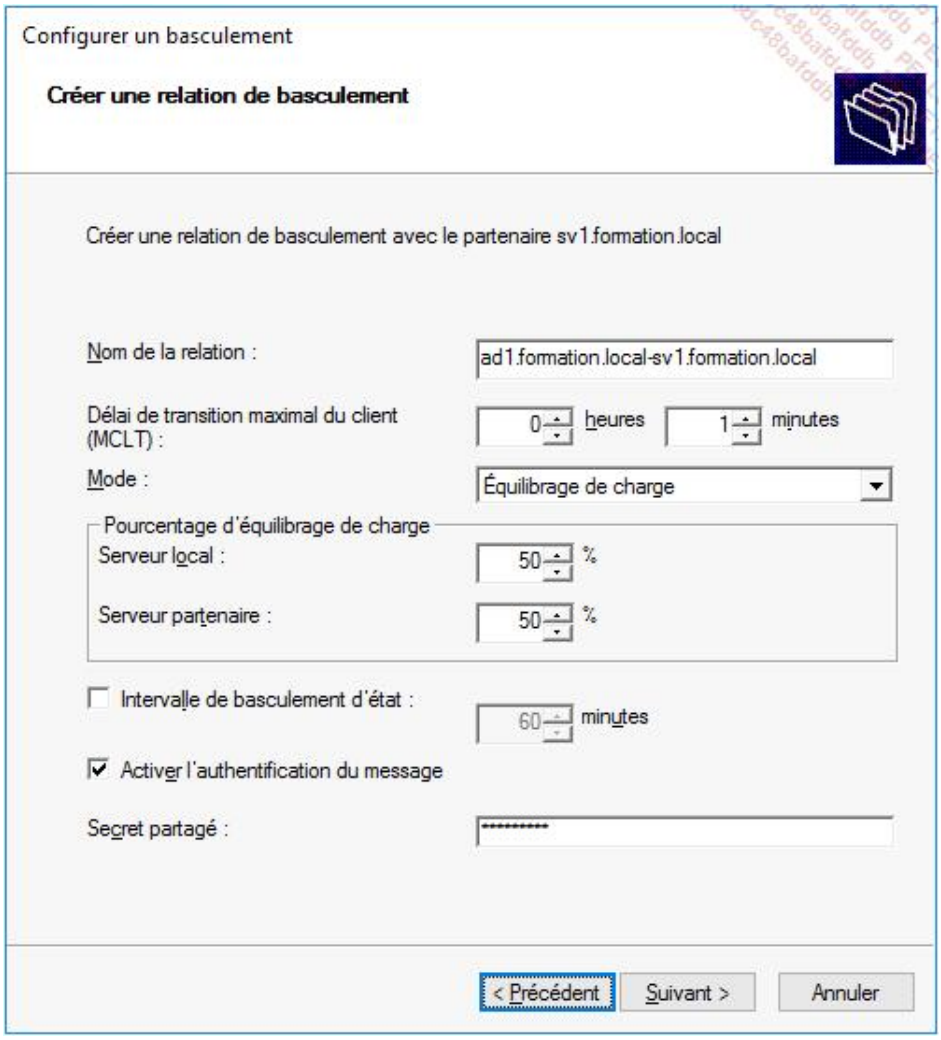


- Dans la fenêtre **Spécifier le partenaire**, cliquez sur **Ajouter un serveur**.
- Sélectionnez **sv1.formation.local** puis cliquez sur **OK**.
- Cliquez sur **Suivant** pour valider le partenaire.

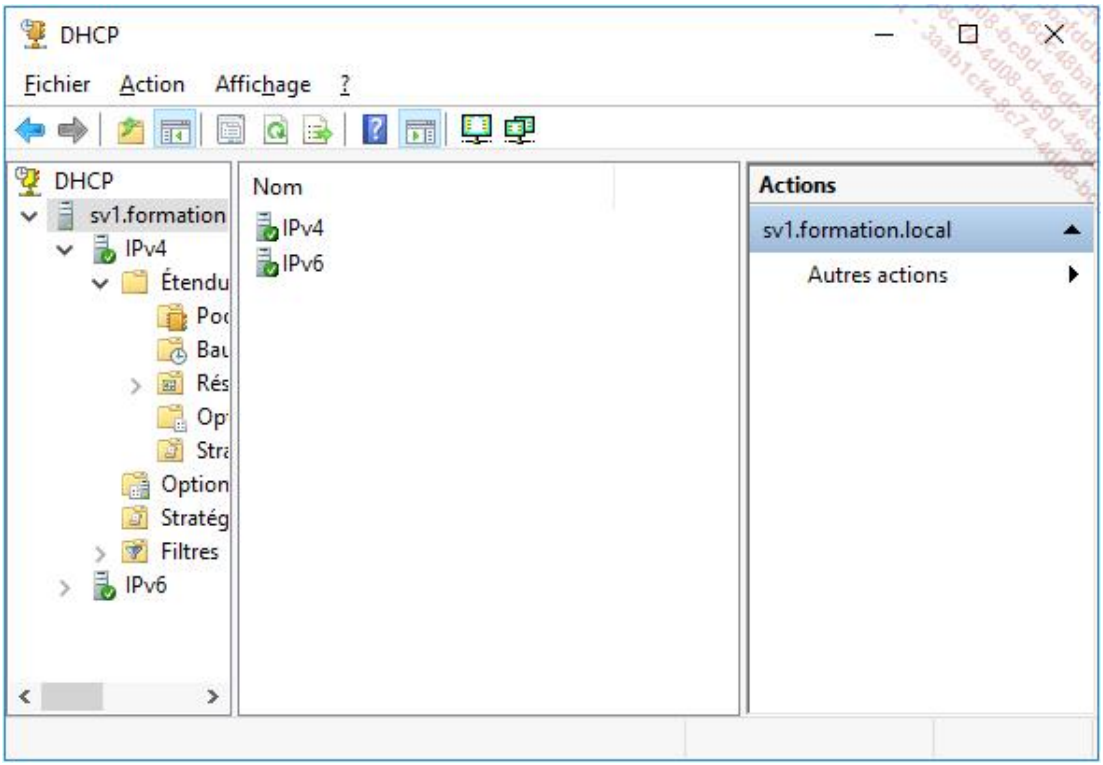


- Saisissez **P@rtDHCP** dans le champ **Secret partagé**.
- Modifiez la valeur du champ **Délai de transition maximale du client** pour afficher 1 minute.

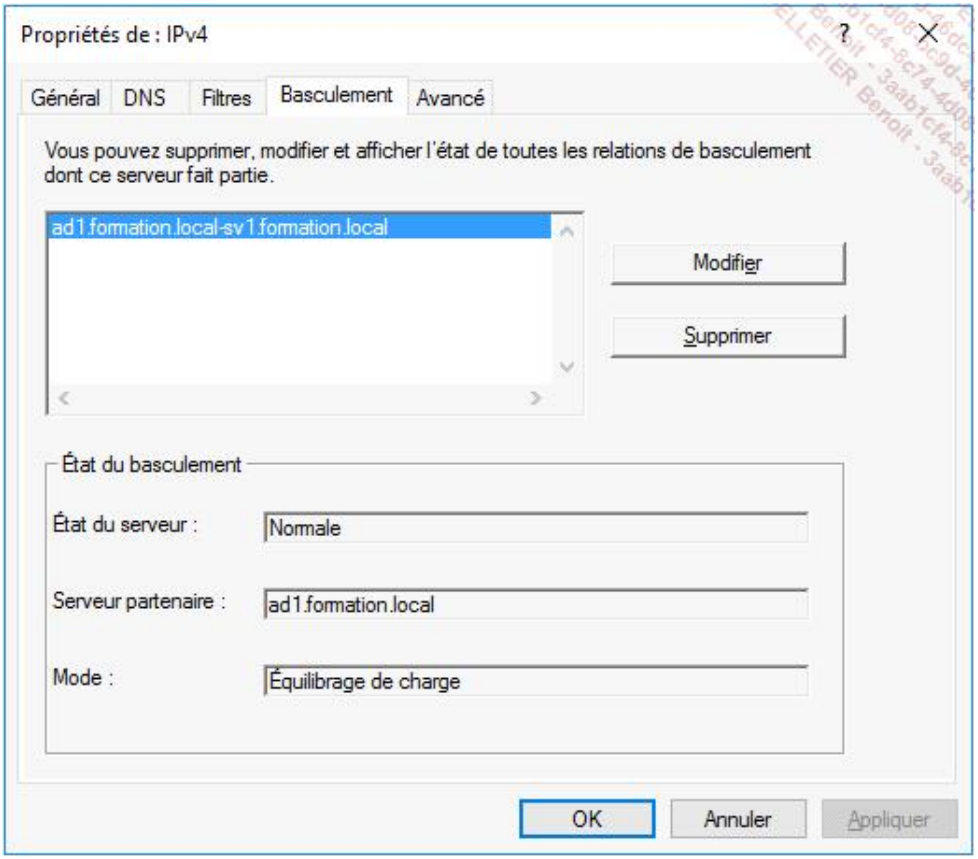
Ce champ spécifie la durée pendant laquelle le serveur DHCP doit attendre, si son partenaire est hors ligne, pour prendre le contrôle de la plage d'adresses IP. La valeur par défaut est de 1 heure.



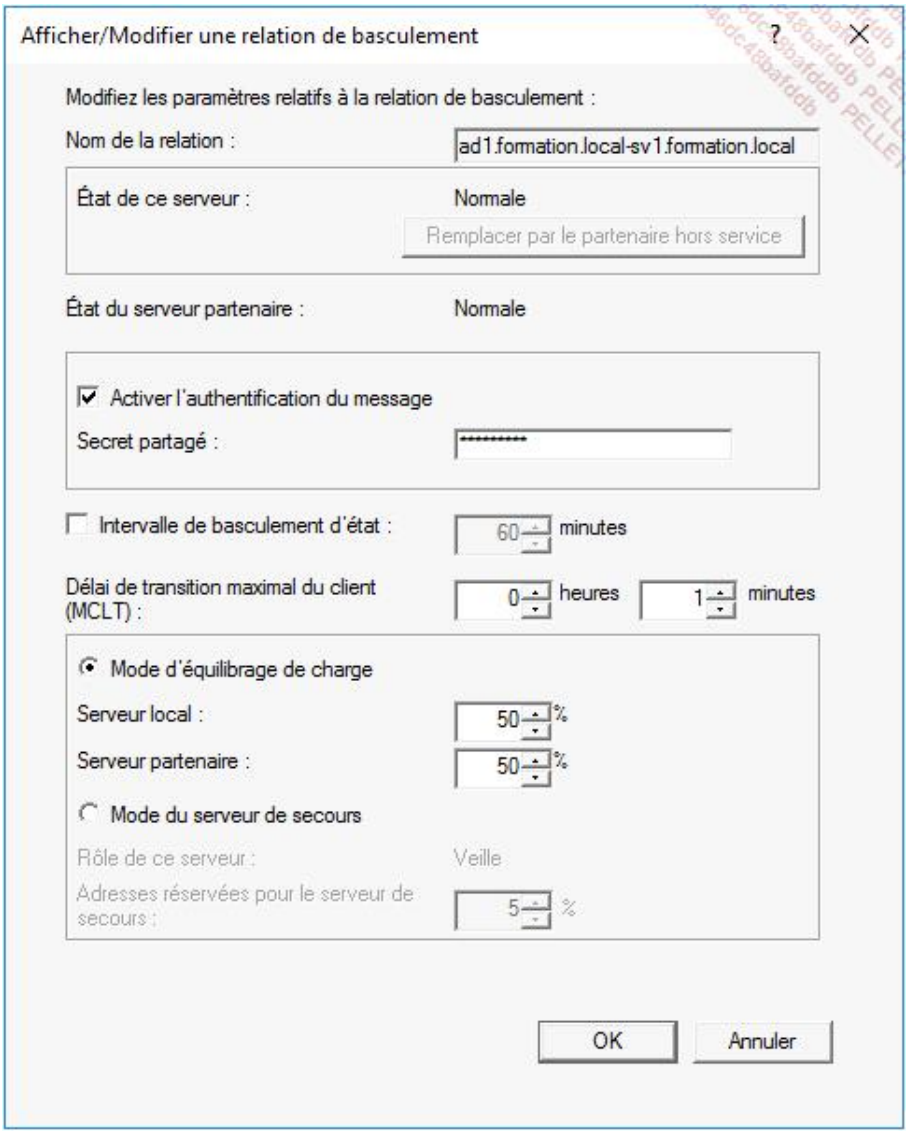
- Cliquez sur **Suivant** puis sur **Terminer**.
- Vérifiez que les étapes ont bien l'état **Réussite** puis cliquez sur **Fermer**.
- Sur SV1, accédez à la console DHCP. L'étendue est maintenant présente.



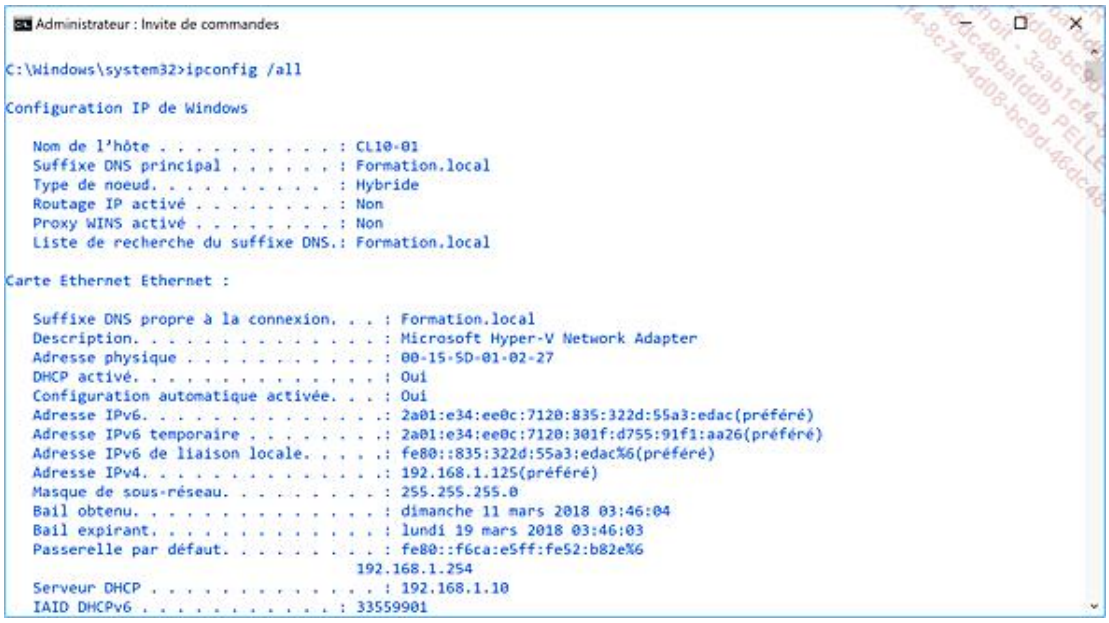
- Effectuez un clic droit sur **IPv4** puis sélectionnez **Propriétés**.
- Sélectionnez l'onglet **Basculement**.



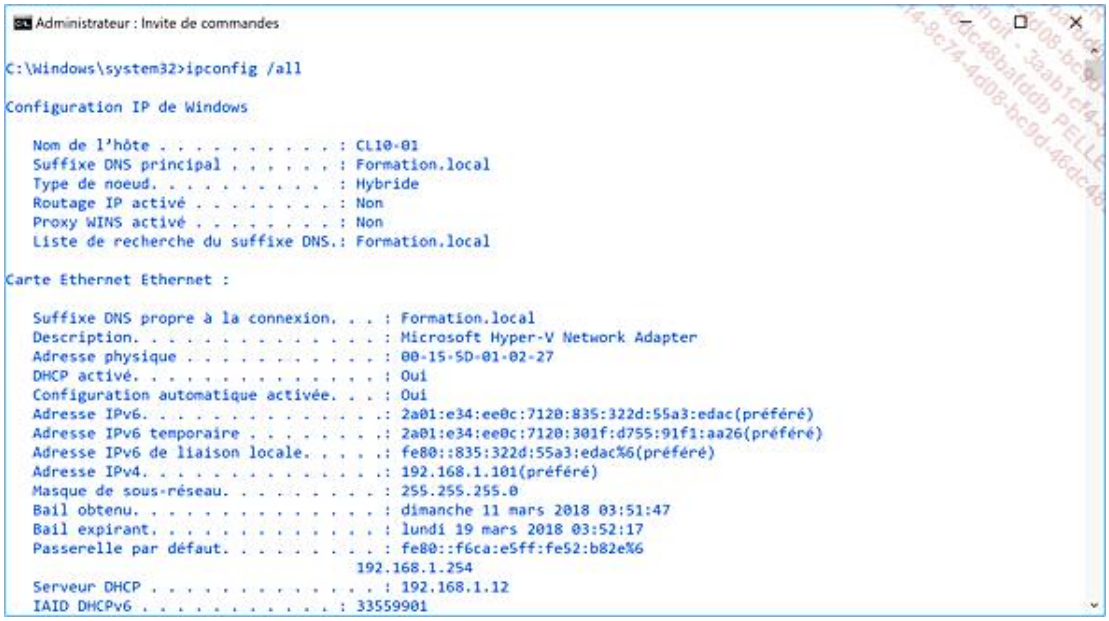
- Cliquez sur **Modifier** pour visualiser les propriétés qui sont modifiables.



- Modifiez le champ **Serveur partenaire** afin qu'il soit égal à 0.
- Effectuez un `ipconfig /all` sur CL10-01. Le serveur DHCP qui a attribué l'adresse est **AD1**.



- Saisissez `ipconfig /release` et appuyez sur la touche [Entrée] du clavier puis `ipconfig /renew` dans l'invite de commandes DOS et appuyez sur la touche [Entrée].
- Utilisez la commande `ipconfig /all` pour visualiser la nouvelle configuration.

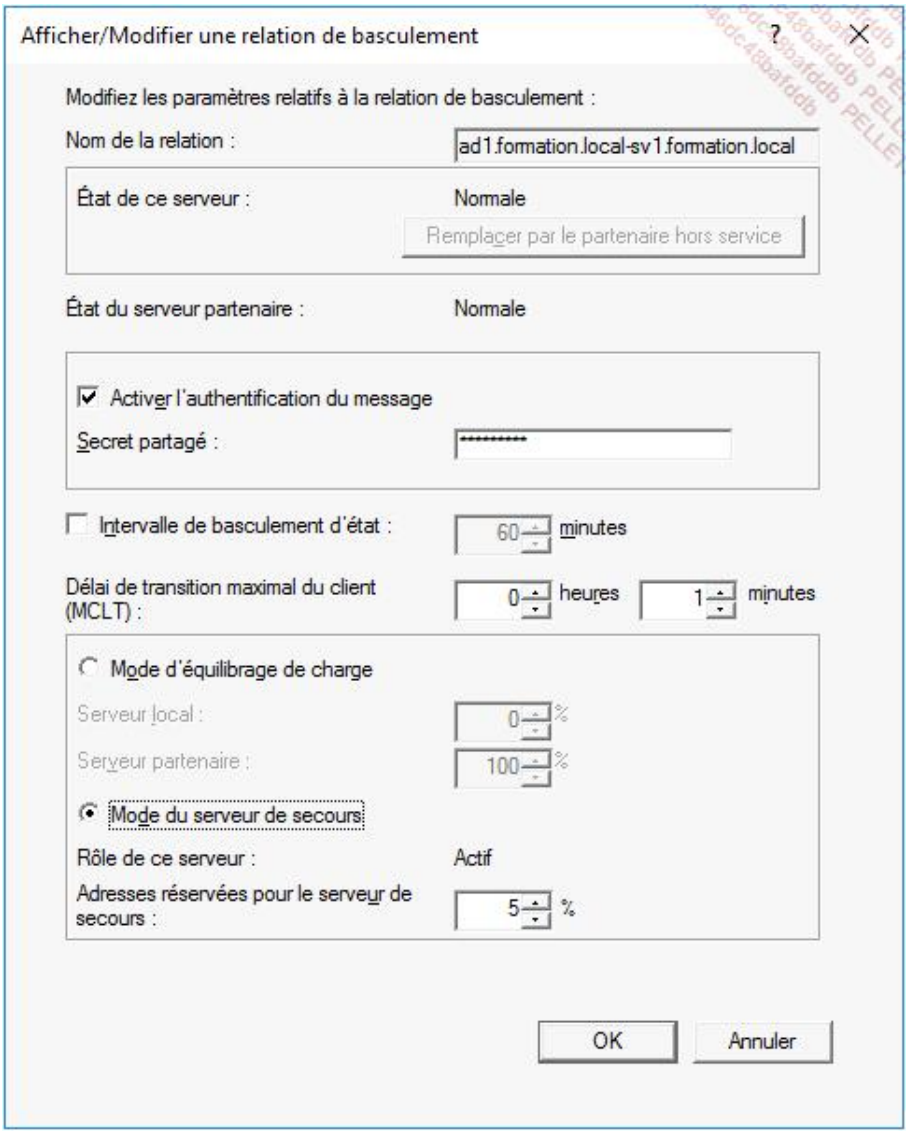


Le serveur DHCP qui a distribué l'adresse est bien **SV1**.

Le basculement peut également être utilisé en mode **Serveur de secours**.

- Sur AD1, effectuez un clic droit sur **IPv4** puis sélectionnez **Propriétés**.
- Sélectionnez **Basculement** puis cliquez sur **Modifier**.
- Cochez **Mode du serveur de secours** puis cliquez sur **OK**.

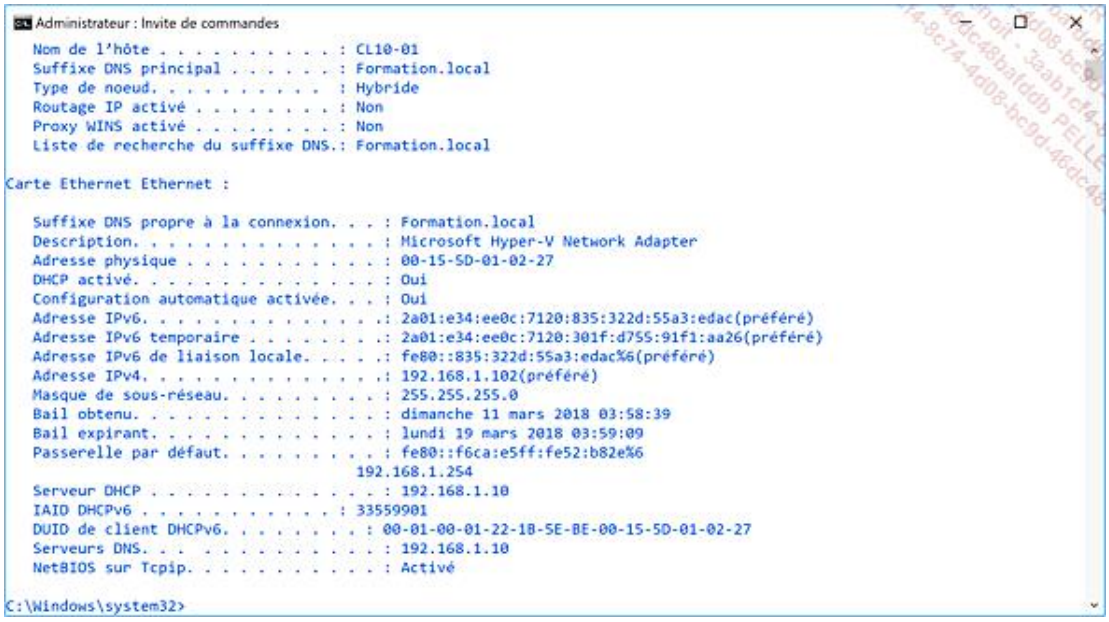
Le mode d'équilibrage de charge permet d'équilibrer les demandes en fonction du pourcentage configuré. Il permet de s'assurer que la charge de travail des serveurs est « égale » pour tous. Le mode du serveur de secours assure lui une haute disponibilité. En cas de crash d'un serveur, le serveur partenaire prend le relais.



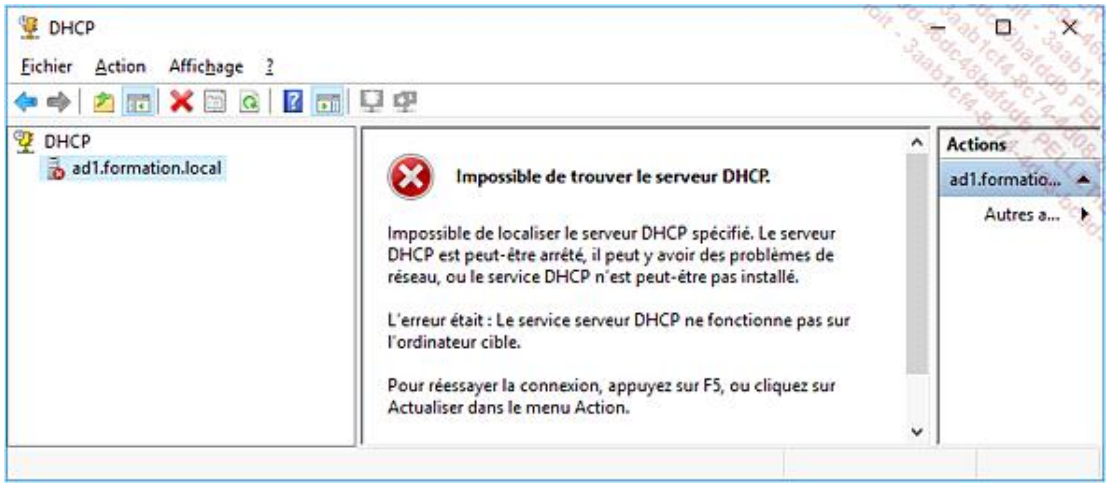
- Cliquez sur **OK**. Ce serveur a le rôle **Actif**.

Le deuxième serveur a le rôle **Veille**.

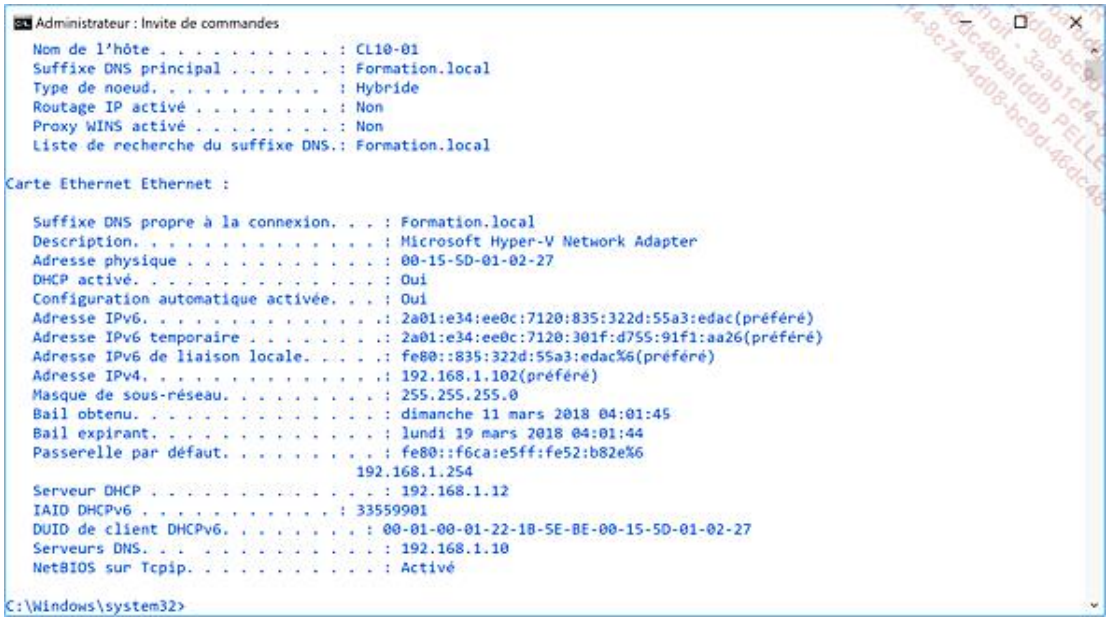
- Renouvelez le bail du poste Windows 10 afin qu'AD1 soit le serveur DHCP qui distribue le bail.



- Sur AD1, lancez la console DHCP.
- Cliquez sur **ad1.formation.local**. Sélectionnez **Toutes les tâches** puis cliquez sur **Arrêter**.



- Sur CL10-01, saisissez `ipconfig /release` et appuyez sur la touche [Entrée] du clavier puis `ipconfig /renew` dans l'invite de commandes DOS et appuyez sur la touche [Entrée].



Le serveur de secours est venu remplacer le serveur actif actuellement hors service.

Gestion du DHCP en PowerShell

Dans cette section, nous allons aborder la gestion du DHCP en PowerShell. Cela complétera la partie graphique vue dans les sections précédentes de ce chapitre. Le dernier point abordé concernera la migration du DHCP à l'aide des outils de migration.

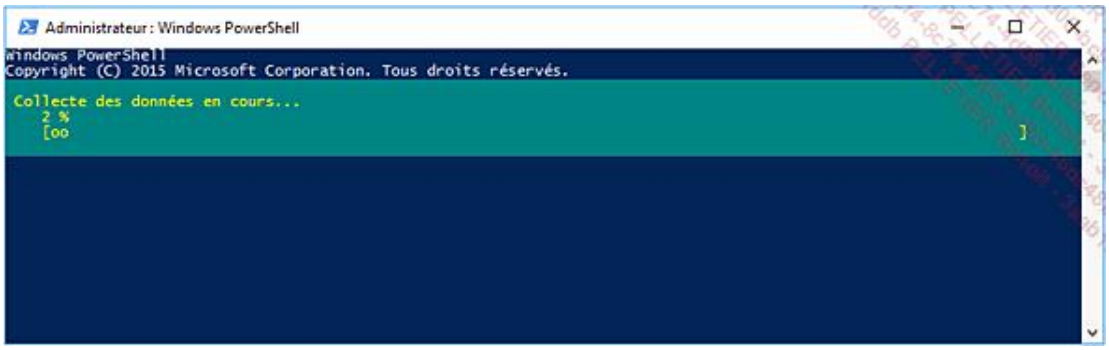
1. Installation du rôle DHCP

L'installation du rôle est la première étape à effectuer. L'opération va consister à installer les consoles et fichiers nécessaires à l'exploitation quotidienne du service.

Pour cela il faut utiliser la commande ci-dessous :

```
Install-WindowsFeature -Name DHCP -IncludeManagementTools
```

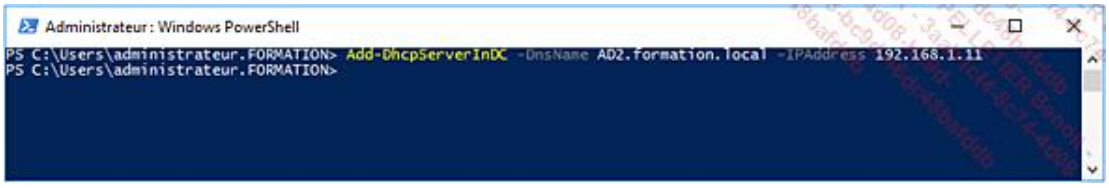
Le script peut être téléchargé depuis la page Informations générales.



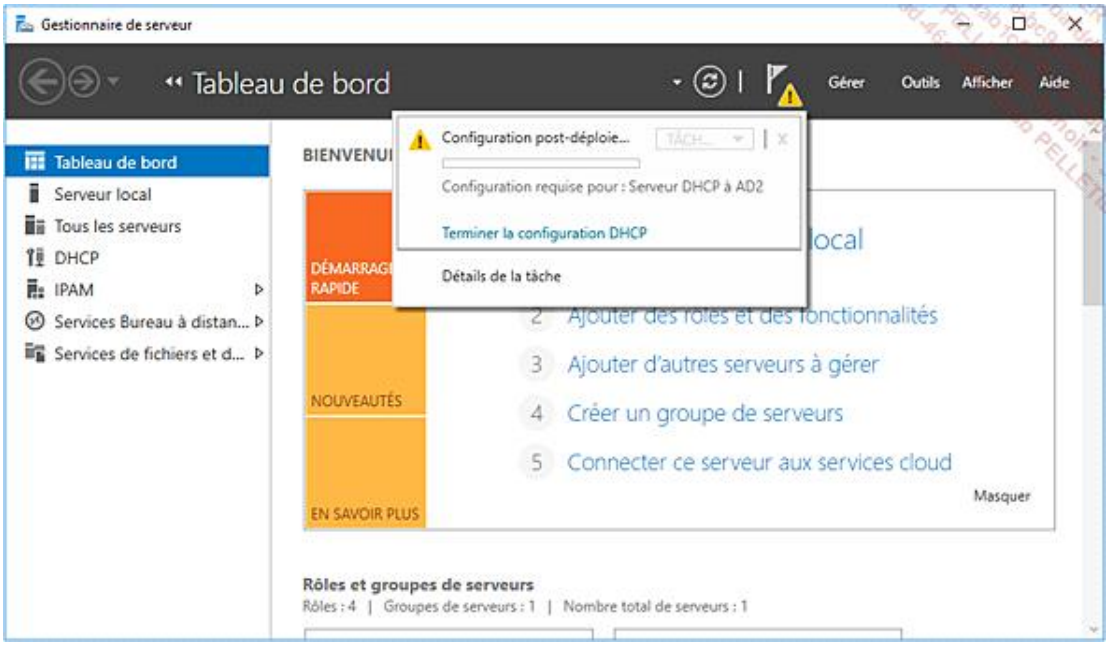
Une fois installée, il est maintenant nécessaire de l'autoriser dans Active Directory. Pour cela, la commande ci-dessous doit être exécutée.

```
Add-DhcpServerInDC -DnsName NomServeurDHCP -IPAddress
AdresseIpServeur
```

Le script peut être téléchargé depuis la page Informations générales.



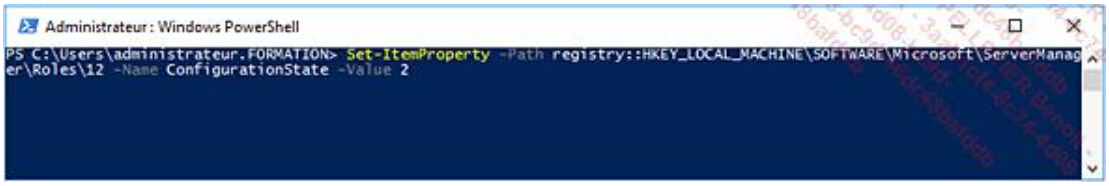
L'installation du rôle est maintenant terminée. En accédant à la console **Gestionnaire de serveur**, on peut voir que l'étape de Post-Installation est toujours présente.



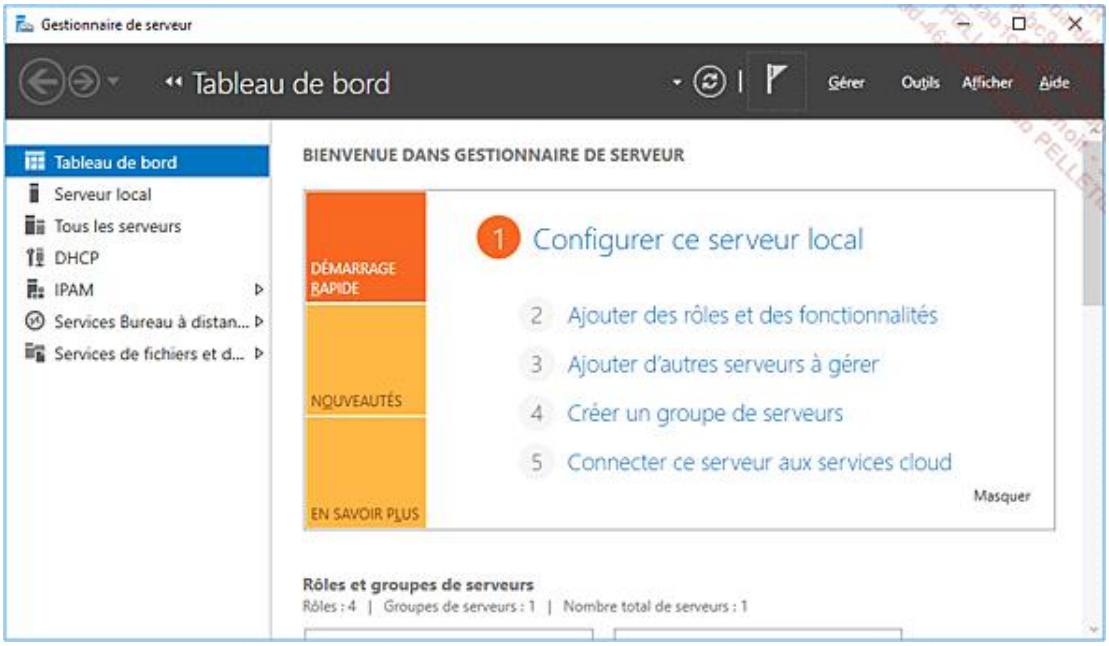
Pour supprimer cette notification à l'aide de PowerShell, exécutez l'instruction suivante :

```
Set-ItemProperty -Path
registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ServerManager\Roles\12
-Name ConfigurationState -Value 2
```

Le script peut être téléchargé depuis la page Informations générales.



La notification n'est plus présente dans la console **Gestionnaire de serveur**.



Le serveur est maintenant prêt à être configuré.

2. Création de l'étendue

L'étendue va contenir la plage d'adresses pouvant être distribuées aux différents postes de travail. Elle peut également contenir d'autres paramètres (serveur DNS, Wins…).

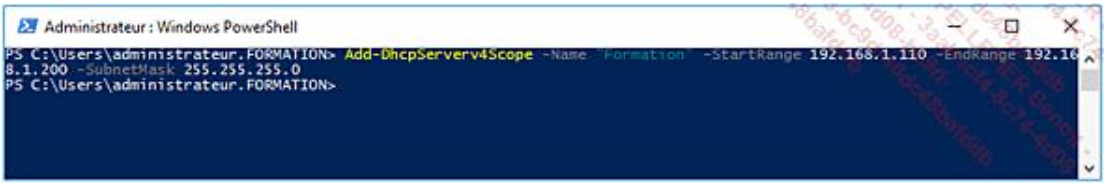
La création s'opère à l'aide de plusieurs cmdlets :

- **Add-DhcpServer4Scope** pour effectuer la création de l'étendue.
- **Add-DhcpServer4ExclusionRange** permet l'exclusion de plusieurs adresses dans une étendue.
- **Set-DhcpServer4OptionDefinition** assure la configuration des options souhaitées.
- **Get-DhcpServer4Scope** donne la liste des étendues DHCP présentes dans le serveur interrogé.

Il est nécessaire dans un premier temps d'effectuer la création de l'étendue. Pour cela la syntaxe ci-dessous peut être utilisée, la plage d'adresses sera de 192.168.1.110 à 192.168.1.200.

```
Add-DhcpServerv4Scope -Name "Formation" -StartRange 192.168.1.110
-EndRange 192.168.1.200 -SubnetMask 255.255.255.0
```

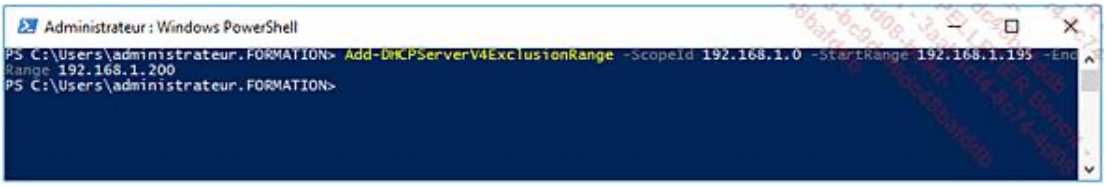
Les scripts peuvent être téléchargés depuis la page Informations générales.



La plage d'adresses IP allant de 192.168.1.195 à 192.168.1.200 peut maintenant être exclue. La syntaxe ci-dessous est utilisée afin de procéder à l'opération d'exclusion.

```
Add-DHCPServerV4ExclusionRange -ScopeId 192.168.1.0
-StartRange 192.168.1.195 -EndRange 192.168.1.200
```

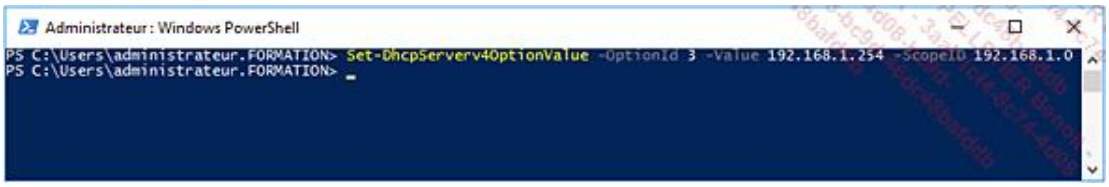
Les scripts peuvent être téléchargés depuis la page Informations générales.



La passerelle doit également être configurée afin de pouvoir être distribuée avec les baux DHCP.

```
Set-DhcpServerv4OptionValue -OptionId 3 -Value 192.168.1.254
-ScopeID 192.168.1.0
```

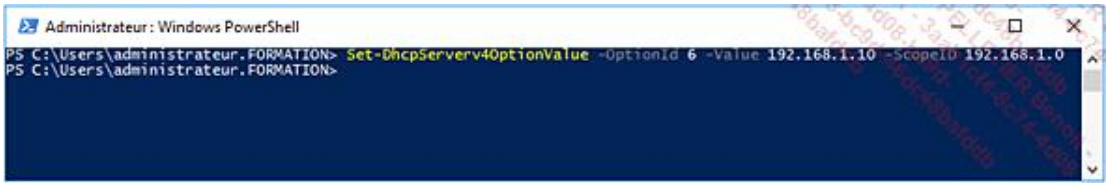
Les scripts peuvent être téléchargés depuis la page Informations générales.



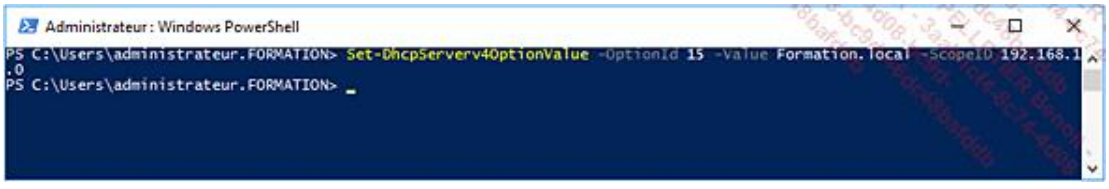
Les options portant l'ID 6 (Serveurs DNS) et 15 (Suffixe DNS) peuvent maintenant être configurées.

Option numéro 6 : Serveur DNS

```
Set-DhcpServerv4OptionValue -OptionId 6 -Value 192.168.1.10
-ScopeID 192.168.1.0
```

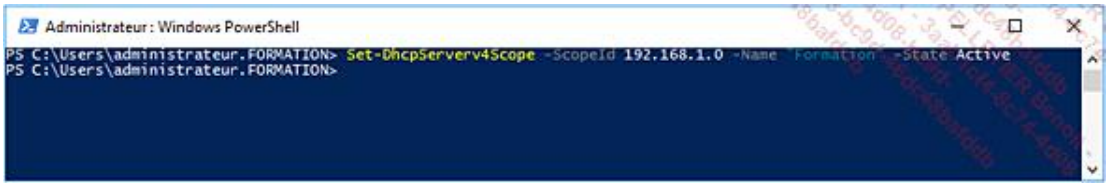



```
Set-DhcpServerv4OptionValue -OptionId 15 -Value Formation.local
-ScopeID 192.168.1.0
```

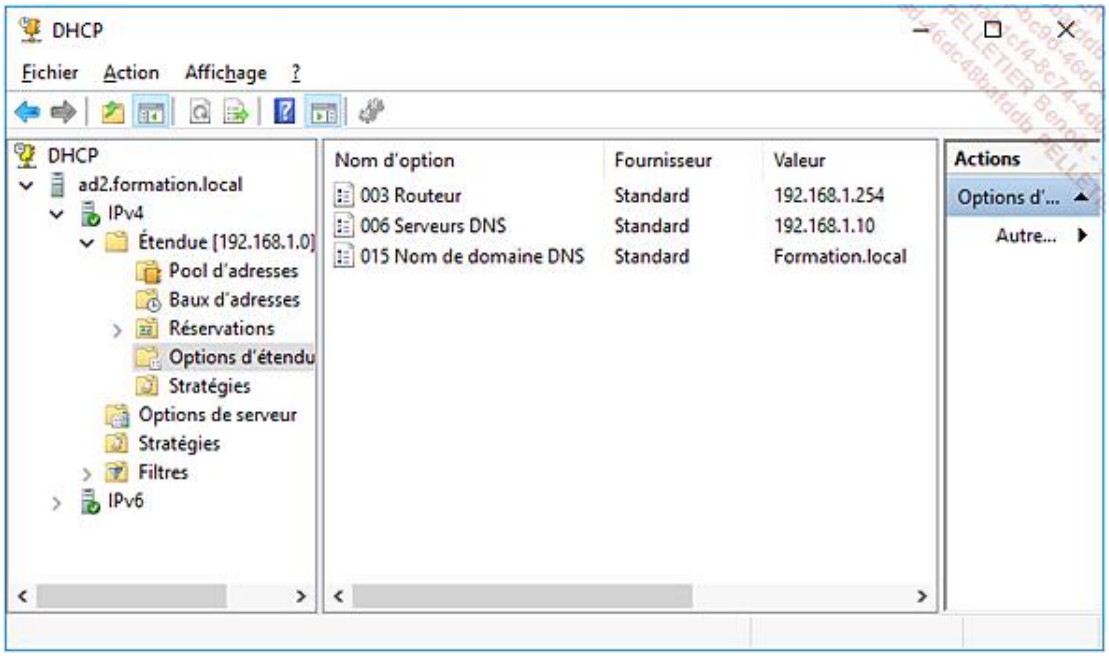


L'étendue peut maintenant être activée.

```
Set-DhcpServerv4Scope -ScopeId 192.168.1.0 -Name "Formation"
-State Active
```



L'étendue est maintenant fonctionnelle.



Les opérations effectuées de manière graphique peuvent être effectuées en ligne de commande.

3. Migration du rôle DHCP

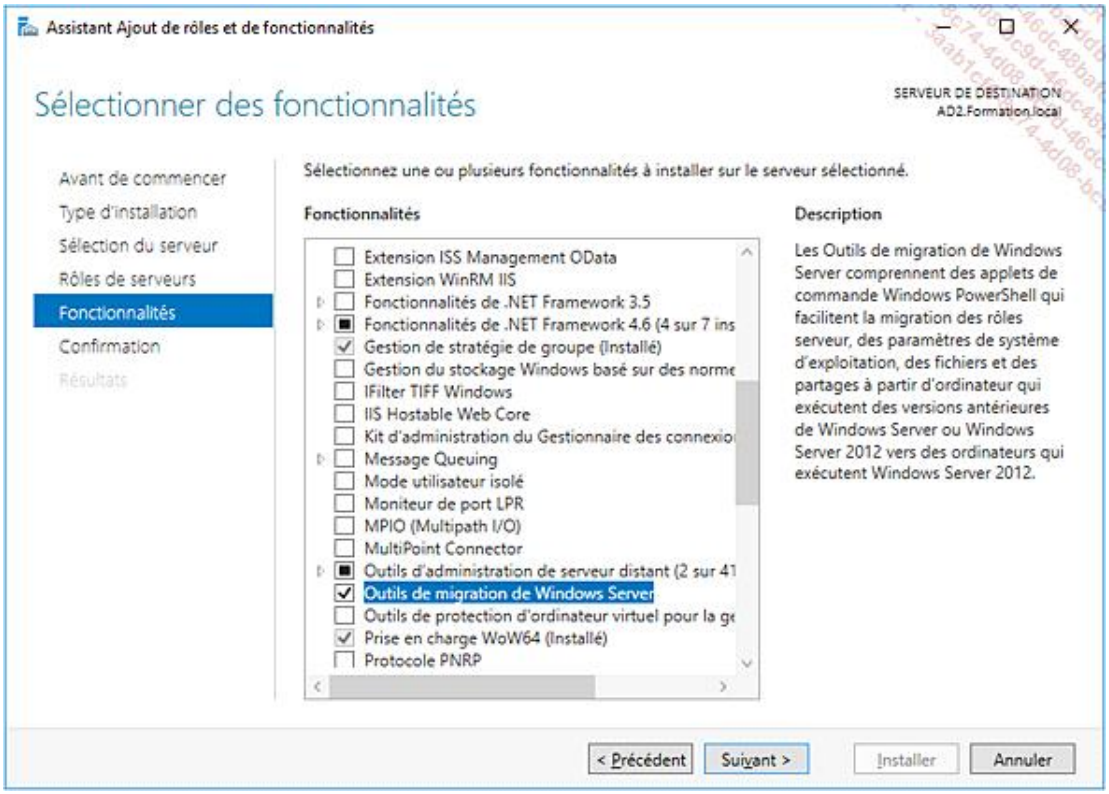
Lors d'un remplacement de serveur physique ou de la mise à niveau d'un système d'exploitation, il peut être nécessaire de procéder à la migration du rôle DHCP. Cette opération peut s'opérer en ligne de commande ainsi qu'avec l'aide des outils de migration. Ces derniers sont fournis par le système d'exploitation en tant que fonctionnalité.

Prérequis à respecter

- Les systèmes d'exploitation source et destination doivent utiliser la même langue d'interface utilisateur.
- Être membre du groupe Admins du domaine au minimum.
- Si le serveur source utilise plusieurs interfaces réseau pour le serveur DHCP, la cible doit également avoir le même nombre d'interfaces.
- Avoir le Framework .NET installé sur le serveur source.

La première opération va consister à installer la fonctionnalité Outils de migration sur le serveur de destination. Ce dernier exécutant Windows Server 2016, la fonctionnalité est nativement présente et nécessite juste d'être

installée.



Création du dossier de déploiement

La migration du serveur source peut maintenant être préparée. Dans notre exemple, le serveur source exécute Windows Server 2012 R2, les différentes opérations vont être effectuées en ligne de commande.

Le dossier de déploiement sur le serveur de destination peut être créé. Pour cela lancez sur le serveur de destination une invite de commandes DOS.

Pour rappel, les outils de migration ont été installés précédemment.

Accédez au répertoire ServerMigrationTools présents dans le dossier System32. La commande ci-dessous peut être utilisée pour effectuer cette opération.

```
cd %Windir%\System32\ServerMigrationTools\
```



Créez un dossier qui contiendra les fichiers générés par la commande `smigdeploy`. Le répertoire peut être un partage réseau sur le serveur source.

Si le serveur source exécute Windows Server 2012 R2, la commande suivante doit être utilisée :

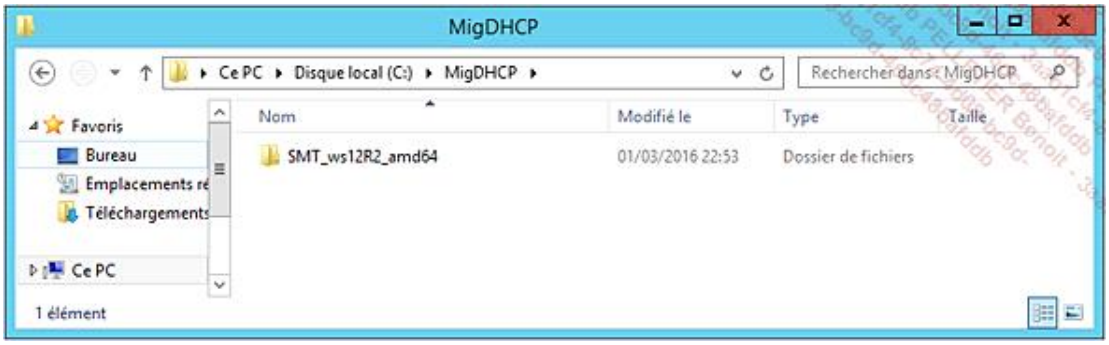
```
SmigDeploy.exe /package /architecture amd64 /os WS12R2 /path
<deployment folder path>
```

Le commutateur `/os` doit avoir au minimum la valeur WS08 pour fonctionner. En fonction du système d'exploitation source, les commutateurs `/architecture` et `/os` devront être modifiés. La valeur amd64 correspond à une architecture 64 bits et non au processeur.

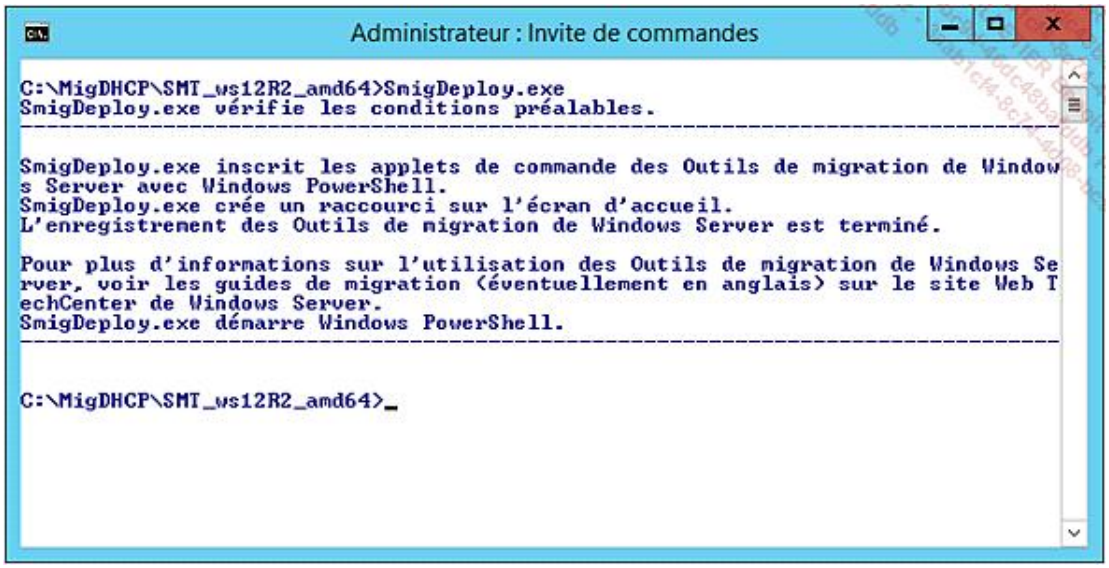


Sur le serveur Windows Server 2012 R2, il est désormais nécessaire d'inscrire le logiciel enfichable Outils de migration. Cette opération s'effectue à l'aide de PowerShell.

Le dossier créé dans MigDHCP doit préalablement être copié sur le serveur source.

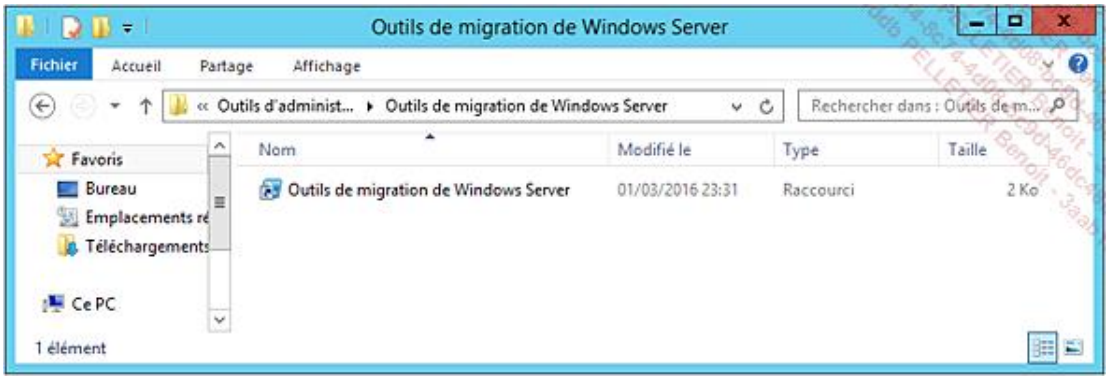


Exécutez une invite de commandes DOS sur le serveur source puis accédez au répertoire précédemment copié. Exécutez la commande `smigdeploy.exe` pour procéder à l'inscription du logiciel enfichable.



Une invite de commandes PowerShell s'exécute. La migration peut maintenant être opérée.

Notez qu'un raccourci est ajouté dans les outils d'administration.



Migration du serveur

Dans un premier temps, le rôle DHCP doit être installé sur le serveur de destination.

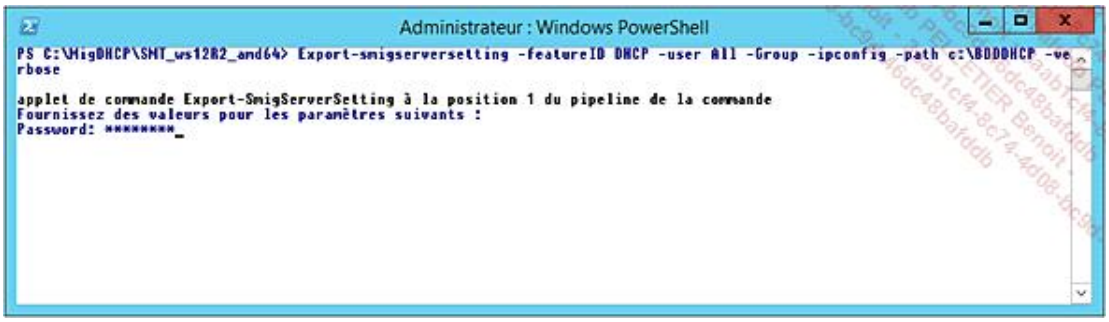
Le service DHCP doit être arrêté sur les serveurs source et cible, l'instruction PowerShell suivante peut être utilisée :

```
Stop-service DHCPserver
```

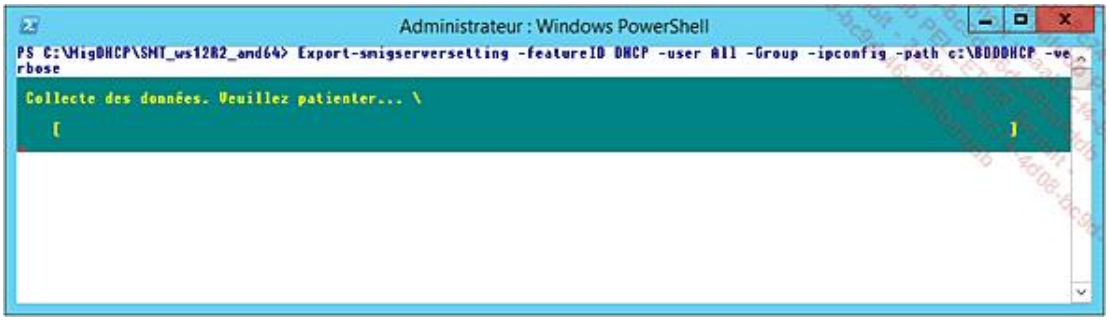
Sur le serveur source, procédez à la migration en utilisant la commande PowerShell suivante :

```
Export-smigserversetting -featureID DHCP -user All -Group
-ipconfig -path c:\BDDDHCP -verbose
```

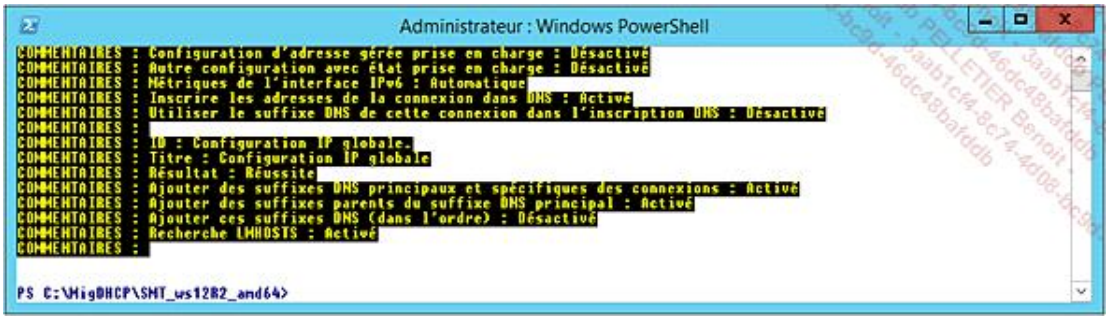
Saisissez un mot de passe afin de chiffrer les données exportées.



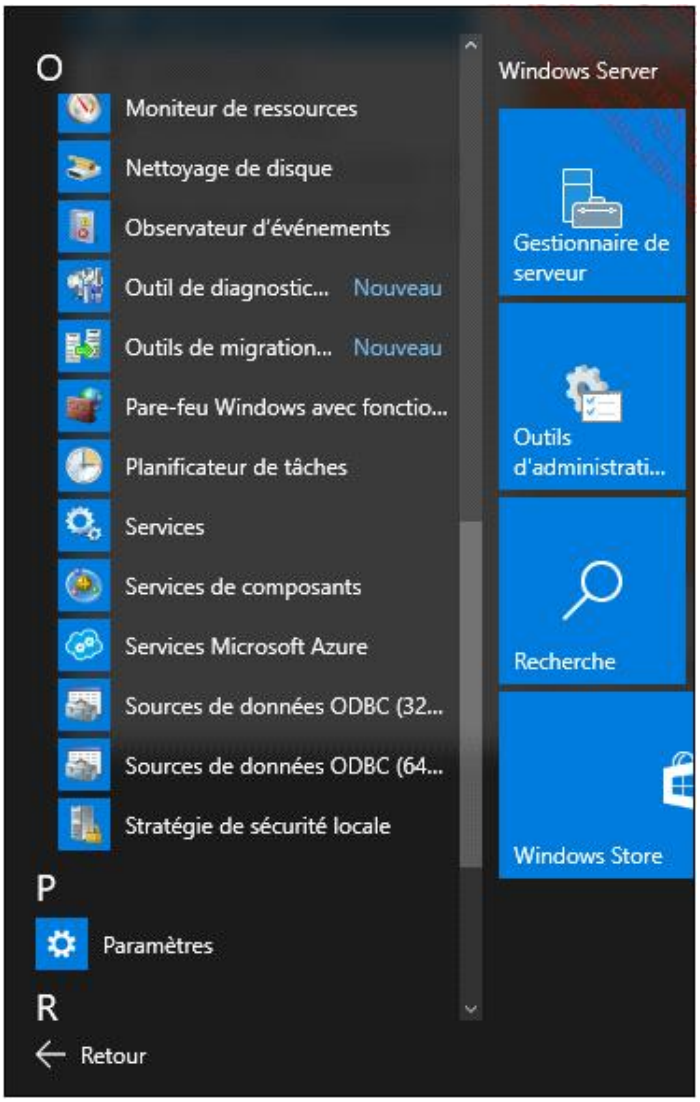
Par la suite, l'opération d'exportation a lieu.



Une fois terminée, un résumé est retourné par la commande.



L'importation peut maintenant être effectuée, cette opération s'effectue depuis le **serveur de destination**. Ici le serveur concerné est AD2. Il s'agit d'utiliser les outils de migration présents dans les outils d'administration.

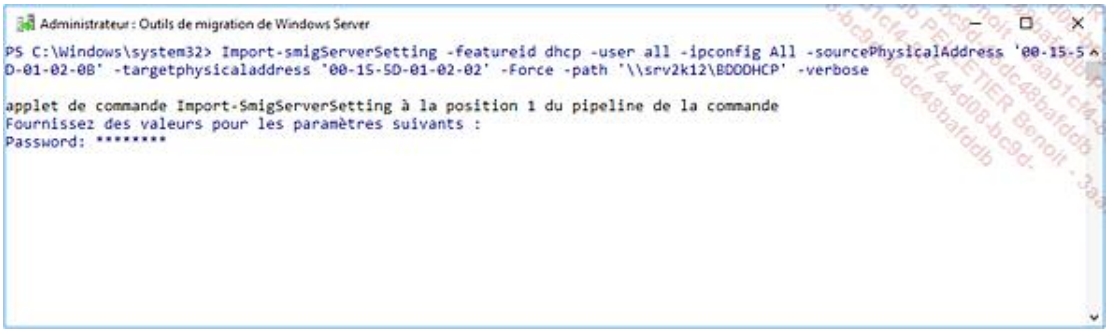


La commande va faire coïncider les adresses MAC sources avec les adresses MAC de destination. De plus le dossier contenant l'exportation doit être partagé afin de pouvoir y accéder par le réseau.

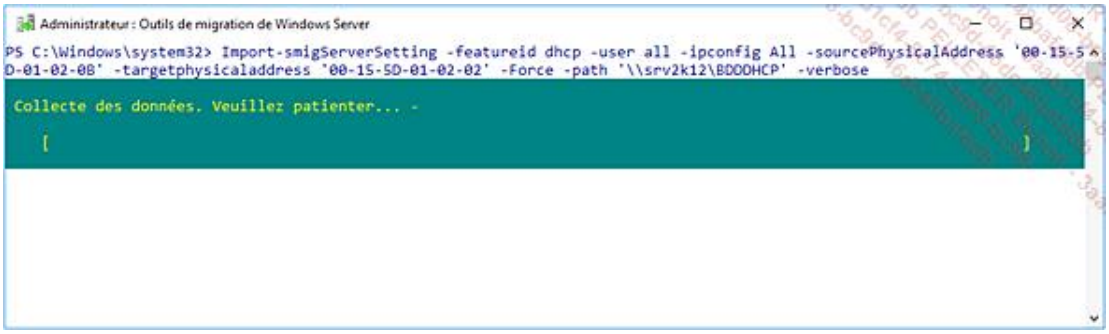
```
Import-smigServerSetting -featureid dhcp -user all -ipconfig All
-sourcePhysicalAddress MacSource1, MacSource2,...
-targetphysicaladdress MacDest1, MacDes2,... -Force -path -verbose
```

Le commutateur ipconfig permet de migrer également la configuration IP du serveur source sur le serveur cible.

Saisissez le mot de passe utilisé lors de l'exportation puis validez avec la touche [Entrée].



Les données sont collectées puis l'importation effectuée.



La configuration du serveur est correctement migrée. En production, il est conseillé de déplacer le fichier contenant la configuration à importer (stocké dans \\srv12\bdddhcp) sur le serveur cible afin d'effectuer les opérations localement.

Le service DHCP sur le serveur cible peut maintenant être redémarré. Par la suite vérifiez la présence de la ou des étendues dans le serveur cible.

IPAM

IPAM (*IP Address Management*) est une fonctionnalité intégrée dans les systèmes d'exploitation Microsoft depuis Windows Server 2012. Elle donne la possibilité de découvrir, surveiller, auditer et gérer une ou plusieurs plages d'adresses IP. De plus il est possible d'effectuer des tâches d'administration et de surveillance des serveurs DHCP et DNS.

Les composants suivants sont compris dans la fonctionnalité :

- **Découverte automatique de l'infrastructure des adresses IP** : cela permet d'effectuer la découverte des contrôleurs de domaine, des serveurs DHCP et des serveurs DNS dans le domaine souhaité.
- **Affichage, création de rapports et gestion personnalisés de l'espace d'adressage IP** : cela permet d'obtenir des informations sur le suivi et l'utilisation des adresses IP. Ainsi les espaces d'adressages IPv4 et IPv6 peuvent être organisés en blocs d'adresses IP, en plages d'adresses IP et en adresses IP individuelles.
- **Audit des modifications de configuration du serveur et suivi de l'utilisation des adresses IP** : permet l'affichage des différents événements opérationnels du serveur IPAM et DHCP géré par la fonctionnalité. Un suivi des adresses IP, ID de client, nom d'hôte ou nom d'utilisateur est également effectué. De plus les événements de baux DHCP et les événements d'ouverture de session utilisateur sont collectés sur les serveurs NPS (*Network Policy Server*), sur les contrôleurs de domaine et sur les serveurs DHCP.

Deux méthodes sont envisageables pour déployer des serveurs IPAM :

- **Distribuée** : un serveur IPAM sur chaque site de l'entreprise.
- **Centralisée** : un serveur pour l'ensemble de l'entreprise.

IPAM effectue des tentatives périodiques de localisation des contrôleurs de domaine, des serveurs DNS et DHCP. Cette opération concerne évidemment les serveurs qui se trouvent dans l'étendue (unité d'organisation, domaine ou site AD) des stratégies de groupe. Afin d'être gérés par IPAM et d'autoriser l'accès à ce dernier, les paramètres de sécurité et les ports du serveur doivent être configurés.

La communication entre le serveur IPAM et les serveurs gérés se fait par le biais de WMI ou RPC.

1. Les spécifications d'IPAM

L'étendue de la découverte pour les serveurs IPAM est limitée uniquement à une seule forêt Active Directory. Les serveurs pris en charge (NPS, DNS et DHCP) doivent exécuter Windows Server 2008 (ou versions ultérieures) et être joints à un domaine. Attention certains éléments réseau (WINS - *Windows Internet Naming Service* -, proxys…) ne sont pas pris en charge par le serveur IPAM.

Une base de données de type interne peut être utilisée, il est également possible d'utiliser SQL Server.

Un serveur IPAM peut prendre en charge plusieurs centaines de serveurs DHCP et serveurs DNS.

Néanmoins aucune stratégie consistant à nettoyer la base de données au bout d'un certain temps n'est présente. L'administrateur doit donc effectuer cette opération manuellement.

Avec l'installation d'IPAM, les fonctionnalités suivantes sont également installées :

- **Outils d'administration de serveur distant** : installation des outils DHCP, DNS et du client IPAM, ceci afin d'effectuer la gestion à distance des différents serveurs gérés.
- **Base de données interne Windows** : une base de données doit être utilisée, elle peut être de type interne

(utilisable uniquement par certains rôles et fonctionnalités du système d'exploitation). Depuis Windows Server 2012 R2, il est possible d'utiliser une base de données SQL Server (sur le serveur IPAM ou un autre serveur).

- **Service d'activation des processus Windows** : élimine la dépendance au protocole HTTP en généralisant le modèle de processus IIS.
- **Gestion des stratégies de groupe** : installe la console MMC permettant la gestion des stratégies de groupe.
- **.NET Framework** : installation de la fonctionnalité .NET Framework 4.5.

2. Fonctionnalité d'IPAM

Lors de l'installation de la fonctionnalité, les groupes locaux suivants sont créés :

- **Utilisateurs IPAM** : les membres de ce groupe ont la possibilité d'afficher toutes les informations de la découverte de serveur, ainsi que celles concernant l'espace d'adressage IP et la gestion de serveur. L'accès aux informations de suivi des adresses IP leur est interdit.
- **Administrateurs IPAM MSM (*Multi-Server Management*)** : des droits d'utilisateur IPAM leur sont attribués, ils ont également la possibilité d'effectuer des tâches de gestion de serveur et des tâches de gestion courantes.
- **Administrateurs IPAM ASM (*Address Space Management*)** : en plus des droits d'utilisateur IPAM qui leur sont attribués, ils ont la possibilité d'effectuer des tâches d'adressage IP et des tâches de gestion courantes.
- **Administrateurs d'Audit IPAM IP** : les membres de ce groupe peuvent effectuer des tâches de gestion courantes ainsi qu'afficher les informations de suivi d'adresse IP.
- **Administrateurs IPAM** : les administrateurs IPAM ont un accès à toutes les données, ils peuvent également effectuer toutes les tâches.

Ces dernières sont régulièrement lancées en fonction d'une périodicité donnée. Elles sont présentes dans le planificateur de tâches (Microsoft / Windows / IPAM).

- **DiscoveryTask** : permet la découverte de manière automatique des serveurs DC, DHCP et DNS.
- **AddressUtilizationCollectionTask** : effectue la collecte des données d'utilisation de l'espace d'adressage pour les serveurs DHCP.
- **AuditTask** : collecte des informations d'audit des serveurs DHCP, IPAM, NPS et DC ainsi que celles des baux DHCP.
- **ConfigurationTask** : les informations de configuration des serveurs DHCP, DNS pour ASM et MSM sont recueillies.
- **ServerAvailabilityTask** : l'état du service des serveurs DHCP et DNS est récupéré.

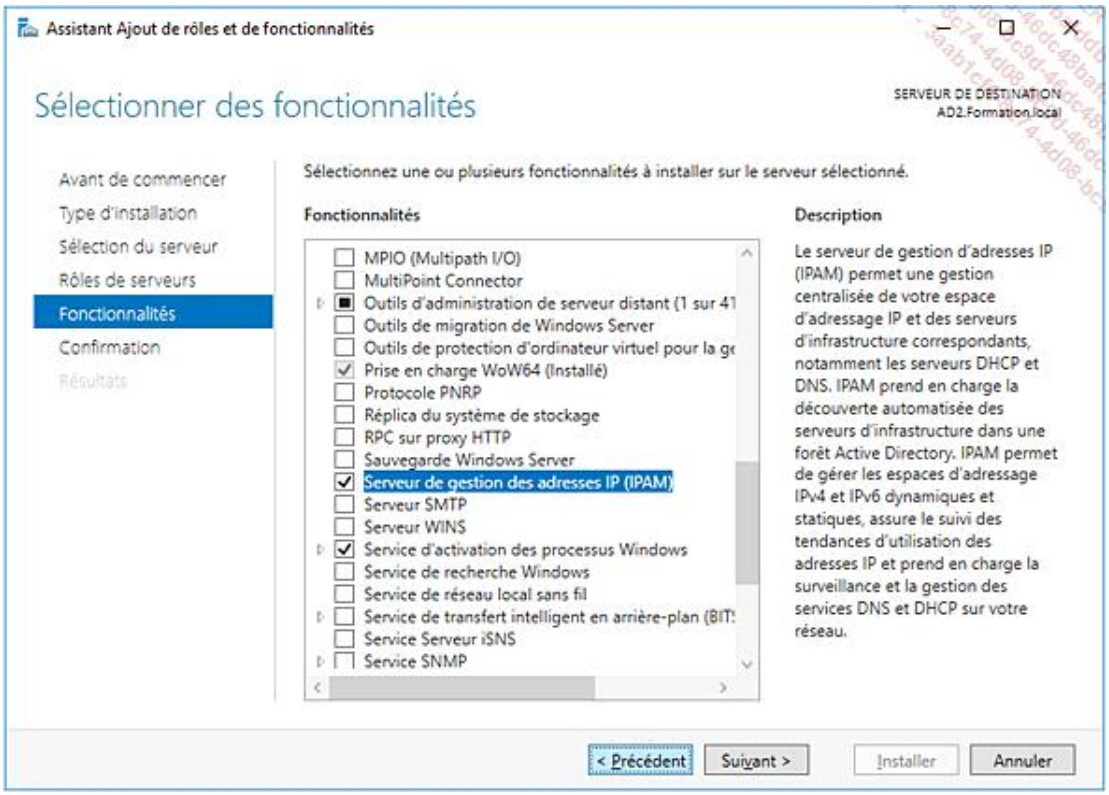
3. Installation d'IPAM

- Sur AD1, supprimez le basculement au niveau DHCP afin que lui seul soit serveur DHCP.
- Sur AD2, lancez la console **Gestionnaire de serveur** puis cliquez sur **Ajouter des rôles et des fonctionnalités**.

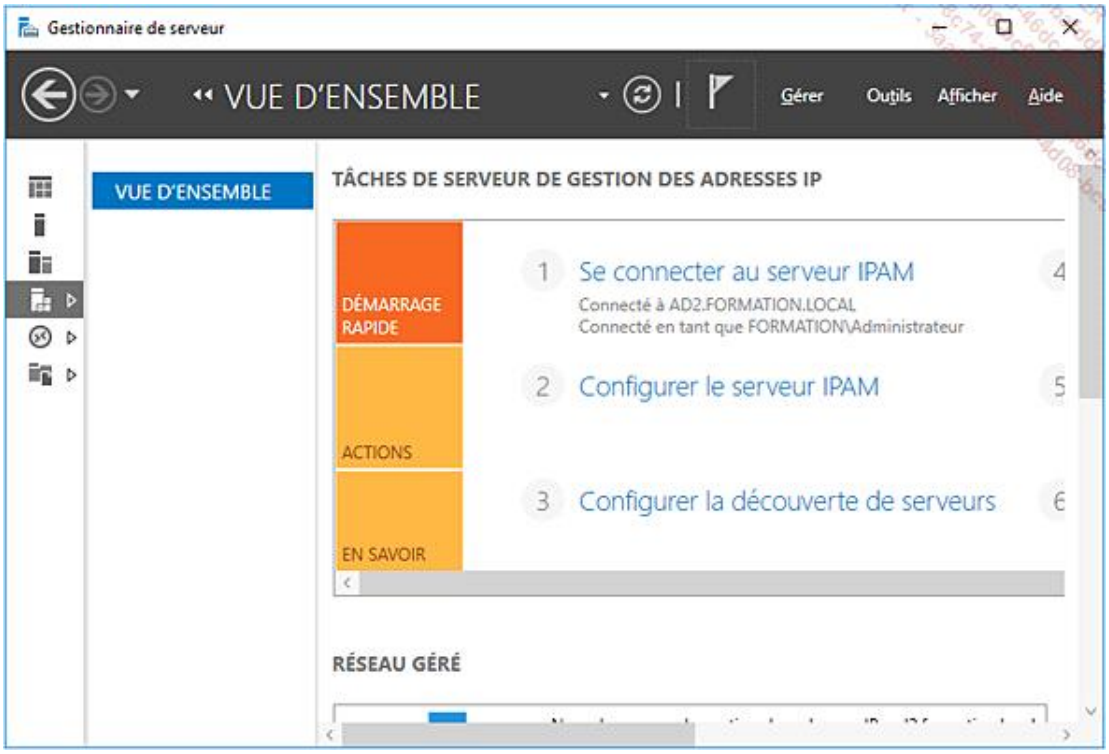
IPAM ne doit pas être installé sur un contrôleur de domaine, AD2 a été rétrogradé dans les chapitres précédents, il n'a donc maintenant plus aucun rôle Active Directory.

- Lancez la console **Gestionnaire de serveur** sur le serveur **AD2**.
- Dans les fenêtres **Sélectionner le type d'installation** et **Sélectionner le serveur de destination**, cliquez sur **Suivant** en laissant le choix par défaut.
- Dans la fenêtre de sélection des fonctionnalités, cochez la case **Serveur de gestion des adresses IP** puis

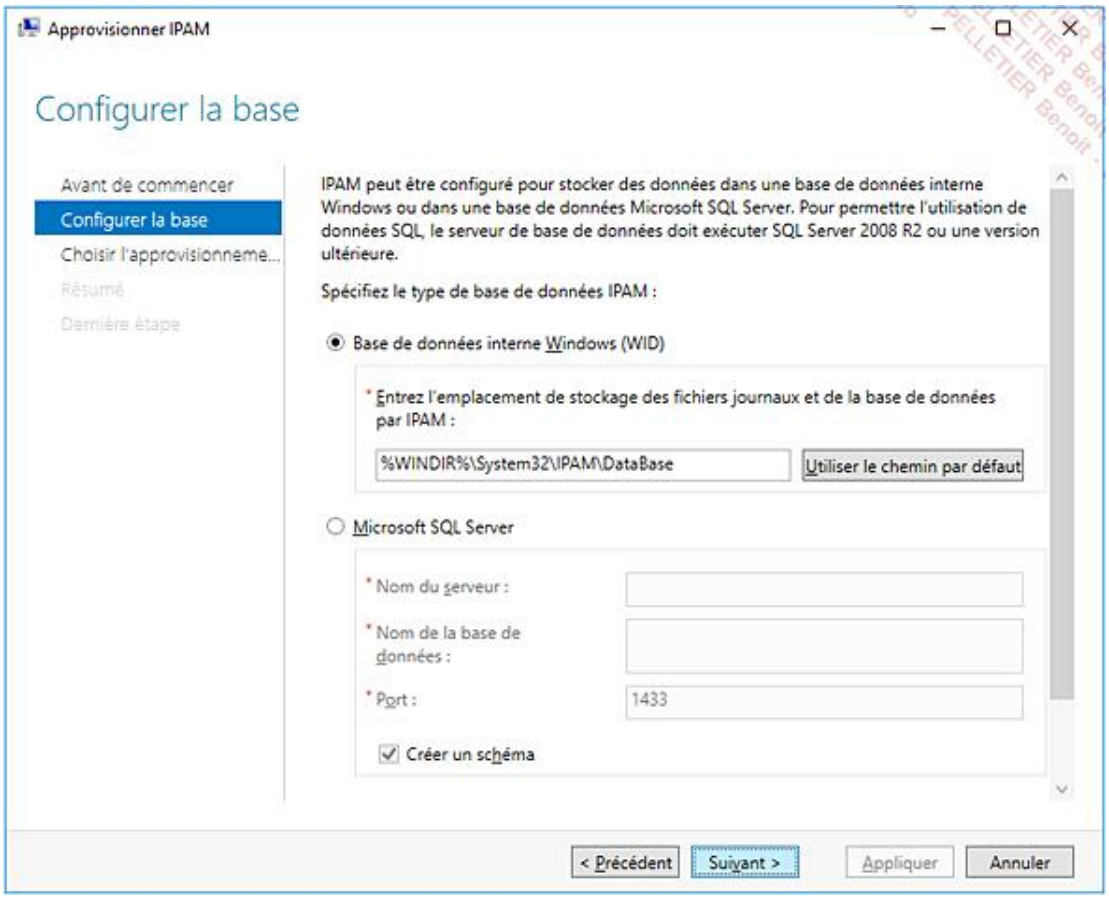
cliquez sur le bouton **Ajouter des fonctionnalités** dans la fenêtre qui apparaît.



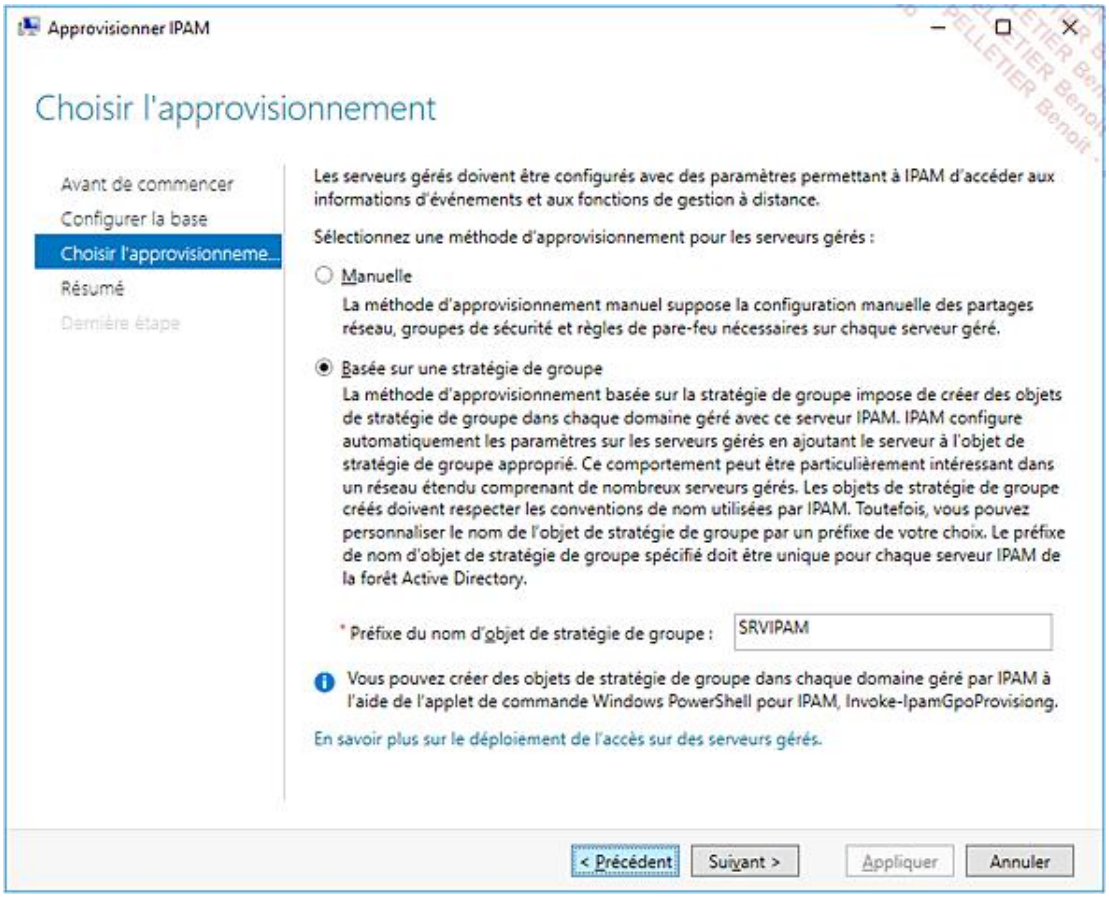
- Cliquez sur **Installer** pour lancer l'installation de la fonctionnalité.
- Dans la console **Gestionnaire de serveur**, cliquez sur **IPAM** afin d'afficher la page de présentation.



- Cliquez sur le lien **Configurer le serveur IPAM**.
- Cliquez sur **Suivant** dans la fenêtre **Avant de commencer**.
- Dans la fenêtre **Configurer la base**, laissez le choix par défaut et cliquez sur **Suivant**.



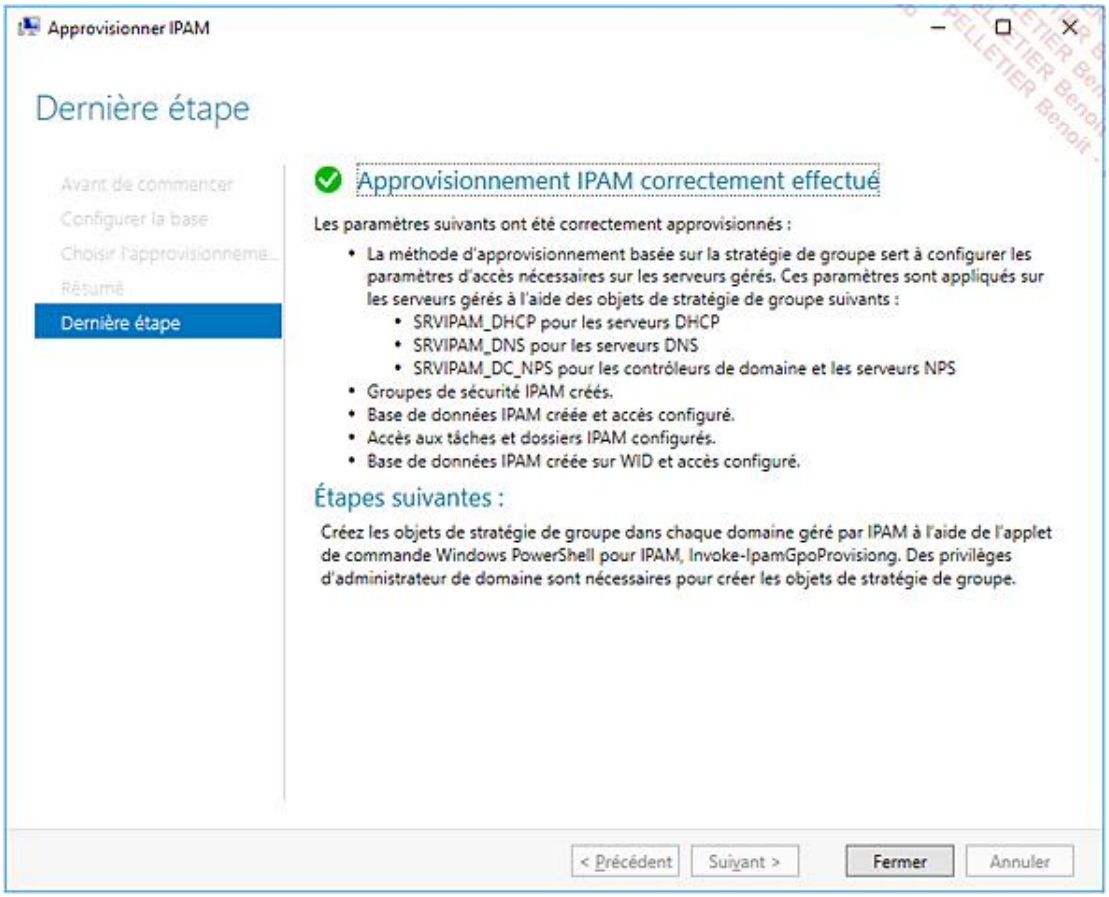
- Choisissez une méthode d'approvisionnement **Basée sur une stratégie de groupe**.
- Dans le champ **Préfixe du nom d'objet de stratégie de groupe**, saisissez **SRVIPAM**.



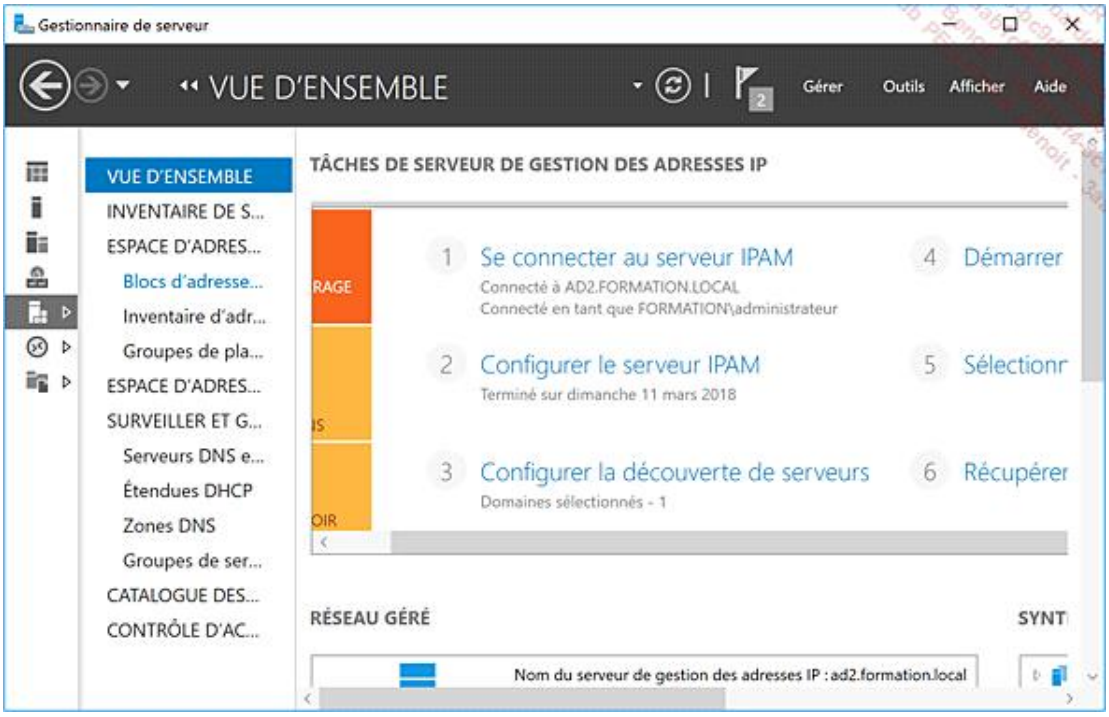
- Validez les choix en cliquant sur **Suivant** et **Appliquer**.

L'approvisionnement est en cours…

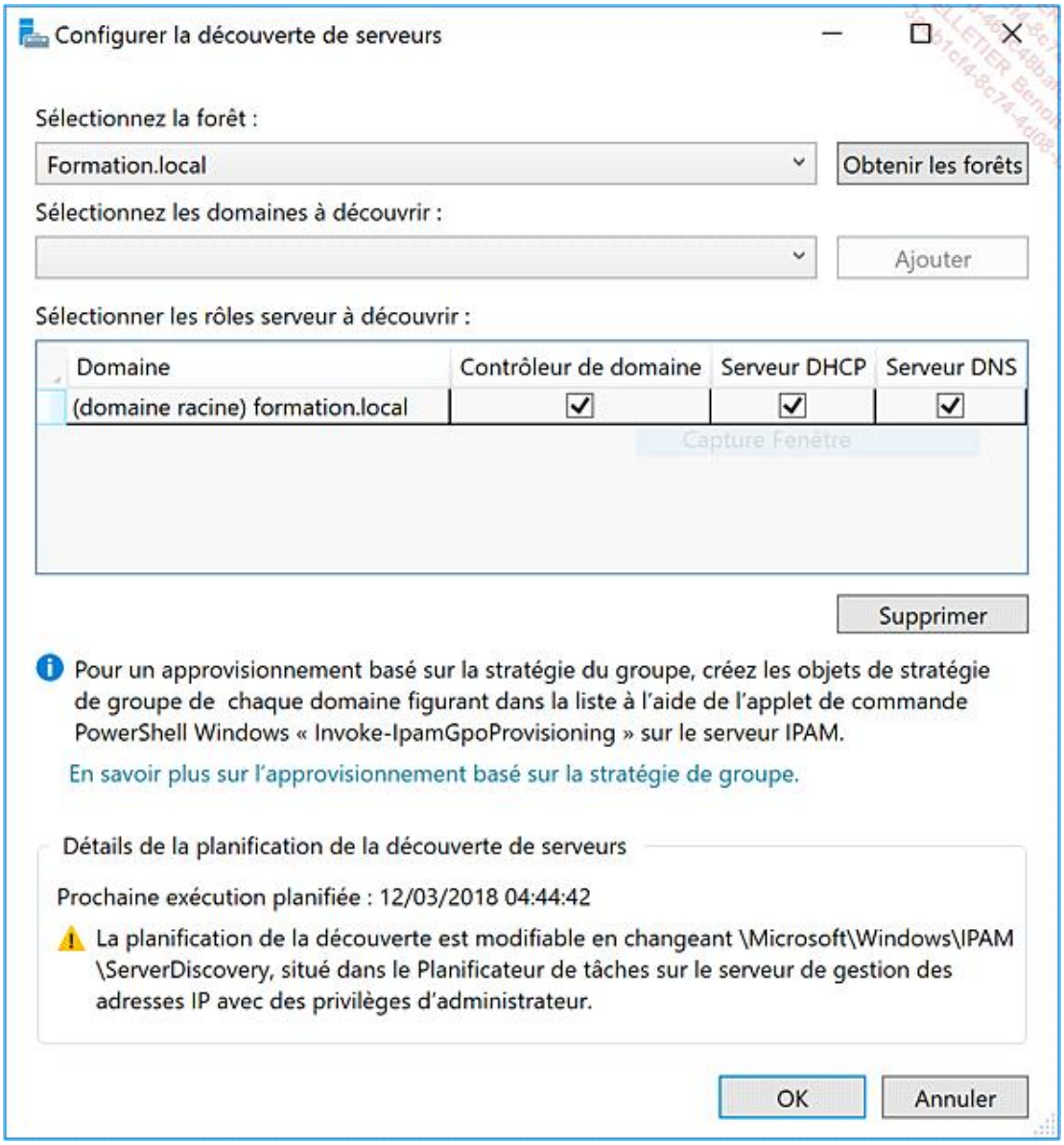
- Vérifiez à la fin la présence du message **Approvisionnement IPAM correctement effectué** puis cliquez sur **Terminer**.



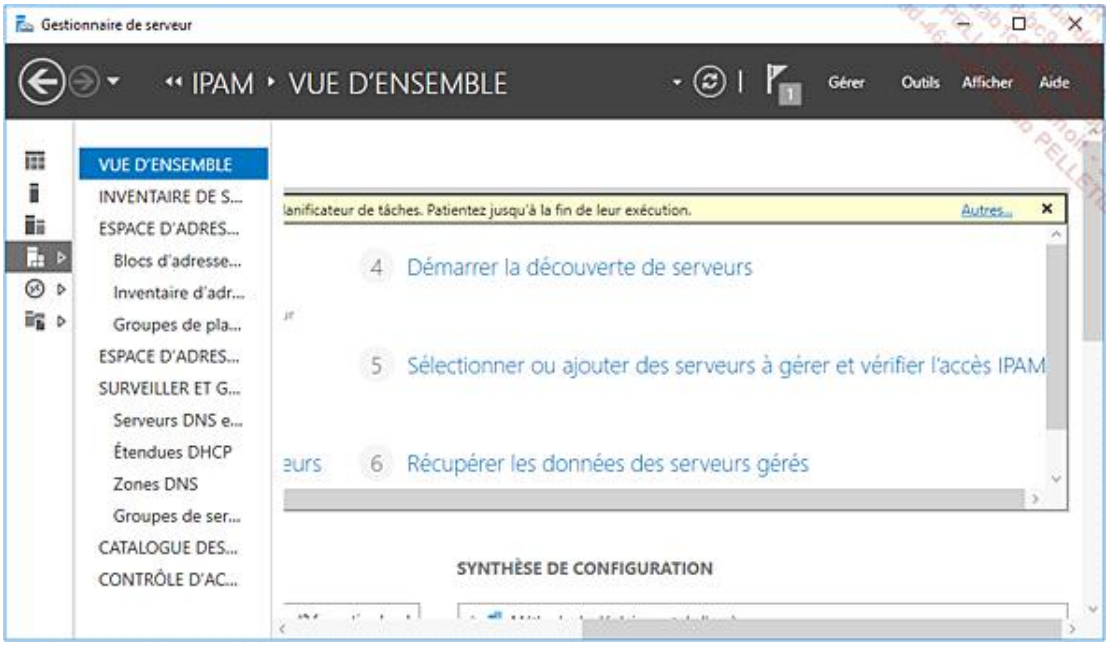
- Cliquez sur **Configurer la découverte de serveurs**.



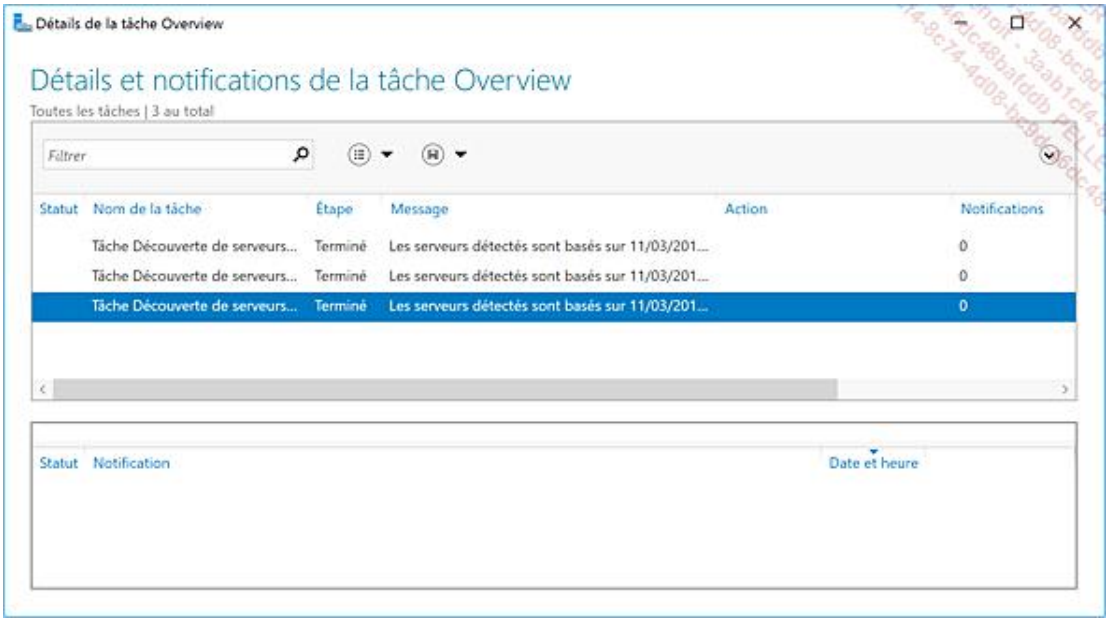
- Cliquez sur **Obtenir les forêts** afin d'ajouter le domaine **Formation.local** dans l'étendue.
- Cliquez sur **Ajouter**.
- Configurez les rôles à découvrir en décochant ceux non souhaités.



- Cliquez sur **OK**.
- Dans la fenêtre **VUE D'ENSEMBLE**, cliquez sur **Démarrer la découverte**.
- Cliquez sur **Autres** dans le bandeau jaune afin d'avoir plus de détails.



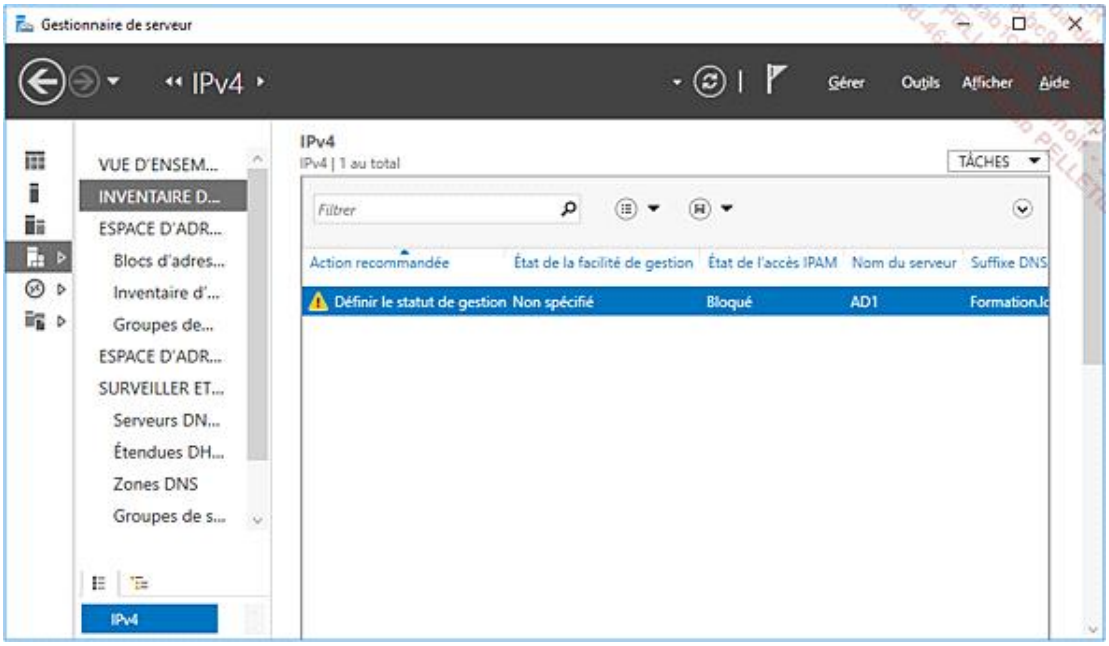
- Attendez la fin de l'exécution.
- Quand le champ **Étape** a la valeur **Terminé** pour l'ensemble des actions, fermez la fenêtre **Détails et notifications de la tâche Overview**.



Afin de limiter le nombre de serveurs utilisé, j'ai effectué une dépromotion du serveur AD3. Vous pouvez ignorer cette dépromotion si vous le souhaitez.

- Cliquez sur **Selectionner ou ajouter des serveurs à gérer et vérifier l'accès IPAM**.

Le ou les serveurs ont l'état **Bloqué** dans **État de l'accès IPAM** et **Non spécifié** dans **État de la facilité de gestion**.



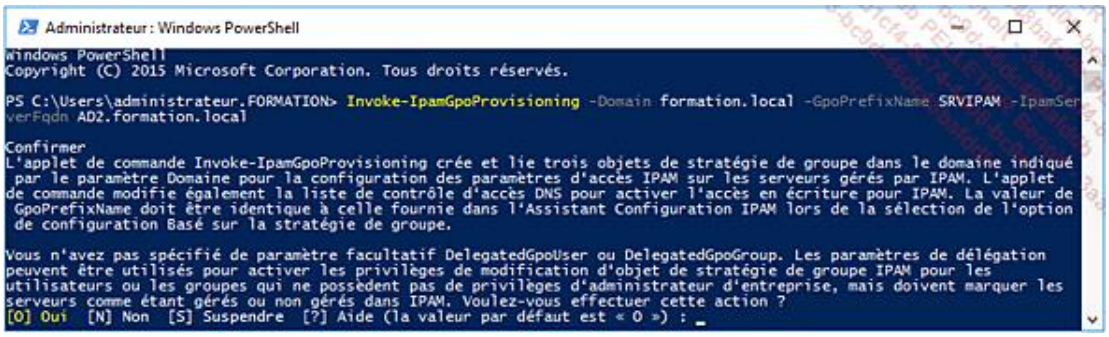
Si aucun serveur n'est affiché, cliquez sur **Actualiser IPv4** (à côté de l'identificateur de notification).

Il est maintenant nécessaire de donner à AD2 le droit de gérer les différents serveurs. Nous allons donc utiliser les objets de stratégie de groupe pour autoriser l'accès aux serveurs NPS (*Network Policy Server*), DHCP (*Dynamic Host Configuration Protocol*) et DNS (*Domain Name System*). Dans notre cas seul, DNS et DHCP sont présents sur le réseau local.

- Sur AD2, lancez une console PowerShell en tant qu'administrateur.
- Saisissez la commande ci-dessous puis appuyez sur [Entrée] :

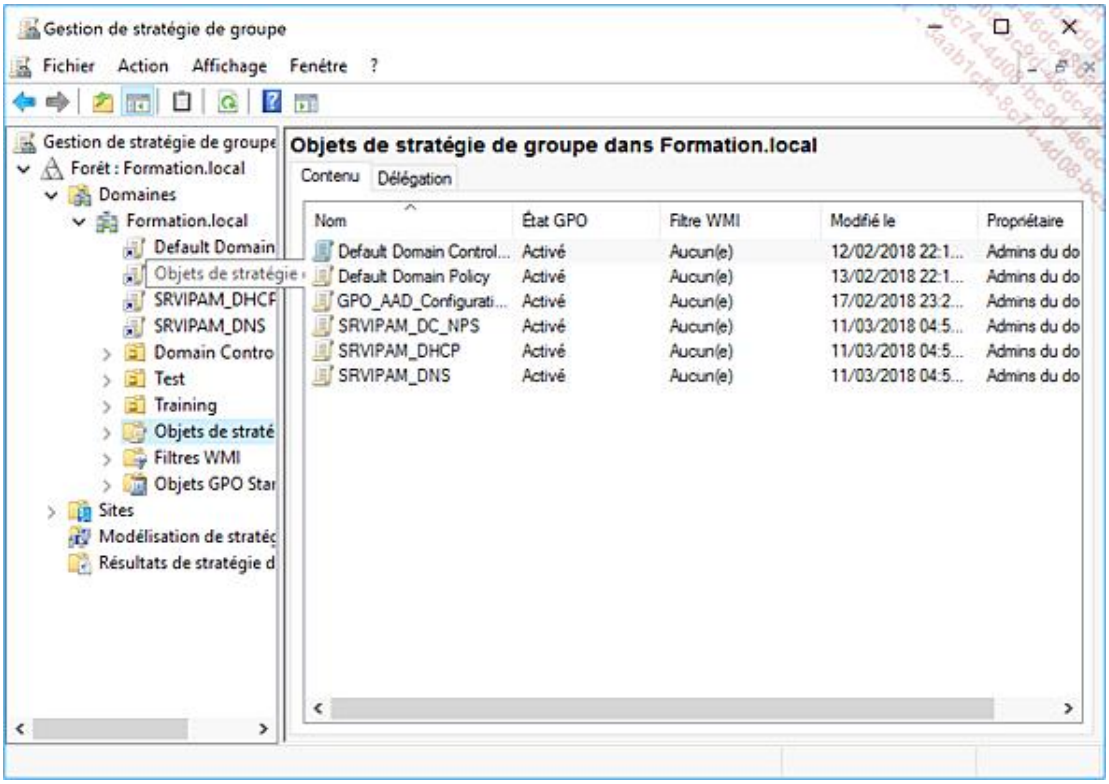
```
Invoke-IpamGpoProvisioning -Domain formation.local -GpoPrefixName
SRVIPAM -IpamServerFqdn ad2.formation.local
```

Le script peut être téléchargé depuis la page Informations générales.

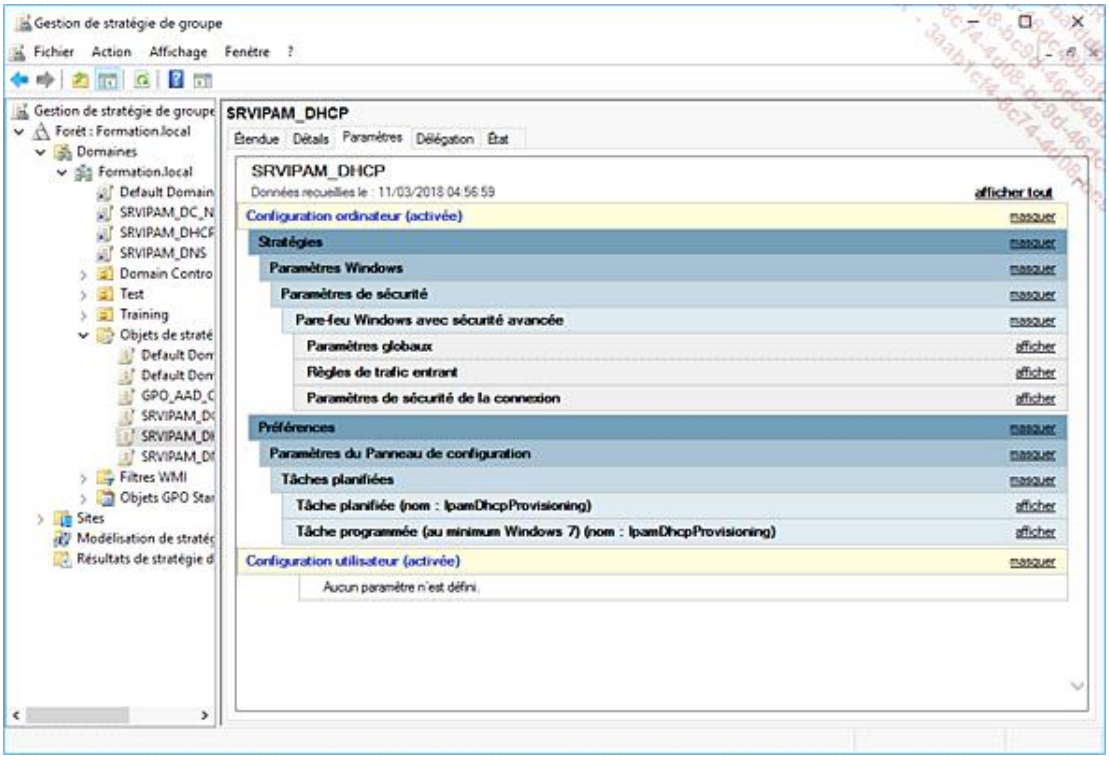


- Cliquez sur la touche du clavier **O**, puis sur la touche [Entrée] pour valider la modification.

De nouvelles stratégies sont présentes dans la console **Gestion de stratégie de groupe**.



La stratégie **SRVIPAM_DHCP** contient les paramètres suivants :

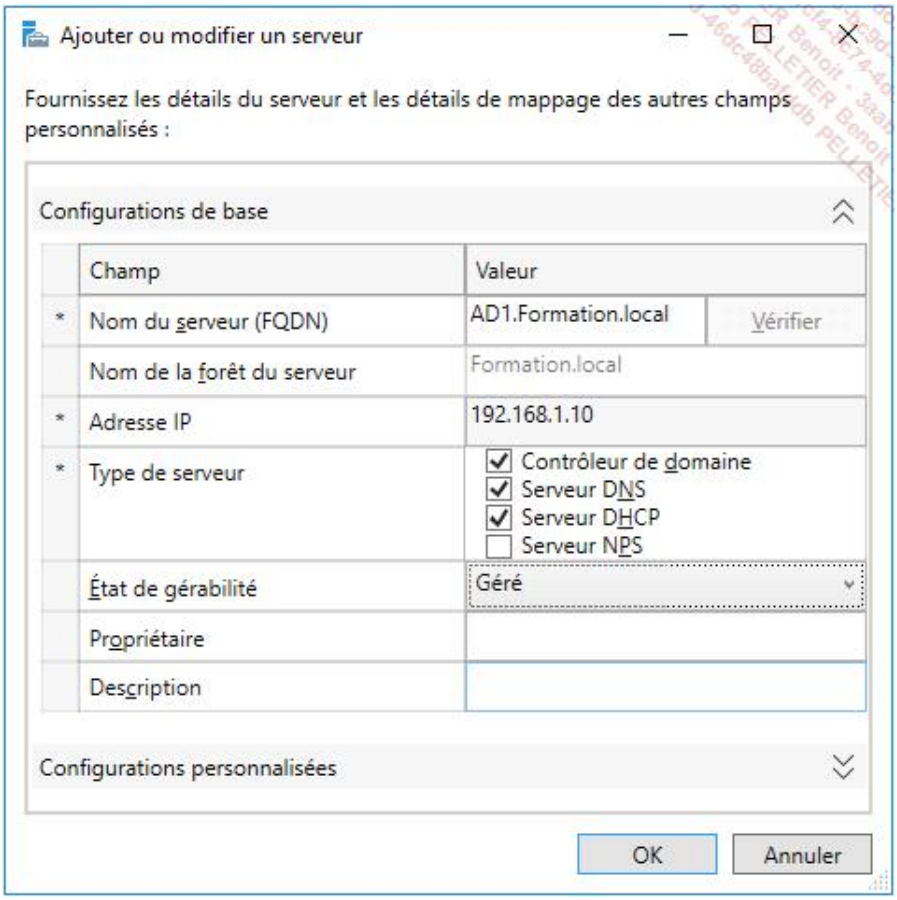


Les stratégies sont liées par défaut à la racine du domaine.

Dans la console de configuration d'IPAM, effectuez un clic droit sur la ligne AD1 puis sélectionnez **Modifier serveur**.

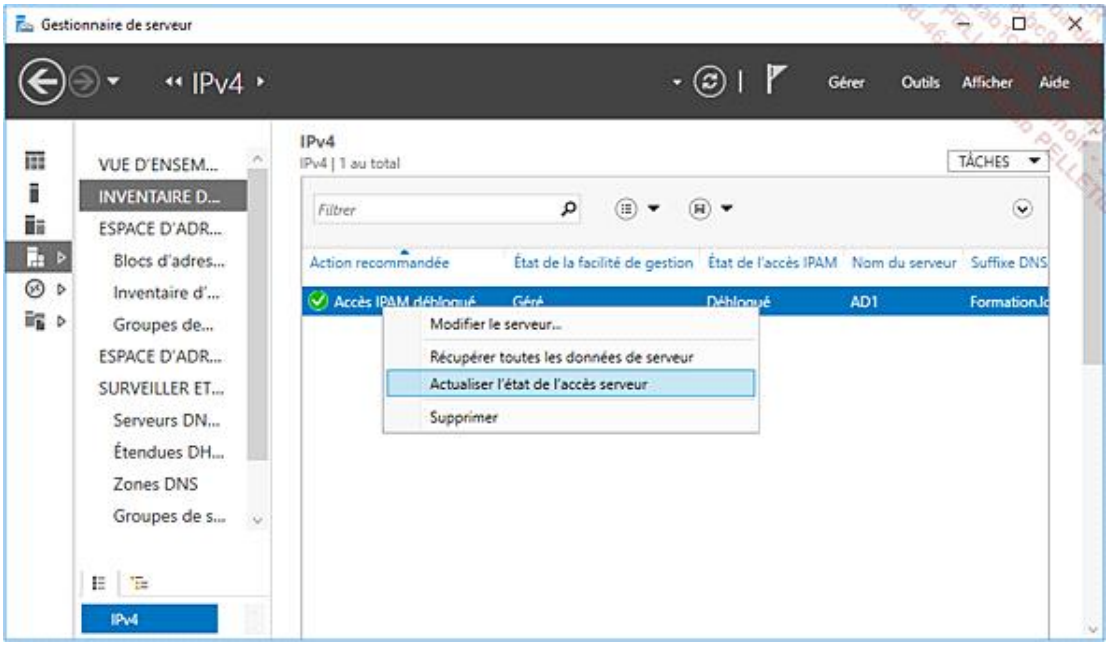
Cette opération devra être effectuée sur les autres serveurs présents dans la console.

- Dans la liste déroulante **État de gérabilité**, sélectionnez **Géré**.



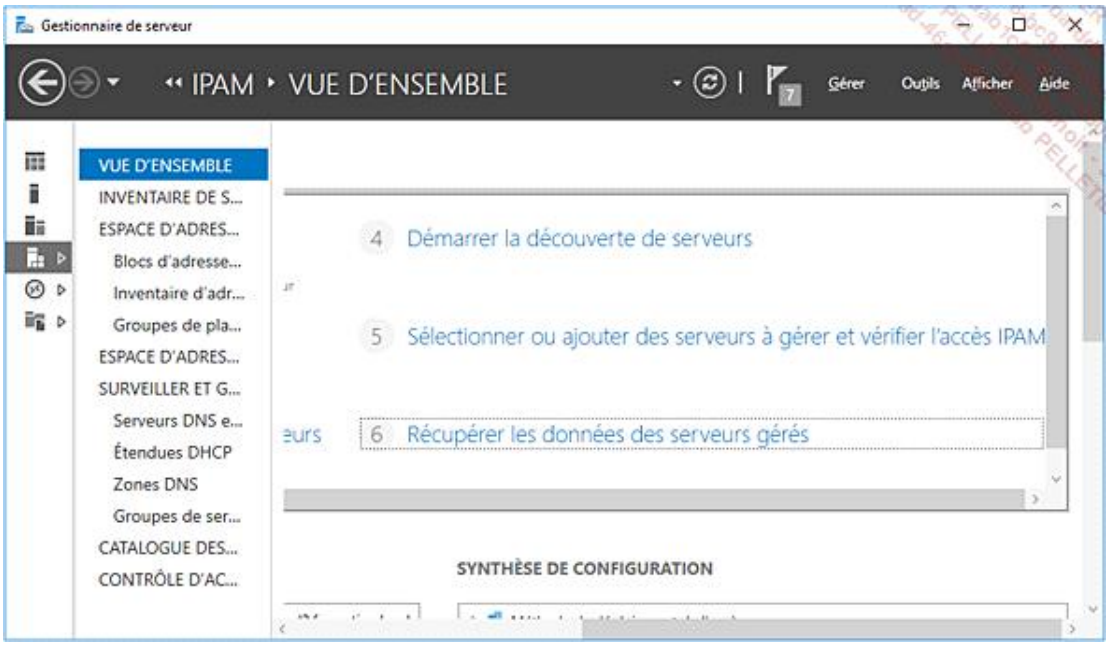
- Cliquez sur **OK**.
- Sur le serveur AD1, ouvrez une invite de commandes DOS et saisissez la commande `gpupdate /force` puis redémarrez le serveur. Ceci permet l'application des stratégies de groupe précédemment créées avec la commande PowerShell.
- Effectuez un clic droit sur la ligne **Débloquer l'accès IPAM** puis cliquez sur **Actualiser l'état de l'accès serveur**. L'état de l'accès IPAM est maintenant **Débloqué**.

Si l'état n'est pas **Débloqué**, actualisez la console **Gestionnaire de serveur**.



Vérifiez l'application des stratégies de groupe si l'état reste bloqué.

- Dans le bandeau **VUE D'ENSEMBLE**, cliquez sur **Récupérer les données des serveurs gérés**.



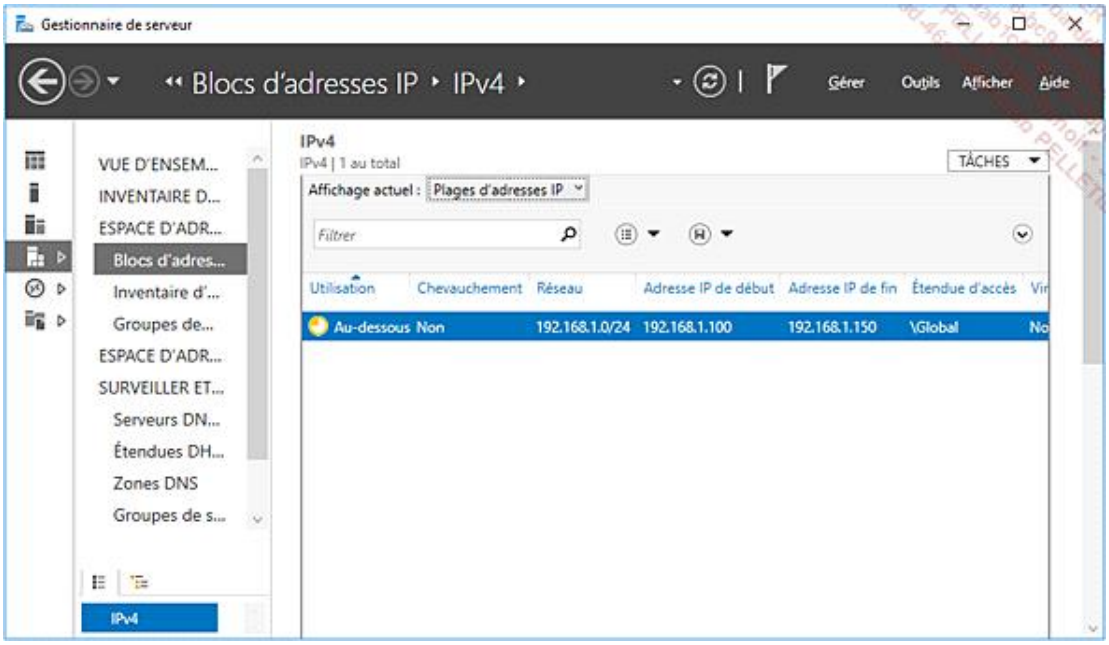
- Attendez la fin de la récupération (baux en cours…).
- Cliquez sur **Blocs d'adresse IP** dans la catégorie **Espace d'adressage IP**.

  Les informations récupérées depuis le serveur DHCP s'affichent.

4. Opérations sur les adresses IP

IPAM a la possibilité de rechercher une adresse IP mais également d'effectuer la réservation et la récupération d'une adresse. Ceci permet de pouvoir attribuer l'adresse fournie par IPAM à un poste de façon statique.

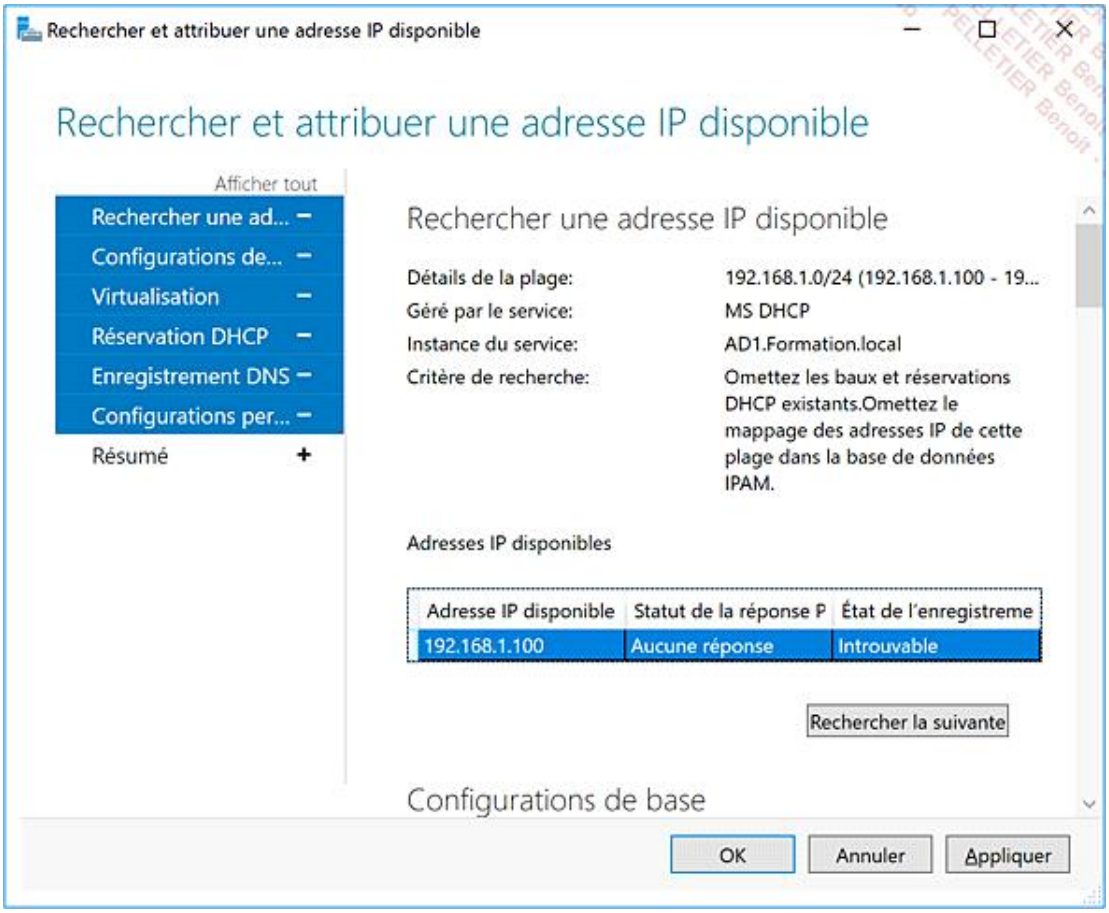
- Cliquez sur **Blocs d'adresse IP**.
- Sélectionnez dans la liste déroulante **Affichage actuel** la valeur **Plages d'adresses IP**.



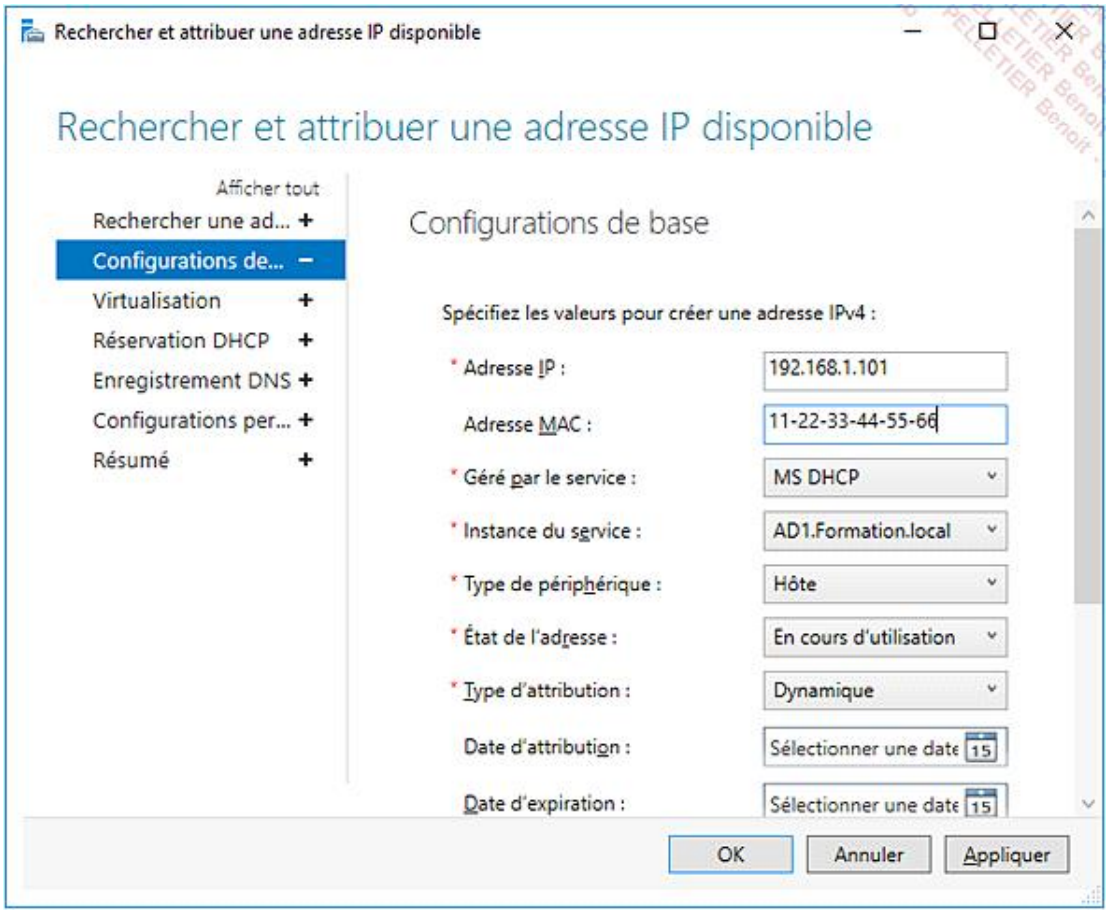
- Effectuez un clic droit sur la ligne de la plage d'adresses puis sélectionnez **Rechercher et attribuer une adresse IP disponible**.

Un test de ping sur l'adresse IP ainsi que la recherche de l'enregistrement dans le DNS sont effectués. Le résultat est affiché dans la fenêtre.

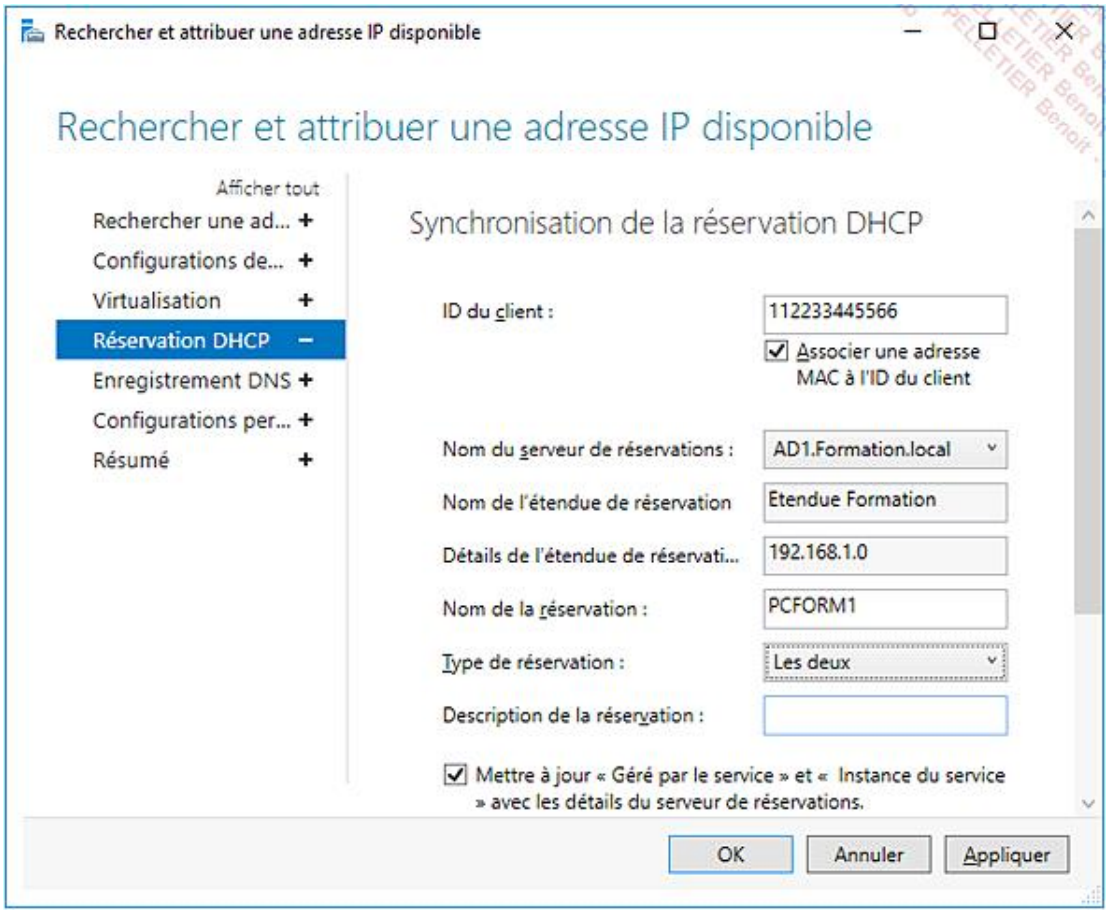
- Cliquez sur le bouton **Rechercher la suivante**.



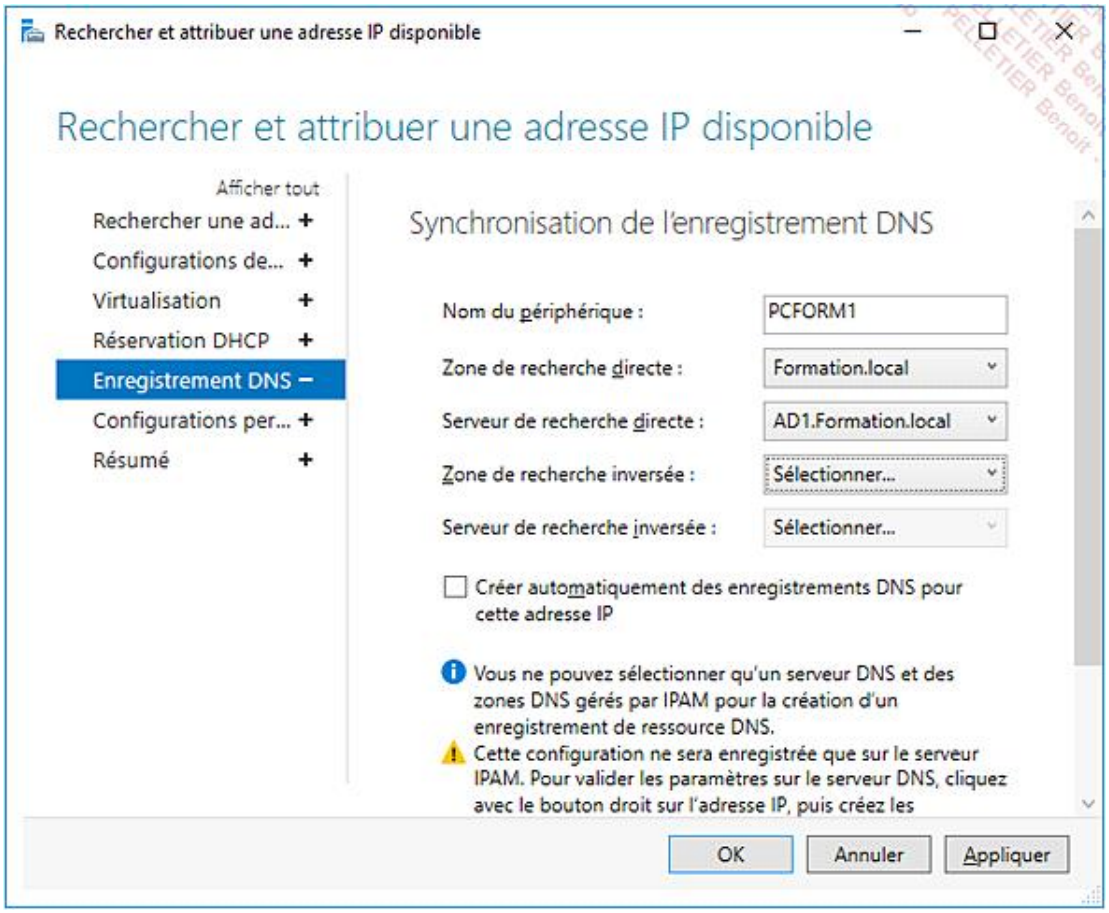
- Cliquez sur le nœud **Configurations de base**.
- Saisissez **11-22-33-44-55-66** dans le champ **Adresse MAC**.



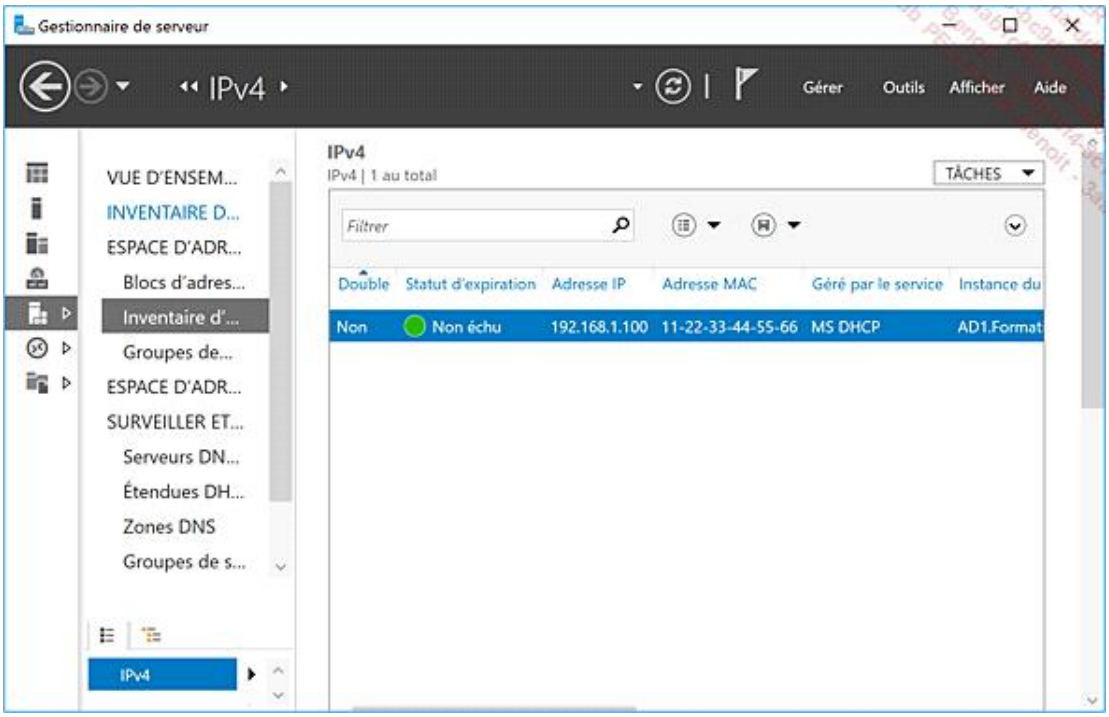
- Cliquez sur le nœud **Réservation DHCP**.
- Cochez la case **Associer une adresse MAC à l'ID du client**.
- Sélectionnez **AD1.Formation.local** dans la liste déroulante **Nom du serveur de réservations**.
- Saisissez **PCFORM1** dans le champ **Nom de la réservation** puis sélectionnez **Les deux** dans la liste déroulante **Type de réservation**.



- Développez le nœud **Enregistrement DNS**.
- Saisissez **PCFORM1** dans le champ **Nom du périphérique** puis sélectionnez **Formation.local** dans la liste déroulante **Zone de recherche directe**.
- Sélectionnez **AD1.Formation.local** dans **Serveur de recherche directe**.



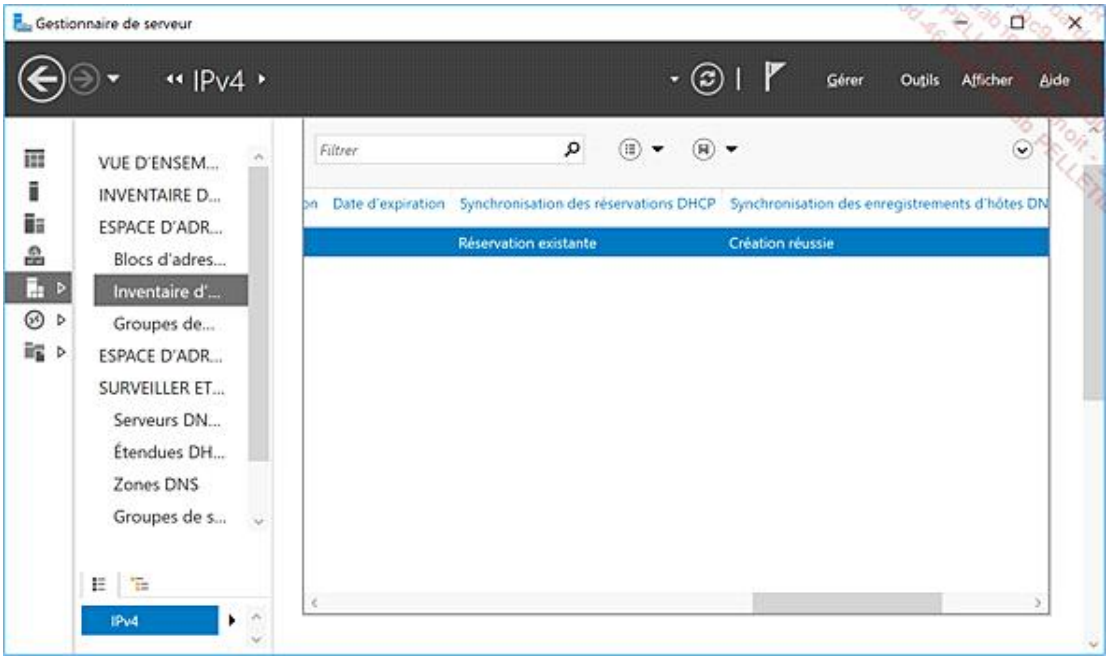
- Cliquez sur **OK** pour créer les enregistrements.
- Dans **ESPACE D'ADRESSAGE IP**, cliquez sur **Inventaire d'adresse IP**.



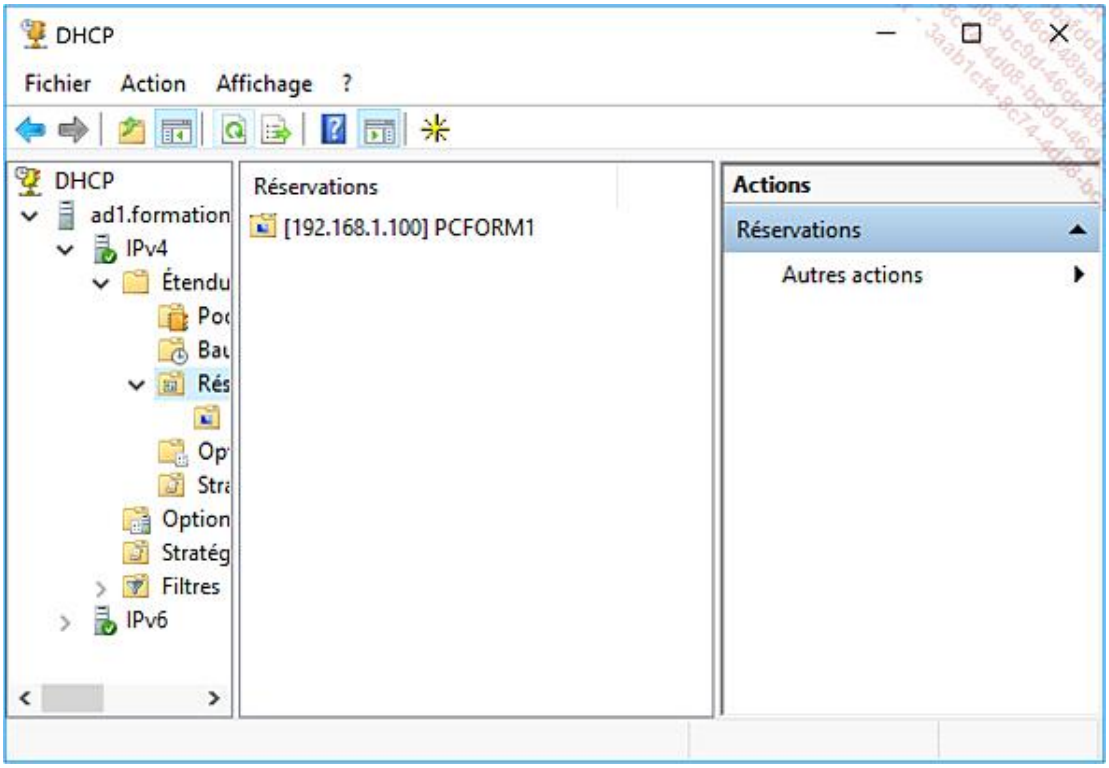
- Effectuez un clic droit sur l'adresse IP **192.168.1.101**, puis sélectionnez **Créer un enregistrement d'hôte DNS**.

Attendez la fin de l'opération…

- Renouvelez l'opération en sélectionnant **Créer une réservation DHCP**.
- Vérifiez si les champs **Synchronisation des réservations DHCP** et **Synchronisation des enregistrements d'hôtes DNS** ne sont pas en erreur.



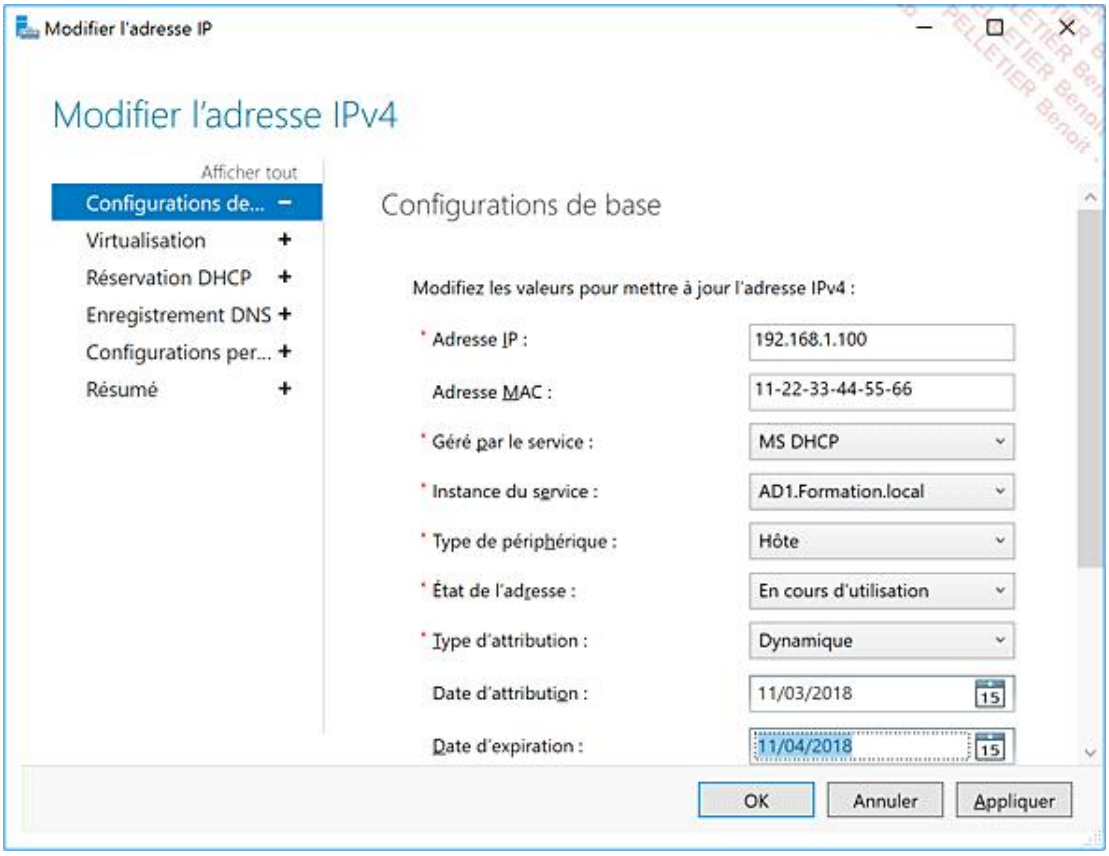
- Vérifiez la présence de la réservation dans la console DHCP.



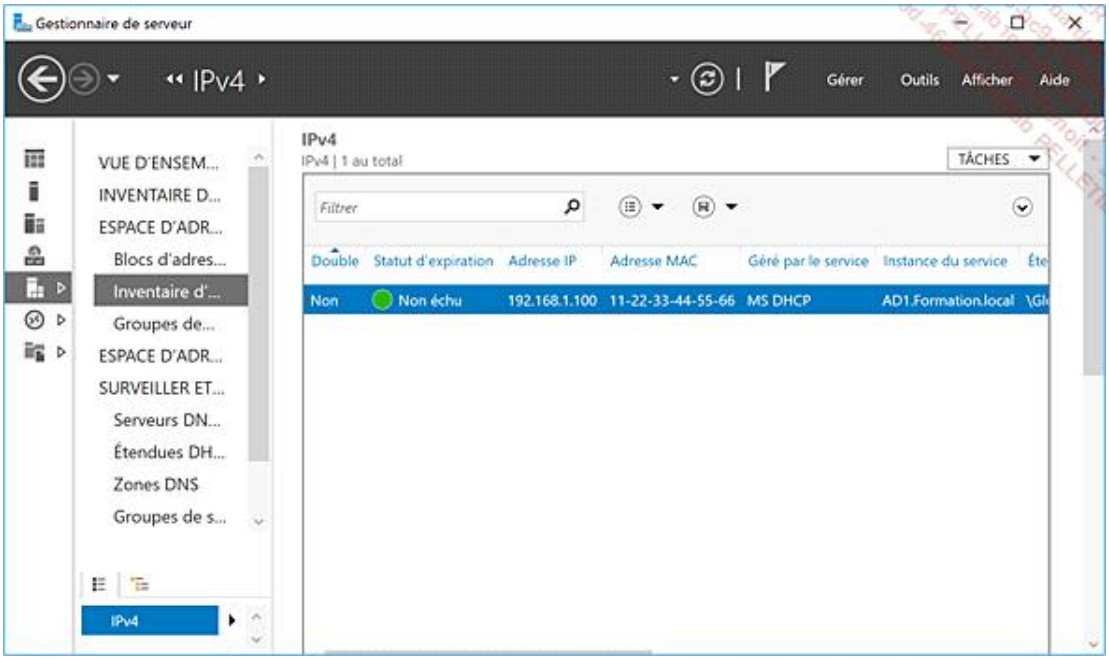
- Vérifiez aussi la présence de l'enregistrement d'hôtes dans le DNS.
- Dans la console IPAM, effectuez un clic droit sur l'adresse IP **192.168.1.101**, puis cliquez sur **Modifier l'adresse IP**.

Dans le champ **Date d'attribution**, sélectionnez la date du jour puis, dans **Date d'expiration**, sélectionnez une date postérieure d'un mois à la date du jour et cliquez sur **OK**.

Les dates d'expiration permettent la mise en place des alertes pour les objets dans la base de données IPAM. Lorsque la date est passée, l'adresse IP sur laquelle l'alerte a été mise n'est pas supprimée des réservations dans le DHCP mais seules des alertes sont remontées par IPAM.

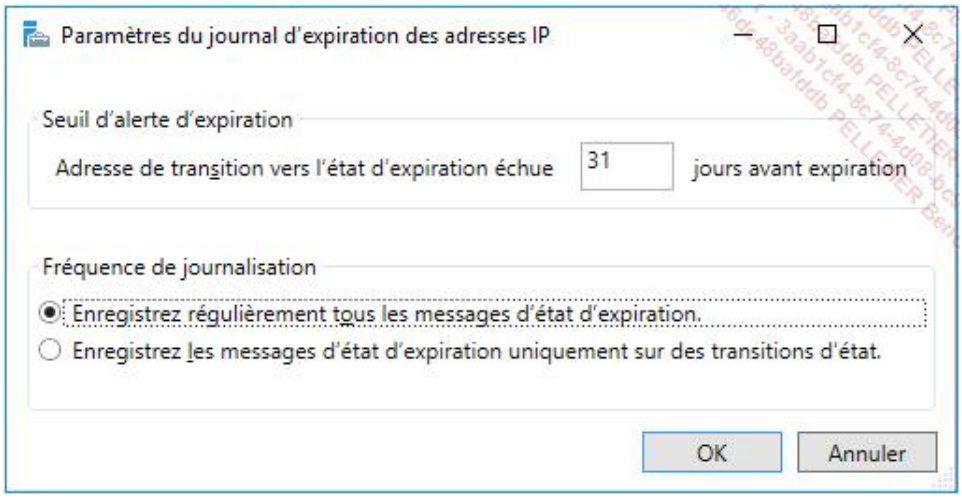


Cliquez sur **Tâches** et sélectionnez **Paramètres du journal d'expiration des adresses IP**.

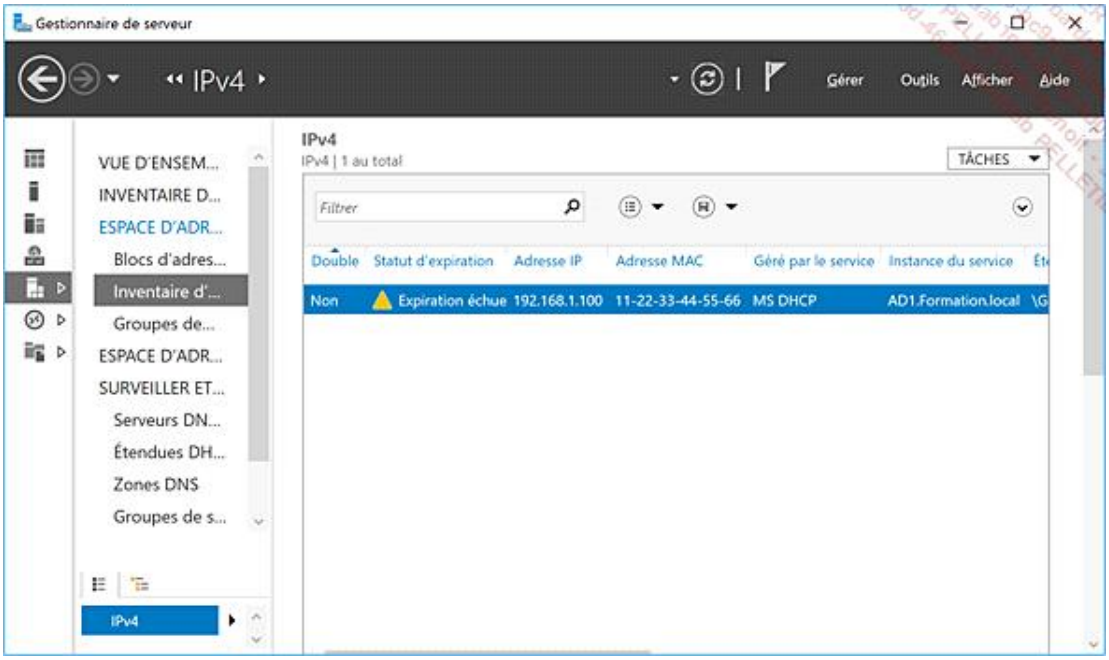


Saisissez **31** dans **Adresse de transition vers l'état d'expiration échue** puis cochez **Enregistrez**

régulièrement tous les messages d'état d'expiration.

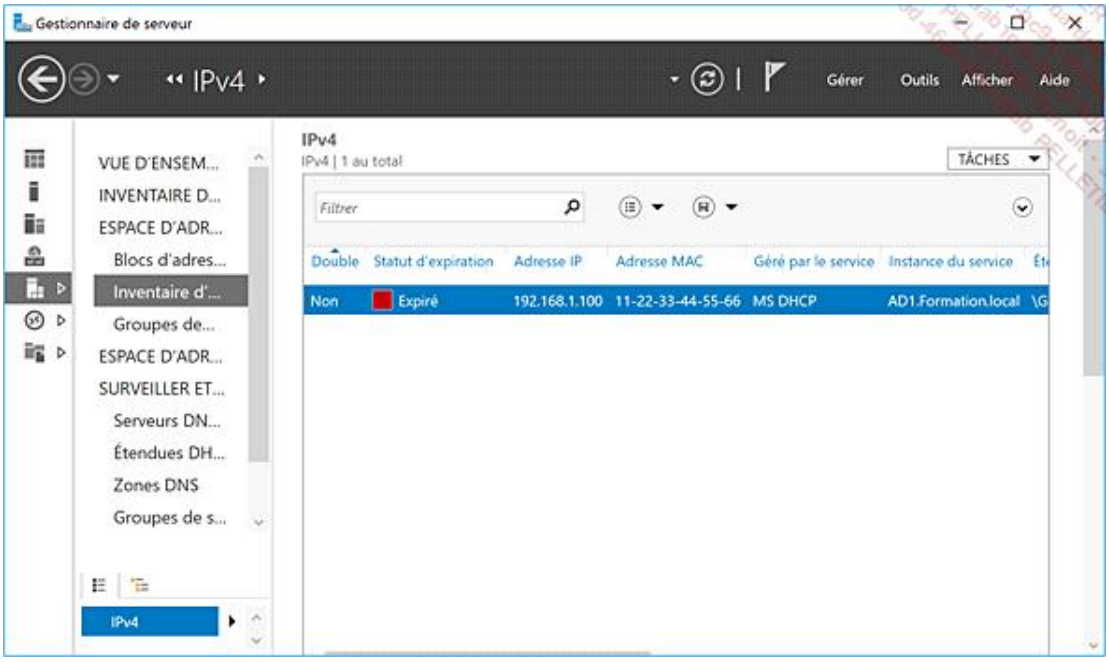


- Validez en cliquant sur **OK**.
- Actualisez la console IPAM et vérifiez la présence du statut **Expiration échue**.



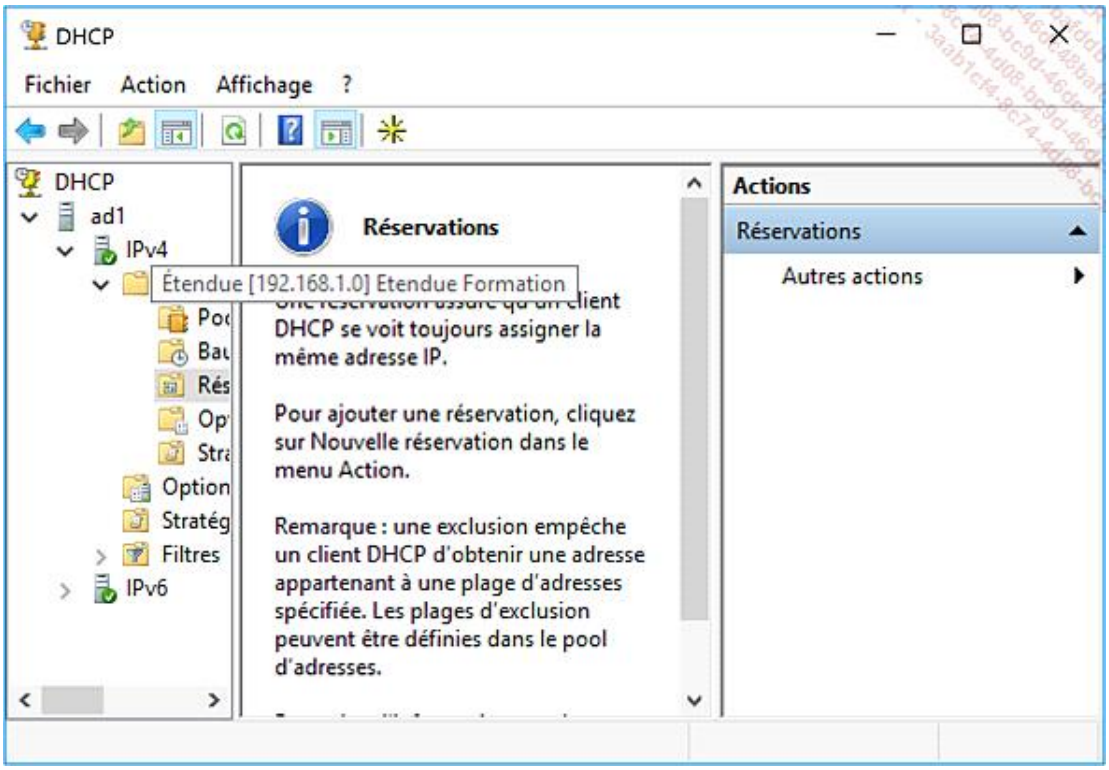
- Effectuez un clic droit sur l'adresse IP **192.168.1.101**, puis cliquez sur **Modifier l'adresse IP**.
- Dans le champ **Date d'expiration**, sélectionnez la date du jour et cliquez sur **OK**.

  Le statut de l'adresse est maintenant **Expiré**.



- Effectuez un clic droit sur l'adresse **192.168.1.100**, puis cliquez sur **Supprimer la réservation DHCP**.

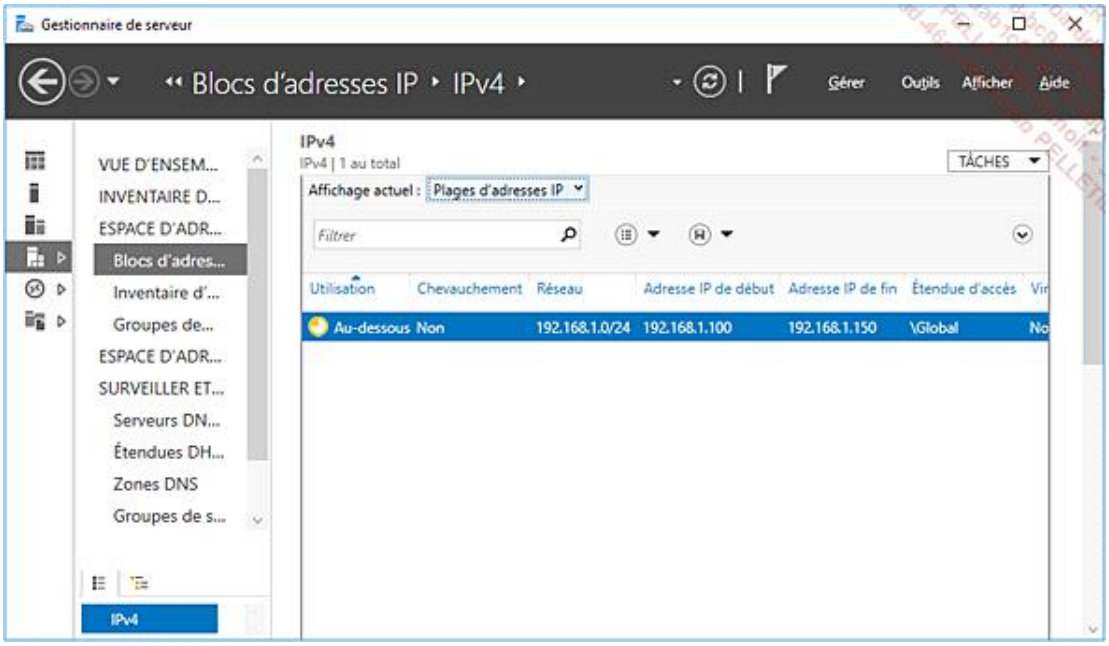
  La réservation DHCP n'est plus présente dans la console DHCP.



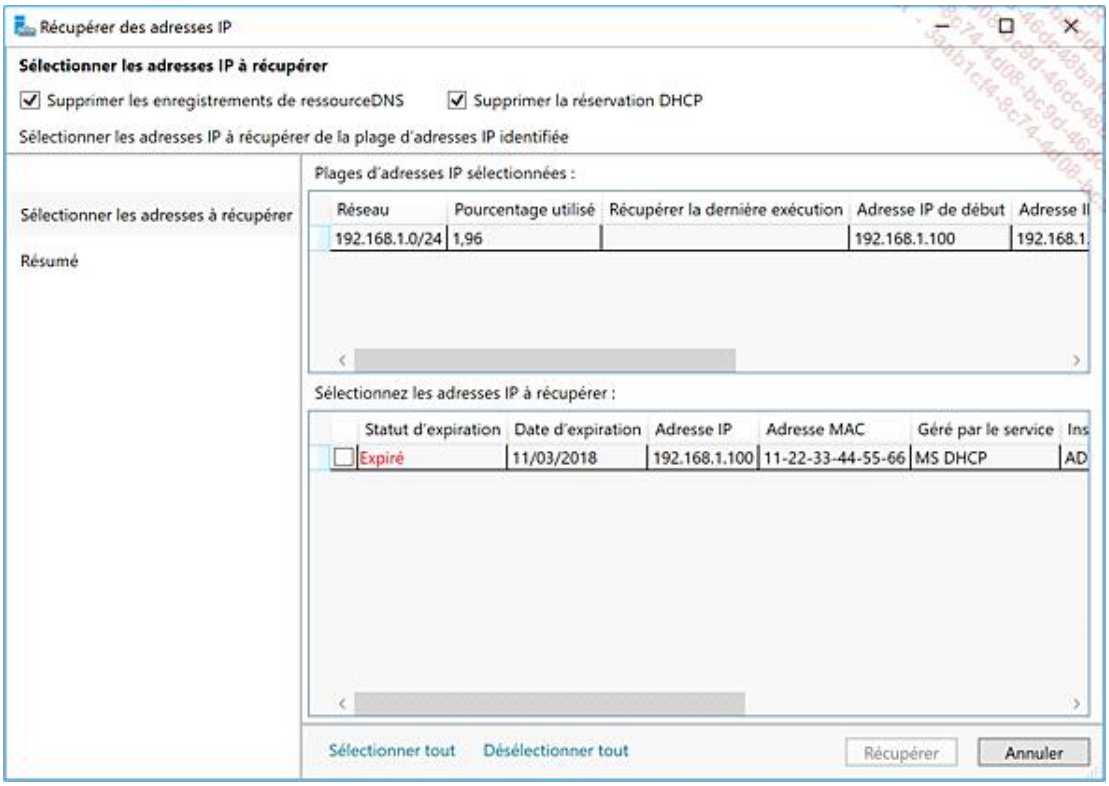
- Recommencez l'opération en sélectionnant cette fois **Supprimer un enregistrement d'hôte DNS**.

  L'enregistrement est également supprimé du serveur DNS.

- Cliquez sur **Blocs d'adresse IP** puis sélectionnez dans la liste déroulante **Affichage actuel** la valeur **Plages d'adresses IP**.



Effectuez un clic droit sur la plage d'adresses IP puis cliquez sur **Récupérer les adresses IP**.



Cochez l'adresse **192.168.1.100**, cliquez sur **Récupérer**, puis cliquez sur **Fermer**.

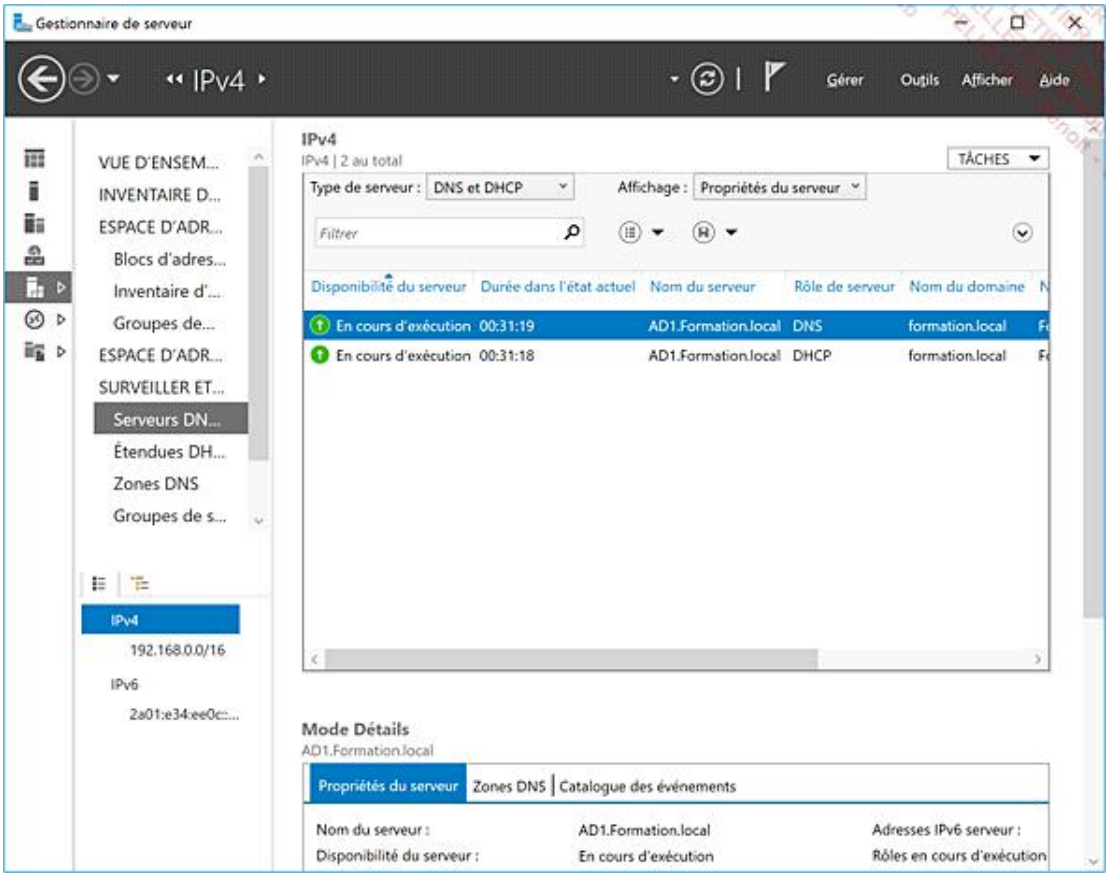
L'adresse sélectionnée est supprimée de la base de données IPAM.

5. Surveillance et gestion des serveurs DNS et DHCP

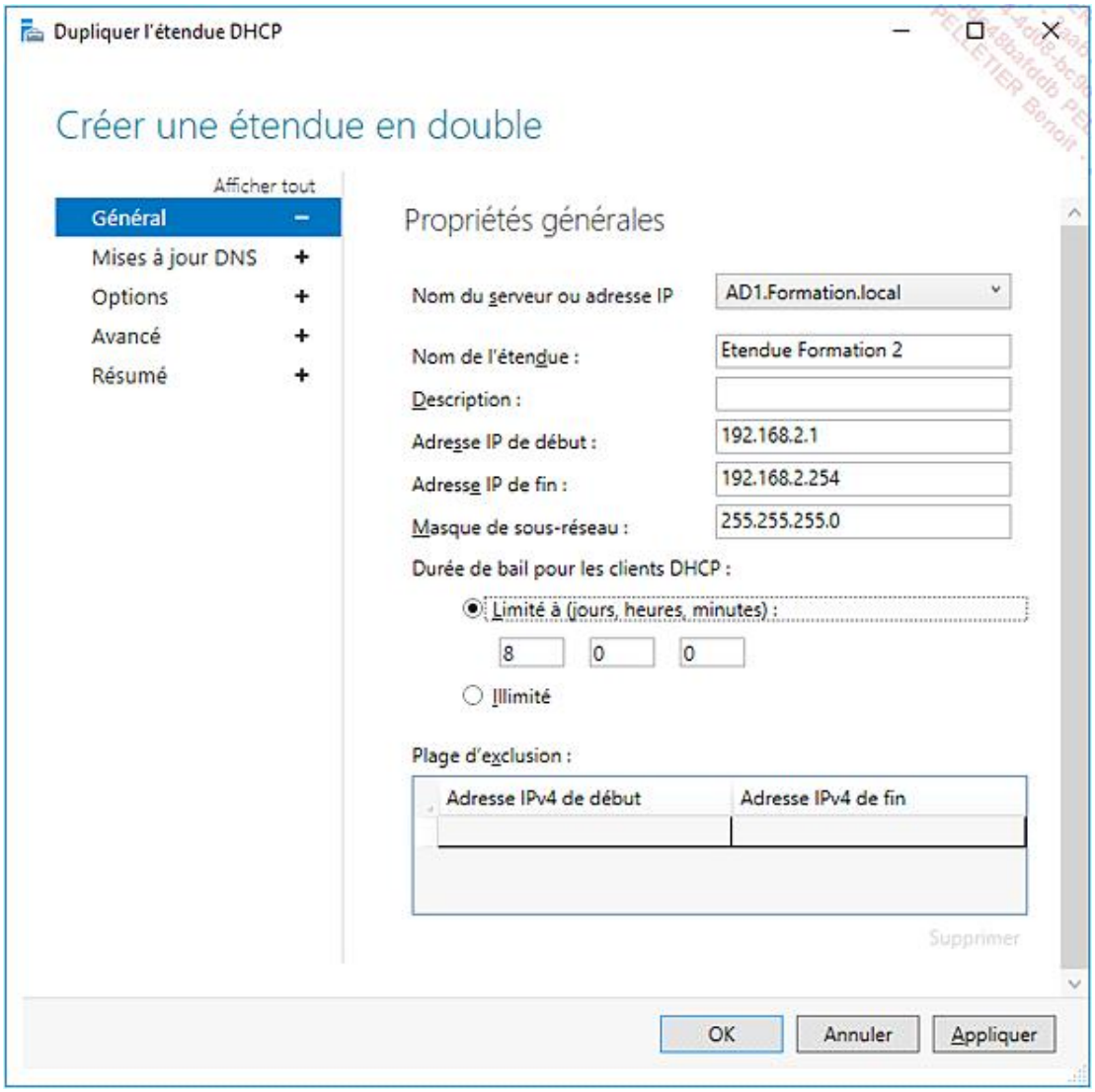
Sélectionnez le nœud de la console **SURVEILLER ET GÉRER** puis cliquez sur **Serveurs DNS et DHCP**.

Il est possible de sélectionner un des deux rôles ou de surveiller DNS et DHCP. La console montre le nom du serveur, le nom de domaine, son adresse IP…

- Cliquez sur une des deux lignes puis dans **Mode Détails**, visualisez les informations fournies.



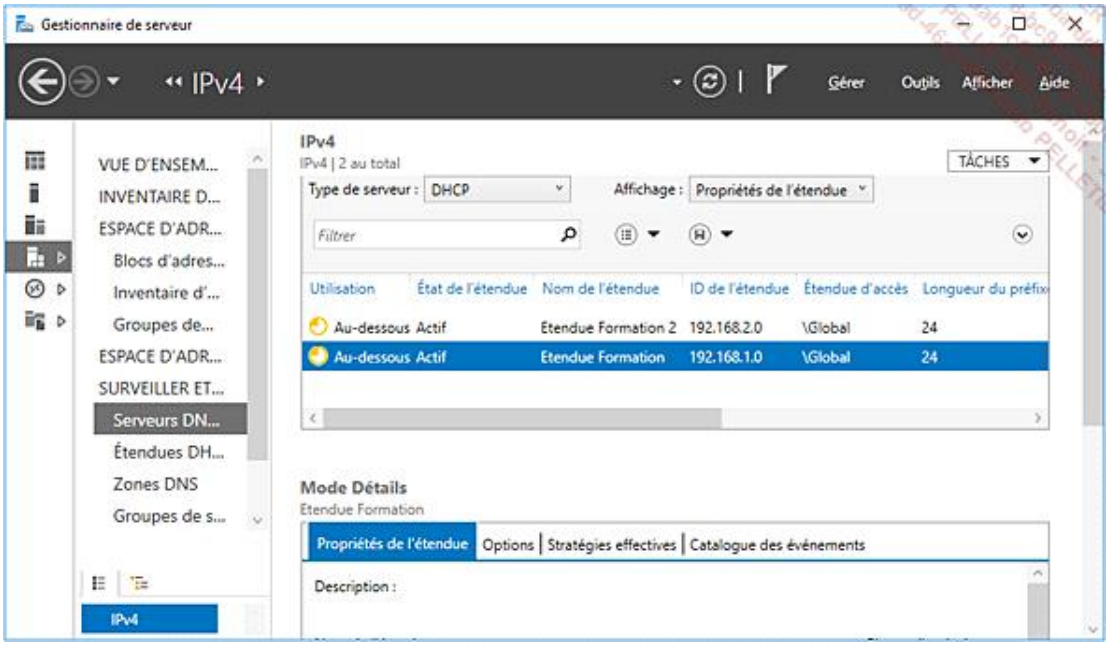
- Cliquez avec le bouton droit sur le serveur DHCP. La configuration du serveur DHCP peut être faite depuis la console IPAM.
- Configurez les listes déroulantes **Type de serveur** et **Affichage** comme ci-dessous :
  - Type de serveur : DHCP
  - Affichage : Propriétés de l'étendue.
- Effectuez un clic droit sur l'étendue DHCP puis cliquez sur **Dupliquer l'étendue DHCP**.
- Modifiez la valeur du champ **Nom de l'étendue** par **Etendue Formation 2**.
- Configurez le reste de la fenêtre comme ci-dessous :
  - Adresse IP de début : 192.168.2.1
  - Adresse IP de fin : 192.168.2.254
  - Masque de sous-réseau : 255.255.255.0



Vérifiez les nœuds **Mises à jour DNS**, **Options** et enfin **Avancé**.

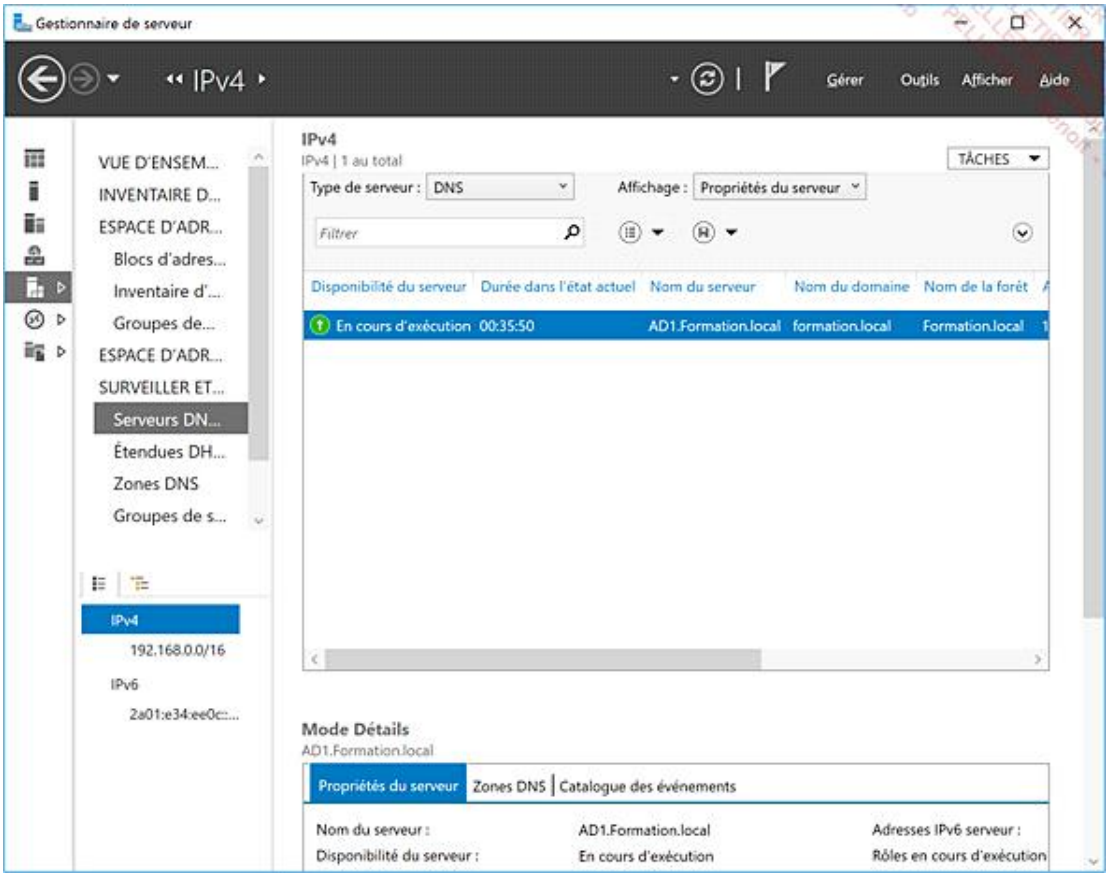
Les propriétés de l'étendue sont configurées de la même manière que les propriétés de celle qui a servi de modèle.

Cliquez sur **OK** et vérifiez la présence d'une nouvelle étendue DHCP dans la console.



L'étendue doit avoir l'état **Actif**.

- Sélectionnez les deux étendues puis, à l'aide d'un clic droit sur la sélection, cliquez sur **Modifier l'étendue DHCP**.
- Développez le nœud **Options** et sélectionnez **Ajouter** dans **Action de configuration**.
- Cliquez sur le bouton **Nouveau**.
- Sélectionnez l'option **003 Routeur**.
- Saisissez **192.168.1.254** dans le champ **Nom du serveur**.
- Cliquez sur **Résoudre** puis sur **OK**.
- Dans la liste déroulante **Type de serveur**, sélectionnez **DNS**.



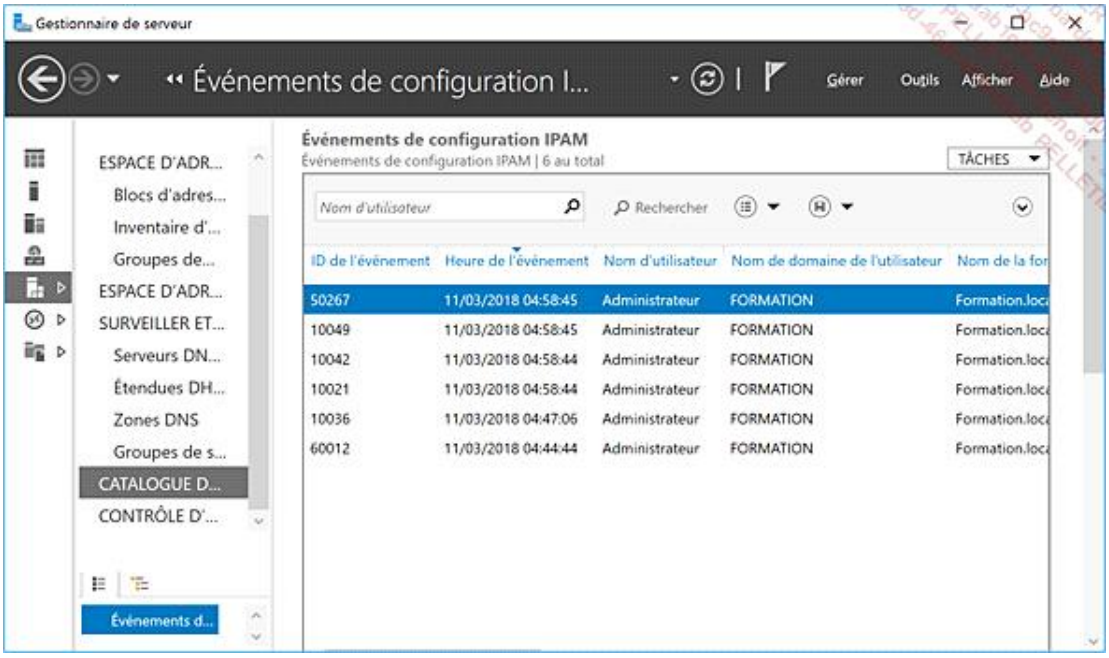
- Examinez les informations présentes sous les onglets **Propriétés du serveur**, **Zones DNS** et **Catalogue des événements**.
- Effectuez un clic droit sur **AD1.Formation.local** et sélectionnez l'option **Lancer la console MMC**.

  La console DNS s'affiche.

6. Consultation des journaux et événements d'audit

IPAM permet d'effectuer un suivi des événements des serveurs DNS et DHCP.

- Cliquez sur le nœud **CATALOGUE DES ÉVÉNEMENTS** de la console IPAM.



- Cliquez sur **TÂCHES**, puis sur **Exporter**.

Les événements peuvent être exportés dans un fichier CSV.

Attribution fondée sur une stratégie

1. Introduction

Cette fonctionnalité apparue avec Windows Server 2012 permet d'effectuer une administration ciblée et de contrôler les paramètres de configuration fournis à une interface réseau.

Une stratégie est composée d'un ensemble de conditions, ces dernières sont évaluées lors de la demande des clients. Ainsi, cette fonctionnalité permet de mettre en place les scénarios suivants :

- **Types de périphériques multiples** : les différents périphériques d'un réseau (imprimantes, téléphone sur IP...) sont classés par plage d'adresses IP.
- **Rôles multiples** : il est possible de fournir différents paramètres de bail en fonction du type d'ordinateur (ordinateur de bureau, ordinateur portable…). Comme l'attribution d'une durée de bail différente pour un ordinateur de bureau ou un ordinateur portable.

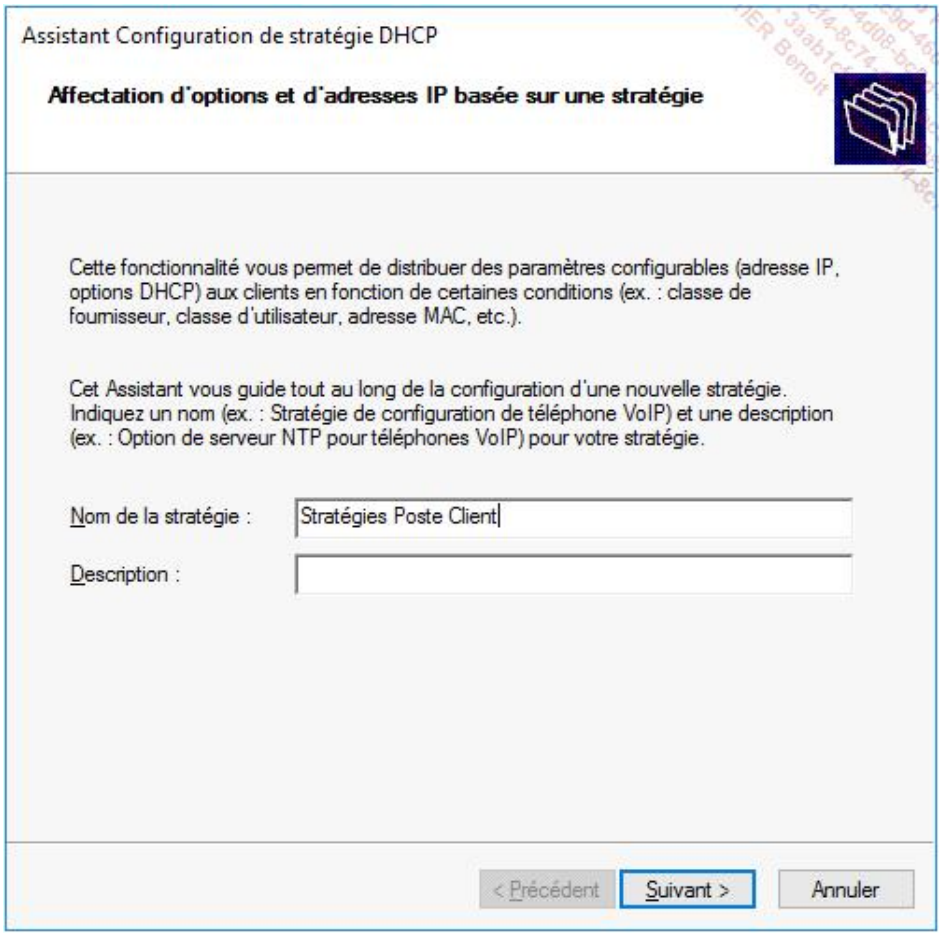
Le serveur DHCP peut être composé de stratégies au niveau de l'étendue ou au niveau du serveur.

2. Attribution d'adresses

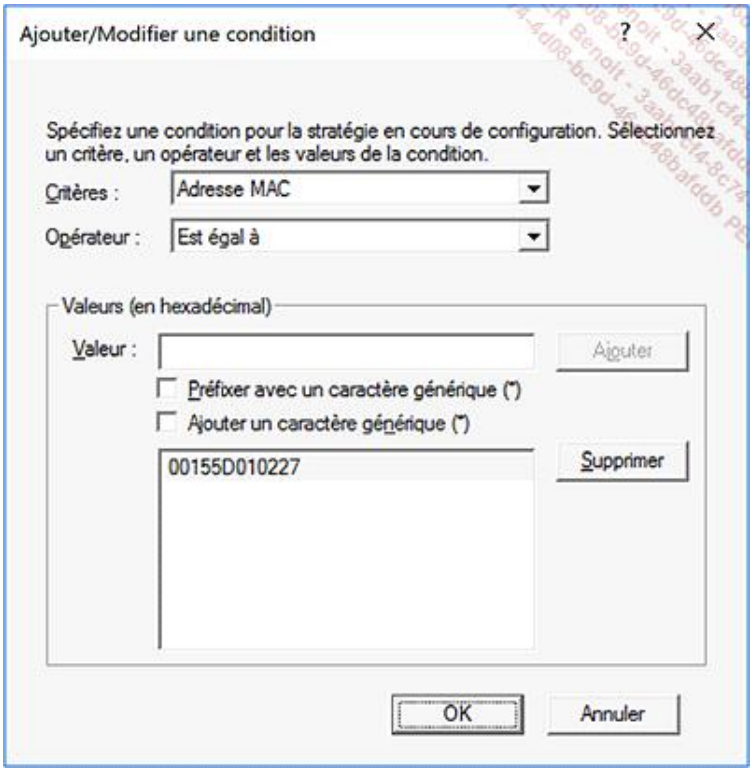
Lors de la réception d'une demande de bail, le serveur DHCP doit déterminer l'étendue du client. L'adresse IP, l'agent de relais ou simplement l'interface du serveur DHCP sur lequel le paquet est reçu permettent de déterminer cette étendue.

Par la suite, le serveur vérifie les stratégies applicables à l'étendue (configurées au niveau de l'étendue ou héritées du serveur) afin d'effectuer l'attribution d'une adresse. Néanmoins, si aucune stratégie ne correspond à la demande, le serveur distribue une adresse IP configurée pour l'étendue (les adresses IP spécifiées dans les stratégies ne pourront être allouées).

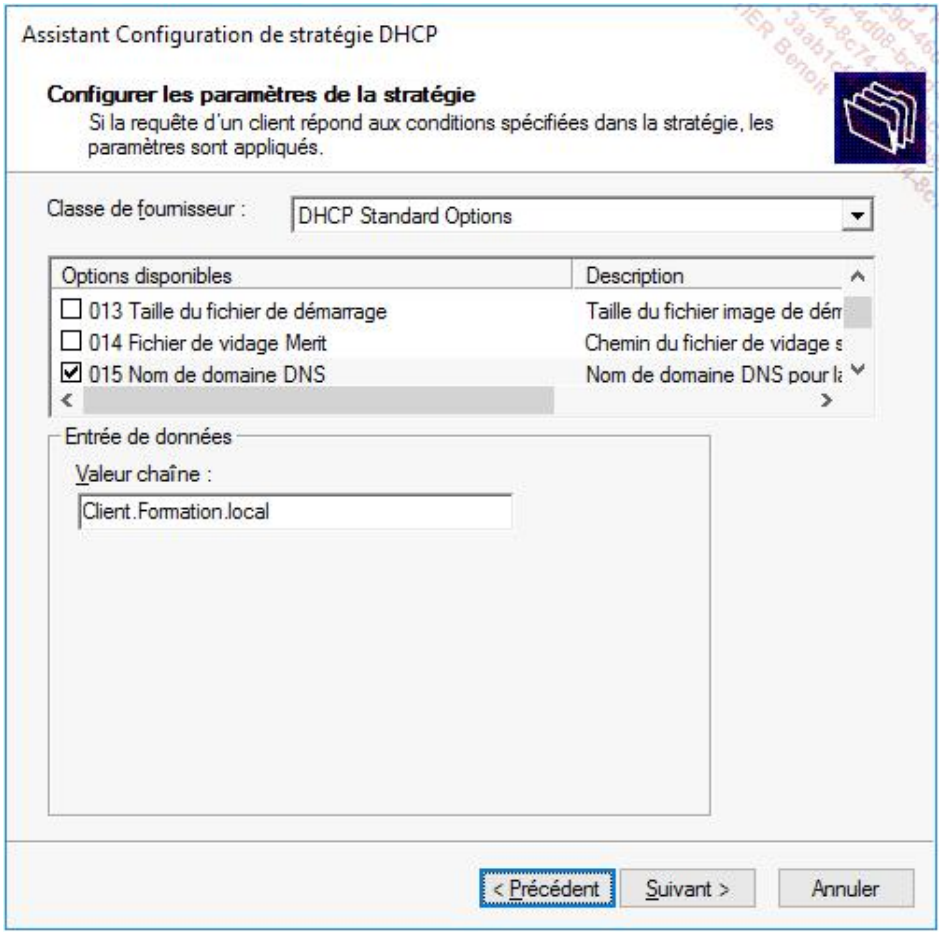
- Sur le poste CL10-01, saisissez la commande `ipconfig /all` afin de récupérer l'adresse MAC du poste.
- Sur AD1, lancez la console DHCP puis effectuez un clic droit sur **Stratégies** au niveau de l'étendue.
- Dans le menu contextuel, cliquez sur **Nouvelle Stratégie**.
- Saisissez **Stratégies Poste Client** dans le champ **Nom de la stratégie** puis cliquez sur **Suivant**.



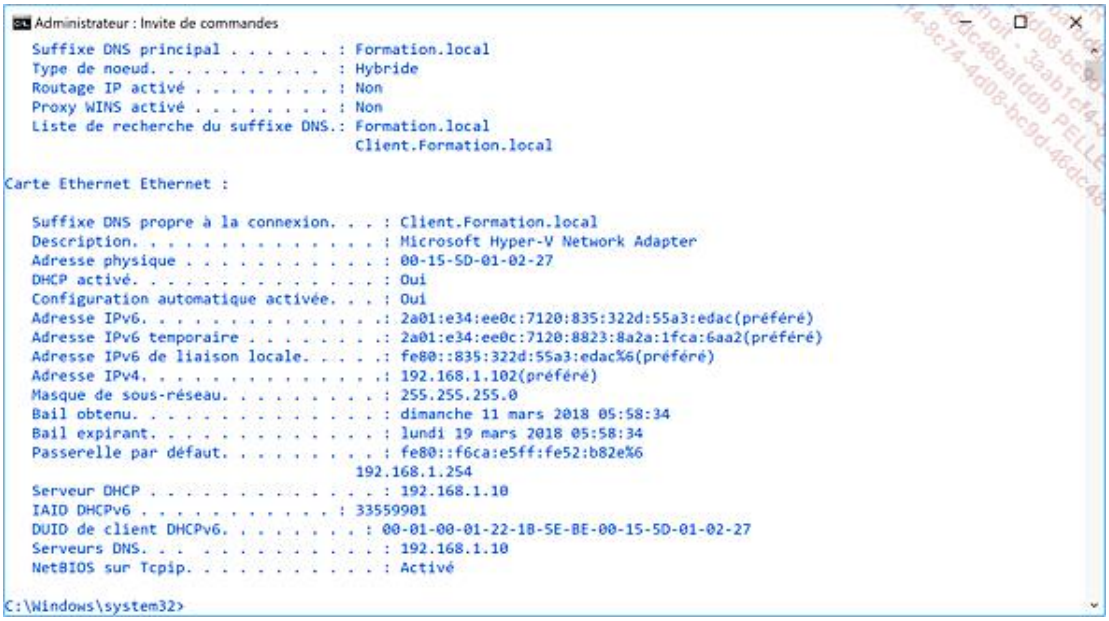
- Dans la fenêtre **Configurer les conditions de la stratégie**, cliquez sur le bouton **Ajouter**.
- Dans la liste déroulante **Critères**, sélectionnez **Addresse MAC** puis saisissez l'adresse MAC du poste CL10-01 dans le champ **Valeur**.



- Cliquez sur le bouton **Ajouter**, puis sur **OK**.
- Cliquez sur **Suivant**.
- Dans la fenêtre **Configurer les paramètres de la stratégie**, cochez l'option **015 Nom de domaine DNS**.
- Saisissez **Client.Formation.local** dans le champ **Valeur chaîne** puis cliquez sur **Suivant**.



- Cliquez sur **Terminer** pour créer la stratégie.
- Sur le poste CL10-01, lancez une invite de commandes DOS puis saisissez `ipconfig /release` afin de libérer le bail DHCP.
- Saisissez maintenant `ipconfig /renew`. Le poste va effectuer une demande de bail au serveur DHCP, puis entrez `ipconfig /all` afin de l'afficher.



Le nom de domaine DNS correspond bien à celui configuré dans la stratégie.

Introduction à l'adressage IPv4

Depuis la création d'ARPANET, beaucoup de normes ont vu le jour. En 1981 IPv4 est créé (RFC 791).

1. Le modèle OSI

Le modèle OSI (*Open Systems Interconnection*) inventé par l'ISO (*International Standards Organization*) est un modèle de communication entre ordinateurs. Il décrit les fonctionnalités nécessaires à la communication.

Il est composé de sept couches, qui ont chacune une utilité différente.

- **Couche application** : elle apporte les services de base offerts par le réseau, comme le transfert de fichier, la messagerie…
- **Couche présentation** : sa principale fonction est de s'intéresser à la syntaxe et à la sémantique des données transmises. L'information est traitée de manière à la rendre compatible entre les différentes entités qui communiquent.
- **Couche session** : elle organise et synchronise les échanges entre l'émetteur et le récepteur.
- **Couche transport** : cette couche est responsable du bon acheminement des messages. Son rôle est la récupération des messages de la couche session, et le découpage en unités plus petites. Par la suite elle peut procéder à la transmission à la couche réseau. L'optimisation des ressources ainsi que le contrôle de flux est également à sa charge.
- **Couche réseau** : elle permet la création des sous-réseaux et le routage des paquets sur ces derniers. L'interconnexion des sous-réseaux est également effectuée par cette couche.
- **Couche liaison de données** : elle permet d'effectuer le fractionnement des données d'entrée de l'émetteur en trames. Par la suite ces dernières sont transmises en séquences. Elle a également à sa charge la gestion des trames d'acquittement renvoyées par le récepteur.

  Un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Pour éviter l'engorgement du récepteur, le contrôle de flux est intégré à la couche liaison.
- **Couche physique** : cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit être un bit 1 à la réception) via le canal de transmission.

2. Les équipements du réseau

Un réseau informatique consiste à relier entre elles plusieurs machines qui souhaitent communiquer et s'échanger des données. Pour effectuer la mise en place du lien, un commutateur (switch) ou, plus ancien, un répéteur (hub) peut être utilisé.

Un hub a pour fonction de renvoyer sur chacun de ses ports une trame reçue (si une trame est envoyée sur le port 1, alors une retransmission est effectuée sur l'ensemble des autres ports). Une multitude d'équipements reçoivent une trame qui ne leur est pas destinée, cela pose des problèmes de sécurité et de bande passante utilisée. Cet équipement a l'avantage de réamplifier le signal, il est présent sur la couche 1 du modèle OSI.

Le switch ou commutateur effectue, contrairement au répéteur, un transfert de la trame reçue sur le port de la machine destinatrice. Ainsi seul le récepteur reçoit la trame. Le switch se situe sur la couche 2 du modèle OSI, il utilise une table de commutation pour transmettre la trame au destinataire.

Le routeur a une fonction différente des deux premiers, son but est de relier deux réseaux différents afin qu'ils puissent communiquer. Pour effectuer les opérations de routage (opération qui consiste à envoyer les trames vers un autre réseau), il est nécessaire de configurer des tables de routage. Sans ces dernières, le routeur n'a pas la possibilité de fonctionner. Contrairement au switch (sauf ceux de niveau 3), le routeur gère les trames en fonction de l'adresse IP du destinataire (adresse MAC pour le switch).

Ces différents équipements sont essentiels de nos jours et nous permettent d'effectuer les diverses actions quotidiennes (envoi de mail, surf sur Internet...).

3. Le routage

Nous venons de voir les différents équipements, dont le routeur qui permet de relier plusieurs réseaux entre eux. En effet, de nos jours le monde informatique ne peut pas fonctionner sans la présence de routeurs. Sans ce type d'équipement, les postes de travail n'ont pas la possibilité de sortir du réseau local.

Lorsqu'une machine tente de communiquer, elle doit d'abord déterminer si la machine destinatrice est sur le même réseau qu'elle. Pour cela, elle utilise l'ID réseau qui va lui permettre de savoir si la machine est présente sur le réseau local ou sur un réseau distant. Dans ce dernier cas, la trame est envoyée à la passerelle par défaut (routeur) configurée dans l'adressage IP de la machine cliente.

Le routeur contient une table de routage qui lui indique le chemin à prendre pour arriver à la destination souhaitée (exemple : pour atteindre le réseau 172.22.0.0, la trame doit être envoyée à 172.22.1.150).

Deux types de routage existent :

- Le routage statique : les tables de routage sont saisies à la main sur l'ensemble des routeurs. Lorsqu'une route est modifiée ou supprimée, une reconfiguration des tables de routage est nécessaire.
- Le routage dynamique : il n'est plus nécessaire d'effectuer la configuration de tous les routeurs. Ces derniers vont automatiquement s'échanger leur table de routage, ainsi une opération de modification ou de suppression est répercutée sur tous les autres routeurs. Il est nécessaire d'utiliser des protocoles de routage (RIP, OSPF…) pour le routage dynamique.

4. Le réseau WAN

Il n'est pas possible de parler de routage sans aborder les réseaux WAN (*Wide Area Network* - zone de réseau étendu). Ce type de réseau est très utilisé par les particuliers et les professionnels. Internet est un réseau WAN car il relie des serveurs présents sur chaque continent, tous les particuliers qui accèdent à Internet utilisent ce réseau. Les entreprises s'en servent également pour relier les différents sites.

Il est fréquent de voir des entreprises implantées dans plusieurs pays ou plusieurs continents. Pour relier les différentes agences entre elles, des liens spécialisés sont utilisés (SDSL, etc.).

Un réseau WAN est tout simplement une succession d'équipements (routeurs principalement) qui permettent de relier deux réseaux locaux entre eux.

5. Adressage IPv4

IPv4, normalisé en septembre 1981 sous la RFC 791, permet d'attribuer à chaque interface d'un hôte (poste de travail, smartphone,…) une adresse. Codées sur 32 bits, les adresses peuvent être rangées dans 3 classes.

La classe A qui permet d'adresser 16 777 216 machines soit 2^{24}. Un octet est réservé à l'identification du réseau, les trois autres octets sont réservés à l'identification des machines hôtes (exemple : 10.0.0.0).

Valeur miminum du 1er octet	Valeur décimale du 1er octet	Valeur maximum du 1er octet	Valeur décimale du 1er octet	Masque de sous-réseau
0000 0001	1	0111 1111	127	255.0.0.0

Les adresses IP de classe A varient de 1.0.0.0 à 126.255.255.255 (127 étant une valeur réservée). Le masque de classe A est lui égal à 255.0.0.0.

La classe B est capable d'adresser 65 536 machines soit 2^{16}, avec 2 octets pour l'ID réseau et 2 octets pour l'ID hôte.

Valeur miminum du 1er octet	Valeur décimale du 1er octet	Valeur maximum du 1er octet	Valeur décimale du 1er octet	Masque de sous-réseau
10000 000	128	1011 1111	191	255.255.0.0

Les adresses IP de classe B varient de 128.0.0.0 à 191.255.255.255 et le masque de classe B est 255.255.0.0.

La classe C est idéale pour les petits réseaux avec une possibilité d'adressage de 254 postes soit 2^8, soit 3 octets pour l'ID réseau et 1 octet pour l'ID hôte.

Valeur miminum du 1er octet	Valeur décimale du 1er octet	Valeur maximum du 1er octet	Valeur décimale du 1er octet	Masque de sous-réseau
11000 000	192	1101 1111	223	255.255.255.0

Les adresses IP de classe C varient de 192.0.0.0 à 223.255.255.255 et le masque de classe C est 255.255.255.0.

Pour pallier le risque de pénurie d'adresses IP, la norme RFC 1918 a été créée. Son but est de réserver des plages d'adresses qui ne seront pas routables sur Internet, leur seul but étant l'identification des postes dans les réseaux locaux. Chaque classe possède sa plage d'adresses privées.

- La classe A : 10.0.0.0 à 10.255.255.255
- La classe B : 172.16.0.0 à 172.31.255.255
- La classe C : 192.168.0.0 à 192.168.255.255

Introduction à l'IPv6

Pour pallier le risque de pénurie d'adresses en IPv4, un nouvel adressage a dû être implémenté. Le protocole **IPv6** a donc vu le jour et se présente en tant que successeur de l'IPv4.

1. Adressage IPv6

Une adresse IPv6 contient 128 bits (soit 16 octets, contre 4 octets pour l'IPv4), elle n'est plus représentée sous forme décimale mais sous forme hexadécimale.

Adresses en IPv6

FE80:0000:0000:0001:0200:F8FF:1F20:203F

Il est évidemment possible de la simplifier. La première étape est la réduction des 0.

F80:0:0:1:200:F8FF:1F20:203F

Ainsi une suite contiguë de zéros apparaît dans l'adresse (une suite de deux zéros dans notre exemple). Une autre simplification est donc possible, nous allons remplacer cette suite par « **::** ».

Ce remplacement ne pourra être effectué qu'une seule fois par adresse.

F80::1:200:F8FF:1F20:203F

2. Types d'adresses IPv6

Nous allons trouver plusieurs types d'adresses :

- **Adresse de bouclage** : l'adresse est de la forme ::1.
- **Adresse multicast** : cette adresse commence toujours par FF00.
- **Adresse de liaison locale** : cette adresse commence toujours par FE80.
- **Adresse globale** : correspond à toutes les adresses non citées au-dessus.

3. Indice de zone

L'adresse de liaison locale utilise un indice de zone si l'ordinateur est composé de plusieurs interfaces. Cet identifiant permet de déterminer la carte réseau utilisée pour envoyer la trame.

L'identifiant est inséré à la fin de l'adresse, il est de la forme **%<IdDeZone>**.

Adresse IP + ID de zone

F80::1:200:F8FF:1F20:203F%10

Configuration de la carte réseau

Une configuration qui contient toutes les informations nécessaires pour un bon fonctionnement de la machine sur le réseau (adresse IP, masque de sous-réseau, passerelle et serveur DNS) peut être attribuée de deux manières :

- Avec un bail DHCP : le serveur DHCP attribue un bail à une machine qui en fait demande. Il contiendra la configuration réseau (adresse IP, masque de sous-réseau, passerelle…) saisie par l'administrateur système ainsi qu'une durée de vie limitée (configurée sur le serveur DHCP).
- De manière manuelle : si aucun serveur DHCP n'est présent sur votre réseau, il est nécessaire d'effectuer la configuration des interfaces réseau à la main. Le risque de conflit IP (une même adresse saisie sur deux postes) est plus élevé avec ce choix.

1. Configuration via la ligne de commande

La commande `netsh` permet d'effectuer une multitude de paramétrages (pare-feu, interface réseau…). Ainsi il va être possible via une invite de commandes de saisir toute la configuration IP.

Les manipulations ci-dessous n'ont pas besoin d'être effectuées, ce point permet de prendre connaissance de la configuration en ligne de commande d'une carte réseau.

- Lancez une invite de commandes.
- Saisissez la commande `netsh interface ip set address Ethernet static` ***`AdresseIP MasqueSous-réseau Passerelle`***.

AdresseIP, MasqueSous-réseau et Passerelle doivent être remplacés par les valeurs souhaitées.

La commande permet de configurer l'adresse IP, le masque de sous-réseau ainsi que la passerelle pour la carte qui s'appelle Ethernet (le nom de l'adresse se trouve dans les connexions réseau).

- Vérifiez, à l'aide de la commande `ipconfig`, la configuration de la carte.
- Afin d'indiquer au poste l'adresse de son serveur, saisissez la commande `netsh interface ip set DNS Ethernet static IPServeurDNS`.

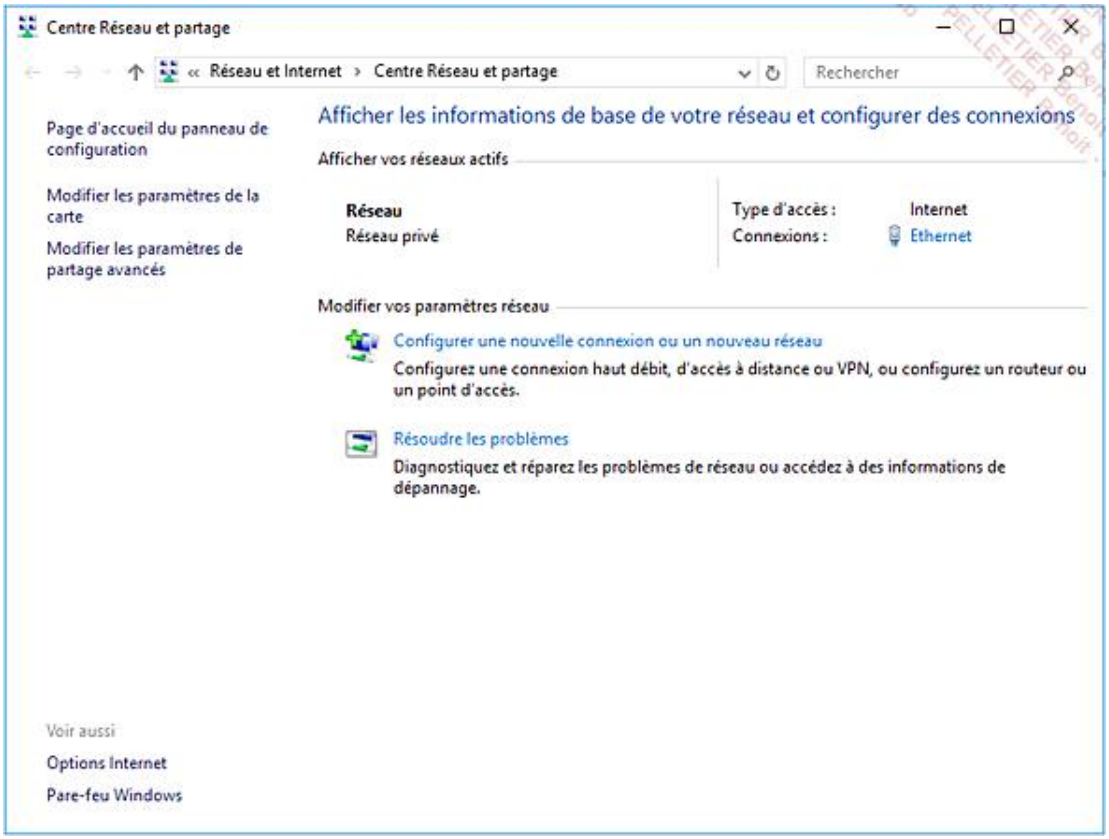
La commande permet la configuration du serveur pour la carte réseau Ethernet.

La configuration d'un serveur auxiliaire se fera également avec la commande `netsh`.

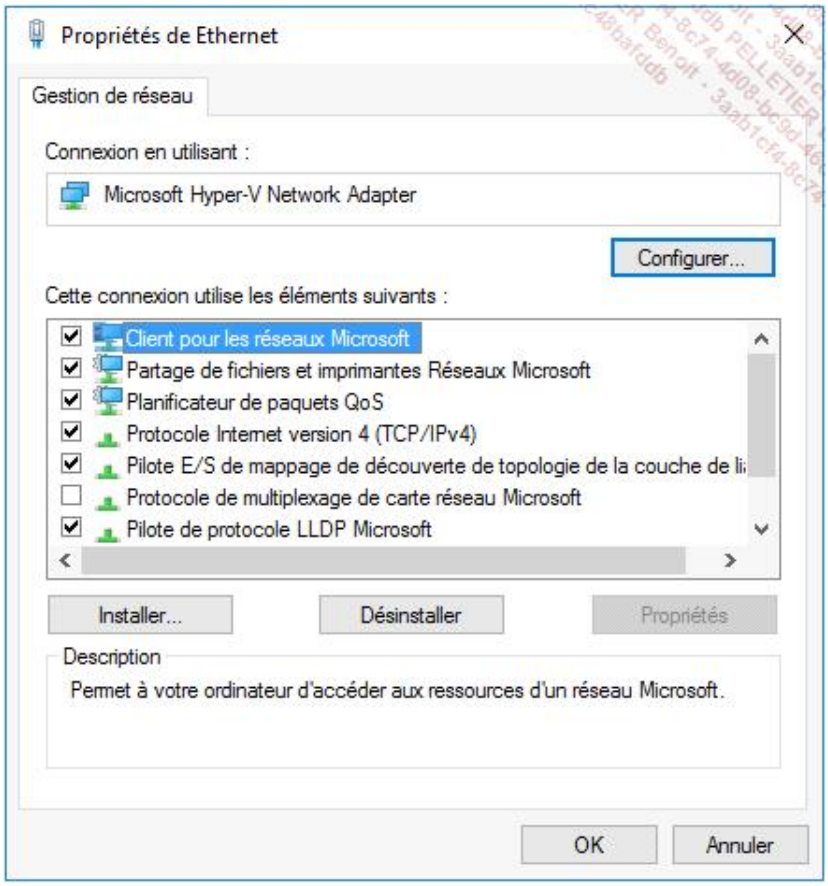
2. Configuration via l'interface graphique

La configuration via une invite de commandes est utile pour les installations minimales ou la création de scripts. Pour les autres cas, il est plus aisé de passer par l'interface graphique.

- Effectuez un clic droit sur le **Centre Réseau et partage** dans la barre des tâches et sélectionnez **Ouvrir le centre réseau et partage**.
- Dans la console, cliquez sur le lien **Modifier les paramètres de la carte** à gauche de la fenêtre.

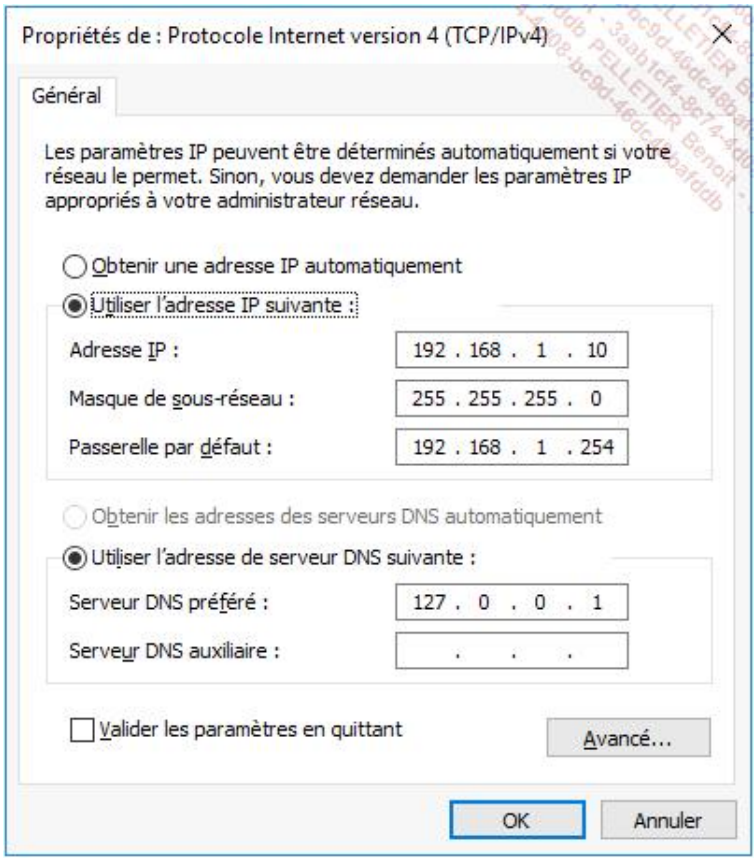


- Effectuez un clic droit sur la carte réseau puis sélectionnez **Propriétés**. Les propriétés de la carte s'affichent.



- Cliquez sur **Internet Protocol version 4 (TCP/IPv4)** puis sur **Propriétés**.

- L'interface est configurée par défaut pour un adressage automatique (adressage par l'intermédiaire du DHCP). Cliquez sur **Utiliser l'adresse IP suivante** et **Utiliser l'adresse de serveur DNS suivante**.
- Configurez la carte comme vous le souhaitez.



3. Création d'une NIC Teaming

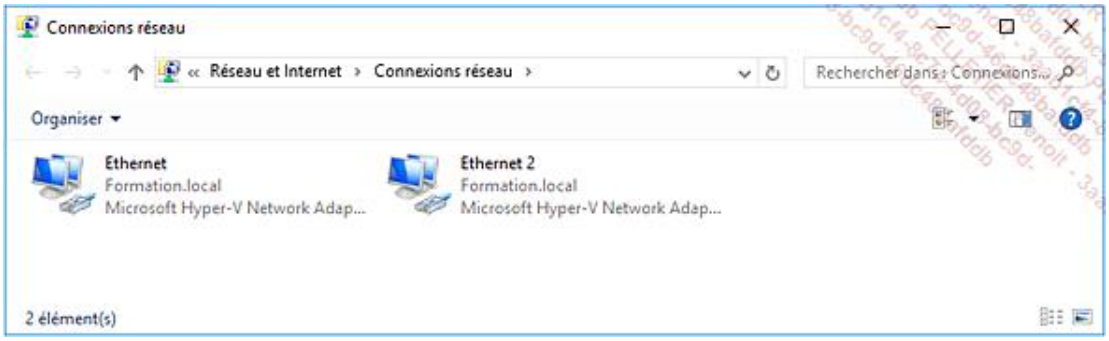
La NIC Teaming (ou association de cartes réseau) permet, depuis Windows Server 2012, de faire fonctionner deux cartes réseau ensemble et ce, même si elles sont de constructeurs différents.

Prenons l'exemple de deux cartes réseau de 1 Gbit/s ; en les associant avec la NIC Teaming, nous obtenons une carte réseau de 2 Gbit/s.

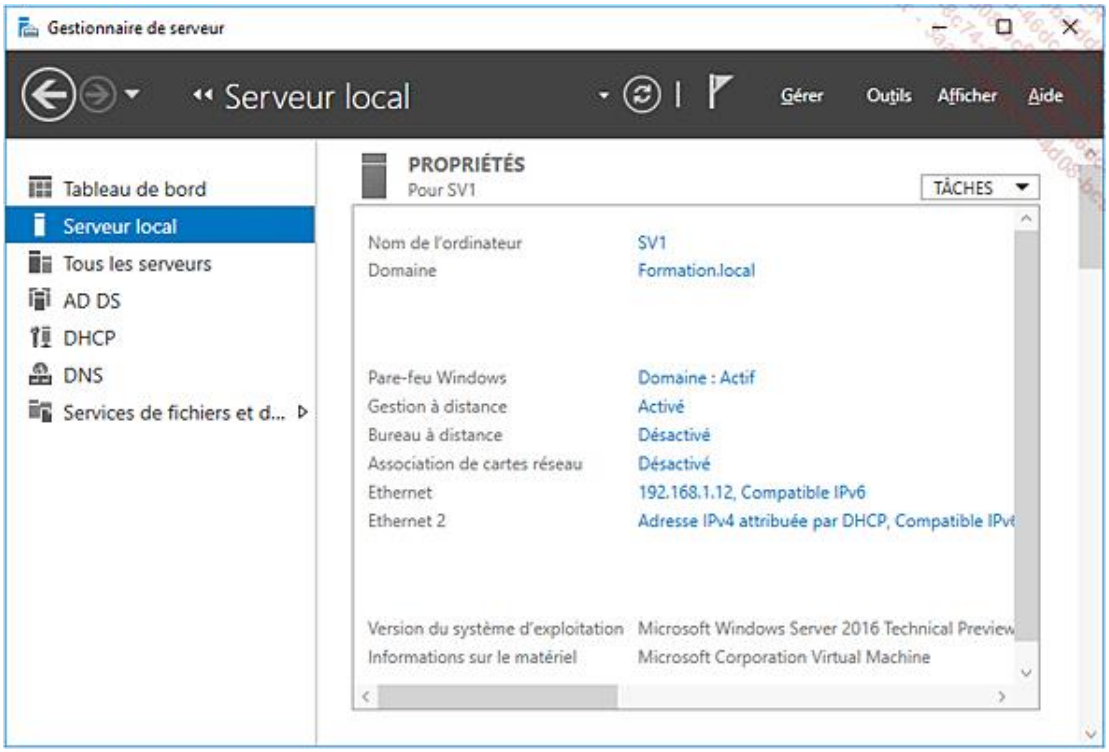
Il est impossible d'utiliser des cartes réseau virtuelles connectées à un commutateur virtuel de type privé ou interne. Ce dernier doit obligatoirement être de type externe.

De plus il n'est pas conseillé d'effectuer ce genre de paramétrage sur un contrôleur de domaine.

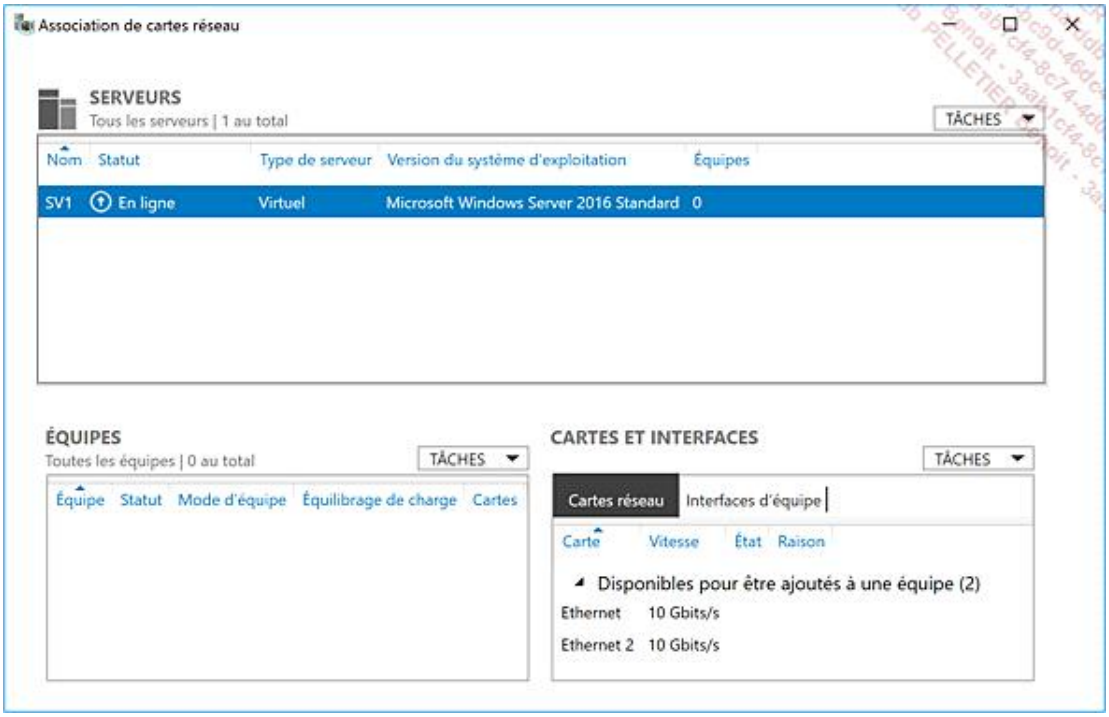
Sur SV1, une deuxième carte réseau a été ajoutée, toutes les deux sont raccordées à un commutateur virtuel de type externe.



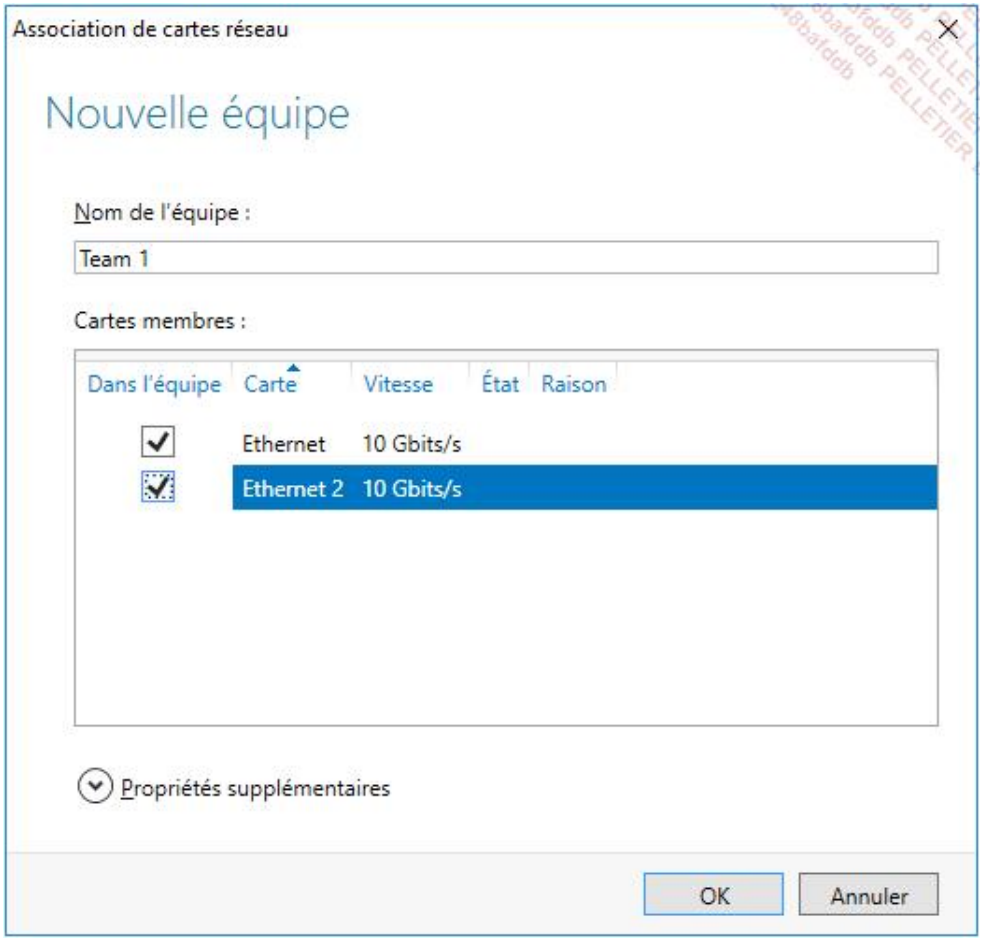
L'option permettant la création d'une association de cartes réseau est présente dans le **Gestionnaire de serveur** (**Serveur local**).



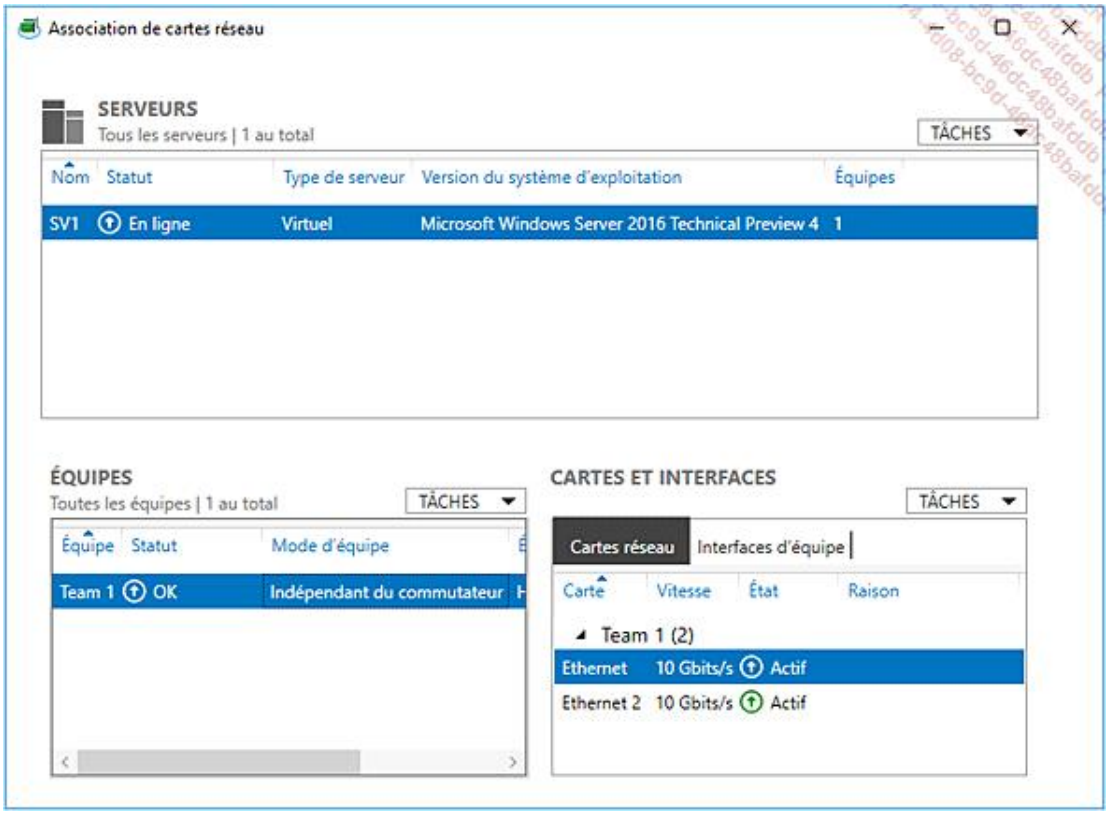
En cliquant sur le lien **Désactivé** (**Association de cartes réseau**), une fenêtre s'affiche. Dans la catégorie **ÉQUIPES**, il est nécessaire de sélectionner l'option **Nouvelle équipe** dans la liste déroulante **TÂCHES**.



Il suffit désormais de donner un nom à l'association puis de sélectionner les cartes réseau concernées.



Un meilleur débit est maintenant offert au serveur. En plus des deux cartes réseau, une nouvelle icône apparaît dans la console **Connexions réseau**. La configuration IP s'effectue par l'intermédiaire de cette nouvelle icône.



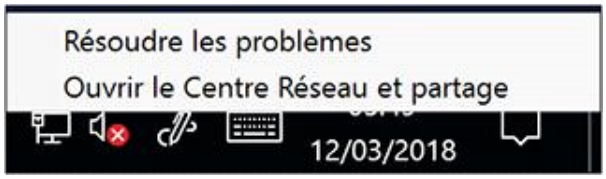
Cette fonctionnalité offre également une tolérance de panne en basculant le trafic d'une carte à l'autre si la carte venait à subir un dysfonctionnement.

Configuration du Centre Réseau et partage

Le **Centre Réseau et partage** est apparu avec Windows Vista, il permet la gestion des interfaces et connexions réseau.

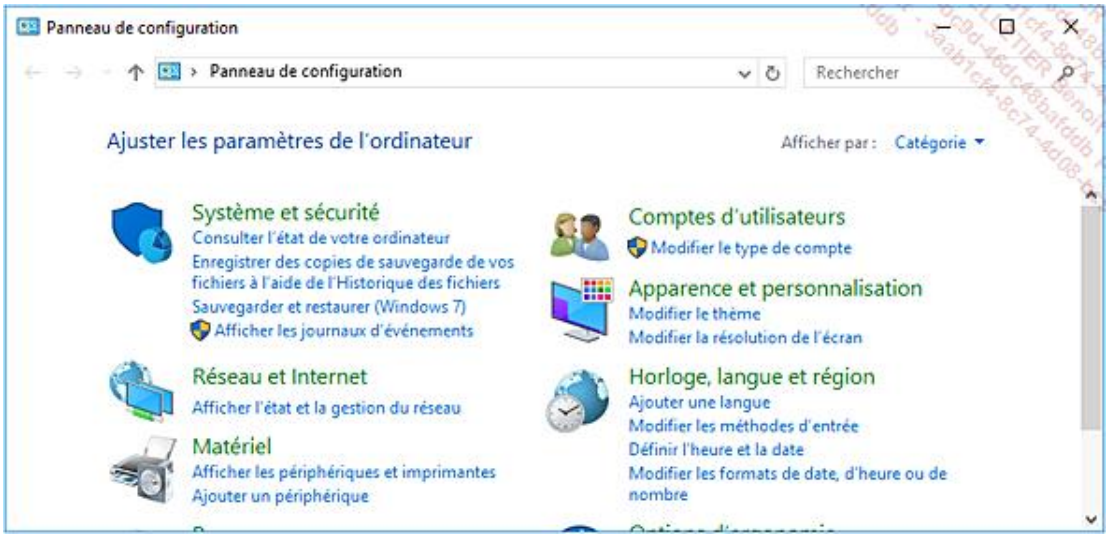
1. Ouvrir le Centre Réseau et partage

Il existe deux manières de lancer le Centre Réseau et partage. La première, en effectuant un clic droit sur l'icône dans la barre des tâches et en sélectionnant l'option **Ouvrir le Centre Réseau et partage** dans le menu contextuel.

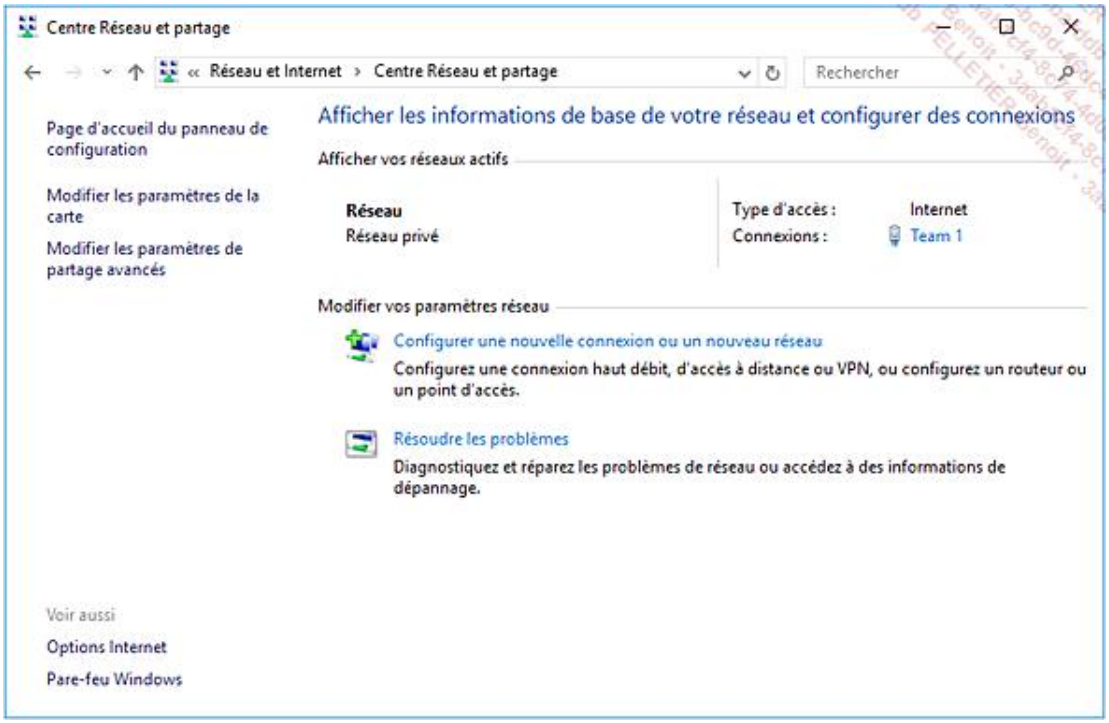


La deuxième manière consiste à passer par le panneau de configuration.

- Effectuez un clic droit sur le bouton **Démarrer**, un menu contextuel s'affiche.
- Sélectionnez l'option **Panneau de configuration**.
- Cliquez sur la catégorie **Réseau et Internet**.



- Cliquez sur **Centre Réseau et partage**.

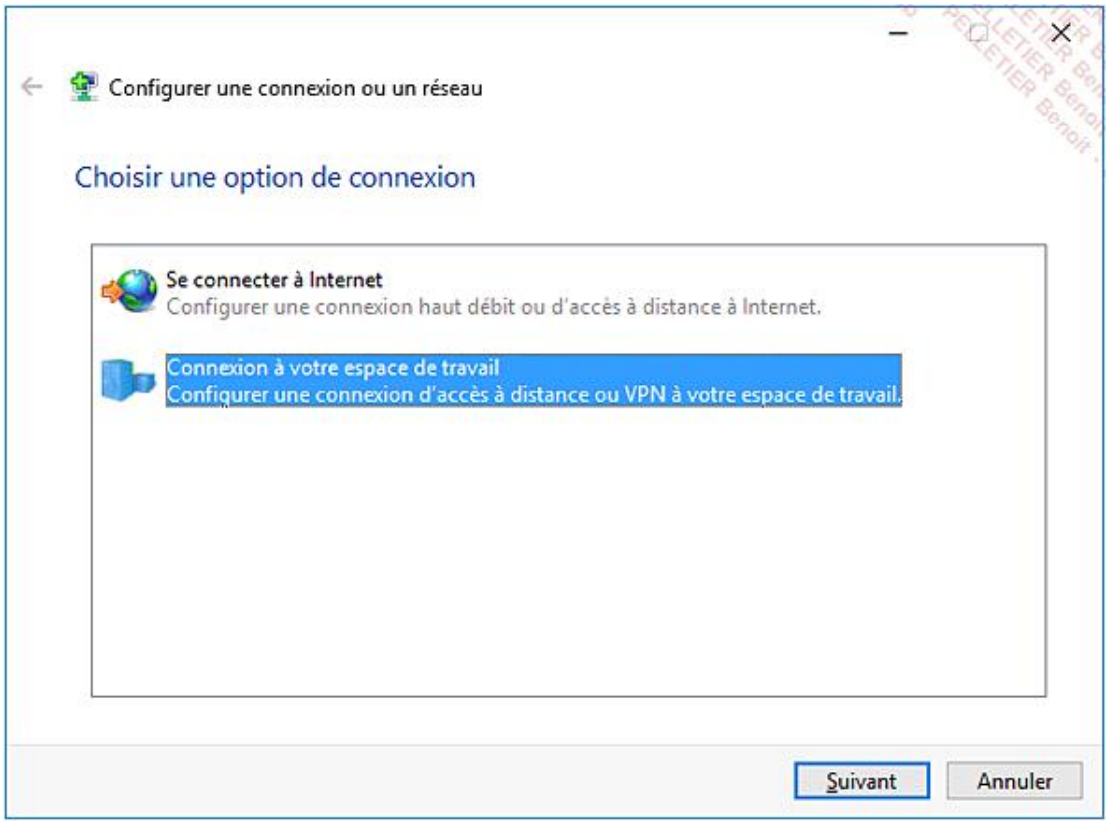


Il est désormais possible de configurer des paramètres réseau (connexion, configuration IP…) mais également d'assurer le support avec le lien **Résoudre les problèmes**.

2. Configurer une connexion réseau VPN

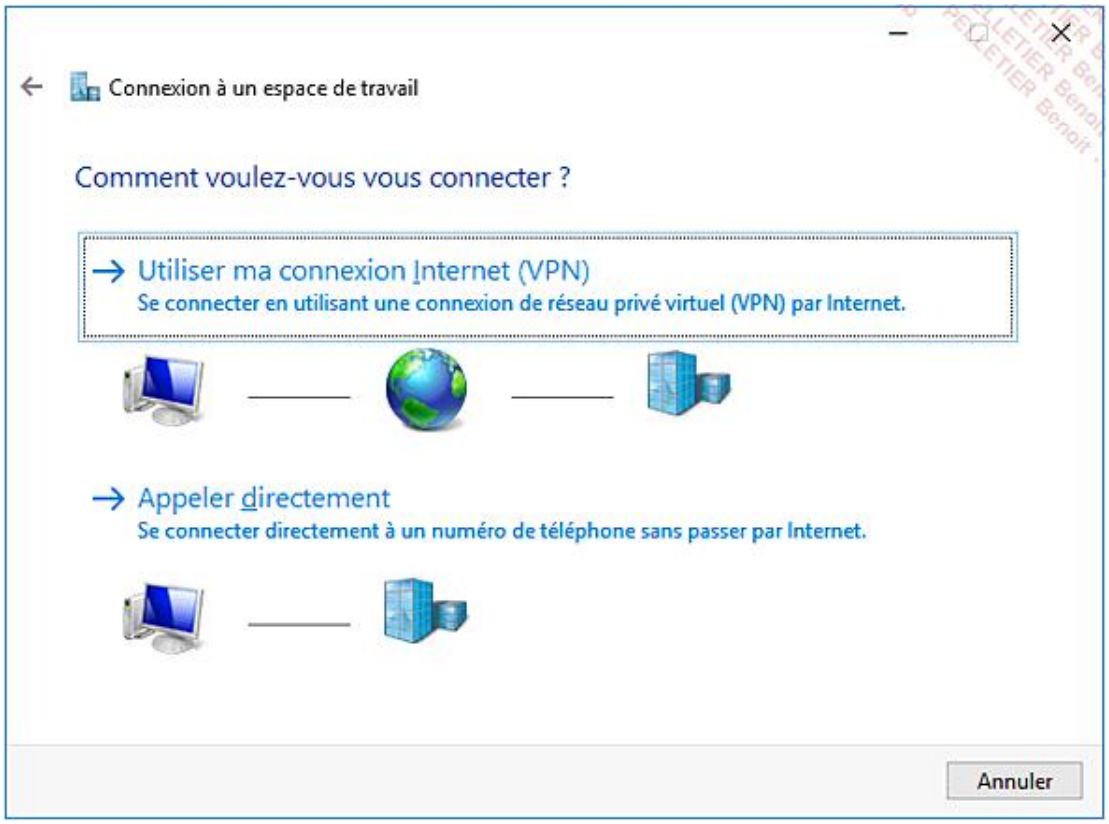
Le lien **Configurer une nouvelle connexion ou un nouveau réseau** permet la création d'une connexion à Internet ou à un réseau d'entreprise.

- Cliquez sur le lien **Connexion à votre espace de travail** puis cliquez sur **Suivant**.

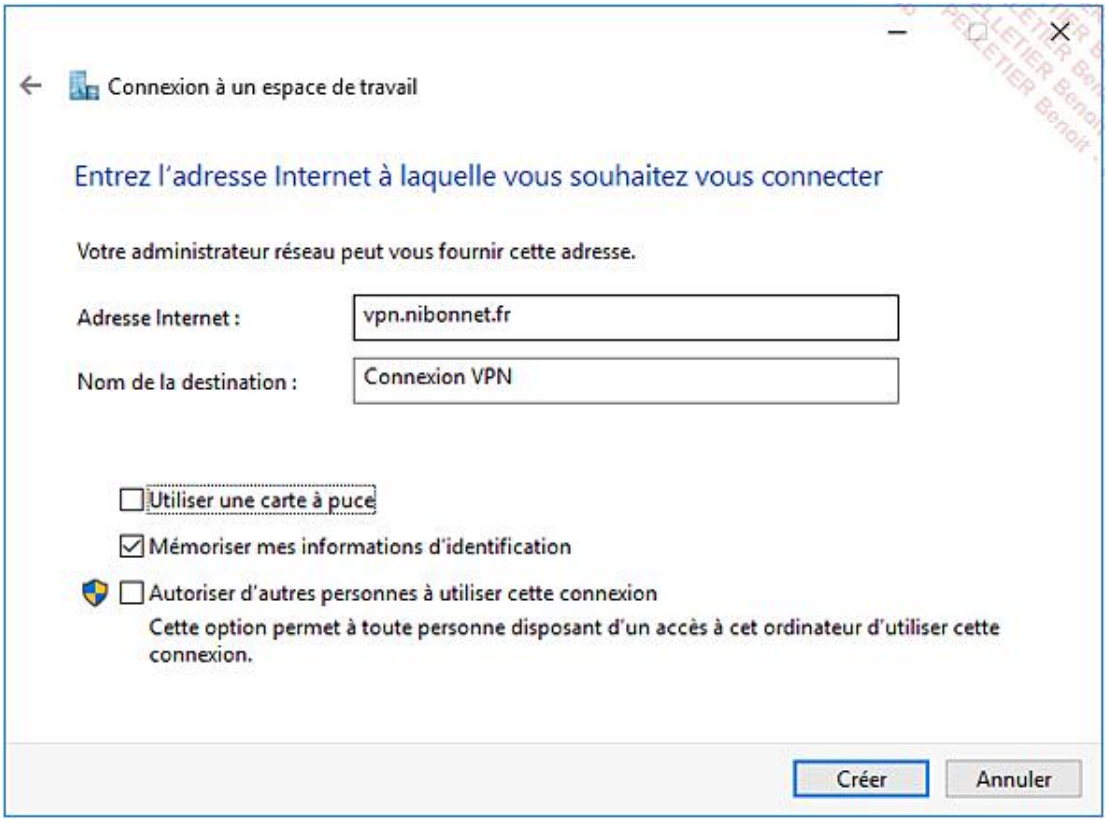


La connexion VPN peut s'effectuer par l'intermédiaire d'une connexion Internet.

Cliquez sur **Utiliser ma connexion Internet (VPN)**.



Il est nécessaire maintenant de saisir l'adresse du serveur VPN (exemple : vpn.nibonnet.fr) ainsi que le nom de la connexion.



- Cliquez sur **Créer** puis lancez la connexion qui vient d'être créée.

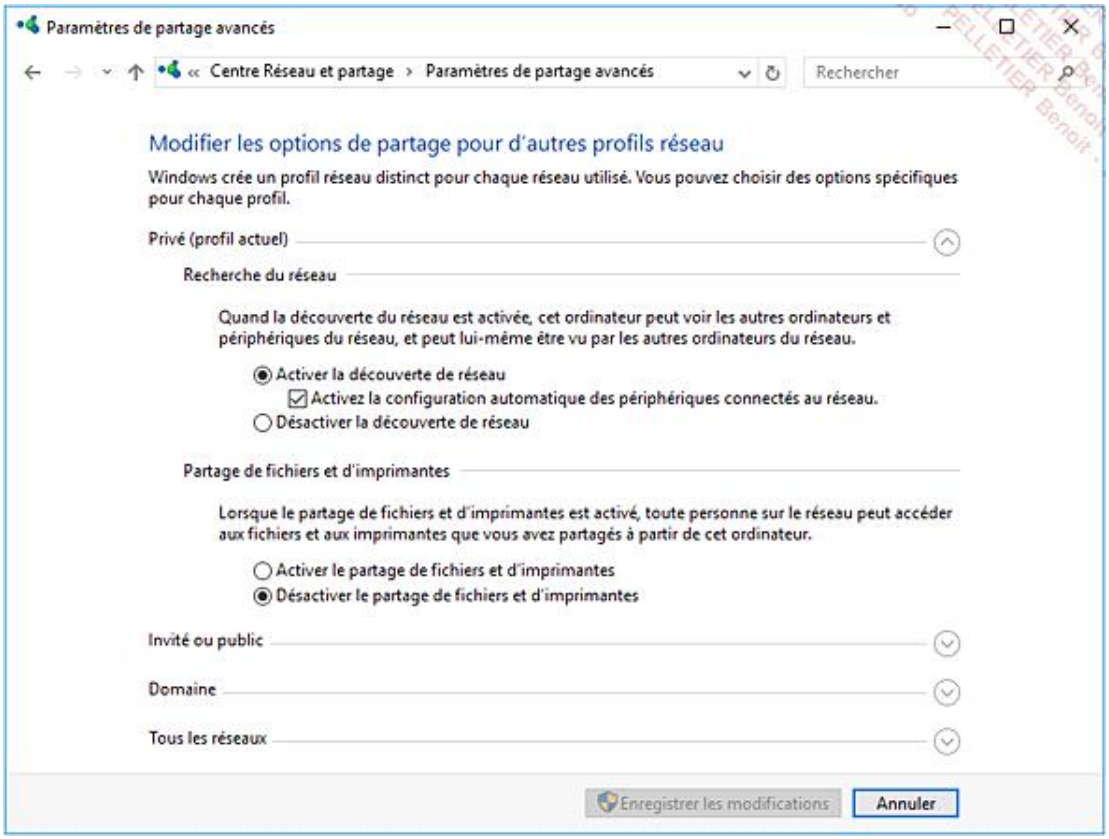
Il est possible d'utiliser une carte à puce pour l'authentification ou la mémorisation des informations d'identification. D'autres utilisateurs peuvent également utiliser cette connexion, l'option correspondante doit pour cela être sélectionnée.

Des options propres au poste sont également configurables.

3. Partage et découverte

Les options de partage et découverte sont configurables par emplacement réseau (voir section suivante). Il est donc possible d'indiquer si les partages configurés sur le poste seront actifs ou non. La découverte est une fonctionnalité existant déjà sur Windows 7, qui consiste à découvrir les équipements (poste, NAS, Freebox…) qui sont sur le même réseau.

- Dans le bandeau gauche de la console **Centre Réseau et partage**, cliquez sur **Modifier les paramètres de partage avancés**.
- Configurez les options comme vous le souhaitez pour les rubriques découverte réseau et partage de fichiers et d'imprimantes.



La configuration peut évidemment être différente en fonction des emplacements réseau.

4. Types d'emplacements réseau

Les emplacements réseau sont utilisés par la couche réseau pour activer ou non les partages et la découverte, ainsi que le pare-feu. Il est possible d'activer ou non le pare-feu, et d'appliquer ou non une règle.

- **Emplacement domicile (privé ou professionnel)** : la recherche du réseau peut être activée. Les partages de fichiers et d'imprimantes peuvent également être autorisés ou refusés.
- **Emplacement de domaine** : la recherche du réseau et le partage de fichiers sont désactivés. Cet emplacement réseau est généralement utilisé par les machines membres d'un domaine.
- **Emplacement public** : les découvertes du réseau et les partages seront désactivés. Cet emplacement est utile pour les connexions à un hotspot, dans un hôtel ou dans un aéroport.

Le serveur VPN SSTP

Un serveur VPN permet à un utilisateur de se connecter au système d'information de l'entreprise lorsqu'il est en dehors de celle-ci.

Il a donc la possibilité de continuer à travailler, d'accéder à ses données comme s'il était à l'intérieur de son entreprise. Cette fonctionnalité offre de plus une grande sécurité car le tunnel VPN créé lors de la connexion de l'entreprise est crypté.

Cette connexion peut être établie à travers un réseau téléphonique (RTC), ADSL ou 3G. Lors de l'installation du serveur, il est possible d'utiliser plusieurs protocoles (IPSec, PPTP…).

Néanmoins ces derniers ont l'inconvénient d'utiliser un port qui n'est pas toujours ouvert à l'endroit où se connecte l'utilisateur (point d'accès Wi-Fi, hotspot…). Dans ce cas, il est impossible d'établir la connexion. Pour remédier à ce problème, il est possible d'implémenter le protocole SSTP qui utilise pour sa part le port 443 (https).

Ce protocole a vu le jour avec Windows Server 2008.

La norme 802.11

Avant d'étudier la norme 802.11, il convient de déterminer ce qu'est le Wi-Fi.

Un réseau sans fil est un réseau où les informations sont échangées à travers des ondes radio dans la plage de fréquences des micro-ondes. Ce type de réseau est composé de plusieurs dispositifs réseau reliés entre eux (bornes Wi-Fi, cartes réseau).

Un réseau Wi-Fi contient un nom (SSID) qui permet de l'identifier.

Une norme a été définie sous le numéro 802.11. Plusieurs versions ont vu le jour depuis septembre 1999.

La norme 802.11a

La bande de fréquence des 5 GHz est utilisée pour un débit théorique de 54 Mbit/s. Elle est normalisée en 1999.

La norme 802.11b

Normalisée également en septembre 1999, elle utilise cette fois la bande de fréquence des 2,4 GHz. Le débit a été réduit et offre un maximum de 11 Mbit/s théorique.

La norme 802.11g

Cette norme est apparue en juin 2003 afin de combiner les avantages des versions a et b. Elle offre donc un débit théorique de 54 Mbit/s et permet d'avoir la portée et la fiabilité de la version b.

La bande de fréquence utilisée est celle des 2,4 GHz.

La norme 802.11n

Normalisée en octobre 2009, elle offre une meilleure bande passante théorique et introduit la notion Multiple-Output Multiple-Input (plusieurs sorties, plusieurs entrées). Elle permet un débit théorique de 450 Mbit/s.

La norme 802.11ac

Apparue en janvier 2014, elle utilise la bande de fréquence des 5 Ghz. Elle offre une bande passante théorique de 1300 Mbits/s.

Un réseau Wi-Fi peut être protégé à l'aide d'une clé (suite de chiffres et de lettres) ou d'un serveur RADIUS.

Commençons par étudier le premier type de sécurité, la clé. Cette dernière consiste à autoriser les équipements (poste de travail, smartphone…) à se connecter au réseau Wi-Fi uniquement s'ils détiennent la bonne clé. La longueur de celle-ci dépend du type de clé sélectionné (WEP, WPA et WPA2). Au nombre de trois, elles possèdent chacune leurs faiblesses et peuvent donc être retrouvées par un pirate plus ou moins facilement. À ce type de sécurité peut être associé un filtrage par adresse MAC. Cette sécurité consiste à autoriser l'accès au réseau uniquement aux cartes réseau dont l'équipement est référencé dans une liste. Cette dernière est configurée par l'administrateur.

Néanmoins, il est assez aisé de modifier l'adressage physique (adresse MAC) de sa carte réseau afin de se faire passer pour un poste autorisé.

Il est possible de mettre en place une sécurité plus robuste en installant un serveur RADIUS. Ce serveur a donc la

fonction d’authentifier les machines qui souhaitent accéder aux réseaux Wi-Fi et d’accorder ou pas l’accès. L’authentification peut s’appuyer sur un couple login/mot de passe ou simplement sur un certificat numérique.

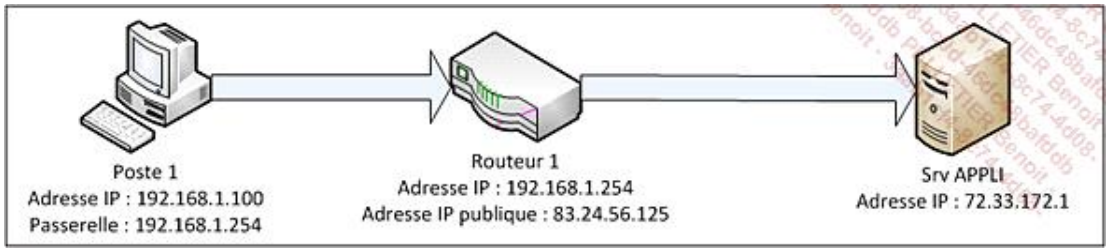
Protocole NAT

La traduction d'adresses réseau NAT permet le partage de la connexion Internet dans un réseau local. Seule l'adresse IP publique est vue du côté Internet et le serveur NAT fait le lien entre le réseau Internet et le réseau interne. Les adresses IP privées ne sont pas routables sur Internet, il est donc nécessaire d'implémenter ce protocole afin de permettre aux machines de sortir du réseau local.

Lorsqu'un ordinateur interne doit avoir accès à Internet, il envoie une trame à son routeur. Celle-ci contiendra :

- L'adresse IP du poste,
- Un port source,
- L'adresse de destination (qui correspond à l'ordinateur cible sur Internet) suivi de son port.

Lors du passage au niveau du serveur NAT, l'adresse IP et le port source sont mis en cache dans une table de correspondance. Le routeur peut désormais remplacer l'adresse IP source du poste par son adresse IP publique, puis envoyer le paquet au destinataire. La réponse sera transmise au serveur NAT qui, par l'intermédiaire de la table de correspondance, va remplacer son adresse IP publique par celle du poste. Par la suite, la trame est envoyée au poste.



Dans l'exemple ci-dessus, le poste essaie de contacter un serveur web nommé Srv APPLI. Le routeur aura le rôle de serveur NAT.

- Trame 1 : du poste vers le routeur

	Adresse IP	Port
Source	192.168.1.100	4500
Destination	72.33.172.1	80

- Table de correspondance renseignée par le routeur :

Table de correspondance			
Adresse IP source	**Port source**	**Adresse IP destination**	**Port destination**
192.168.1.100	4500	72.33.172.1	80

- Trame 2 : du routeur au serveur

	Adresse IP	Port
Source	83.24.56.125	4500
Destination	72.33.172.1	80

- Trame 3 : du serveur au routeur

	Adresse IP	Port

Source	72.33.172.1	80
Destination	83.24.56.125	4500

- Récupération de l'adresse IP source dans la table de correspondance par le routeur

Table de correspondance			
Adresse IP source	**Port source**	**Adresse IP destination**	**Port destination**
192.168.1.100	4500	72.33.172.1	80

- Trame 4 : du routeur vers le poste

	Adresse IP	**Port**
Source	72.33.172.1	80
Destination	192.168.1.100	4500

1. Ajout du service de routage et d'accès distant

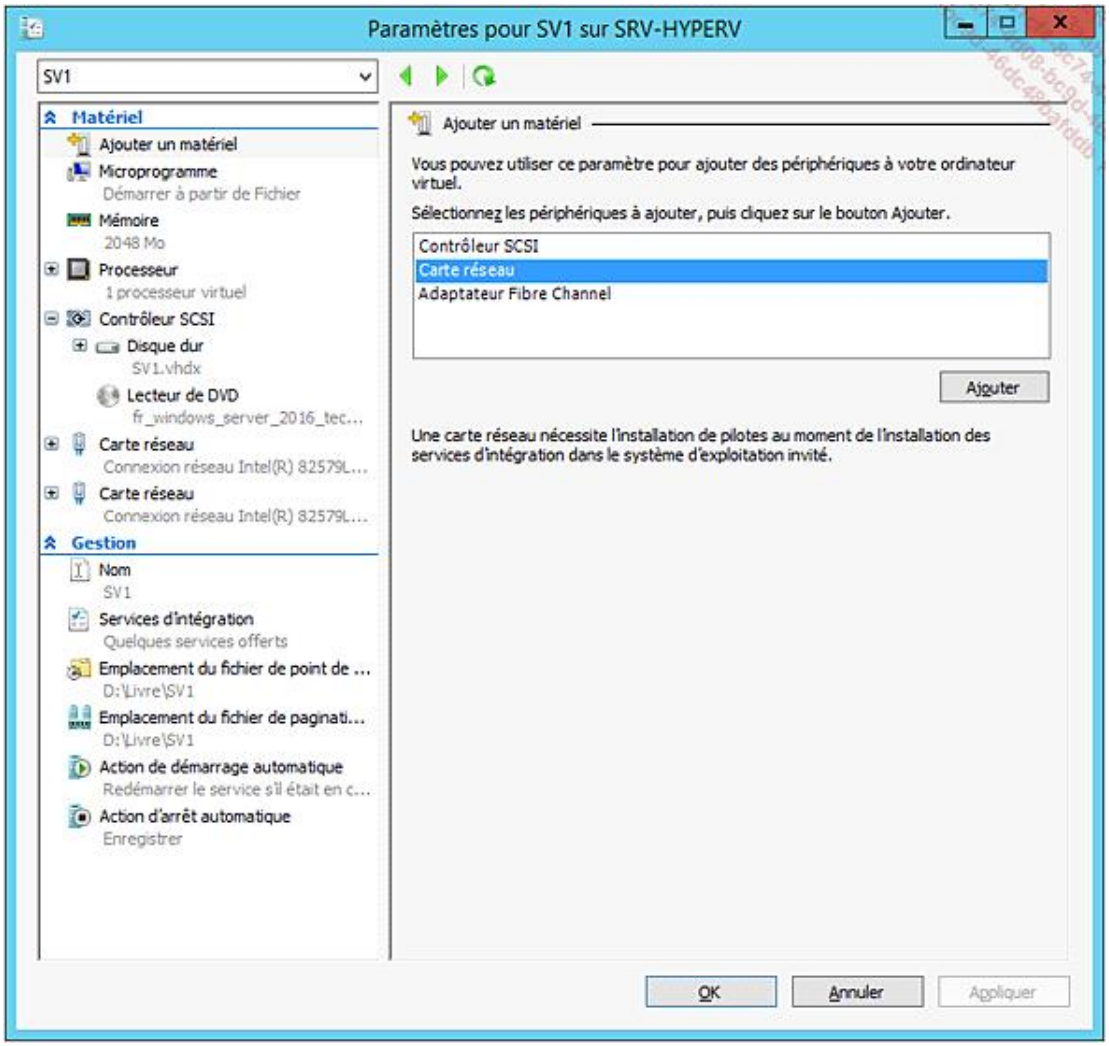
Il est nécessaire d'ajouter une carte réseau sur l'ordinateur SV1 pour effectuer les manipulations ci-dessous.

Ouvrez la console Hyper-V et éteignez si ce n'est pas déjà fait la machine SV1.

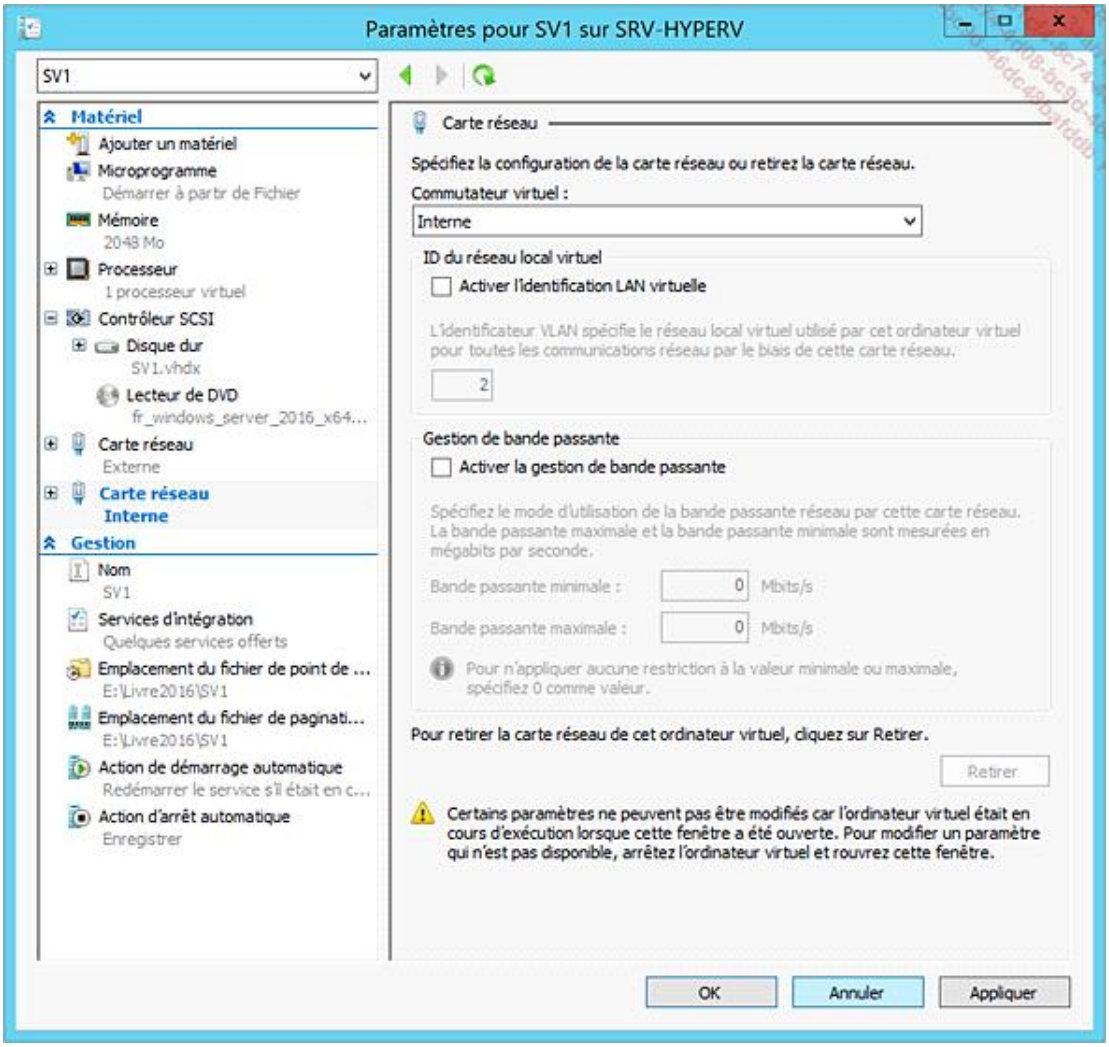
Sélectionnez **SV1** puis cliquez sur **Paramètres** dans le bandeau **Actions**.



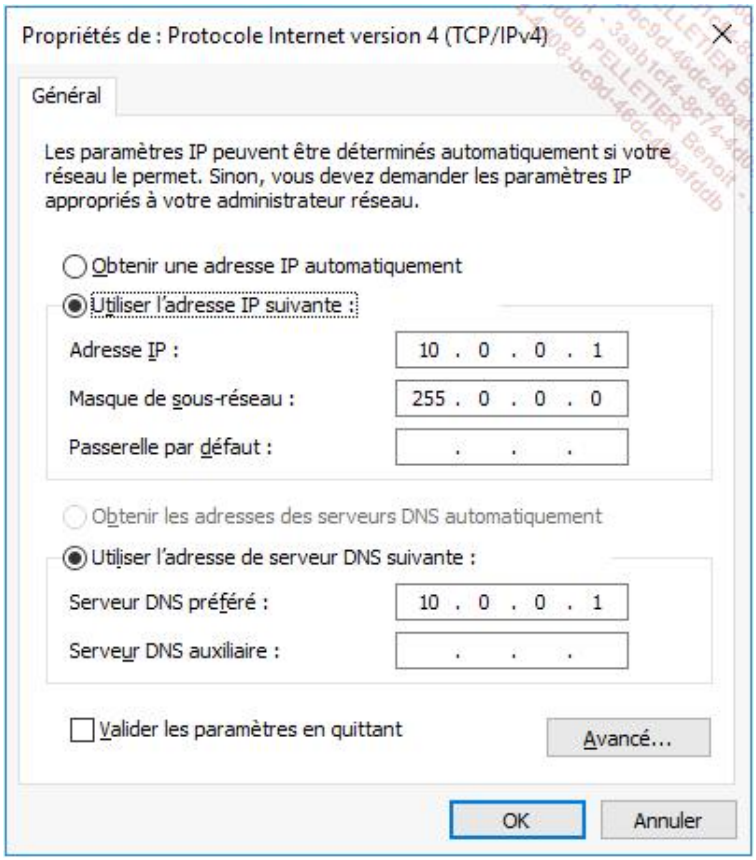
Cliquez sur **Ajouter un matériel**, puis sur **Carte réseau** et enfin sur **Ajouter**.



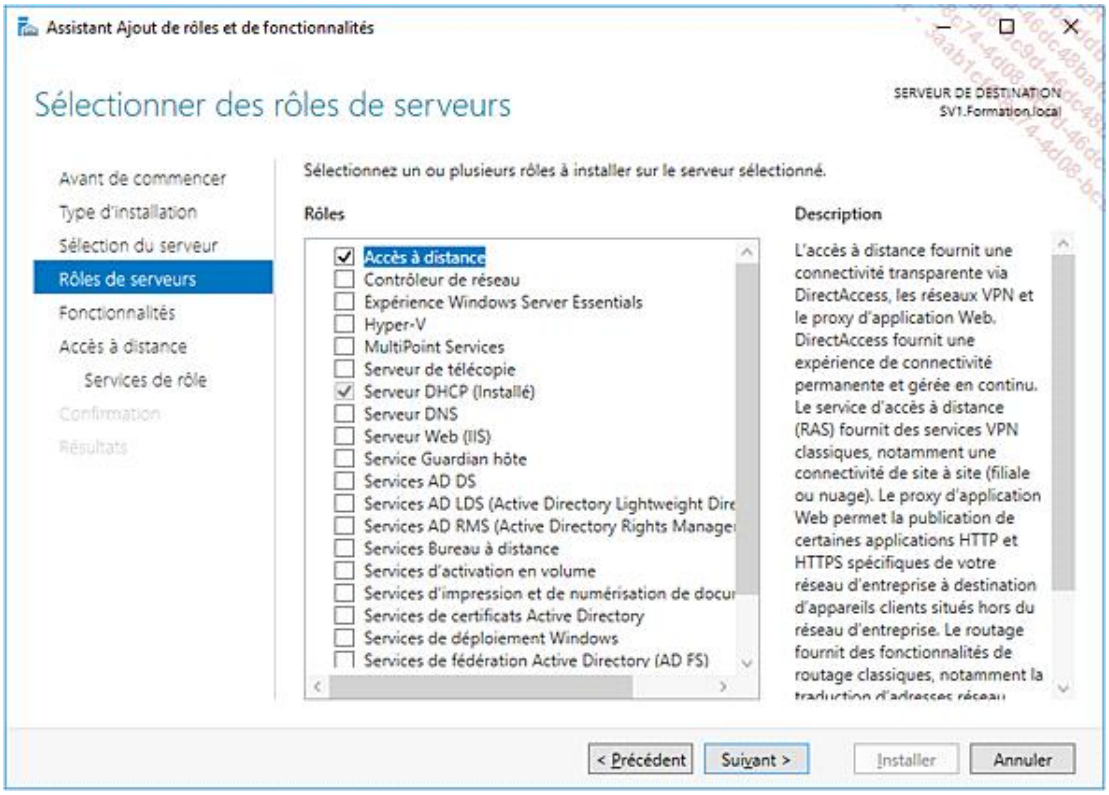
- Connectez la carte sur un commutateur virtuel différent de la première.



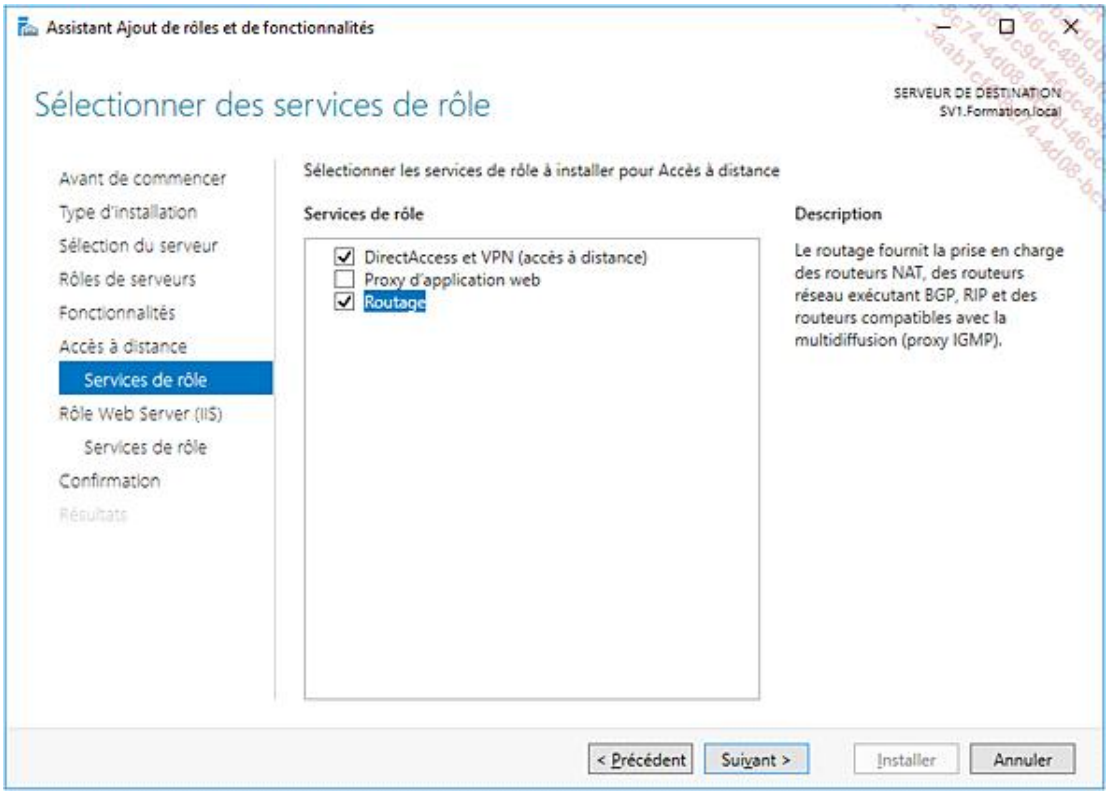
- Cliquez sur **Appliquer** puis sur **OK**.
- Effectuez un clic droit sur la VM SV1 et sélectionnez **Démarrer**.
- Double cliquez sur la machine afin de vous y connecter.
- Ouvrez une session en tant qu'administrateur puis configurez la carte réseau ajoutée comme ci-dessous.



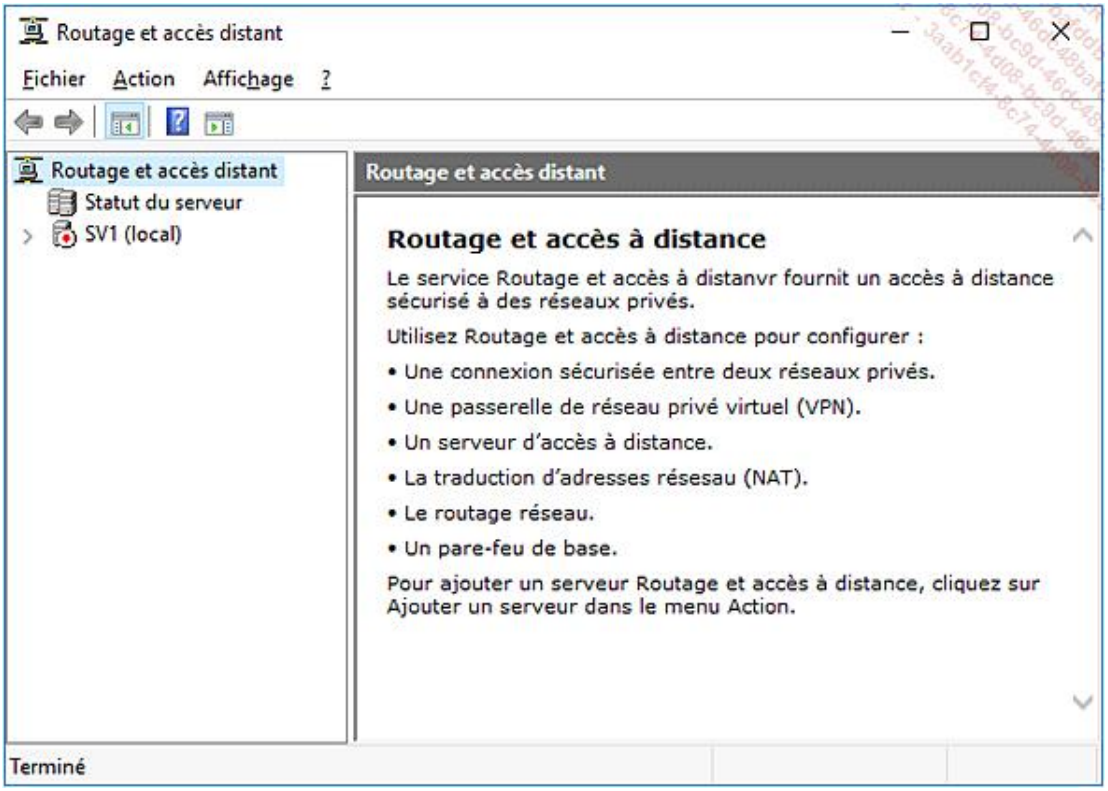
- Lancez la console **Gestionnaire de serveur**.
- Cliquez sur **Ajouter des rôles et fonctionnalités**.
- Cliquez sur **Suivant** dans la page d'accueil de l'assistant.
- Laissez le type d'installation par défaut dans la fenêtre **Sélectionner le type d'installation**.
- Sélectionnez SV1 puis cliquez sur **Suivant** dans la fenêtre **Sélectionner le serveur de destination**.
- Cochez la case **Accès à distance** puis cliquez sur **Suivant**.



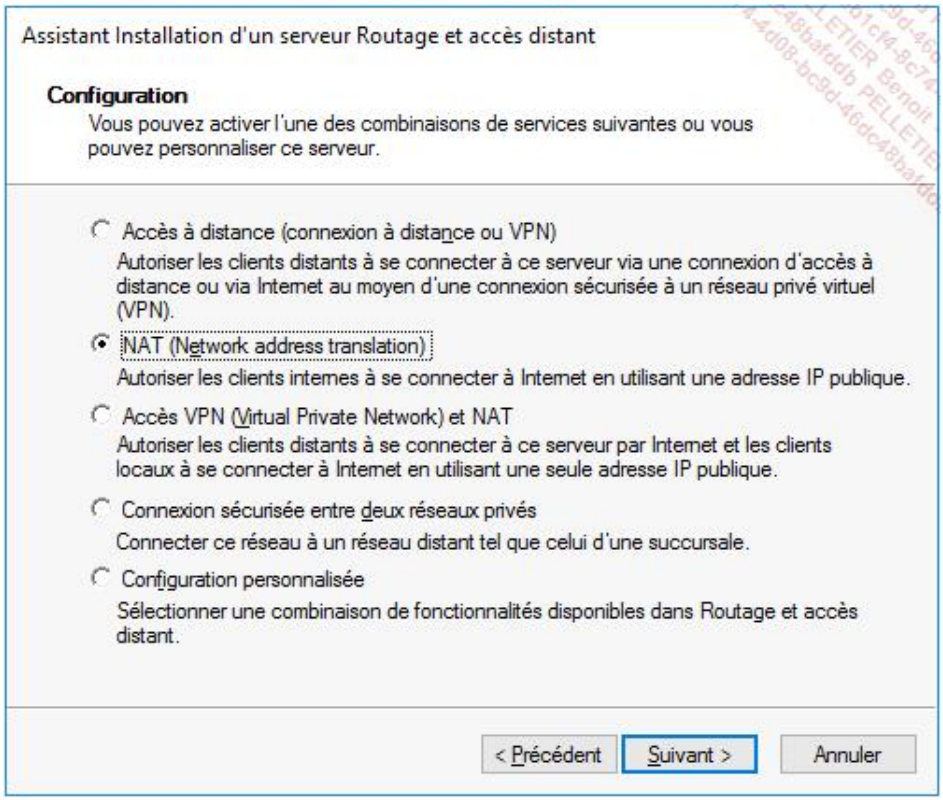
- Laissez les paramètres par défaut dans la fenêtre de choix des fonctionnalités à installer.
- Cochez **Routage** dans le choix des services de rôle puis cliquez sur **Ajouter des fonctionnalités**.



- Laissez les services de rôle IIS par défaut et cliquez sur **Suivant**.
- Cliquez sur **Installer** pour lancer l'installation.
- Ouvrez la console **Routage et accès distant**.

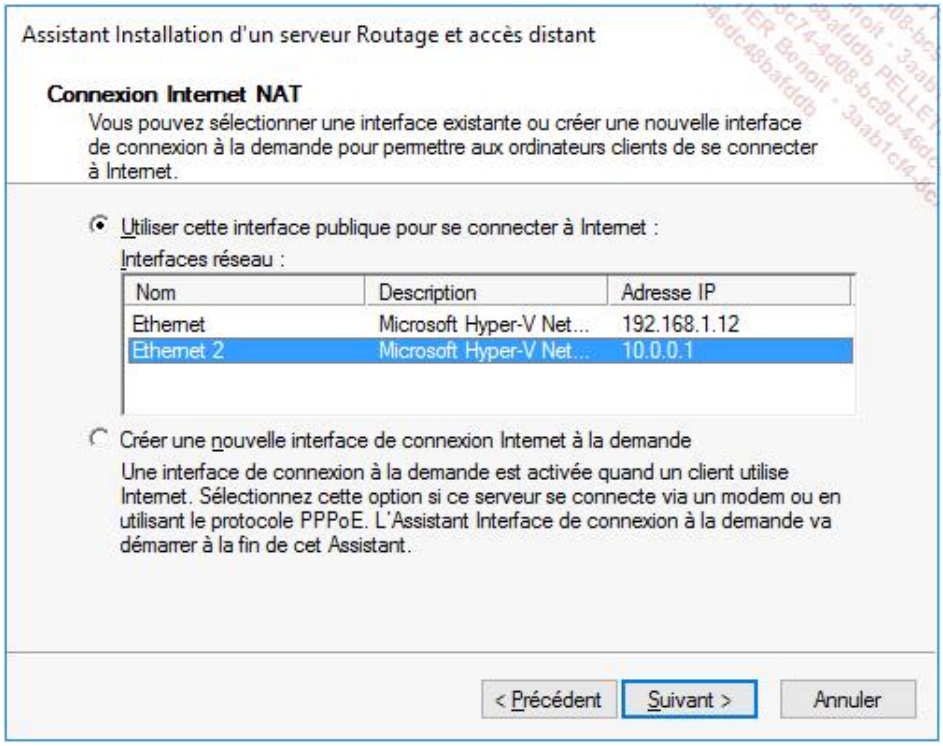


- Effectuez un clic droit sur SV1 et sélectionnez **Configurer et activer le routage et l'accès distant**.
- Cliquez sur **Suivant**.
- Sélectionnez **NAT (Network address translation)** dans la fenêtre **Configuration**.



- Sélectionnez l'interface qui est connectée au réseau Internet.

Nous allons simuler la connexion au réseau Internet par l'interface réseau qui possède l'IP 10.0.0.1.

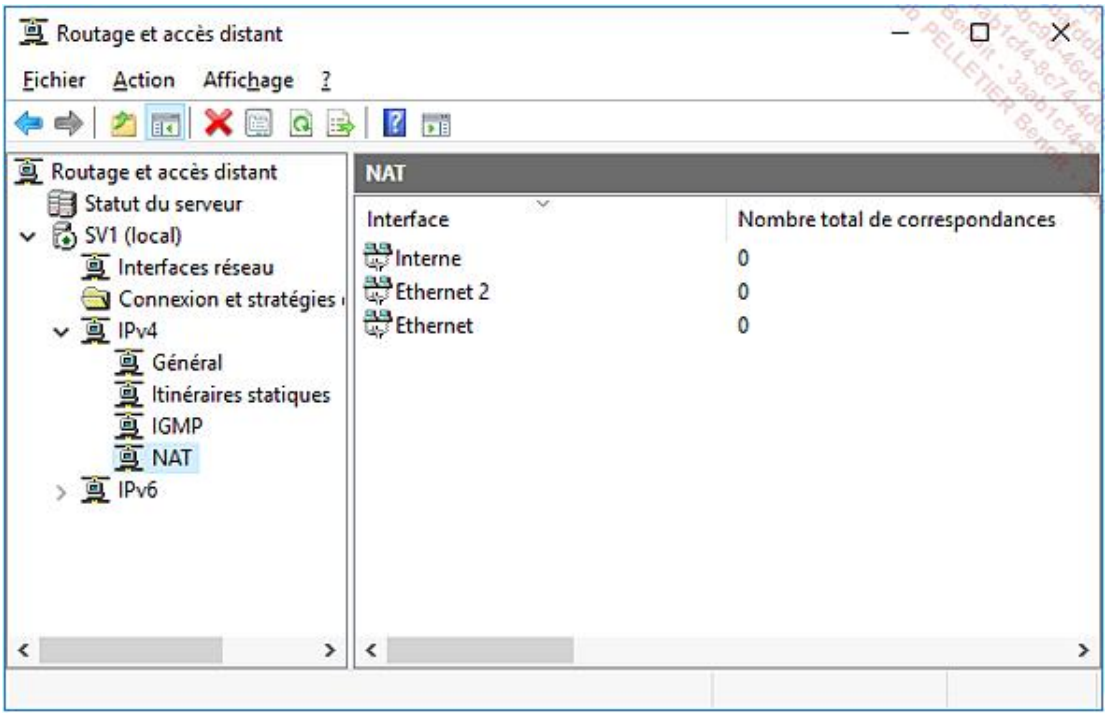


Cliquez sur **Terminer** afin de mettre fin à l'assistant.

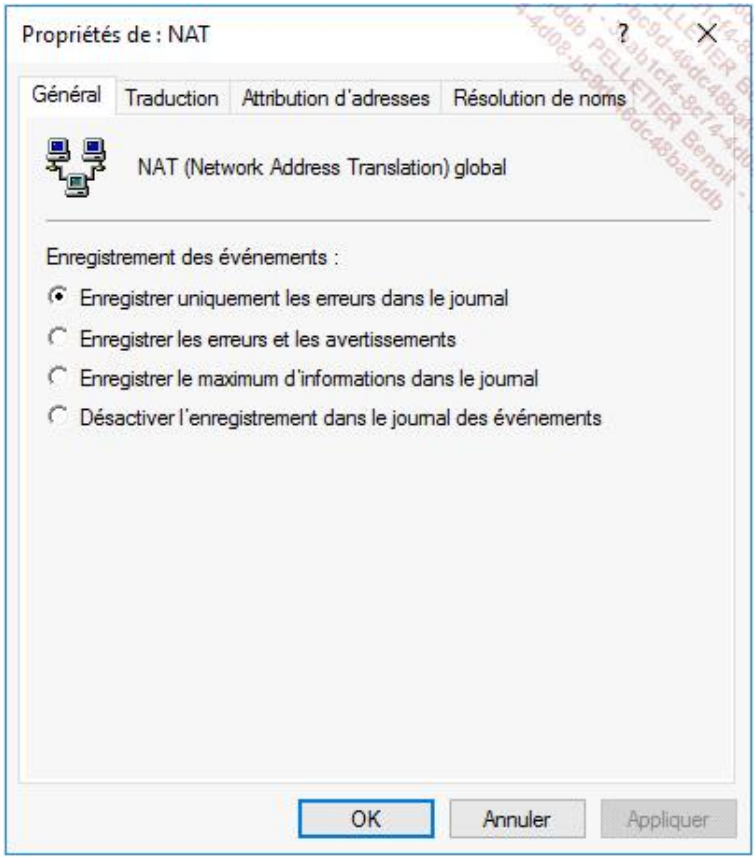
Le serveur est maintenant configuré.

2. Propriétés du serveur NAT

Dans l'arborescence de la console, effectuez un clic droit sur **NAT** puis sélectionnez **Propriétés**.

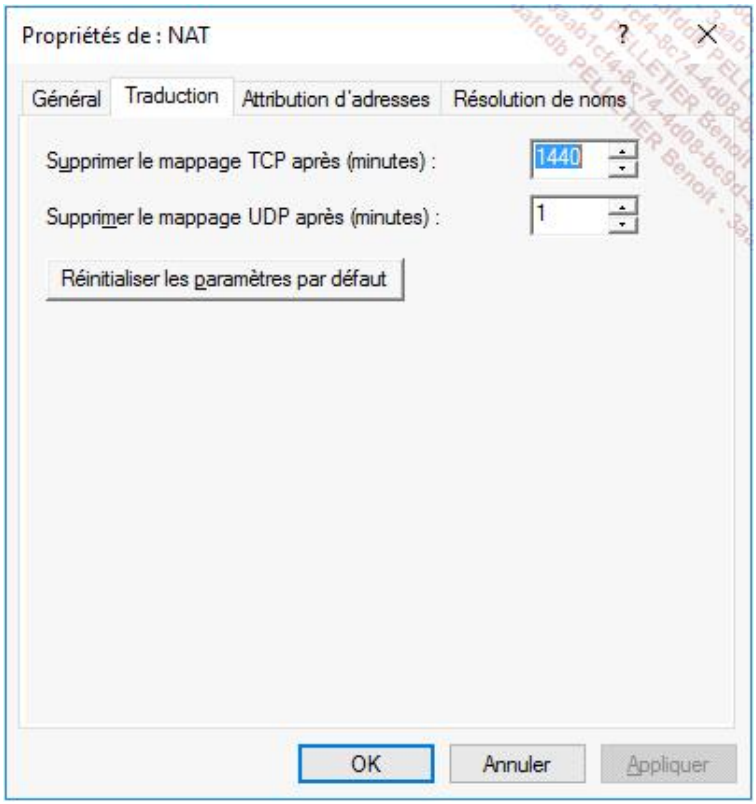


L'onglet **Général** permet de paramétrer le type d'enregistrement souhaité.

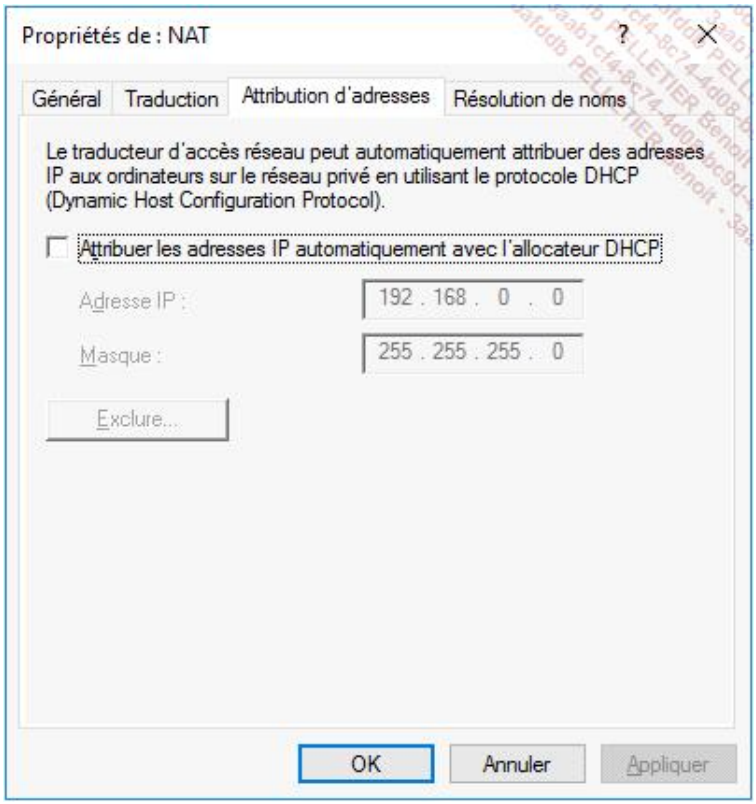


L'onglet **Traduction** permet de déterminer la durée des mappages pour les connexions TCP (suppression après 1440 minutes) et les connexions UDP (suppression après 1 minute).

Ces valeurs peuvent être modifiées.



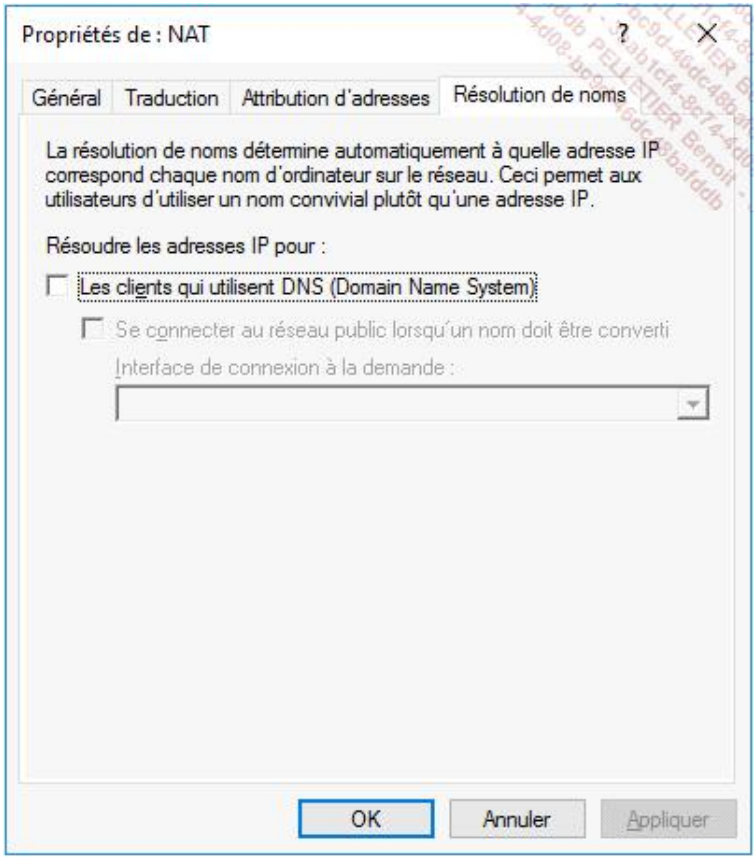
L'onglet **Attribution d'adresses** permet de configurer une distribution d'adresse IP. Il est nécessaire d'indiquer l'adresse du réseau ainsi que le masque.



Aucune option ne peut être définie mais il est possible d'exclure des adresses IP.

L'onglet **Résolution de noms** permet de relayer les demandes DNS des ordinateurs clients vers un serveur DNS. Le

serveur NAT agit comme un proxy DNS.

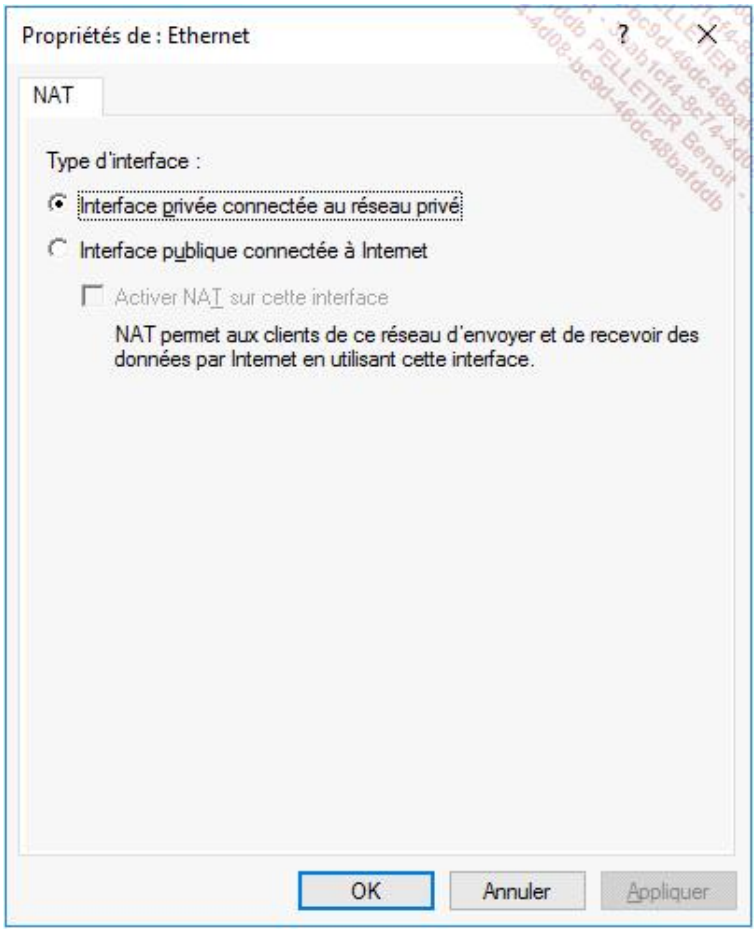


3. Propriétés des interfaces utilisées par NAT

Un serveur NAT possède généralement deux interfaces, l'une connectée sur le réseau public (Internet) et l'autre sur le réseau privé.

Propriétés de l'interface connectée au réseau local

Seul l'onglet **NAT** est présent. Les propriétés de la carte réseau offrent peu de choix puisqu'elles permettent uniquement de choisir le type d'interface de la carte réseau (interface privée ou interface publique).

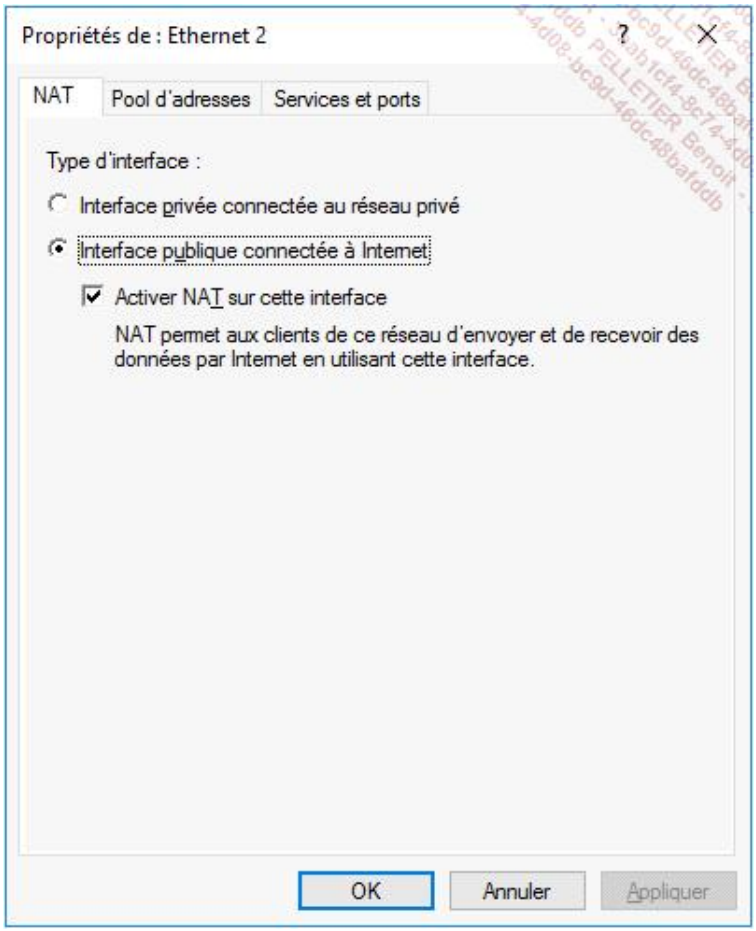


Propriétés de l'interface connectée au réseau Internet

Les propriétés sont composées de trois onglets :

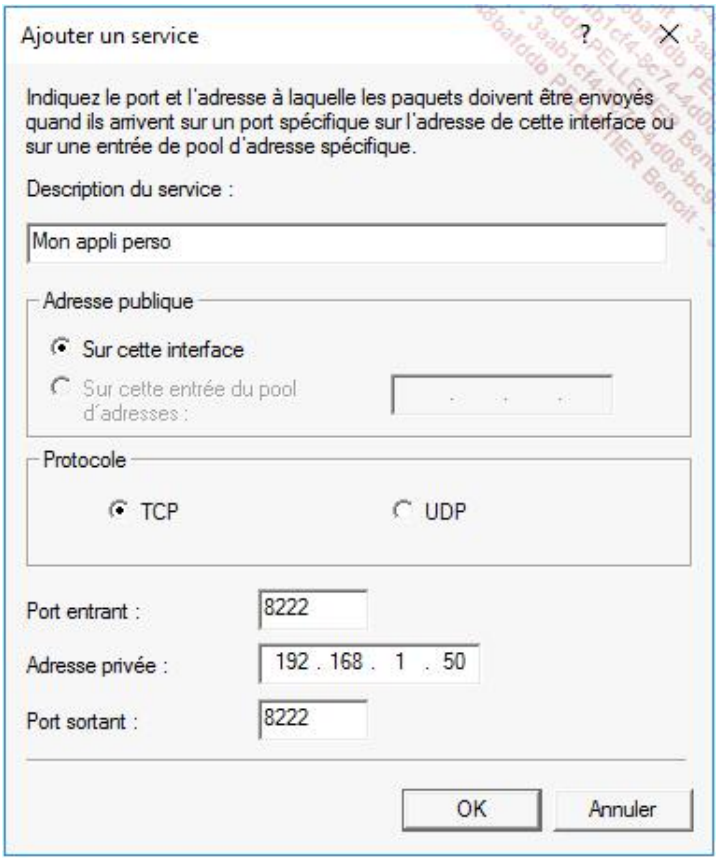
- **NAT** qui permet de choisir le type d'interface de la carte réseau.
- **Pool d'adresses** qui permet de saisir les IP publiques attribuées par le fournisseur d'accès. Le bouton **Réservations** permet de mapper une IP publique sur une IP privée.
- **Services et ports** qui permettent de définir les services internes disponibles depuis Internet. Si le service n'est pas présent, il suffit de le créer depuis cet onglet.

Ainsi, il est possible de rediriger le flux HTTP ou mail provenant de l'interface réseau connectée au réseau public vers les serveurs web et messagerie du réseau interne.



Les informations nécessaires pour l'ajout d'un service sont les suivantes :

- La description du service.
- L'adresse publique.
- Le protocole.
- Le port d'entrée/sortie.
- L'adresse privée.



Le flux provenant du réseau public et du port 8222 est redirigé vers le serveur ayant l'IP 192.168.1.50. Le port 8222 est également utilisé pour le serveur en interne.

La console **Routage et accès distant** permet également de configurer les connexions réseau à distance.

La protection d'accès réseau (NAP)

NAP est un rôle présent depuis Windows Server 2008 et Windows Vista. Avec ce rôle, il est maintenant possible de restreindre l'accès aux ordinateurs qui ne respectent pas les contraintes exigées par l'administrateur. Il assure néanmoins la mise à jour des ordinateurs considérés comme non conformes.

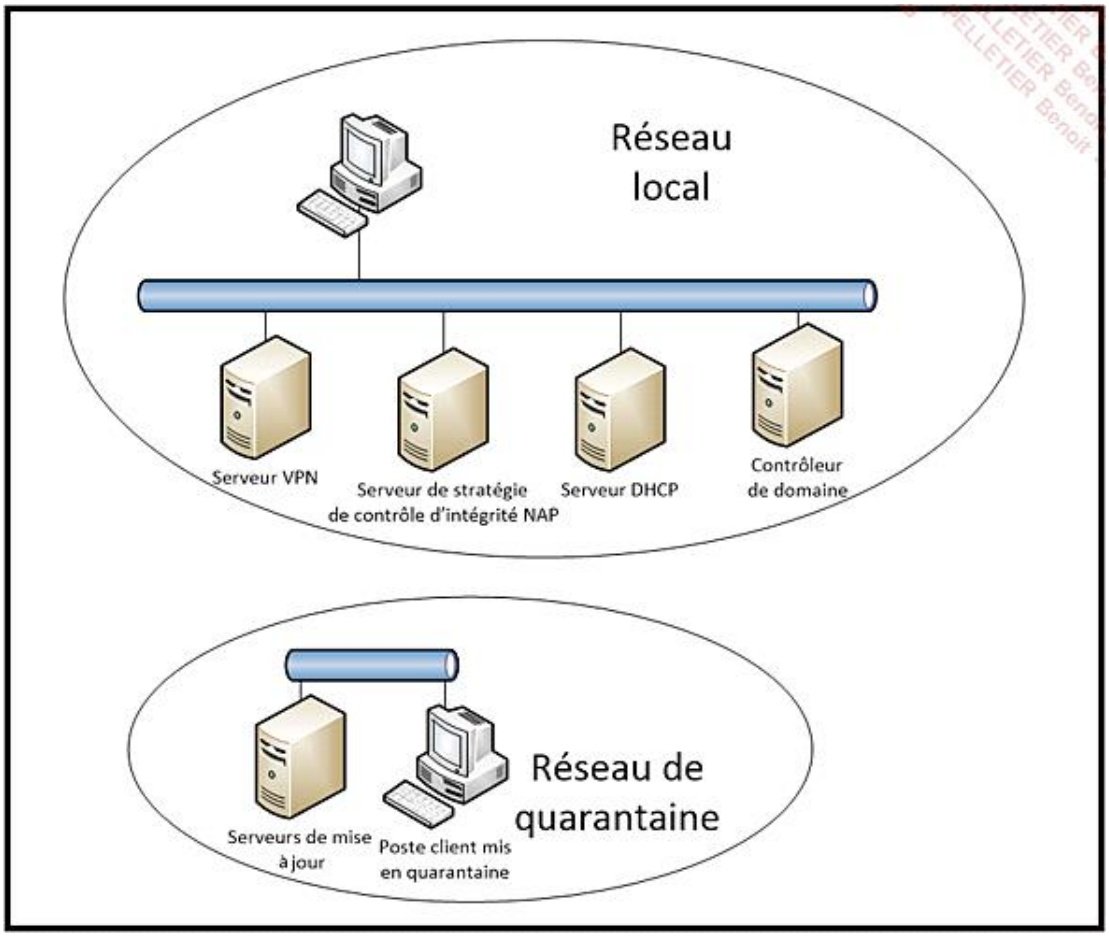
Il est impossible à la fonctionnalité NAP d'empêcher un utilisateur autorisé d'effectuer des opérations malveillantes sur le réseau.

1. Présentation du service NAP

Le service NAP possède plusieurs méthodes de contrainte de mise en conformité. Chacune d'entre-elles permettent de gérer les différents accès au réseau local (VPN…).

- **Contrainte de mise en conformité IPsec** : l'ordinateur doit être conforme pour pouvoir communiquer avec d'autres ordinateurs conformes.
- **Contrainte de mise en conformité 802.1x pour les connexions câblées ou sans fil** : l'ordinateur doit être conforme pour pouvoir obtenir un accès illimité via une connexion 802.1x.
- **Contrainte de mise en conformité VPN pour les accès VPN** : l'ordinateur doit être conforme pour pouvoir obtenir un accès illimité via une connexion 802.1x.

Contrairement aux précédents systèmes d'exploitation serveur, il n'est pas possible de mettre en place NAP pour le service DHCP. Le service NAP va contenir un serveur de stratégie de contrôle d'intégrité NAP présent sur le réseau local. Ce serveur a la charge de décider si le poste client qui demande l'accès doit être positionné sur le réseau local (accès autorisé) ou sur le réseau restreint appelé également réseau de quarantaine (poste non conforme, accès interdit). Sur le réseau de quarantaine, un groupe de serveurs de mise à jour (WSUS…) est mis à disposition du client afin qu'il puisse se mettre à jour. Une fois l'opération effectuée, il lui est possible de joindre le réseau de production.



Le service NAP est composé d'une architecture serveur et d'une architecture client différentes l'une de l'autre.

2. Architecture du client NAP

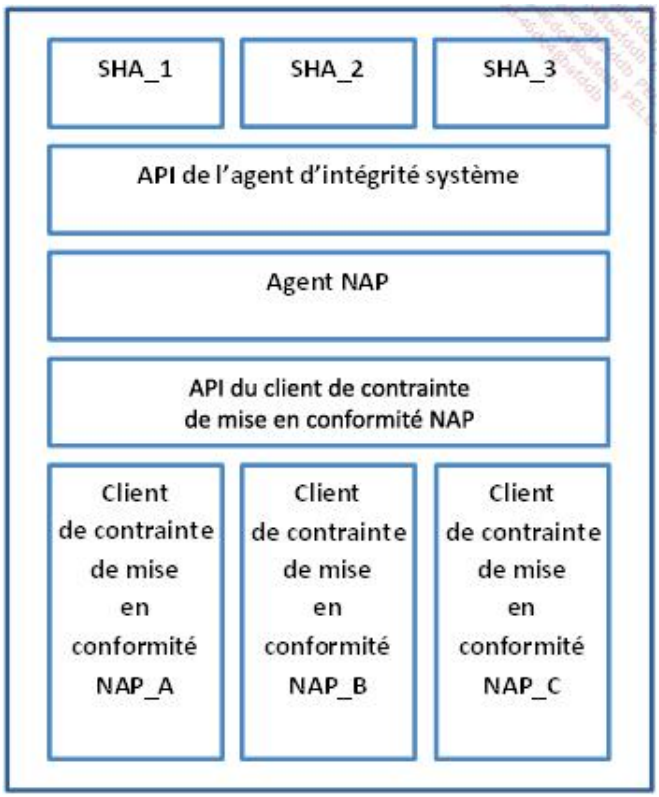
Le client possède une couche de composants Client de contrainte. Chaque client est défini pour un type d'accès réseau spécifique (VPN, Wi-Fi…). Ils sont conçus pour fonctionner avec un type de point de contrainte de mise en conformité (le client de contrainte de mise en conformité NAP par VPN est conçu pour fonctionner avec un point de contrainte de mise en conformité NAP basé sur VPN). Certains éditeurs de logiciels tiers peuvent fournir d'autres clients de contrainte.

Une couche de composants d'Agent d'intégrité système (SHA) comprend des composants qui gèrent et signalent un ou plusieurs éléments de l'état de santé du poste. Par exemple, un agent d'intégrité système peut être utilisé pour les signatures antivirus, et un autre agent d'intégrité système peut être utilisé pour les mises à jour du système d'exploitation.

L'agent d'intégrité système va être mis en correspondance avec un serveur de mise à jour. Comme pour le client de contrainte, les éditeurs tiers peuvent fournir des agents.

L'agent NAP gère les informations d'état d'intégrité actuelles du client NAP et facilite la communication entre les couches client de contrainte de mise en conformité et agent d'intégrité système.

L'API (interface de programmation d'applications) de l'agent d'intégrité système permet une inscription auprès de l'agent NAP, ceci afin d'indiquer l'état d'intégrité système. Il lui est également demandé de répondre aux requêtes de l'agent NAP.



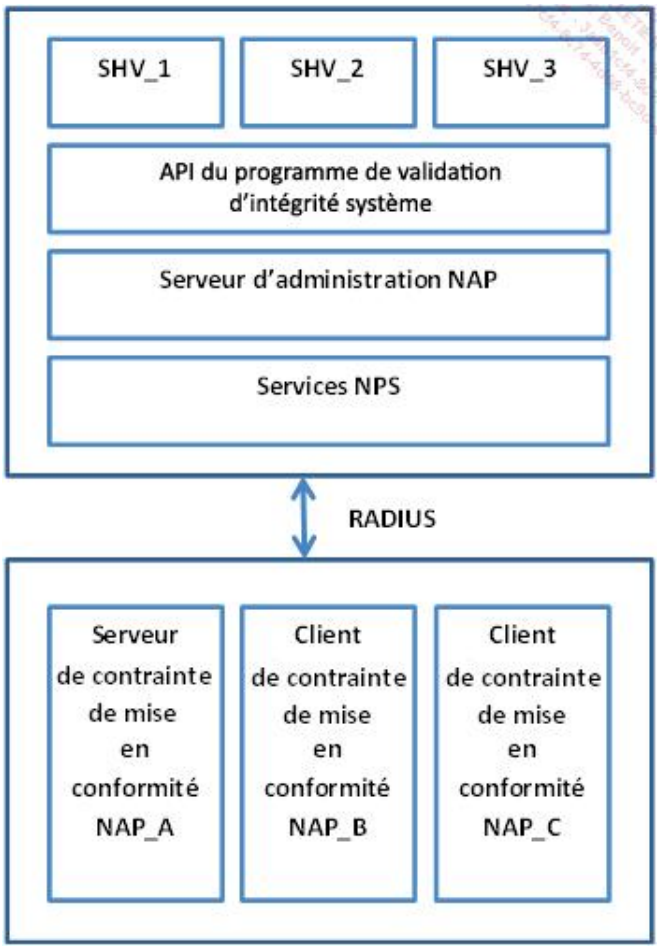
Le client de contrainte de mise en conformité va dialoguer avec le serveur de contrainte de mise en conformité.

3. Architecture du serveur NAP

Le service NPS reçoit le message de demande d'accès RADIUS (*Remote Access Dial-In User Service*) et extrait la déclaration d'intégrité système. Il la transmet au composant Serveur d'administration NAP.

Ce dernier facilite la communication entre le service NPS et les programmes de validation d'intégrité système. Chaque programme de validation d'intégrité système est défini pour un ou plusieurs types d'éléments et il peut être mis en correspondance avec un agent.

L'API du programme de validation d'intégrité système fournit un jeu d'appels de fonctions qui permettent de s'inscrire auprès du composant Serveur d'administration NAP, de recevoir des déclarations d'intégrité et d'envoyer les réponses.



4. Les différentes stratégies dans NAP

NAP contient trois types de stratégies : les stratégies réseau, les stratégies de contrôle de l'intégrité et les stratégies de demande de connexion.

La stratégie réseau permet d'indiquer quel client peut se connecter ainsi que les conditions à respecter.

La stratégie réseau possède plusieurs éléments :

- Activation ou non de la stratégie.
- Accès autorisé ou bloqué ainsi que la méthode de connexion réseau.
- Condition de déclenchement (horaire, système d'exploitation…).
- La méthode d'authentification.
- Le type de média utilisé (Wi-Fi, câble Ethernet...).

Afin d'exploiter le programme de validation d'intégrité de la sécurité Windows, il est nécessaire de configurer une stratégie de contrôle d'intégrité et de lui affecter le programme de validation d'intégrité système.

Plusieurs comportements sont possibles (réussite de tous les contrôles SHV, réussite d'un ou plusieurs contrôles SHV...). Cette stratégie permet de déterminer l'accès qui va être donné au poste qui a effectué la demande. Plusieurs accès sont possibles :

- Accès complet

- Accès limité
- Accès refusé

La stratégie de demande de connexion permet d’indiquer où se fait le traitement (localement ou par l’intermédiaire d’un serveur RADIUS).

La fonctionnalité Équilibrage de charge réseau

La fonctionnalité Équilibrage de charge réseau permet de s'assurer que l'ensemble des serveurs ont une charge de travail identique.

Afin d'offrir une tolérance de panne à un utilisateur, le service IT peut mettre en place plusieurs serveurs ayant le même rôle (exemple : serveur web).

Il est donc utile d'implémenter la fonctionnalité Équilibrage de la charge réseau. En effet, cette dernière a pour fonction d'envoyer les trames aux serveurs en fonction de leur occupation. Ainsi, il n'est pas possible d'avoir un serveur très occupé et un autre qui ne fait rien.

Une fois la fonctionnalité installée et configurée, l'utilisateur accède à une adresse IP virtuelle (choisie lors de la configuration de la fonctionnalité) différente de l'adresse IP des serveurs. Par la suite l'utilisateur est redirigé vers l'un des serveurs parmi ceux qui ont le moins de charge.

Présentation du service DNS

1. Introduction

DNS (*Domain Name System*, Système de noms de domaine) permet de traduire un nom de domaine en adresse IP.

Avant DNS, le système de résolution d'un nom sur Internet devait se faire à l'aide d'un fichier texte, le fichier Hosts. Ce dernier était maintenu par le NIC du Stanford Research Institute (SRI), les postes devaient récupérer le fichier par transfert de fichier.

Le système montre assez vite ses limites et DNS est alors créé pour succéder à la résolution par fichier Hosts.

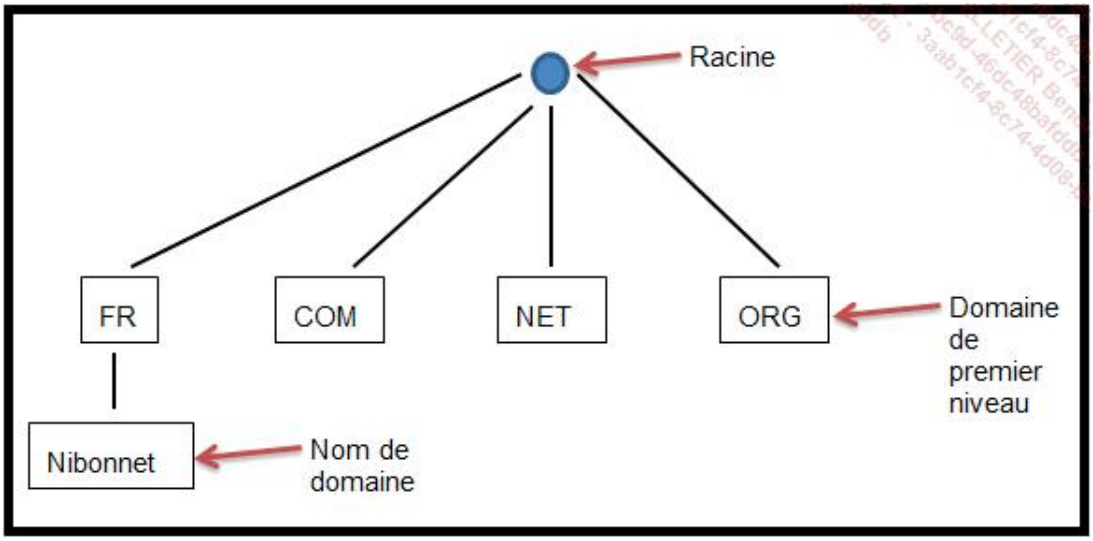
2. Système hiérarchique

DNS est construit sur un système hiérarchique. Les serveurs racines permettent de rediriger les requêtes vers les serveurs DNS de premier niveau (fr, com…). Le domaine racine est représenté par un point. On trouve en dessous les différents domaines de premier niveau (fr, net, com…). Chacun de ces domaines est géré par un organisme (AFNIC pour le .fr, etc.), IANA (*Internet Assigned Numbers Authority*) gère pour sa part les serveurs racines.

Au second niveau se trouvent les noms de domaine qui sont réservés par les entreprises ou les particuliers (nibonnet, editions-eni). La réservation s'effectue chez un registrar qui peut également héberger un serveur web.

On trouve sur chaque niveau des serveurs DNS différents, chacun a autorité sur sa zone (le serveur racine contient uniquement l'adresse et le nom des serveurs de premier niveau). Il en est de même pour tous les serveurs de chaque niveau.

Il est possible pour une entreprise ou un particulier de rajouter pour le nom de domaine qu'il a réservé des enregistrements ou des sous-domaines (par exemple, mail.nibonnet.fr, qui me permet de transférer tout le trafic mail vers un routeur, plus précisément à destination d'une adresse IP publique).

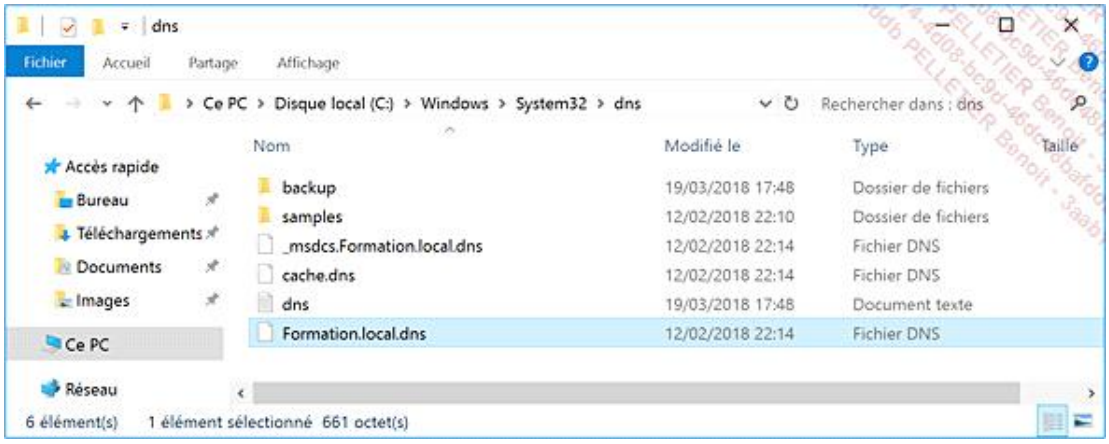


Chaque serveur DNS ne peut résoudre que les enregistrements de sa zone. Le serveur de la zone fr peut résoudre l'enregistrement nibonnet mais il ne sait pas résoudre le nom de domaine shop.nibonnet.fr.

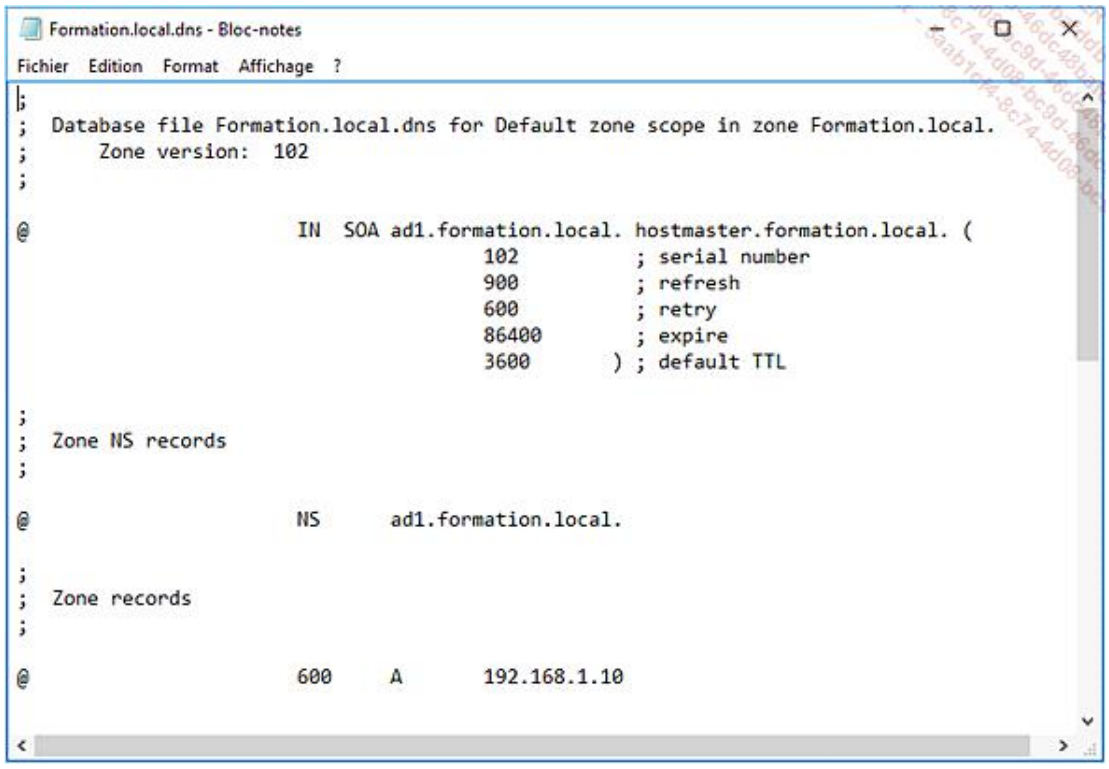
Installation du rôle Serveur DNS

Le rôle DNS peut être installé sur un contrôleur de domaine ou un serveur membre.

Sur un contrôleur de domaine, la zone peut être intégrée à Active Directory ou contenue dans un fichier texte (le fichier est enregistré dans c:\windows\system32\dns).



Le fichier de la zone contient l'ensemble des enregistrements.

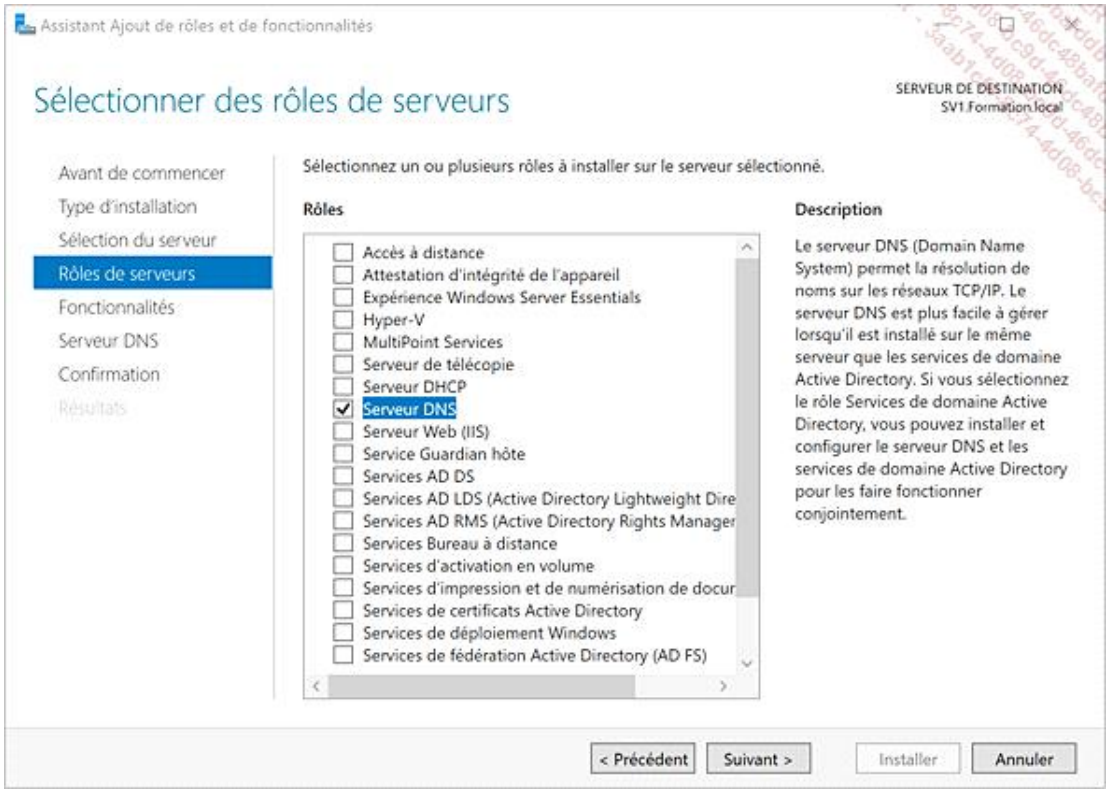


Si le serveur est seulement un serveur membre, la zone DNS ne peut pas être intégrée à AD.

Installation du rôle sur SV1

- Ouvrez la console **Gestionnaire de serveur**.
- Cliquez sur **Ajouter des rôles et des fonctionnalités**.

- Dans la fenêtre **Sélectionner le type d'installation**, laissez le choix par défaut.
- Le destinataire est SV1. Laissez le choix par défaut dans la fenêtre du destinataire.
- Cochez la case **Serveur DNS** puis cliquez sur le bouton **Ajouter des fonctionnalités** dans la fenêtre qui s'affiche.



- Cliquez sur **Suivant** dans la fenêtre de sélection des fonctionnalités.
- Dans la fenêtre de confirmation, cliquez sur **Installer**.

Le rôle est maintenant installé mais n'est pas opérationnel. Il est nécessaire de le configurer afin qu'il puisse résoudre les noms du domaine **Formation.local**.

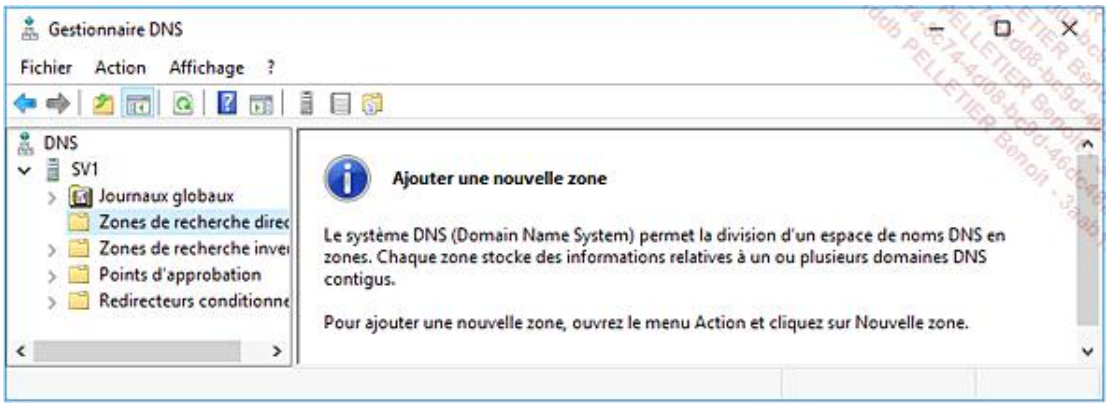
Gestion des zones DNS

Une zone DNS est une portion du nom de domaine dont le responsable est le serveur DNS qui a autorité sur la zone. Ce dernier gère la zone et ses différents enregistrements.

1. Création d'une zone de recherche directe secondaire

Les zones de recherche directe prennent en charge la résolution des noms d'hôtes en adresses IP. La création d'une zone nécessite l'appartenance de l'opérateur au groupe Administrateurs.

- Sur SV1, ouvrez la console DNS.
- Déroulez **SV1** puis **Zones de recherche directes**.



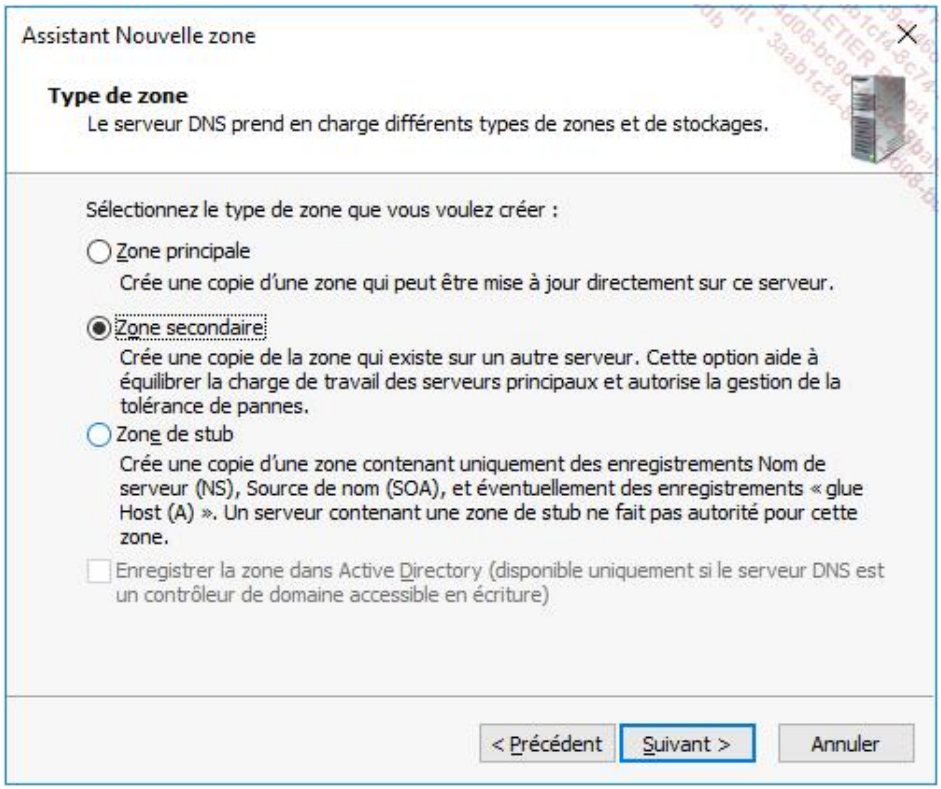
- Effectuez un clic droit sur le dossier **Zones de recherche directes** puis sélectionnez **Nouvelle zone**.

Trois types de zones peuvent être créés :

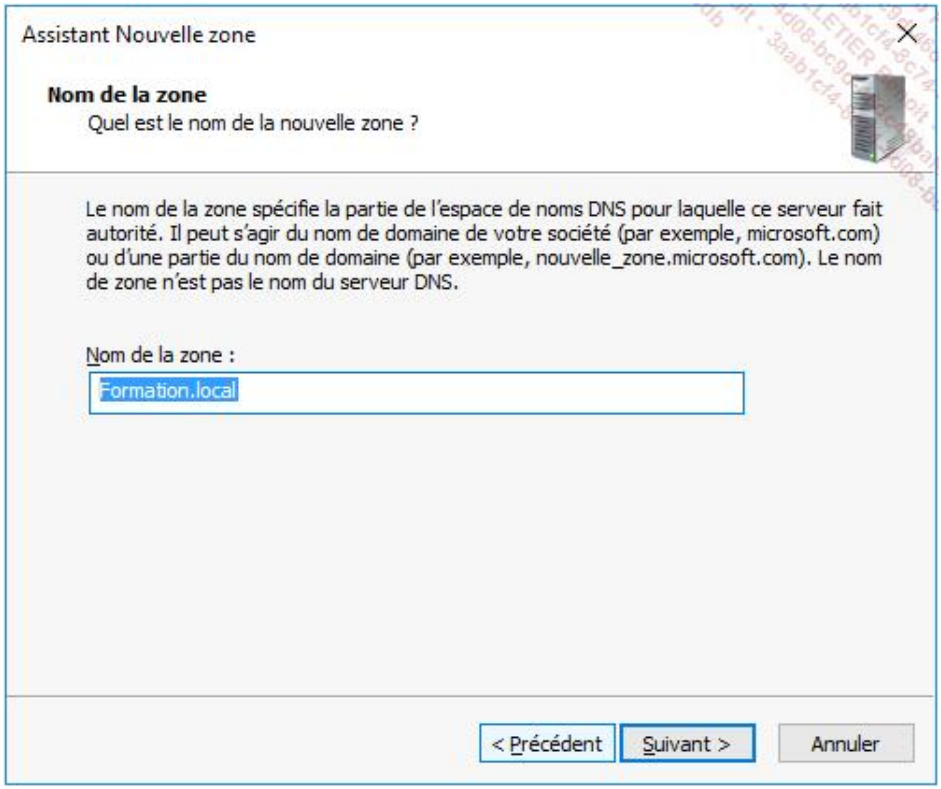
- **Zone primaire** : le serveur peut modifier les enregistrements de sa zone, il a des accès en lecture et en écriture aux enregistrements.
- **Zone secondaire** : ce type de zone est une copie d'une zone primaire. Le serveur ne peut pas modifier les enregistrements contenus dans la zone. Son but est de répondre aux requêtes faites par les clients.
- **Zone de stub** : la zone contient uniquement les enregistrements SOA, NS et A des serveurs DNS responsables de la zone.

- Sélectionnez **Zone secondaire** puis cliquez sur **Suivant**.

Il est impossible de cocher l'enregistrement de la zone dans AD car le serveur n'est pas contrôleur de domaine.

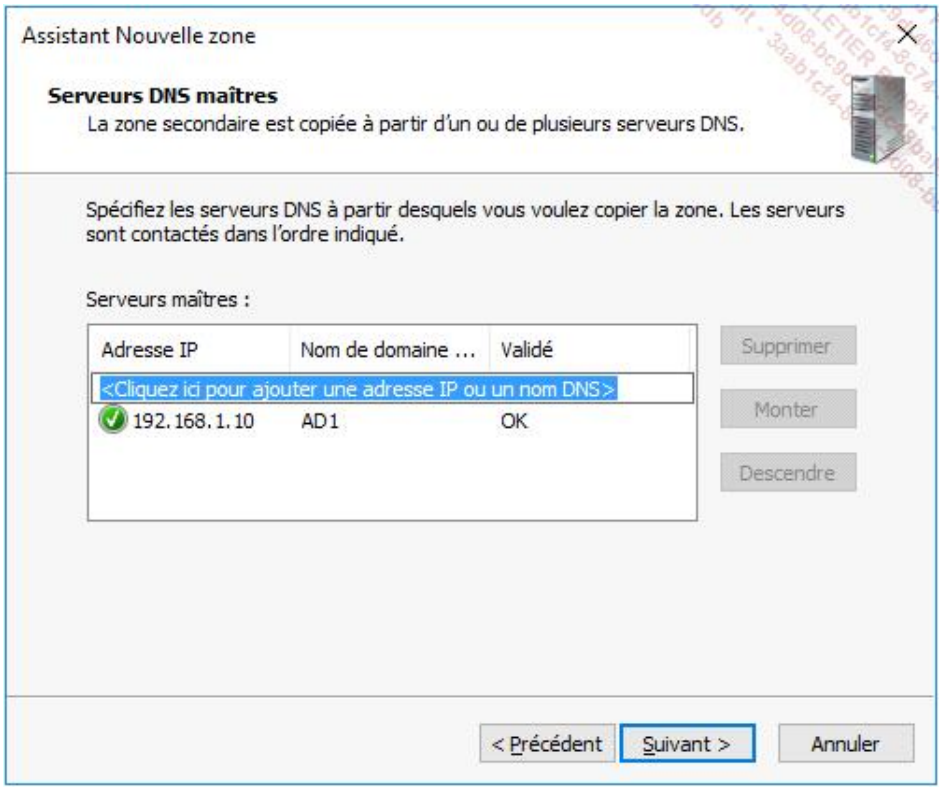


- Saisissez **Formation.local** dans le champ **Nom de la zone**.



- Saisissez dans le champ du serveur maître l'adresse IP du serveur AD1 (192.168.1.10) et validez en appuyant sur la touche [Entrée].

Le serveur maître est le serveur qui a un accès en écriture sur la zone, contrairement à la zone secondaire qui elle, a un accès en lecture.

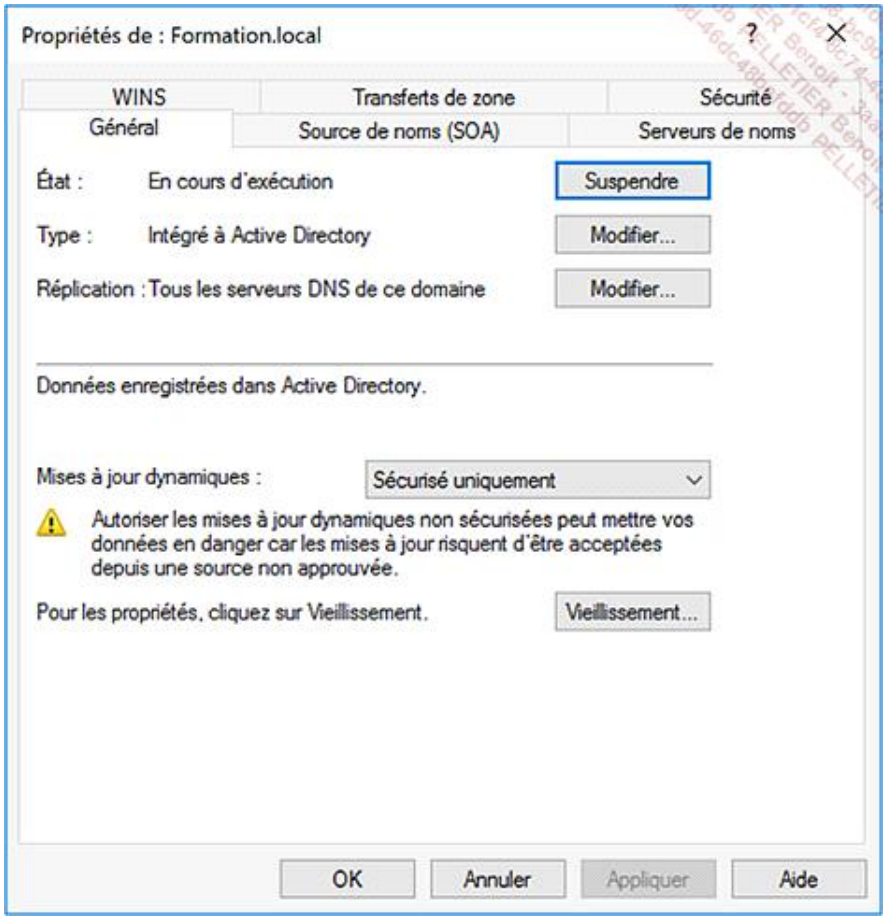


- Cliquez sur **Suivant** lorsque la résolution du nom est terminée.
- Cliquez sur **Terminer**.

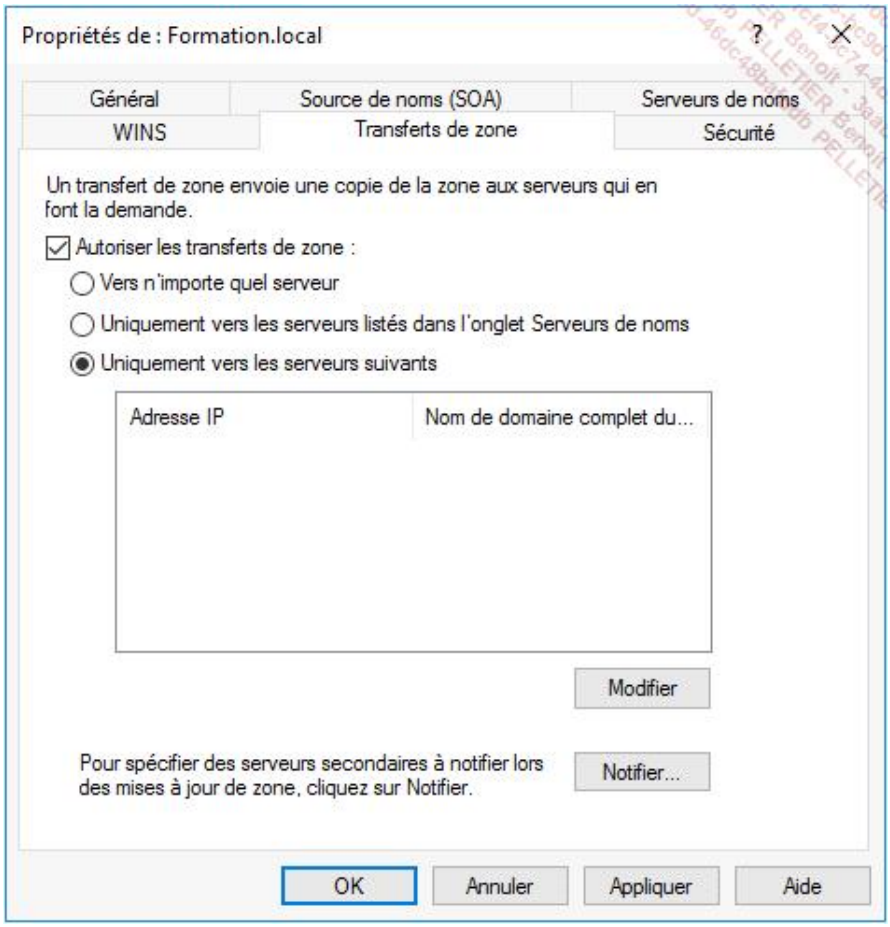
Un message avertit qu'il est impossible de charger la zone. Ce message est dû au transfert de zone non configuré. Deux types de réplication avec DNS sont possibles :

- **La réplication avec AD** : ce type de réplication est utilisé pour les zones intégrées à AD. La réplication s'effectue en même temps que la réplication Active Directory.
- **La réplication avec le transfert de zone** : pour les zones qui ne sont pas intégrées à Active Directory, le transfert de zone est utilisé. Contrairement aux zones intégrées à AD, ce type de réplication nécessite une configuration.

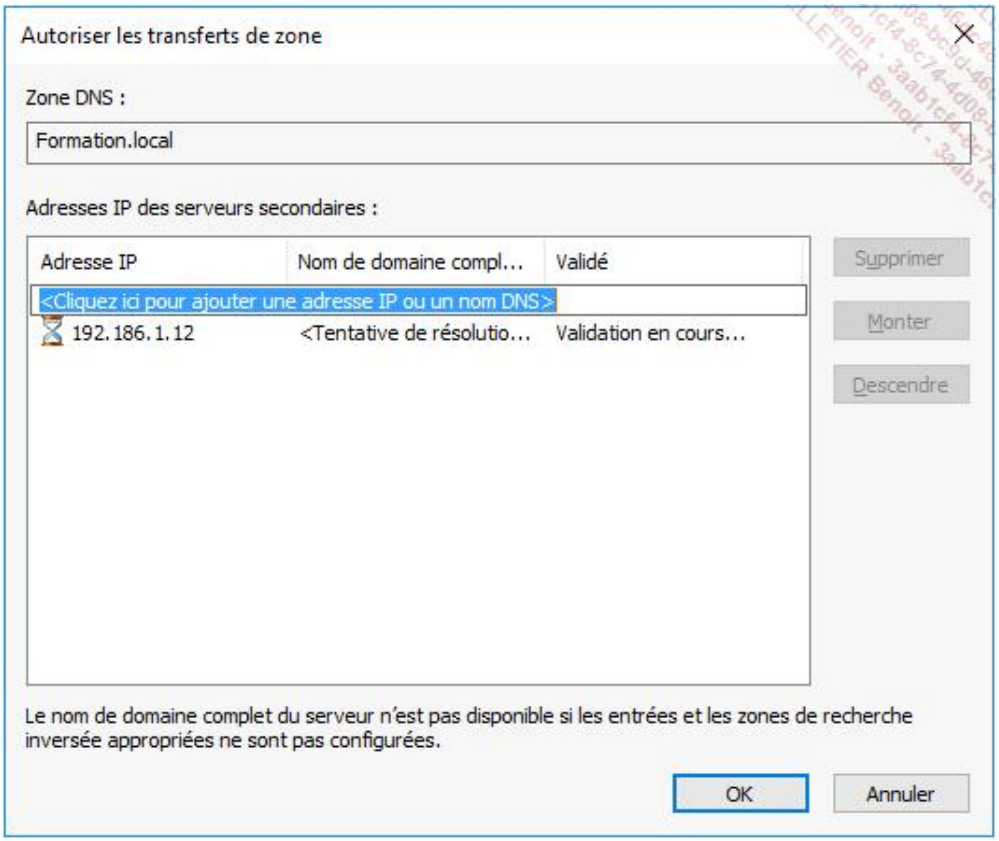
- Sur AD1 lancez la console DNS.
- Effectuez un clic droit sur la zone puis sélectionnez **Propriétés**.



- Cliquez sur l'onglet **Transferts de zone**.
- Cochez la case **Autoriser les transferts de zone** puis sélectionnez le bouton radio **Uniquement vers les serveurs suivants**.

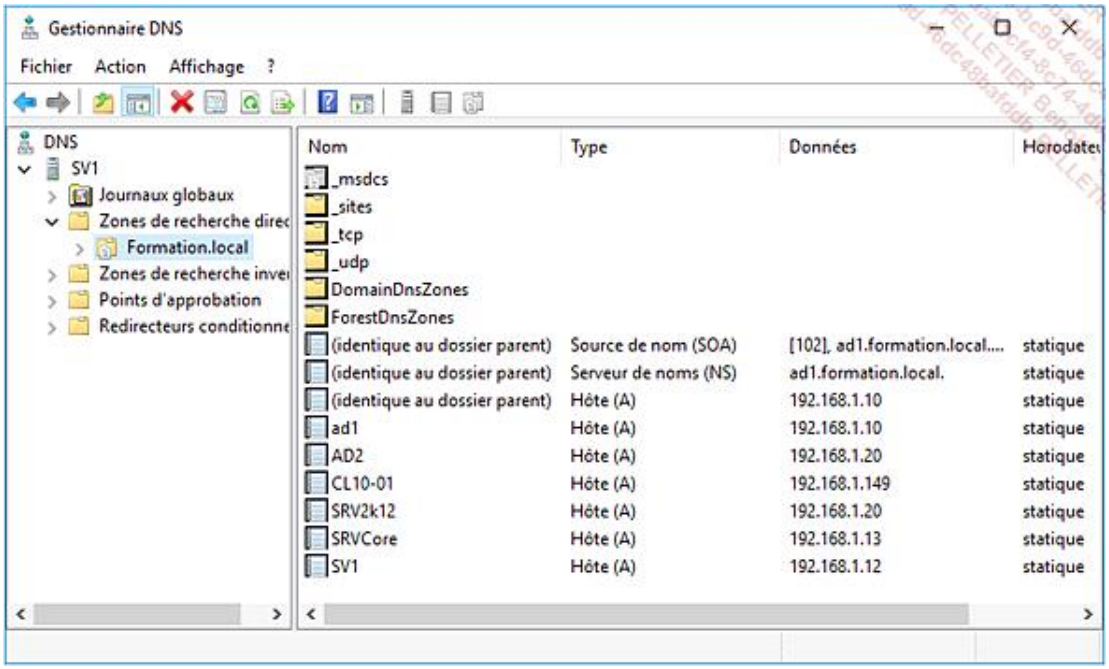


Cliquez sur le bouton **Modifier** et saisissez l'adresse IP du serveur maître (SV1, 192.168.1.12).



Cliquez deux fois sur **OK** pour valider et fermer les fenêtres.

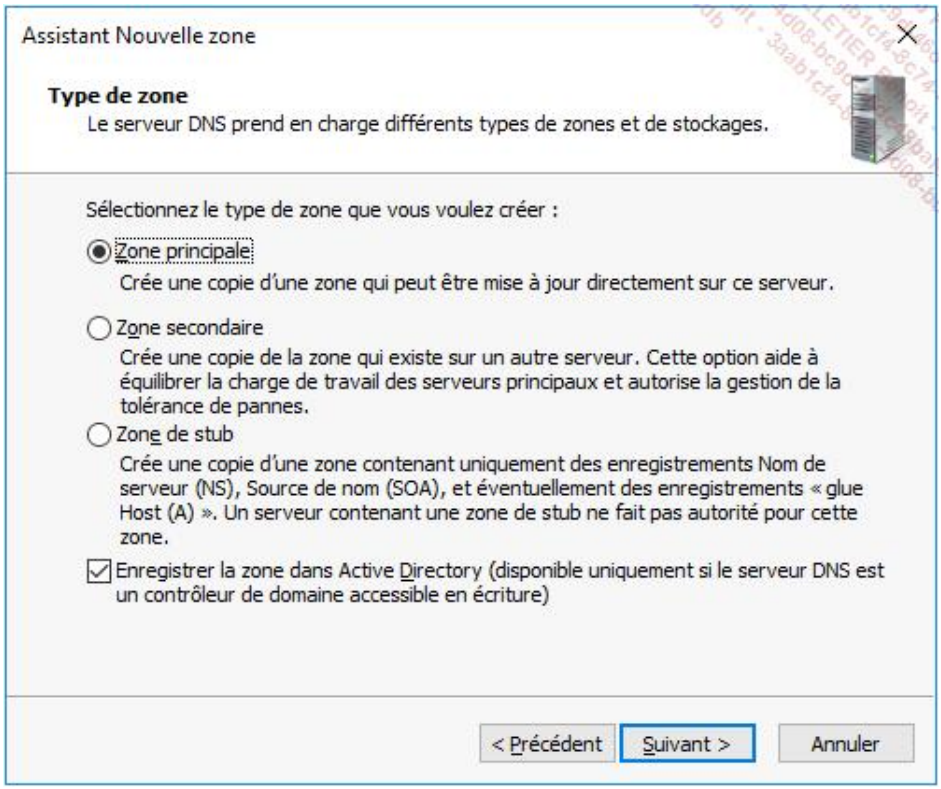
Au bout de quelques minutes, le transfert de zone est terminé.



2. Création d'une zone de recherche directe principale

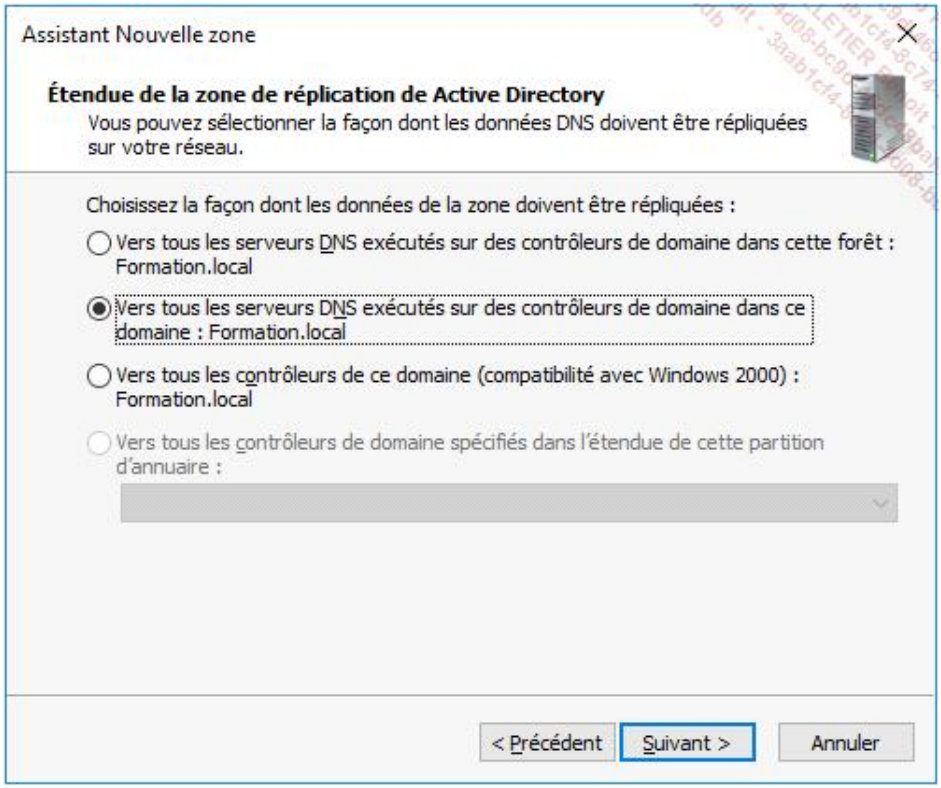
La zone Forms.msft doit être créée sur AD1 pour être intégrée à AD.

- Lancez la console DNS sur AD1.
- Déroulez **AD1** puis **Zones de recherche directes**.
- Effectuez un clic droit sur le dossier **Zones de recherche directes** puis sélectionnez **Nouvelle zone**.
- Laissez les paramètres par défaut dans le type de zone.

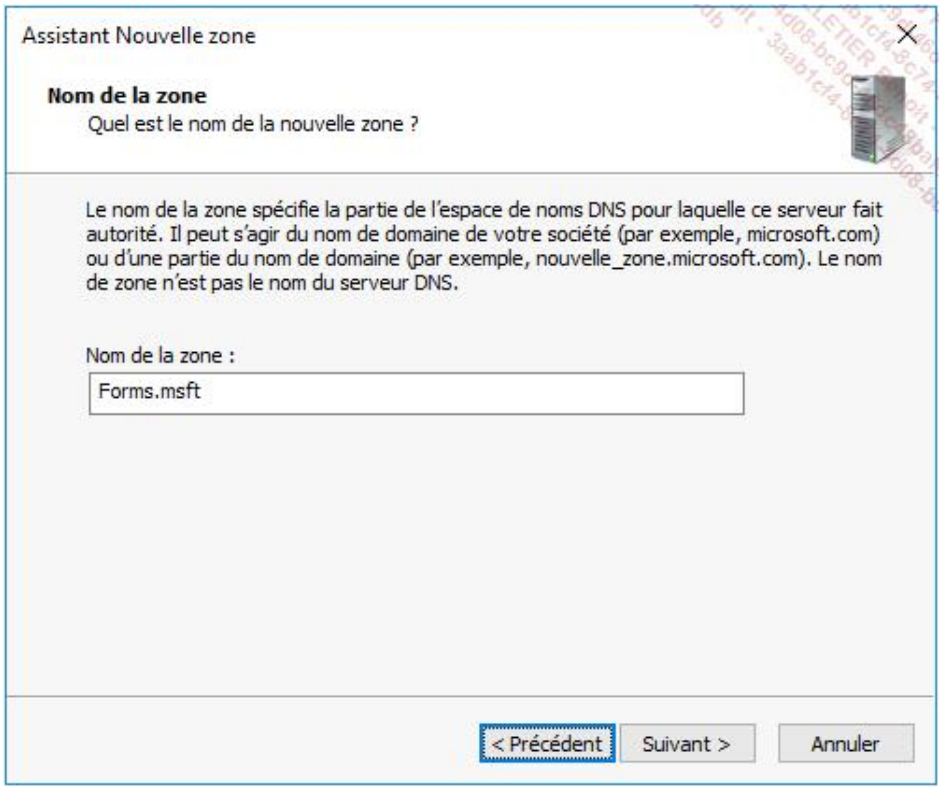


La réplication de la zone peut se faire sur tous les serveurs DNS du domaine Formation.local ou sur les serveurs DNS de la forêt Formation.local.

- Laissez la réplication sur **Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : Formation.local** et cliquez sur **Suivant**.

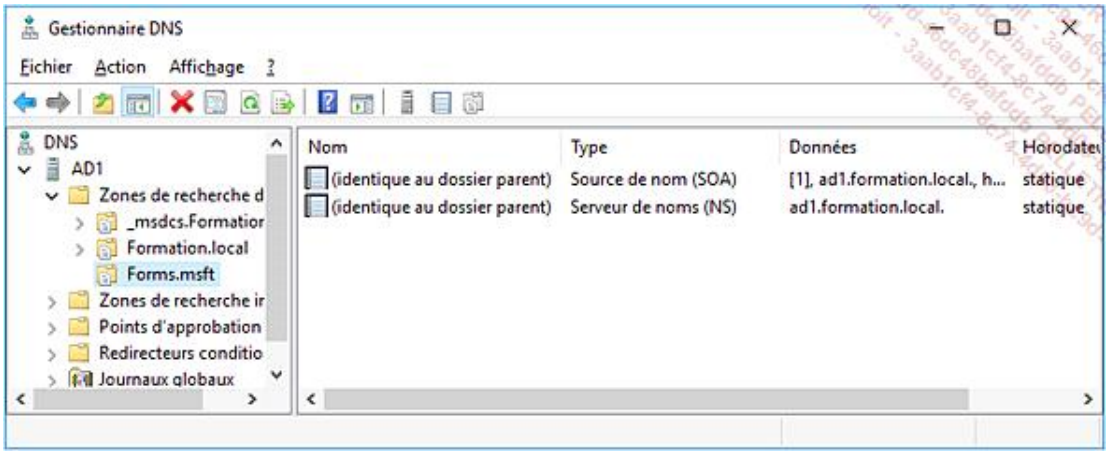


- Saisissez **Forms.msft** dans le champ **Nom de la zone**.

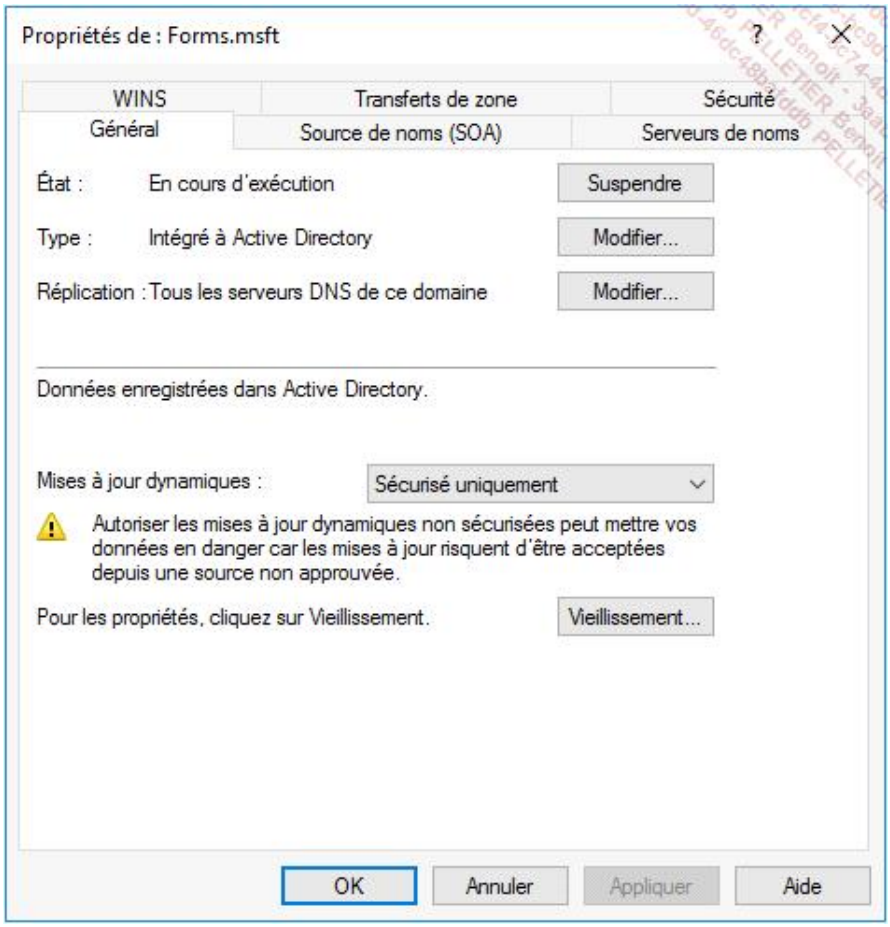


- Laissez le choix par défaut dans la fenêtre **N'autoriser que les mises à jour dynamiques sécurisées** (recommandé pour Active Directory) puis cliquez sur **Next**.

La zone est maintenant présente dans la console DNS.



Dans les propriétés de celle-ci, on peut voir qu'elle est bien intégrée à AD.



Le serveur DNS peut maintenant résoudre des noms du domaine Forms.msft.

3. Création d'une zone de recherche inversée

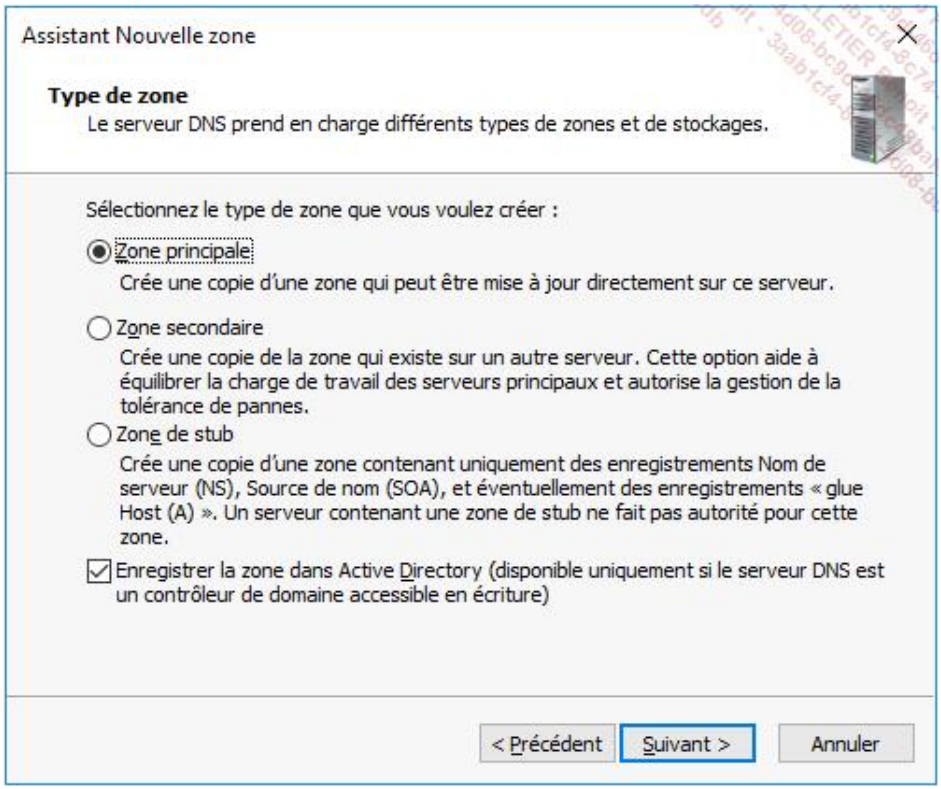
L'ajout d'une zone de recherche inversée dans DNS est semblable sous de nombreux aspects à la création d'une zone de recherche directe. Elle permet la résolution d'adresses IP en noms de postes.

La zone de recherche inversée est un sous-domaine du domaine in-addr.arpa. Les recherches pour les domaines IPv4 et IPv6 (ip6.arpa) sont prises en charge.

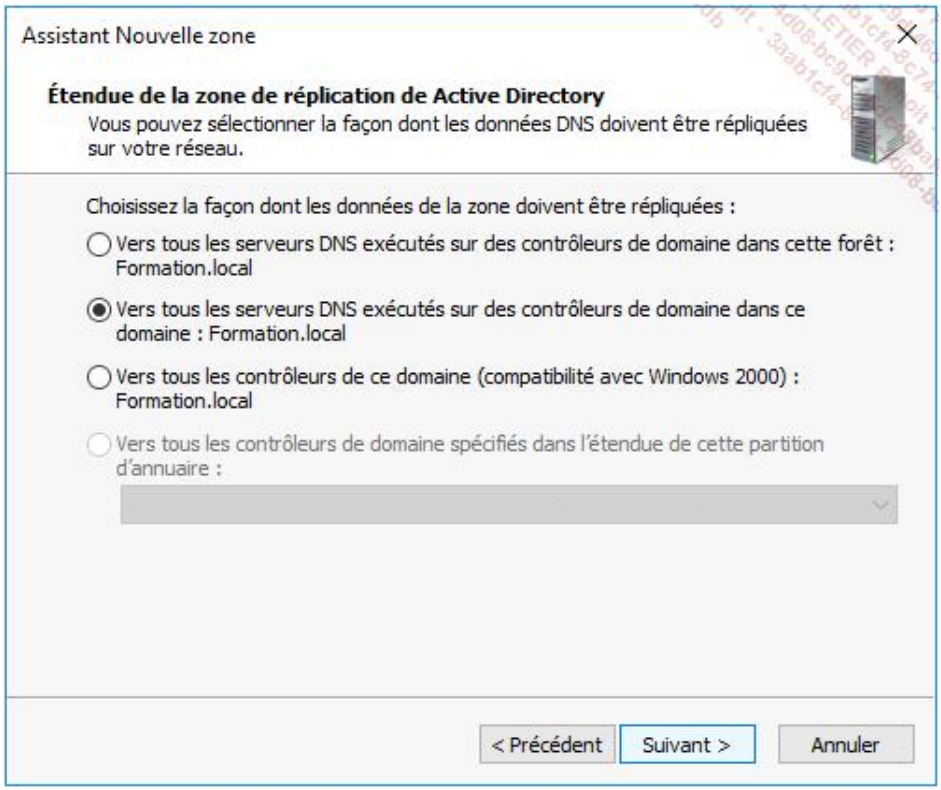
Le nom est construit avec l'adresse réseau. Ainsi le nom de la zone est créé en effectuant une inversion de l'ordre des octets de l'adresse IP, suivie de in-addr.arpa ou ip6.arpa.

Si l'ID réseau est 172.16, le nom de la zone de recherche inversée est alors 16.172.in-addr.arpa. L'outil de ligne de commande dnscmd permet également la création de zone.

- Lancez la console DNS sur AD1.
- Déroulez **AD1** puis **Zones de recherche inversée**.
- Effectuez un clic droit sur le dossier **Zones de recherche inversée** puis sélectionnez **Nouvelle zone**.
- Laissez le choix par défaut dans le type de zone (**Enregistrer la zone dans Active Directory**).



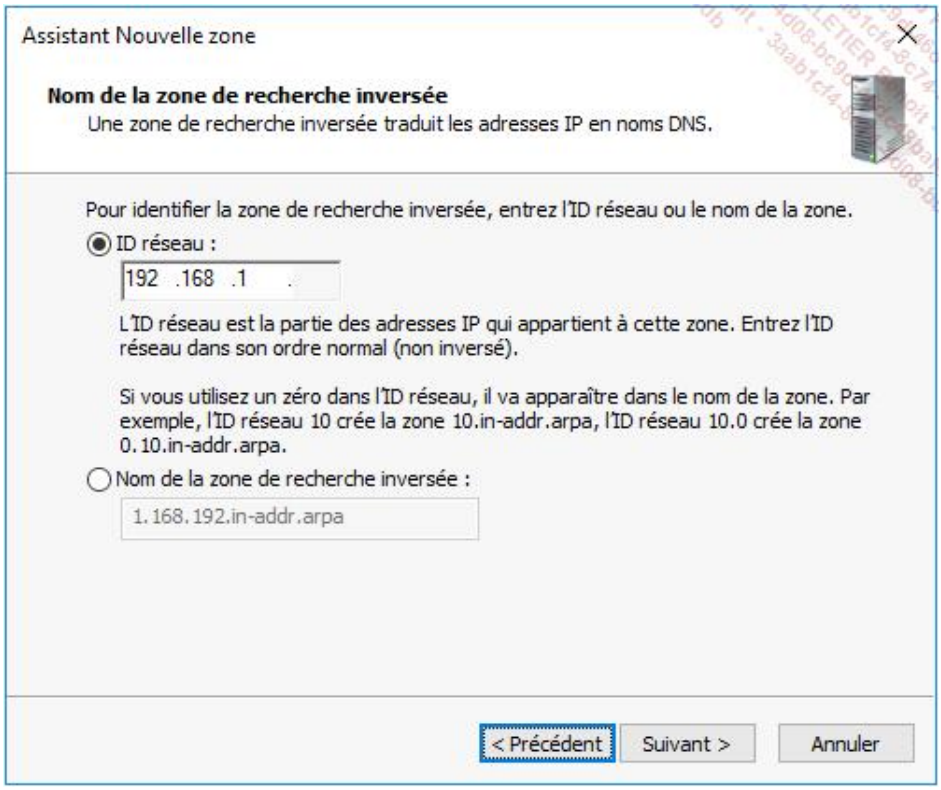
- Laissez le choix par défaut dans la fenêtre **Étendue de la zone de réplication de Active Directory**.



- La zone doit être capable de résoudre des adresses IP en IPv4, laissez le choix par défaut dans la fenêtre du choix du type de zone.

L'adresse IP du serveur est 192.168.1.10 et le masque de sous-réseau est 255.255.255.0. L'ID réseau est donc sur 3 octets soit 192.168.1.

- Saisissez 192.168.1 dans le champ **ID réseau**.



- La zone est intégrée à AD. Autorisez uniquement les mises à jour dynamiques sécurisées (recommandé pour Active Directory).

La zone apparaît dans la console.

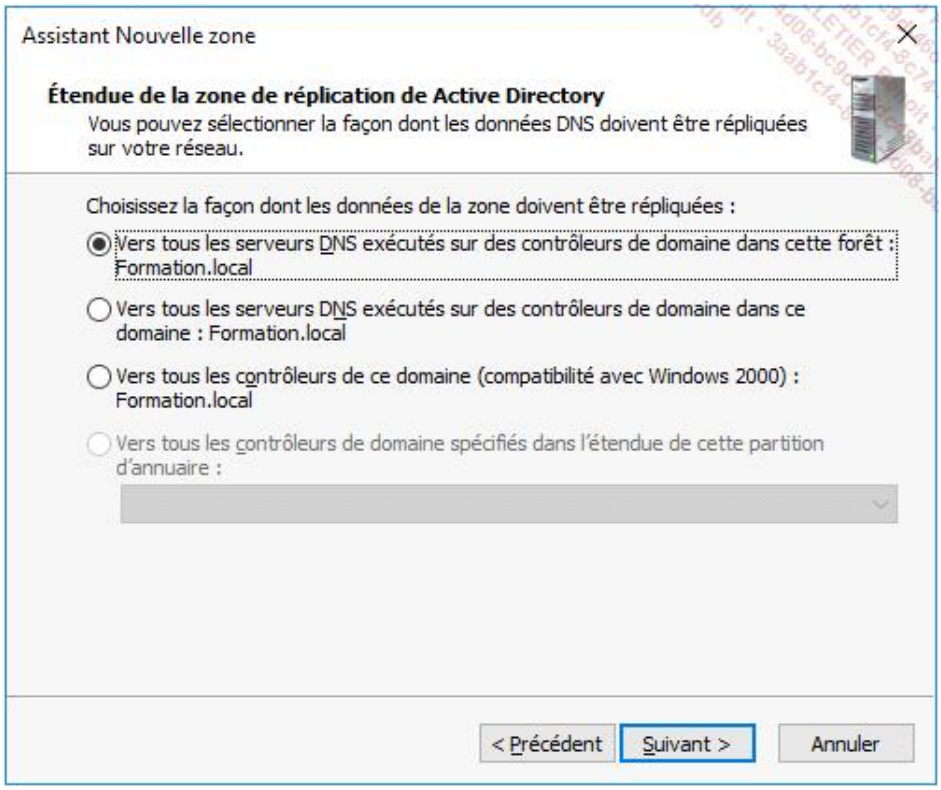
4. Création d'une zone GlobalNames

Une des opérations les plus courantes sur les réseaux informatiques est la résolution de noms. Outre les noms DNS, on trouve également la résolution de noms NetBIOS. Ce dernier n'est pas composé du nom du domaine mais d'un simple nom en une partie (exemple : **POSTE01**). Dans certains cas, il est nécessaire de déployer un serveur WINS (*Windows Internet Naming Service*), alternative à DNS. WINS et NetBIOS ne prennent pas en charge le protocole IPv6. Ils sont donc appelés à disparaître progressivement.

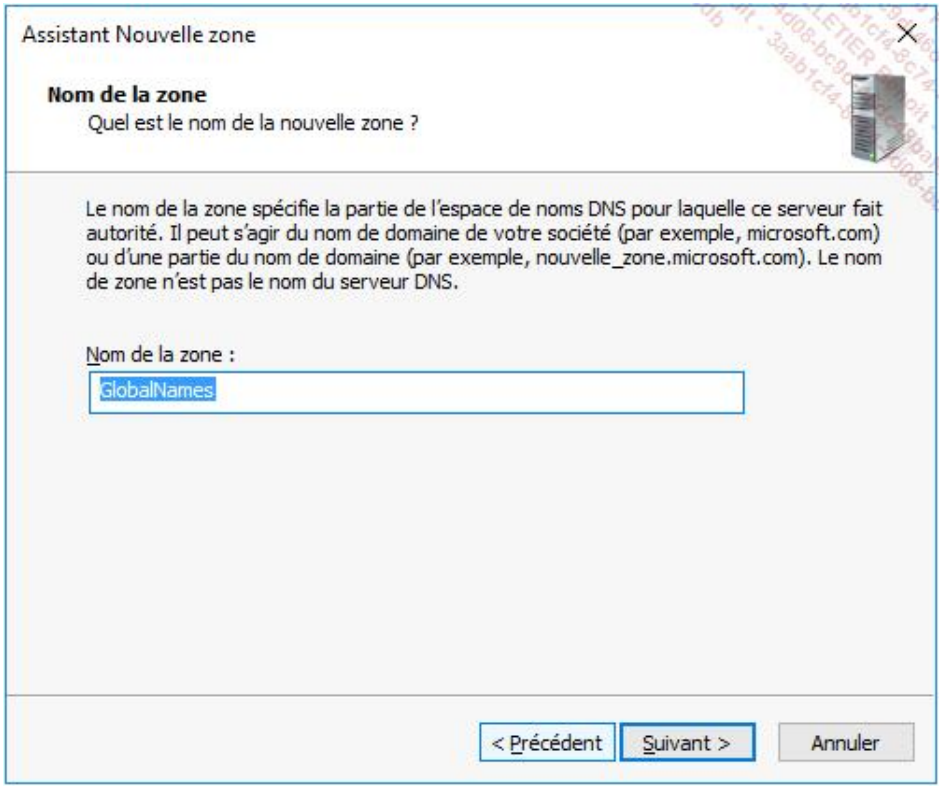
Depuis Windows Server 2008, il est possible de créer une zone spéciale nommée GlobalNames dans le serveur DNS. Avec cette dernière, on peut faire résoudre des noms en une partie par le serveur DNS.

Néanmoins, la zone GlobalNames n'a pas pour fonction de remplacer totalement le service WINS. En effet, la zone ne doit servir qu'à résoudre des noms statiques (les serveurs les plus utilisés…) ; les enregistrements inscrits de manière dynamique doivent continuer à être traités par le serveur WINS.

- Sur AD1, ouvrez la console DNS.
- Déroulez **AD1** puis **Zones de recherche directes**.
- Effectuez un clic droit sur le dossier **Zones de recherche directes** puis sélectionnez **Nouvelle zone**.
- La zone créée est une zone principale intégrée à AD. Laissez le choix par défaut dans la fenêtre **Type de zone**.
- Sélectionnez l'option **Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : Formation.local** puis cliquez sur **Suivant**.

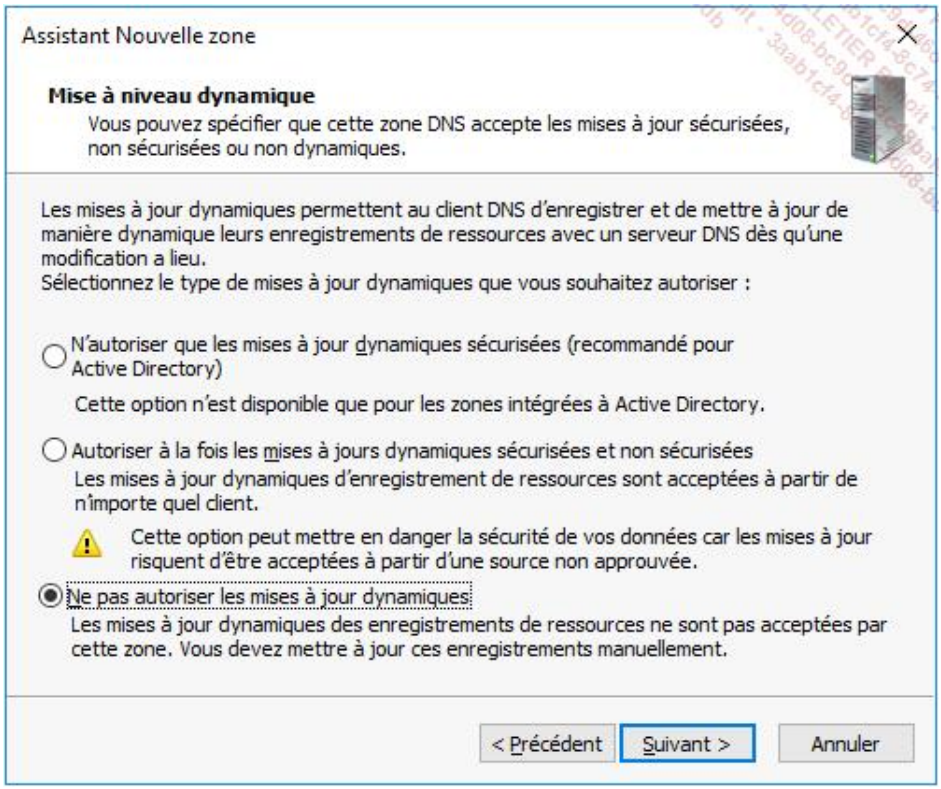


- Saisissez **GlobalNames** dans le champ **Nom de la zone**.



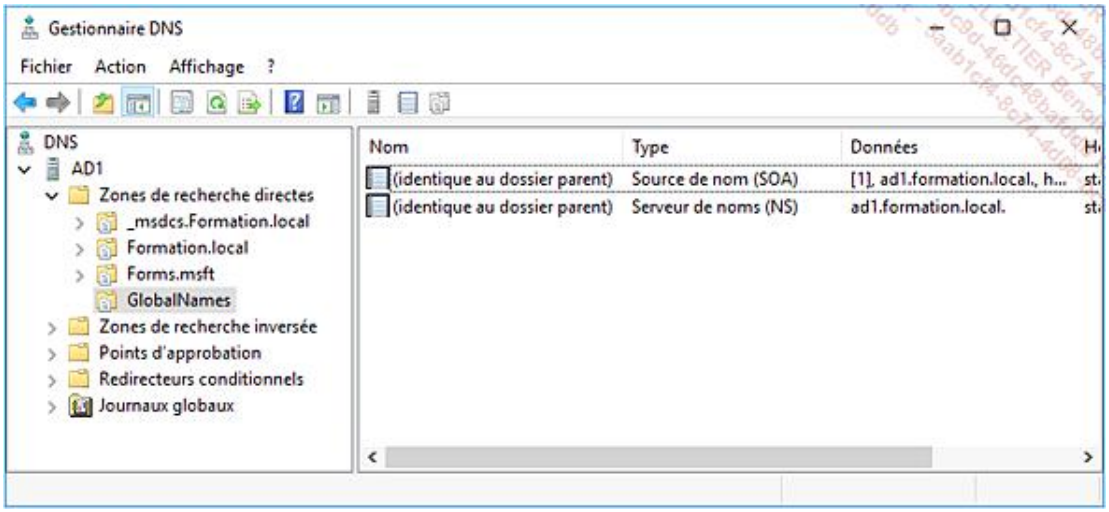
Les enregistrements sont créés par l'administrateur, aucune mise à jour dynamique n'est nécessaire.

- Sélectionnez le bouton radio correspondant au choix **Ne pas autoriser les mises à jour dynamiques**.



- Cliquez sur **Suivant** puis sur **Terminer**.

La zone GlobalNames est maintenant présente dans la console DNS.



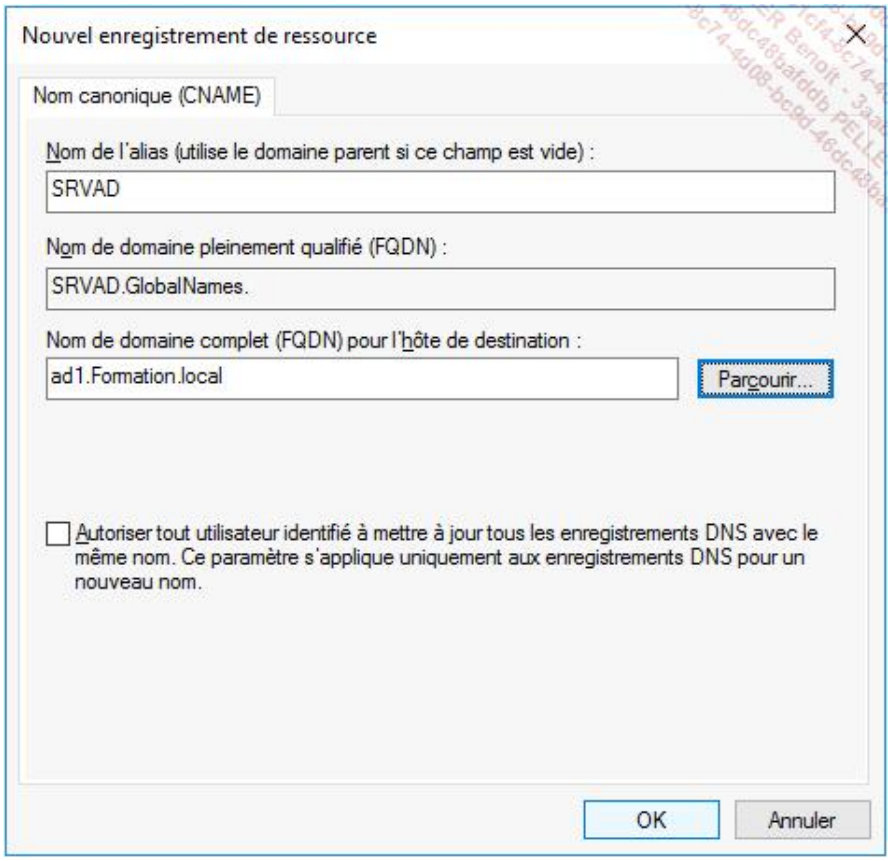
Il faut maintenant activer la prise en charge de la zone GlobalNames.

- Ouvrez une invite de commandes DOS.
- Saisissez la commande `dnscmd AD1 /config /enableglobalnamessupport 1`

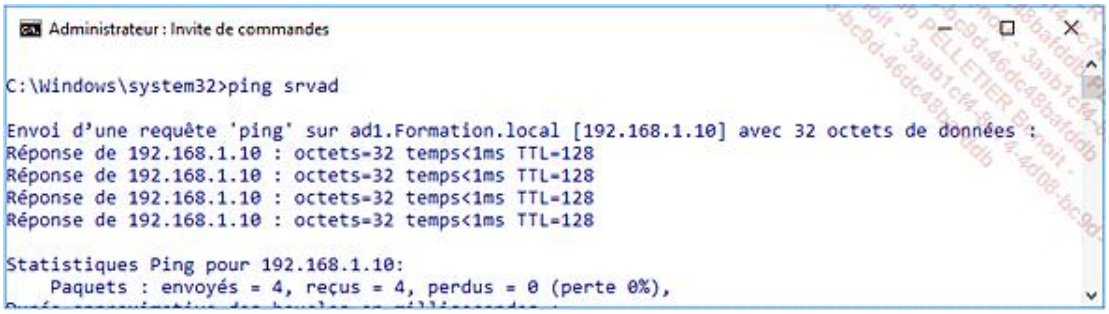
La zone GlobalNames n'est pas disponible pour la résolution de noms tant que la prise en charge de cette zone n'est pas activée de manière explicite au moyen de la commande ci-dessus sur chaque serveur DNS de référence dans la forêt.



- Effectuez un clic droit sur la zone GlobalNames puis sélectionnez **Nouvel alias (CNAME)**.
- Saisissez **SRVAD** dans le champ **Nom de l'alias** puis saisissez **ad1.Formation.local** dans le champ **Nom de domaine complet (FQDN)**.



- Dans une invite de commandes DOS, saisissez `ping SRVAD`. Le serveur **ad1.formation.local** répond.



La résolution se fait correctement et le serveur nous répond.

Gestion du serveur DNS

La mise à jour des enregistrements est un point important. Elle permet d'avoir une base de données qui contient des enregistrements à jour.

Le nettoyage de la zone, qui consiste à supprimer des enregistrements devenus obsolètes, est aussi un point important. Néanmoins, il est nécessaire de s'assurer que l'enregistrement et la zone DNS peuvent être nettoyés et qu'un serveur a la possibilité d'effectuer cette manipulation.

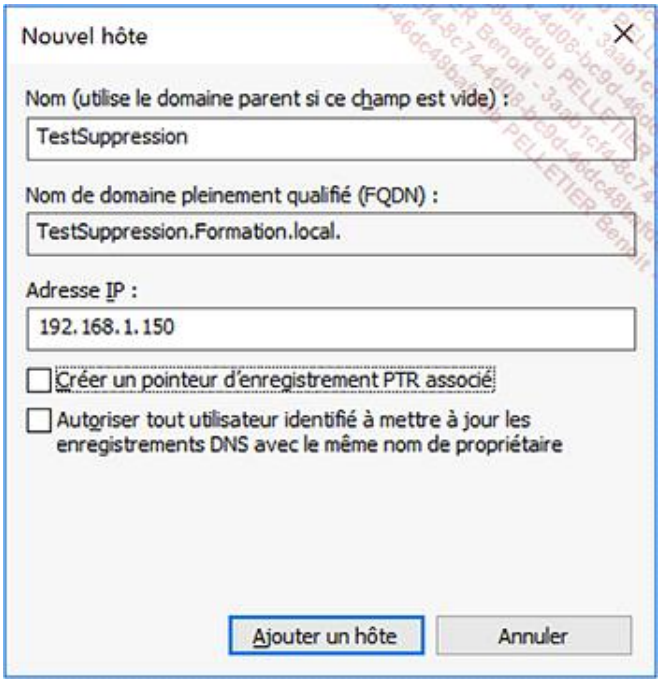
La première vérification concerne l'enregistrement, ce dernier doit être supprimable. Deux types d'enregistrements sont présents dans une zone :

- Les enregistrements statiques.
- Les enregistrements dynamiques.

1. Supprimer des enregistrements

Pour les enregistrements statiques, la suppression automatique est impossible. Une intervention est nécessaire pour autoriser cette opération. La valeur de l'horodateur est à 0 pour les enregistrements statiques.

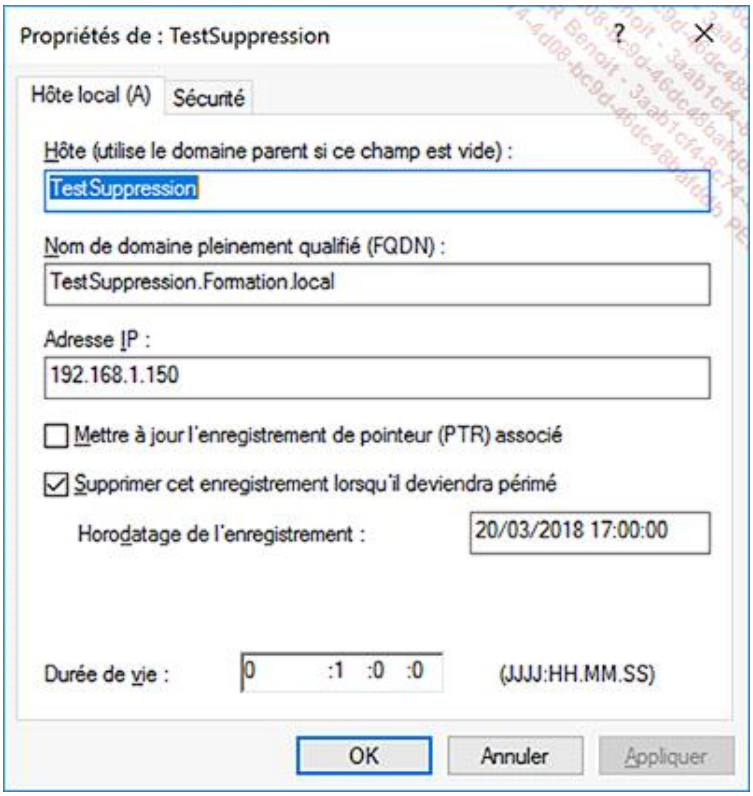
- Lancez la console DNS sur AD1.
- Déroulez **AD1** puis **Zones de recherche directes**.
- Double cliquez sur la zone **Formation.local**.
- Créez un enregistrement de type A, saisissez **TestSuppression** dans le champ **Nom** de l'hôte et **192.168.1.150** dans le champ **Adresse IP**.



- Double cliquez sur l'enregistrement qui vient d'être créé.

Si le champ **Durée de vie** n'est pas présent, activez l'affichage détaillé dans le menu **Affichage** de la console DNS.

- Cochez la case **Supprimer cet enregistrement lorsqu'il deviendra périmé** puis cliquez sur **Appliquer**.



L'horodatage de l'enregistrement s'affiche dans le champ prévu à cet effet.

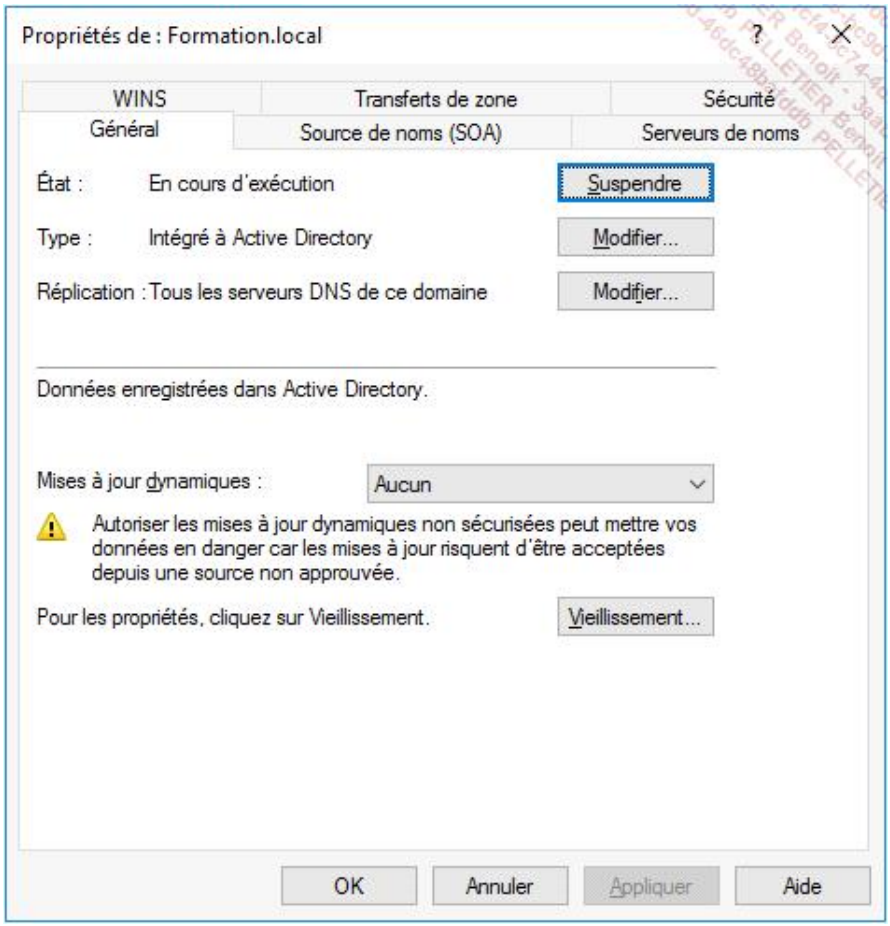
Pour les enregistrements dynamiques, les postes tentent de mettre à jour l'enregistrement toutes les 24 heures. Un horodatage est associé à l'enregistrement et il est mis à jour si la zone permet le nettoyage. La valeur de l'horodateur correspond à la date de création de l'enregistrement ou à la date de la mise à jour.

2. Définir le vieillissement pour les zones

Le vieillissement, qui consiste à supprimer les enregistrements obsolètes, peut être configuré pour une ou l'ensemble des zones du serveur DNS.

Pour la configuration du vieillissement, la manipulation est à faire sur une zone ou dans les propriétés du serveur pour l'application sur l'ensemble des zones.

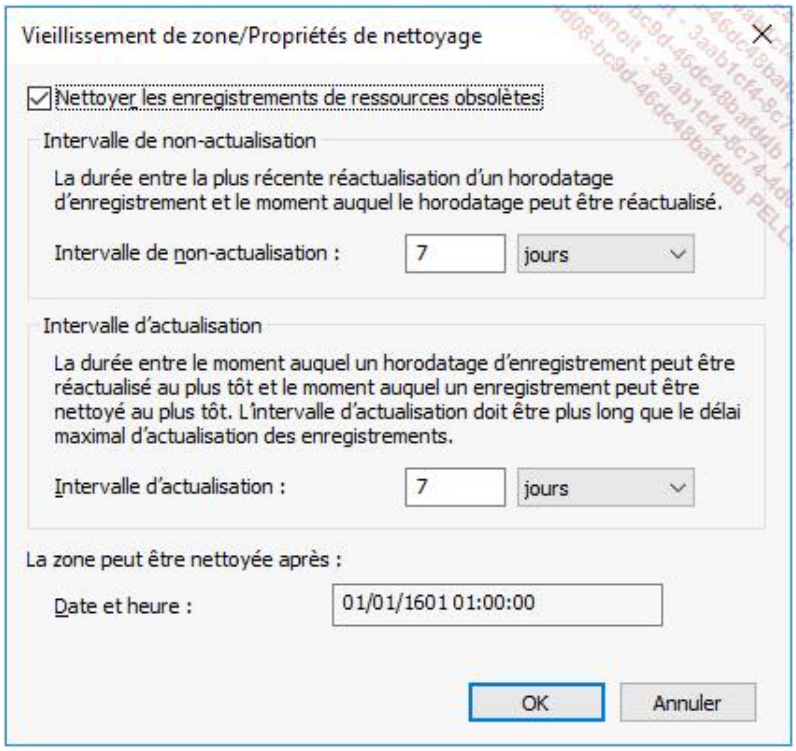
- Cliquez avec le bouton droit sur la zone **Formation.local** puis sélectionnez **Propriétés**.
- Dans la fenêtre qui s'affiche, cliquez sur le bouton **Vieillissement**.



La fenêtre est composée de deux champs :

- **Intervalle de non-actualisation** : indique une constante de temps durant laquelle l'horodatage ne peut être modifié.
- **Intervalle d'actualisation** : indique le moment où un horodatage peut être actualisé et l'enregistrement supprimé.

La case à cocher **Nettoyer les enregistrements de ressources obsolètes** doit être cochée pour activer le nettoyage automatique.

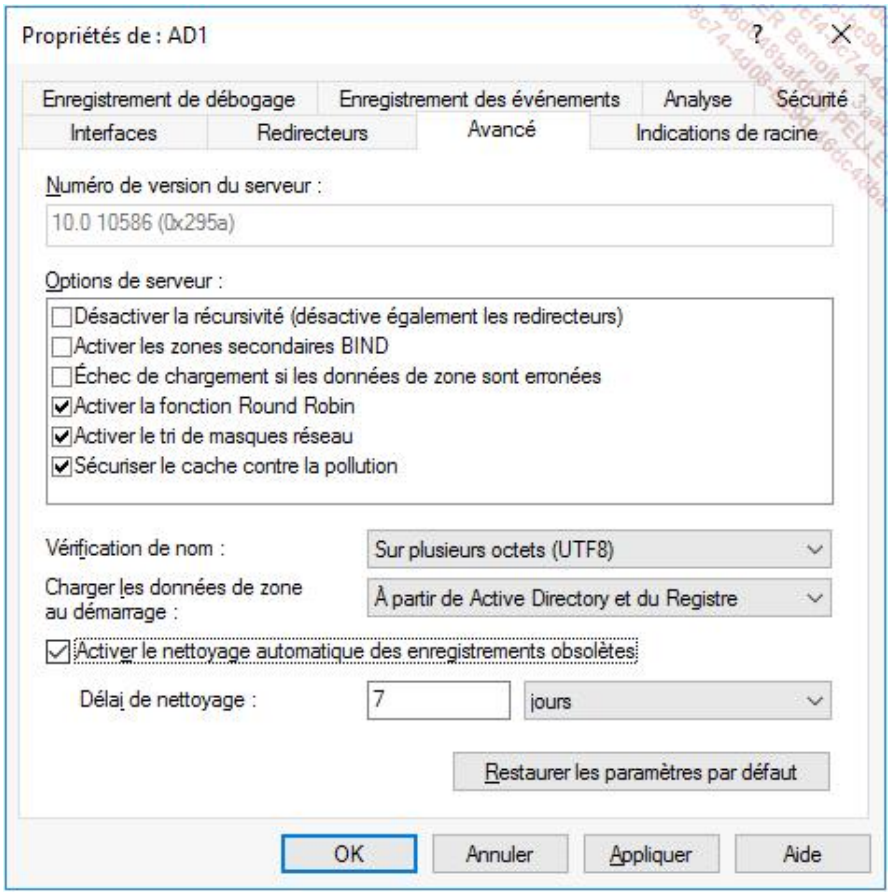


- Pour configurer de la même façon toutes les zones, effectuez un clic droit sur le serveur puis sélectionnez **Définir le vieillissement/nettoyage pour toutes les zones...**.

Ces valeurs sont configurées pour toutes les zones.

3. Activer le nettoyage automatique

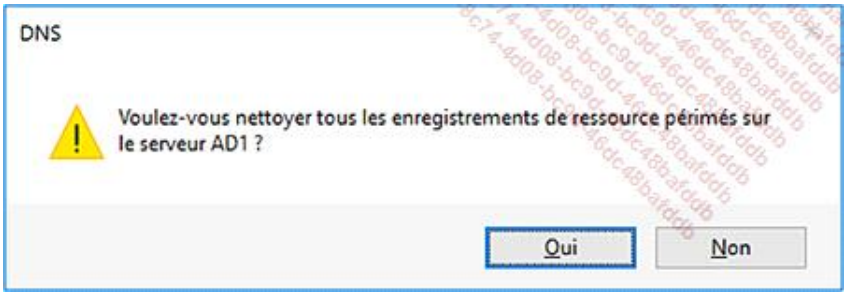
- Dans la console DNS, effectuez un clic droit sur **AD1** puis sélectionnez **Propriétés**.
- Cliquez sur l'onglet **Avancé** et cliquez sur la case à cocher **Activer le nettoyage automatique des enregistrements obsolètes**.



- Indiquez le **Délai de nettoyage** souhaité puis cliquez sur **OK**.

4. Effectuer un nettoyage manuel

- Dans la console DNS, effectuez un clic droit sur le serveur puis sélectionnez **Nettoyer les enregistrements de ressources obsolètes**.
- Cliquez sur **Oui** dans la boîte de dialogue afin de lancer le nettoyage.



5. Les différents types de redirecteurs

Quand un serveur DNS doit résoudre un nom externe à la zone sur laquelle il a autorité, il doit interroger des serveurs externes (exemple : un utilisateur veut contacter le site web de nibonnet.fr).

Deux possibilités s'offrent à lui :

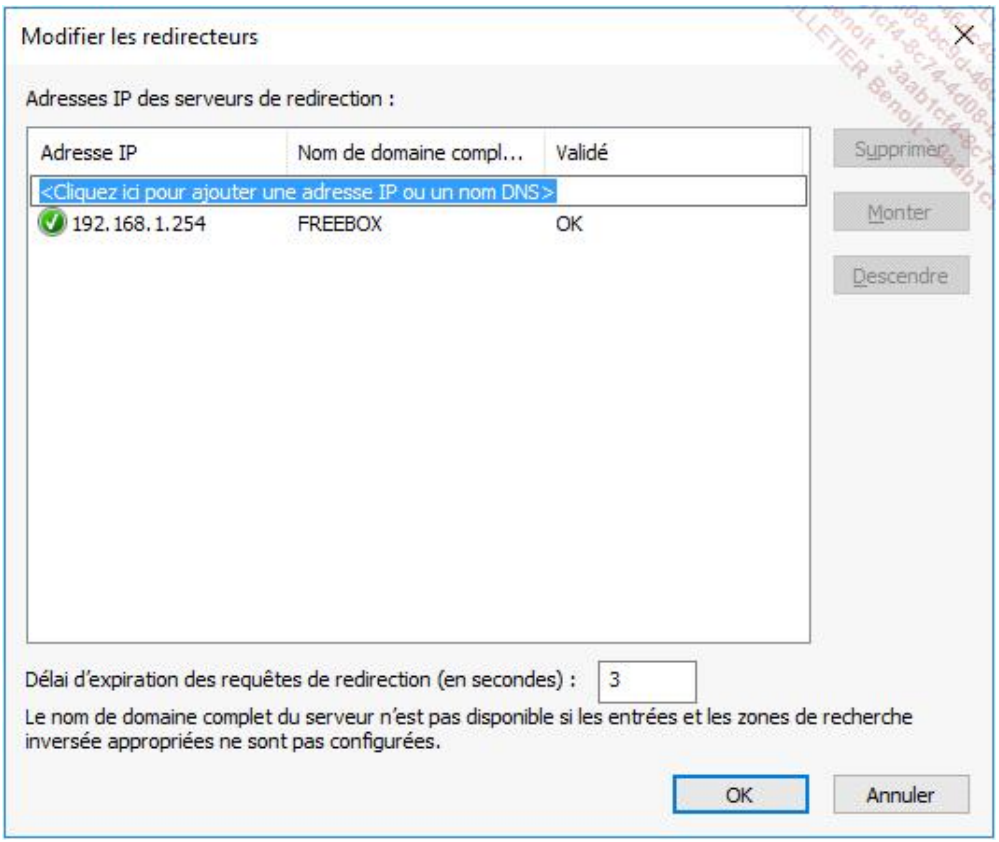
- **Effectuer une requête itérative** : le poste envoie à son serveur DNS interne une requête afin de résoudre le nom

www.nibonnet.fr. Le serveur DNS interroge successivement le serveur racine, qui le renvoie vers le serveur ayant autorité sur la zone FR, et le serveur de la zone FR qui le renvoie vers le serveur prenant en charge la zone nibonnet. Enfin, le serveur ayant autorité sur la zone nibonnet peut résoudre le nom www.nibonnet.fr. Le serveur DNS interne peut désormais répondre à son client.

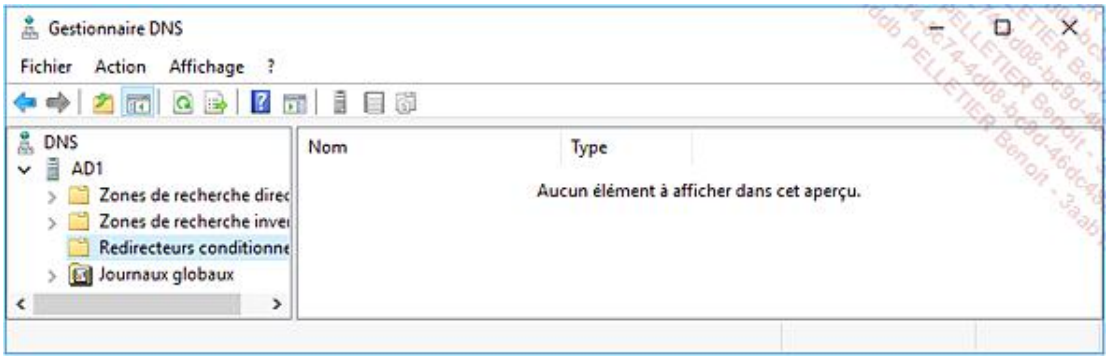
- **Effectuer une requête récursive** : le client fait une demande de résolution du nom www.nibonnet.fr à son serveur DNS interne. Ce dernier, n'ayant pas autorité sur la zone nibonnet, va utiliser le redirecteur configuré par l'administrateur pour envoyer la demande à un autre serveur DNS (généralement le serveur DNS du FAI). Ce dernier peut posséder dans son cache la réponse à la demande faite ou effectuer une requête itérative.

Pour toute demande pour laquelle le serveur n'a pas autorité, le redirecteur est utilisé. Dans certains cas (approbation de forêt AD…) il est nécessaire que la demande de résolution qui va être envoyée à un autre serveur DNS soit redirigée en fonction du nom de domaine (exemple : pour le domaine Eni.fr, envoyer la demande à SRVDNS1). Le redirecteur conditionnel permet d'effectuer cette modification et d'aiguiller les requêtes vers le bon serveur si la condition (nom de domaine) est validée.

- Pour configurer un redirecteur, effectuez un clic droit sur le serveur **AD1** puis sélectionnez **Propriétés**.
- Cliquez sur l'onglet **Redirecteurs** puis sur le bouton **Modifier**.
- Saisissez l'adresse du redirecteur à utiliser puis appuyez sur [Entrée].



- Cliquez deux fois sur **OK** pour valider le redirecteur.
- Si vous souhaitez créer un redirecteur conditionnel, effectuez un clic droit sur le dossier **Redirecteurs conditionnels** puis cliquez sur **Nouveau redirecteur conditionnel**.

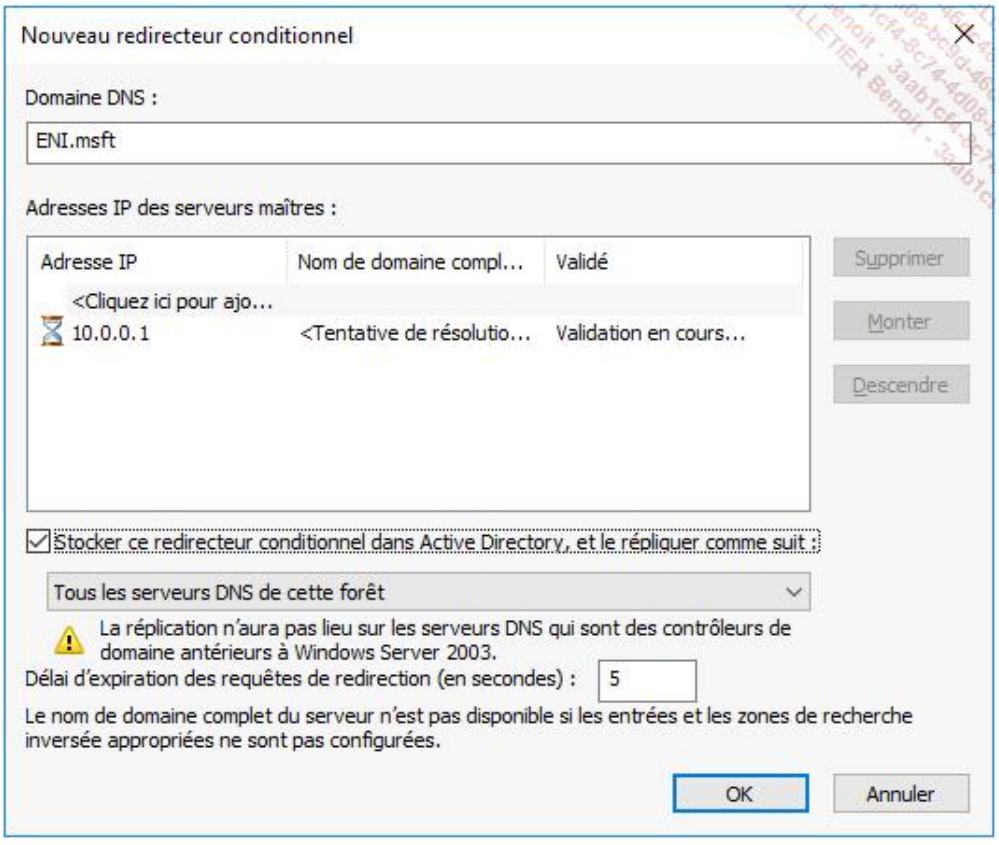


- Saisissez **ENI.msft** dans le champ **Domaine DNS** puis l'adresse IP du redirecteur (**10.0.0.1**).

Le redirecteur peut être répliqué dans toute la forêt ou uniquement sur le domaine.

- Laissez le choix de la réplication sur **Tous les serveurs DNS de cette forêt**.

L'adresse IP du serveur ne sert que d'exemple et n'est pas présente dans la maquette.

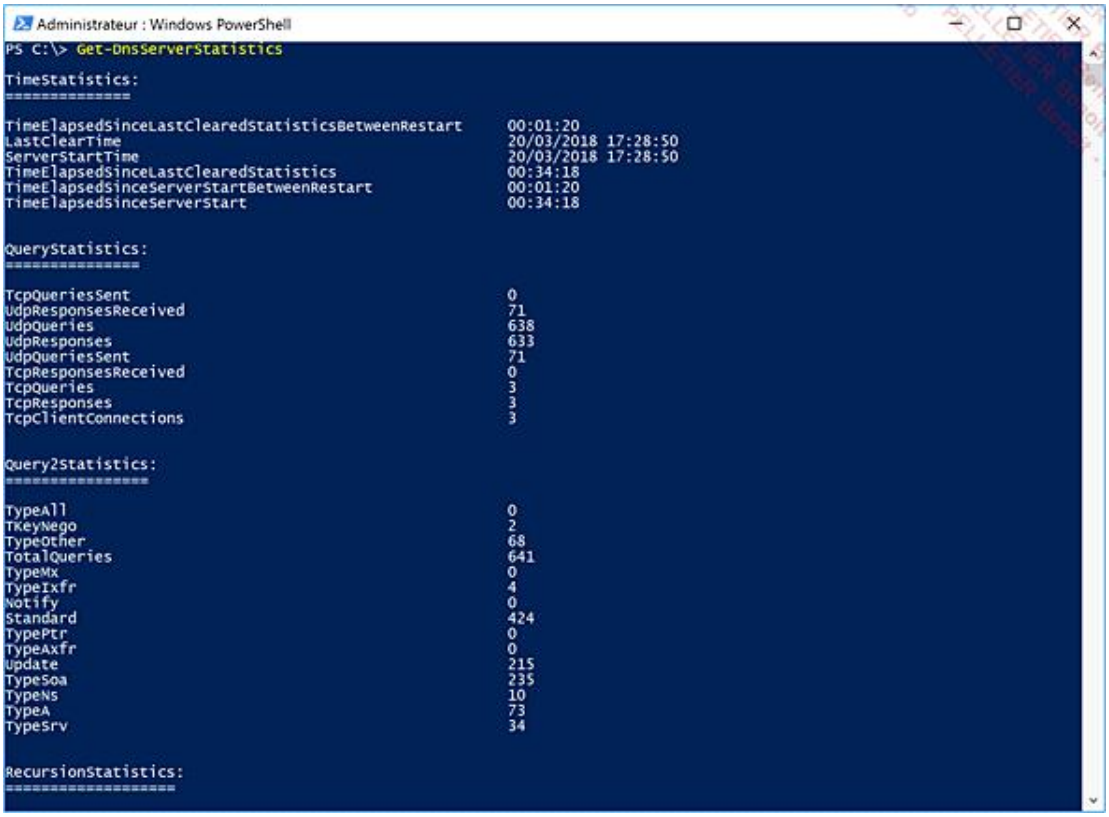


- Cliquez sur **OK**.

6. Utilisation des statistiques au niveau du service DNS

Depuis Windows Server 2012 R2, il est possible d'obtenir des statistiques aux niveaux d'une zone.

La récupération de ces informations s'effectue à l'aide de la cmdlet PowerShell Get-DnsServerStatistics.

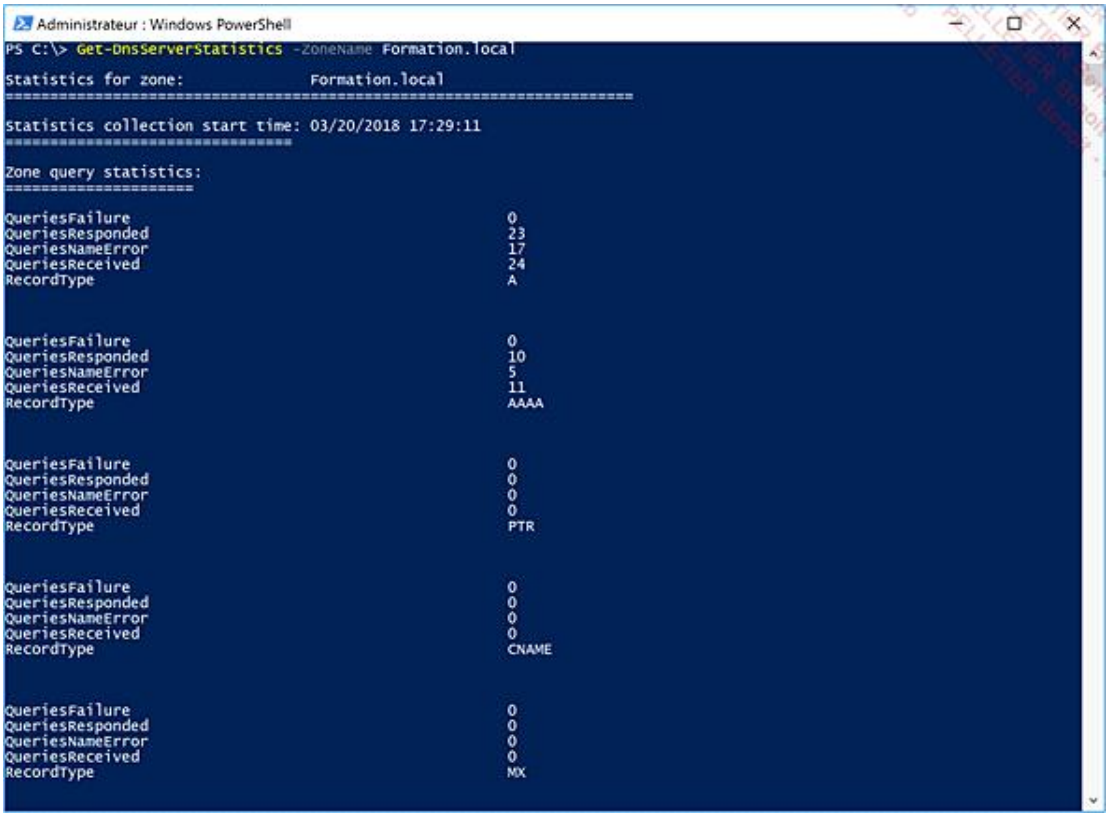


En utilisant le commutateur **-ZoneName** suivi du nom de la zone, d'autres informations sont disponibles.

ZoneQueryStatistics permet de récupérer des informations importantes telles que les requêtes en échec ou des erreurs au niveau des requêtes.

Il est également possible de connaître le nombre total de requêtes reçues pour un type d'enregistrement ou le nombre de requêtes qui ont abouti sur une réponse valide.

Enfin, on peut avoir des renseignements sur les différents types de ressources (enregistrement A, AAAA, PTR, CNAME, MX…).



ZoneTransferStatistics fournit des informations sur le transfert de zone (transactions AXFR et IXFR), soit le nombre total de requêtes de transfert de zone reçues et envoyées par le serveur DNS.

ZoneUpdateStatistics fournit des informations concernant les mises à jour dynamiques. On peut ainsi voir le nombre de requêtes reçues et le nombre de requêtes en échec.

7. Création de politique DNS

Il est maintenant possible de créer des politiques DNS, ces dernières offrent la possibilité de contrôler la gestion des requêtes (demande d'adresse IP d'un serveur web, …). Il est ainsi possible de contrôler la réponse en fonction d'un critère (serveur proche du poste qui a fait la demande…).

D'autres types de règles peuvent être configurés. Il est ainsi possible de gérer la redirection des clients afin qu'ils contactent un serveur proche d'eux.

Mais cette fonctionnalité peut également servir à mettre en place des politiques pour les transferts de zone. On peut ainsi indiquer si un transfert de zone est autorisé ou interdit. Cette opération peut être effectuée au niveau du serveur ou simplement pour la zone concernée. Ainsi il est maintenant aisée de configurer des listes blanches (autorisant le transfert de zone) ou des listes noires (interdisant le transfert de zone).

La commande DNS ci-dessous permet de refuser le transfert de la zone nibonnet.local pour toute requête provenant du réseau 192.168.1.0.

```
Add-DnsServerZoneTransferPolicy -Name DenyTransferNibonnet
-Zone nibonnet.local -Action DENY -ClientSubnet "EQ,192.168.1.0/24"
```

La personnalisation du serveur DNS peut être faite de manière plus fine.

8. Gestion du DNS à l'aide de PowerShell

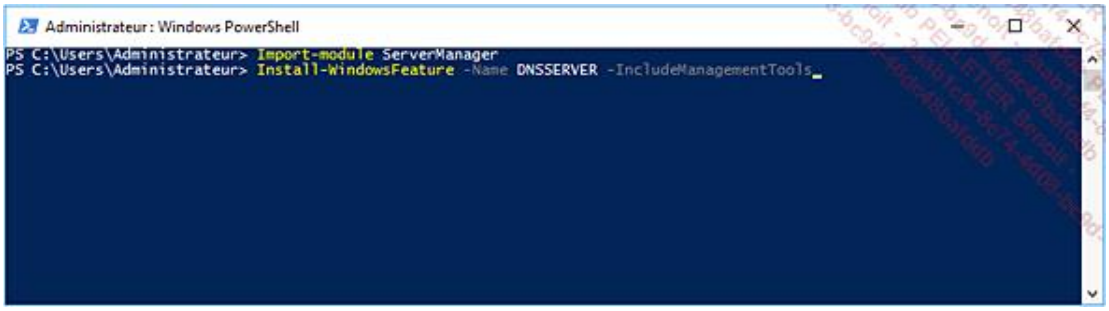
Le rôle DNS peut être administré par l'intermédiaire de l'interface graphique ou via des cmdlets PowerShell. Les différents exemples ci-dessous permettent d'effectuer l'installation du rôle mais également la création de zones ou d'enregistrements.

Installation du rôle

L'ajout du rôle s'effectue à l'aide de la cmdlet.

La commande ci-dessous peut être utilisée pour procéder à l'installation d'un serveur DNS.

```
Import-module ServerManager
Install-WindowsFeature -Name DNSSERVER -IncludeManagementTools
```



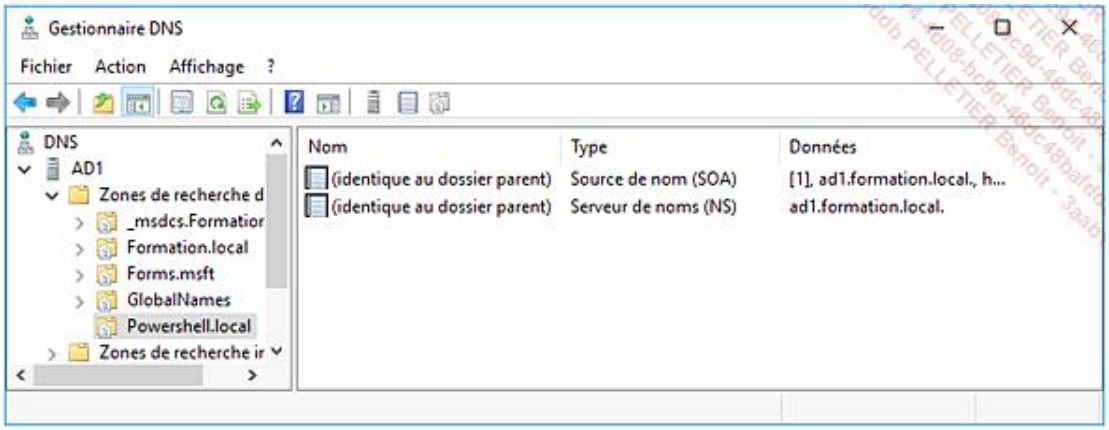
Après avoir procédé à l'installation, il est maintenant possible d'ajouter une zone primaire, cette dernière ne sera pas intégrée à AD. Un fichier nommé Powershell.local.dns va être créé afin de contenir les différents enregistrements de la zone.

La commande ci-dessous permet d'effectuer cette opération.

```
Add-dnsserverprimaryzone -name "Powershell.local"
-zonefile "Powershell.local.dns"
```



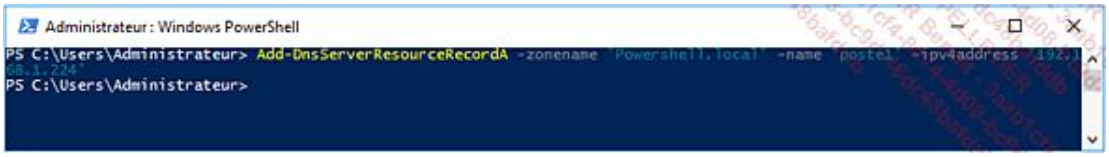
La zone est maintenant créée.



Il est maintenant possible d'ajouter des enregistrements dans la zone Powershell.local.

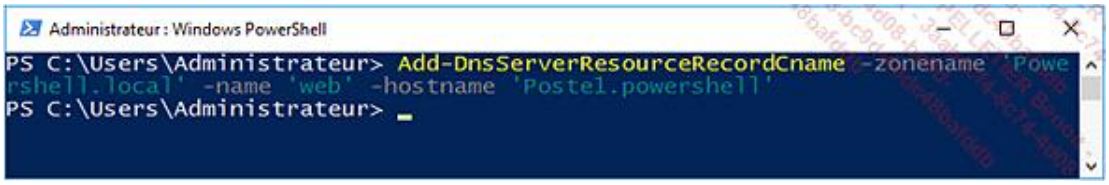
Enregistrement de type A

```
Add-DnsServerResourceRecordA -zonename 'Powershell.local'
-name 'poste1' -ipv4address '192.168.1.224'
```

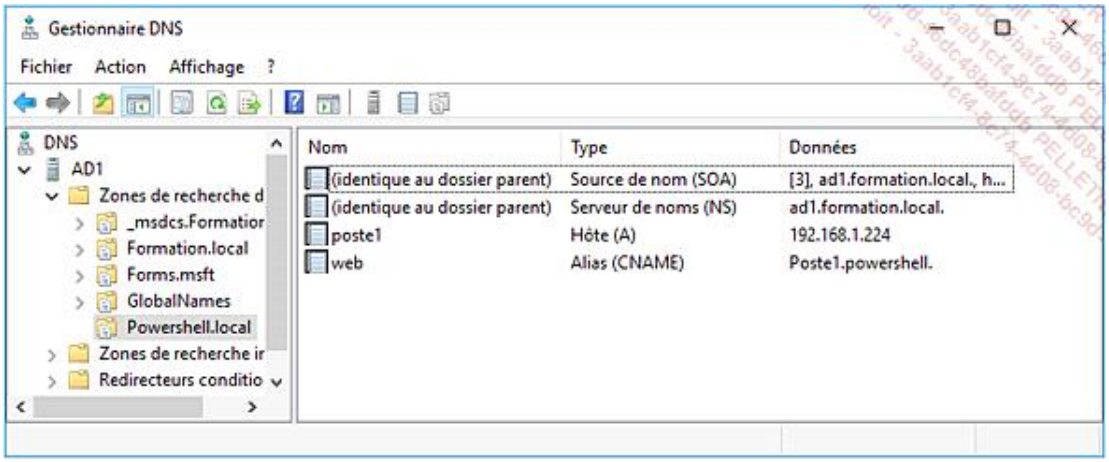


Enregistrement de type CName

```
Add-DnsServerResourceRecordCname -zonename 'Powershell.local'
-name 'web' -hostname 'Poste1.powershell.local'
```



Les enregistrements sont présents dans la zone.


Gestionnaire DNS
Fichier Action Affichage ?
DNS
AD1
Zones de recherche d
_msdcs.Formatior
Formation.local
Forms.msft
GlobalNames
Powershell.local
Zones de recherche ir
Redirecteurs conditio
Nom
Type
Données
(identique au dossier parent)
Source de nom (SOA)
[3], ad1.formation.local., h...
(identique au dossier parent)
Serveur de noms (NS)
ad1.formation.local.
poste1
Hôte (A)
192.168.1.224
web
Alias (CNAME)
Poste1.powershell.

Gestion des enregistrements

Plusieurs types d'enregistrements peuvent être créés dans le serveur DNS. Ils permettent la résolution d'un nom de poste, d'une adresse IP ou tout simplement de trouver un contrôleur de domaine, un serveur de noms ou un serveur de messagerie.

La liste ci-dessous présente les enregistrements les plus courants :

- **Enregistrements A et AAAA (Address Record)** : permettent de faire correspondre un nom de poste à une adresse IPv4. L'enregistrement AAAA permet la résolution de noms de poste en adresse IPv6.
- **CNAME (Canonical Name)** : un alias est créé vers le nom d'un autre poste. Le poste concerné est accessible via son nom ainsi que via son alias.
- **MX (Mail Exchange)** : définit les serveurs de courrier pour le domaine.
- **PTR (Pointer Record)** : associant une adresse IP à un enregistrement de noms de domaine, il est le contraire d'un enregistrement de type A. Cet enregistrement est créé dans la zone de recherche inverse.
- **NS (Name Server)** : définit les serveurs de noms du domaine.
- **SOA (Start Of Authority)** : l'enregistrement donne les informations générales de la zone (serveur principal, e-mail de contact, durée d'expiration…).
- **SRV** : permet de définir un serveur spécifique pour une application, notamment pour la répartition de charge.

Le système de fichiers NTFS

NTFS (*New Technology File System*) est créé et utilisé par Windows NT et ses versions supérieures. Apparu en 1993, il est inspiré du système conçu pour OS/2.

Il permet la gestion des droits de sécurité (ACL - *Access Control List*) positionnés sur une ressource (boîte mail, fichier…). Ce système permet d'effectuer également le chiffrement du contenu d'un répertoire à l'aide du protocole EFS, de compresser un fichier ou de mettre en place une politique de quota.

1. Les autorisations NTFS

L'ACL, ou liste de contrôle d'accès, donne des permissions d'accès sur une ressource à un ensemble d'utilisateurs ou groupe.

L'ACE (*Access Control Entries*) est une liste qui est composée généralement de comptes utilisateurs, de comptes ordinateurs ou de groupes qui ont accès à la ressource. Pour chacune de ces entrées ACE, une autorisation d'accès (autoriser ou refuser) est attribuée.

De la racine d'un lecteur jusqu'au fichier, toutes les ressources possèdent une ACL. Les autorisations d'accès se cumulent toujours avec celles du parent, on appelle cela l'héritage (un dossier enfant hérite des autorisations du dossier parent). Le cumul des autorisations d'accès produit les droits finaux que l'utilisateur, l'ordinateur ou le groupe obtient.

Les autorisations sont positionnables sur un répertoire ou sur un fichier. Sur un dossier, la liste des autorisations est la suivante :

- **Contrôle total** : ce droit permet d'effectuer la modification des autorisations sur cette ressource, de devenir propriétaire mais également de modifier ou supprimer le contenu du répertoire (fichier, sous-dossier…).
- **Modification** : cette autorisation donne le droit de suppression d'un répertoire. L'objet qui se voit octroyer ce droit a également celui de lecture et d'exécution.
- **Lecture et exécution** : l'utilisateur peut lire n'importe quel fichier et exécuter un fichier exécutable.
- **Affichage du contenu du dossier** : l'utilisateur peut rentrer dans les sous-répertoires mais la lecture du contenu d'un fichier est interdite.

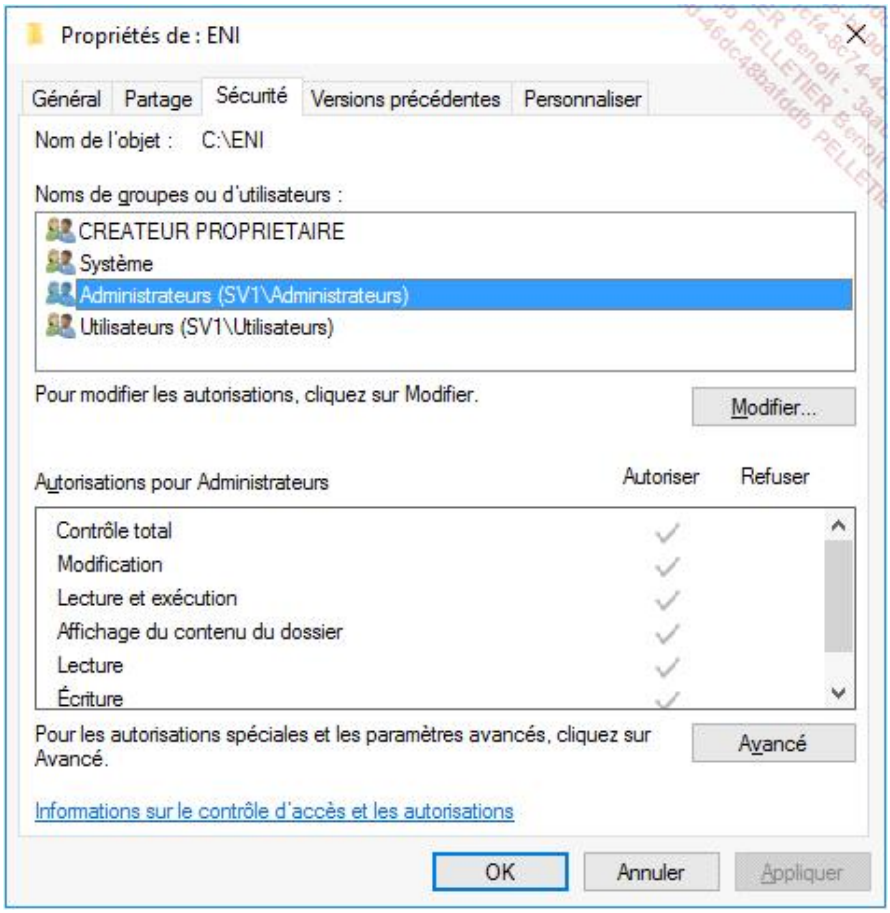
Si l'autorisation est positionnée sur **Refuser**, alors elle deviendra prioritaire. Ce type d'autorisations est à utiliser avec précaution.

Les autorisations peuvent également être positionnées sur un fichier. Comme pour les répertoires, elles permettent de définir le droit accordé à un utilisateur ou à un groupe. Elles sont identiques à celles positionnées sur un dossier (à l'exception de l'autorisation **Affichage du contenu du dossier** qui n'est pas présente sur l'ACL d'un fichier).

2. Héritage des autorisations

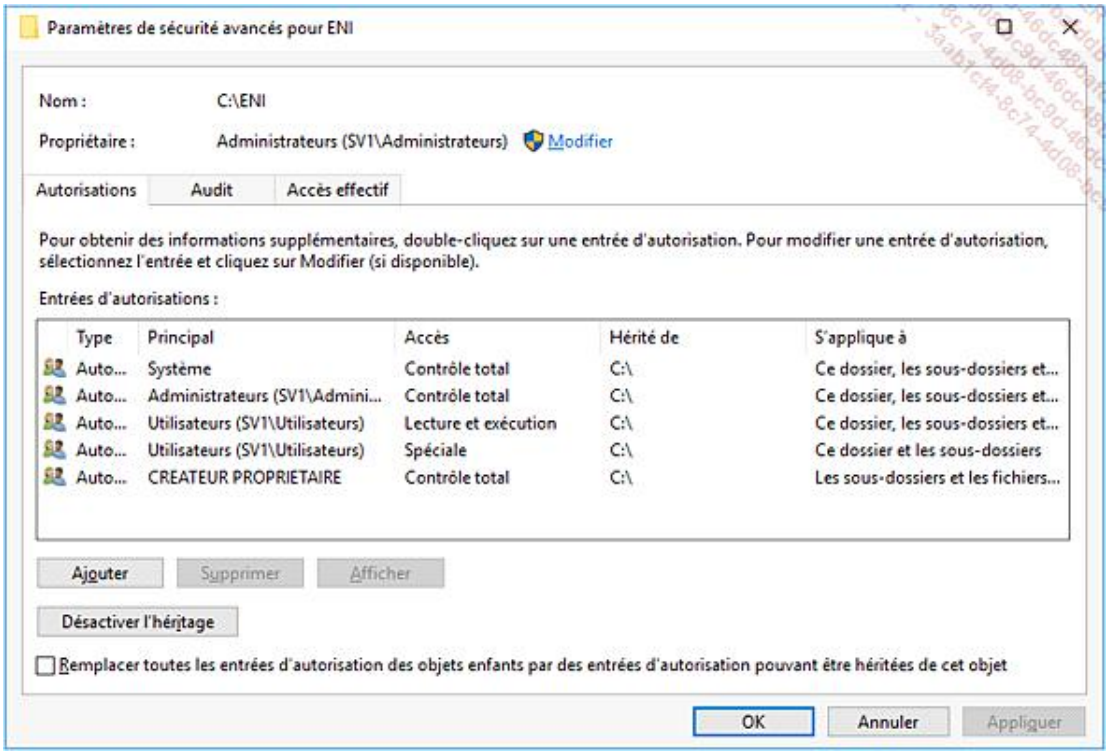
L'héritage facilite la mise en place d'autorisations sur une ressource. Lorsqu'une autorisation est appliquée à une ressource, l'héritage est fait de façon automatique. Des autorisations explicites peuvent malgré tout être positionnées.

Les permissions héritées apparaissent en grisé et ne peuvent être modifiées directement.



L'héritage peut être bloqué sur l'enfant afin de permettre la configuration d'autorisations explicites.

- Dans l'onglet **Sécurité**, cliquez sur **Avancé**.
- Cliquez sur le bouton **Désactiver l'héritage**.



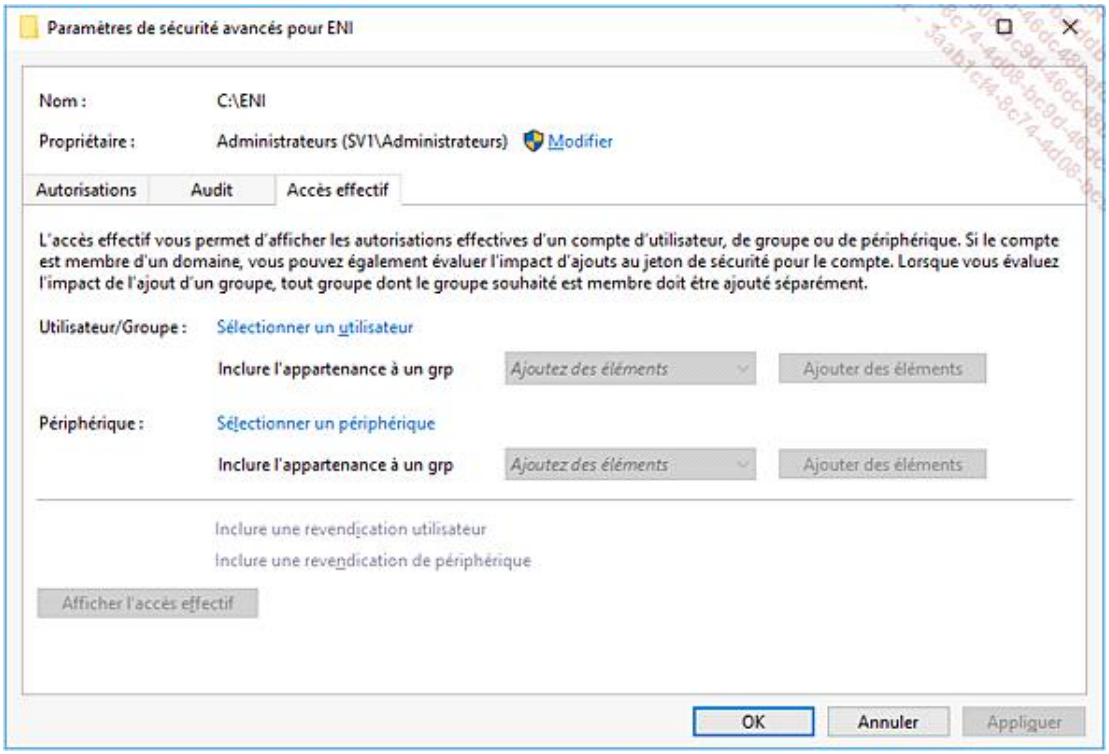
Deux possibilités sont proposées :

- **Convertir les autorisations héritées** : les autorisations héritées présentes dans l'ACL sont transformées en autorisations explicites.
- **Supprimer toutes les autorisations héritées** : les autorisations présentes dans l'ACL sont supprimées et l'ajout de nouvelles autorisations est alors nécessaire.

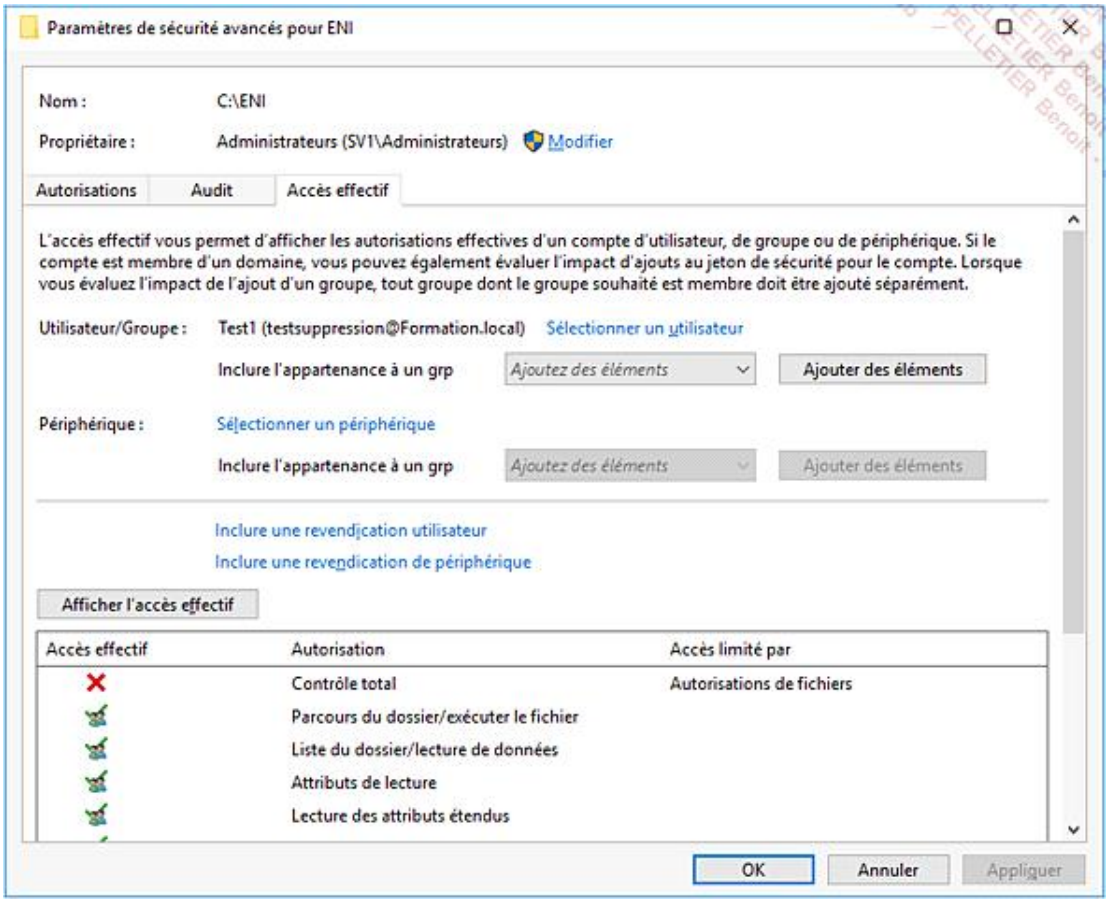
3. L'autorisation effective

Une autorisation effective est une permission finale octroyée à un objet Active Directory (utilisateur, groupe ou ordinateur). Il peut être compliqué de connaître cette autorisation car un résultat différent de celui souhaité peut être obtenu par l'imbrication de plusieurs groupes ou l'affiliation de l'utilisateur à plusieurs groupes. Depuis quelques années, un outil permettant de calculer cette autorisation finale est présent sur les systèmes d'exploitation Microsoft. Très pratique sur des architectures complexes, il permet de savoir en quelques clics le droit qui est donné à un utilisateur.

- Sur un répertoire, accédez à l'onglet **Sécurité**, cliquez sur le bouton **Avancé**.
- Dans la fenêtre qui apparaît, cliquez sur l'onglet **Accès effectif**.



- Cliquez sur le lien **Sélectionner un utilisateur** puis saisissez le nom de l'utilisateur souhaité.
- Validez la saisie en cliquant sur **Vérifier les noms** puis sur **OK**.
- Cliquez sur **Afficher l'accès effectif** pour visualiser les autorisations de l'utilisateur.



Il est possible d'effectuer ces opérations en ligne de commande avec icals.

Tolérance de panne d'un système de fichiers

Le RAID (*Redundant Arrays of Inexpensive Disk*) offre une tolérance de panne au niveau des données en effectuant une répartition de ces dernières sur plusieurs disques.

Cette solution permet de grouper plusieurs disques durs physiques afin d'effectuer la création d'une unité logique appelée volume. Dans le poste de travail, les différents disques n'apparaîtront plus sous la forme de plusieurs partitions mais bien d'un seul volume.

La technologie possède néanmoins un prérequis au niveau du nombre de disques. En effet, il est nécessaire d'avoir un minimum de deux disques. Plusieurs types de configuration existent afin d'offrir aux administrateurs la possibilité d'obtenir un gain de performances (temps d'accès disque), une plus grande capacité ou une meilleure sécurité.

1. RAID 0

Appelée RAID 0 ou *stripping*, cette technologie permet une nette amélioration des performances au niveau des accès disques. Les n disques présents dans le RAID travaillent en parallèle, ce qui permet l'amélioration des accès en lecture et écriture. Cette configuration possède néanmoins un inconvénient au niveau de la taille des disques. En effet la capacité du volume est égale à la taille du plus petit disque multipliée par le nombre de disques composant la grappe.

Exemple

*Si Mon RAID 0 est composé de deux disques, le premier a une capacité de 1 To, le deuxième de 2 To. La capacité du volume est donc de 2 To (taille du plus petit disque * nombre de disques = 1 To * 2 soit 2 To).*

Cela s'explique par le fait que le système d'agrégation par bandes (RAID 0) ne peut plus écrire de données dès lors que le plus petit disque est rempli. Il est fortement conseillé de prendre des disques de tailles égales.

Aucune tolérance n'est offerte par ce type de RAID : si un des disques casse, c'est l'ensemble des données qui sont perdues.

2. RAID 1

Comme pour le RAID 0, plusieurs disques sont utilisés, chacun possédant à l'instant t exactement les mêmes données. On parle ainsi de miroir ou *mirroring* en anglais. La capacité du volume est égale à celle des plus petits disques présents dans la grappe.

Comme pour le RAID 0, il est conseillé d'utiliser des disques de tailles identiques. Ce type de RAID offre une bonne protection des données. En cas de défaillance d'un des disques, une désactivation de ce dernier est opérée par le contrôleur RAID sans que l'utilisateur s'en aperçoive. Lors du remplacement, le contrôleur reconstitue le mirroir. Une fois la reconstitution terminée, la redondance et la haute disponibilité sont de nouveau assurées.

Lors de l'écriture des données sur le volume, l'opération est effectuée sur l'ensemble des disques de la grappe.

Si les deux disques cassent, les données sont perdues.

3. RAID 5

Le **RAID 5** est une solution qui associe le stripping (RAID 0) à un mécanisme de parité. Ainsi, les données ne sont jamais écrites de la même manière sur les différents disques, ceci afin d'avoir sur chacun les informations de parité et les données. Cette solution assure la reconstruction du RAID en combinant les bits de parité et les

données. Néanmoins, en cas de perte de plus d’un disque, les données ne pourront être retrouvées.

Cette solution de RAID apporte de bons accès en lecture mais le calcul de la parité implique des temps d’écriture beaucoup plus longs.

Différences entre un DAS et un SAN

Un DAS (*Direct-Attached Storage*) est un équipement de stockage branché directement sur le serveur. Son usage est généralement dédié principalement à ce serveur. Les disques peuvent être de deux types :

- disque interne au serveur,
- disque externe.

Les disques sont néanmoins distingués par le bus qu'ils utilisent. Ces derniers peuvent être de type SSD, SCSI, SATA. Les DAS utilisant des disques externes sont généralement de type périphérique USB.

Le DAS offre l'avantage d'être connecté directement au serveur, ce qui en simplifie l'administration. De plus, il s'agit généralement de périphériques Plug and Play, donc reconnus par le serveur sans que l'administrateur ait besoin d'effectuer des opérations. Néanmoins, cet espace de stockage ne peut pas servir de point central à tous les serveurs (les disques ne seront jamais considérés comme internes aux autres serveurs, ces derniers passeront par des partages réseau).

Enfin, cette technologie peut être plus lente que la technologie SAN.

Avant de parler de la technologie SAN, il peut être opportun de traiter le point du NAS (*Network Attached Storage*). Il se distingue du DAS par le fait qu'il n'est pas rattaché directement au serveur. En effet, l'équipement est connecté au réseau de l'entreprise et les serveurs ou postes de travail y accèdent par l'intermédiaire du réseau (une adresse IP doit être attribuée au NAS). Un firmware permet l'administration quotidienne de ce NAS. Il est développé et maintenu par le constructeur. Cette solution offre l'avantage d'être moins onéreuse qu'une solution SAN et offre un espace de stockage centralisé pour l'ensemble des serveurs et postes de travail.

Enfin, le SAN permet l'utilisation d'un espace de stockage connecté à un réseau à haute vitesse et haute performance. Ce système est très utilisé en entreprise surtout avec l'implémentation de systèmes de virtualisation. Il est implémenté avec des technologies de type fibre optique ou iSCSI.

1. Tables de partition MBR et GPT

Depuis 1980, les ordinateurs et serveurs utilisent des partitions de type MBR (*Master Boot Record*) pour leurs disques durs. Ce type de table de partition possède certaines caractéristiques. Un disque ne peut pas avoir plus de quatre partitions principales et chacune peut avoir une taille maximale de 2 To (Teraoctets), il est conseillé d'utiliser une table de partition de type GPT (*GUID Partition Table*) pour les disques de plus de 2 To.

Introduite avec Windows Server 2003 et Windows XP 64 bits, la table de partition au format GPT permet de s'affranchir des limites imposées par le MBR. Un maximum de 128 partitions par disque est supporté par le GPT. La taille d'une partition peut atteindre 8 Zettaoctets (10^{21}), néanmoins il est nécessaire que le BIOS prenne en charge le GPT pour pouvoir effectuer un boot sur ce type de partition.

Implémentation d'un espace de stockage

Depuis Windows Server 2012, l'implémentation d'un espace de stockage ainsi que ses fonctionnalités ont été améliorées.

1. La fonctionnalité Espace de stockage

Depuis Windows Server 2012, il est possible d'avoir la redondance et le stockage en commun pour des disques internes et externes. Ces derniers peuvent être de différentes tailles et utiliser différentes interfaces. Cet espace de stockage permet la création de disques durs virtuels hautement disponibles. Afin d'opérer l'opération de création, il est nécessaire d'avoir des volumes accessibles depuis le système d'exploitation regroupés dans un ou plusieurs pools de stockage. Par la suite, des disques virtuels (à ne pas confondre avec les fichiers VHD) peuvent être créés. Beaucoup plus flexibles, ils offrent des fonctionnalités identiques à celles d'un disque physique (résilience, etc.).

Avant de pouvoir ajouter un disque physique (SATA ou SAS) à un pool, il est nécessaire que ce disque respecte un minimum de prérequis.

Avant tout, il est nécessaire d'avoir un disque pour créer un pool de stockage. Deux disques sont eux nécessaires pour la mise en place d'un disque virtuel en miroir. Enfin, les disques qui peuvent utiliser une interface iSCSI, SAS, SATA, USB... **doivent être non partitionnés**.

2. Options de configuration des disques virtuels

Depuis les pools de stockage, il est possible de créer des disques virtuels. Si plusieurs disques composent ce pool, alors il est possible de créer des disques virtuels redondants. Cette opération s'effectue à l'aide de la console **Gestionnaire de serveur** ou par l'intermédiaire de PowerShell. Avant toute chose, il convient de prendre en compte le nombre de disques qui vont permettre la mise en place d'une redondance ou un gain en performance.

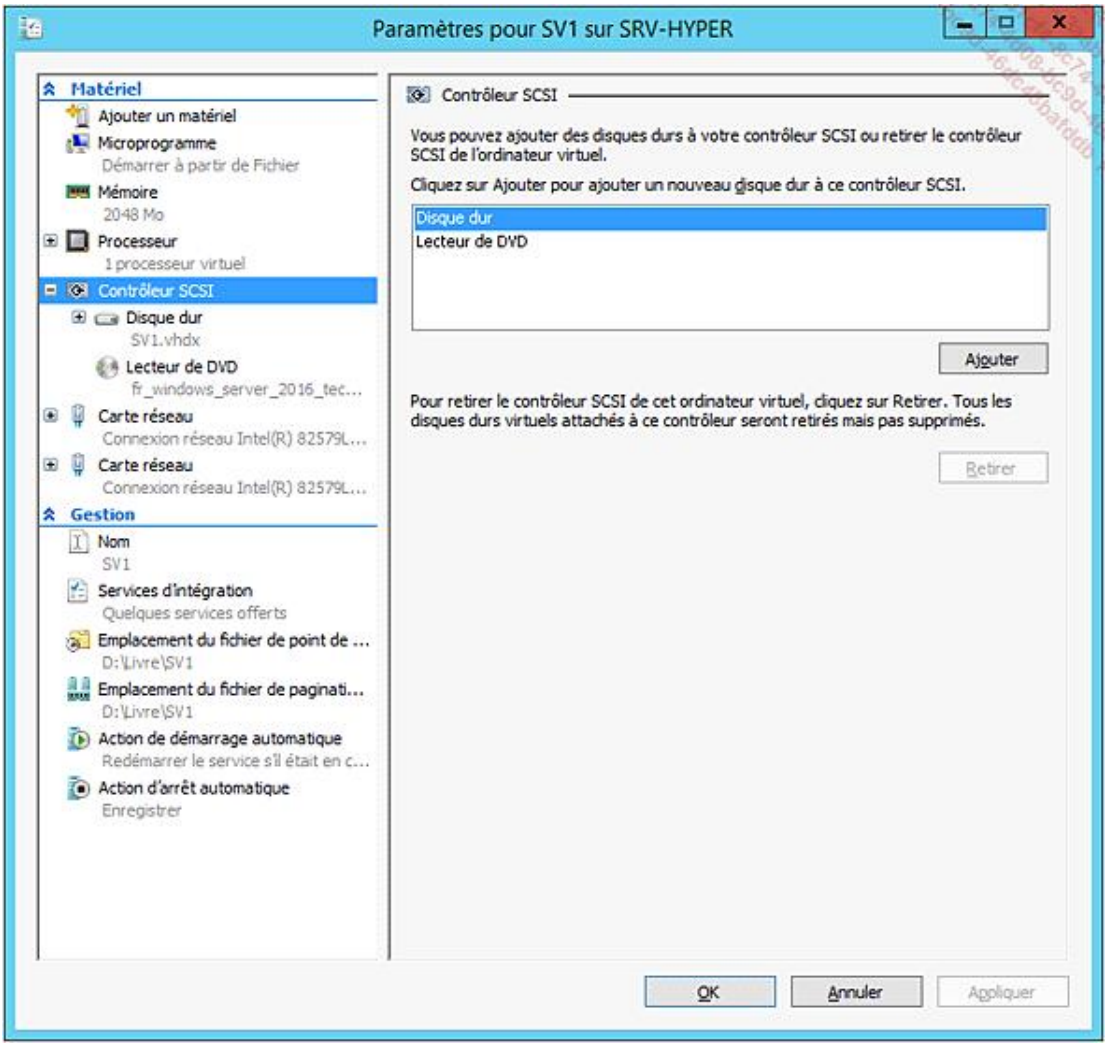
Trois options peuvent être mises en place :

- Un **espace simple** qui permet d'obtenir de meilleures performances grâce au RAID 0. Aucune redondance n'est mise en place, les données sont perdues en cas de crash.
- Le **miroir** permet la redondance des données en assurant la duplication des données sur plusieurs disques. Cette solution permet un bon débit avec une latence d'accès assez faible. De plus, une tolérance de panne est assurée.
- Enfin, la **parité** est similaire au RAID 5. Les données ainsi que le bit de parité sont répartis sur plusieurs disques. Cette dernière solution nécessite trois disques physiques. Comme pour le miroir, une tolérance de panne est présente avec cette solution.

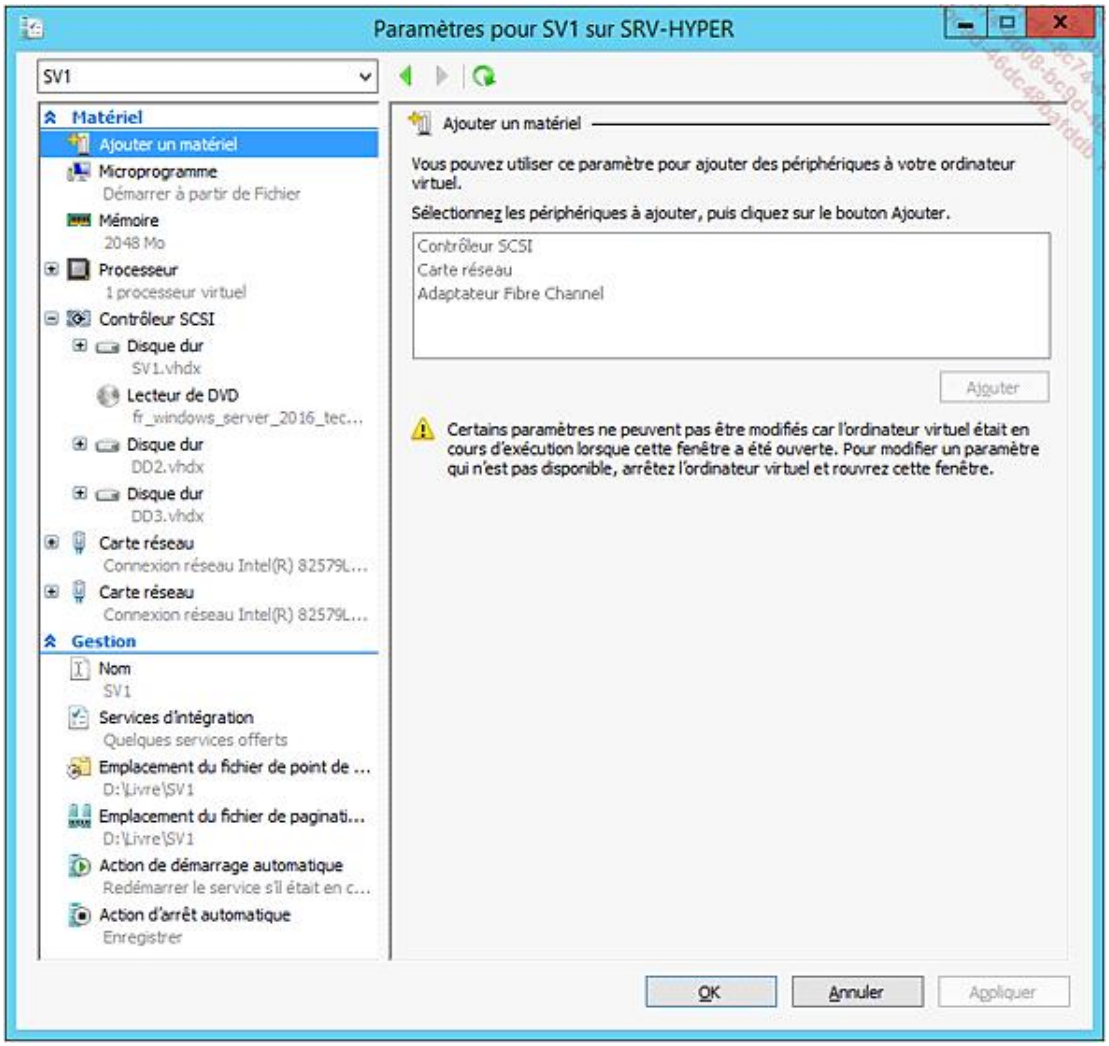
Pour gérer le pool de stockage et les différents disques virtuels, il est possible d'utiliser les instructions PowerShell ci-dessous :

Get-StoragePool	Liste les pools de stockage.
Get-VirtualDisk	Liste les disques virtuels.
Repair-VirtualDisk	Répare les disques virtuels.
Reset-PhysicalDisk	Supprime un disque physique d'un pool de stockage.
Get-VirtualDisk | Get-PhysicalDisk	Répertorie les disques physiques qui sont utilisés pour un disque virtuel.

Depuis la console Hyper-V, accédez aux propriétés du serveur SV1.

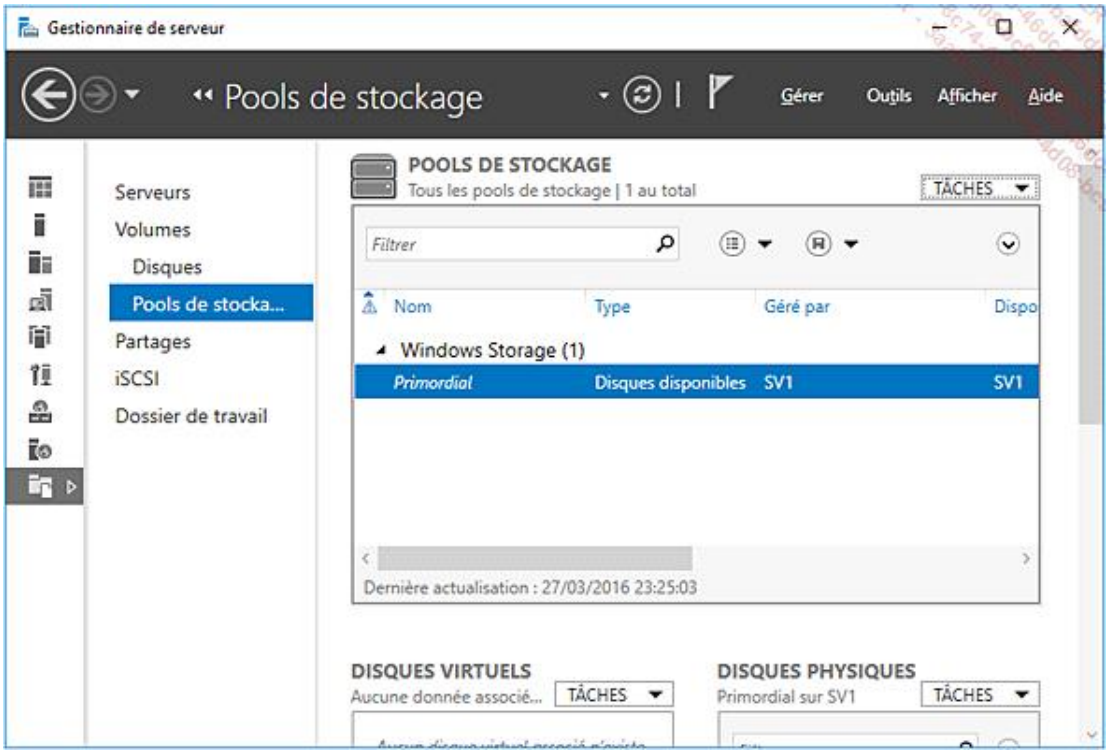


- Ajoutez un nouveau disque dur de 20 Go à la machine virtuelle.
- Recommencez l'opération afin de créer un deuxième disque virtuel.

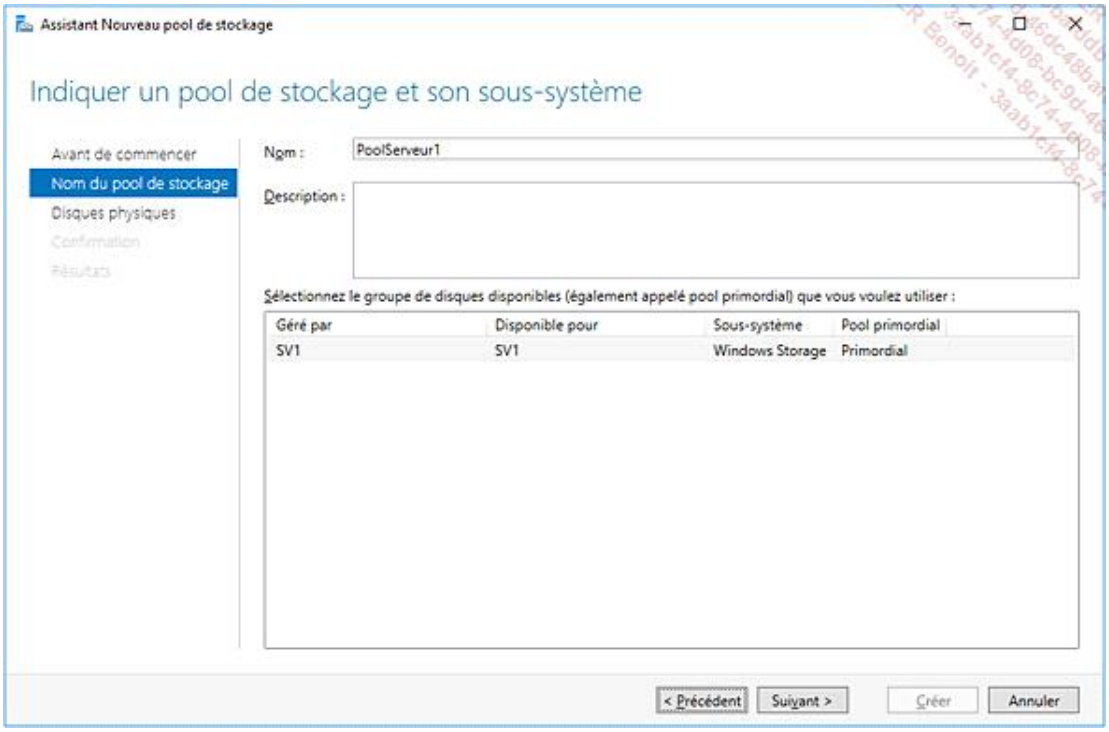


Il n'est pas nécessaire de partitionner les disques ou de les initialiser.

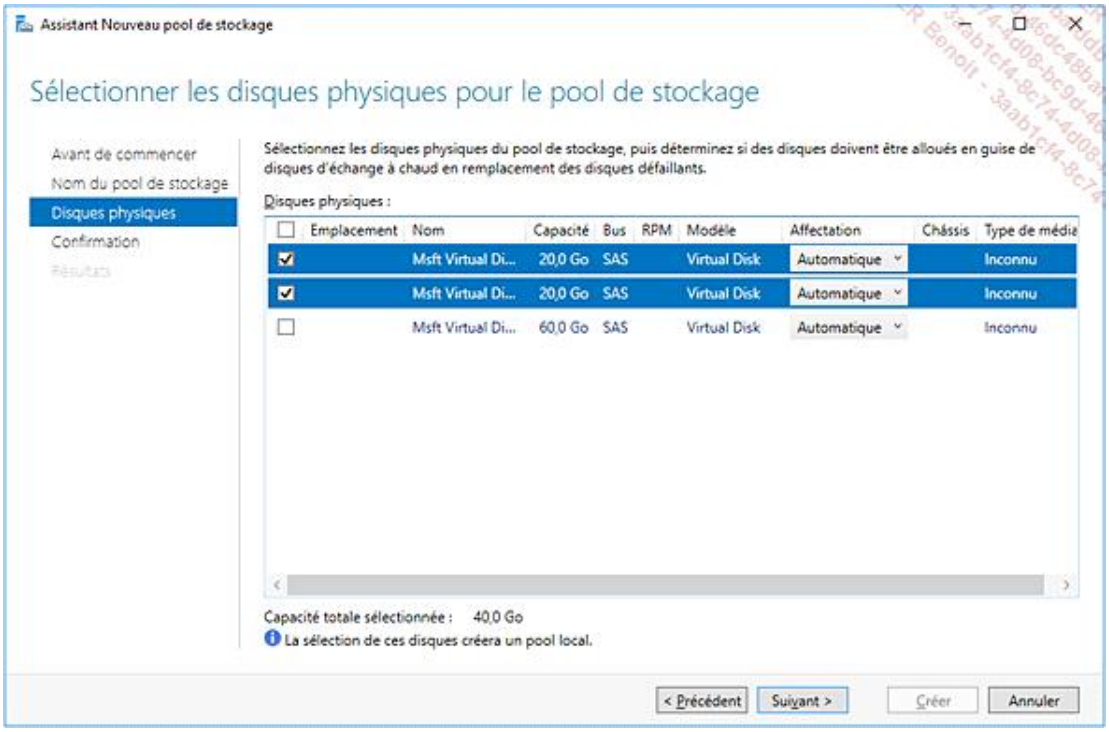
- Lancez la console **Gestionnaire de serveur** puis cliquez sur **Services de fichiers et de stockage**.
- Sélectionnez l'onglet **Pools et stockage** puis à l'aide du bouton **TÂCHES** cliquez sur **Nouveau pool de stockage**.



- Un assistant se lance, dans la fenêtre **Avant de commencer** cliquez sur **Suivant**.
- Saisissez **PoolServeur1** dans le champ **Nom** puis cliquez sur **Suivant**.

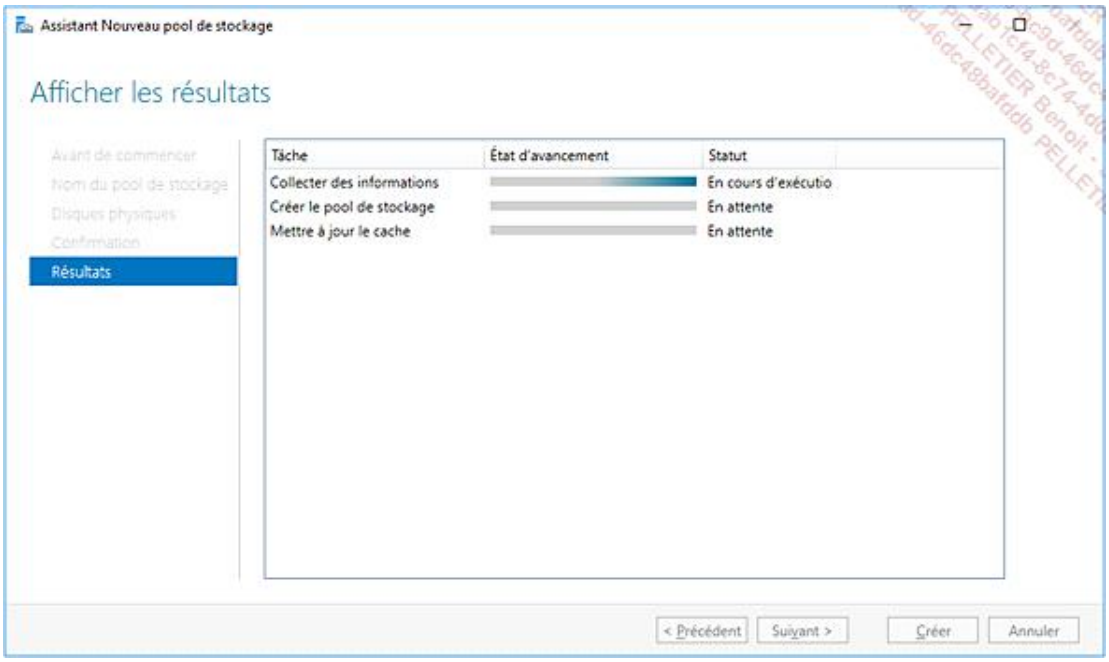


- Dans la fenêtre **Sélectionner les disques physiques pour le pool de stockage**, cochez les deux disques présents.

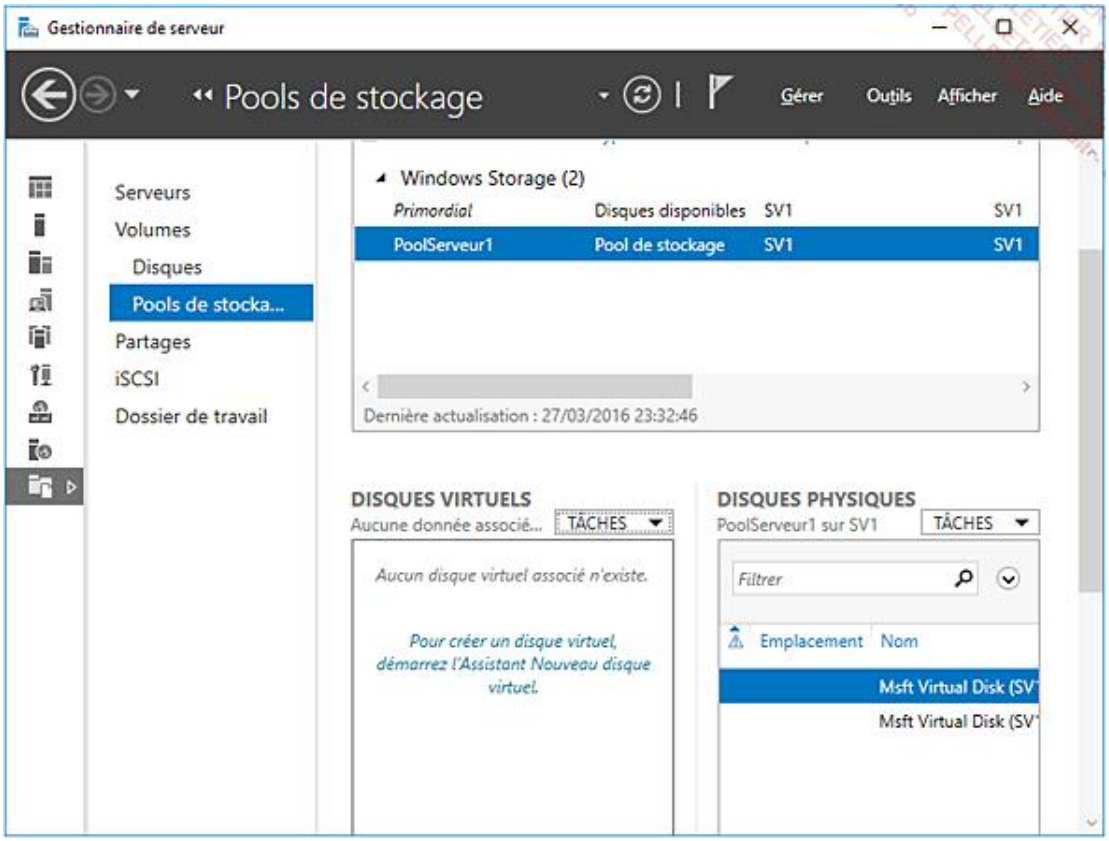


- Cliquez sur **Suivant** puis sur **Créer**.

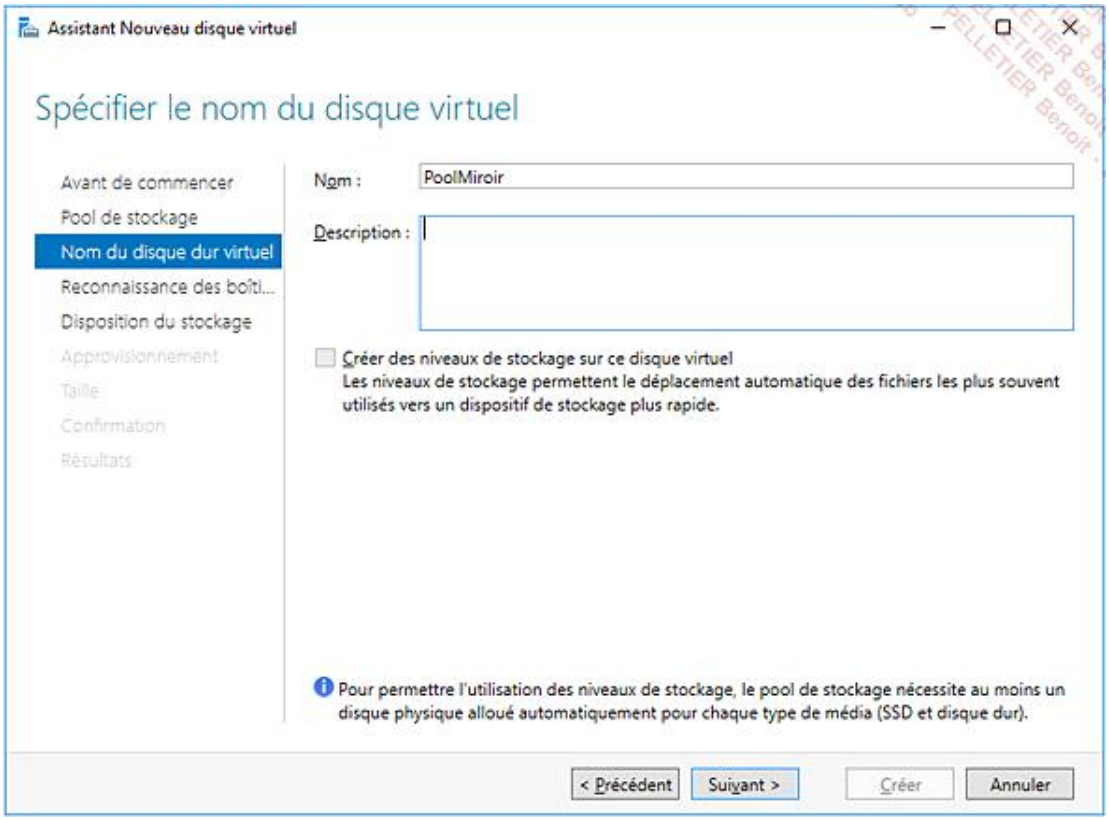
La création du pool de stockage est en cours.



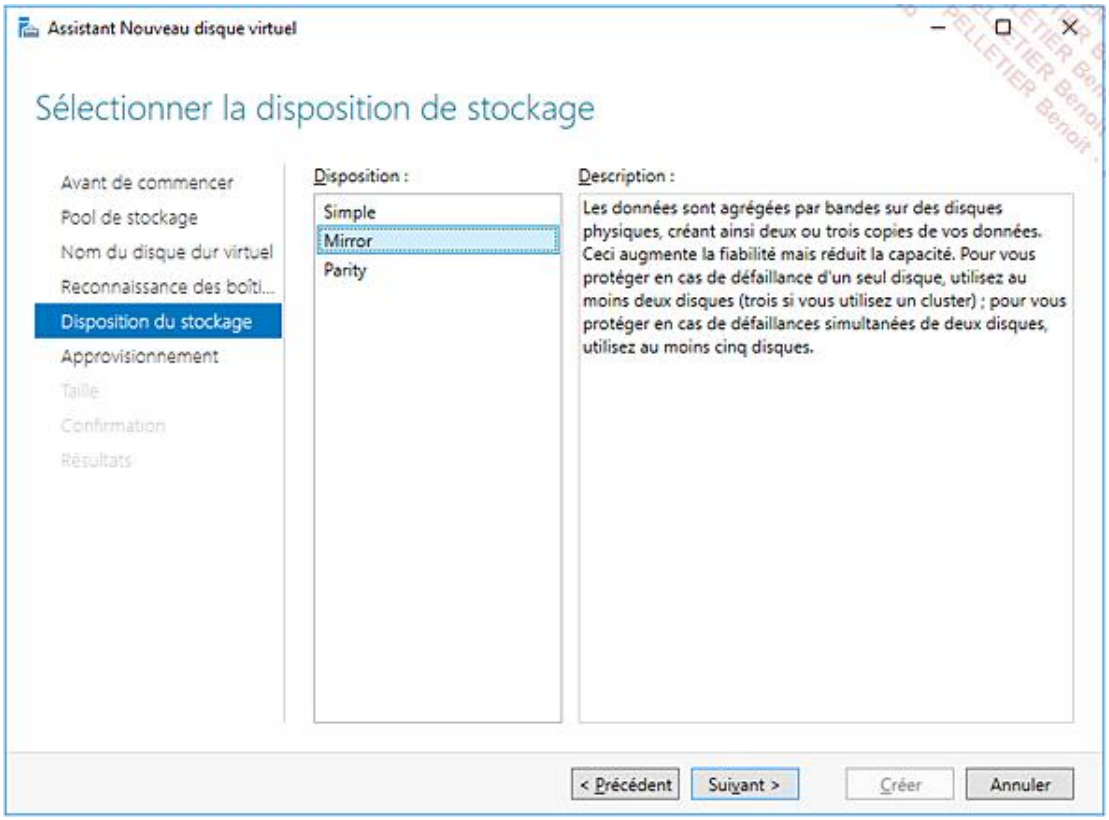
- Cliquez sur **Fermer** à la fin de la création.
- Cliquez sur le bouton **TÂCHES** dans **Disques virtuels** et cliquez sur **Nouveau disque virtuel**.



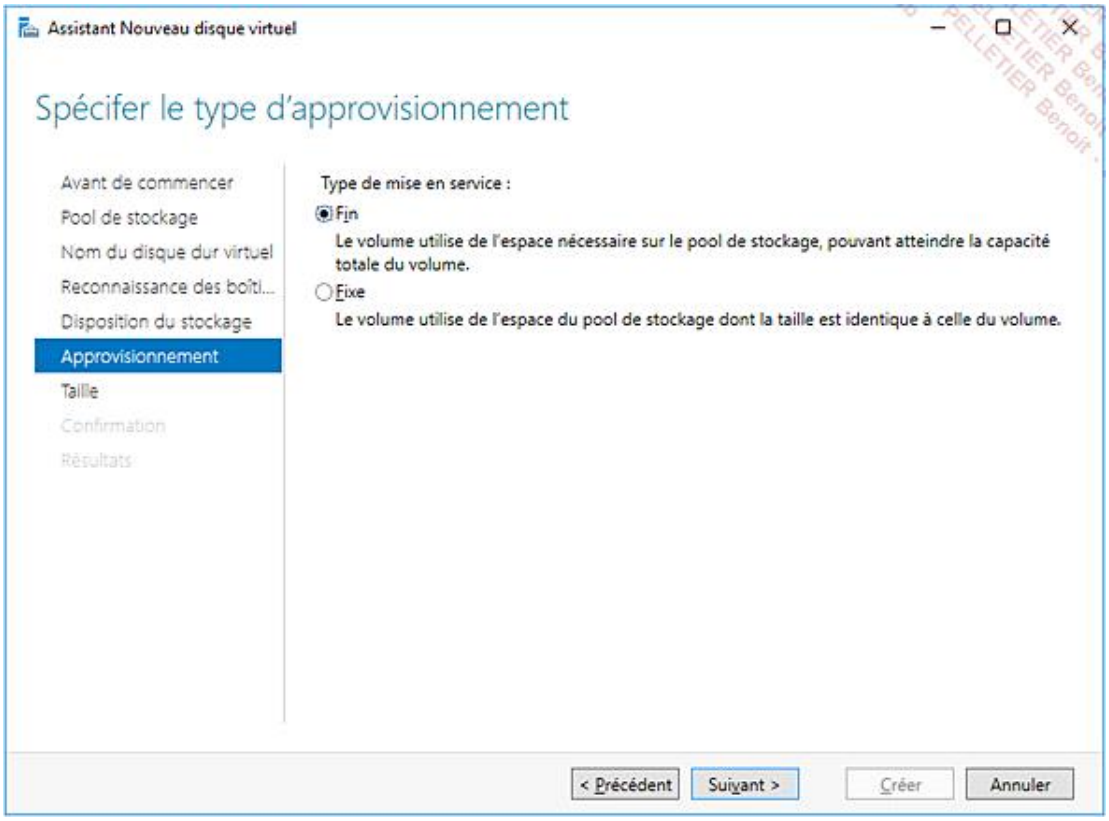
- Cliquez sur **Suivant** dans les fenêtres **Avant de commencer** et **Sélectionner le pool de stockage**.
- Saisissez **PoolMiroir** dans le champ **Nom** puis cliquez sur **Suivant**.



- Sélectionnez **Mirror** dans la liste **Sélectionner la disposition de stockage**.



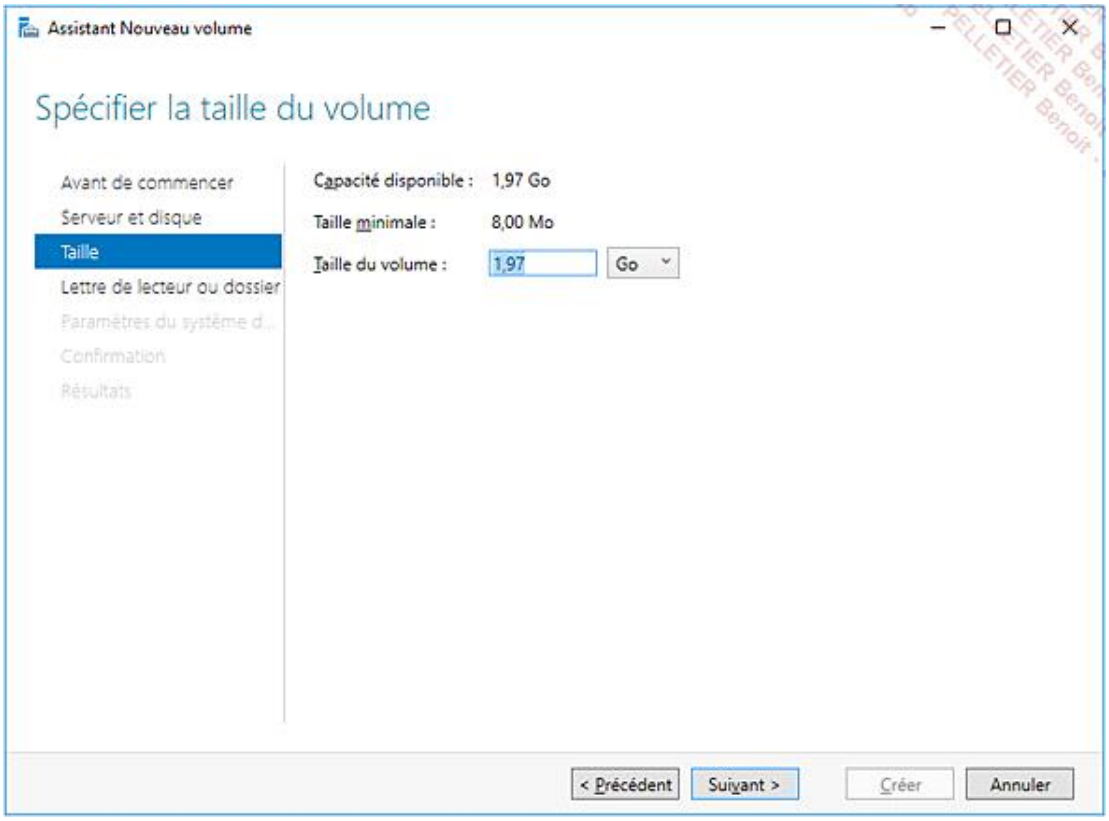
- Choisissez **Fin** dans la fenêtre **Spécifier le type d'approvisionnement**.



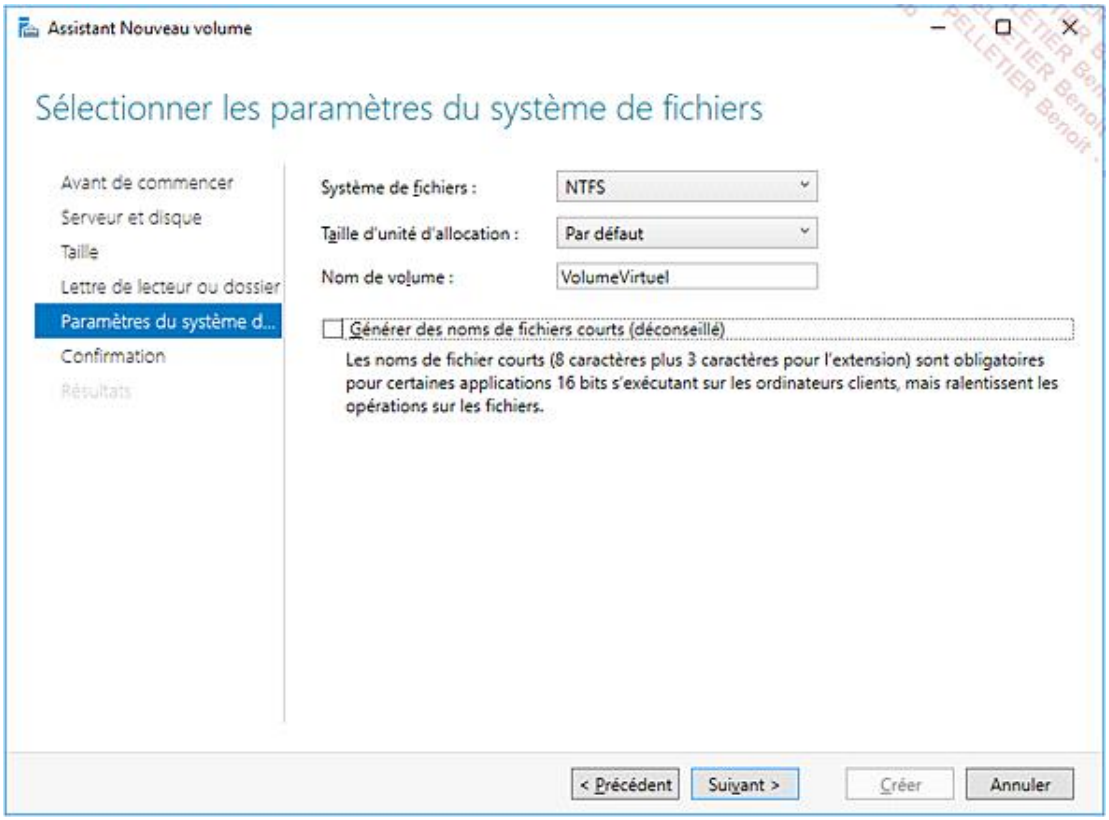
- Dans le champ **Spécifier la taille du disque dur virtuel**, spécifiez **2** afin de créer un disque virtuel de 2 Go.
- Cliquez sur **Suivant** puis sur **Créer**.
- À la fin de la création, cliquez sur **Fermer**.

L’assistant de création d’un nouveau volume se lance.

- Cliquez sur **Suivant** dans les pages **Avant de commencer** et **Sélectionner le serveur et le disque**.
- Laissez la taille du volume par défaut et validez le choix à l’aide du bouton **Suivant**.

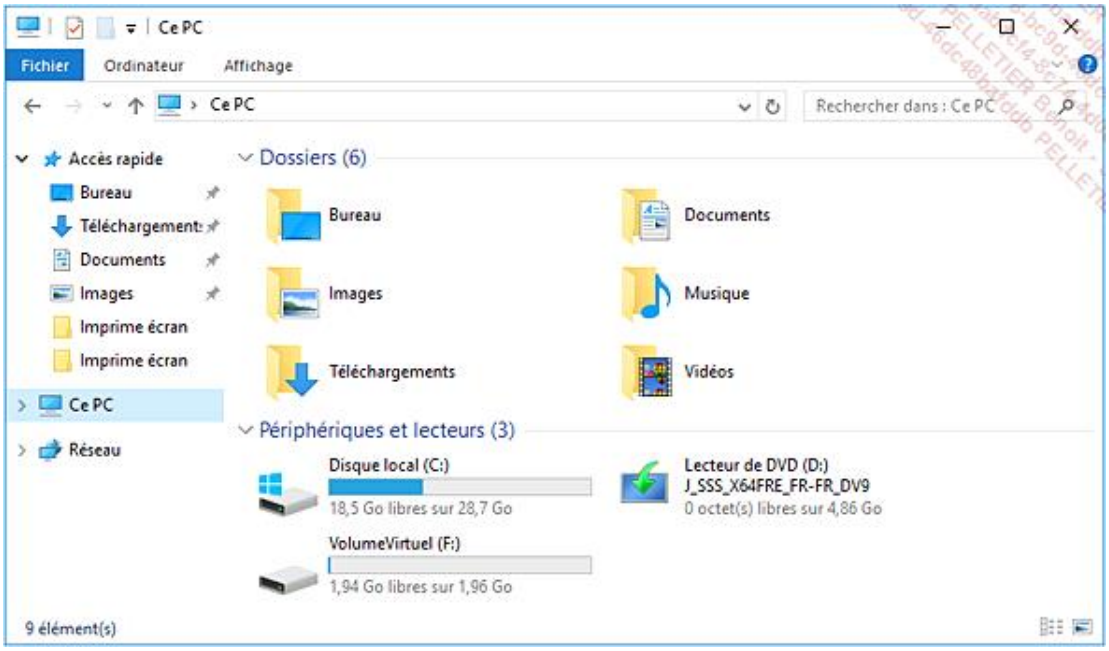


- Affectez la lettre **F** au nouveau volume.
- Saisissez **VolumeVirtuel** dans le champ **Nom du volume** puis cliquez sur **Suivant**.

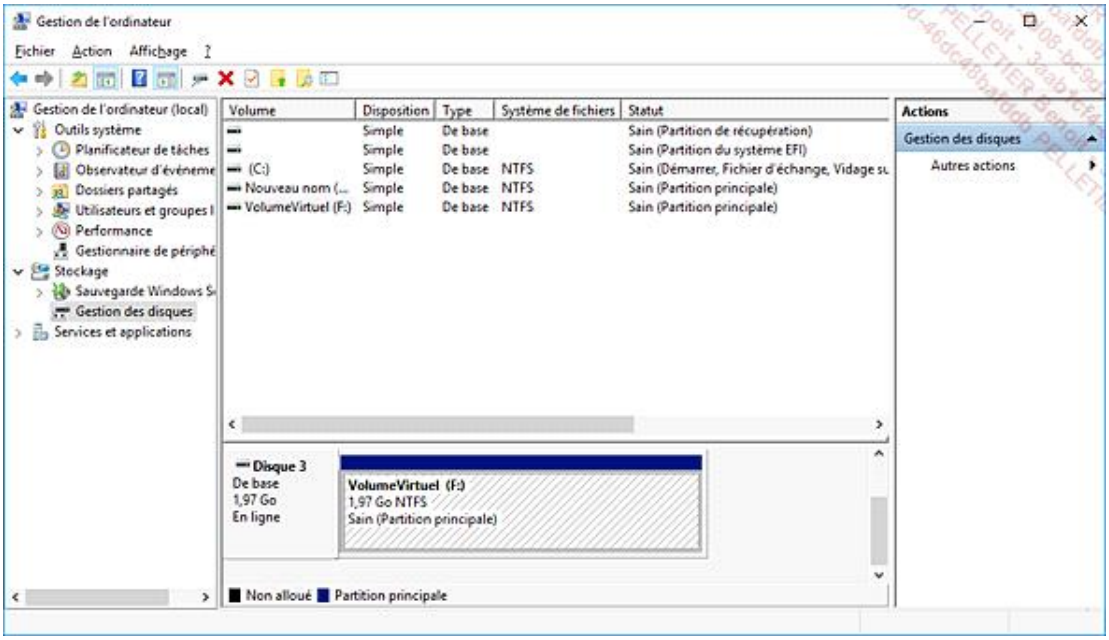


Cliquez sur **Créer** afin de valider la création du volume.

Le volume apparaît maintenant dans l'Explorateur.



Les disques physiques de la machine n'apparaissent plus dans la console **Gestion des disques**, seule la partition créée précédemment est présente. La gestion des volumes s'effectue désormais depuis le pool de stockage (console **Gestionnaire de serveur**).

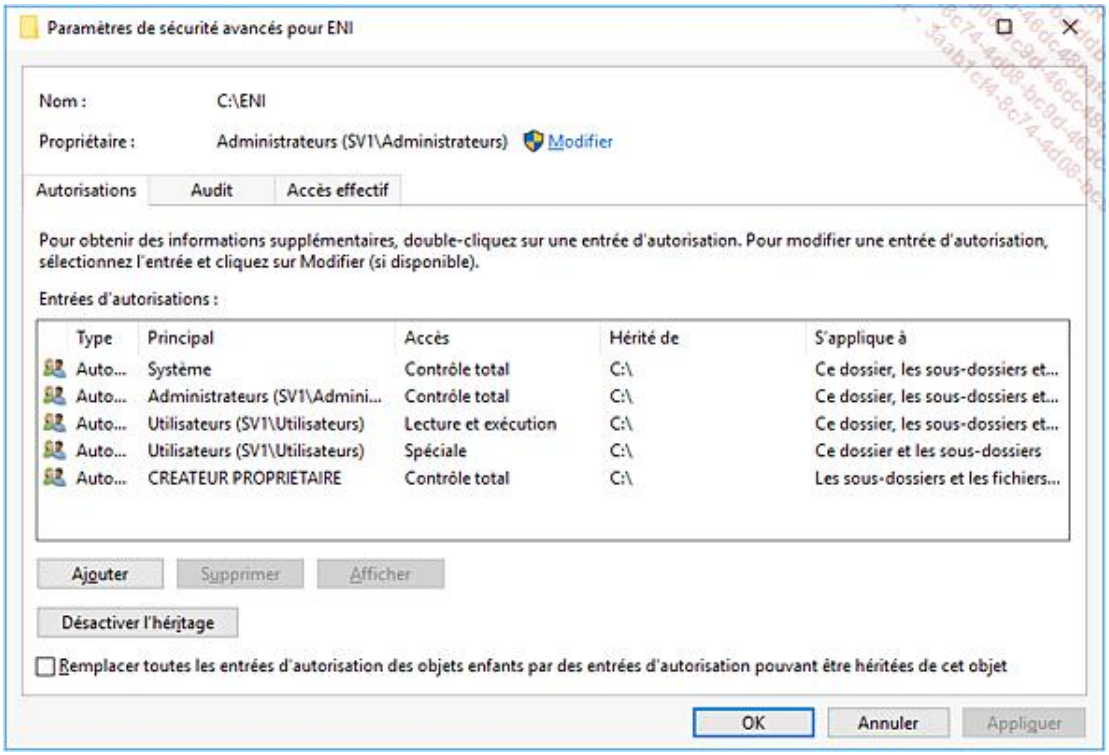


3. Définition d'un répertoire partagé

Les répertoires partagés permettent un accès direct à une ressource stockée sur un serveur. Lors du partage d'un dossier, celui-ci devient disponible pour les utilisateurs raccordés au réseau. Afin de limiter les accès et donc assurer la confidentialité, il est nécessaire de positionner des autorisations de sécurité. Ces dernières peuvent être mises sur un répertoire ou un fichier.

L'accès s'effectue à l'aide d'un chemin UNC (*Universal Naming Convention*). Il contient le nom du serveur qui héberge la ressource ainsi que le nom de partage de la ressource (exemple : \\SRV1\Datas). Les partages administratifs sont utilisés depuis de nombreuses années, ils permettent de rendre un partage disponible sur le réseau sans qu'un utilisateur puisse le voir. Pour y accéder, il est nécessaire de saisir le chemin UNC suivie d'un $. Des partages comme c$, admin$ sont présents lors de l'installation d'un système d'exploitation client ou serveur. Pour cacher un partage et le transformer en partage administratif, il convient de rajouter un $ à la fin du partage (\\SRV1\Data$).

Par défaut, le système NTFS utilise l'héritage pour qu'un dossier transmette à son enfant (dossier placé en dessous) les permissions d'accès. Lors de l'ajout d'un fichier ou d'un dossier, ces derniers récupèrent automatiquement les permissions de sécurité qui sont appliquées à son parent. Dans certains cas, il peut arriver que les autorisations héritées viennent contredire des autorisations explicites. On parle alors de conflit. Dans ce cas les autorisations explicitement déclarées par l'administrateur ont la priorité sur les autorisations héritées d'un dossier parent. Ces dernières peuvent être désactivées en bloquant l'héritage sur un dossier ou un fichier. Cette opération est effectuée dans les options avancées d'un fichier ou d'un répertoire (clic droit sur le répertoire - **Propriétés** - onglet **Sécurité** - **Avancé**).

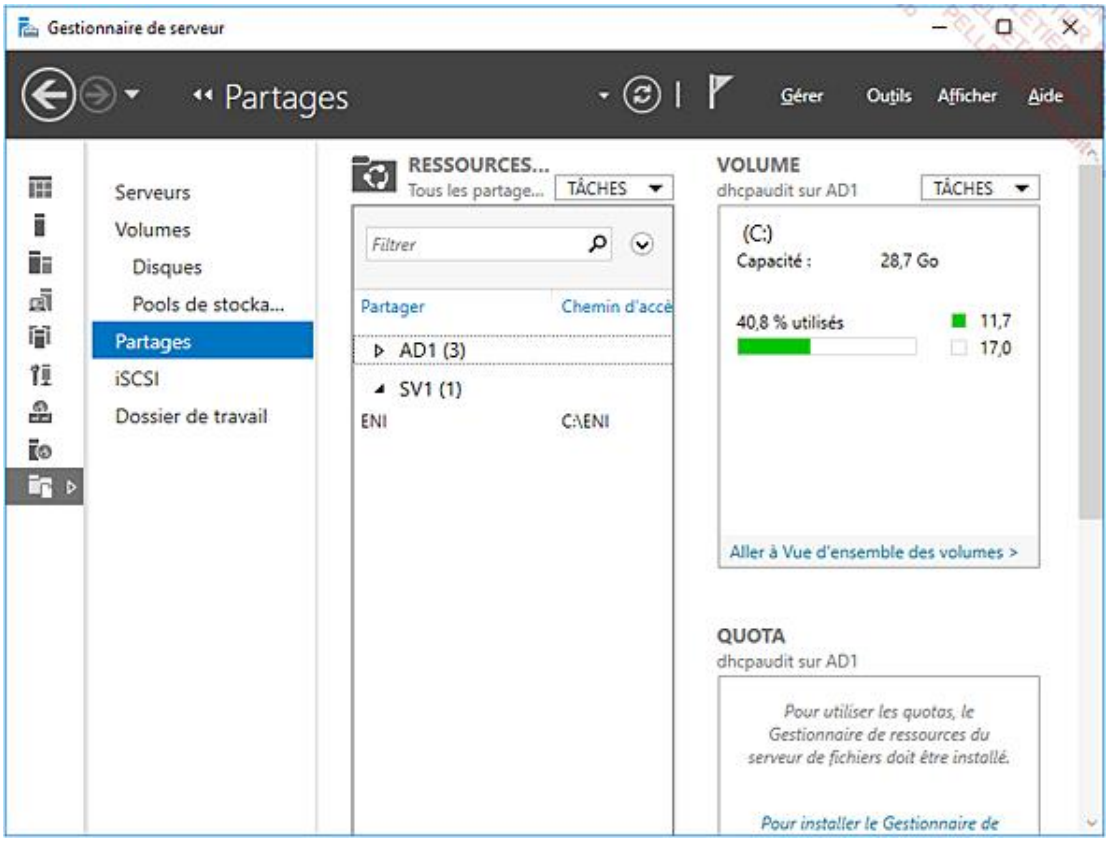


Après avoir bloqué l'héritage, les modifications des autorisations du parent ne s'appliquent plus sur l'enfant. Il est parfois nécessaire de réinitialiser les autorisations placées sur chaque nœud de l'arborescence en assignant les autorisations du parent à l'enfant. Pour cela, l'option **Remplacer toutes les entrées d'autorisation des objets enfants par des entrées d'autorisation pouvant être héritées de cet objet** doit être utilisée. L'opération consiste à propager à tout sous-dossier les autorisations définis sur le dossier parent.

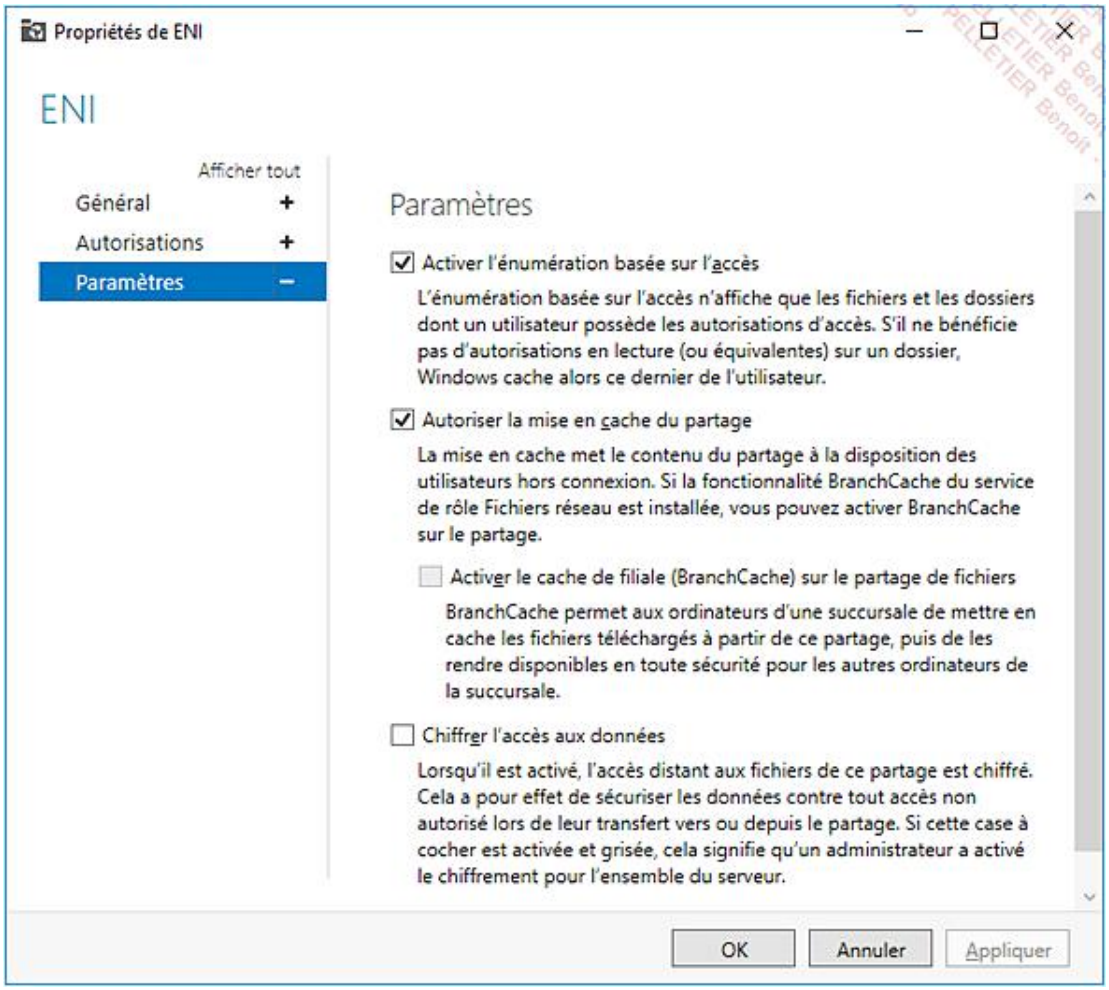
4. Affichage des partages en fonction des droits d'accès

L'énumération basée sur l'accès (ABE - *Access-Based Enumeration*) consiste à afficher uniquement les dossiers contenus dans un partage auquel l'utilisateur a accès. Ainsi, les accès aux partages ou les accès aux fichiers s'en trouvent simplifiés. L'activation de cette fonction s'effectue depuis la console **Gestionnaire de serveur**.

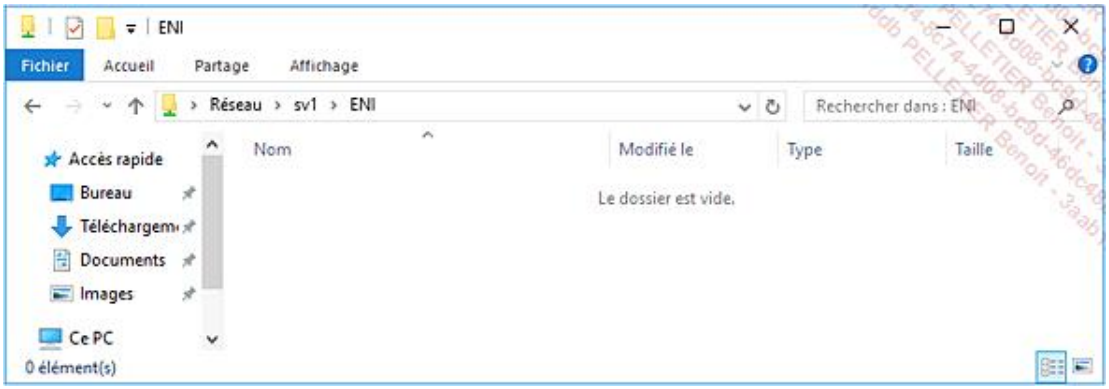
Une fois la console lancée, il est nécessaire d'accéder aux nœuds **Services de fichiers et de stockage** puis **Partages**.



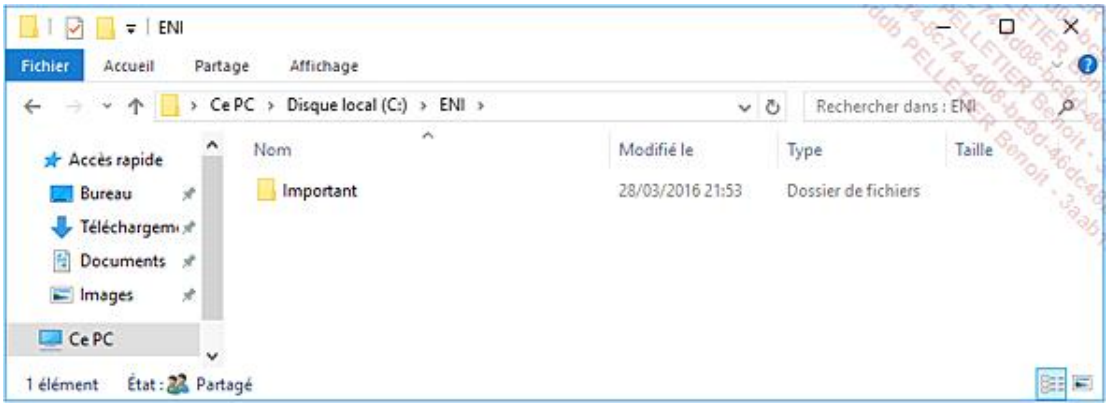
En accédant aux **Propriétés** d'un partage puis en se rendant dans l'onglet **Paramètres**, il est possible d'activer l'option.



Si le droit **Refuser** est appliqué à un dossier présent dans le partage (et que ABE a été activé), le dossier ne sera pas visible par l'utilisateur.



Le dossier est pourtant bien présent.



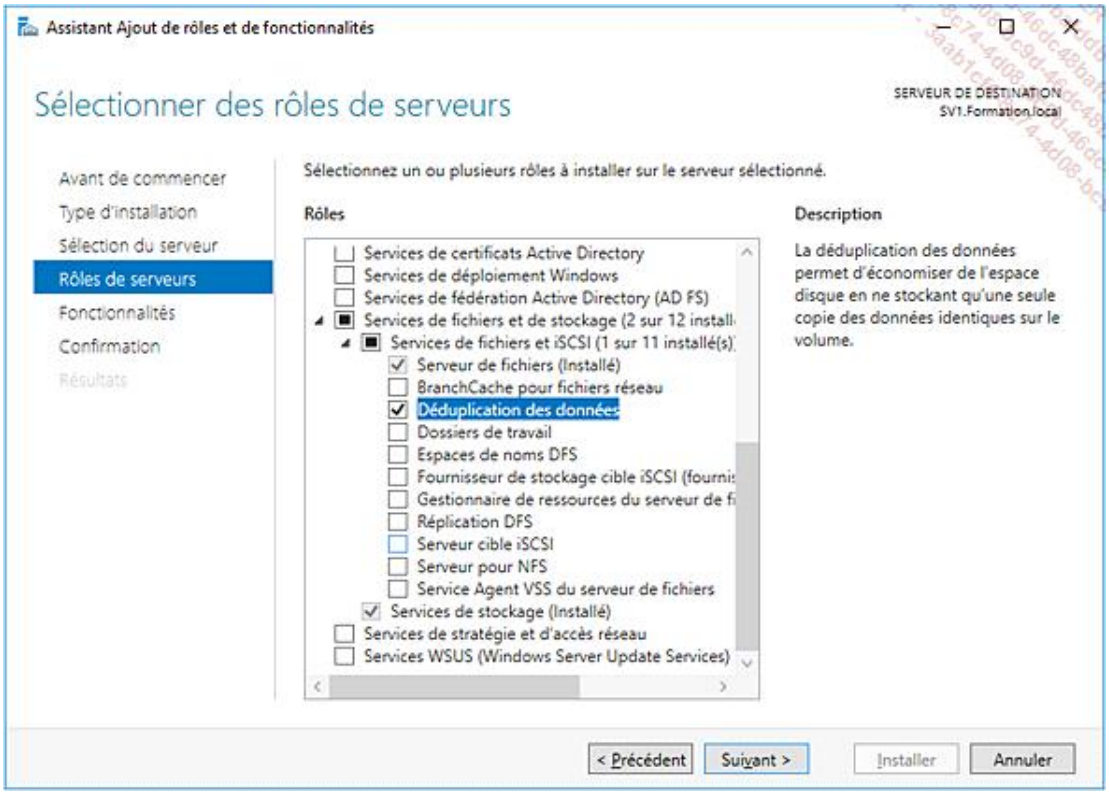
Cette fonctionnalité permet de n'afficher que les dossiers pour lesquels l'utilisateur possède un droit d'accès.

5. La déduplication de données

Depuis Windows Server 2012, il est possible d'activer la déduplication de données. Le but est d'optimiser l'espace disque. Ainsi, un bloc identique à plusieurs fichiers n'est stocké qu'une seule fois. **Néanmoins, cette fonctionnalité ne peut pas être utilisée sur une partition système**.

La déduplication de données offre plusieurs avantages, dont celui d'optimiser l'espace disque lorsque celui-ci est réduit.

La première étape de l'implémentation est l'installation de la fonctionnalité. L'opération peut s'effectuer par l'intermédiaire de la console **Gestionnaire de serveur**.



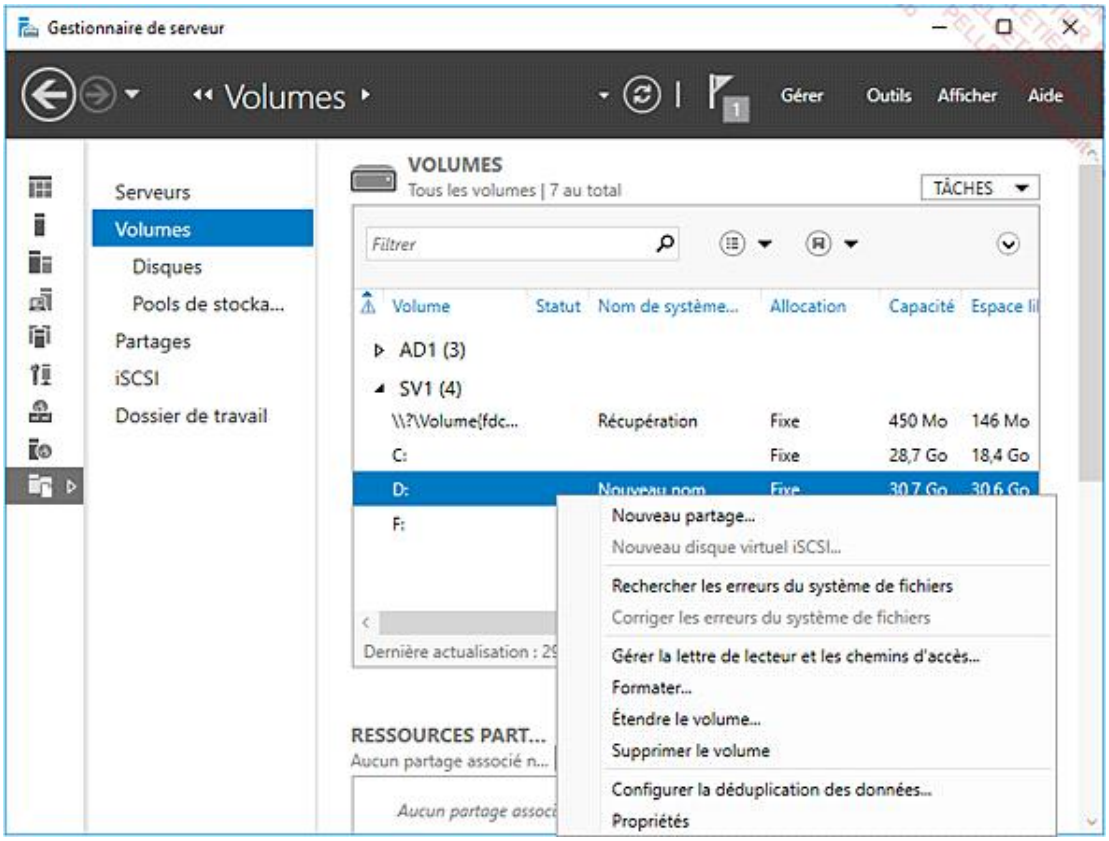
Il est également possible de procéder à l'installation par le biais d'un applet de commande PowerShell.

Par la suite, il est nécessaire d'activer la fonctionnalité sur le volume souhaité. Cette étape peut être réalisée avec l'interface graphique.

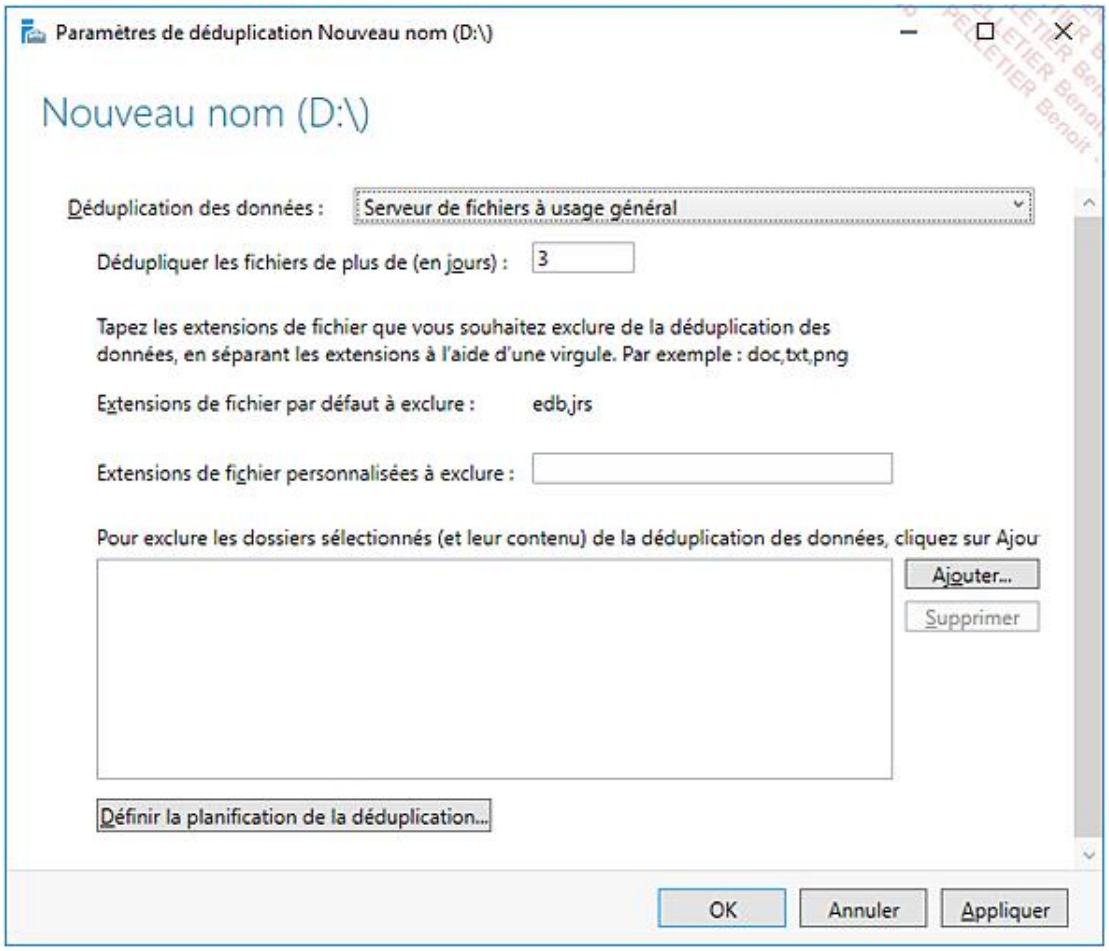
- Dans la console **Gestionnaire de serveur**, sélectionnez **Services de fichiers et de stockage**.
- Sélectionnez **Volumes** puis effectuez un clic droit sur le volume souhaité.

Tous sauf le volume système.

- Cliquez sur **Configurer la déduplication des données**.



- Dans la liste déroulante **Déduplication des données**, sélectionnez **Serveur de fichiers à usage général**.



Des extensions de fichier ou des dossiers peuvent être exclus.

Comme pour l'installation, l'étape d'activation peut s'effectuer en ligne de commande.

```
Enable-DedupVolume D:
```

Cliquez sur **OK** afin d'activer la fonctionnalité.

Les clichés instantanés

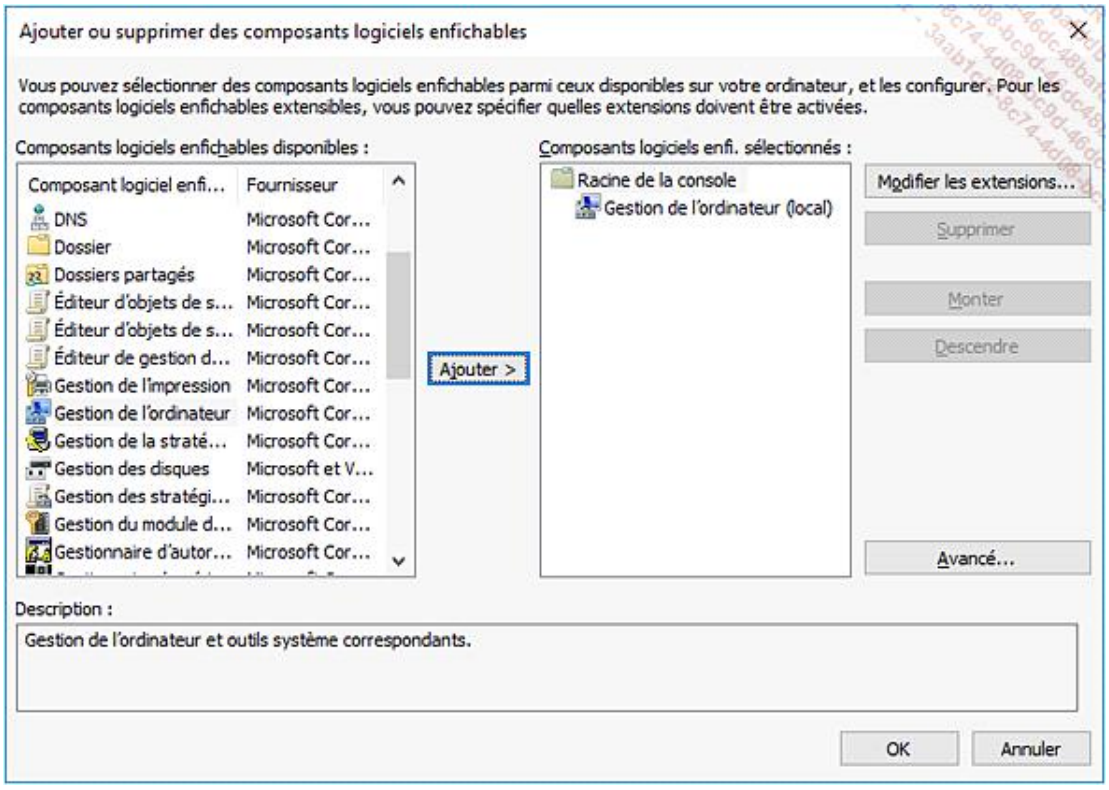
Intégrée depuis quelques années aux systèmes d'exploitation, cette fonctionnalité permet de conserver automatiquement les versions précédentes des fichiers hébergés sur un partage réseau. La partie cliente est intégrée aux systèmes d'exploitation depuis Windows XP. L'utilisateur peut donc restaurer un fichier supprimé accidentellement ou modifié par erreur sans l'aide de l'administrateur.

Un disque formaté avec un système de fichiers NTFS est nécessaire pour bénéficier de cette fonctionnalité. Une fois celle-ci activée, une empreinte des fichiers est effectuée à une heure fixée (à 7h et à 12h par défaut) ou lancée manuellement par un administrateur.

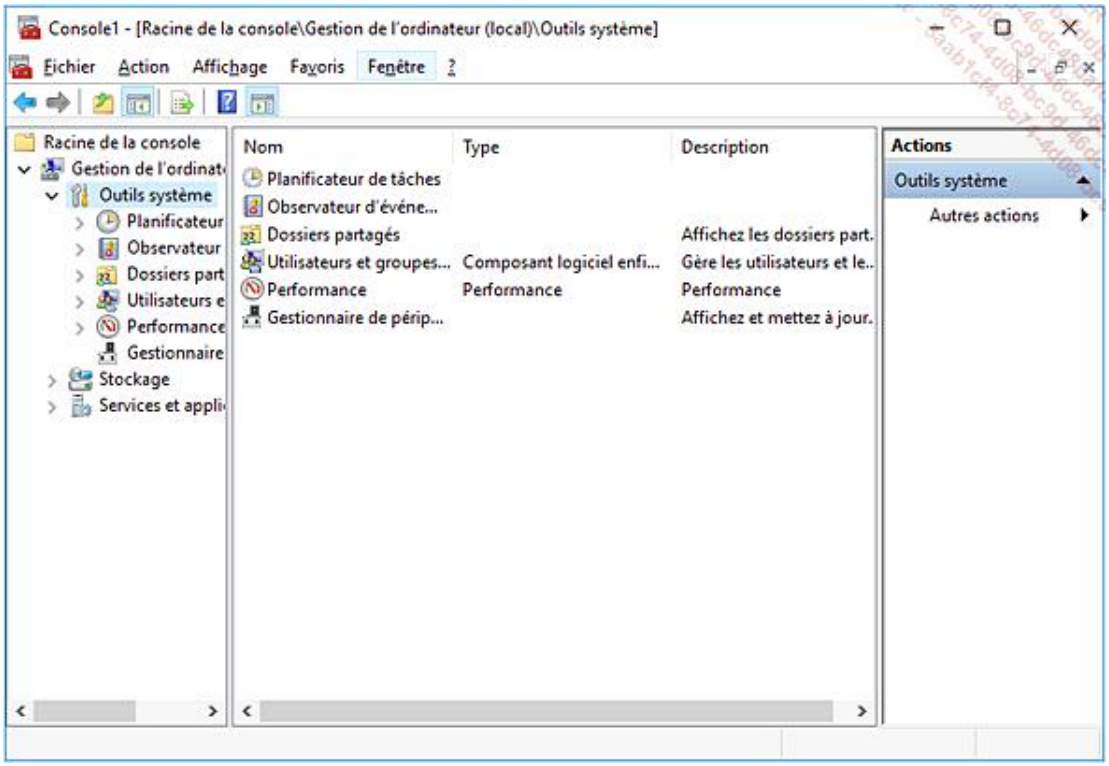
L'activation peut être faite sur toutes les partitions ou volumes NTFS.

1. Mise en œuvre des clichés instantanés sur le serveur

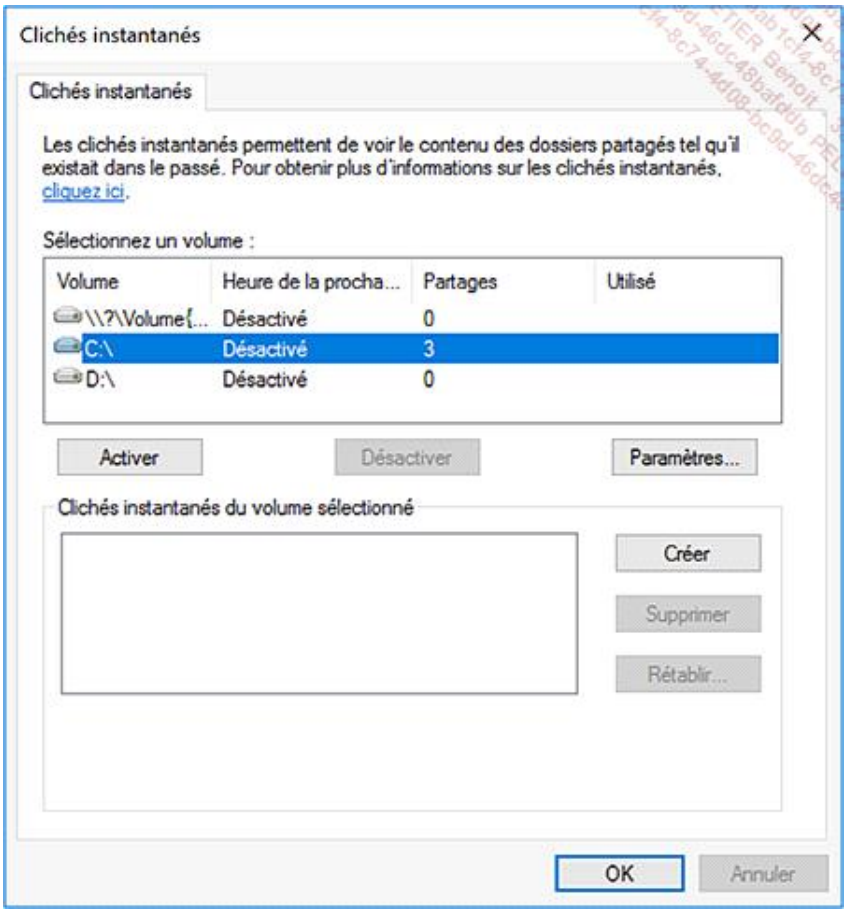
- Sur le serveur SV1, effectuez un clic droit sur le bouton **Démarrer**.
- Cliquez sur **Exécuter** et, dans le champ, saisissez **mmc** puis cliquez sur **OK**.
- Cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
- Cliquez sur **Gestion de l'ordinateur** puis sur **Ajouter**.



- Cliquez sur **OK** pour valider votre choix et accéder à la console.
- Déroulez les nœuds **Gestion de l'ordinateur** et **Outils système**.



- Effectuez un clic droit sur **Dossiers partagés** puis sélectionnez **Configurer les clichés instantanés** dans le menu **Toutes les tâches**.
- Sélectionnez le volume C:.

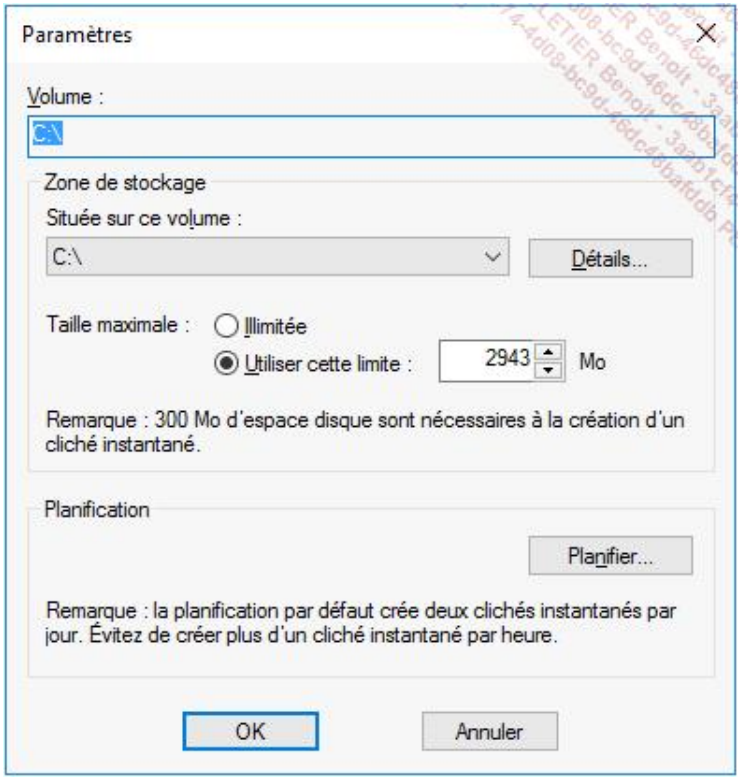


Il est possible d'activer les clichés instantanés en sélectionnant la partition souhaitée puis en cliquant sur **Activer**. Il

est nécessaire par la suite de cliquer sur le bouton **Créer** pour effectuer une création manuelle ou d'attendre pour la création d'un cliché de façon automatique (par défaut, des clichés sont créés à 7h et à 12h).

- Cliquez sur **Paramètres** afin de pouvoir configurer la planification et la taille des clichés.

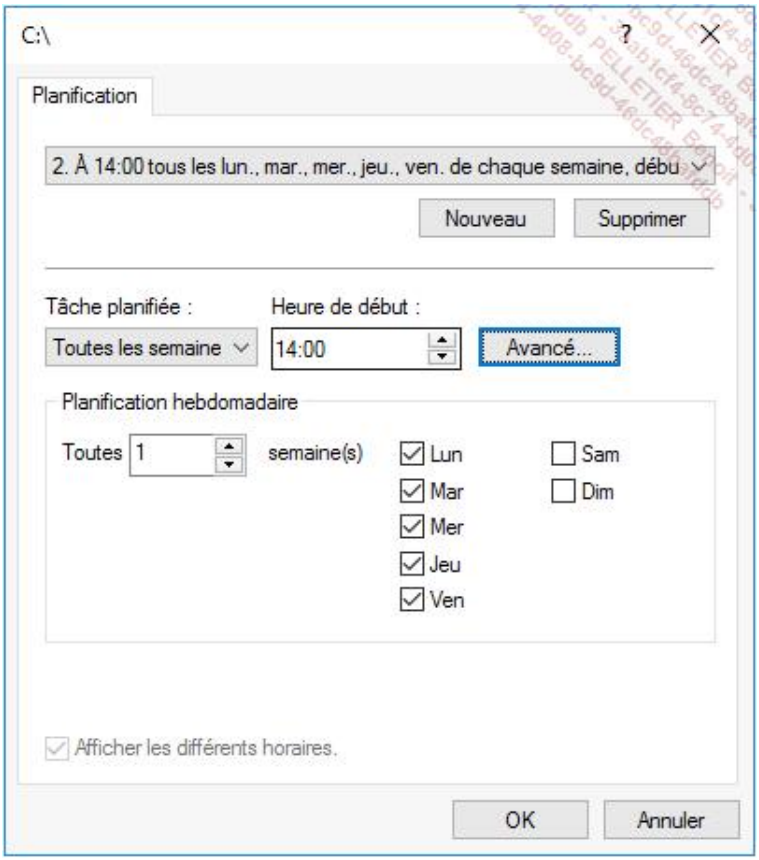
Il est ainsi possible de voir sur quel volume sont situés les clichés instantanés. La fenêtre offre également la possibilité de configurer la taille maximale et la planification.



- Cliquez sur **Planifier** afin de modifier la planification.

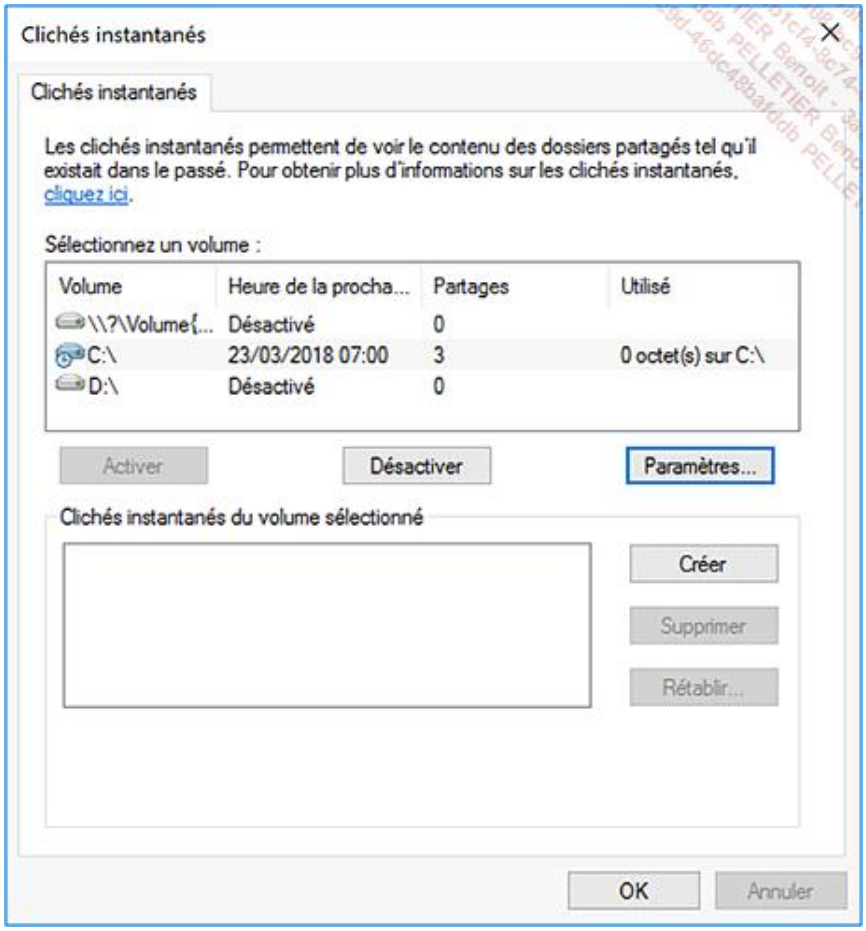
La liste déroulante permet de sélectionner l'exécution souhaitée, ceci dans le but de la modifier ou de la supprimer définitivement.

- Sélectionnez dans la liste déroulante le choix **2. A 12:00**.
- Modifiez l'heure de début afin d'avoir une exécution à 14h puis cliquez sur **OK**.



Il est possible de configurer de nouvelles exécutions à l'aide du bouton **Nouveau**. Une date de fin peut être configurée à l'aide du bouton **Avancé**.

Cliquez deux fois sur **OK**. L'heure de la prochaine exécution apparaît maintenant dans la console.



Les clichés instantanés fonctionnent sur des partages réseau. Nous allons donc créer sur le serveur un nouveau partage.

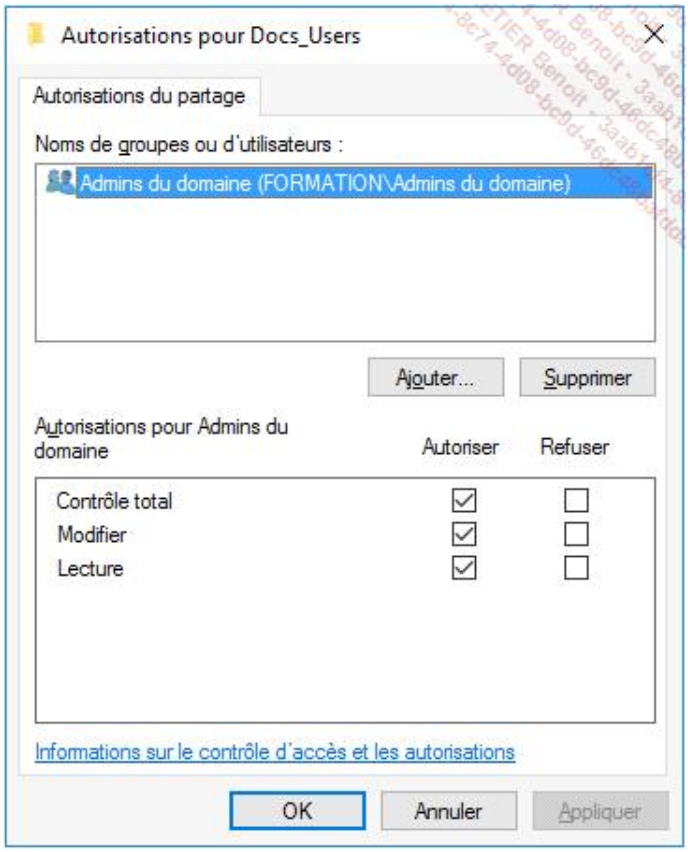
- Cliquez sur la partition **C:** puis créez le dossier **Docs_Users**.

Le nom n'a pas d'importance, votre répertoire peut utiliser un autre nom.

- Effectuez un clic droit sur le dossier puis sélectionnez **Propriétés**.
- Cliquez sur l'onglet **Partage** puis sur **Partage avancé**.
- Cochez la case **Partager ce répertoire**, puis cliquez sur **Autorisations**.

Ces dernières vont être configurées afin que seul l'administrateur possède un accès **Contrôle total**.

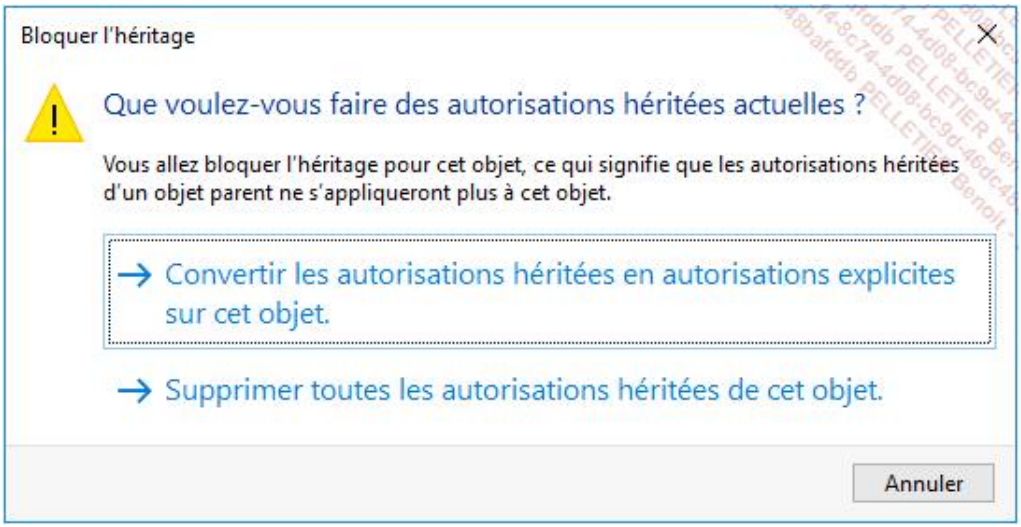
- Supprimez le groupe **Tout le monde** puis, avec le bouton **Ajouter**, insérez le groupe **Admins du domaine**.
- Assignez à ce dernier le droit **Contrôle total**.



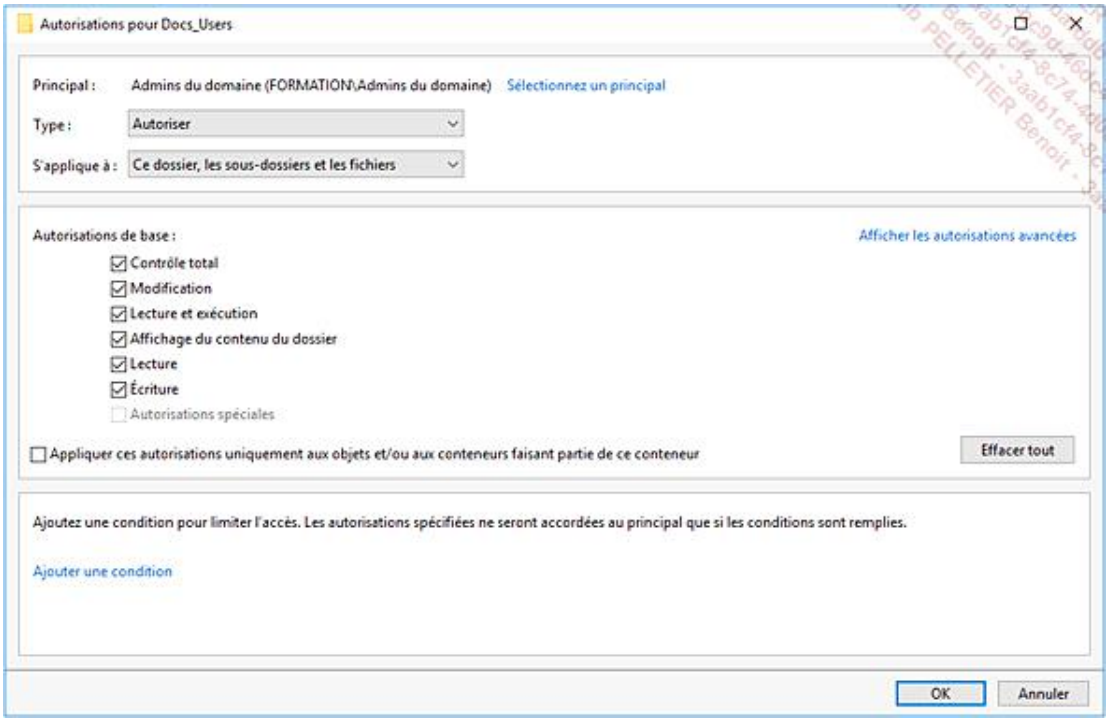
- Cliquez sur **Appliquer**, puis deux fois sur **OK**.
- Cliquez sur l'onglet **Sécurité** puis sur le bouton **Avancé**.

Le dossier hérite du parent (racine de la partition), il nous faut donc casser cet héritage afin de configurer les ACL comme nous le souhaitons.

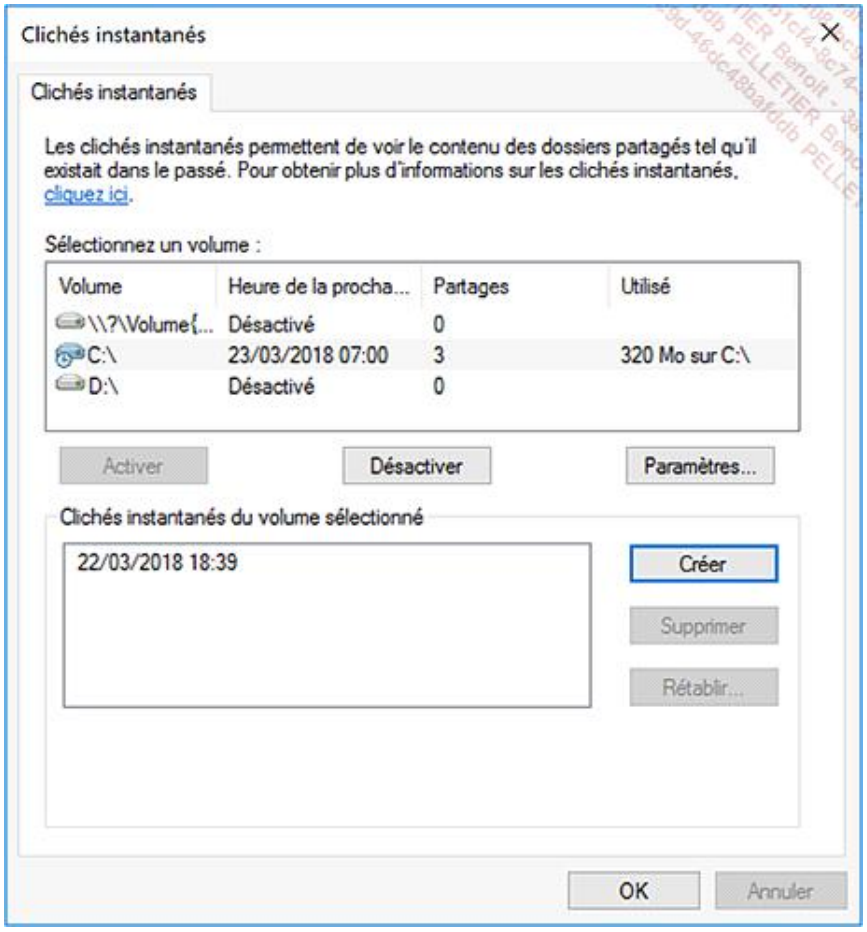
- Dans les options avancées, cliquez sur **Désactiver l'héritage**.
- Cliquez sur **Supprimer toutes les autorisations héritées de cet objet**.



- Cliquez sur **Ajouter** puis insérez le groupe **Admins du domaine**.
- Assignez-lui le droit **Contrôle total**.



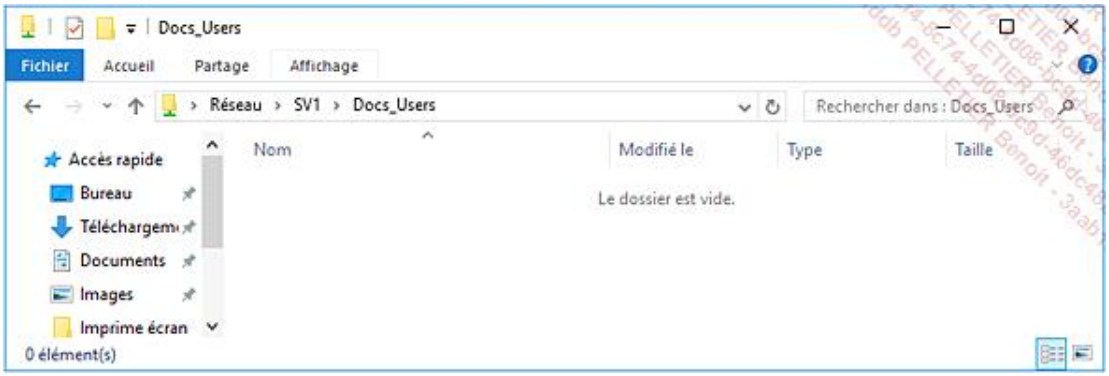
- Cliquez deux fois sur **OK** puis sur **Fermer**.
- Accédez de nouveau aux **Clichés instantanés**.
- Cliquez sur **Créer**.



La partie serveur a maintenant été configurée.

2. Récupération d'un fichier

- Accédez au partage depuis l'explorateur Windows. Pour cela saisissez dans ce dernier le chemin UNC (**\\SV1\Docs_Users**).

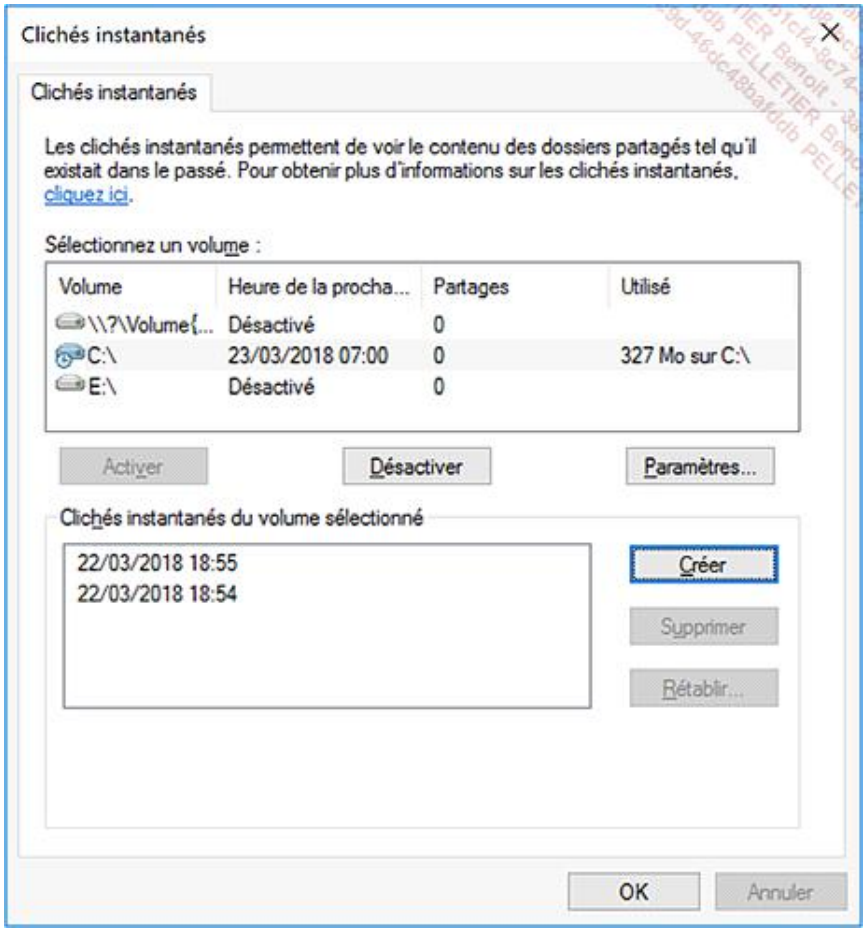


- Insérez dans le partage **Docs_Users** un fichier texte.

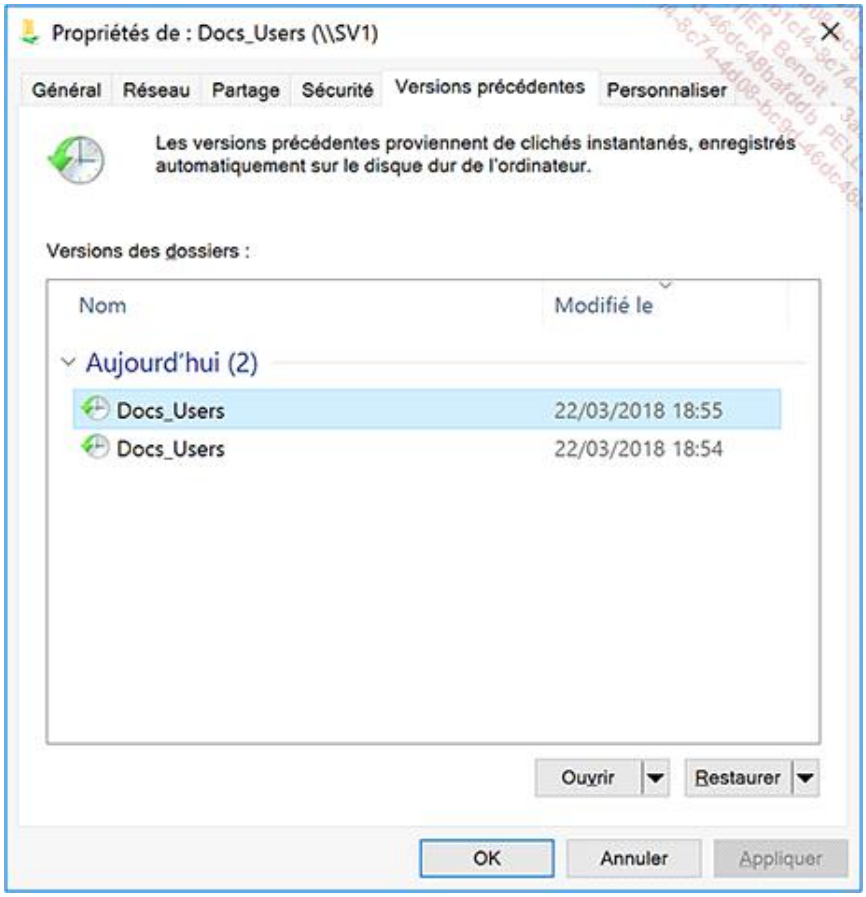
Insérez dans le fichier texte quelques caractères.

- Effectuez la création d'un nouveau cliché instantané depuis la fenêtre **Clichés instantanés**.

Désormais deux lignes composent le champ **Clichés instantanés du volume sélectionné**. Le premier cliché a été créé alors que le partage était vide et le deuxième comprend le fichier texte.

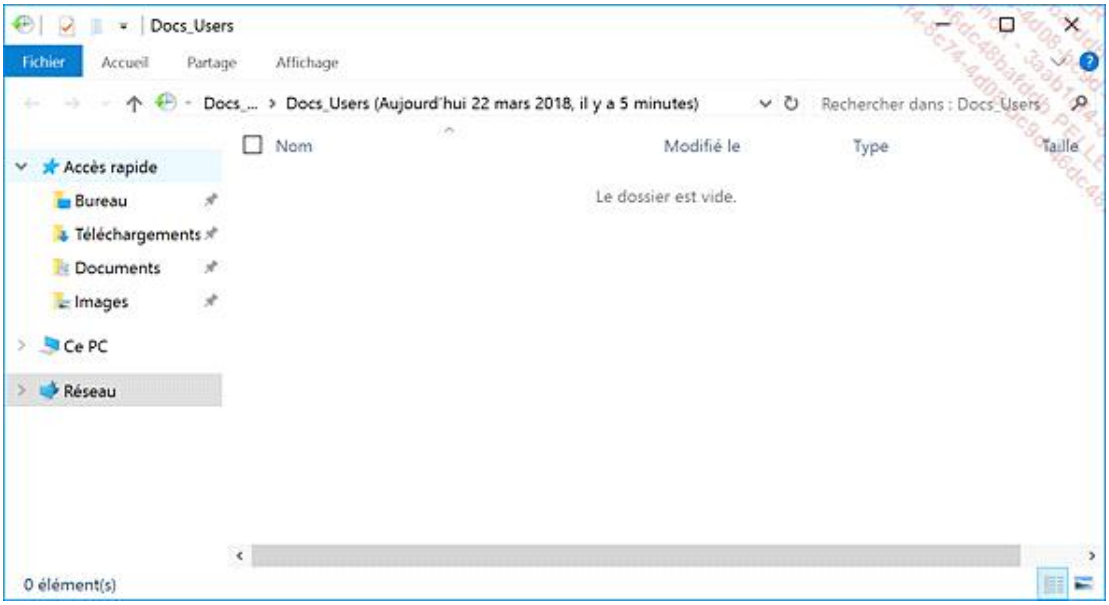


- Accédez au partage puis supprimez le fichier texte présent.
- Dans les propriétés du partage, cliquez sur l'onglet **Versions précédentes**.

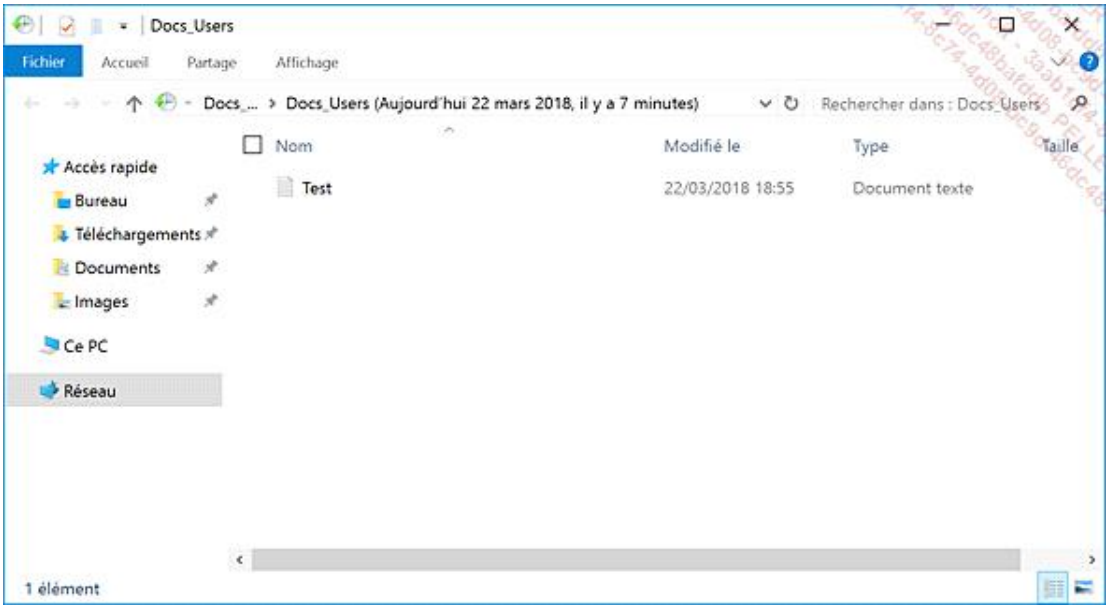


- Cliquez sur le cliché instantané le plus ancien puis sélectionnez **Ouvrir**.

Le dossier est bien vide.



- Recommencez l'opération sur la version la plus récente. Le fichier est bien présent. Il est possible de l'ouvrir ou de faire un copier-coller.



Dans l'onglet **Versions précédentes**, une autre option est présente : **Restaurer**, permettant que la restauration s'effectue dans l'emplacement d'origine.

Pour la restauration d'un seul fichier, il est préférable d'utiliser l'option **Ouvrir** et d'effectuer un copier coller.

Cliquez sur l'option **Restaurer**.

Un utilisateur peut ainsi restaurer un document sans l'assistance de l'administrateur système.

Le rôle Services d'impression

La console **Gestion de l'impression** est installée par l'intermédiaire du **Gestionnaire de serveur** et permet l'administration des imprimantes et serveurs d'impression.

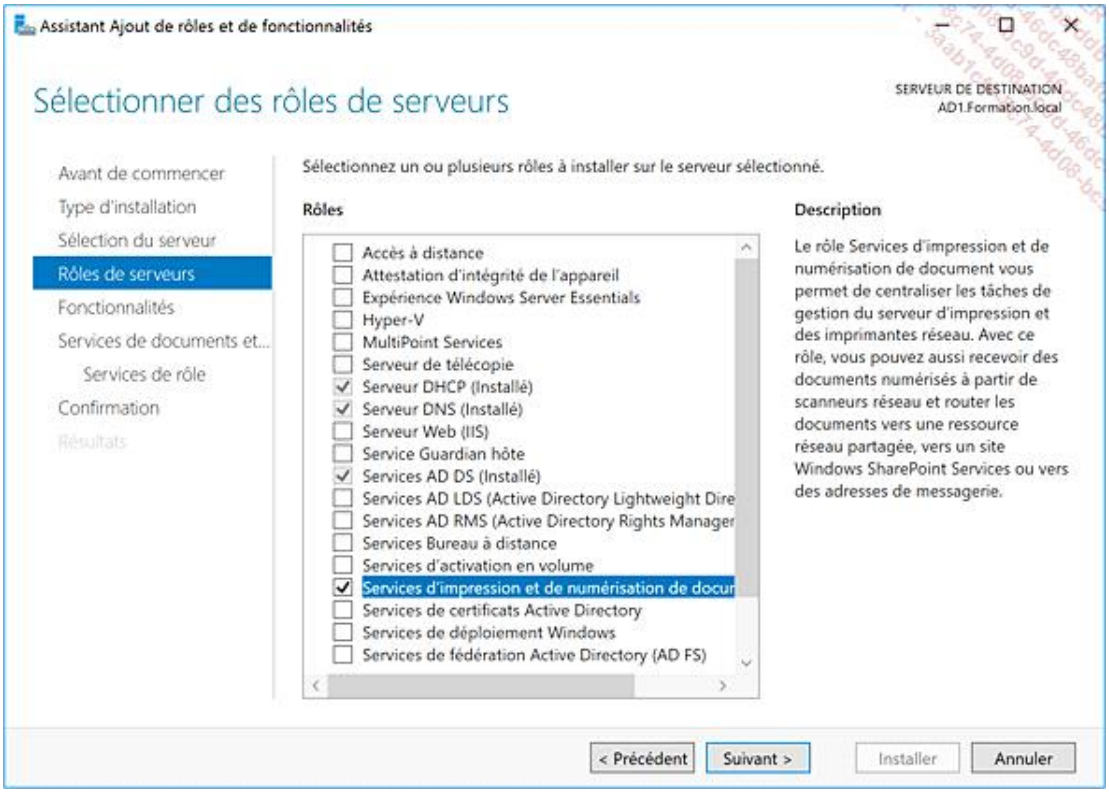
Des informations détaillées en temps réel sur l'état des différentes imprimantes et serveurs d'impression connectés au réseau sont fournies par l'intermédiaire de ce rôle.

Ainsi, il est possible d'effectuer des opérations de maintenance et de diagnostic à distance. La surveillance des files d'attente ou la détection des imprimantes posant problème est également prise en charge par la console. Pour les imprimantes qui nécessitent une attention particulière, des notifications par courrier électronique ou par des scripts peuvent être utilisées.

Le niveau de toner et de papier peut également être affiché pour les imprimantes qui fournissent une interface de gestion web.

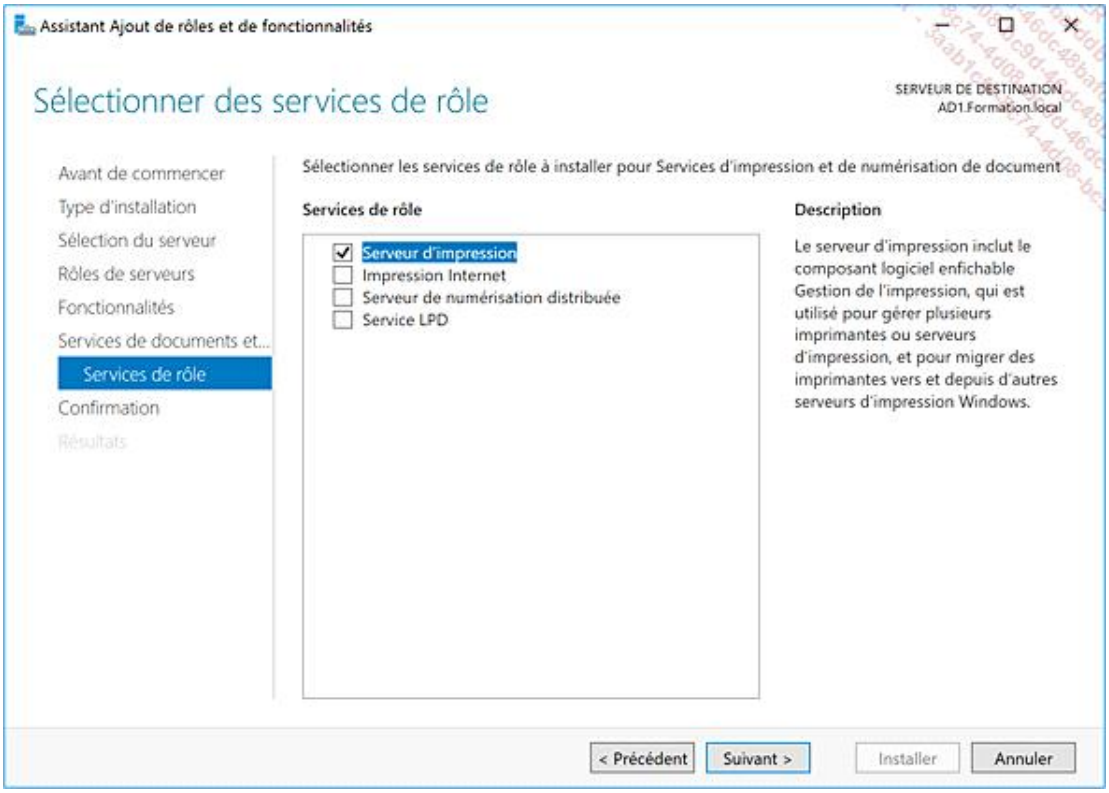
1. Ajout du rôle Services d'impression

- Ouvrez une session en tant qu'administrateur sur AD1.
- Lancez la console **Gestionnaire de serveur**.
- Cliquez sur **Ajouter des rôles et des fonctionnalités**.
- Dans la fenêtre **Sélectionner le type d'installation**, laissez le choix par défaut puis cliquez deux fois sur **Suivant**.
- Cochez la case du rôle **Services d'impression et de numérisation** dans la fenêtre **Sélectionner des rôles de serveurs**.



- Cliquez sur le bouton **Ajouter des fonctionnalités** dans la fenêtre qui s'affiche.
- Dans la fenêtre du choix des fonctionnalités, cliquez sur **Suivant**.

Laissez les services de rôle par défaut puis cliquez sur **Suivant**.



Le rôle serveur d'impression installe la console **Serveur d'impression** qui permet la gestion des imprimantes ou des serveurs d'impression. Il est possible de migrer des imprimantes vers les serveurs d'impression.

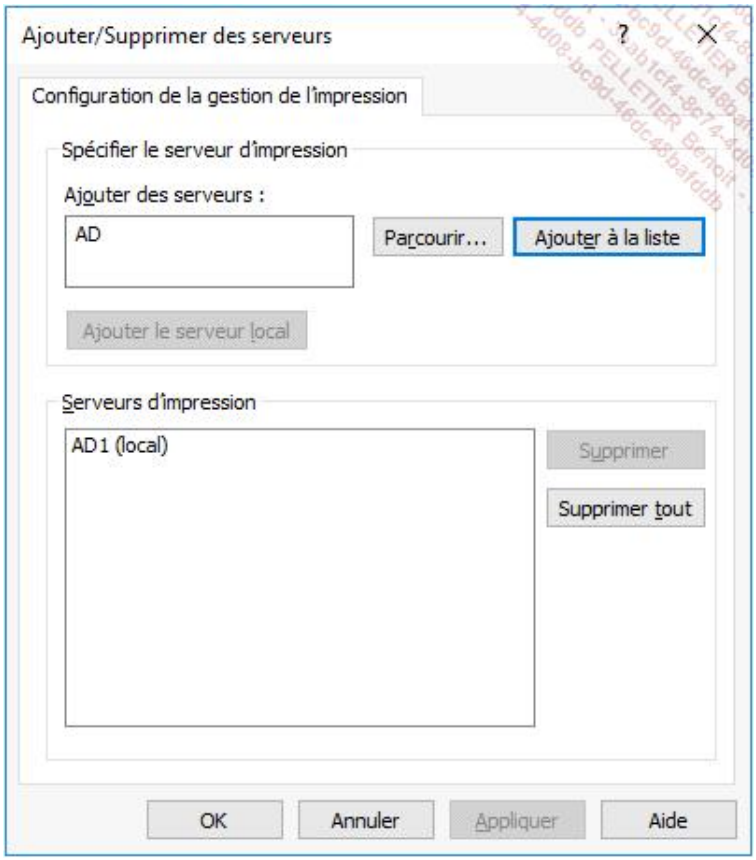
Le service de rôle Service LPD (*Line Printer Daemon*) installe le service **Serveur d'impression TCP/IP**. Ce dernier permet aux ordinateurs UNIX ou à d'autres ordinateurs utilisant le service LPR d'imprimer sur des imprimantes partagées sur ce serveur.

L'installation d'Impression Internet permet la création d'un site web hébergé par IIS. Ce site web permet aux utilisateurs de gérer des travaux d'impression sur le serveur.

Cliquez sur **Installer** pour lancer l'installation du rôle.

La console peut être lancée en saisissant la commande `printmanagement.msc` dans le menu **Exécuter**.

Il est possible d'ajouter un autre serveur d'impression afin de le gérer depuis la console. L'opération s'effectue à l'aide d'un clic droit sur le nœud **Serveur d'impression**. Il suffit par la suite de saisir le nom du serveur dans le champ et de cliquer sur **Ajouter à la liste**.

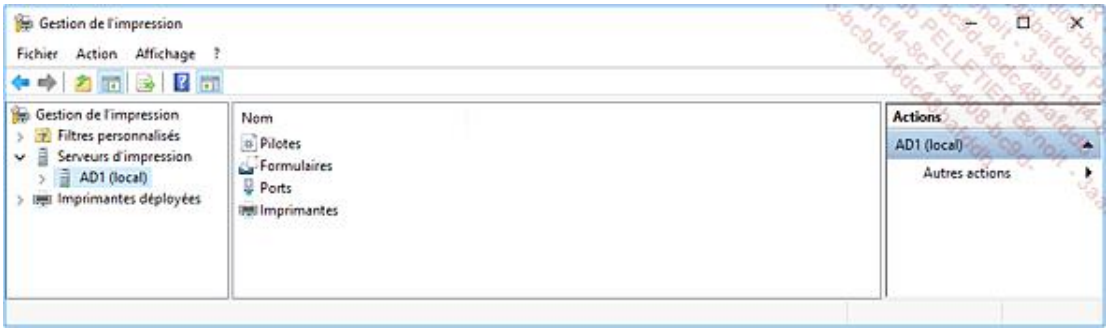


La console est accessible également en ouvrant la console MMC et en ajoutant le logiciel enfichable.

2. Ajout d'une imprimante réseau

L'imprimante réseau permet d'effectuer des impressions sur des imprimantes connectées au réseau informatique. La première étape est l'installation de l'imprimante sur le serveur d'impression. La console **Gestion de l'impression** permet d'effectuer cette opération. Il est par la suite possible d'effectuer un déploiement sur les postes de travail à l'aide de stratégies de groupe.

- Dans la console **Gestion de l'impression**, développez les nœuds **Serveurs d'impression** puis AD1 (local).

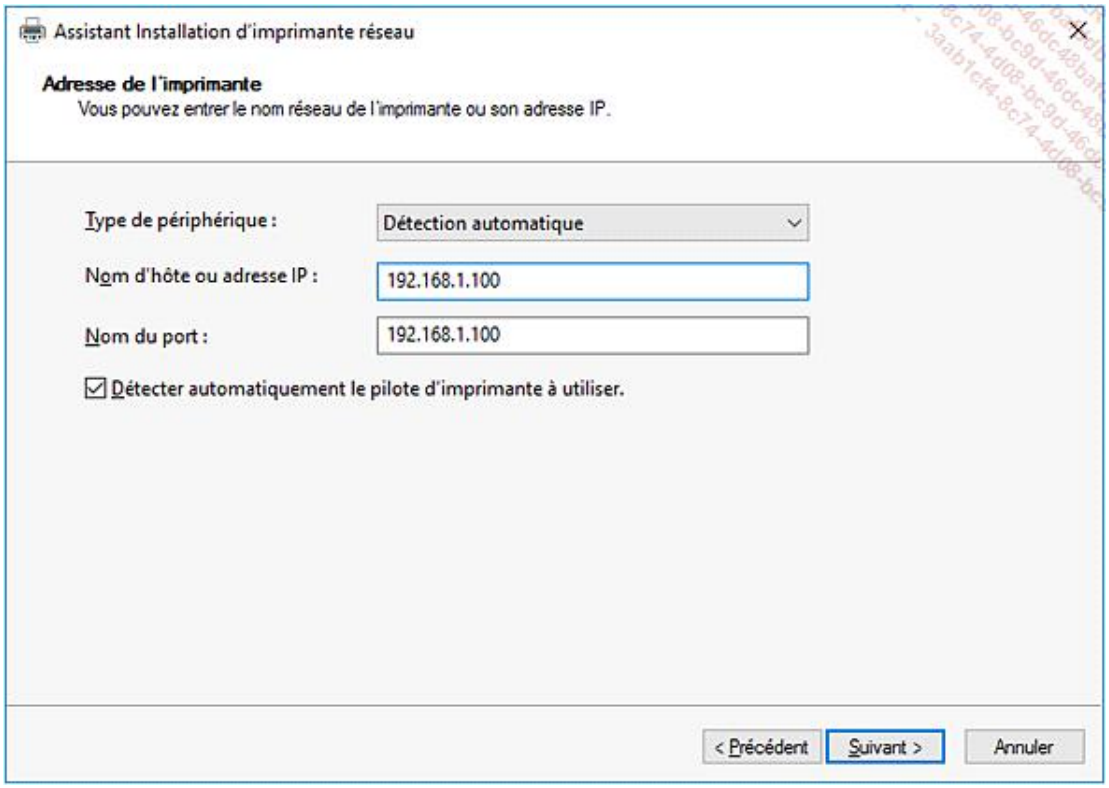


- Effectuez un clic droit sur **Imprimantes** puis sélectionnez **Ajouter une imprimante...**.
- Dans l'assistant, sélectionnez le choix **Ajouter une imprimante TCP/IP**.
- Dans la fenêtre **Adresse de l'imprimante**, configurez les champs comme ci-dessous :

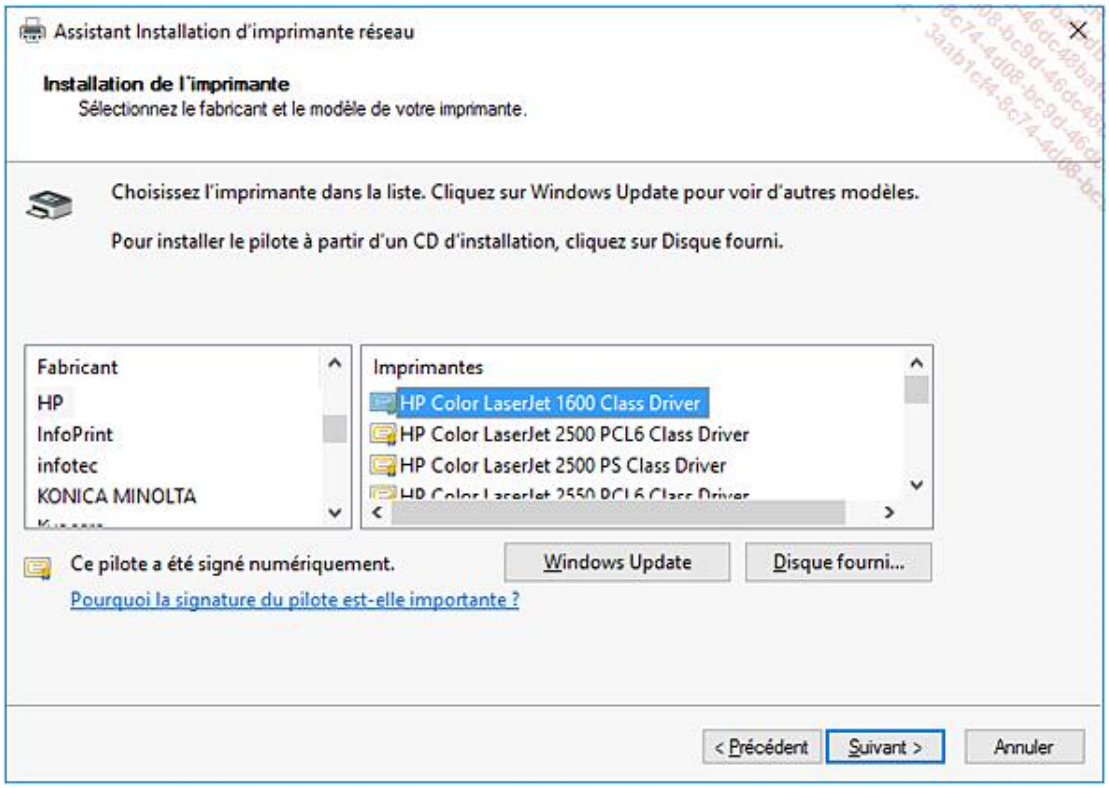
  Type de périphérique : Détection automatique

Nom d'hôte ou Adresse IP : 192.168.1.100

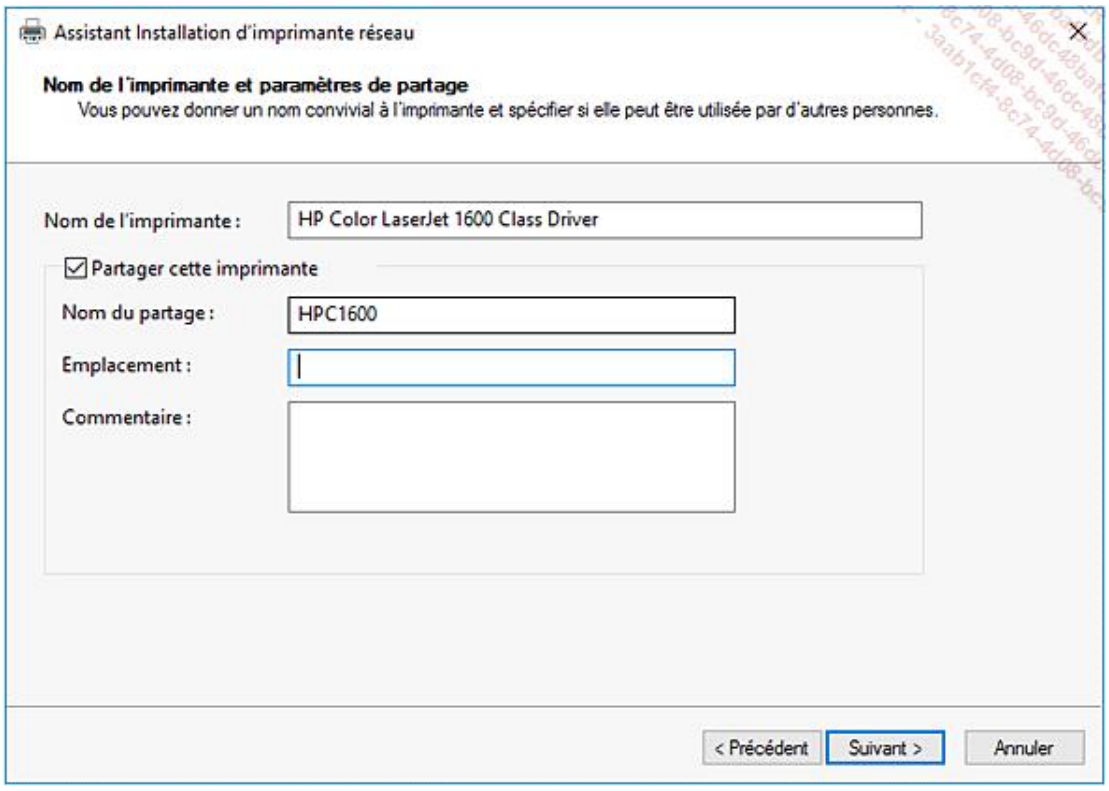
L'adresse IP utilisée n'existe pas dans le lab. En production, il est nécessaire d'utiliser l'adresse IP de l'imprimante.



- Dans la fenêtre **Informations supplémentaires requises concernant le port**, laissez le choix par défaut et cliquez sur **Suivant**.
- Dans la fenêtre **Pilotes d'imprimantes**, sélectionnez **Installer un nouveau driver** puis cliquez sur **Suivant**.
- Sélectionnez l'imprimante souhaitée puis cliquez sur **Suivant**.



- Dans la fenêtre **Nom de l'imprimante et paramètres de partage**, modifiez le nom du partage si nécessaire.



- Cliquez sur **Suivant** puis sur **Terminer**.

L'imprimante apparaît maintenant dans la console.

L'installation est terminée et il est maintenant possible d'effectuer la gestion de l'imprimante depuis la console

(déploiement…).

3. Gestion des imprimantes à l'aide de la console

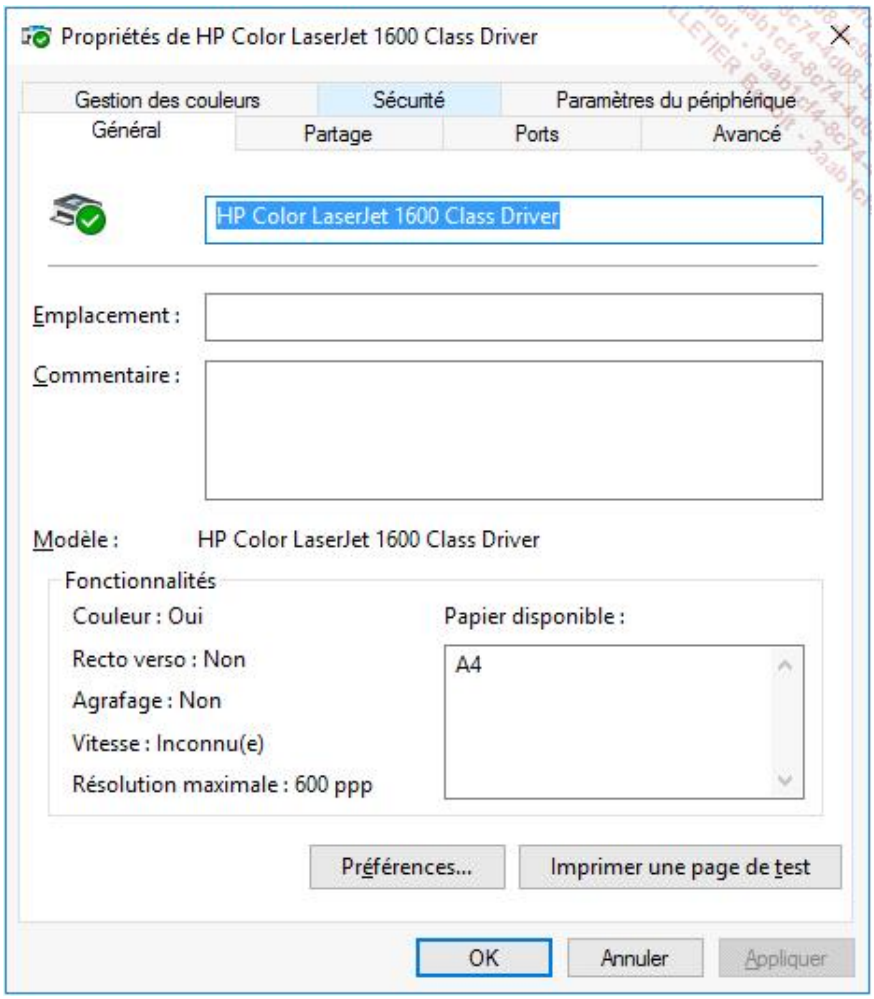
La console possède trois nœuds :

- **Filtres personnalisés**
- **Serveurs d'impression**
- **Imprimantes déployées**

Intéressons-nous au nœud **Serveur d'impression**. Ce dernier permet d'effectuer l'administration du serveur sélectionné. Comme vu précédemment, il est possible de rajouter une imprimante en effectuant un clic droit sur **Imprimantes** puis en sélectionnant **Ajouter une imprimante**. Il est également possible de configurer les propriétés de cette dernière.

- Effectuez un double clic sur l'imprimante précédemment ajoutée.

L'onglet **Général** permet d'imprimer une page de test, de saisir l'emplacement (bureau A12…) mais également de configurer les préférences de l'imprimante (orientation, papier, qualité).



- Cliquez sur l'onglet **Partage**.
- Si ce n'est pas déjà fait, cochez la case **Lister dans l'annuaire**.

Cette option permet à un utilisateur d'effectuer la recherche d'une imprimante afin de pouvoir l'installer sur son poste.

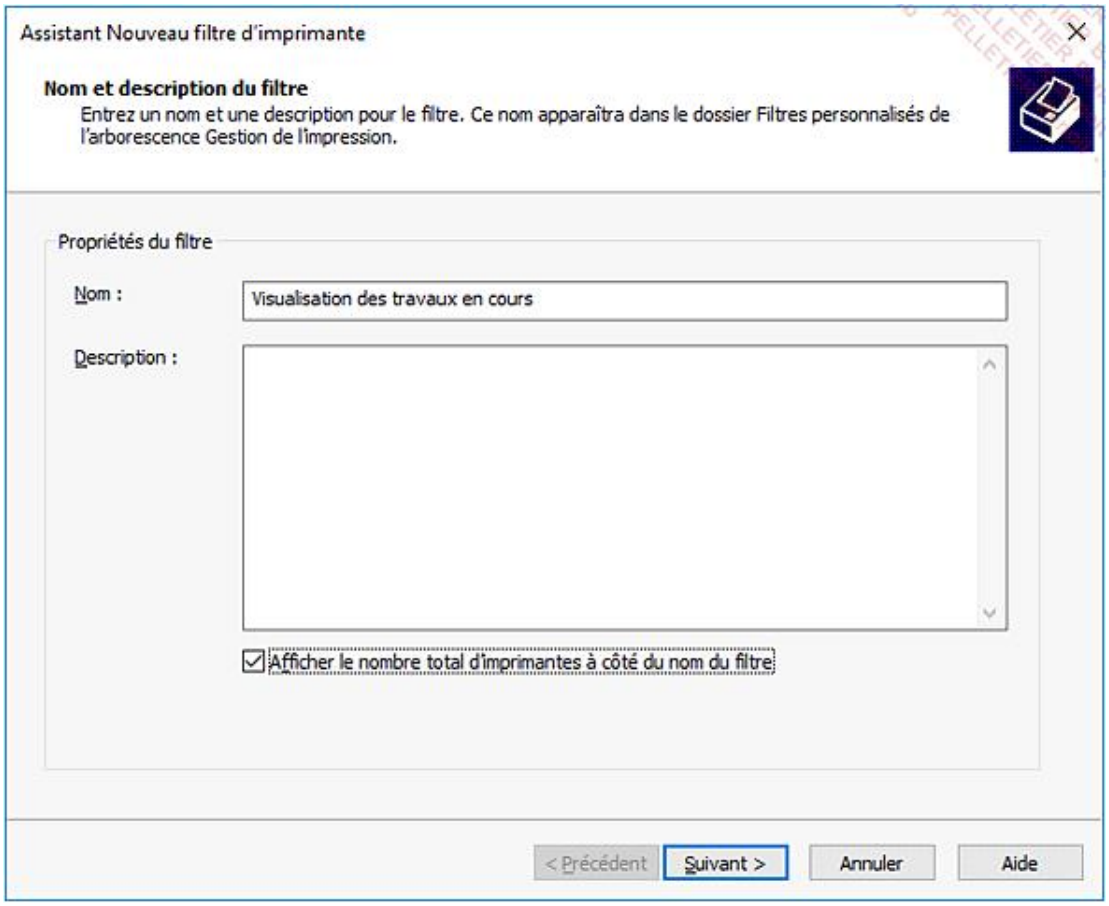
- Cliquez sur l'onglet **Sécurité**.

Il est possible de configurer les autorisations afin d'attribuer plus de droits ou d'interdire l'impression à un utilisateur.

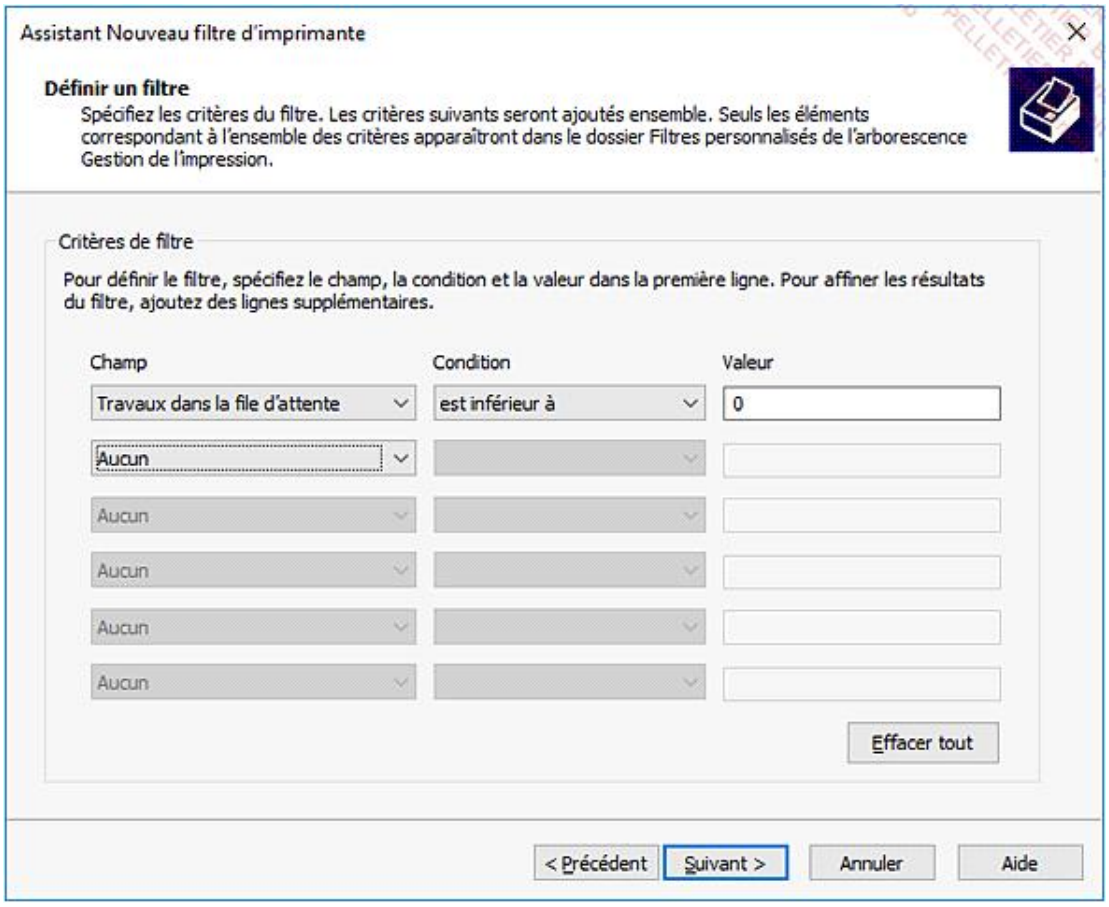
Par défaut, le groupe **Tout le monde** a le droit d'imprimer et les **Administrateurs** peuvent gérer l'imprimante (gestion des options, du partage…) et les documents (suppression d'un travail…).

Les filtres personnalisés permettent d'afficher des informations sur les imprimantes. Il est ainsi possible de visualiser très simplement l'ensemble des imprimantes et des pilotes mais également celles « avec travaux » (celles qui possèdent au moins un travail en cours) ou non prêtes (l'ensemble des imprimantes qui ne possèdent pas le statut « prêt »). Il est possible de créer son propre filtre afin d'obtenir l'information souhaitée.

- Effectuez un clic droit sur le nœud **Filtres personnalisés** puis cliquez sur **Ajouter un nouveau filtre d'imprimante**.
- Saisissez le nom du filtre souhaité dans le champ **Nom**.
- Cochez la case **Afficher le nombre total d'imprimantes à côté du nom du filtre** puis cliquez sur **Suivant**.



- Définissez les critères souhaités puis cliquez sur **Suivant**.



- La configuration des notifications est facultative. Cliquez sur **Terminer** en laissant les deux cases décochées.

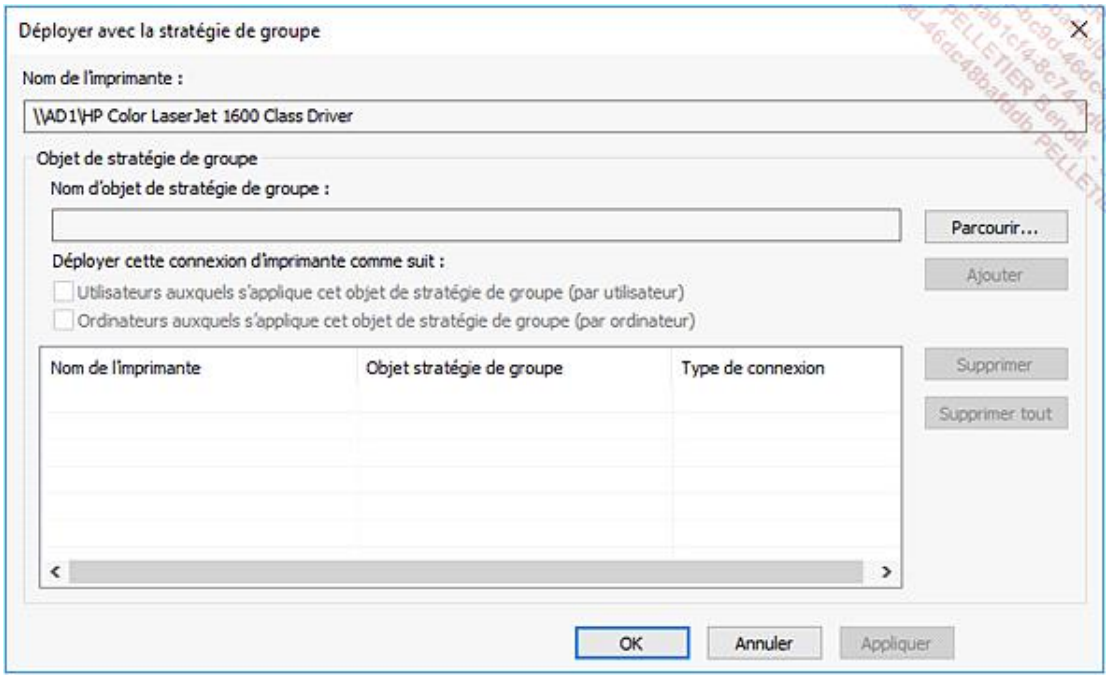
Le filtre est maintenant prêt à être utilisé.

4. Gestion du déploiement d'imprimantes

Le troisième nœud (imprimantes déployées) permet d'obtenir très rapidement des informations sur le déploiement configuré. Il est ainsi possible de connaître le nom du serveur mais également la stratégie de groupe utilisée.

- Effectuez un clic droit sur l'imprimante puis cliquez sur **Déployer avec la stratégie de groupe**.

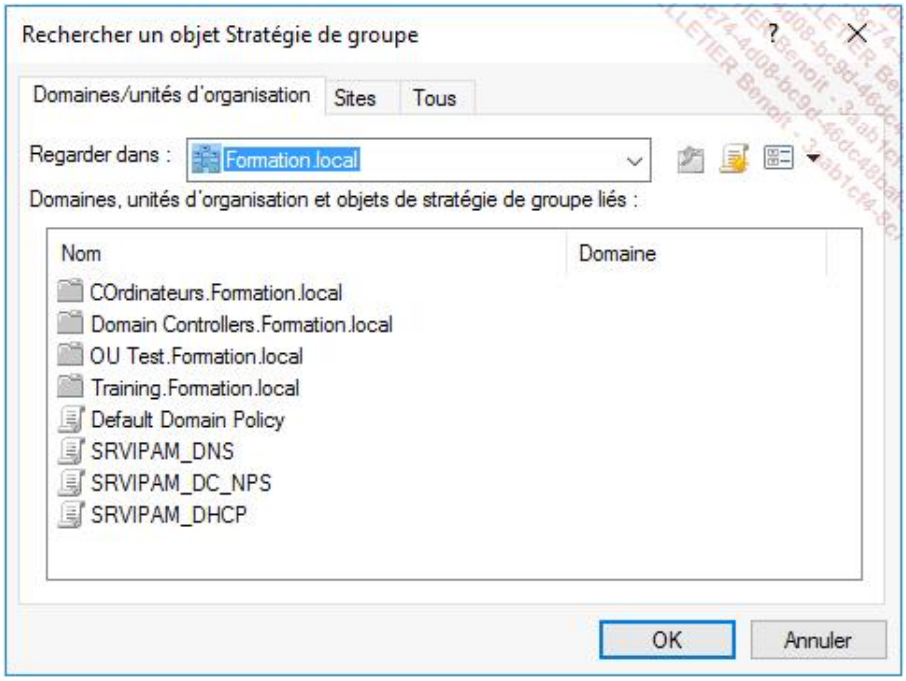
  La fenêtre **Déployer avec la stratégie de groupe** apparaît.



Cliquez sur le bouton **Parcourir** à droite du champ **Nom d'objet de stratégie de groupe**.

La fenêtre présente l'ensemble des stratégies de groupe déjà créées au niveau OU (unité d'organisation), domaine et site Active Directory.

Cliquez sur le bouton permettant la création d'une stratégie de groupe.



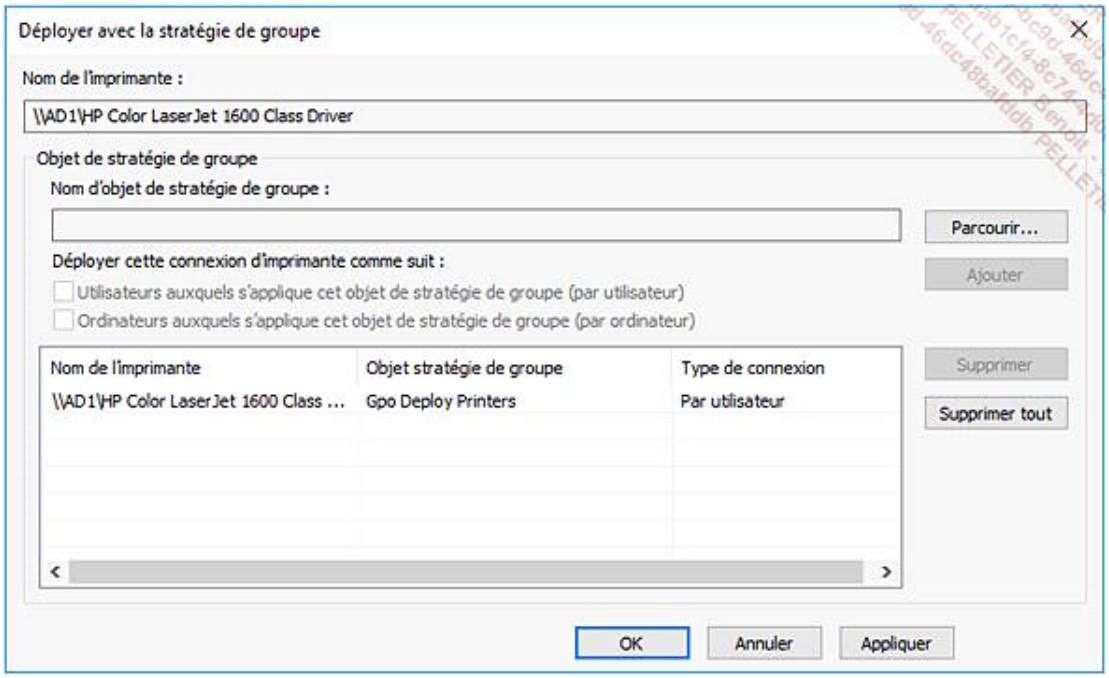
Saisissez le nom qui doit être donné à la stratégie de groupe puis cliquez sur **OK**.

La stratégie de groupe est créée à la racine du domaine. Il est possible de l'appliquer à une unité d'organisation.

La stratégie de groupe peut s'appliquer à un objet utilisateur ou à un objet ordinateur. Si vous cochez « par utilisateur », l'imprimante est installée sur les postes où l'utilisateur se connecte. Une application sur la partie ordinateur permet l'utilisation de l'imprimante pour l'ensemble des personnes qui ouvrent une session sur celui-ci.

- Cochez la case **Utilisateurs auxquels s'applique cet objet de stratégie de groupe (par utilisateur)**.
- Cliquez sur le bouton **Ajouter**.

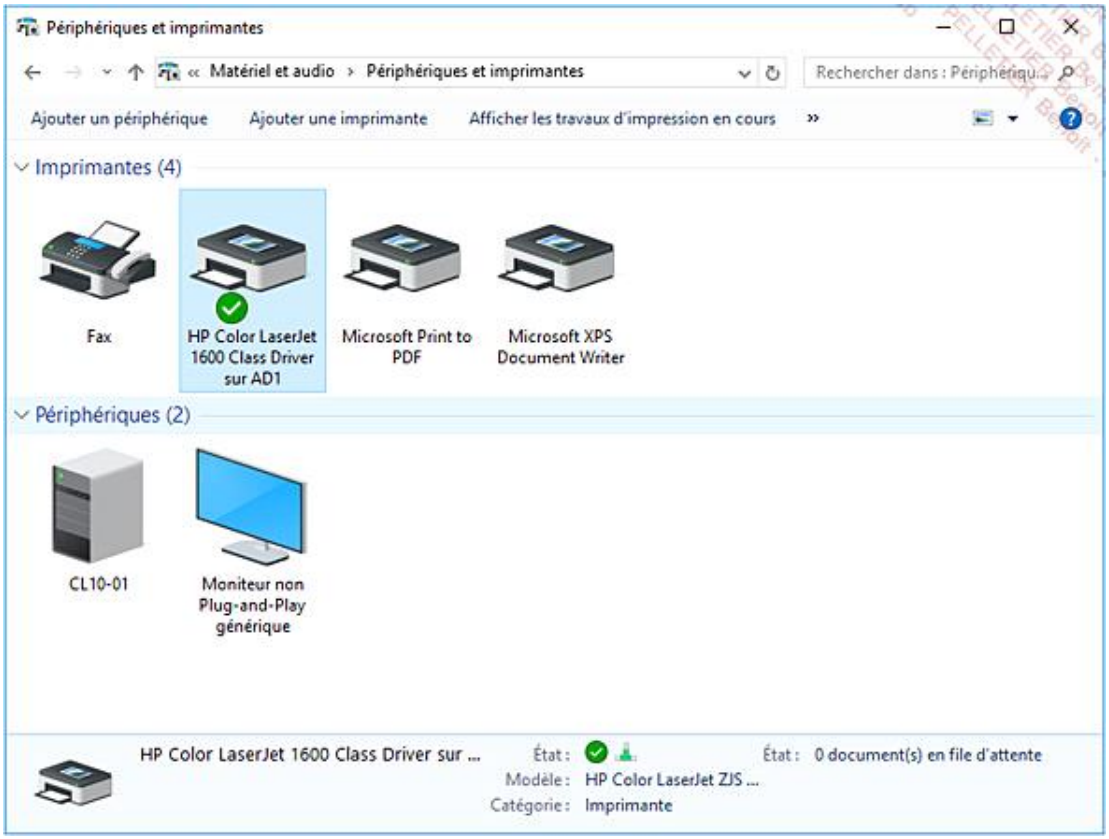
La stratégie de groupe est maintenant configurée pour déployer l'imprimante.



- Cliquez sur **OK**.
- Ouvrez une session en tant qu'administrateur sur CL10-01.
- Lancez une invite de commandes DOS (Admin) puis saisissez la commande `gpupdate /force`.

La commande permet au poste d'interroger son contrôleur de domaine afin de connaître d'éventuelles modifications sur les stratégies de groupe (ajout, modification d'un paramètre…). Cette opération s'effectue de façon automatique toutes les 90 à 120 minutes.

L'imprimante a été ajoutée dans **Périphériques et imprimantes** du panneau de configuration et il est impossible de la supprimer.



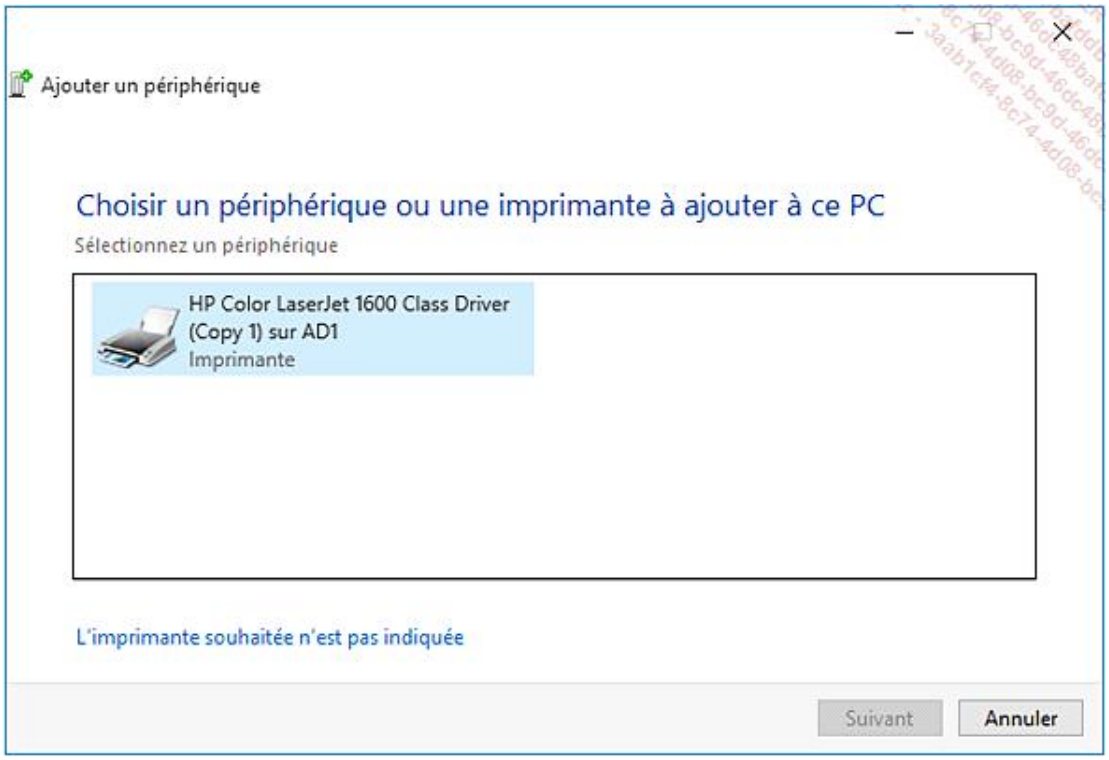
La stratégie de groupe a été appliquée au domaine et l'ensemble des objets utilisateurs reçoivent la stratégie. Il est possible de limiter l'étendue en l'appliquant à une OU. Les stratégies de groupe sont étudiées dans les chapitres suivants.

5. Recherche d'imprimantes dans Active Directory

Lors du partage d'une imprimante sur un serveur d'impression il est possible d'effectuer une publication de ce partage dans l'annuaire Active Directory. Cette opération permet d'alléger l'administration des postes de travail. L'utilisateur peut effectuer une recherche afin de trouver l'imprimante qu'il souhaite et effectuer l'installation sur son poste.

- Sur la machine virtuelle CL10-01, ouvrez le **Panneau de configuration**.
- Cliquez sur **Périphériques et imprimantes**.
- Dans la console, cliquez sur **Ajouter une imprimante**.

Après une recherche dans l'annuaire, une liste d'imprimantes est disponible. L'emplacement, si celui-ci a été saisi par l'administrateur, s'affiche dans le champ **Adresse**.



- Cliquez sur **Suivant**.

Une fenêtre apparaît informant de l'installation de l'imprimante.

- Cliquez sur **Terminer** pour finaliser l'installation.

L'imprimante est bien présente dans la console Périphériques et imprimantes.

La saisie de l'emplacement n'est pas obligatoire, mais permet aux utilisateurs une identification plus aisée de l'imprimante.

Rôle de serveur de fichiers

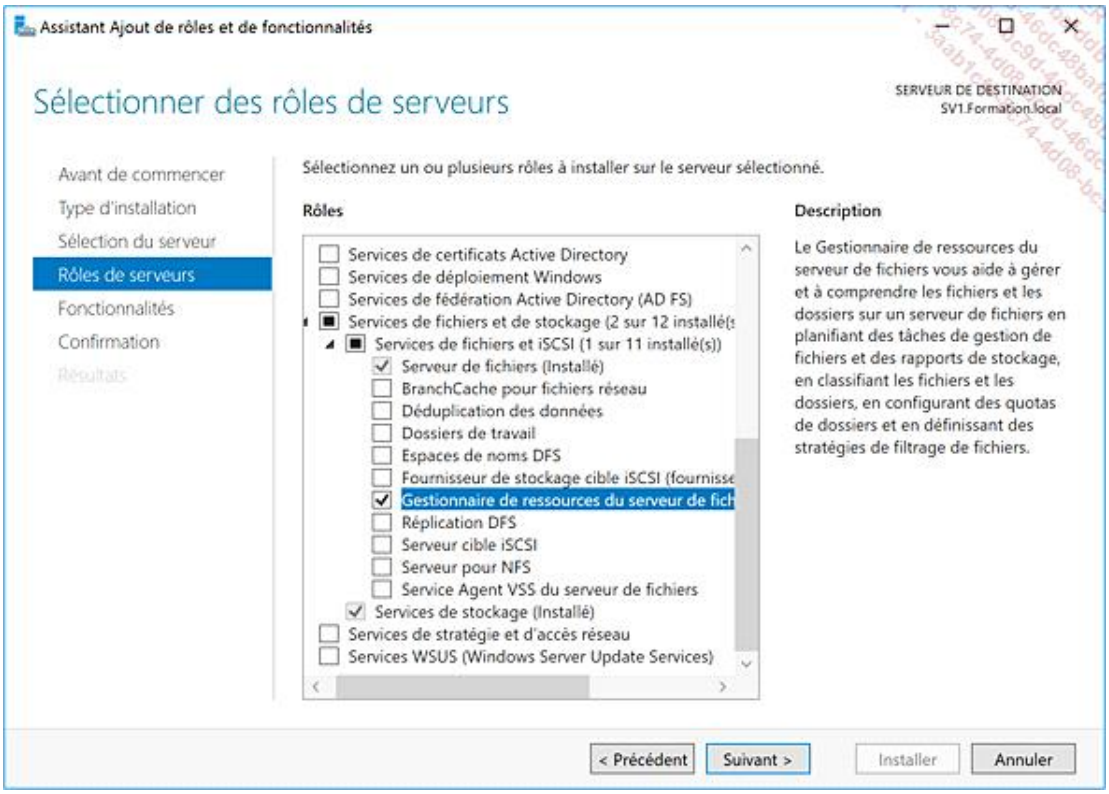
Un besoin croissant en matière de stockage ainsi qu'une disponibilité permanente sont les principales difficultés dans la gestion du stockage de fichiers. Pour répondre à tous ces impératifs, il est important de définir des stratégies de gestion des ressources de stockage.

1. Installation du rôle de serveur de fichiers

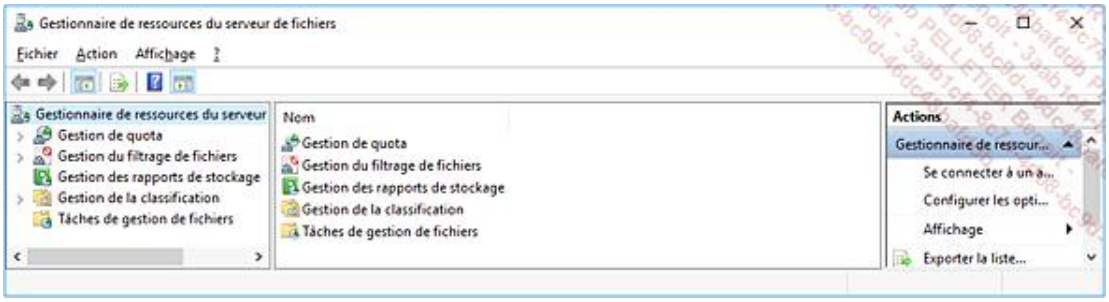
Le rôle serveur de fichiers met à disposition des administrateurs des outils pour la gestion du système de fichiers.

Il est donc possible d'en gérer la capacité en appliquant des quotas mais également avec un système de filtrage par extension. Les rapports permettent d'obtenir très rapidement une multitude d'informations (utilisation des quotas…).

- Démarrez la machine virtuelle **SV1**.
- Dans la console **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et des fonctionnalités**.
- Dans la fenêtre **Sélectionner le type d'installation**, laissez le choix par défaut.
- Dans la fenêtre de sélection du serveur de destination, laissez le choix par défaut et cliquez sur **Suivant**.
- Déroulez **Services de fichiers et de stockage** puis **Services de fichiers et iSCSI**.
- Cochez **Gestionnaire de ressources du serveur de fichiers** puis cliquez sur le bouton **Ajouter des fonctionnalités** dans la fenêtre qui s'affiche.



- Cliquez sur **Installer** pour confirmer l'installation.
- Dans les outils d'administration présents dans le menu démarrer, accédez à la console **Gestionnaire de ressource du serveur de fichiers**.



La gestion du système de fichiers (création de modèle de quota, filtrage de fichiers, création des rapports) s'effectue par l'intermédiaire de cette console.

2. Mise en place et gestion des quotas

Le gestionnaire de ressources du serveur de fichiers permet de créer des quotas pour limiter l'espace alloué à un volume ou un dossier. Il est possible lors de la création d'un quota de s'appuyer sur un modèle (qui va faciliter d'éventuelles modifications) ou de configurer les propriétés lors de la création du quota.

On peut attribuer à une ressource deux types de quota :

- **L'inconditionnel** : il ne permet pas de dépasser la limite configurée par l'administrateur et des notifications sont mises en place afin d'avertir l'administrateur et l'utilisateur du pourcentage d'utilisation de l'espace alloué. Ces paliers sont configurés par l'administrateur lors de la création des quotas, etc.
- **Le conditionnel** : le système de notification est identique mais l'utilisateur pourra dépasser la taille allouée par l'administrateur.

Plusieurs types de notifications sont configurables et peuvent être envoyés au moment souhaité (50 % d'utilisation du quota, etc.) :

- **Message électronique** : un courrier électronique est envoyé afin d'avertir l'utilisateur du dépassement du seuil.
- **Journal d'événements** : un événement informant du dépassement du seuil est ajouté dans le journal.
- **Commande** : une commande ou un script est exécuté. Il est possible d'exécuter la commande en tant que service local, service réseau ou système local.
- **Rapports** : un rapport peut être généré et envoyé par mail à l'administrateur ou à l'utilisateur.

Plusieurs modèles de quotas sont fournis au moment de l'installation du rôle et il est également possible d'en créer de nouveaux. Un modèle définit une limite d'espace, un type (conditionnel ou inconditionnel) ainsi qu'un ensemble de notifications à générer.

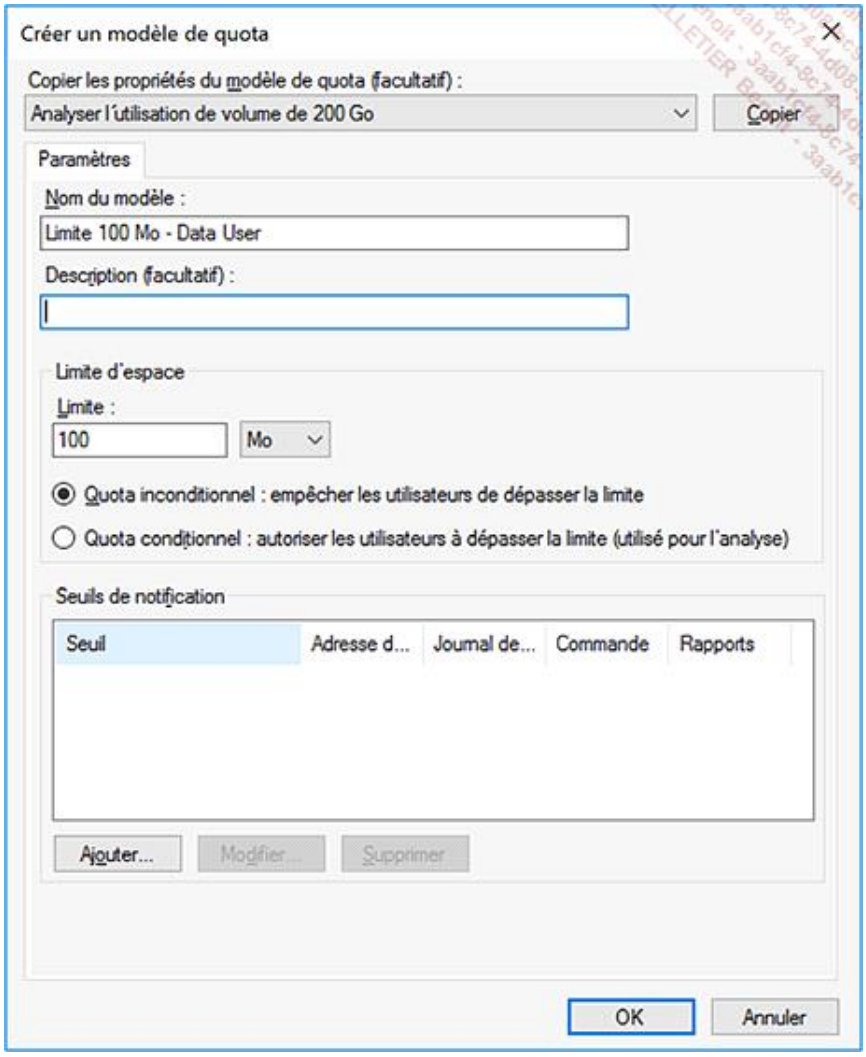
Lors de la création d'un quota, ce dernier récupère les paramètres définis dans le modèle. Il peut être appliqué sur un chemin d'accès ou automatiquement sur les sous-dossiers existants et sur les nouveaux dossiers.

Lors de la mise à jour d'un modèle, les quotas créés par l'intermédiaire de ce dernier sont également mis à jour.

- Dans la console, développez le nœud **Gestion de quota**.
- Effectuez un clic droit sur **Modèles de quotas** puis cliquez sur **Créer un modèle de quota**.

Il est possible de copier les propriétés d'un modèle déjà existant en choisissant le modèle souhaité dans la liste déroulante puis en cliquant sur **Copier**.

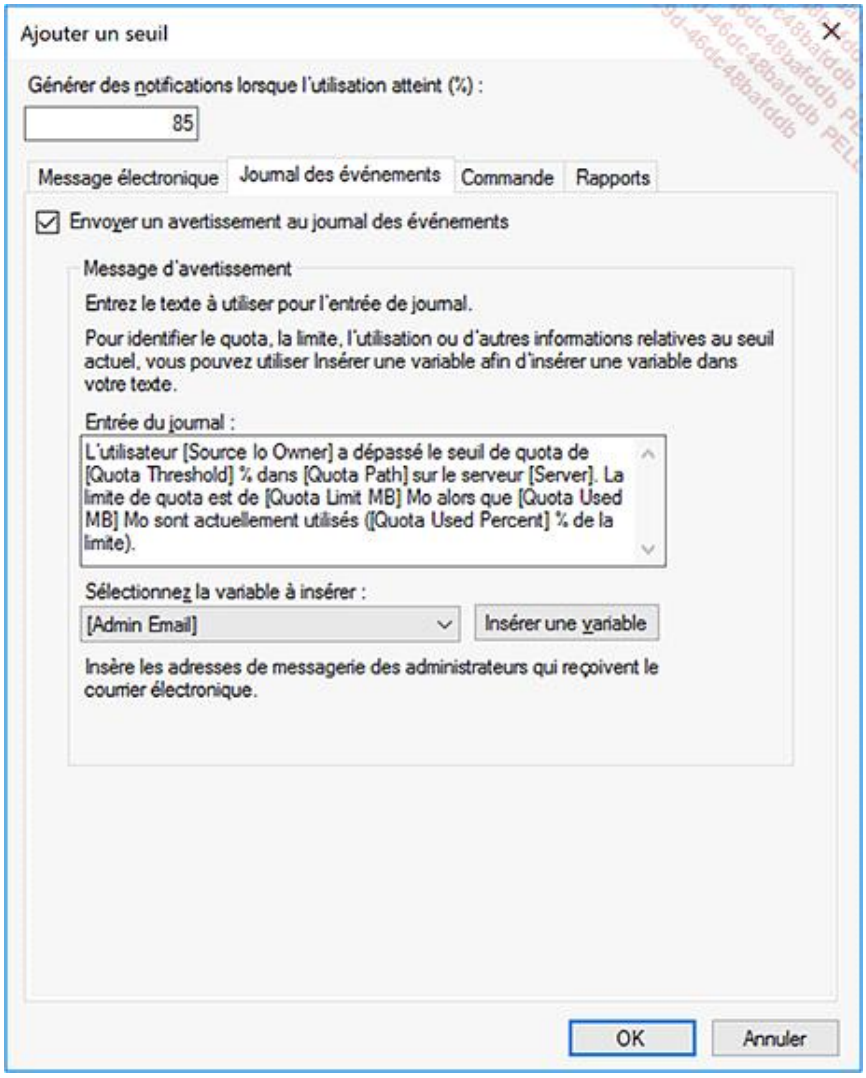
- Saisissez **Limit 100 Mo - Data User** dans le champ **Nom du modèle**.
- Laissez la limite à **100 Mo** et le type de quota à **Quota inconditionnel**.



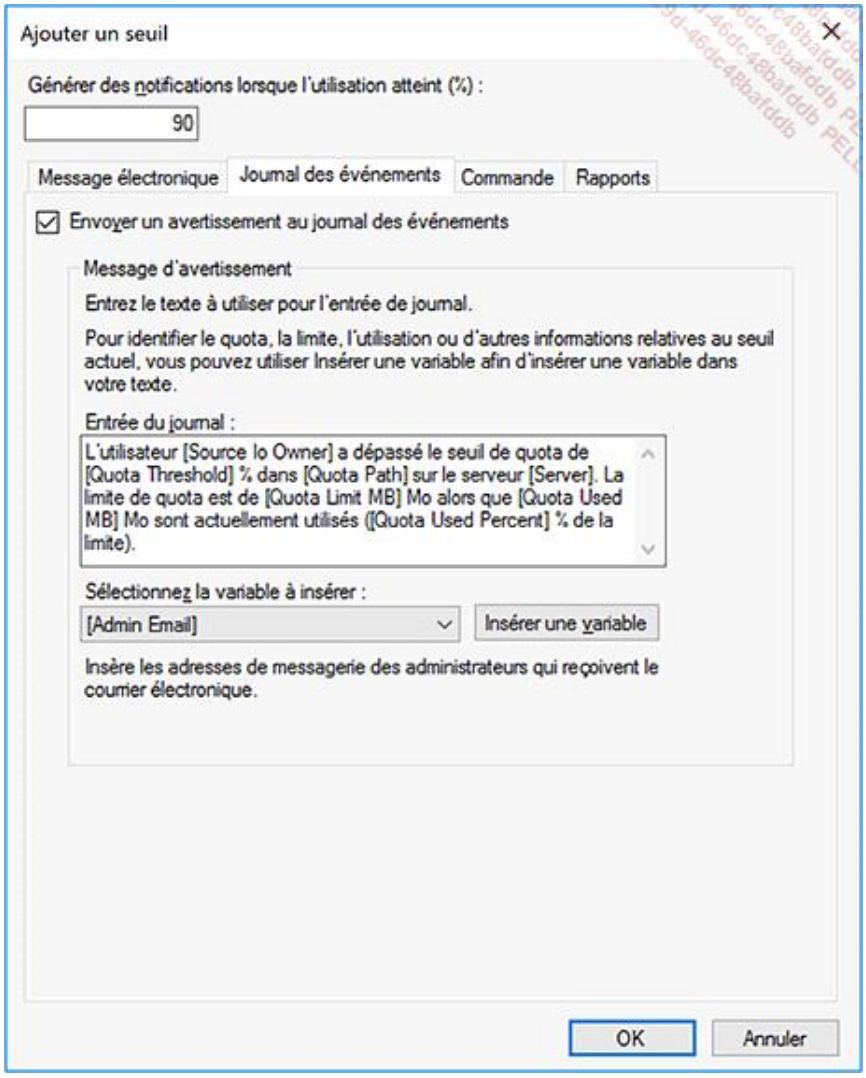
- Dans la zone **Seuils de notification**, cliquez sur le bouton **Ajouter**.

La notification qui est utilisée est l'ajout d'un événement dans le journal d'événements. Le champ **Journal des événements** contient du texte ainsi que des variables. Il est possible de modifier le texte en y ajoutant les variables souhaitées.

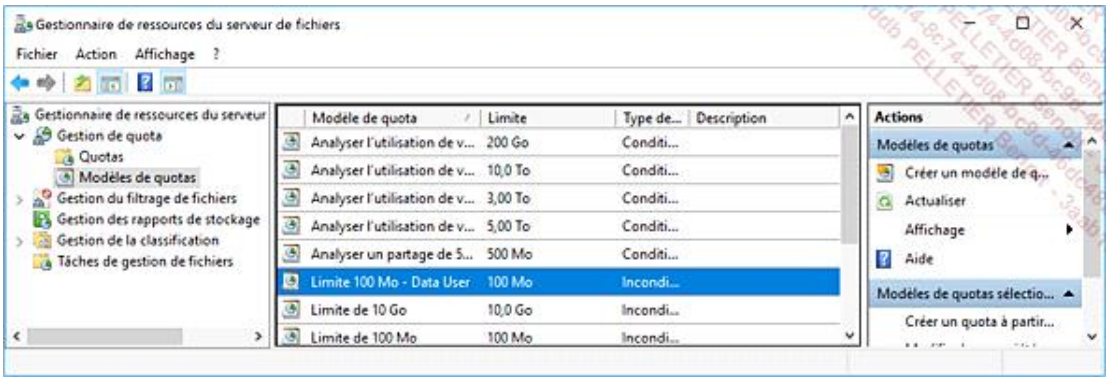
- Cochez la case **Envoyer un avertissement au journal des événements**.



Cliquez sur **OK** puis recommencez l'opération pour un seuil de notification à 90 %.



Cliquez sur **OK**. Le modèle a bien été ajouté.



Les quotas peuvent maintenant être ajoutés. Avant d'effectuer cette opération, les répertoires utilisateurs doivent être créés.

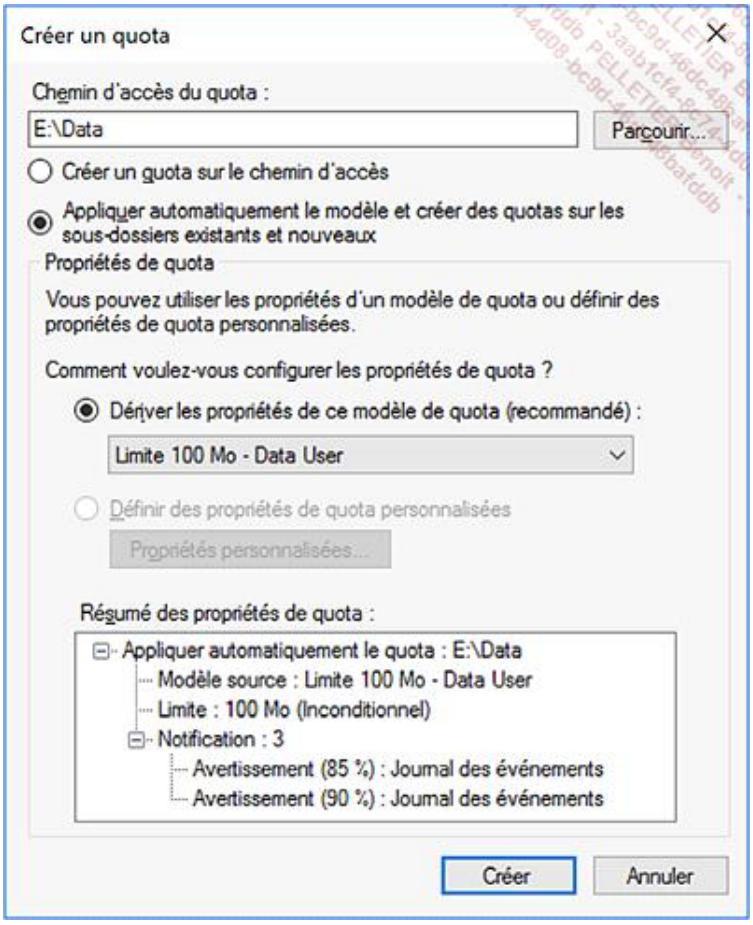
Sur le disque dur de la machine virtuelle, créez un dossier nommé **Data**.

Dans la console du **Gestionnaire de ressources du serveur de fichiers**, déroulez **Gestion de quota**.

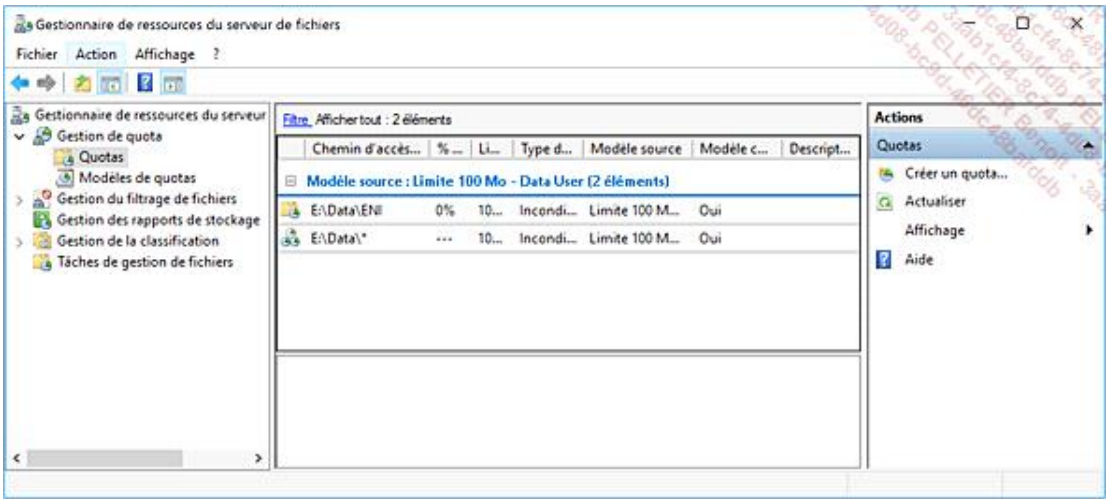
Effectuez un clic sur **Quotas** puis dans le bandeau **Actions**, cliquez sur **Créer un quota**.

Cliquez sur le bouton **Parcourir** afin de sélectionner le répertoire **Data** précédement créé.

- Sélectionnez le bouton radio **Appliquer automatiquement le modèle et créer des quotas sur les sous-dossiers existants et nouveaux**.
- Sélectionnez le modèle de quota **Limite 100 Mo - Data User**.



- Cliquez sur **Créer**. Le modèle apparaît maintenant dans la console.
- Dans le répertoire **Data**, créez un sous-répertoire **ENI**.
- Actualisez la console. Le quota positionné sur le sous-dossier apparaît.



- Lancez une invite de commandes DOS puis saisissez l'instruction suivante :

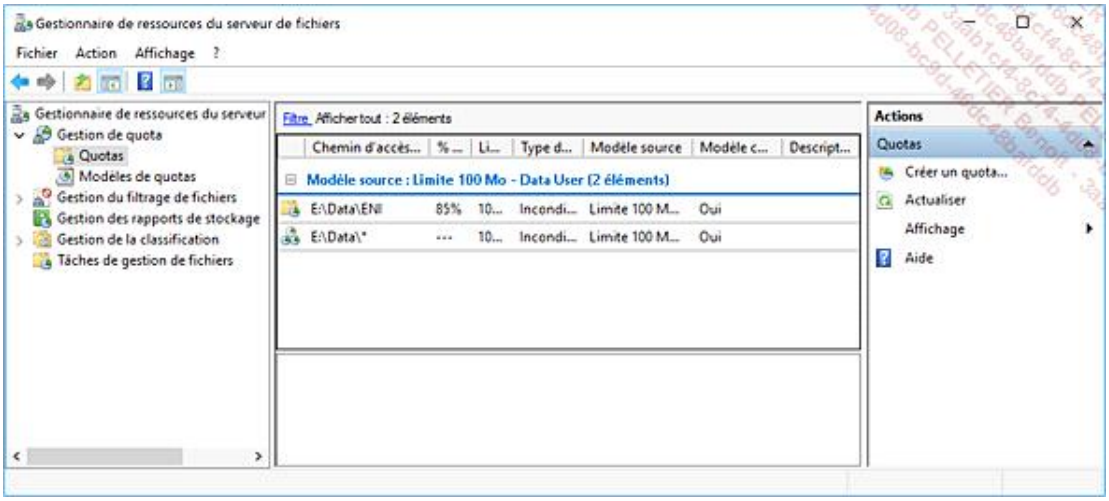
```
fsutil file createnew e:\Data\ENI\file1.txt 89400000
```

Le script est téléchargeable depuis la page Informations générales.

La commande permet de créer un fichier texte vide de 85 Mo.



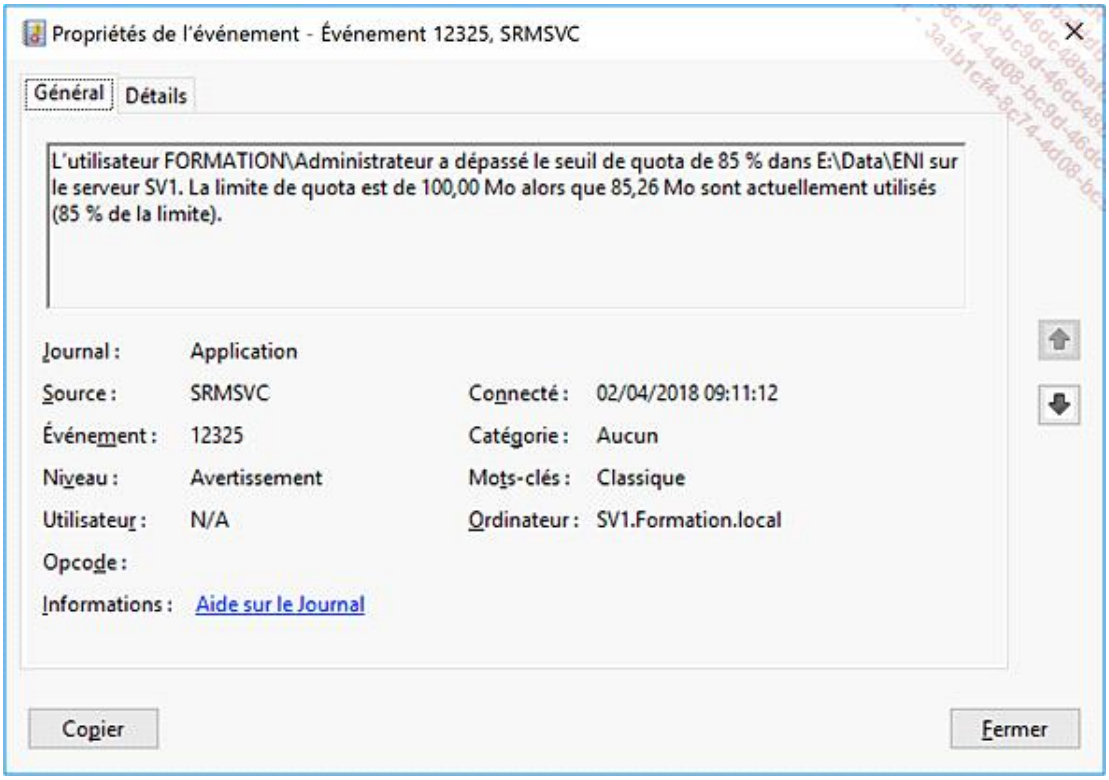
Le fichier est créé dans le sous-dossier **ENI** et possède une taille de 85 Mo.



Avec la création de ce fichier, le premier seuil d'alerte est atteint.

- Lancez la console **Gestionnaire de serveur** puis, à l'aide de la liste déroulante **Outils**, sélectionnez **Observateur d'événements**.
- Développez **Journaux Windows** puis cliquez sur le journal **Application**.

L'événement portant l'ID 12325 est présent. Il informe du dépassement du seuil.



Dans une invite de commandes DOS, saisissez l'instruction suivante :

```
fsutil file createnew e:\Data\ENI\file2.txt 16400000
```

Le script est téléchargeable depuis la page Informations générales.

Un message apparaît indiquant un espace disque insuffisant. Le quota est dépassé. Il est donc impossible d'ajouter le fichier.



À l'aide des quotas, il est plus aisé de gérer l'espace disque.

3. Implémentation du filtrage de fichiers

Le filtrage de fichiers est une méthode qui permet de contrôler les fichiers enregistrés sur un serveur de fichiers de l'entreprise.

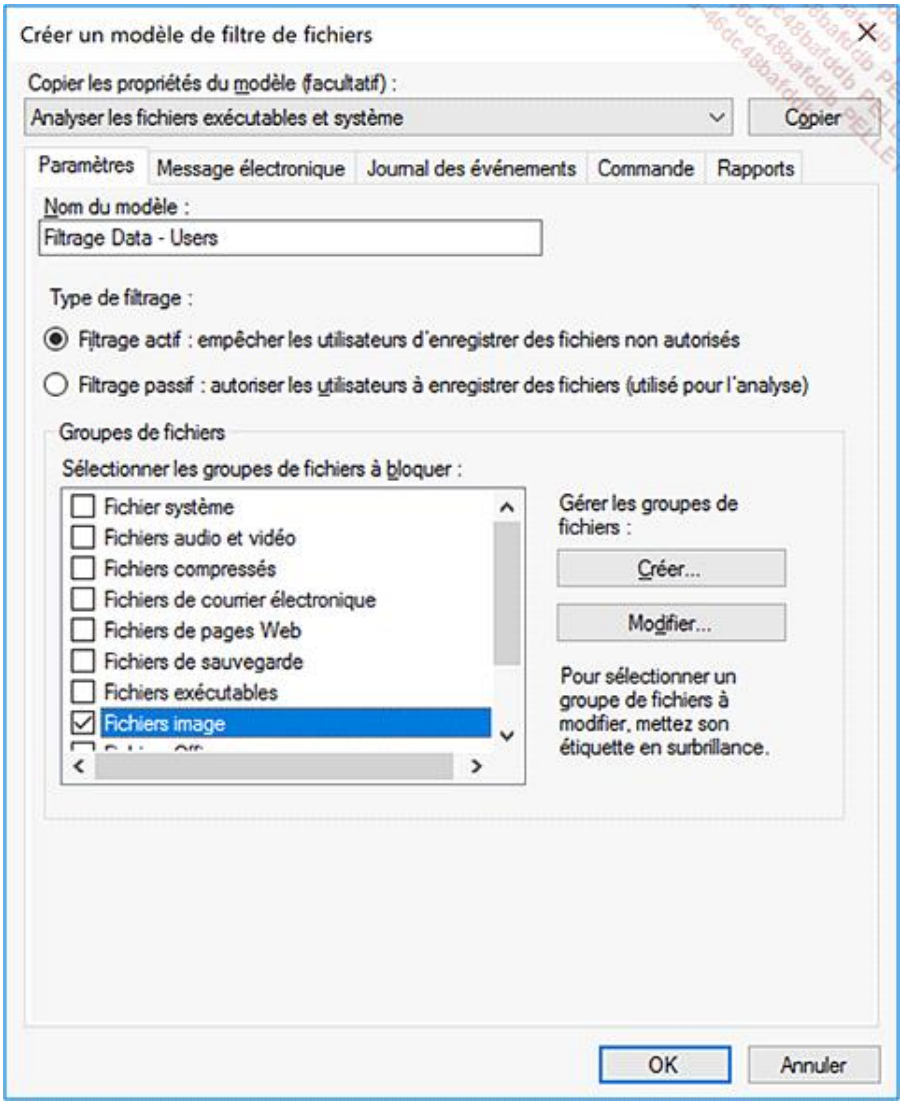
Comme pour les quotas, le nœud **Gestion du filtrage de fichiers** permet la création de filtres. Ces derniers sont appliqués à un chemin d'accès et ne permettent pas l'enregistrement de fichiers portant une extension interdite (jpg…).

Le modèle de filtre de fichier autorise la création de modèles servant par la suite à la création des filtres. Ils sont composés du groupe de fichiers à bloquer (fichiers image, fichiers exécutables…) qui permet d'indiquer les extensions à bloquer. Deux types de filtrages existent : les filtrages actifs qui empêchent l'enregistrement de fichiers non autorisés et les filtrages passifs qui autorisent eux l'enregistrement de fichiers non autorisés et qui servent uniquement à effectuer une analyse. Un modèle contient également des alertes (journaux d'événements, courrier électronique…), il est donc nécessaire de configurer les alertes souhaitées pour le modèle.

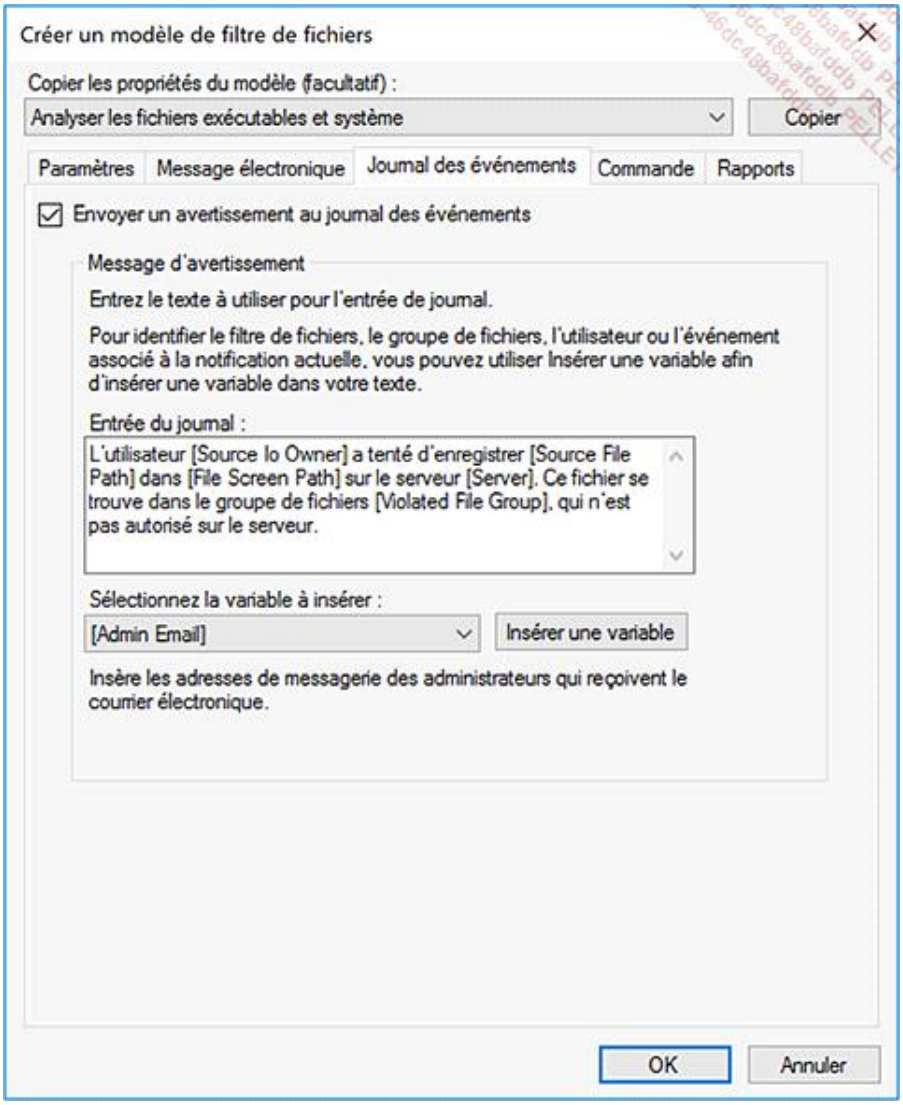
Lors de l'installation du rôle, des groupes de fichiers sont automatiquement ajoutés et la majorité des extensions trouvées sont présentes. Il est possible d'ajouter de nouveaux groupes si aucun de ceux présents ne répond à vos attentes.

Un groupe de fichiers contient deux catégories de fichiers, les fichiers à inclure et les fichiers à exclure. Si un groupe de fichiers est créé avec un filtrage sur l'extension *.mp*, les fichiers portant une extension commençant par mp sont bloqués (mp3, mpg, mpp). Néanmoins, il peut être nécessaire de stocker des fichiers Project portant l'extension mpp. Les fichiers à exclure permettent d'effectuer cette opération en indiquant au système de mettre une exception dans le filtre.

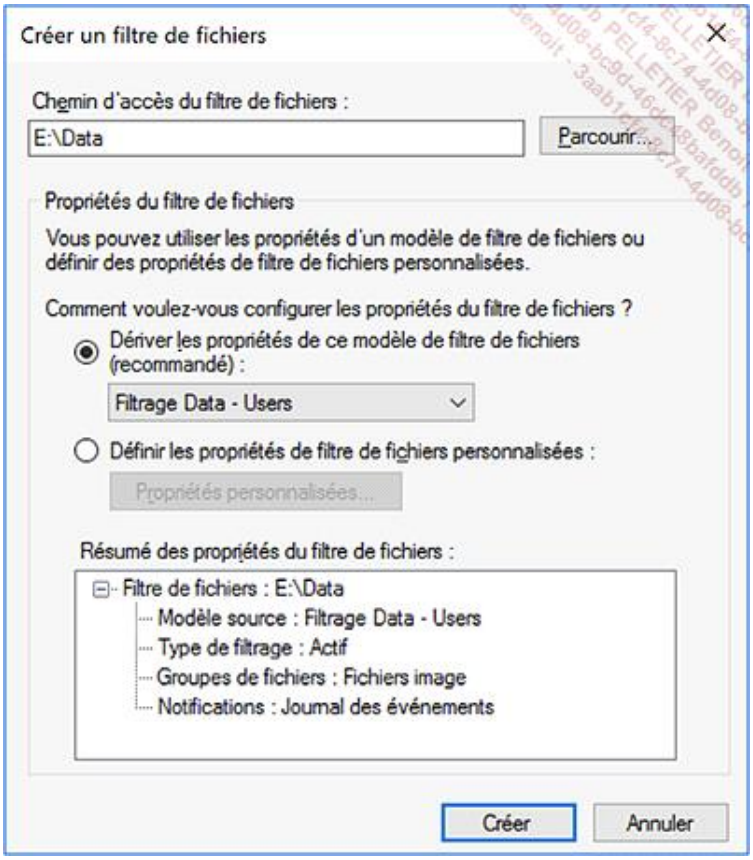
- Dans la console **Gestionnaire de ressources du serveur de fichiers**, développez le nœud **Gestion du filtrage de fichiers**.
- Effectuez un clic droit sur **Modèles de filtre de fichier** puis sélectionnez **Créer un modèle de filtre de fichier**.
- Saisissez **Filtrage Data - Users** dans le champ **Nom du modèle**.
- Sélectionnez **Filtrage actif** dans le type de filtrage puis **Fichiers image** dans le groupe de fichiers.



- Cliquez sur l'onglet **Journal des événements** puis cochez la case **Envoyer un avertissement au journal des événements**.



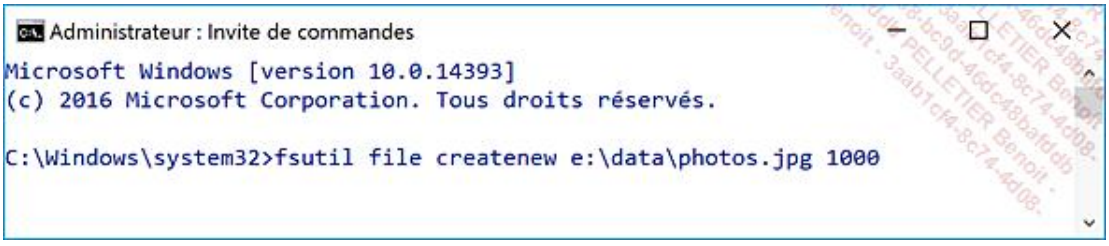
- Cliquez sur **OK** pour valider la création du modèle.
- Effectuez un clic droit sur **Filtres de fichiers** puis sélectionnez **Créer un filtre de fichier**.
- À l'aide du bouton **Parcourir**, sélectionnez le dossier **Data** puis le modèle **Filtrage Data - Users**.



- Cliquez sur le bouton **Créer**. Le filtre apparaît maintenant dans la console.
- Dans une invite de commandes DOS, saisissez l'instruction suivante :

```
fsutil file createnew e:\Data\photos.jpg 1000
```

Le script est téléchargeable depuis la page Informations générales.



L'écriture d'un fichier image est bien interdite dans **e:\Data**.

- Ouvrez l'**Observateur d'événement**, développez **Journaux Windows** puis cliquez sur le journal **Application**.

L'événement portant l'ID 8215 indique la tentative d'écriture d'un fichier dont l'extension est interdite.

- Dans une invite de commandes DOS, saisissez l'instruction suivante :

```
fsutil file createnew e:\Data\ENI\photos.jpg 1000
```

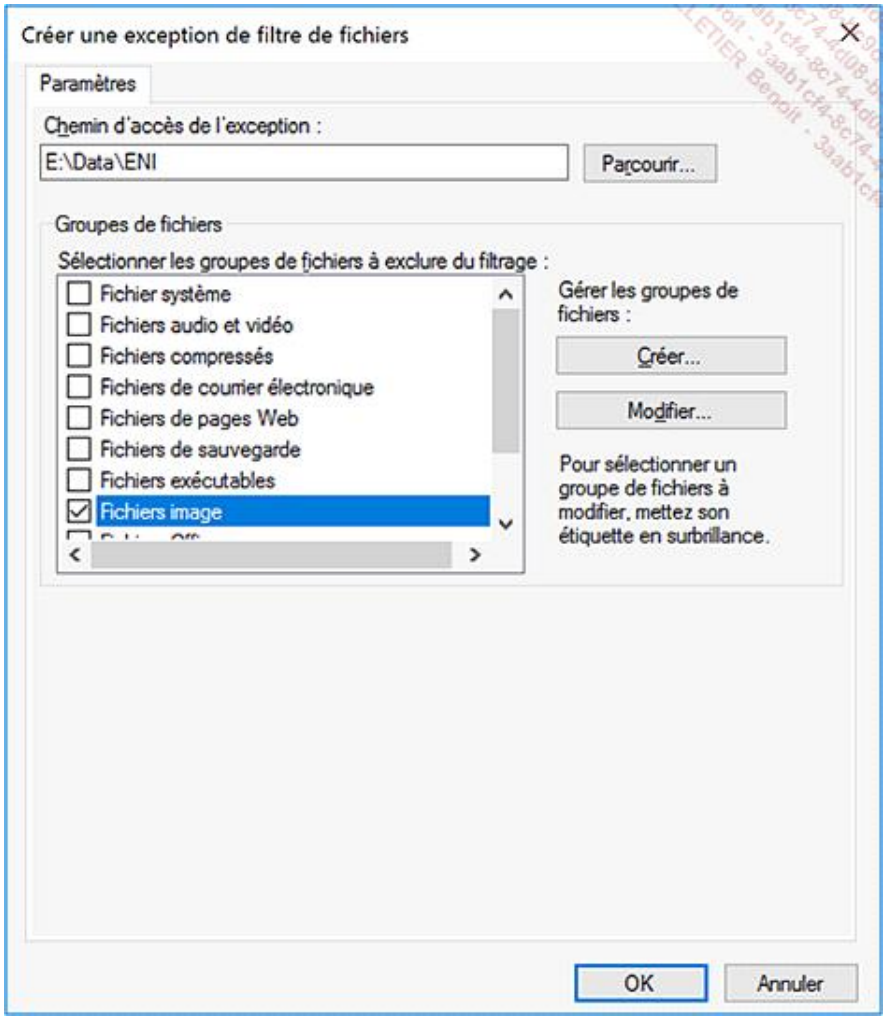
Le fichier bat est téléchargeable depuis la page Informations générales.

L'interdiction est également présente dans **e:\Data\ENI**.



Il est néanmoins possible d'autoriser dans le sous-dossier **ENI** les fichiers de type image. Il faut donc pour cela créer une exception de filtre de fichiers.

- Dans la console **Gestionnaire de ressources du serveur de fichiers**, développez **Gestion du filtrage de fichier**.
- Effectuez un clic droit sur **Filtre de fichiers** puis cliquez sur **Créer une exception de filtre de fichier**.
- À l'aide du bouton **Parcourir**, sélectionnez le dossier **E:\Data\ENI**.
- Cochez **Fichiers image** dans **Groupes de fichiers**.



- Cliquez sur **OK** pour créer l'exception.
- Dans une invite de commandes DOS, saisissez l'instruction suivante :

```
fsutil file createnew e:\Data\ENI\photos.jpg 1000
```



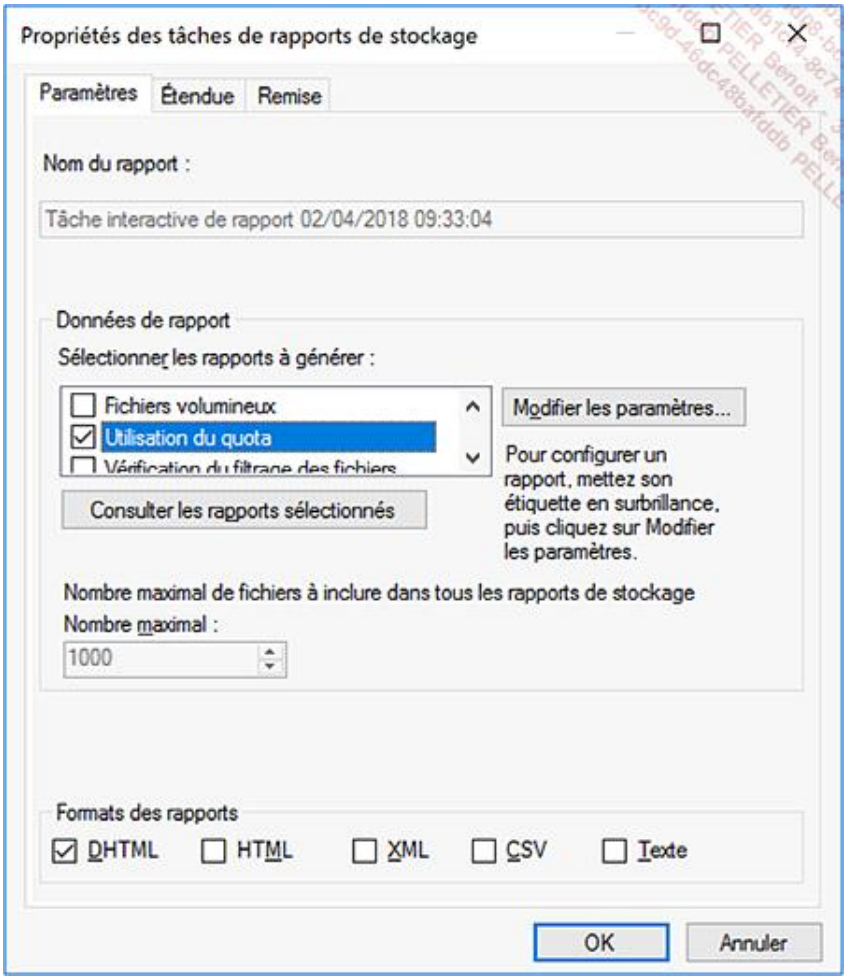
Le fichier peut maintenant être créé. Un utilisateur peut néanmoins passer outre le filtrage en modifiant l'extension du fichier.

4. Gestion des rapports de stockage

Les rapports de stockage fournissent des informations sur l'utilisation de fichiers sur un serveur. Ces rapports peuvent donner aux administrateurs une multitude d'informations. Il est ainsi possible de connaître la liste des documents les plus ou les moins ouverts (très pratique pour proposer une liste de fichiers à archiver). Il est également possible d'avoir des informations sur l'utilisation des quotas ou sur la vérification du filtrage de fichiers.

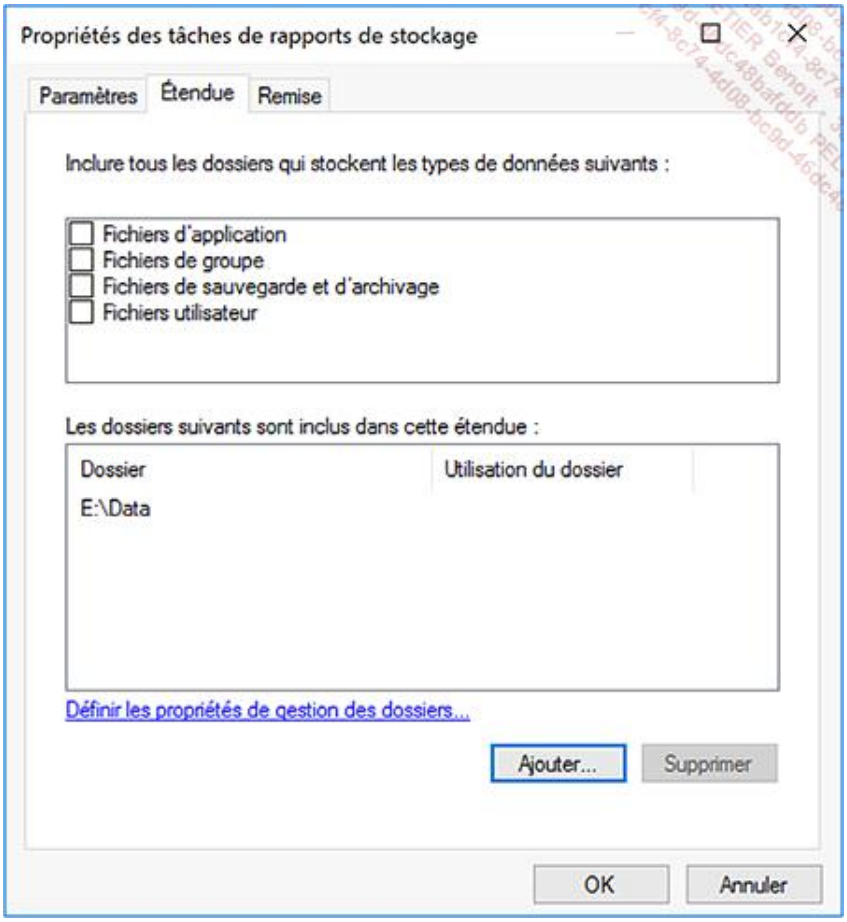
Un rapport peut être créé manuellement ou planifié en définissant une tâche de création de rapport. Cette dernière spécifie les volumes ou les dossiers sur lesquels porte le rapport, les types de rapports à générer mais également le format souhaité pour les rapports (DHTML, HTML, XML…) et la fréquence de génération.

- Dans la console **Gestionnaire de ressources du serveur de fichiers**, effectuez un clic droit sur **Gestion des rapports de stockage** puis cliquez sur **Générer les rapports maintenant**.
- Dans les données de rapport, sélectionnez **Utilisation du quota**.
- Laissez le format à **DHTML**.

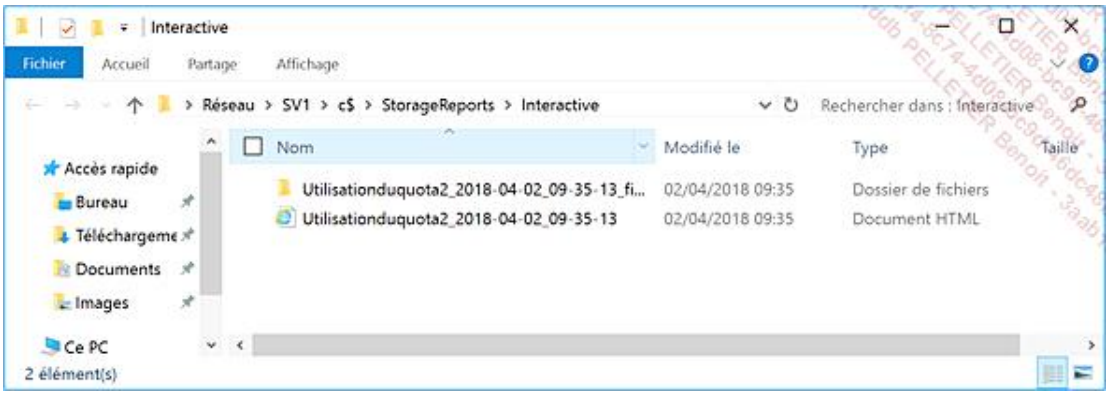


L'onglet **Étendue** permet d'ajouter des répertoires dans l'étendue d'application du rapport. L'onglet **Remise** permet lui un envoi par mail du rapport.

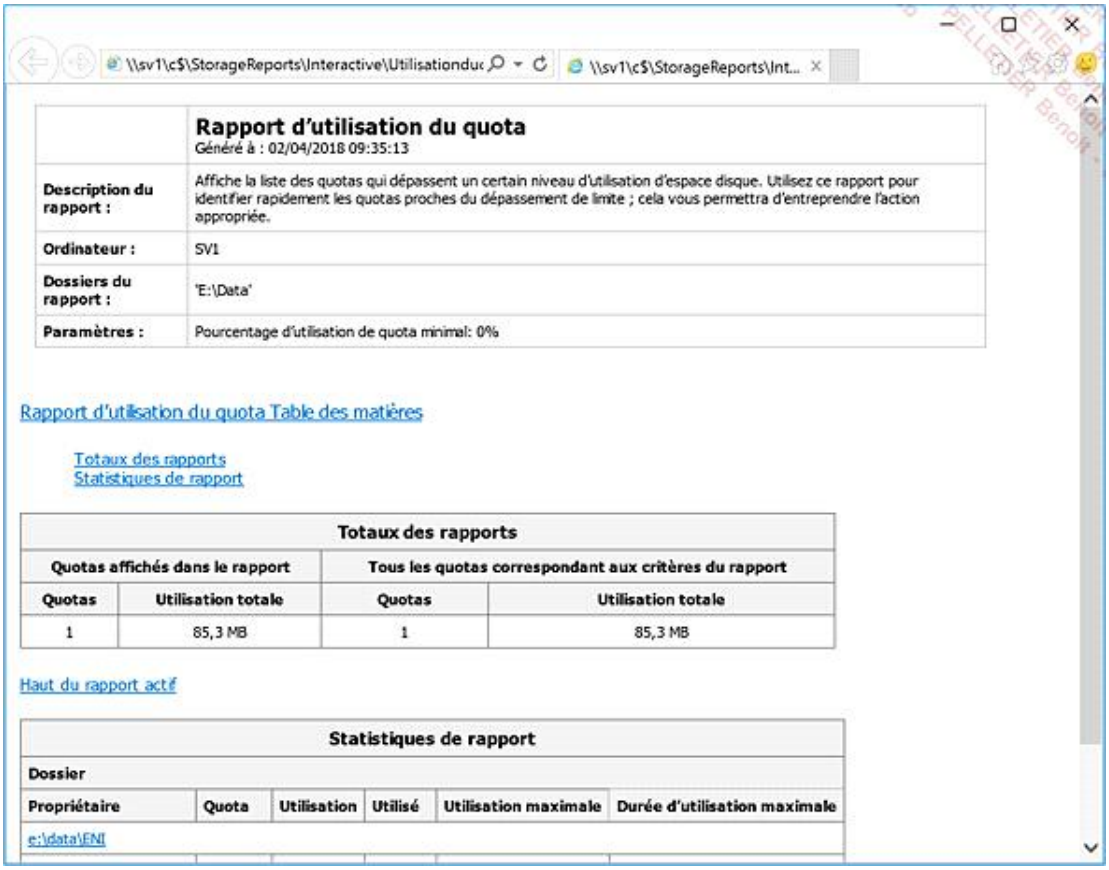
- Cliquez sur l'onglet **Étendue** puis sur le bouton **Ajouter**.
- Sélectionnez le dossier **E:\Data**.



- Cliquez sur **OK**.
- Laissez le choix d'attendre la génération de tous les rapports puis cliquez sur **OK**.
- Ouvrez la page HTML qui vient d'être générée.



Le rapport présente l'utilisation des quotas sur le dossier **Data**.



\\sv1\c$\StorageReports\Interactive\Utilisationduc

\\sv1\c$\StorageReports\Int...

Rapport d'utilisation du quota
Généré à : 02/04/2018 09:35:13

Description du rapport :	Affiche la liste des quotas qui dépassent un certain niveau d'utilisation d'espace disque. Utilisez ce rapport pour identifier rapidement les quotas proches du dépassement de limite ; cela vous permettra d'entreprendre l'action appropriée.
Ordinateur :	SV1
Dossiers du rapport :	'E:\Data'
Paramètres :	Pourcentage d'utilisation de quota minimal: 0%

Rapport d'utilisation du quota Table des matières

Totaux des rapports
Statistiques de rapport

Totaux des rapports

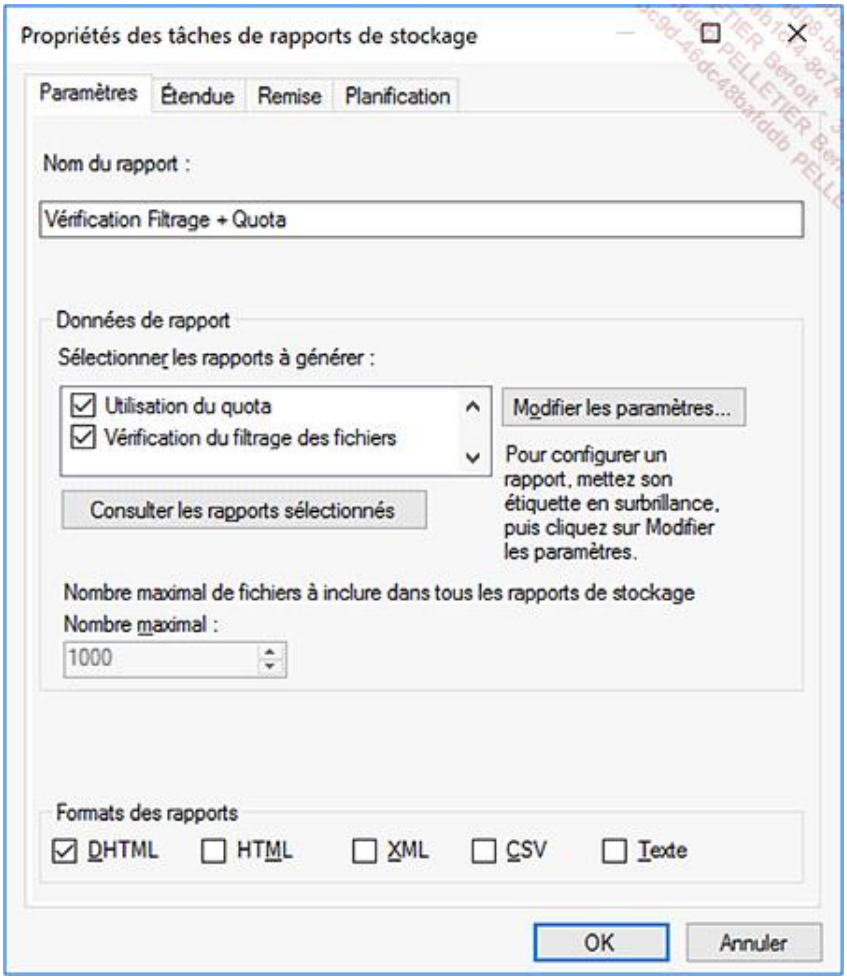
Quotas affichés dans le rapport		Tous les quotas correspondant aux critères du rapport	
Quotas	**Utilisation totale**	**Quotas**	**Utilisation totale**
1	85,3 MB	1	85,3 MB

Haut du rapport actif

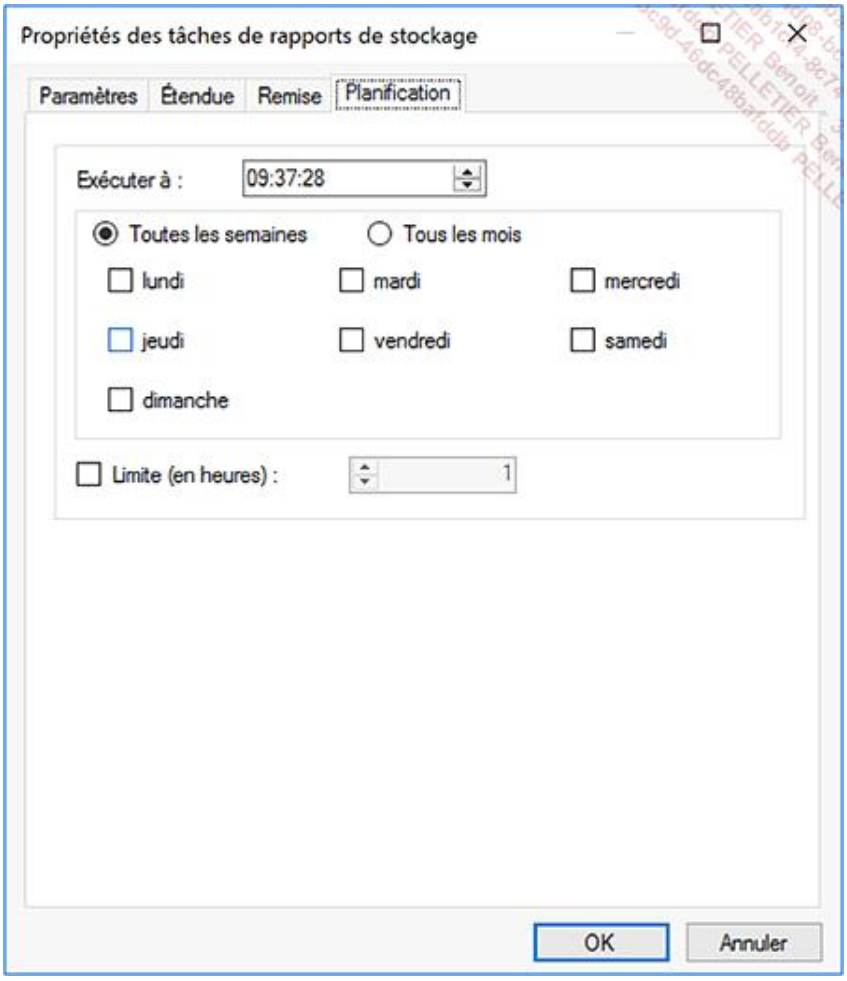
Statistiques de rapport

Dossier					
Propriétaire	**Quota**	**Utilisation**	**Utilisé**	**Utilisation maximale**	**Durée d'utilisation maximale**
e:\data\ENI					

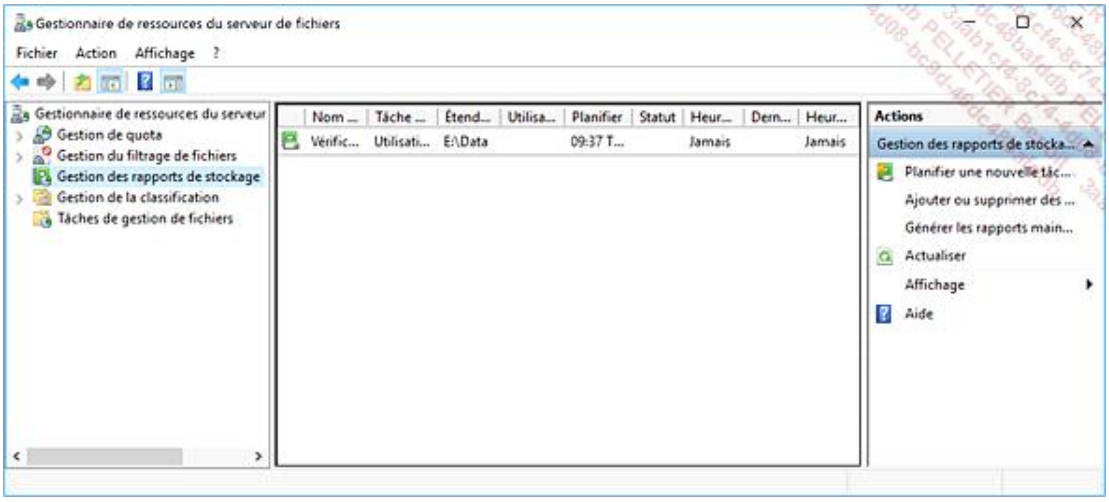
- Effectuez un clic droit sur **Gestion des rapports de stockage** puis cliquez sur **Planifier une nouvelle tâche de rapport**.
- Dans **Nom du rapport**, saisissez **Vérification Filtrage + Quota** puis cochez seulement les rapports **Utilisation du quota** et **Vérification du filtrage des fichiers**.



- Cliquez sur l'onglet **Étendue** puis sur le bouton **Ajouter**.
- Sélectionnez le dossier **E:\Data**.
- Cliquez sur l'onglet **Planification**, cochez le jour souhaité et saisissez l'heure d'exécution.



La planification apparaît dans la console.



Le rapport sera créé dans **C:\StorageReports\Scheduled** à l'heure d'exécution définie.

Les rapports permettent d'obtenir très rapidement des informations très complètes sur un serveur de fichiers. L'administration du serveur de fichiers en est simplifiée.

5. Migration d'un serveur de fichiers à l'aide de PowerShell

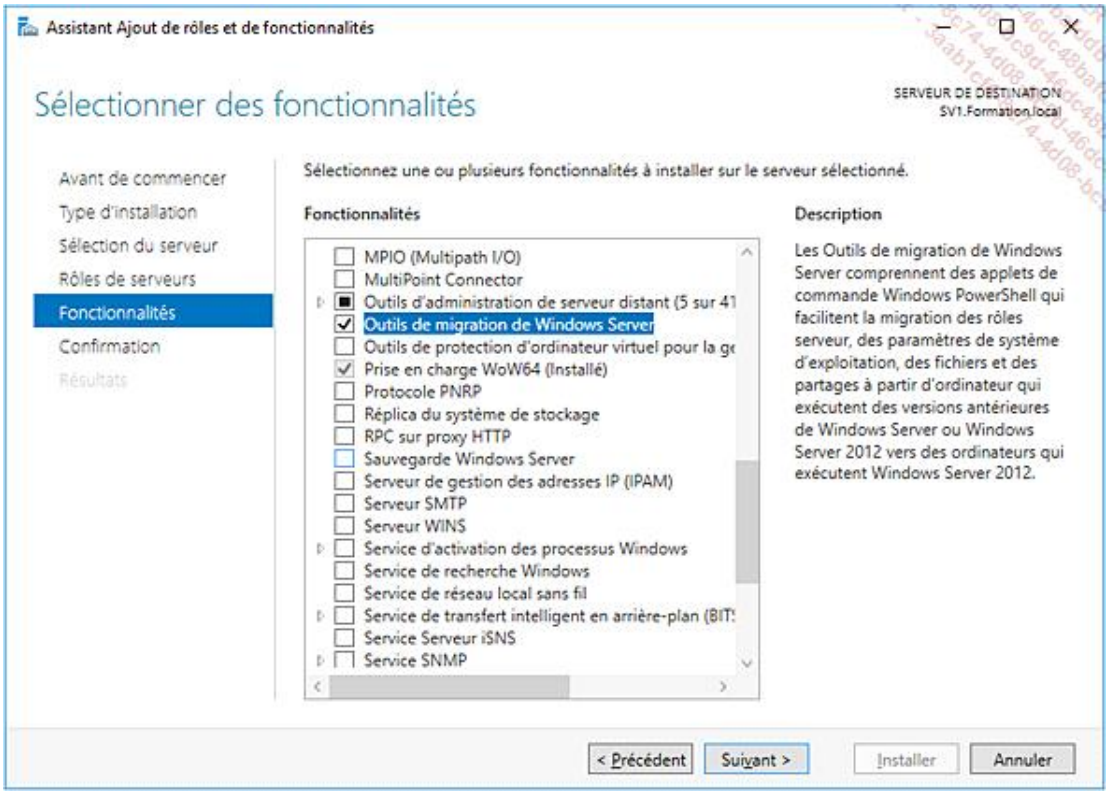
Comme nous l'avons vu dans le chapitre traitant du DHCP, les outils de migration permettent d'effectuer une migration. Dans le cas ci-après, le service de fichier est concerné. Avec Windows Server 2016, les serveurs exécutant Windows Server 2003 ne sont plus pris en charge.

De plus, les outils de migration ne peuvent pas être utilisés si les serveurs source et destination fonctionnent dans des langues différentes (FR et US par exemple). La migration depuis des systèmes 32 bits vers des systèmes 64 bits est supportée.

Deux cmdlets PowerShell vont être utilisées, **Send-SmigServerData** et **Receive-SmigServerData**. Ces dernières vont utiliser le port UDP 7000, pour l'établissement de la connexion ainsi que le transfert des données. Il est donc nécessaire de s'assurer que ce port n'est pas utilisé par une autre application. De plus en cas de présence d'un pare-feu, l'ouverture du port doit être effectuée. Ces opérations sont à réaliser sur les serveurs source et destination.

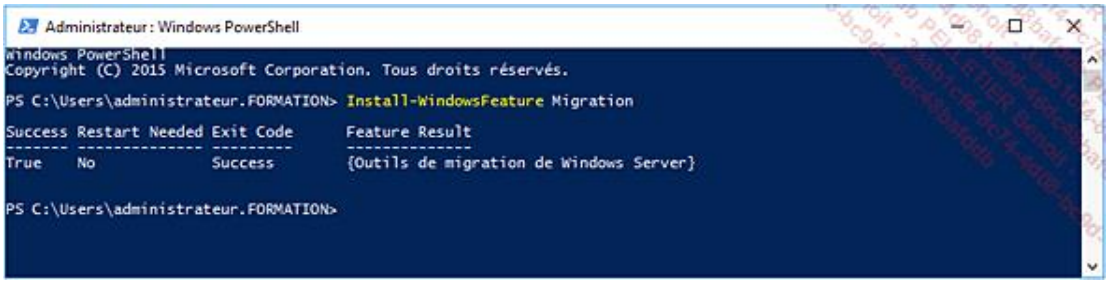
Dès lors, le rôle **Outils de migration Windows Server** peut être installé sur le serveur de destination.

L'ajout de la fonctionnalité s'opère par l'intermédiaire de la console **Gestionnaire de serveur** ainsi que l'assistant d'installation des rôles et fonctionnalités.



PowerShell peut également être utilisé, pour cela exécutez la commande suivante :

```
Install-WindowsFeature Migration
```

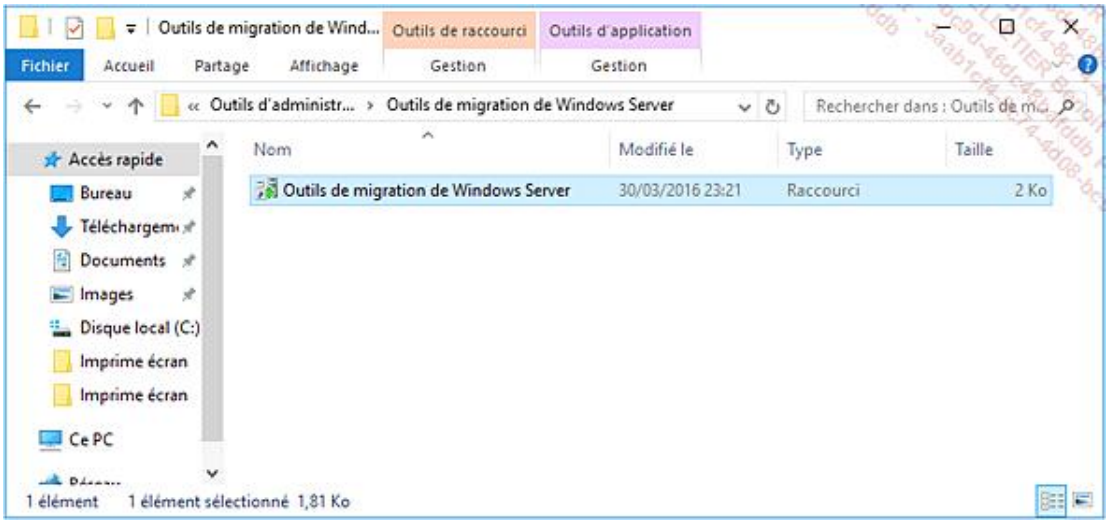


Création du dossier de déploiement

La migration du serveur source peut maintenant être préparée. Ce dernier exécute Windows Server 2012 R2 et les différentes opérations vont être effectuées en ligne de commande.

La migration peut avoir lieu uniquement si les outils sont de la même version sur la source et la destination.

- Dans le menu **Démarrer** sur le serveur de destination, accédez au dossier **Outils d'administration** puis à **Outils de migration de Windows Server**. Cliquez sur **Outils de migration de Windows Server** afin de lancer la console.



- Accédez au répertoire **ServerMigrationTools** présent dans le dossier System32. La commande ci-dessous peut être utilisée pour effectuer cette opération.

```
cd ServerMigrationTools
```



Créez un dossier qui contiendra les fichiers créés par la commande `smigdeploy`. Le répertoire peut être un partage réseau sur le serveur source, un répertoire sur le serveur de destination, etc.

Si le serveur source exécute Windows Server 2012 R2, la commande suivante doit être utilisée :

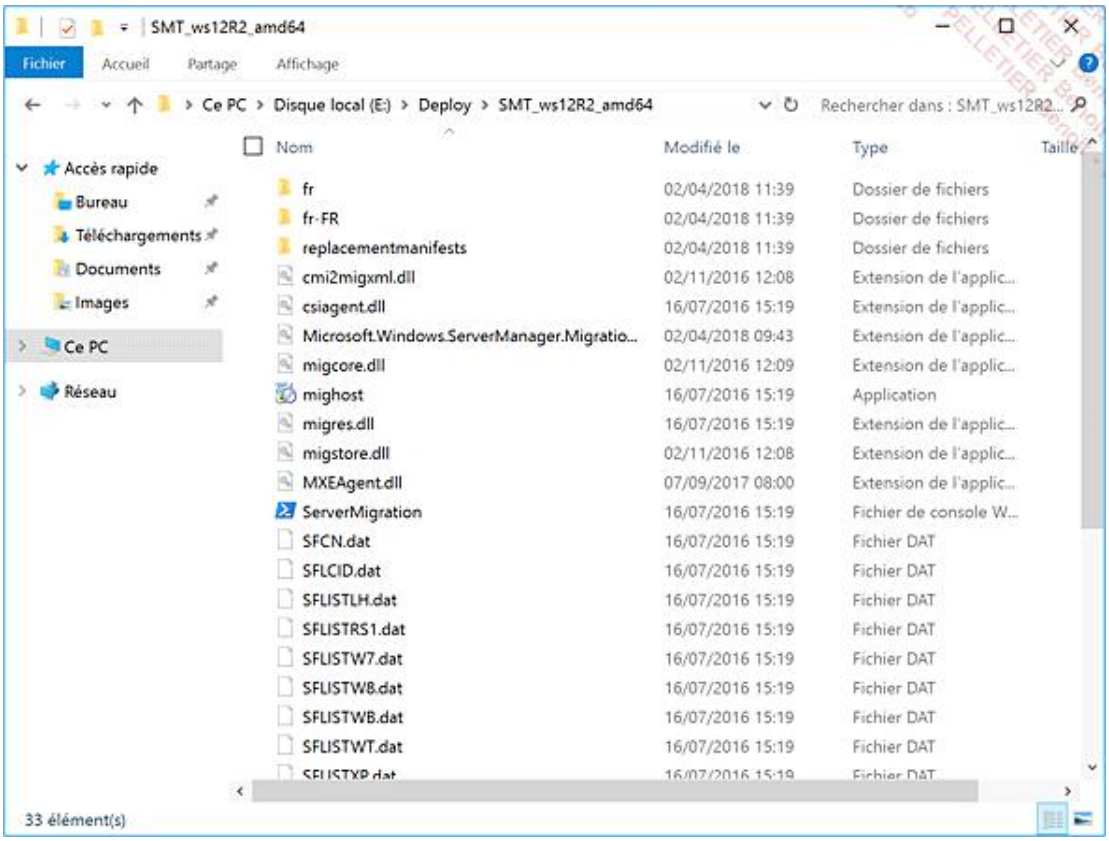
```
.\SmigDeploy.exe /package /architecture amd64 /os WS12R2 /path
<deployment folder path>
```

Le commutateur `/os` doit avoir au minimum la valeur WS08 pour fonctionner. En fonction du système d'exploitation source, les commutateurs `/architecture` et `/os` devront être modifiés. La valeur amd64 correspond à une architecture 64 bits et non au processeur.

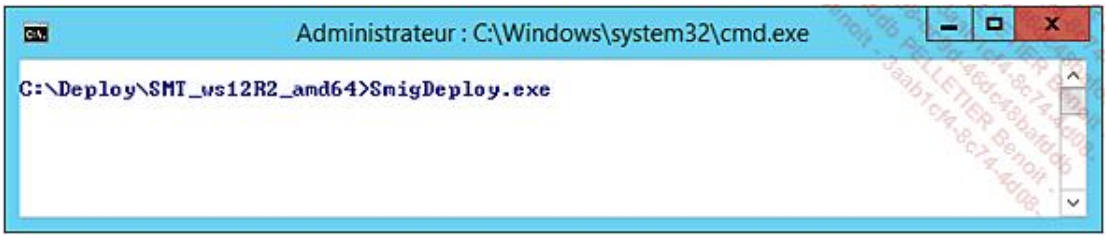


Sur le serveur Windows Server 2012 R2, il est désormais nécessaire d'inscrire le logiciel enfichable Outils de migration. Cette opération est réalisée à l'aide de PowerShell.

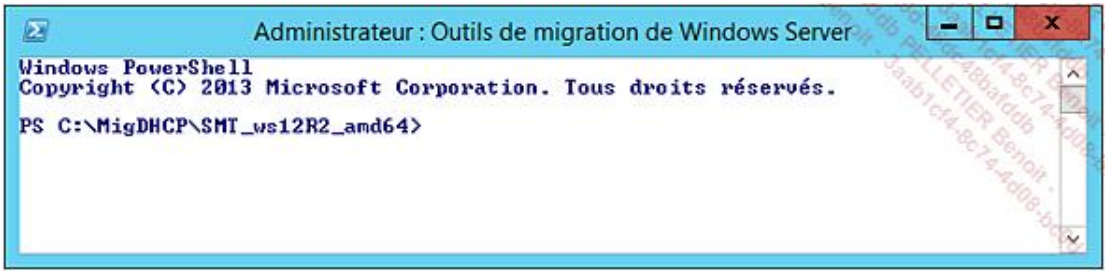
Le dossier créé dans deploy doit pour cela être copié sur le serveur source.



Exécutez une invite de commandes DOS sur le serveur source puis accédez au répertoire précédemment copié. Exécutez la commande `smigdeploy.exe` pour procéder à l'inscription du logiciel enfichable.



Dans les outils d'administration, lancez les outils de migration précédemment installés. Une fenêtre PowerShell apparaît. Cette dernière permettra l'exécution de la cmdlet nécessaire à la migration.



La migration peut dès lors être lancée.

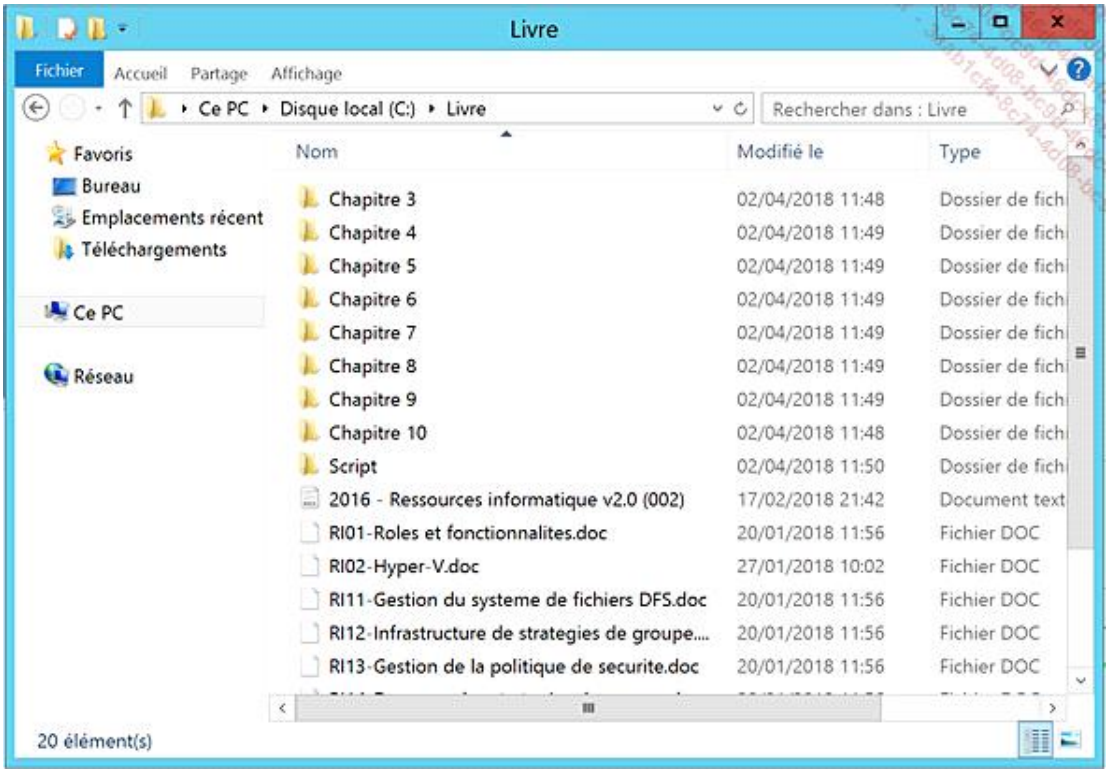
Migration des fichiers et dossiers

Les applets de commande **Send-SmigServerData** et **Receive-SmigData** doivent être exécutées dans un délai de 5 minutes. En effet les cmdlets expirent si une connexion n'a pas été établie dans un délai de 300 secondes.

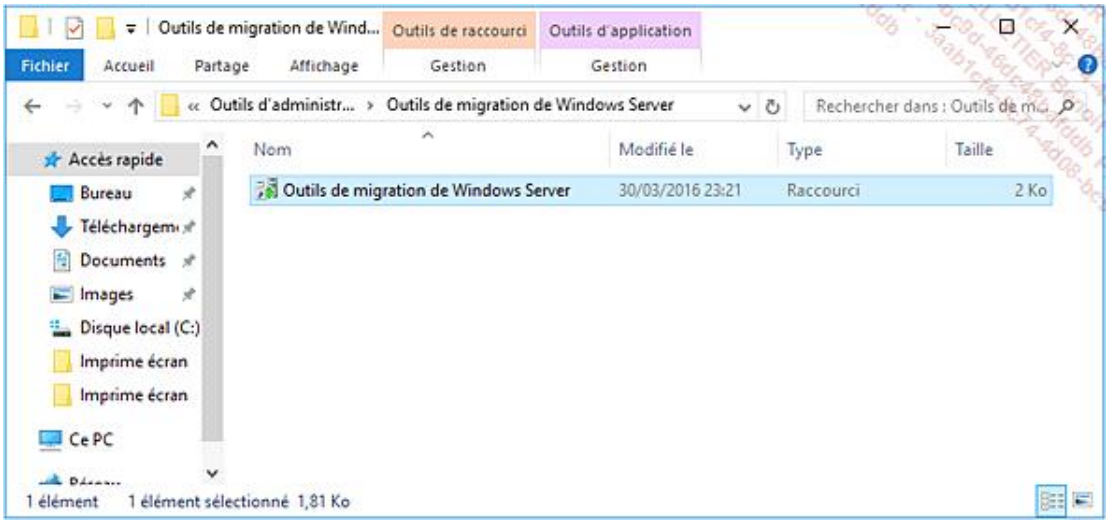
Cette valeur est stockée dans la base de registre et peut être modifiée.

- **Sous-clé** : HKEY_LOCAL_MACHINE\Software\Microsoft\ServerMigration
- **Valeur** : MaxConnectionTime (REG_DWORD)
- **Données** : Entre 1 et 3600 (valeur en seconde)

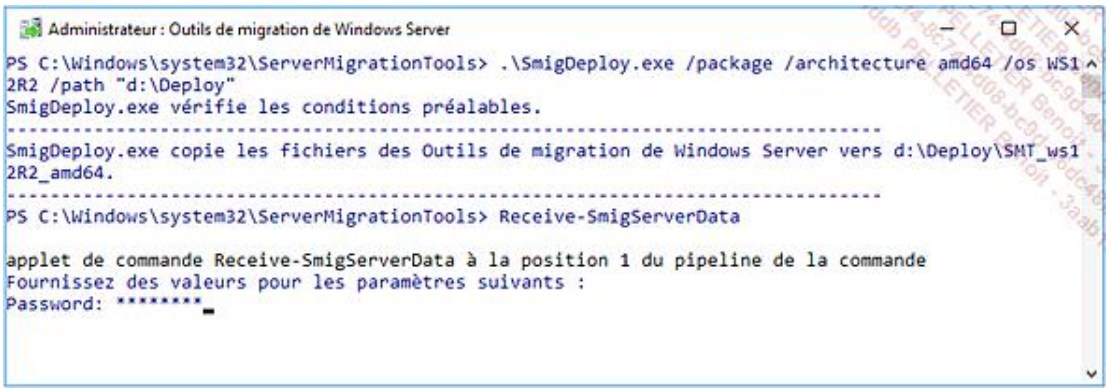
Le dossier est bien présent à la racine C: du serveur source sous Windows Server 2012 R2.



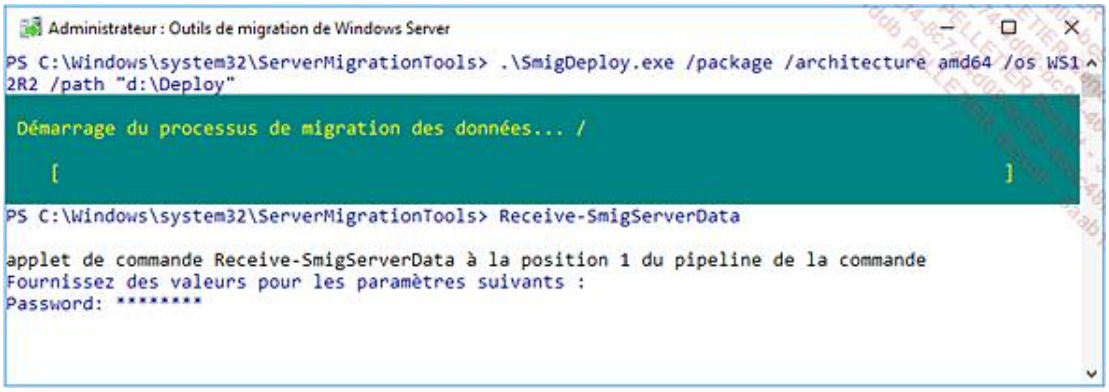
- Dans le menu **Démarrer** sur le serveur de destination, accédez au dossier **Outils d'administration**. Cliquez sur **Outils de migration de Windows Server** afin de lancer la console.



- Exécutez la commande `Receive-SmigServerData` puis indiquez le mot de passe à utiliser.



Le serveur est maintenant en attente du serveur source.



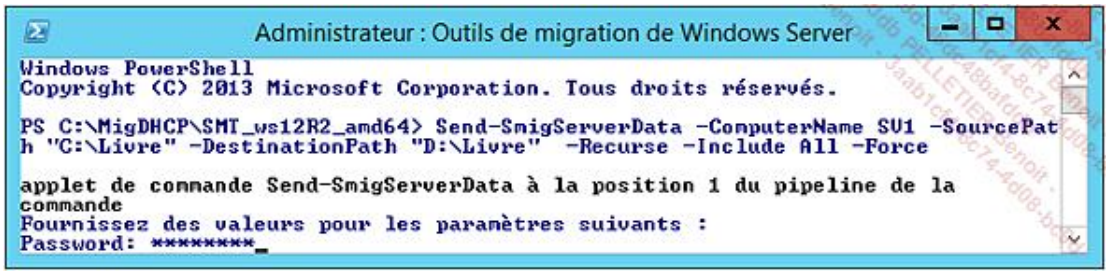
La commande ci-dessous doit être lancée dans délai de 5 minutes sans quoi il est nécessaire d'exécuter une nouvelle fois la commande sur la cible.

Sur le serveur source, lancez également la console Windows Server Migration Tools puis saisissez la commande :

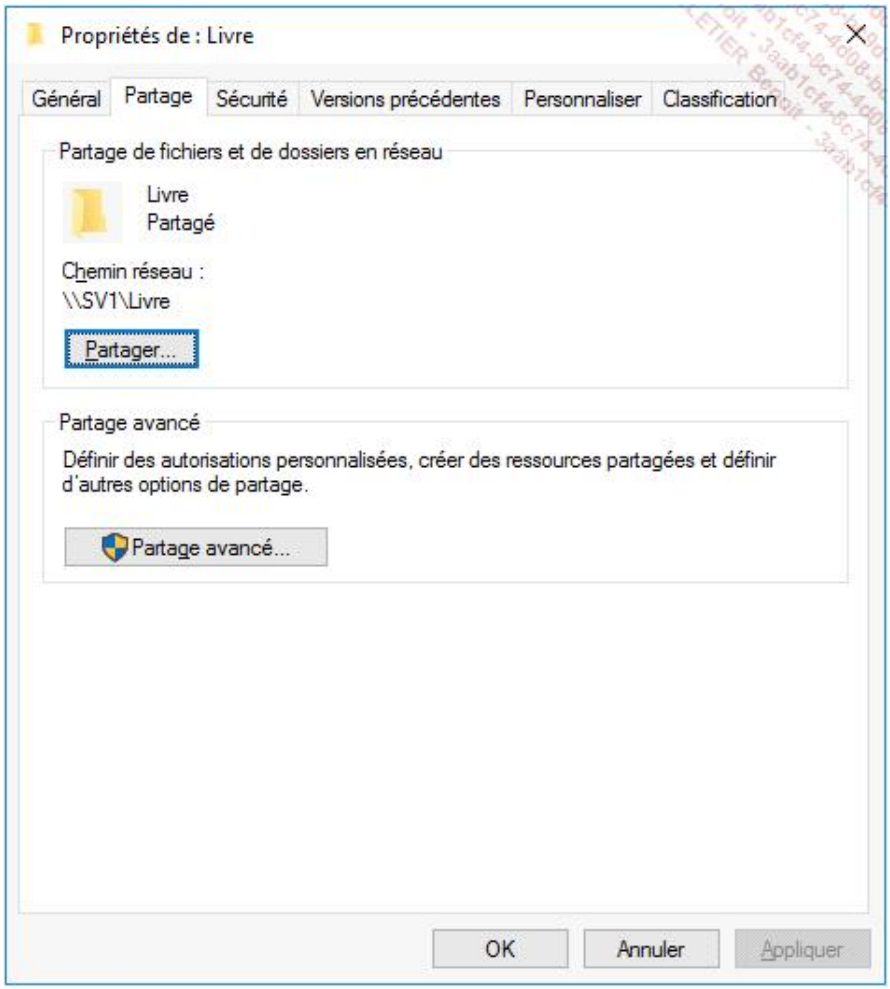
```
Send-SmigServerData -ComputerName <DestinationServer>
-SourcePath "C:\Livre" -DestinationPath
"C:\Livre"  -Recurse -Include All -Force
```

- `-ComputerName <DestinationServer>` : indique le nom du serveur de destination.
- `-SourcePath "C:\Livre"` : indique le chemin du répertoire source
- `-DestinationPath "C:\Livre"` : indique le chemin du répertoire destination

Les chemins source et destination peuvent être différents.



Les données sont envoyées vers le serveur de destination.



Les permissions présentes dans l'onglet **Sécurité** sont également migrées. De plus si le répertoire était partagé sur la source, il est également partagé sur la destination.

Vue d’ensemble du système de fichiers DFS

Un système de fichiers distribués (DFS) permet d’avoir une tolérance de panne aux niveaux des serveurs fichiers situés dans différentes zones géographiques ou sur un même réseau local.

1. Technologie de systèmes de fichiers DFS

Les technologies de systèmes DFS incluent un espace de noms qui permet un affichage des dossiers partagés situés sur différents serveurs. L’utilisateur n’a plus besoin de connaître le nom du serveur pour accéder à la ressource. La réplication DFS permet d’assurer la tolérance de panne et donc une meilleure disponibilité des données. Il est ainsi aisé d’effectuer la réplication des fichiers et dossiers sur un autre serveur de l’espace de noms. La compression différentielle à distance est utilisée pour effectuer l’identification d’éventuelles modifications opérées dans des fichiers. Seules ces modifications seront répliquées, ceci dans le but d’économiser la bande passante.

2. Fonctionnement des espaces de noms DFS

Lors de l’accès à un dossier de l’espace de noms par un utilisateur, son poste de travail contacte le serveur d’espaces de noms. Ce dernier lui retourne une liste des serveurs (référence) présents dans l’espace de noms et qui hébergent les dossiers partagés (appelés cibles de dossier).

Le poste client met en cache cette référence, puis tente de contacter le premier serveur. Il va par défaut favoriser le serveur présent dans son site AD.

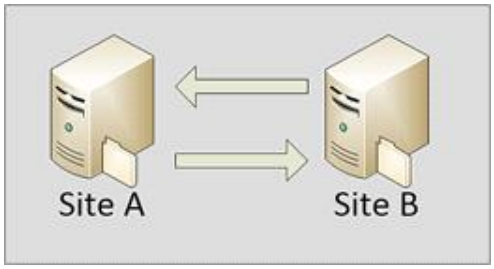
Le serveur qui héberge la ressource (le dossier partagé) n’est pas visible par l’utilisateur. En effet, ce dernier voit uniquement un ou plusieurs dossiers.

Si un des serveurs devient indisponible (arrêt du serveur, panne…), un autre serveur présent dans la référence sera contacté.

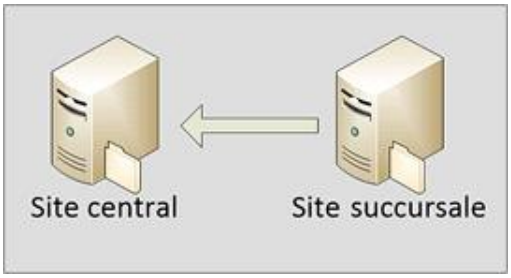
3. Scénarios mettant en jeu le système de fichiers DFS

La solution DFS permet la mise en place de plusieurs scénarios.

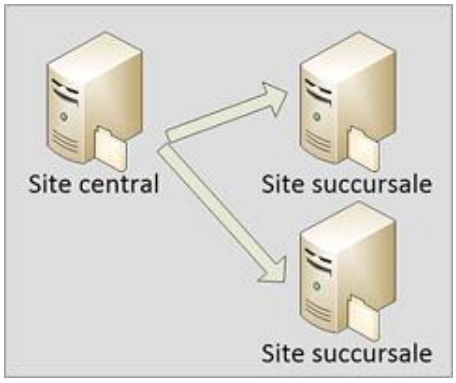
Le partage de fichiers entre deux serveurs géographiquement distants ou présents dans le même réseau local (bidirectionnel).



La collecte de données permet, quant à elle, de répliquer des données d’un site distant vers un site central. Ainsi la sauvegarde des données du ou des sites annexes sera effectué plus facilement.



À l'inverse de la collecte de données, la distribution de données permet une réplication vers des serveurs de succursales. Après avoir effectué une modification sur un site, la réplication est effectuée vers les serveurs des autres sites.



La réplication DFSR peut être utilisée sans la présence d'espaces de noms, de plus elle offre l'avantage de pouvoir gérer le débit utilisé pour la réplication.

L’espace de noms

1. Types d’espaces de noms DFS

Il est nécessaire de choisir entre deux types d’espaces de noms DFS : basé sur un domaine AD ou autonome.

Lorsqu’un serveur DFS est basé sur Active Directory, le chemin d’accès contient le nom de domaine AD puis le nom de l’espace de noms (**\\formation\Public**). Les données de configuration sont stockées dans l’annuaire Active Directory. Il est ainsi possible d’avoir jusqu’à plusieurs milliers de dossiers avec des cibles. La disponibilité des données est assurée en ajoutant plusieurs serveurs dans l’espace de noms.

Le mode autonome, lui, nécessite un cluster afin d’assurer la haute disponibilité. Les données de configuration sont cette fois stockées dans le registre de serveur. Pour finir, le chemin d’accès est sensiblement différent puisqu’il est composé du nom du serveur et du nom de l’espace de noms (**\\SRV1\Public**).

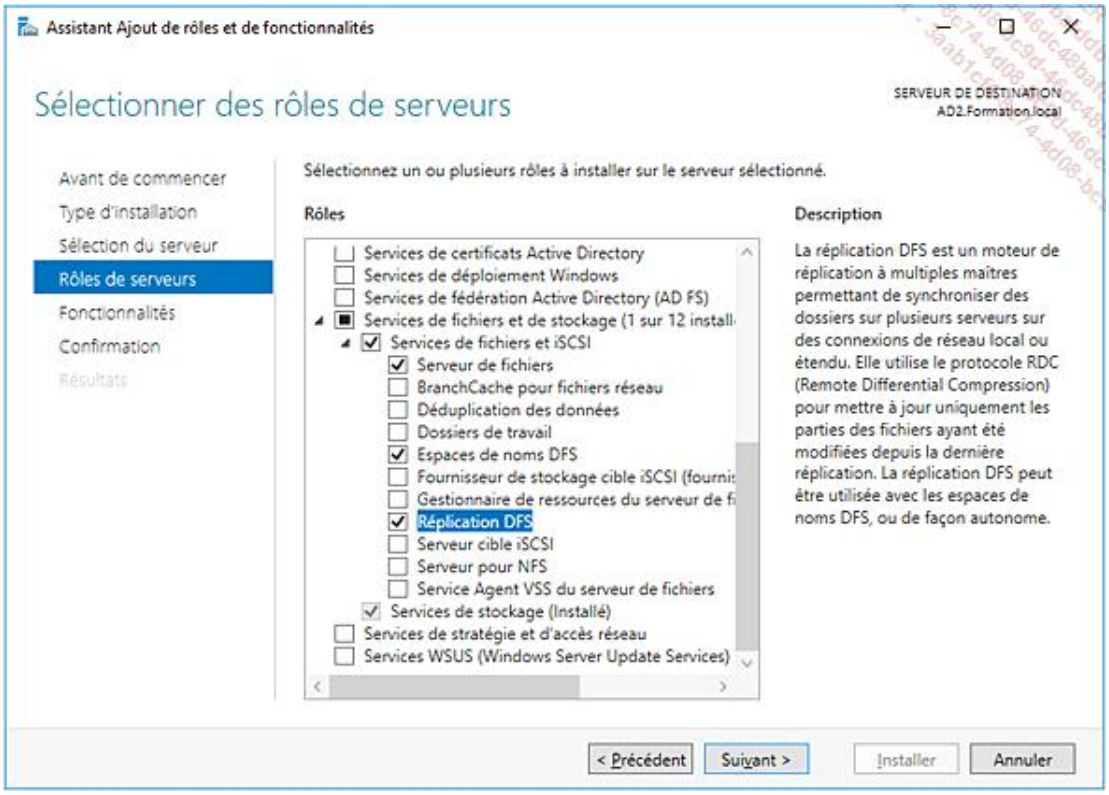
La disponibilité dans DFS est assurée en spécifiant des cibles de dossiers supplémentaires. Ceci implique d’effectuer la réplication à l’aide de DFSR.

2. Installation de l’espace de noms

- Si ce n’est pas déjà fait, démarrez la machine virtuelle AD2.

  En production, il est préférable de ne pas l’installer sur des contrôleurs de domaine.

- Ouvrez une session en tant qu’administrateur.
- Lancez la console **Gestionnaire de serveur**.
- Cliquez sur **Ajouter des rôles et des fonctionnalités**.
- Dans la fenêtre **Sélectionner le type d’installation**, laissez le choix par défaut puis cliquez sur **Suivant**.
- Cliquez sur **Suivant** dans la fenêtre de sélection du serveur de destination.
- Déroulez les rôles **Services de fichiers et de stockage** puis **Services de fichiers et iSCSI**.
- Cochez **Espaces de noms DFS**, puis cliquez sur **Ajouter des fonctionnalités** dans la fenêtre qui s’affiche.
- Cochez également **Réplication DFS**.

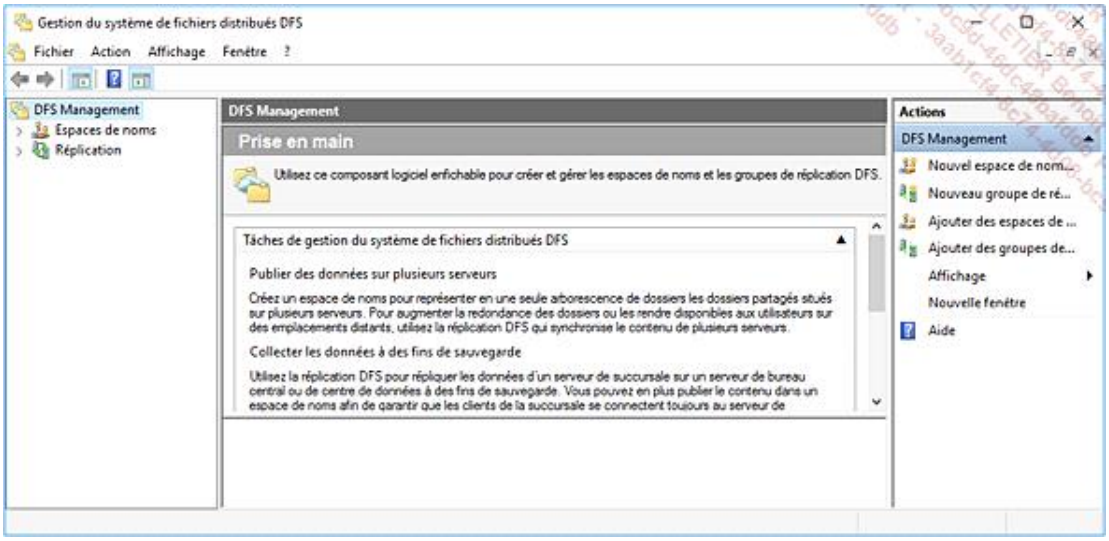


- Validez en cliquant sur **Suivant**.
- Cliquez sur **Suivant** dans la fenêtre **Confirmer les sélections d'installation**, puis sur **Installer**.
- Cliquez sur **Fermer** à la fin de l'installation puis effectuez la même opération sur le serveur SV1.

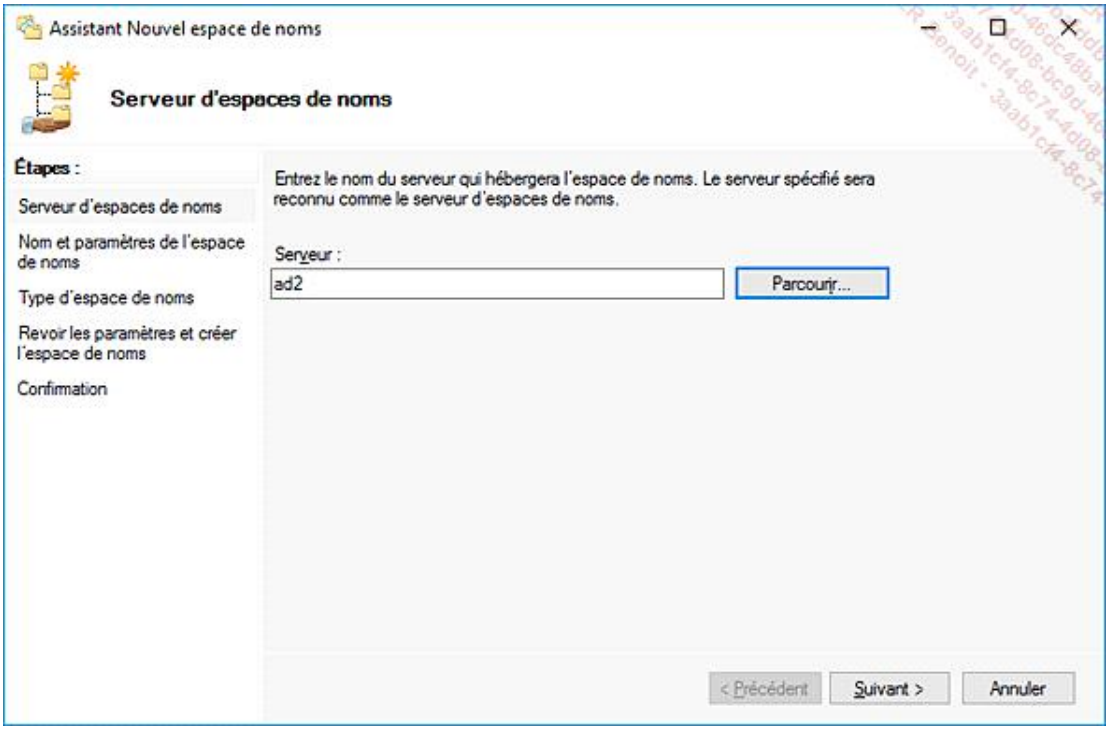
3. Configuration de l'espace de noms

L'installation est maintenant terminée et il est nécessaire d'effectuer la configuration (choix du type de l'espace de noms, création des cibles de dossier…).

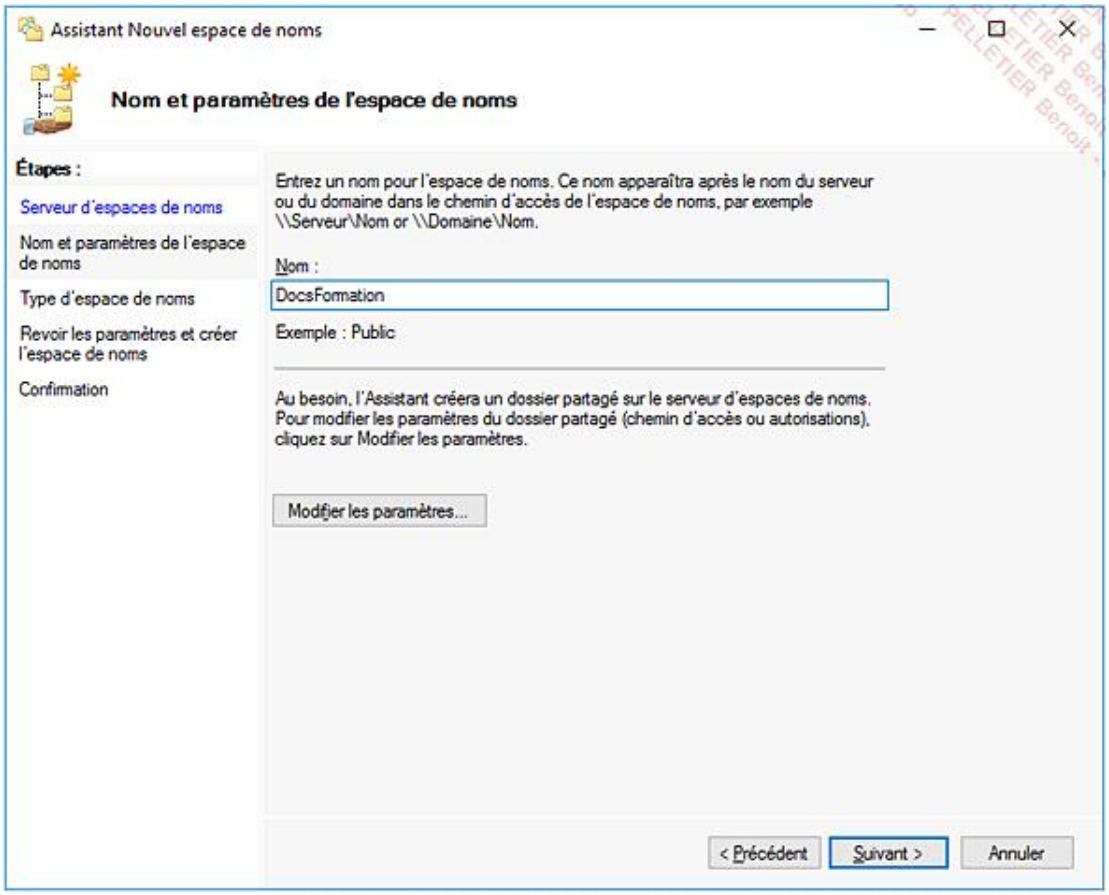
- Sur AD2, double cliquez sur **Gestion du système de fichiers distribués DFS** dans **Outils d'administration Windows**.
- Cliquez sur **Nouvel espace de noms** (bandeau **Actions**) dans la console qui vient de s'ouvrir.



- À l'aide du bouton dans la fenêtre **Serveur d'espaces de noms**, sélectionnez **AD2** puis cliquez sur **Suivant**.



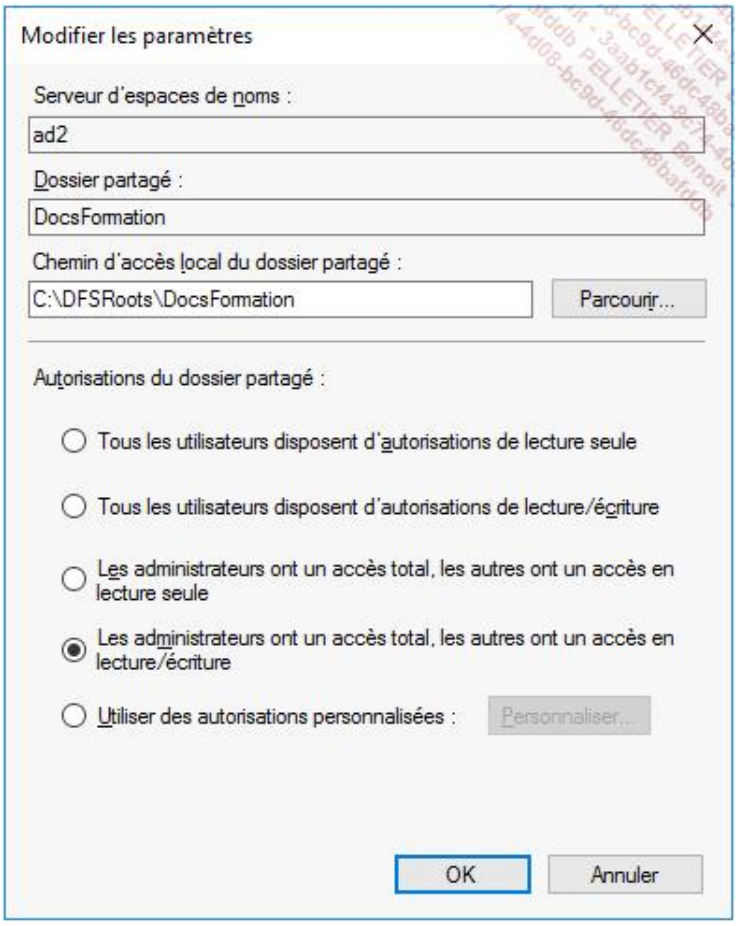
- Dans le champ **Nom** de l'espace de noms, saisissez **DocsFormation**.



- Cliquez sur le bouton **Modifier les paramètres**.

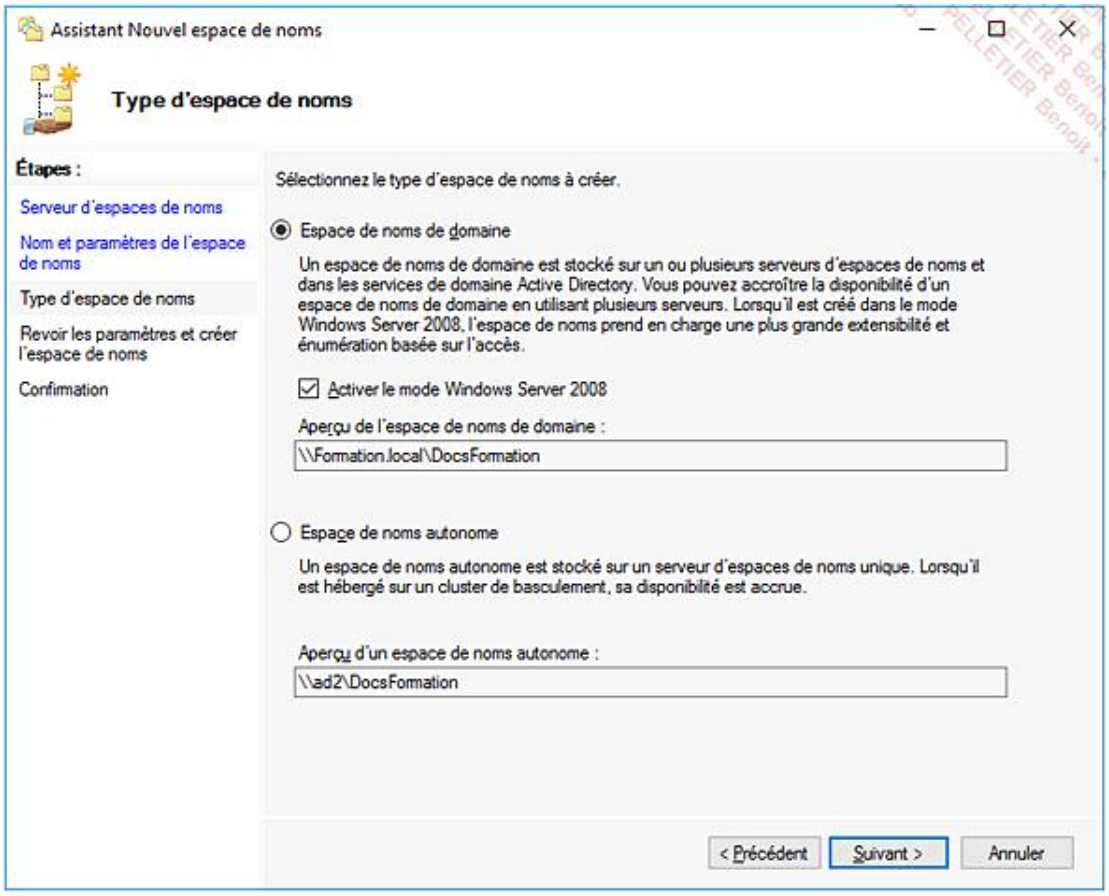
Il est possible à l'aide de ce menu de configurer le chemin d'accès local du dossier partagé mais également ses autorisations.

- Dans la zone **Autorisations du dossier partagé**, cliquez sur le bouton radio donnant aux administrateurs le contrôle total et aux autres un accès en lecture/écriture.



- Dans la fenêtre **Type d'espace de noms**, laissez les paramétrages par défaut et cliquez sur **Suivant**.

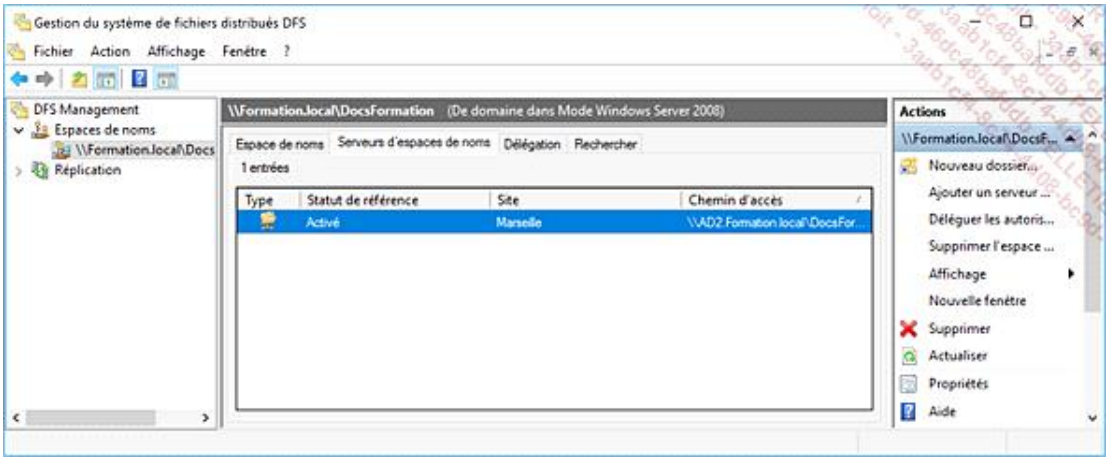
En activant le mode Windows Server 2008, des fonctionnalités supplémentaires comme l'énumération basée sur l'accès sont activées.



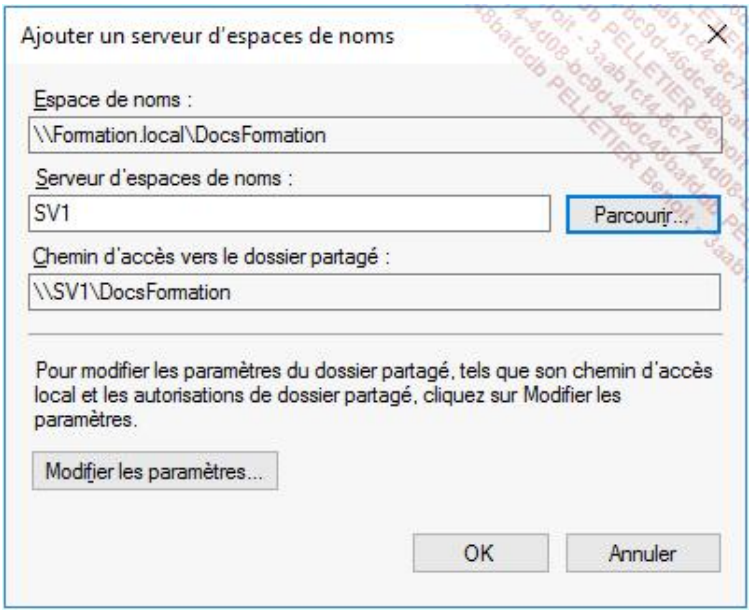
- Cliquez sur **Créer** pour lancer la création.

Si aucune erreur n'est affichée, fermez l'assistant.

- Développez le nœud **Espace de noms** puis l'espace de noms, et cliquez sur l'onglet **Serveurs d'espaces de noms**.

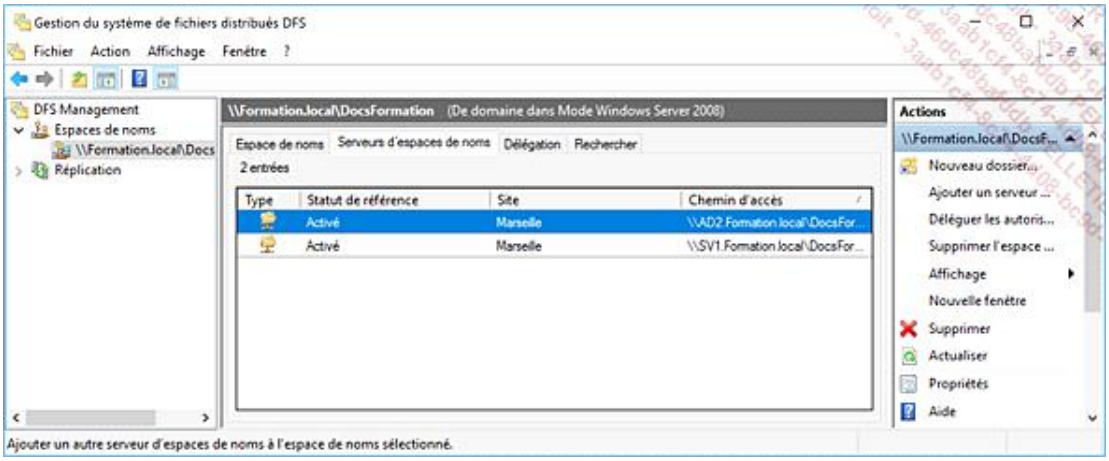


- Dans le bandeau **Actions**, cliquez sur **Ajouter un serveur d'espace de noms**.
- À l'aide du bouton **Parcourir**, sélectionnez le serveur **SV1**.



- Cliquez sur le bouton **Modifier les paramètres**.
- Dans **Autorisations du dossier partagées**, cliquez sur le bouton radio donnant aux administrateurs le contrôle total et aux autres un accès en lecture/écriture puis cliquez deux fois sur **OK**.

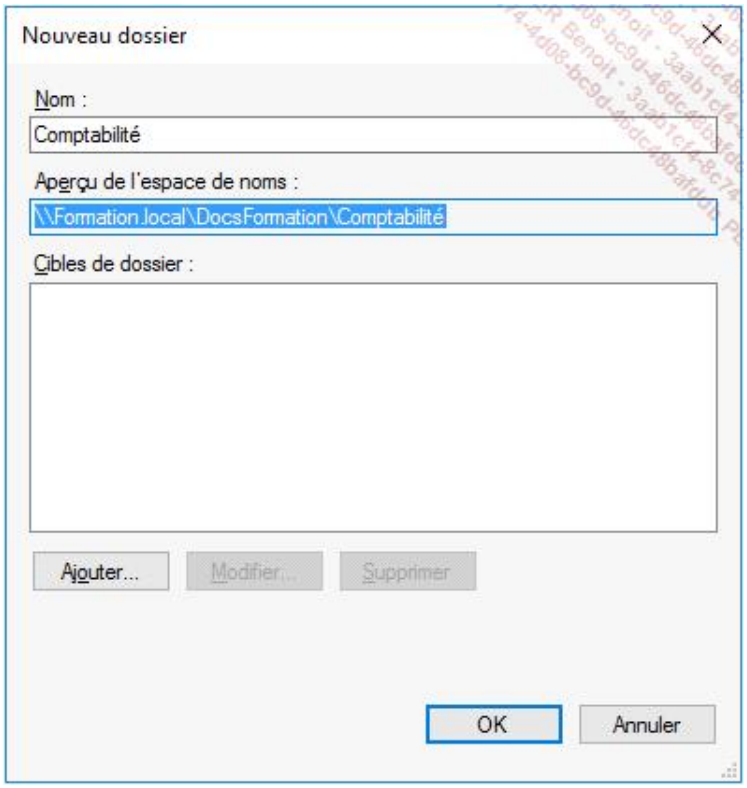
Le serveur est maintenant ajouté à l'espace de noms.



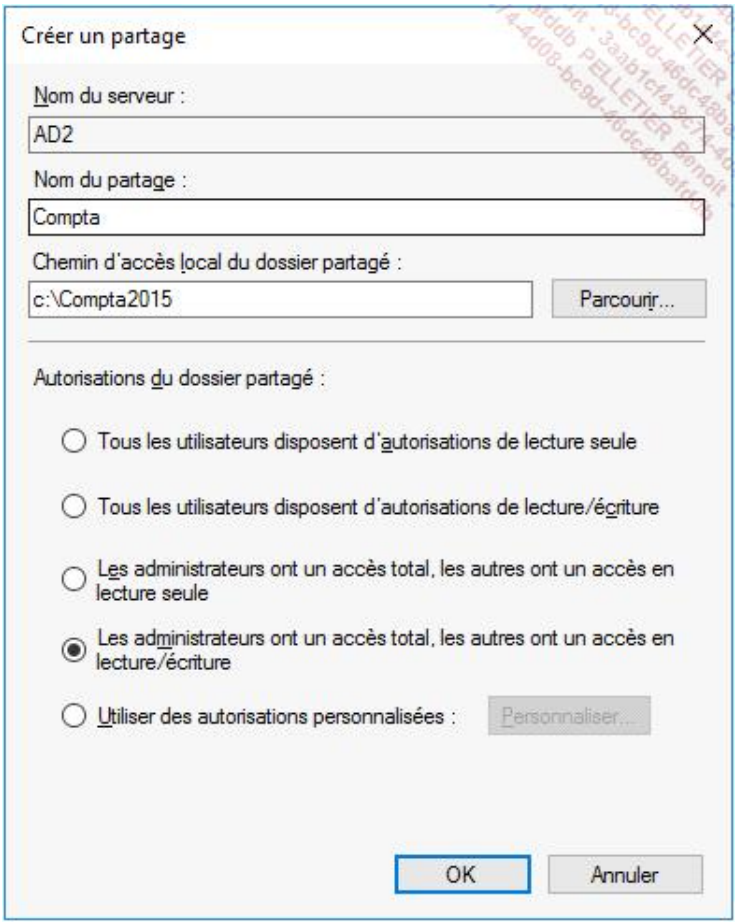
- Cliquez sur l'onglet **Espace de noms** puis sur **Nouveau dossier** dans le bandeau **Actions**.

Un dossier contient les données à stocker et utilisables par un utilisateur. Pour accéder à ce répertoire, des cibles de dossier sont créées. Ces derniers peuvent être présents sur un dossier et pointer sur des serveurs différents.

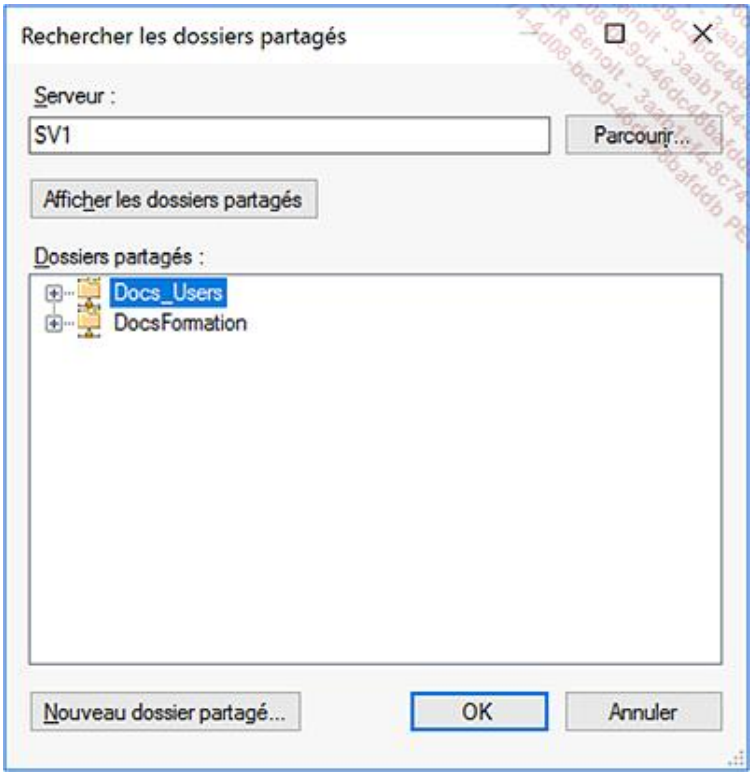
- Saisissez **Comptabilité** dans le champ **Nom** puis cliquez sur **Ajouter**.



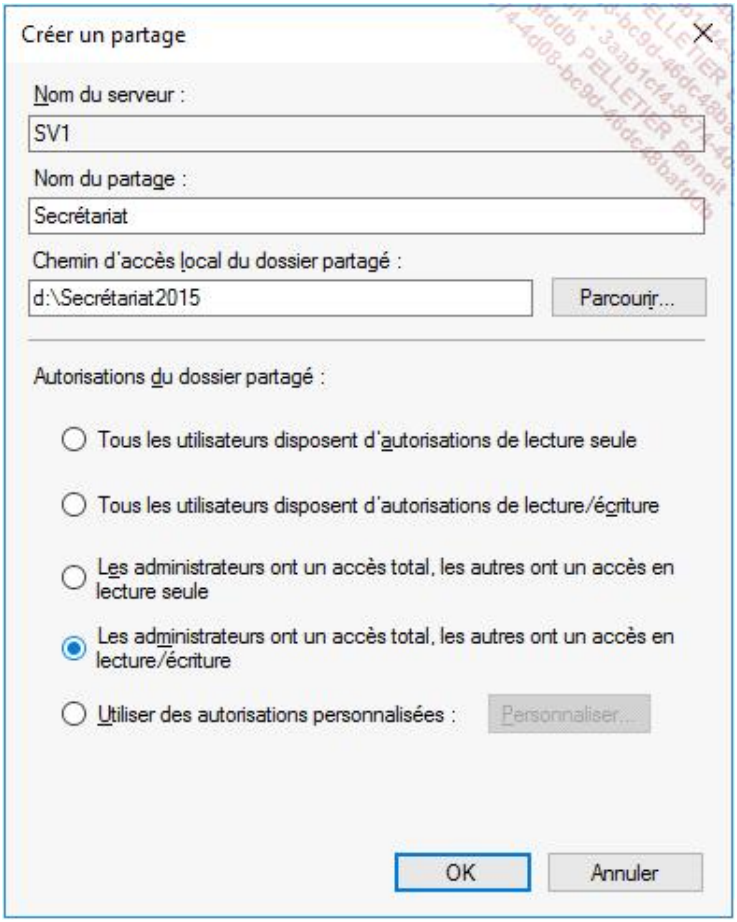
- Dans la fenêtre **Ajouter des cibles de dossier**, cliquez sur **Parcourir**.
- Cliquez sur **Nouveau dossier partagé**.
- Dans **Nom du partage** saisissez **Compta** puis à l'aide du bouton **Parcourir**, créez un dossier partagé sur **C** portant le nom **Compta2015**.
- Cochez le bouton radio **Les administrateurs ont un accès total, les autres ont un accès en lecture/écriture**.



- Cliquez trois fois sur **OK** pour valider toutes les fenêtres.
- Cliquez une nouvelle fois sur **Nouveau dossier**.
- Dans le champ **Nom**, saisissez **Secrétariat** puis cliquez sur **Ajouter**.
- Dans la fenêtre **Ajouter une cible de dossier**, cliquez sur **Parcourir**.
- Saisissez SV1 dans le champ **Serveur** puis cliquez sur **Afficher les dossiers partagés**.



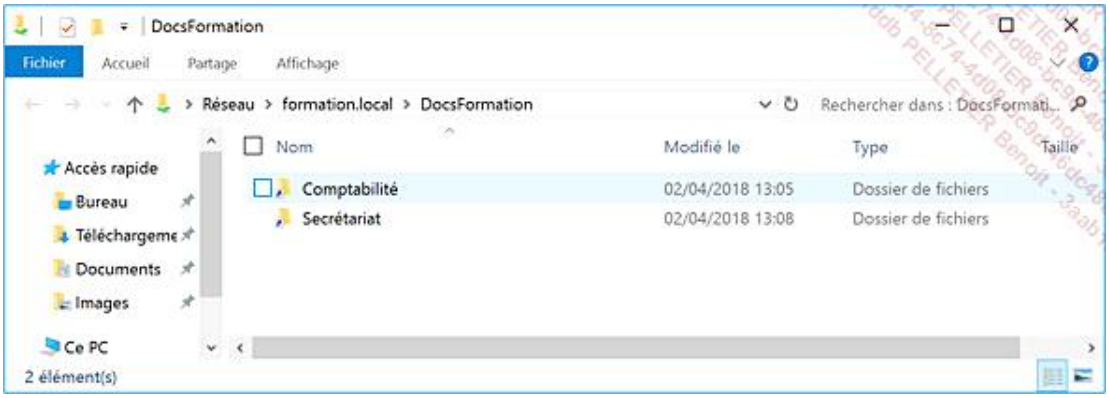
Créez un nouveau dossier nommé **Secrétariat** en suivant la même procédure que précédemment.



Validez les fenêtres en cliquant sur **OK**.

Les deux dossiers apparaissent dans la console. Le chemin **\\formation.local\DocsFormation** permet d'accéder

aux répertoires sans avoir à connaître le serveur sur lequel ils sont hébergés.



Les deux répertoires présents dans l'espace de noms se trouvent sur deux serveurs séparés. Il est utile de mettre la réplication DFS en place afin d'assurer la disponibilité des données.

Rappel des fonctionnalités offertes par Windows Server 2012 R2

Le rôle DFS a eu quelques nouveautés intéressantes avec Windows Server 2012 R2. Notons en premier lieu les cmdlets PowerShell. Comme pour la majorité des rôles, l'administration peut désormais s'effectuer en ligne de commande. Il est donc plus facile d'automatiser certaines tâches. On trouve également le nouveau fournisseur WMI qui permet la gestion de la réplication DFS.

Une fonctionnalité très intéressante est la possibilité de cloner la base de données de la réplication DFS afin de l'importer sur un autre serveur. Ainsi on réduit le temps initial d'installation. Contrairement aux anciennes versions, il est désormais possible de restaurer des fichiers présents dans les dossiers ConflictandDeleted. L'opération s'effectue à l'aide des commandes PowerShell `Get-DfsrPreservedFiles` et `Restore-DfsrPreservedFiles`.

La réplication dans DFS

La réplication DFS est un moteur de réplication multimaître, elle permet d'effectuer la planification de la réplication ainsi que la limitation de la bande passante.

1. Présentation de la réplication

La compression différentielle à distance permet d'effectuer la mise à jour des fichiers sur un réseau. Les modifications apportées à un fichier sont détectées à l'aide du journal USN. Ce dernier permet d'enregistrer tout changement effectué sur un volume NTFS. Ainsi seules ces modifications sont répliquées. Avant d'effectuer la réplication vers le serveur distant, une copie est effectuée dans un dossier intermédiaire.

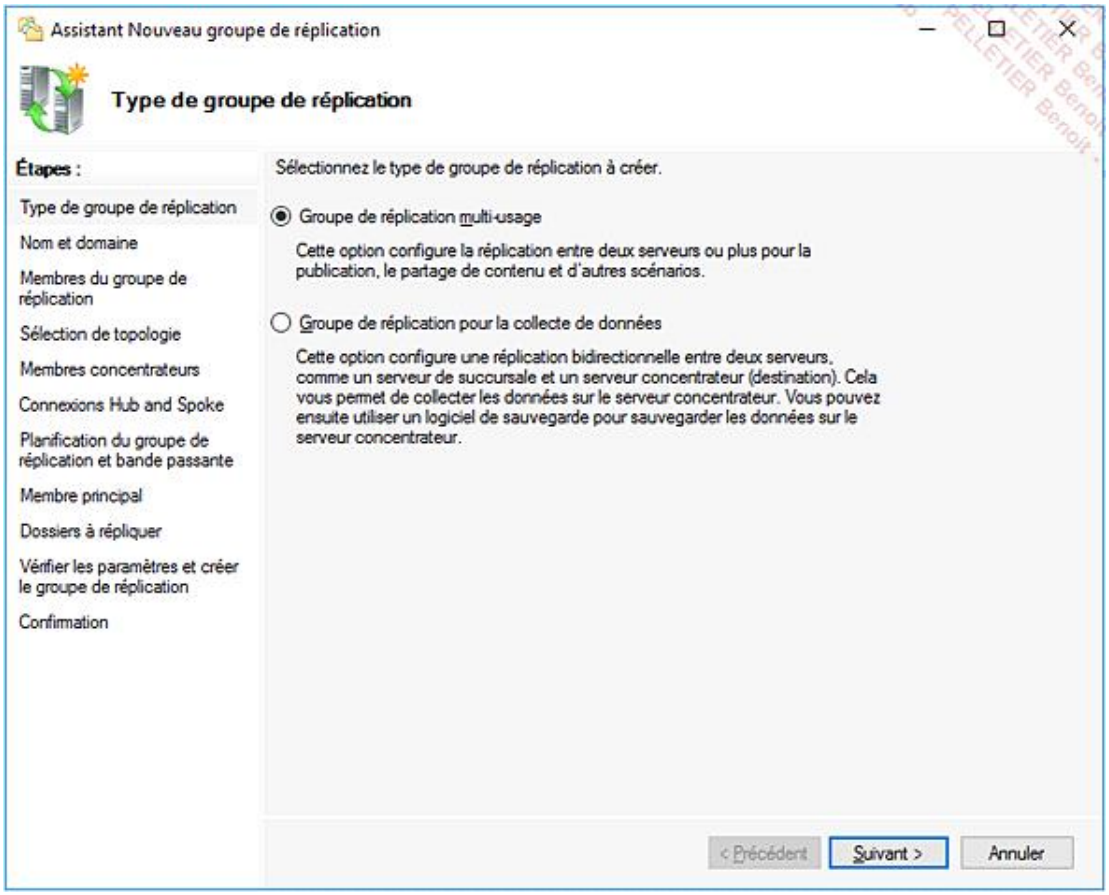
2. Groupe de réplication

Un groupe de réplication contient des serveurs connus comme membres, ces derniers participant à la réplication d'un ou plusieurs répertoires. Il est possible de les configurer pour un mode multi-usage ou pour la collecte de données.

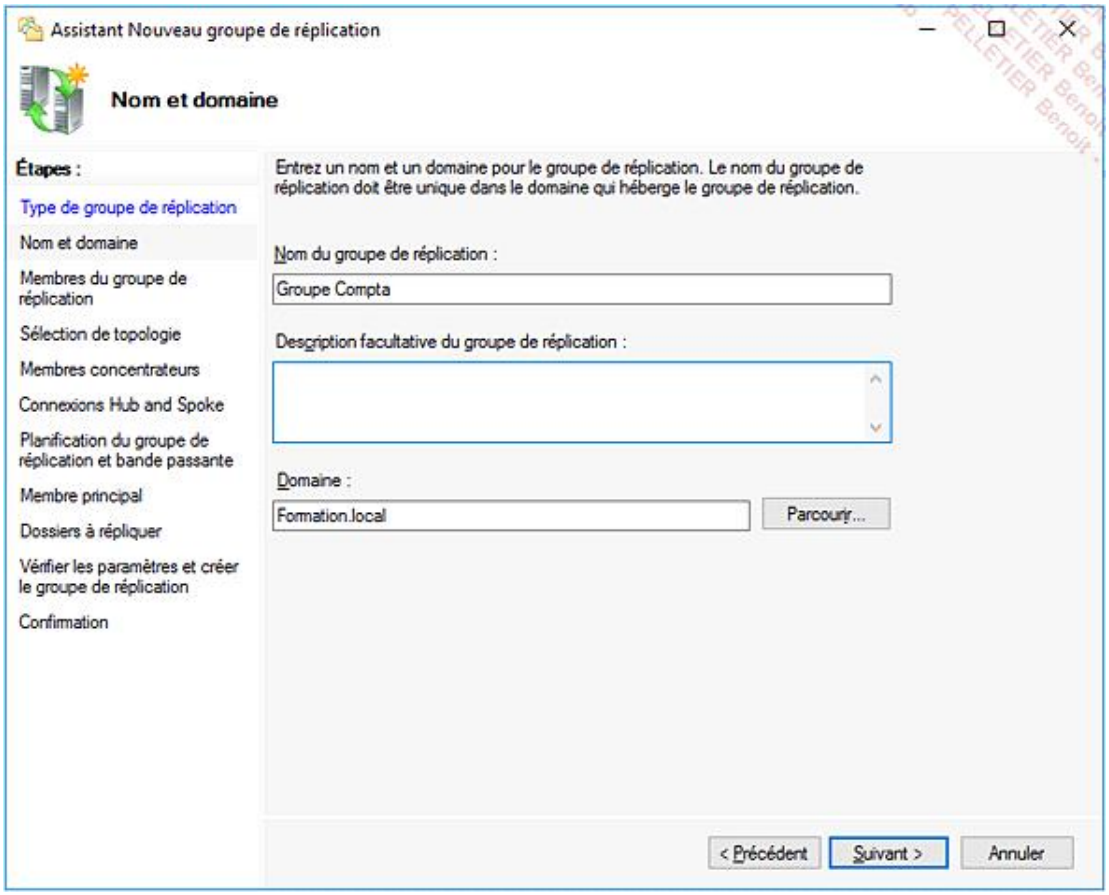
Tous les serveurs présents dans un groupe doivent être membres de la même forêt Active Directory, de plus les dossiers répliqués doivent être stockés sur des volumes NTFS.

3. Mise en place de la réplication DFS

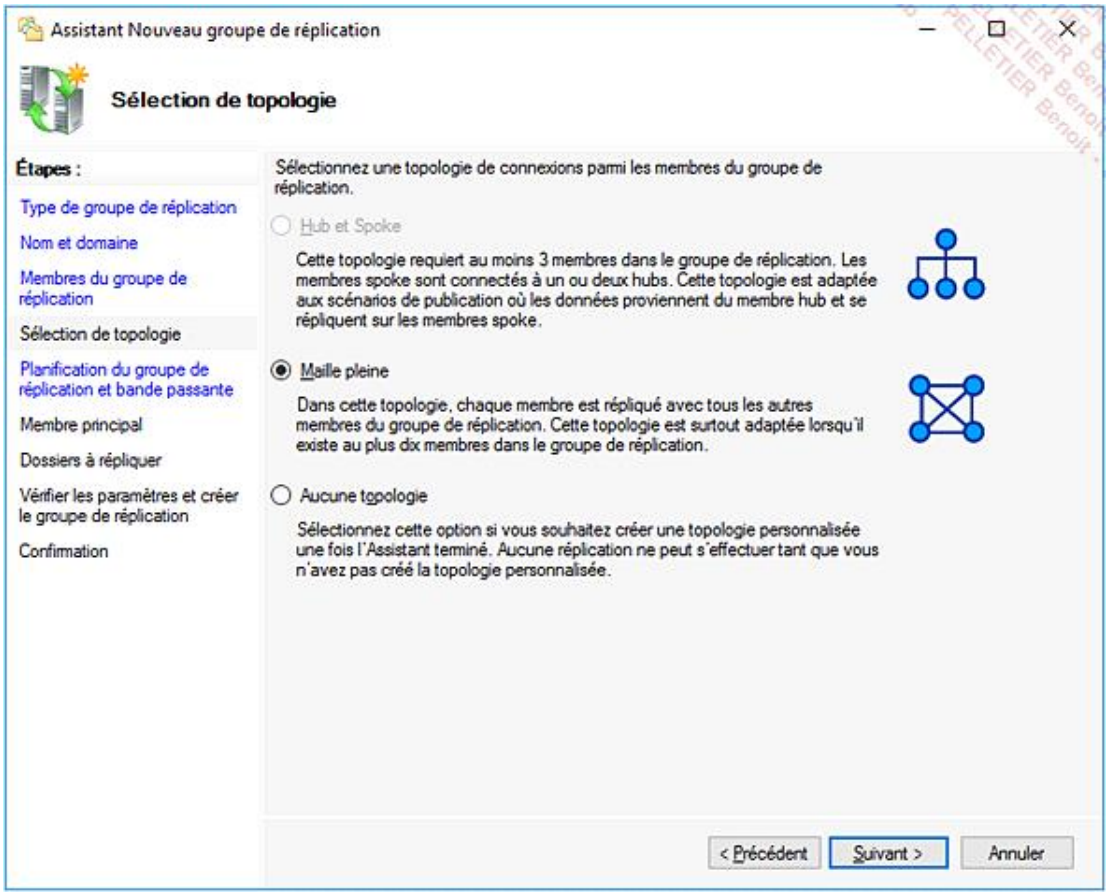
- Dans la console **Gestion du système de fichiers distribués DFS**, cliquez sur le nœud **Réplication** puis sur **Nouveau groupe de réplication** dans le panneau **Actions**.
- Dans la fenêtre du choix du type de groupe, sélectionnez **Groupe de réplication multi-usage** puis cliquez sur **Suivant**.



Dans **Nom du groupe de réplication**, saisissez **Groupe Compta** puis validez en cliquant sur **Suivant**.



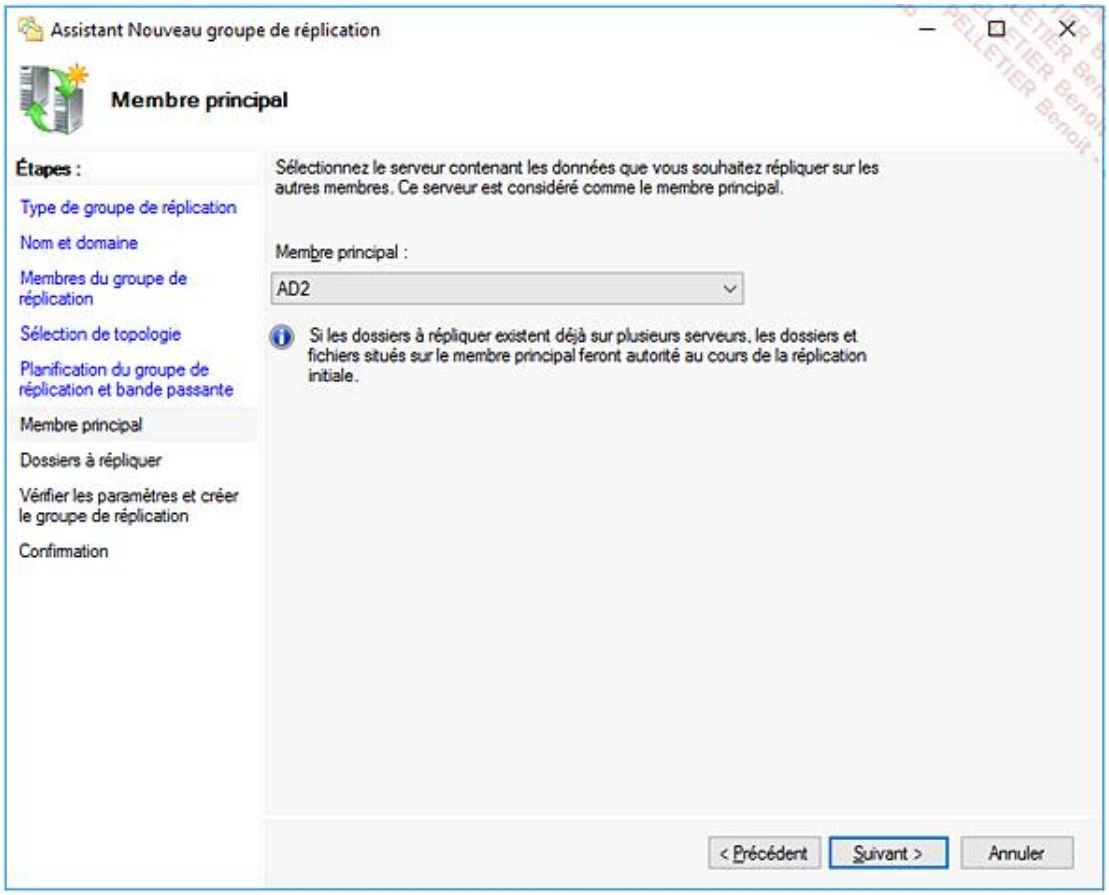
- Les serveurs à ajouter dans le groupe sont **AD2** et **SV1**. Pour effectuer cette opération, cliquez sur le bouton **Ajouter**.
- Sélectionnez le type de topologie **Maille pleine** puis cliquez sur **Suivant**.



Il est possible de planifier ou de limiter la bande passante afin d'éviter de créer un goulet d'étranglement. Dans notre cas, aucune limitation ne va être appliquée.

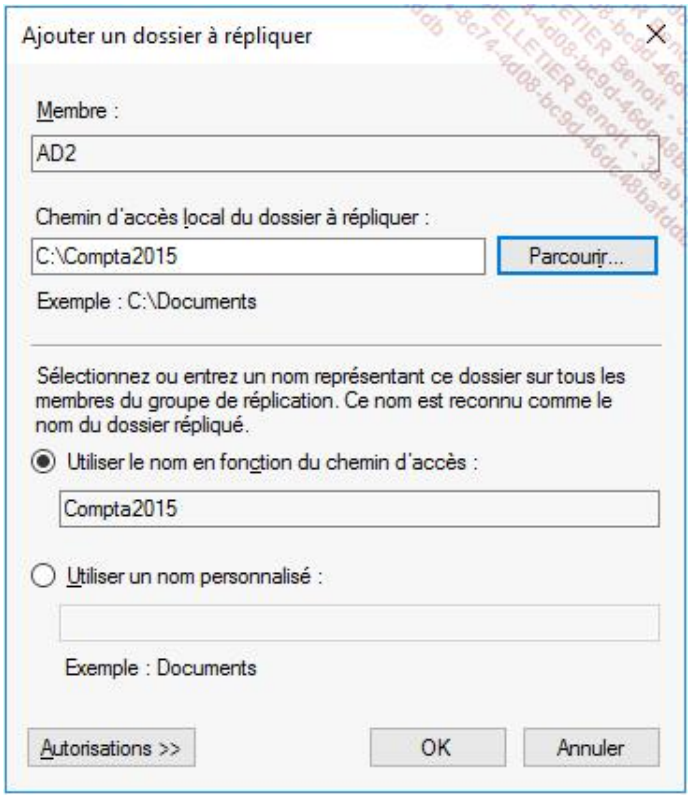
- Laissez les choix par défaut dans la fenêtre **Répliquer en continu à l'aide de la bande passante spécifiée** puis cliquez sur **Suivant**.
- Dans la liste déroulante qui permet d'effectuer le choix du **Membre principal**, sélectionnez **AD2** puis cliquez sur **Suivant**.

Le membre principal est le serveur qui a autorité lors de la première réplication.

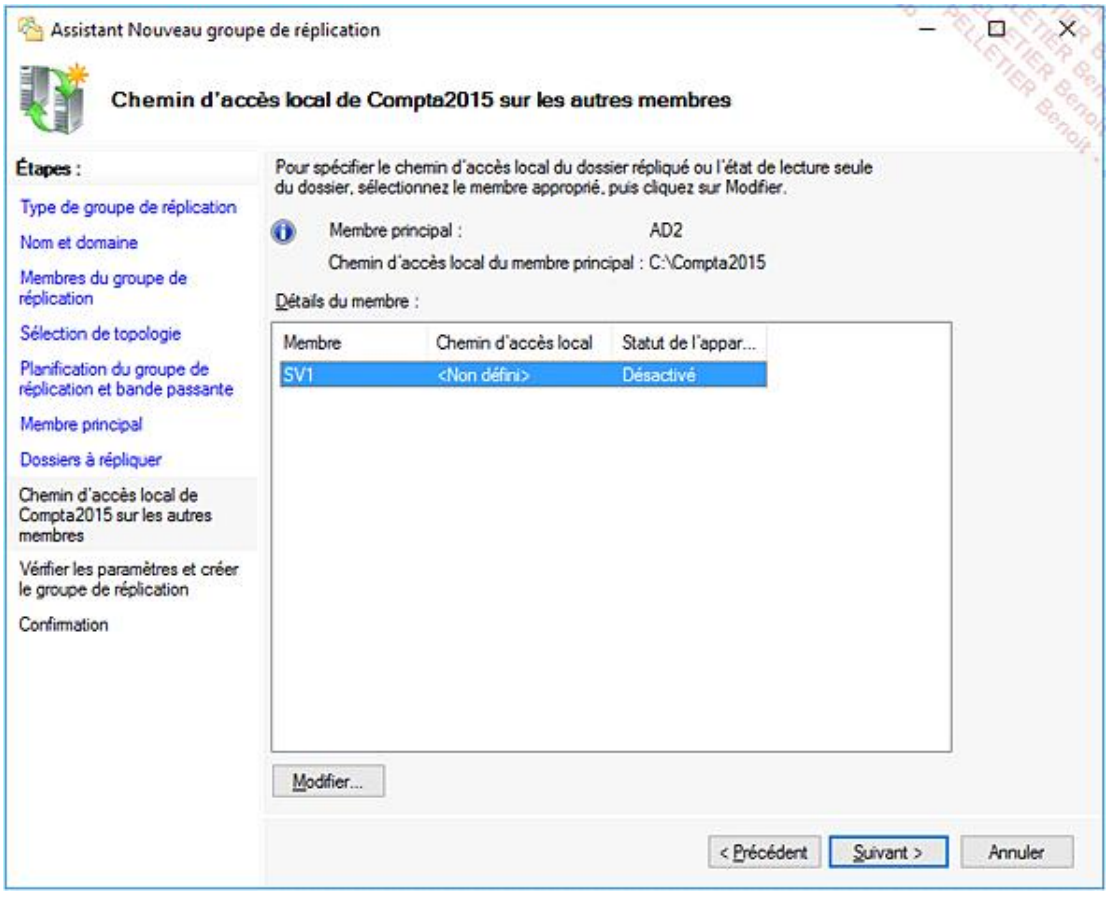


Il est nécessaire désormais de sélectionner les répertoires à répliquer.

- Cliquez sur le bouton **Ajouter**.
- Dans la fenêtre **Ajouter un dossier répliqué**, cliquez sur **Parcourir** puis sélectionnez le dossier **Compta2015**.



- Validez à l'aide du bouton **OK**.
- Dans la fenêtre **Chemin d'accès local de Compta2015 sur les autres membres**, cliquez sur le bouton **Modifier**.

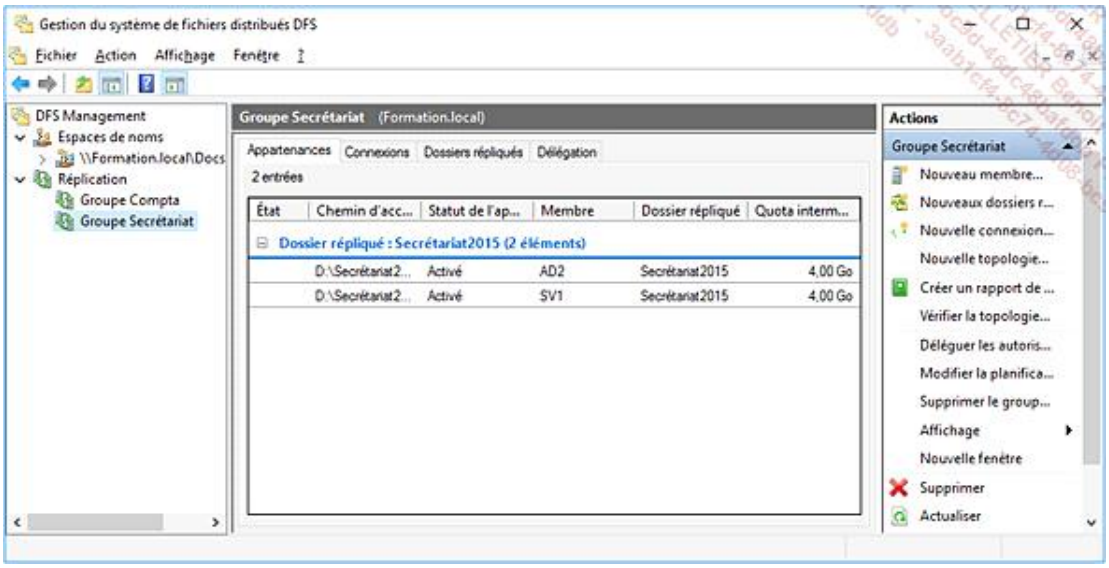


- Cliquez sur le bouton radio **Activé** puis sur le bouton **Parcourir**.

- Créez un nouveau dossier appelé **Compta2015** sur la partition **E:** du serveur **SV1**.
- Cliquez sur **Suivant** puis sur **Créer**.
- Si tout est vert, cliquez sur **Fermer**.

La réplication peut prendre un certain temps.

- Recommencez la même opération pour le dossier **Secrétariat**. Le membre principal est **SV1**, le groupe de réplication portera le nom de **Groupe Secrétariat**.



- Accédez à l'aide de l'explorateur au chemin UNC \\formation.local\docsformation.
- Créez un fichier texte nommé **TVA2015** dans **Comptabilité** puis un autre nommé **Contrat2015** dans **Secrétariat**.
- Vérifiez la présence des deux fichiers dans les dossiers **Compta2015** et **Secrétariat** sur les deux serveurs. Attention, la première réplication prend quelques minutes avant de débuter.

La réplication est effective et les fichiers sont répliqués.

En production, il est nécessaire de configurer le quota intermédiaire.

4. Les cmdlets PowerShell

Les cmdlets permettent d'effectuer des opérations sans passer par l'interface graphique. De plus, il est possible à l'aide de ces dernières d'automatiser certaines tâches.

Get-Dfsrbacklog

Get-Dfsrbacklog permet d'afficher les fichiers en attente de réplications entre deux partenaires.

```
Get-DfsrBacklog -GroupName "NomGroupe -FolderName "NomDossier"
-SourceComputerName "NomSrvSource" -DestinationComputerName
"NomDestination"
```

Get-DfsrState

La commande permet d'obtenir l'état des réplications pour le membre indiqué.

```
Get-DfsrState -ComputerName "NomServeur"
```

Get-DfsrConnection

Permet de voir les connexions établies entre les partenaires.

```
Get-DfsrConnection -GroupName "NomGroupe -SourceComputerName
"NomSrvSource" -DestinationComputerName "NomDestination" -DomainName
"NomDomaine"
```

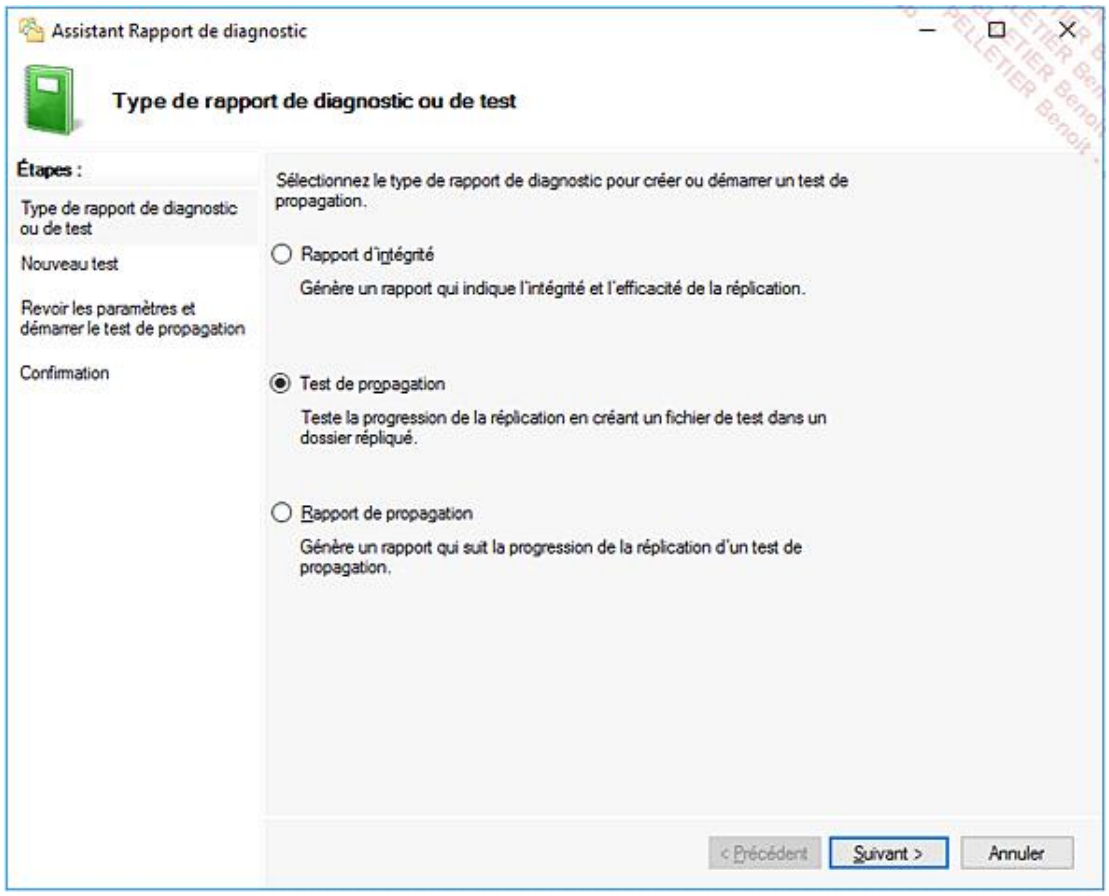
Utilisation des rapports

Les rapports permettent de récupérer une multitude d'informations sur l'espace de noms DFS. Il en existe trois types, chacun fournit des informations différentes.

- **Rapport d'intégrité** : deux éléments sont testés et présentés dans le rapport (l'état de la réplication ainsi que son efficacité).
- **Test de propagation** : ce test concerne la progression de la réplication. Pour effectuer cette opération, un fichier est créé dans un dossier répliqué.
- **Rapport de propagation** : le rapport affiche le suivi de la réplication pour le fichier de test créé lors de l'exécution du test de propagation.

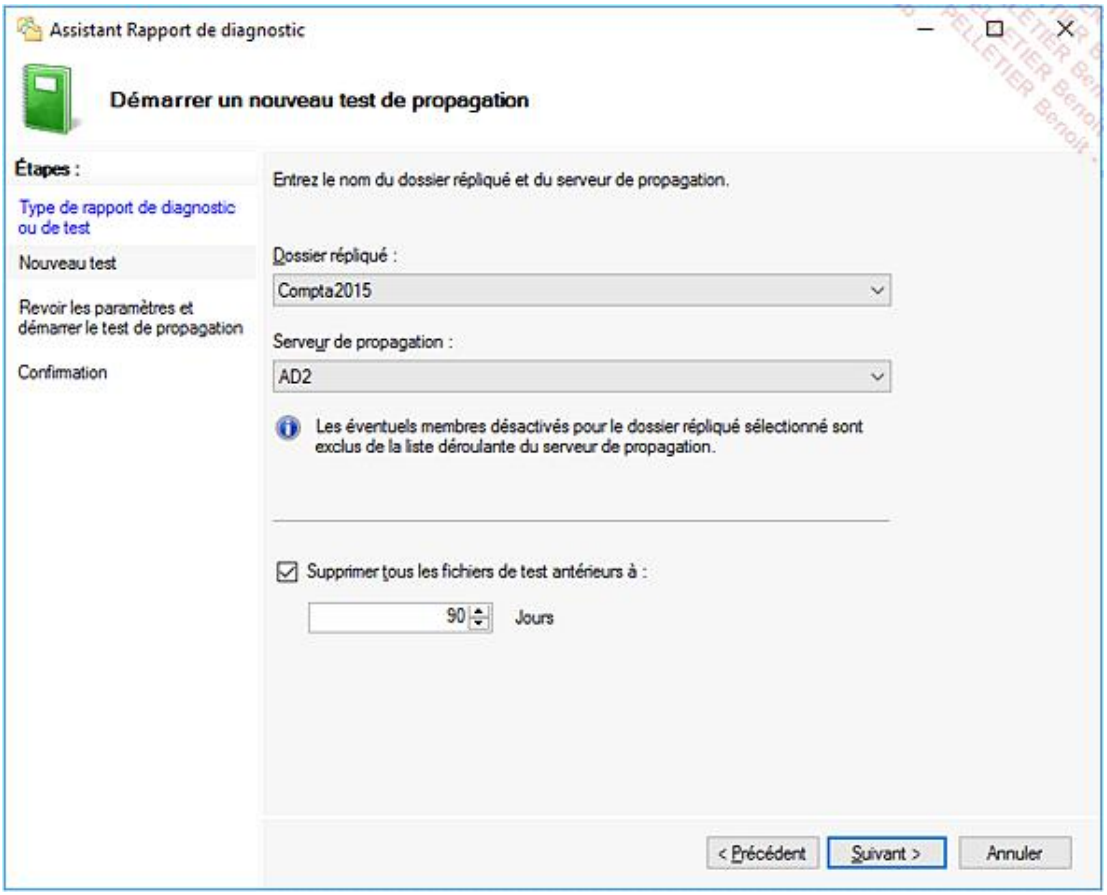
Cliquez sur le groupe de réplication **Groupe Compta** puis dans le bandeau **Actions**, cliquez sur **Créer un rapport de diagnostics**.

Sélectionnez le bouton radio **Test de propagation** puis cliquez sur le bouton **Suivant**.



L'assistant nous permet de sélectionner un répertoire configuré dans le groupe. Dans notre exemple, seul le dossier Compta2015 est présent. Il est également possible de configurer un serveur de propagation ainsi qu'un nombre de jours à l'issue desquels les fichiers de test sont supprimés.

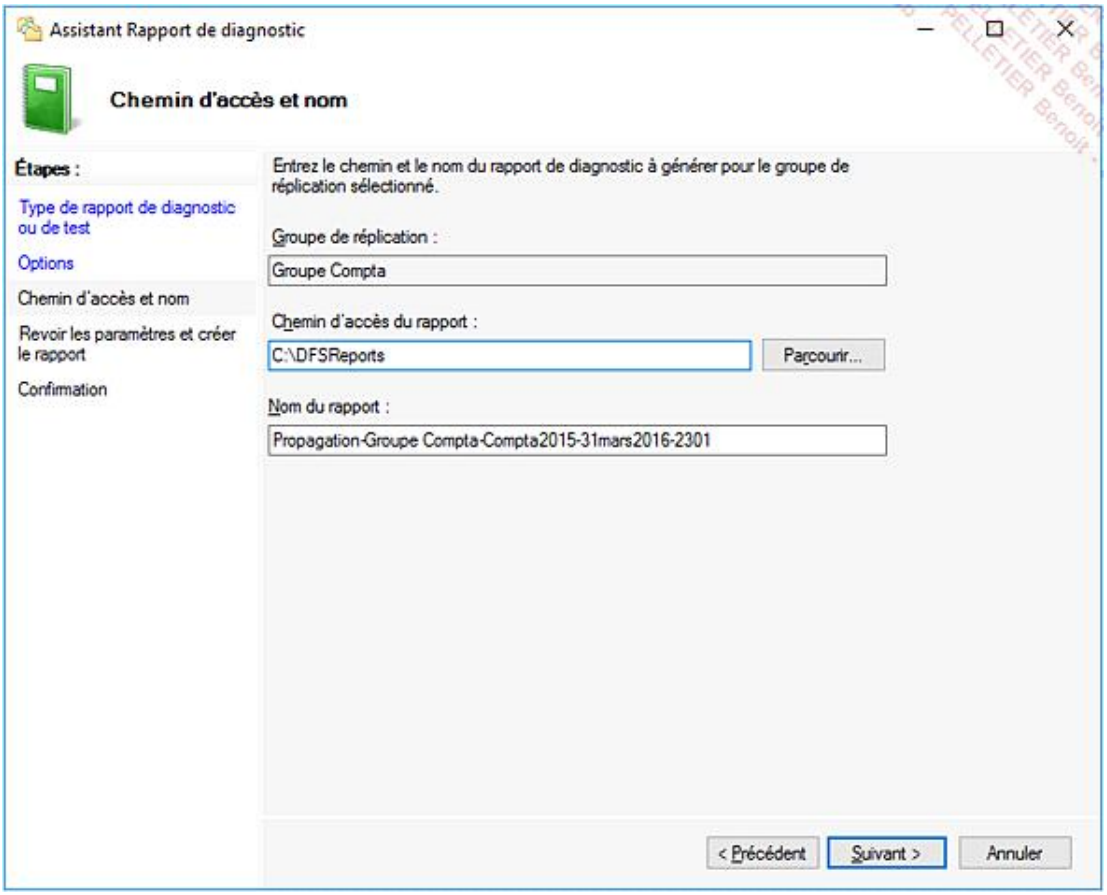
Laissez les valeurs par défaut puis cliquez sur **Suivant**.



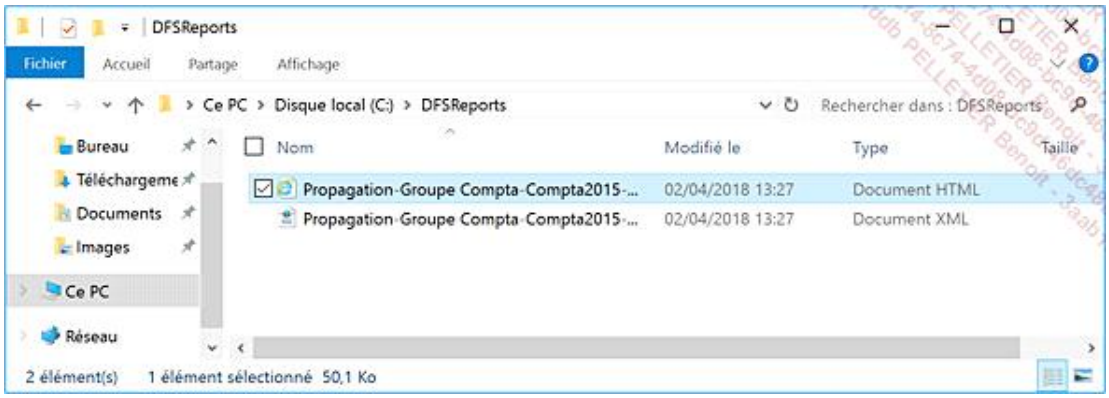
- Cliquez sur le bouton **Créer** afin de lancer l'opération.
- Si aucune erreur n'est présente, cliquez sur **Fermer**.
- Cliquez sur le groupe de réplication **Groupe Compta** puis dans le bandeau **Actions** cliquez sur **Créer un rapport de diagnostics**.
- Sélectionnez le bouton radio **Rapport de propagation**.
- Dans la fenêtre **Options de rapport**, cliquez sur **Suivant**.

La fenêtre **Chemin d'accès et nom** permet de sélectionner le répertoire qui va accueillir le rapport.

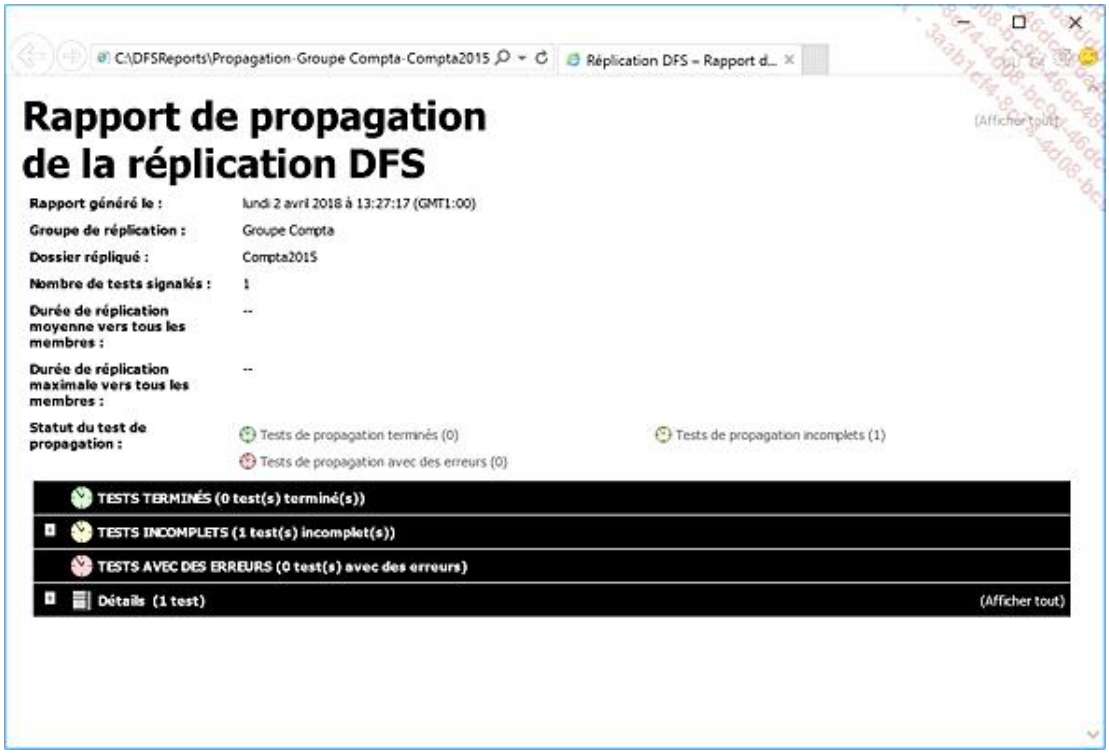
- Laissez le chemin par défaut puis cliquez sur **Suivant**.



- Cliquez sur **Créer** pour lancer l'opération de création. Le rapport est exécuté à la fin de l'assistant.
- Accédez au rapport **DFSReports**.



- Effectuez un clic droit sur le fichier HTML puis dans le menu contextuel sélectionnez l'option **Ouvrir avec**. Sélectionnez **Internet Explorer** dans le menu.



Les rapports permettent de s'assurer du bon fonctionnement de l'espace de noms DFS mais également de la partie Réplication.

Création d'un espace de noms avec PowerShell

L'espace de noms peut être créé à l'aide de l'interface graphique ou tout simplement à l'aide de commandes PowerShell.

Une grosse partie de ces scripts PowerShell sont disponibles sur le blog de l'auteur www.nibonnet.fr.

Dans un premier temps, le module ServerManager doit être importé. Ceci permet l'installation d'un rôle, dans notre cas DFS.

```
Import-Module Servermanager
#Install the DFS name space role
Add-WindowsFeature FS-DFS-Namespace -restart
```

La console DFS va également être installée.

```
#Install the mmc console to manage the DFS Namespace
install-WindowsFeature RSAT-DFS-Mgmt-Con
```

L'ajout de l'espace de noms peut maintenant être effectué. Le serveur concerné est srvad, le nom de l'espace de noms est DFS. De plus le type d'espace de noms choisi est intégré à un domaine AD avec le mode Windows Server 2008 (-Type domainv2).

Les différents composants (ABE...) devront être configurés en fonction du besoin. Pour cela vous pouvez utiliser la documentation Technet pour sélectionner la bonne valeur.

https://technet.microsoft.com/fr-fr/library/jj884286.aspx

```
#Adds space integrated names AD, configured with the 2008 Mode
ABE options ... are automatically configured by the script
#It is necessary to create the share (\\ srvad \ DFS in our example)
New-DfsnRoot -TargetPath \\srvad\DFS -Type domainv2
-EnableSiteCosting $true -EnableInsiteReferrals $false
-EnableAccessBasedEnumeration $true -EnableRootScalability $true
-EnableTargetFailback $true -State online -TimeToLiveSec 900
-GrantAdminAccounts "nibonnnet\admins du domaine" -TargetState online
-ReferralPriorityClass SiteCostNormal -Path \\formation.local\DFS -Confirm
```

Les dossiers et les cibles de dossiers peuvent maintenant être créés. Pour cela deux fichiers textes sont utilisés. Les chemins des fichiers sont insérés dans deux variables.

```
#Configures the necessary variables to create the folder targets

#$DFSUNCname the DFS path to access directories (exemple
\\formation.local\NameDFS\Folder)
$DFSUNCname = "C:\temp\dfsunc.txt"

#$UNCname the UNC path to access directories (exemple
\\SRVAD\Folder)
$UNCname = "C:\temp\unc.txt"
```

Nous pouvons maintenant créer les tableaux qui vont permettre de contenir les valeurs présentes dans les fichiers.

```
#Creating tables to retrieve the values of two text files

$TableauPath = @()

$TableauTargetPath = @()
```

Les boucles vont permettre la récupération des valeurs présentes dans les fichiers txt et l'ajout dans le tableau.

```
#first for each loop for the recovery of the first text file
foreach ($Cible in (get-content $DFSUNCname))

{

     $TableauPath+=$Cible


}
  #first for each loop for the recovery of the second text file
foreach ($Cible2 in (get-content $UNCname))

{

    $TableauTargetPath+=$Cible2

}
```

Les dossiers et les cibles peuvent maintenant être créés. L'ajout des cibles impose que les partages soient effectifs sur les différents serveurs.

```
#Creating folder targets. The shares must exist ...The values are
retrieved from the two tables. To navigate it, a variable is used
then incremented (variable i)
for ($i=0;$i -lt $TableauPath.Length;$i++)

{

    New-DfsnFolder -Path $TableauPath[$i] -TargetPath
$TableauTargetPath[$i] -EnableInsiteReferrals $false
-EnableTargetFailback $true -State online

}
```

Introduction aux stratégies de groupe

Une stratégie de groupe permet l'automatisation de la configuration de l'environnement utilisateur et ordinateur. Il est possible d'appliquer des configurations (autoriser ou bloquer certain menu…), de déployer des logiciels (fichiers MSI) ou simplement de mettre en place une politique de sécurité. Ainsi les stratégies de groupes permettent de rendre homogène la configuration du parc informatique. Un poste de travail ou un serveur membre peuvent se voir attribuer des GPO (*Group Policy Object*) du domaine. Ces dernières étant configurées sur un serveur possédant le rôle de contrôleur de domaine. Il est possible également de procéder à la configuration de GPO locales configurées directement sur le poste (à l'exception des contrôleurs de domaine).

1. Ordre d'attribution sur les postes de travail

Les stratégies de groupes sont appliquées sur le poste en fonction d'un ordre bien précis. La première stratégie à s'appliquer sur le poste est la stratégie locale (si une stratégie est présente). Les GPO Active Directory sont par la suite récupérées et appliquées, dans l'ordre ci-dessous :

La GPO du site AD est la première à être récupérée. Les stratégies appliquées à la racine du domaine (Default Domain Policy ou toute autre stratégie positionnée) sont ensuite récupérées. Enfin, celles positionnées sur une OU ou sous-OU sont récupérées.



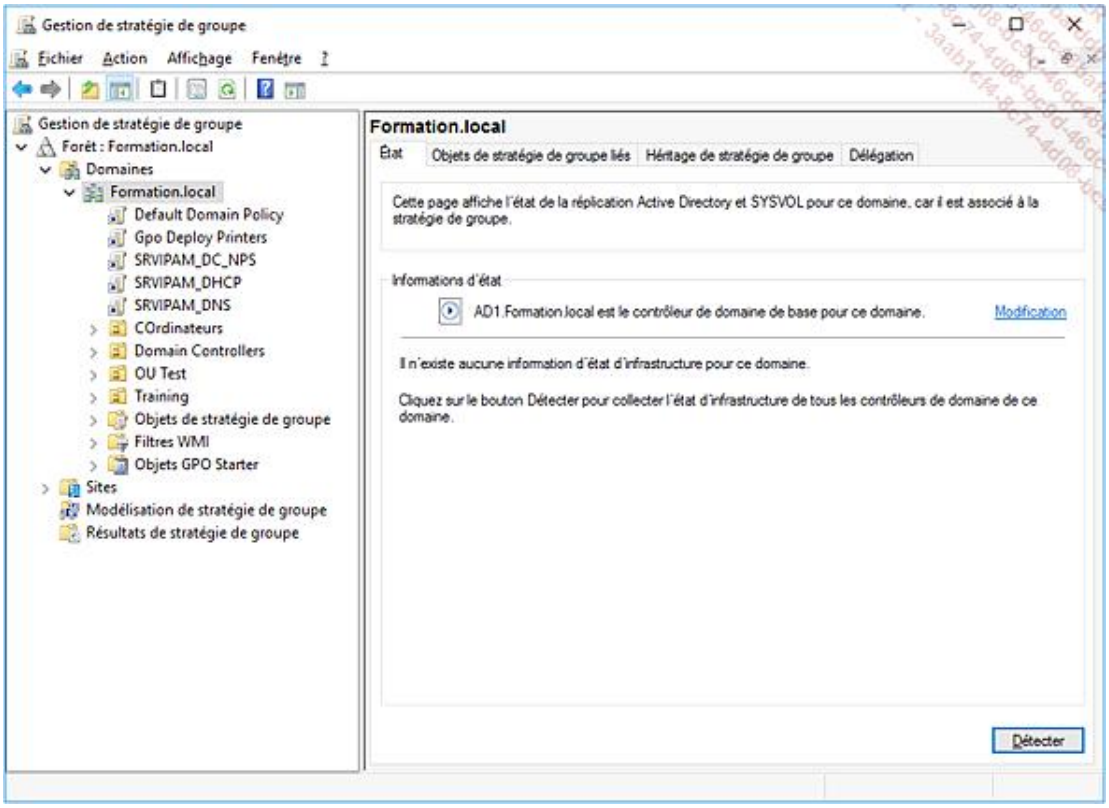
La liaison ne peut pas être faite directement sur une entité de sécurité (ordinateur ou utilisateur). Il est nécessaire de la lier à un conteneur (OU, domaine…). La stratégie qui s'applique en dernier est celle positionnée sur l'OU. En cas de conflit sur un paramètre, c'est la dernière GPO récupérée (donc celle de l'OU) qui l'emporte. Pour modifier cet ordre de priorité, il est possible de bloquer l'héritage ou d'appliquer (forcer) une stratégie. Cette dernière action n'est pas sans conséquence, car elle rend prioritaire toute GPO qui se voit attribuer cette option et permet de passer outre le blocage de l'héritage.

2. Outil de gestion des GPO (GPMC)

Depuis Windows Server 2003, un outil a été développé par Microsoft afin de pouvoir afficher et maintenir les

différentes stratégies de groupe de l'administration. Cet outil appelé **Console de gestion de stratégies de groupe (GPMC)** devait jusqu'à l'arrivée de Windows Server 2008 être téléchargé. Avec ce dernier, une nouvelle console est fournie lors de la promotion du serveur en tant que contrôleur de domaine.

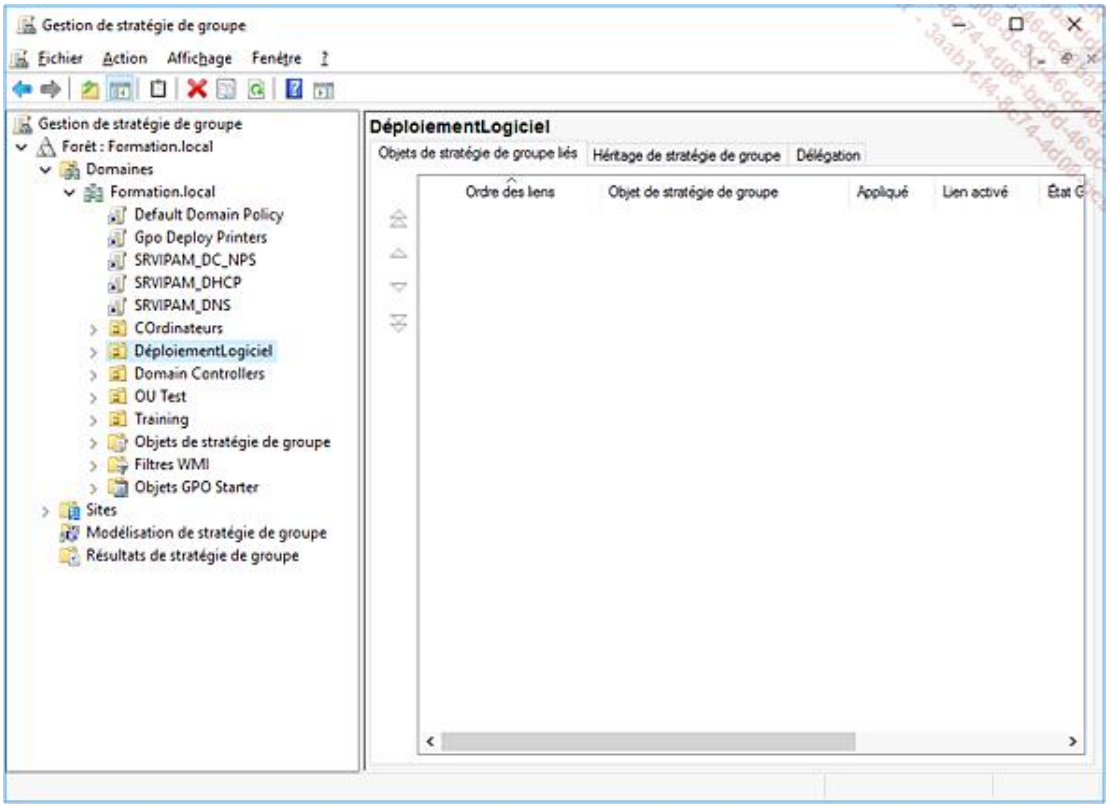
- Ouvrez une session sur le serveur **AD1**.
- Depuis le menu **Démarrer** accédez au dossier **Outils d'administration**.
- Cliquez sur **Gestion de stratégie de groupe** afin de lancer la console.
- Dans la console, développez les nœuds **Forêt** et **Domaines**.



Les unités d'organisation (OU) présentes dans Active Directory apparaissent également dans cette console. De plus la création d'une nouvelle OU est possible depuis cet outil.

- Effectuez un clic droit sur la racine du domaine **Formation.local**.
- Dans le menu contextuel, cliquez sur **Nouvelle unité d'organisation**.
- Dans le champ **Nom**, saisissez **DéploiementLogiciel**.

L'OU **DéploiementLogiciel** est maintenant présente dans la console.



La console est composée d'autres fonctionnalités qui sont pour la majorité traitées dans ce chapitre et les suivants.

- **Objet de stratégie de groupe** : ce conteneur contient l'ensemble des stratégies de groupe liées ou non à un conteneur. Il est préférable d'effectuer la création ici, afin que ces nouvelles GPO ne possèdent pas de liaison. Cette dernière est effectuée une fois tous les paramètres configurés, ceci afin d'éviter qu'une station ou un serveur ne récupère une GPO non finalisée et non testée.
- **Filtres WMI** : il existe plusieurs méthodes pour filtrer les utilisateurs ou les ordinateurs qui se voient attribuer une stratégie de groupe. Les filtres WMI sont une de ces méthodes. Ils permettent de limiter l'application des paramètres si le critère (type de système d'exploitation, quantité de mémoire…) présent dans le filtre est validé.
- **Modélisation de stratégie de groupe** : l'assistant permet de simuler le déplacement d'un objet utilisateur ou ordinateur dans un conteneur différent du sien. Ce déplacement va impliquer un changement des paramètres qui lui sont appliqués. La modélisation permet de générer un rapport présentant le détail de la stratégie résultante (stratégies de groupe qui seront appliquées et celles qui seront refusées).
- **Résultats de stratégie de groupe** : la stratégie résultante et donc les paramètres appliqués sur un poste peuvent être différents de ceux souhaités par l'administrateur. Différentes causes peuvent causer ce genre de désagréments, une liaison lente, un héritage bloqué ou une stratégie appliquée. L'assistant permet la récupération sur la machine concernée des stratégies de groupe appliquées ou refusées. Un rapport est créé présentant les causes des GPO refusées, les paramètres appliqués sur le poste, etc. Il est néanmoins nécessaire que l'utilisateur ait ouvert une session au moins une fois.

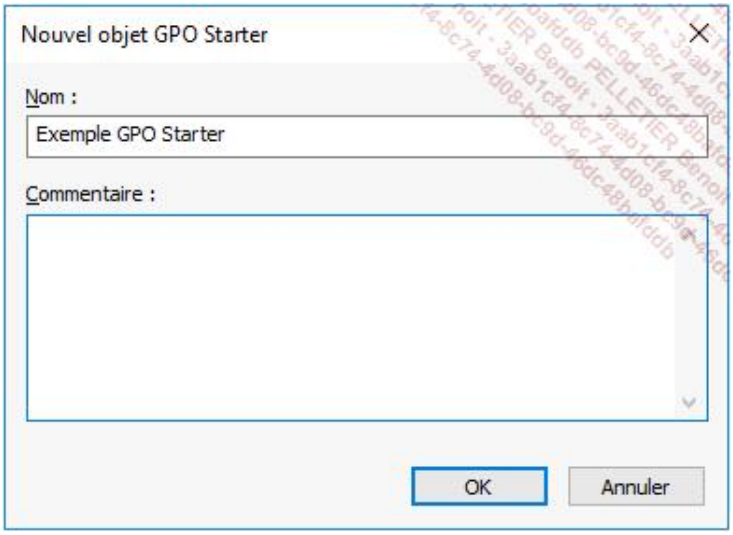
3. Objets GPO Starter

Apparus avec Windows Server 2008, les **Objets GPO Starter** offrent la possibilité d'avoir une base de paramètres applicables à toutes les GPO.

Seuls les paramètres du modèle d'administration sont configurables. Cette base peut être exportée dans un fichier **cab** afin de pouvoir être importée sur d'autres contrôleurs de domaine.

Effectuez un clic droit sur **Objets GPO Starter** puis, dans le menu contextuel, cliquez sur **Nouveau**.

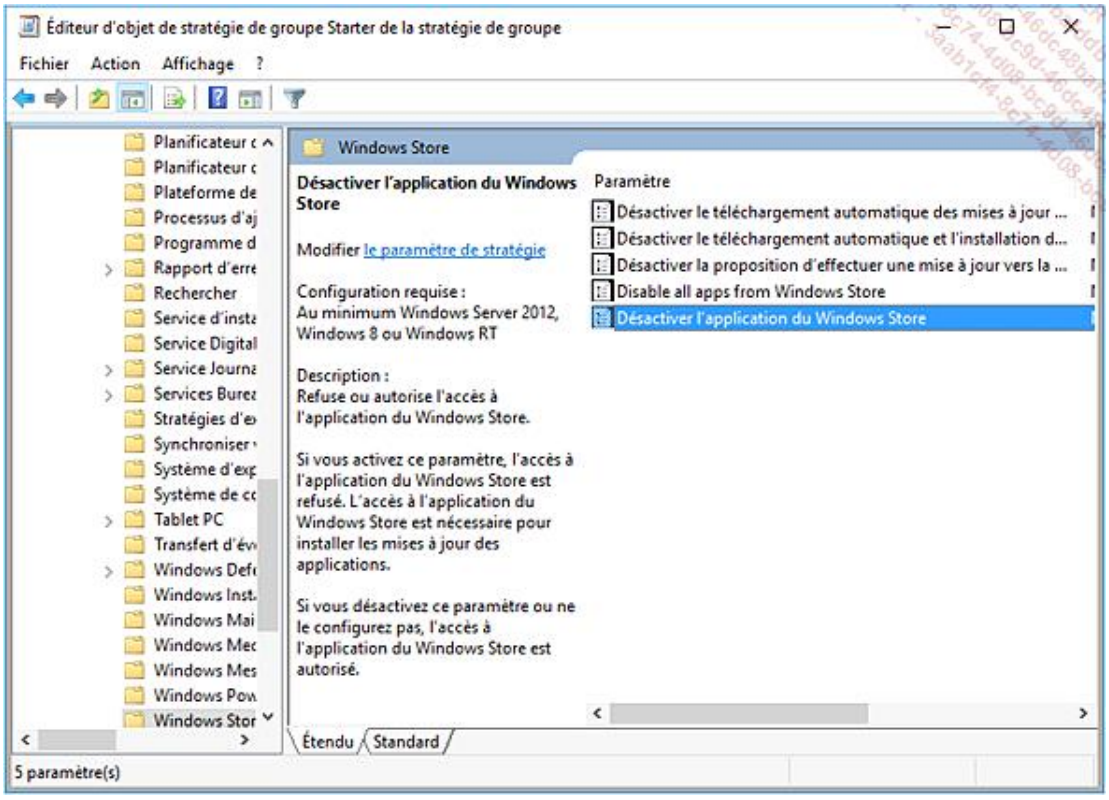
- Dans le champ **Nom**, saisissez **Exemple GPO Starter** puis cliquez sur **OK**.



- Effectuez un clic droit sur l'objet qui vient d'être créé puis cliquez sur **Modifier**.

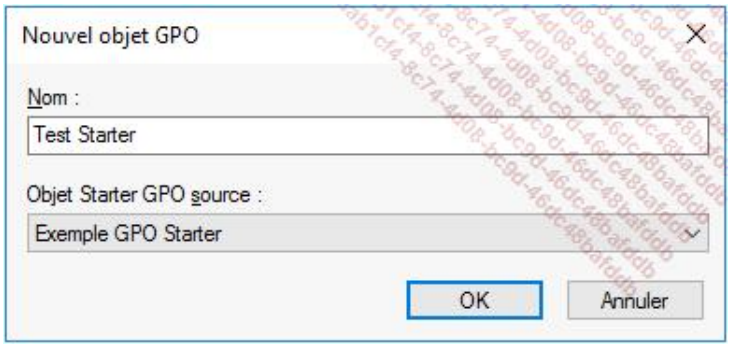
Seuls les modèles d'administration sont présents.

- Développez **Modèles d'administration** dans **Configuration ordinateur**.
- Double cliquez sur le paramètre **Désactiver l'application du Windows Store** présent dans **Composants Windows\Windows Store**.



- Cochez le bouton radio **Activé** puis cliquez sur **OK**.
- Effectuez la même opération pour le paramètre **Ne pas autoriser l'exécution du magnétophone** présent dans **Configuration utilisateur\Composants Windows\Magnétophone**.

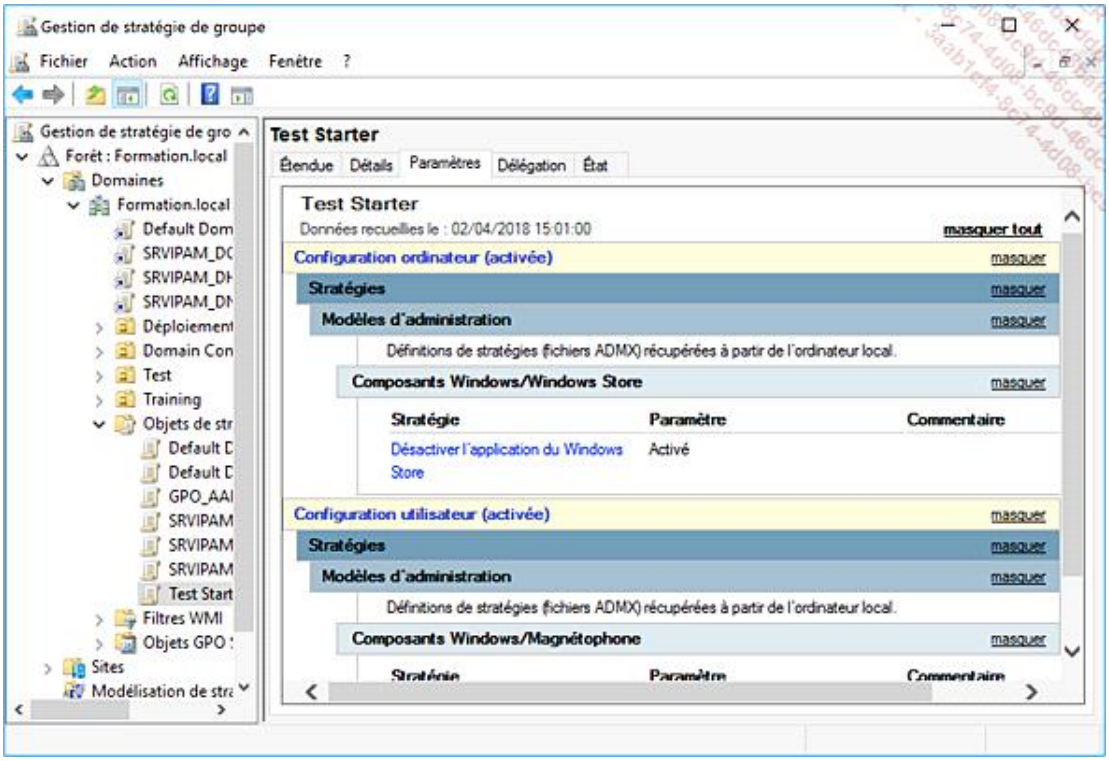
- Fermez la console **Éditeur d'objets de stratégie de groupe** puis dans la console **Gestion de stratégie de groupe**, cliquez sur **Objets de stratégie de groupe**.
- Effectuez un clic droit sur le conteneur puis cliquez sur **Nouveau**.
- Saisissez **Test Starter** dans le champ **Nom** puis, dans la liste déroulante, sélectionnez la stratégie qui vient d'être créée.



- Cliquez sur **OK** et effectuez un double clic sur la stratégie **Test Starter**.

À l'aide de l'onglet **Étendue**, on peut voir que le champ **Liaisons** est vide. La stratégie n'est donc pour le moment pas liée.

- Cliquez sur l'onglet **Paramètres** puis sur le lien **Afficher tout**.



Les paramètres configurés dans l'objet **GPO Starter** sont bien présents.

4. Présentation des CSE (extensions côté client)

Le client de stratégie de groupe présent sur les postes clients ou les serveurs membres récupère une liste triée d'objets GPO depuis le contrôleur de domaine. Si une stratégie de groupe à laquelle l'utilisateur/ordinateur a accès

a été modifiée depuis la dernière récupération, le téléchargement et la mise en cache sont opérés.

Les extensions côté client (CSE) présentes sur tous les systèmes Microsoft récupèrent alors les paramètres de la GPO concernée afin d'appliquer les modifications. Une extension CSE existe pour chaque type de paramètres de stratégie (sécurité, préférences, registre, installation de logiciel, etc.). Seules les extensions CSE de sécurité appliquent obligatoirement les modifications toutes les 16 heures.

Traitement en boucle

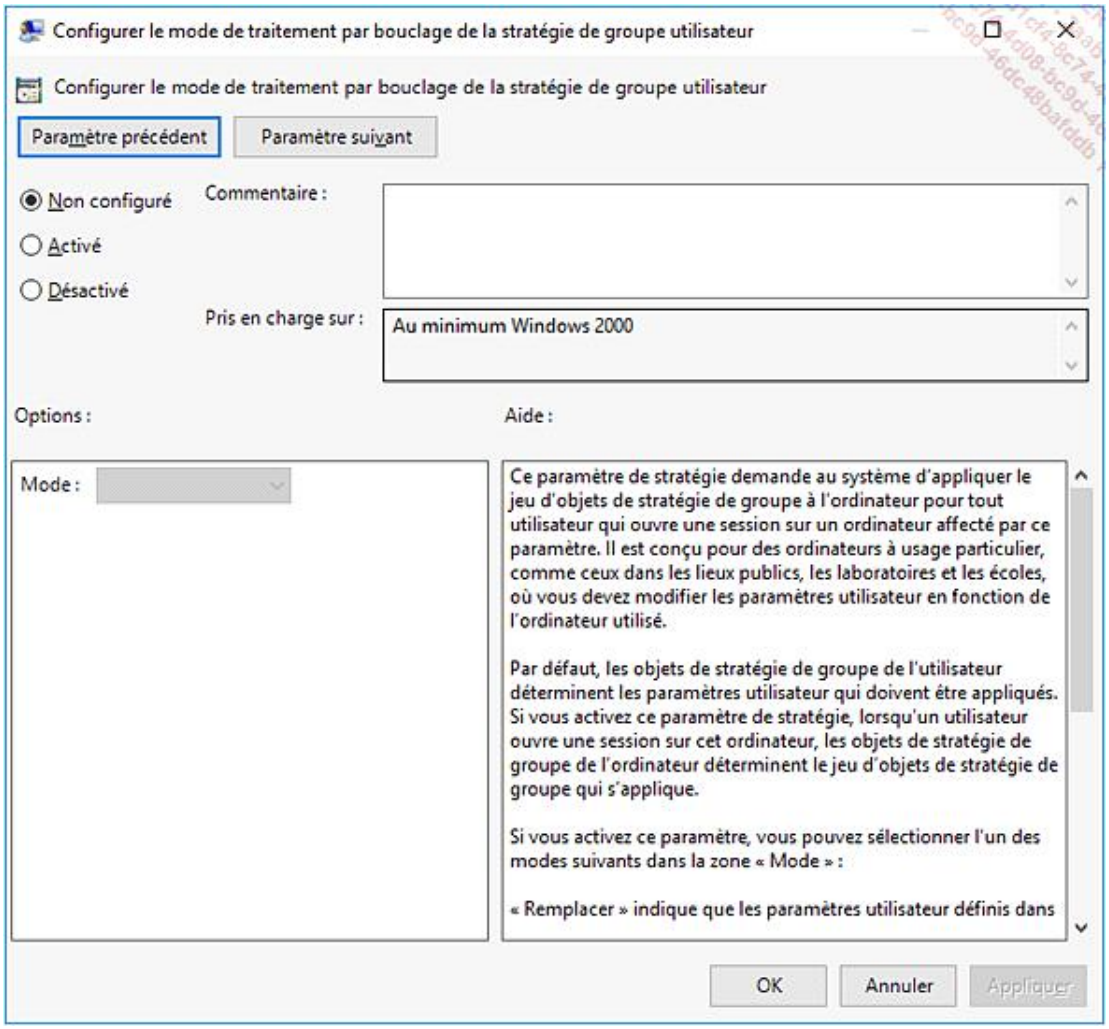
1. Introduction

Lors de l'ouverture de session sur un serveur TS (*Terminal Server*) ou un poste client, la stratégie résultante qui est appliquée est une combinaison des paramètres utilisateur et ordinateur. Il peut être nécessaire sur un serveur TS d'interdire l'application des paramètres de l'utilisateur connecté.

Le traitement en boucle permet l'application des paramètres Configuration utilisateur de la stratégie de groupe de l'ordinateur sur lequel la session est ouverte. Tous les utilisateurs recevront ces mêmes paramètres.

Deux modes peuvent être configurés : le mode **Remplacer** et le mode **Fusion**. Le premier effectue la suppression des paramètres Configuration utilisateur configurés pour le compte utilisateur afin de lui attribuer ceux configurés dans la GPO du compte ordinateur sur lequel la session est ouverte. Le deuxième mode effectue une fusion entre les paramètres Configuration utilisateur du compte utilisateur et ceux configurés dans la stratégie de groupe du compte ordinateur.

On peut ainsi s'assurer de l'uniformité des paramètres pour l'ensemble des utilisateurs qui ouvrent une session sur le serveur TS (*Terminal Server*). Le mode est sélectionné à l'aide du paramètre **Configurer le mode de traitement par bouclage de la stratégie de groupe utilisateur** présent dans **Configuration ordinateur\Stratégies\Modèles d'administration\Système\Stratégie de groupe**.



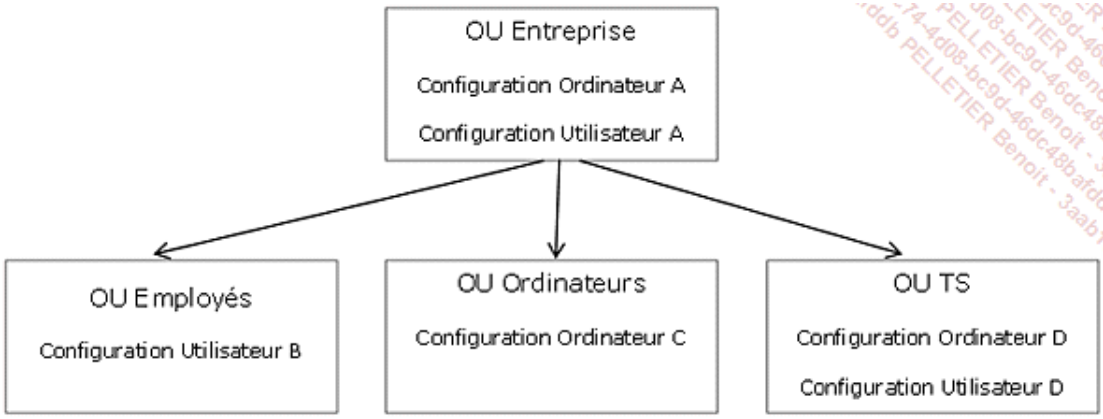
2. Les modes Fusion et Remplacer

Pour expliquer les modes **Remplacer** et **Fusion**, prenons un exemple concret.

La stratégie **SRVTSE** est positionnée sur l'unité d'organisation **Entreprise**, elle possède des paramètres dans **Configuration utilisateur** et dans **Configuration ordinateur** (nous nommerons la stratégie à l'aide de la lettre A).

L'unité d'organisation Entreprise est composée de trois sous-OU :

- **Employés** contient les comptes utilisateurs. Une GPO contenant uniquement des paramètres utilisateurs est configurée. Donnons à cette stratégie la lettre B.
- **Ordinateurs** contenant uniquement les comptes des postes de travail, avec le paramètre Configuration ordinateur uniquement configuré. La lettre C est attribuée à cette stratégie.
- **TS** qui héberge les comptes des serveurs TS. La stratégie configurée contient des paramètres utilisateurs et ordinateurs, et la lettre D lui est attribuée. Le traitement en boucle est activé pour ces serveurs.



Lors du démarrage du poste, les stratégies A et C s'appliquent sur le poste alors que les paramètres contenus dans les GPO A et B s'appliqueront eux lors de l'ouverture de session. Si l'utilisateur ouvre une session sur le serveur TS, la stratégie résultante pour les configurations utilisateur et ordinateur est cette fois A + D. Contrairement au mode **Remplacer**, le mode **Fusion** ne supprime pas la stratégie configurée sur l'OU Employés. Une fusion des deux est effectuée, et en cas de conflit la GPO D liée à l'OU TS est prioritaire.

Gestion des stratégies de groupe

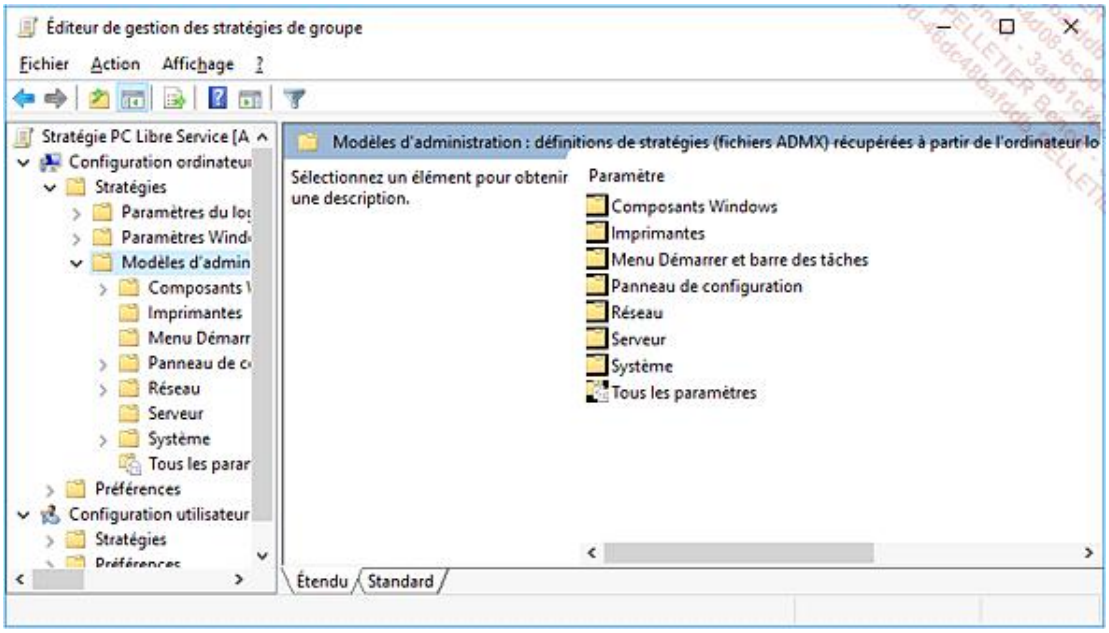
Toute opération sur une stratégie de groupe est réalisée à l'aide de la console **Gestion de stratégie de groupe**. La console est présente au niveau des **Outils d'administration** dans le menu Démarrer.

1. Création d'un objet et liaison à une OU

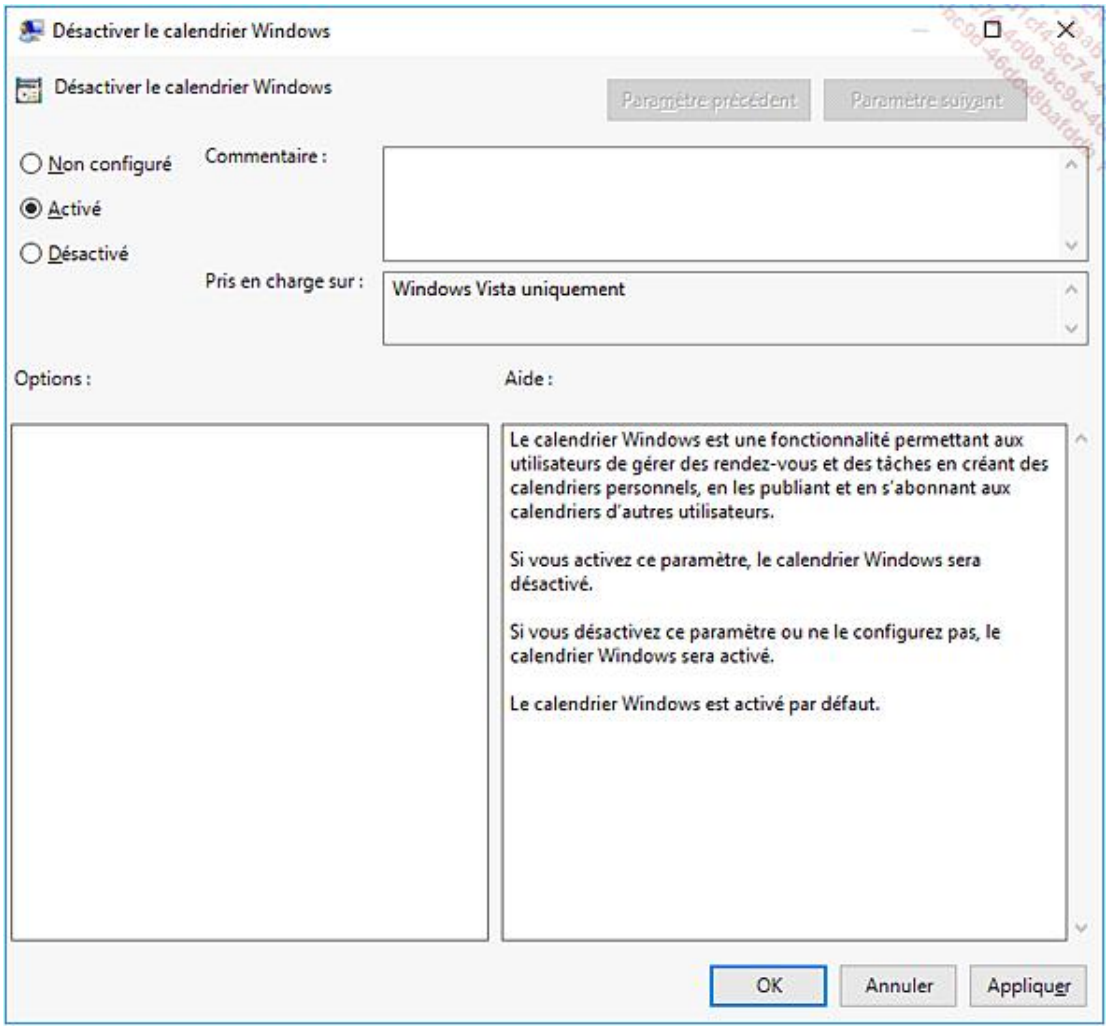
- Lancez la console **Gestion des stratégies de groupe**.
- Développez les nœuds **Forêt**, **Domaines** puis **Formation.local**.
- Effectuez un clic droit sur le conteneur **Objets de stratégie de groupe** puis cliquez sur **Nouveau**.
- Dans le champ **Nom**, saisissez PC Libre Service puis cliquez sur **OK**.
- Effectuez un clic droit sur la stratégie qui vient d'être créée puis sélectionnez l'option **Modifier**.

L'**Éditeur de gestion des stratégies de groupe** se lance.

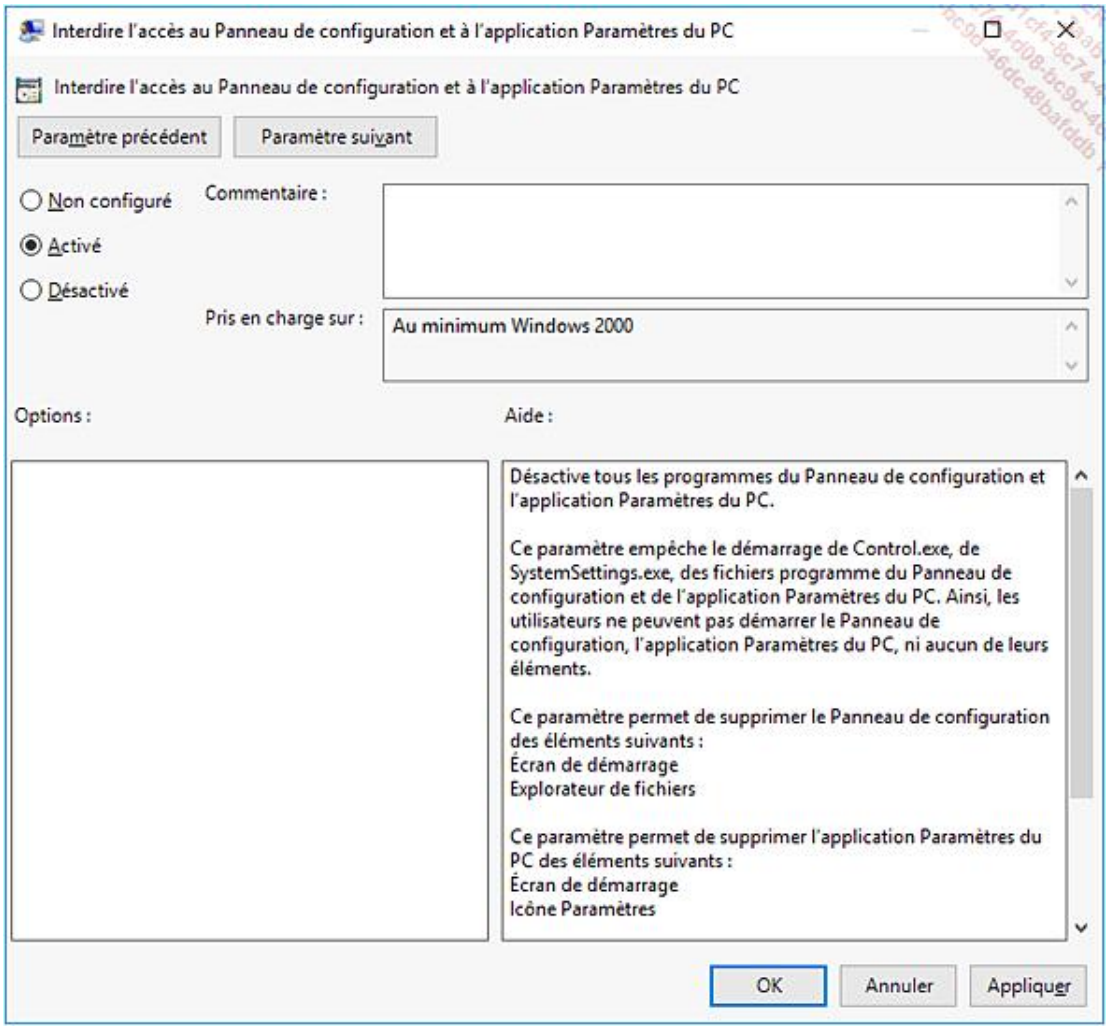
- Dans **Configuration ordinateur**, développez **Stratégies** puis **Modèles d'administration**.



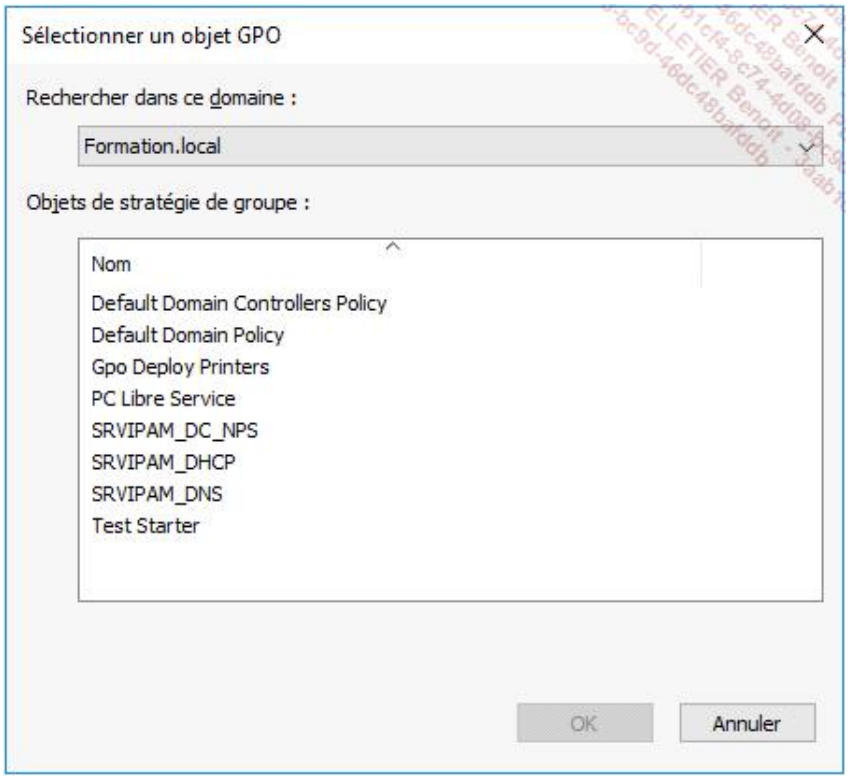
- Double cliquez sur **Composants Windows** puis sélectionnez **Calendrier Windows**.
- Double cliquez sur **Désactiver le calendrier Windows**.
- Cochez le bouton **Activé** puis cliquez sur **Appliquer** et **OK**.



- Dans **Configuration utilisateur**, développez **Stratégies**, **Modèles d'administration** puis **Panneau de configuration**.
- Double cliquez sur **Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC** puis cochez le bouton **Activé**.



- Cliquez sur **Appliquer** puis sur **OK**.
- Fermez l'**Éditeur des stratégies de groupe**.
- Effectuez un clic droit sur la racine du domaine **Formation.local** puis cliquez sur **Lier une stratégie de groupe existant**.
- Dans la fenêtre **Sélectionner un objet GPO**, cliquez sur **PC Libre Service** puis sur **OK**.

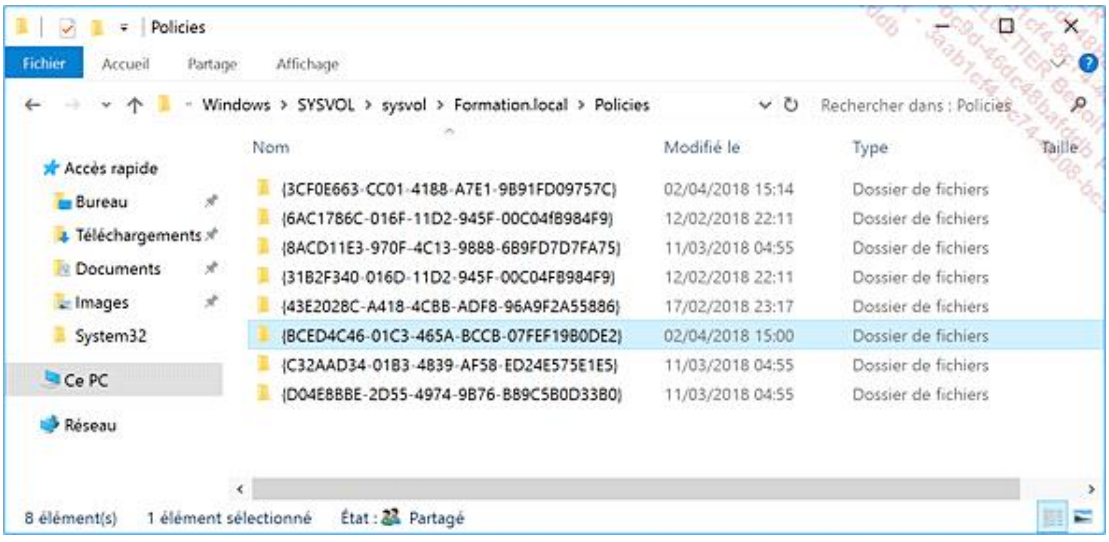


La stratégie est maintenant liée à la racine du domaine.

L'onglet **Étendue** permet de visualiser le conteneur auquel la GPO est liée. Il est possible de mettre un filtre de sécurité afin de limiter l'application de la stratégie aux membres du groupe. Par défaut, le groupe **Utilisateurs authentifiés** est configuré et l'ensemble des utilisateurs du domaine reçoivent les paramètres. Les boutons **Ajouter** et **Supprimer** permettent d'intervenir sur ce champ en ajoutant ou en supprimant des groupes.

Cliquez sur l'onglet **Détails**.

L'onglet permet d'obtenir très rapidement les dates de création et de modification ainsi que le propriétaire. **Version utilisateur** et **Version ordinateur** indiquent le nombre de modifications apportées (chaque paramètre ajouté ou modifié implique une incrémentation du compteur). L'**ID unique** identifie la stratégie. Le même numéro est présent dans SYSVOL.

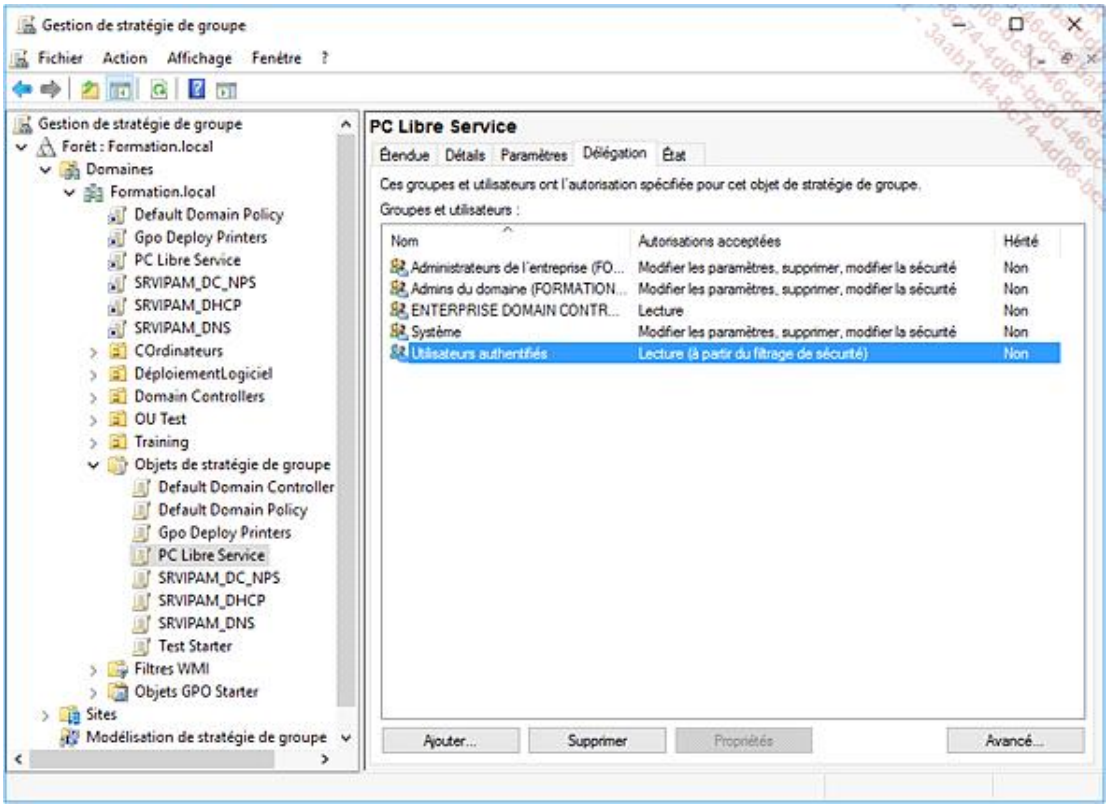


La propriété **État GPO** permet de déterminer l'état, **Désactivé** ou **Activé**, de la stratégie. Il est possible de désactiver les paramètres de configuration utilisateur ou ordinateur.

- Cliquez sur l'onglet **Paramètres**.

L'ensemble des paramètres configurés dans la stratégie pour les utilisateurs et ordinateurs s'affichent.

- Cliquez sur l'onglet **Délégation**.



La délégation permet de donner une autorisation de gestion de la stratégie à un utilisateur non membre du groupe **Admins du domaine**.

- Sur le poste client exécutant Windows 10, lancez une invite de commandes DOS.
- Saisissez la commande `gpupdate /force` puis appuyez sur [Entrée].

Une interrogation des contrôleurs de domaine est lancée toutes les 90 à 120 minutes ou lors de l'ouverture de session pour les paramètres utilisateurs, et au démarrage du poste pour les paramètres ordinateur. Il est donc nécessaire d'exécuter la commande `gpupdate /force` afin d'obliger le poste à interroger son serveur et récupérer les modifications qui ont été apportées.

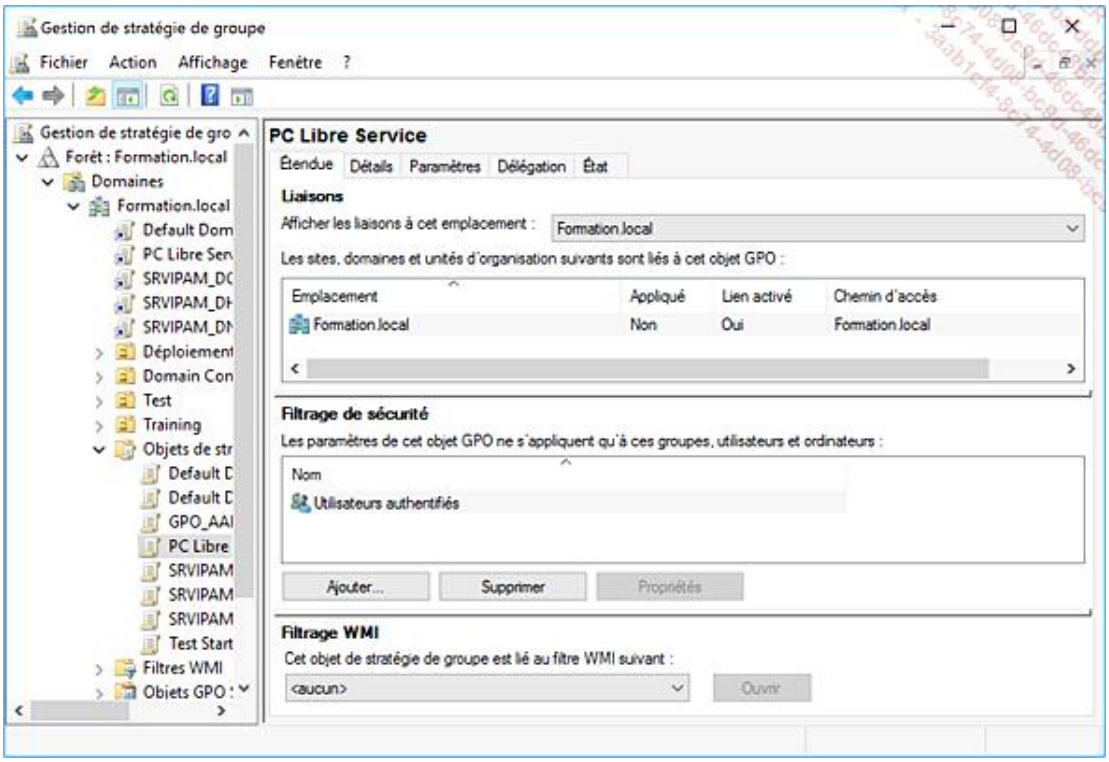


Le paramètre s'applique et la restriction est désormais active.

La restriction n'est plus active si l'objet utilisateur ou ordinateur est déplacé dans un conteneur différent (GPO lié à une OU et non au domaine) ou si le lien de la stratégie est supprimé.

2. Suppression d'une liaison

- Dans la console **Gestion de stratégie de groupe** sur **AD1**, cliquez sur la stratégie précédemment créée afin d'afficher ses propriétés.
- Dans le champ **Étendue**, effectuez un clic droit sur **Formation.local** puis cliquez sur **Lien activé** afin de décocher l'activation (annulation de la liaison).



- Sur le poste client, exécutez une nouvelle fois la commande `gpupdate /force`.

La restriction n'est désormais plus active.

En supprimant la liaison, la stratégie ne s'applique plus sur le poste. Les paramètres par défaut ont donc été réappliqués sur le client.

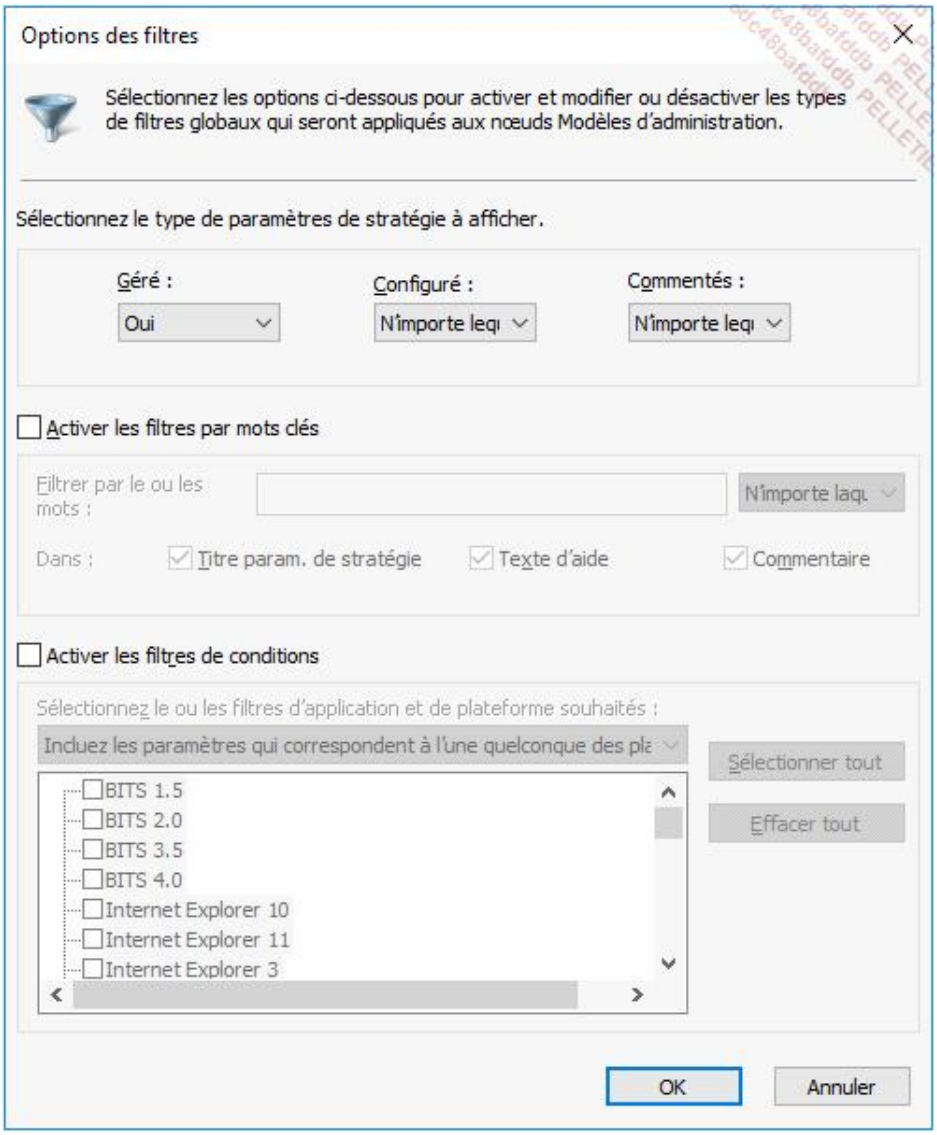
3. Utilisation des filtres sur le modèle d'administration

Les modèles d'administration contiennent une multitude de paramètres configurables. Afin d'en faciliter la recherche, Microsoft a implémenté depuis Windows Server 2008 une fonctionnalité de filtrage.

Il est donc possible de chercher les paramètres qui correspondent à un mot clé ou d'afficher uniquement ceux configurés.

- Dans la console **Gestion de stratégie de groupe**, effectuez un clic droit sur la stratégie **PC Libre Service** puis cliquez sur **Modifier**.

Effectuez un clic droit sur **Modèles d'administration** présent dans **Configuration utilisateur** puis sélectionnez **Options des filtres**.



La fenêtre est composée de plusieurs bandeaux. Le premier des trois est composé de trois listes déroulantes :

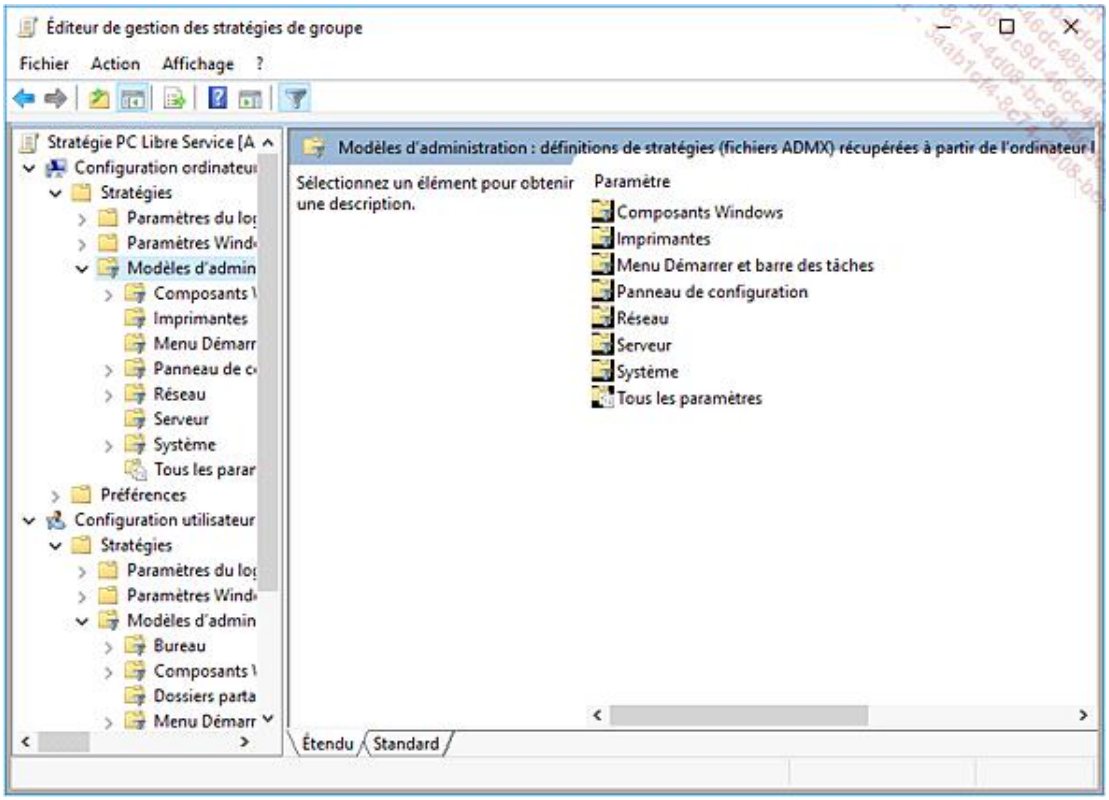
- **Géré** : il permet de déterminer si le paramètre filtré est un paramètre géré ou non géré.
- **Configuré** : cette liste permet d'afficher uniquement les paramètres qui sont configurés dans la stratégie de groupe.
- **Commentés** : ce paramètre du filtre est identique au précédent, il filtre par contre sur les commentaires laissés dans la stratégie.

Le deuxième permet un filtrage par un mot-clé alors que le troisième et dernier bandeau filtre sur une application ou une plateforme (Windows Server 2003, Internet Explorer 10).

Cochez la case **Activer les filtres par mots clés**.

Dans le champ **Filtrer par le ou les mots** saisissez **Menu Exécuter**.

Le filtre est positionné dans **Configuration utilisateur** et **Configuration ordinateur**.



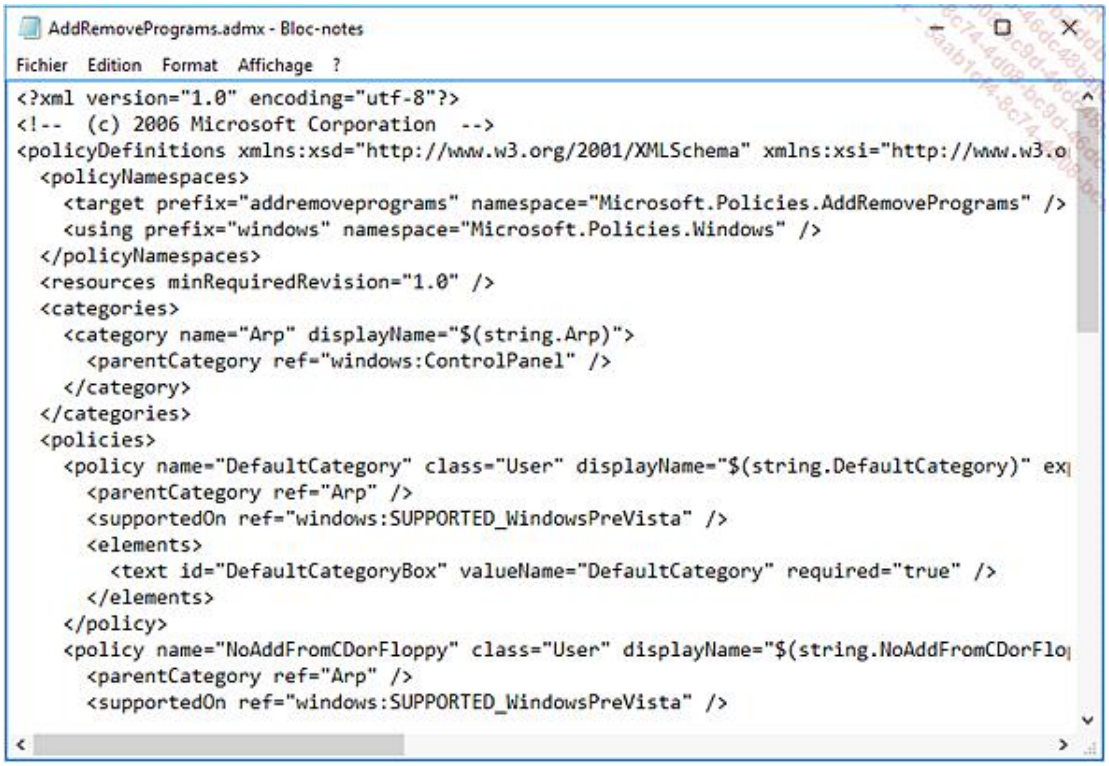
Les paramètres contenant les mots **Menu Exécuter** sont affichés.

Modèles d'administration

Les modèles d'administration permettent de mettre en place des restrictions sur un ensemble de composants du système d'exploitation.

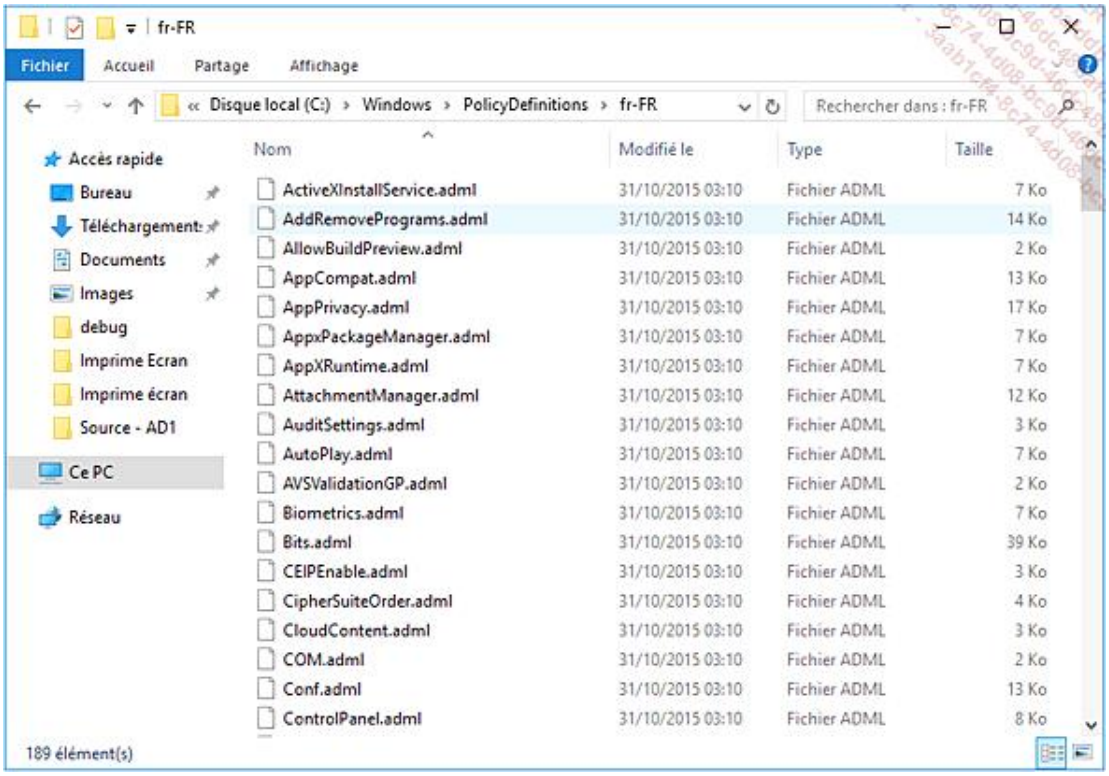
1. Fichiers ADMX/ADML

Les paramètres des modèles d'administration sont contenus dans des fichiers portant l'extension ADMX. Ces fichiers présents dans **C:\Windows\PolicyDefinitions** peuvent être ouverts avec Notepad.



Contrairement aux anciens modèles d'administration sous Windows Server 2003, les fichiers ADMX sont des fichiers XML. Il est donc beaucoup plus aisé de créer un fichier personnalisé. Deux types de fichiers sont utilisés :

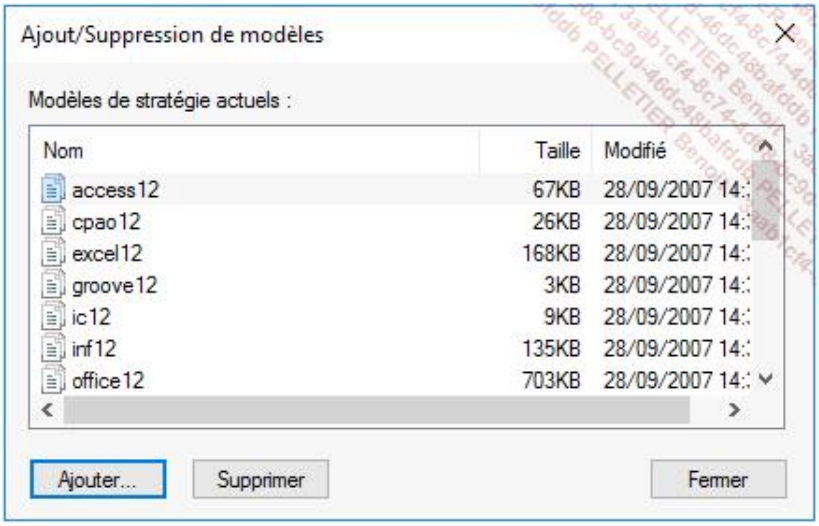
- Les fichiers portant l'extension admx permettent de définir l'emplacement du paramètre, les éléments de la boîte de dialogue **Propriétés** et la modification du registre à apporter.
- Les fichiers portant l'extension adml sont chargés d'afficher le texte de l'interface utilisateur dans une langue spécifique. Il est ainsi très aisé de changer la langue d'affichage en récupérant les fichiers adml adéquats. Le dossier **fr-FR** contient ceux pour la langue française.



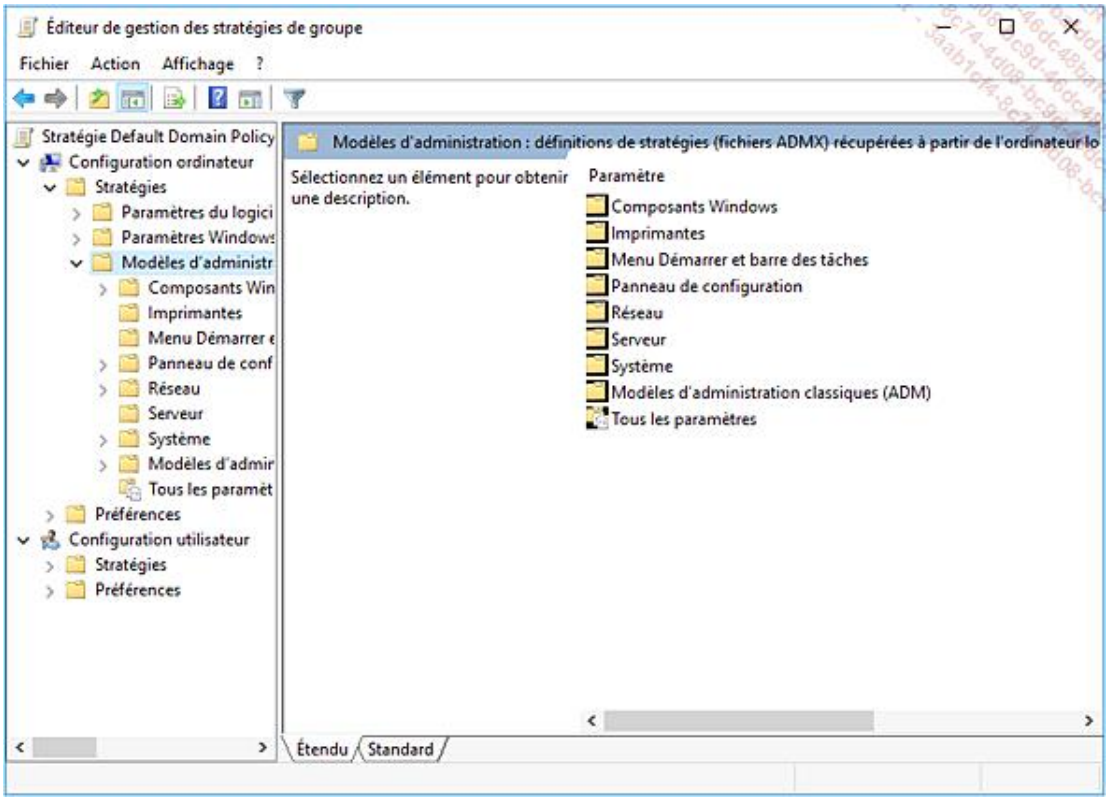
Il est envisageable d'ajouter d'anciens modèles d'administration au format **adm**.

- Effectuez un clic droit sur **Default Domain Policy** puis sélectionnez **Modifier**.
- Développez le dossier **Stratégies** pour la configuration utilisateur puis effectuez un clic droit sur **Modèles d'administration** et cliquez sur **Ajout/Suppression de modèles**.
- Cliquez sur le bouton **Ajouter** et sélectionnez les fichiers d'administration d'Office.

Le fichier est téléchargeable depuis la page Informations générales.



- Cliquez sur **Fermer**.
- Développez le nœud **Modèles d'administration** dans **Configuration utilisateur**.
- Cliquez sur **Modèles d'administration classiques (ADM)**.



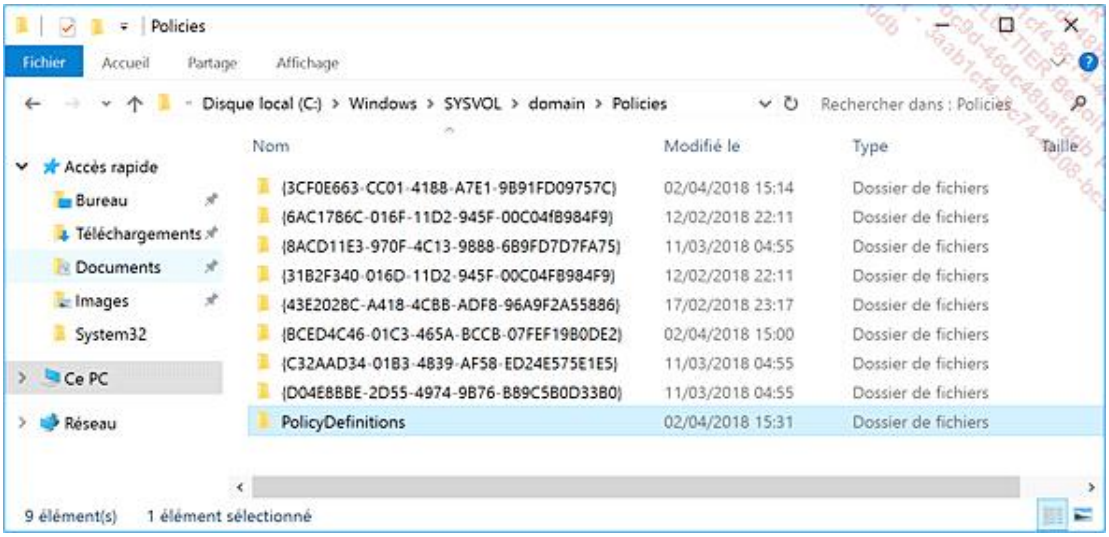
Les modèles d'administration ajoutés sont présents.

2. Création d'un magasin central

Le magasin central consiste à positionner les fichiers du modèle d'administration sur un point central. La console GPMC est ainsi redirigée vers ces fichiers.

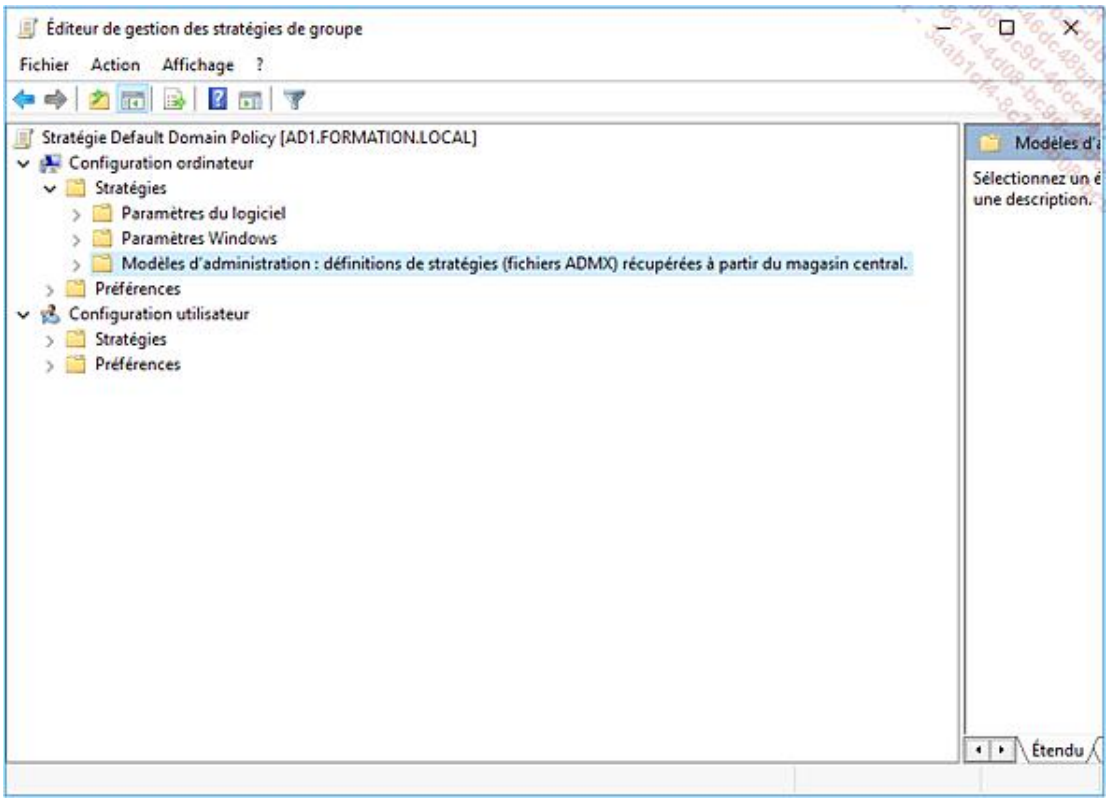
Les fichiers sont donc placés dans le dossier **SYSVOL**, ce qui implique la réplication sur les autres contrôleurs de domaine. Utile en cas d'utilisation d'un fichier ADMX personnalisé, cette fonctionnalité permet de s'assurer que l'ensemble des contrôleurs de domaine contiennent le fichier et surtout le fichier à jour.

- Lancez l'Explorateur Windows, cliquez sur **Ce PC** puis double cliquez sur **Disque local (C:)**.
- Double cliquez sur **Windows** puis copiez le dossier **PolicyDefinitions**.
- Double cliquez sur le dossier **SYSVOL** présent dans le répertoire **Windows**.
- Ouvrez les dossiers **domain** et **Policies** puis collez le répertoire.



- Lancez la console **Gestion de stratégie de groupes**.
- Développez les nœuds **Forêt**, **Domaines** puis **Formation.local**.
- Effectuez un clic droit sur **Defaut Domain Policy** et sélectionnez **Modifier**.
- Double cliquez sur **Stratégies** au niveau de la configuration ordinateur ou au niveau de la configuration utilisateur.

Les modèles d'administration sont bien récupérés depuis le magasin central.



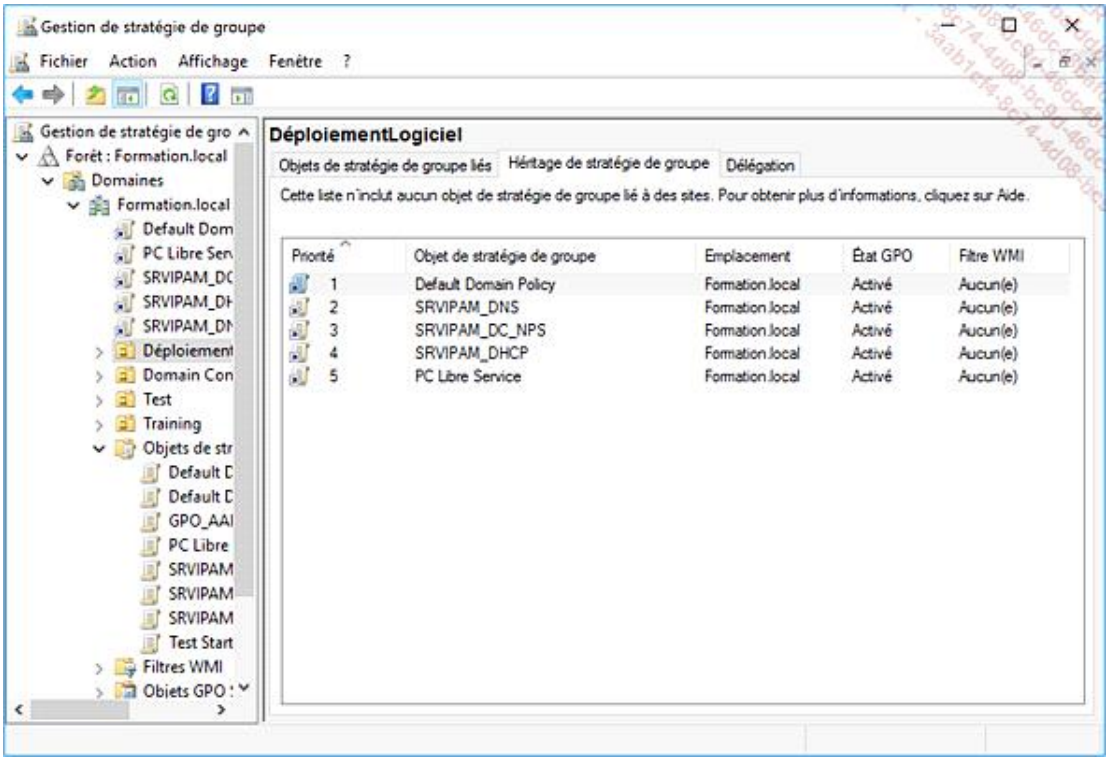
Gestion de l'héritage

L'héritage permet à un conteneur enfant de récupérer des paramètres configurés au-dessus de lui (sur le parent). La stratégie résultante peut donc être différente du résultat souhaité. Comme pour les autorisations NTFS, un conflit peut modifier le résultat final et donc supprimer une restriction configurée par l'administrateur.

Pour gérer l'héritage, il est possible de le bloquer ou à l'opposé d'appliquer la stratégie.

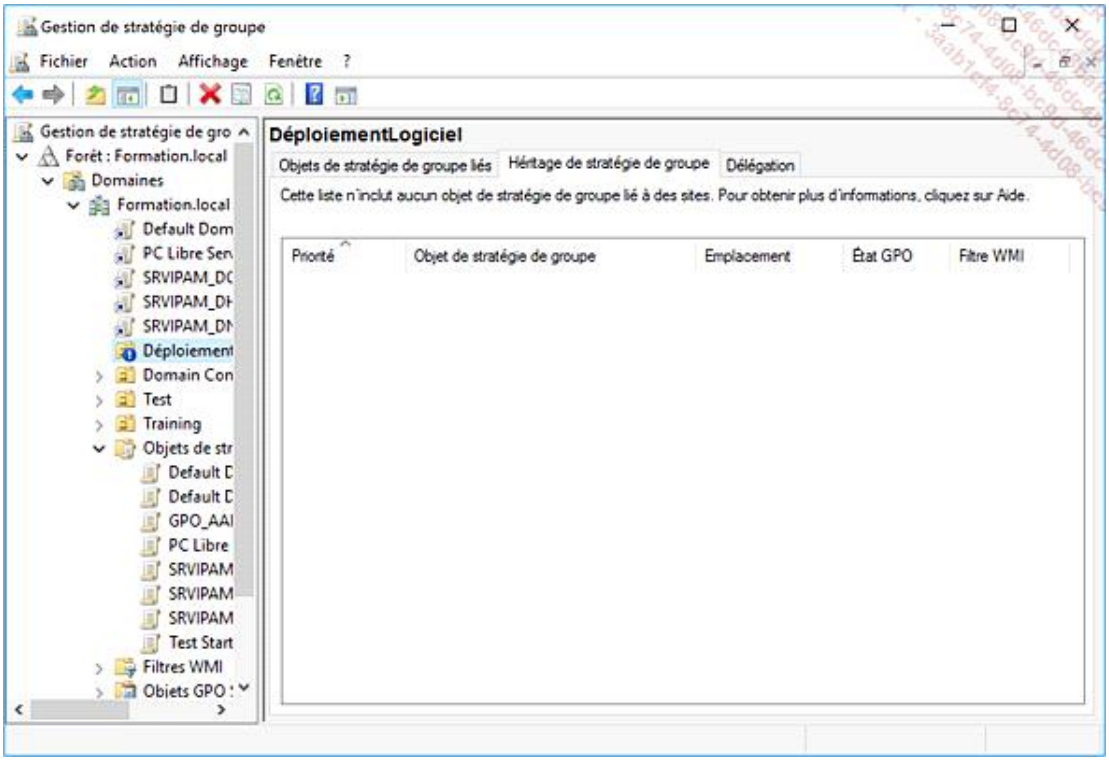
1. Blocage de l'héritage

Le blocage de l'héritage consiste à mettre en place un blocage à un certain niveau de l'arborescence. Cette fonctionnalité permet d'éviter les conflits (deux paramètres appliqués qui se contredisent) en s'assurant que les GPO configurées sur le parent ne sont pas attribuées à l'enfant. Pour vérifier l'ordre d'attribution des stratégies, l'onglet **Héritage de stratégie de groupe** doit être utilisé. Cet onglet est présent en cliquant sur une OU.



- Effectuez un clic droit sur l'OU **DéploiementLogiciel** puis sélectionnez l'option **Bloquer l'héritage**.

Aucune stratégie ne s'applique désormais sur l'OU.



Le rond bleu positionné sur l'icône de l'OU permet de signaler le blocage de l'héritage.

2. Appliquer une stratégie de groupe

L'option **Appliquer une stratégie de groupe** ne consiste pas à lier une GPO à une OU. Le but de cette option étant de s'assurer que la stratégie de groupe est désormais prioritaire en cas de conflit et passe outre le blocage d'héritage. Il est donc possible de donner l'option **Appliqué** à n'importe quelle stratégie de groupe afin d'obtenir le résultat souhaité.

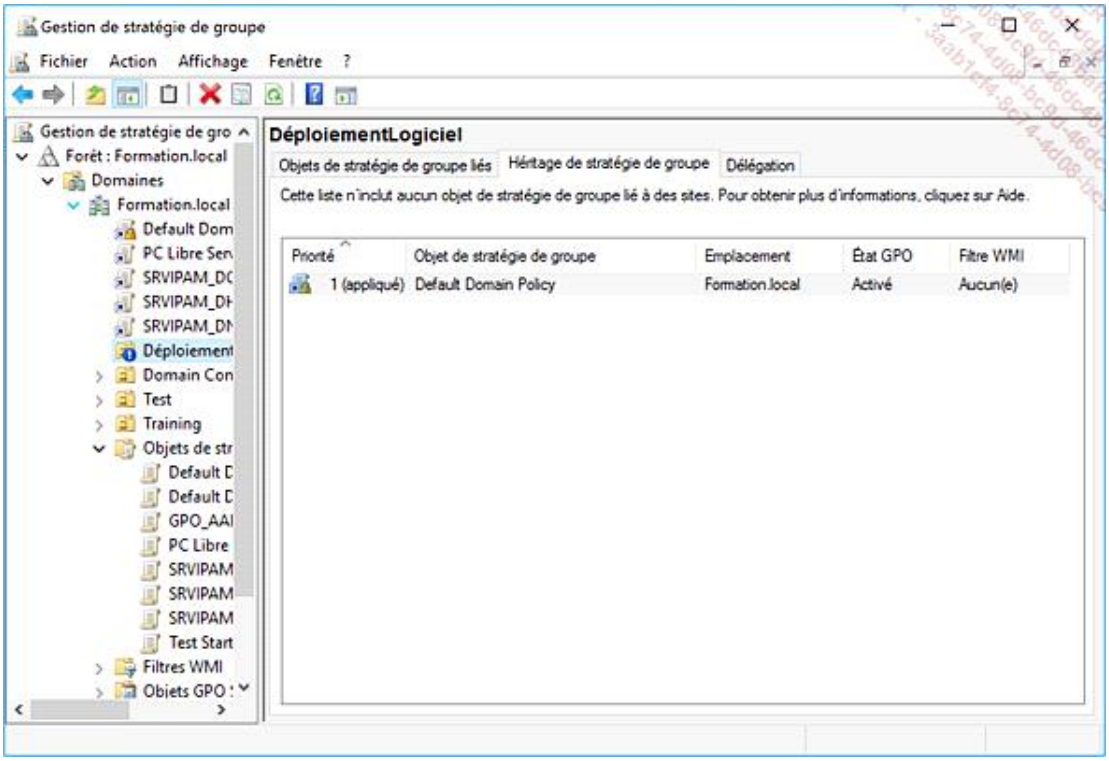
Dans le point précédent, nous avons pu visualiser qu'aucune stratégie ne s'applique si le blocage de l'héritage est activé.

- Effectuez un clic droit sur la stratégie **Default Domain Policy** puis sélectionnez **Appliqué**.

L'icône de la GPO a changé et le champ **Appliqué** possède maintenant la valeur **Oui**.

Si ce n'est pas déjà le cas, activez le blocage de l'héritage sur l'OU **DéploiementLogiciel**. Pour cela effectuez un clic droit puis sélectionnez l'option **Bloquer l'héritage**.

- Cliquez sur l'OU **DéploiementLogiciel** puis sur l'onglet **Héritage de stratégie de groupe**.



Seule la stratégie de groupe **Default Domain Policy** est présente.

- Enlevez le blocage d'héritage sur l'OU **DéploiementLogiciel**.

Les autres GPO sont maintenant présentes dans l'onglet **Héritage de stratégie de groupe**.

La **Default Domain Policy** a le numéro le plus petit dans le champ **Priorité**, ce qui la rend prioritaire.

Préférences de stratégies de groupe

1. Présentation des préférences de stratégies

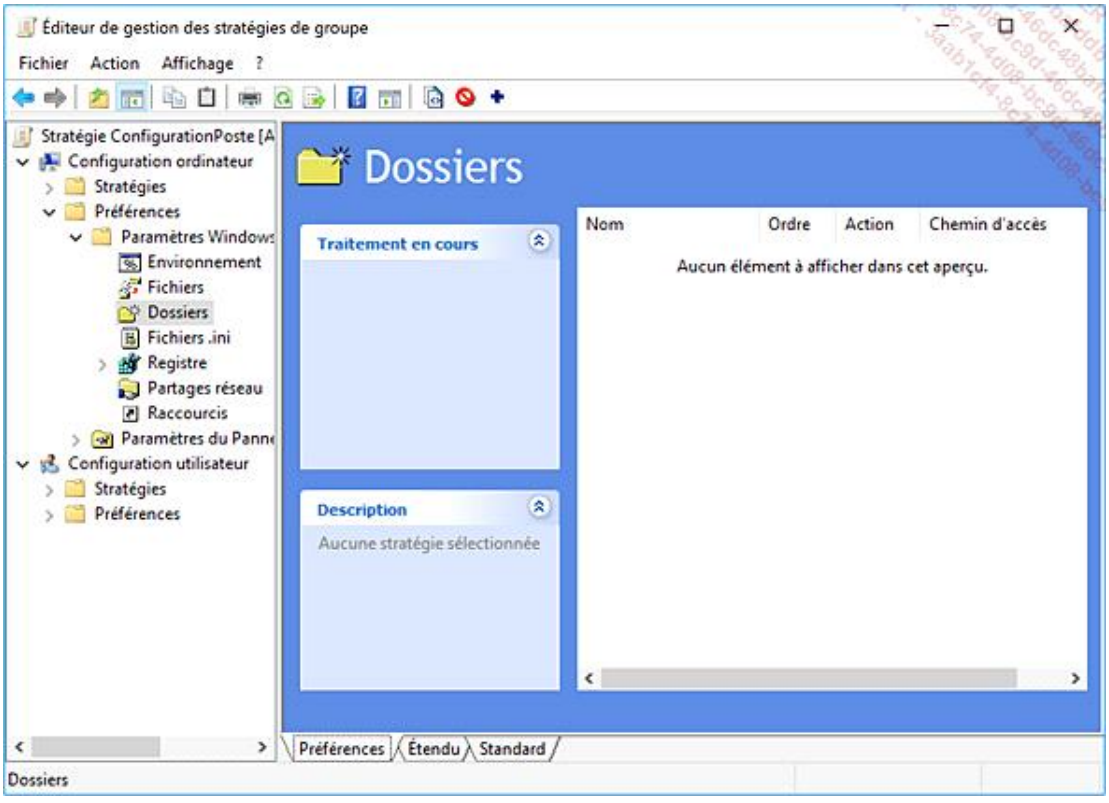
Les préférences de stratégies de groupe offrent aux administrateurs la possibilité de configurer de nouveaux paramètres. Il est maintenant possible de paramétrer les options des dossiers, les lecteurs mappés, les imprimantes, les tâches planifiées, les services, le menu Démarrer…

De plus, le ciblage offre une plus grande souplesse que les stratégies (GPO). Il est possible de cibler sur plusieurs éléments (système d'exploitation, plage d'adresses IP…).

Contrairement aux stratégies qui verrouillent l'interface utilisateur (l'utilisateur ne peut pas modifier le paramètre configuré par l'administrateur), les préférences laissent la possibilité à un utilisateur de le modifier. Prenons l'exemple du proxy IE : si vous configurez la connexion au proxy dans IE par les préférences, l'utilisateur a la possibilité d'annuler la connexion à un proxy lorsqu'il est en dehors de la société.

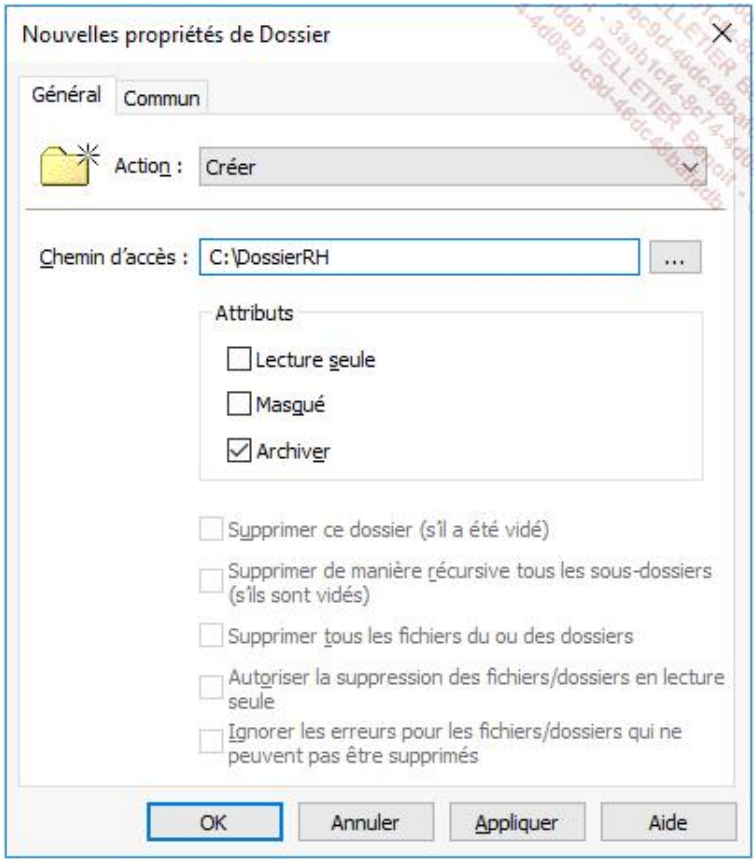
2. Configuration de paramètres avec les préférences

- Lancez la console **Gestion de stratégie de groupe**.
- Procédez à la création d'une GPO appelée **ConfigurationPoste** puis effectuez un clic droit sur cette dernière. Dans le menu contextuel, cliquez sur **Modifier**.
- La GPO doit être liée à la racine du domaine.
- Dans **Configuration ordinateur**, développez le nœud **Préférences**.
- Cliquez sur **Paramètres Windows** puis double cliquez sur **Dossiers**.



- Effectuez un clic droit sur **Dossiers** et dans le menu contextuel, cliquez sur **Nouveau** puis sur **Dossier**.

- Dans la liste déroulante, sélectionnez l'action **Créer**.
- Saisissez **C:\DossierRH** dans le champ **Chemin d'accès**.

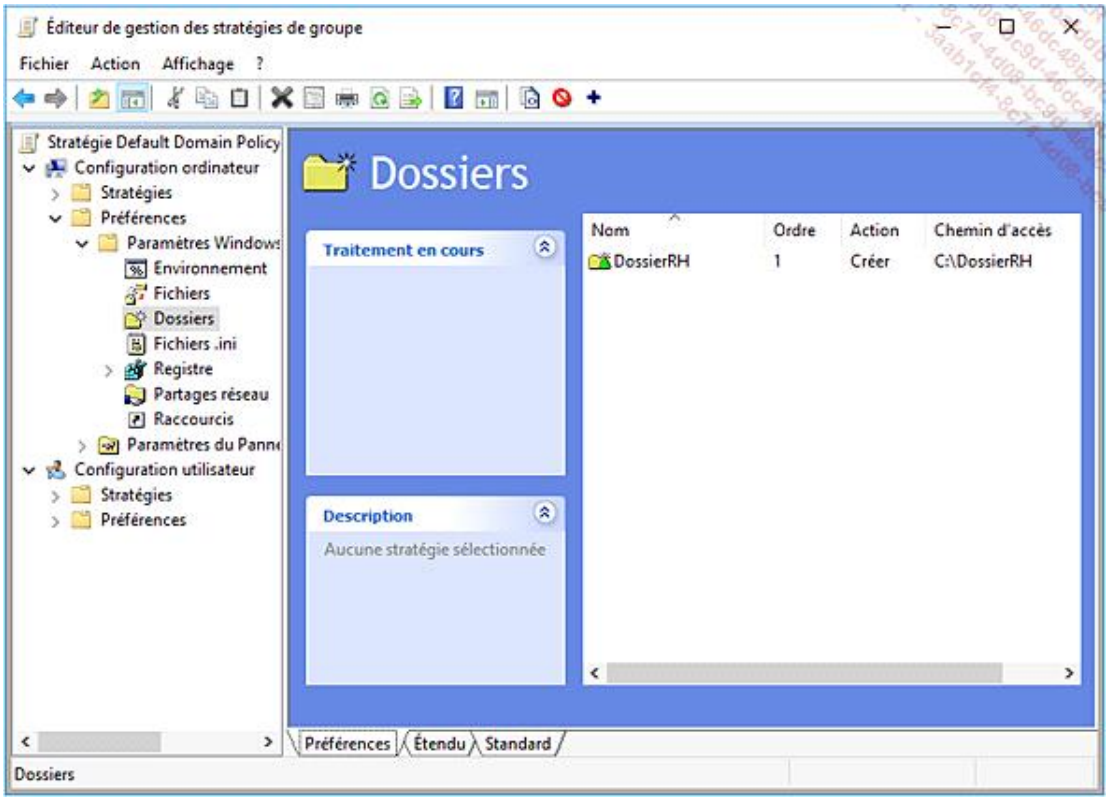


- Cliquez sur l'onglet **Commun** puis cochez l'option **Ciblage au niveau de l'élément**.
- Cliquez sur le bouton **Ciblage...**.
- Dans la fenêtre **Éditeur cible**, déroulez le menu **Nouvel élément** puis cliquez sur **Système d'exploitation**.

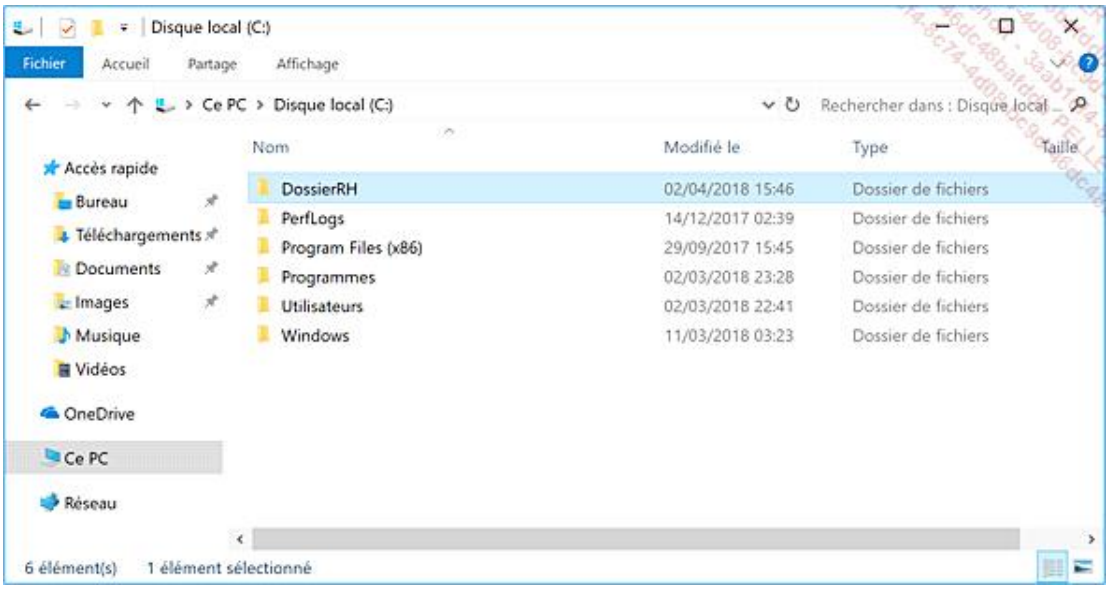
Le ciblage va être fait sur le système d'exploitation. Seuls les ordinateurs exécutant Windows 10 recevront le paramètre. Il est possible d'affiner le ciblage en sélectionnant une édition, une version ou un rôle d'ordinateur.

- Vérifiez la présence de **Windows 10** dans la liste déroulante **Produit** puis cliquez sur **OK**.
- Cliquez sur le bouton **Appliquer**, puis sur **OK**.

Une nouvelle ligne apparaît dans la console.



- Liez la stratégie de groupe à la racine du domaine.
- Sur le poste CL10-01, lancez une invite de commandes DOS.
- Exécutez la commande `gpupdate /force`.
- Lancez l'Explorateur Windows puis cliquez sur le lecteur **C:**.



- Recommencez la même opération sur le serveur SV1.

Le dossier n'est pas présent car le ciblage a été effectué sur le système d'exploitation. Il est donc nécessaire d'avoir un ordinateur exécutant Windows 10.

Exécution de script PowerShell avec une GPO

Comme nous l'avons vu précédemment, une stratégie de groupe est capable de déployer un lot de paramètres. Il est également possible de déployer des scripts.

Il est possible de retrouver une partie de ces scripts ici : http://bit.ly/2cPKCFr

1. Création d'un utilisateur local

La première étape est l'élaboration du script. Les différentes étapes sont détaillées ci-dessous, il est néanmoins possible de récupérer le script final (CompteLocal.ps1) depuis la page Informations générales.

Nous allons dans un premier temps définir les variables qui contiendront le nom du compte utilisateur local et celui de l'ordinateur.

```
$localUsers='LocalAdmin'
$ComputerName=$Env:COMPUTERNAME
```

Nous allons maintenant récupérer dans la variable $AllLocalAccounts l'ensemble des comptes utilisateurs présents dans la base SAM de l'ordinateur. Le nom de ce dernier est définit à l'aide de la variable $Computer.

```
$AllLocalAccounts = Get-WmiObject -Class Win32_UserAccount
-Namespace "root\cimv2" -Filter "LocalAccount='$True'"
-ComputerName $ComputerName -ErrorAction Stop
```

Si l'ordinateur contient un compte nommé LocalAdmin, le script s'arrête. Sinon Le compte est créé. Le mot de passe défini dans la variable $pass est utilisé pour l'utilisateur. Le compte local est ajouté au groupe Administrateurs de l'ordinateur local puis l'option "le mot de passe n'expire jamais" est configuré.

```
if($AllLocalAccounts.name -Contains $localUsers)
   {
       exit
   }
    else
    {
        Add-Type -Assembly System.Web
        $pass='Pa$$w0rd'
        NET USER LocalAdmin "$pass" /ADD /y
        NET LOCALGROUP "Administrateurs" "LocalAdmin" /add
        WMIC USERACCOUNT WHERE "Name='LocalAdmin'" SET
PasswordExpires=FALSE
     }
```

Le script PowerShell n'est pas signé, il est donc nécessaire de baisser le niveau de la politique de sécurité. Pour cela un fichier bat va être utilisé, ce dernier sera configuré dans la GPO. Son rôle sera l'exécution du script et la configuration de la politique d'exécution.

La commande contenue dans ce fichier est la suivante :

```
Powershell -ExecutionPolicy Bypass -file
```

```
\\Formation.local\SysVol\Formation.local\scripts\ CompteLocal.ps1
```

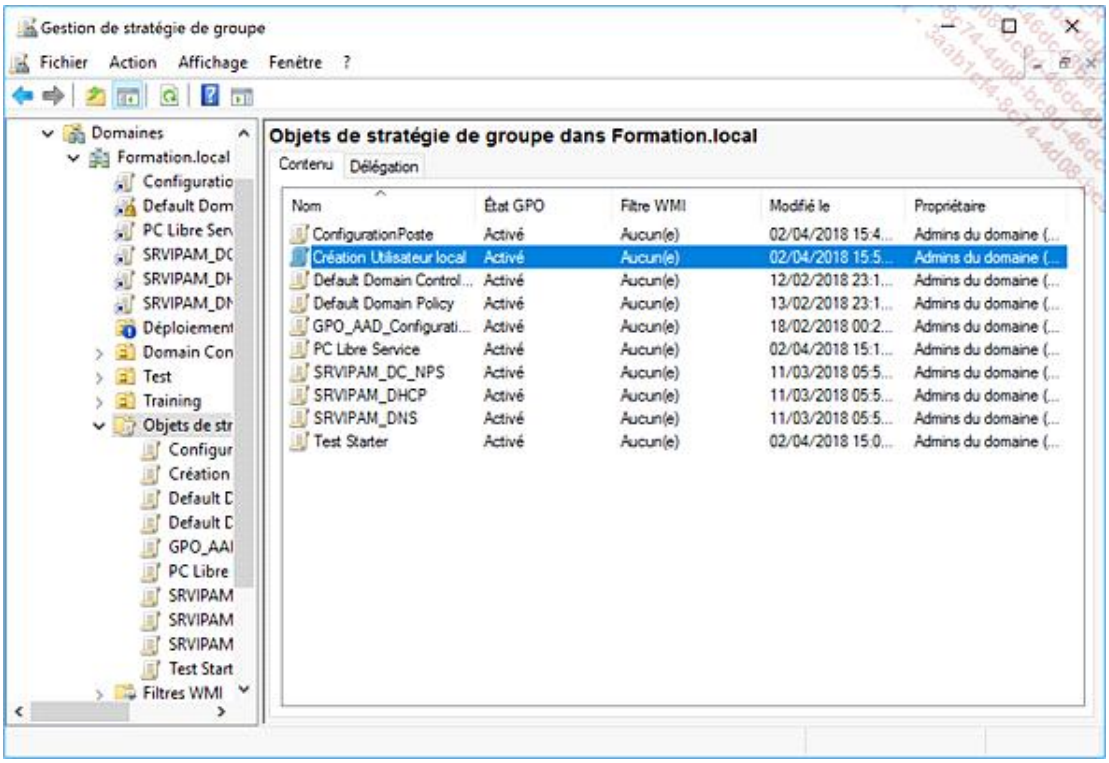


Les fichiers (ps1 et bat) peuvent maintenant être copiés dans le chemin UNC suivant : \\Formation.local\SysVol\Formation.local\scripts\

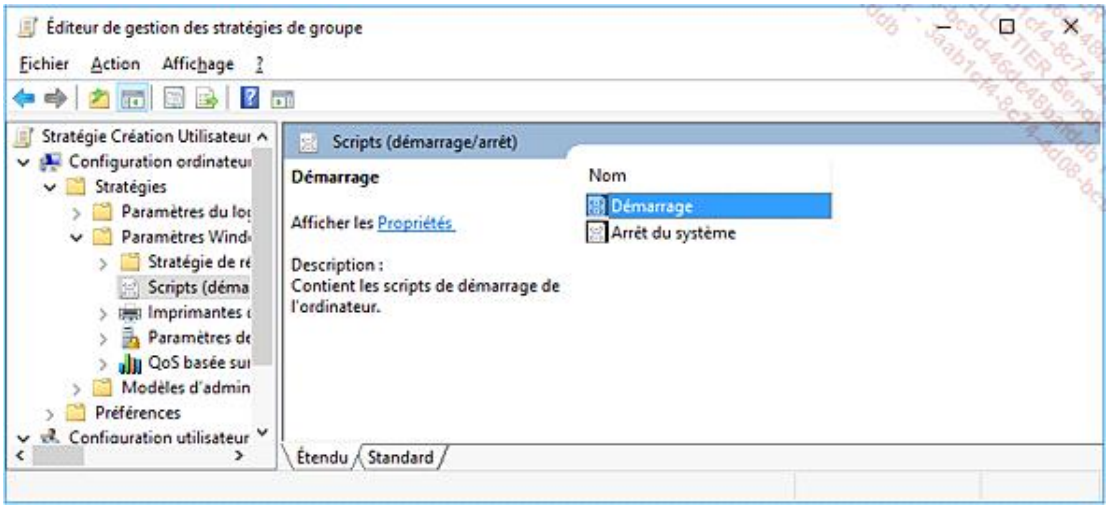
La création de la stratégie de groupe peut maintenant être effectuée.

- Sur **AD1**, ouvrez la commande **Gestion de stratégie de groupe**.
- Effectuez un clic droit sur **Objet de stratégie de groupe**, puis sélectionnez l'option **Nouveau** dans le menu contextuel.
- Dans le champ **Nom** saisissez **Création Utilisateur local** puis cliquez sur **OK**.

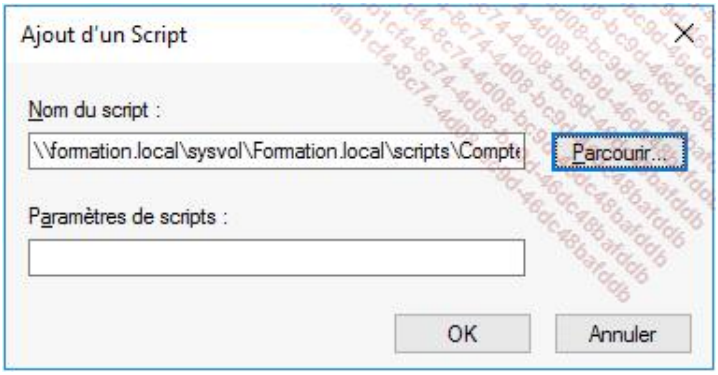
La stratégie de groupe est maintenant présente dans la console.



- Effectuez un clic droit sur la GPO puis, dans le menu contextuel, cliquez sur **Modifier**.
- Dans la console **Éditeur de gestion des stratégies de groupe**, développez les nœuds **Configuration ordinateur** - **Stratégies** - **Paramètres Windows** - **Scripts**.



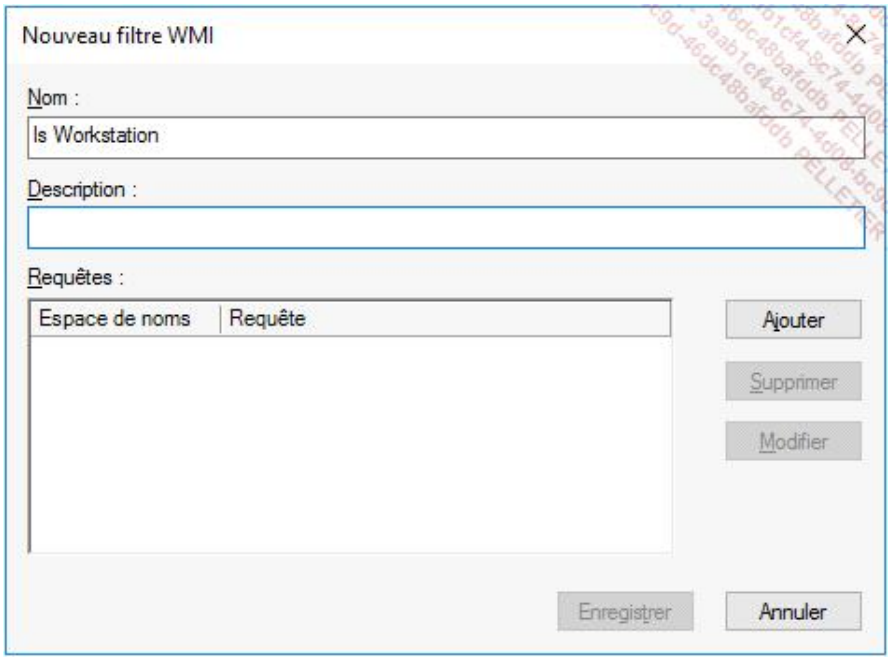
- Effectuez un double clic sur **Démarrage** puis cliquez sur **Ajouter**.
- À l'aide du bouton **Parcourir**, sélectionnez le fichier bat présent dans **\\Formation.local\SysVol\Formation.local\scripts**.



- Cliquez deux fois sur **OK** puis fermez la console **Éditeur de gestion des stratégies de groupe**.

Nous allons positionner la GPO au niveau de la racine du domaine puis filtrer à l'aide d'un filtre WMI.

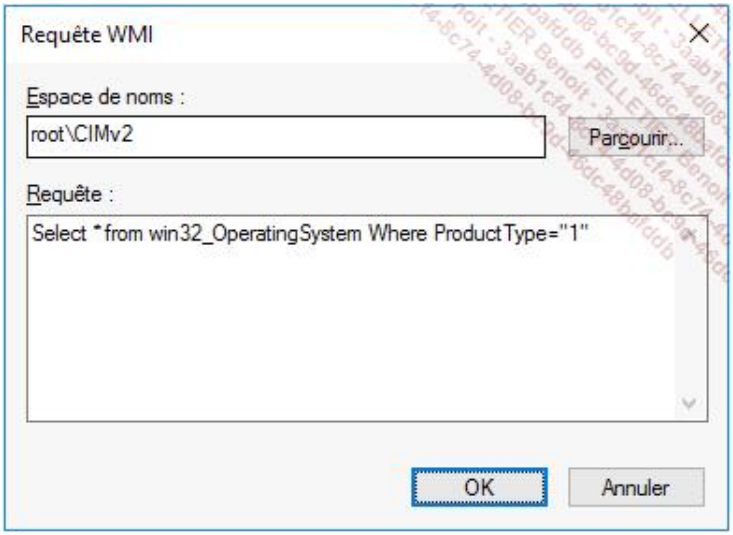
- Depuis la console **Gestion de stratégie de groupe**, effectuez un clic droit sur **Filtres WMI**. Dans le menu contextuel, cliquez sur **Nouveau**.
- Saisissez **Is Workstation** dans le champ **Nom** puis cliquez sur **Ajouter**.



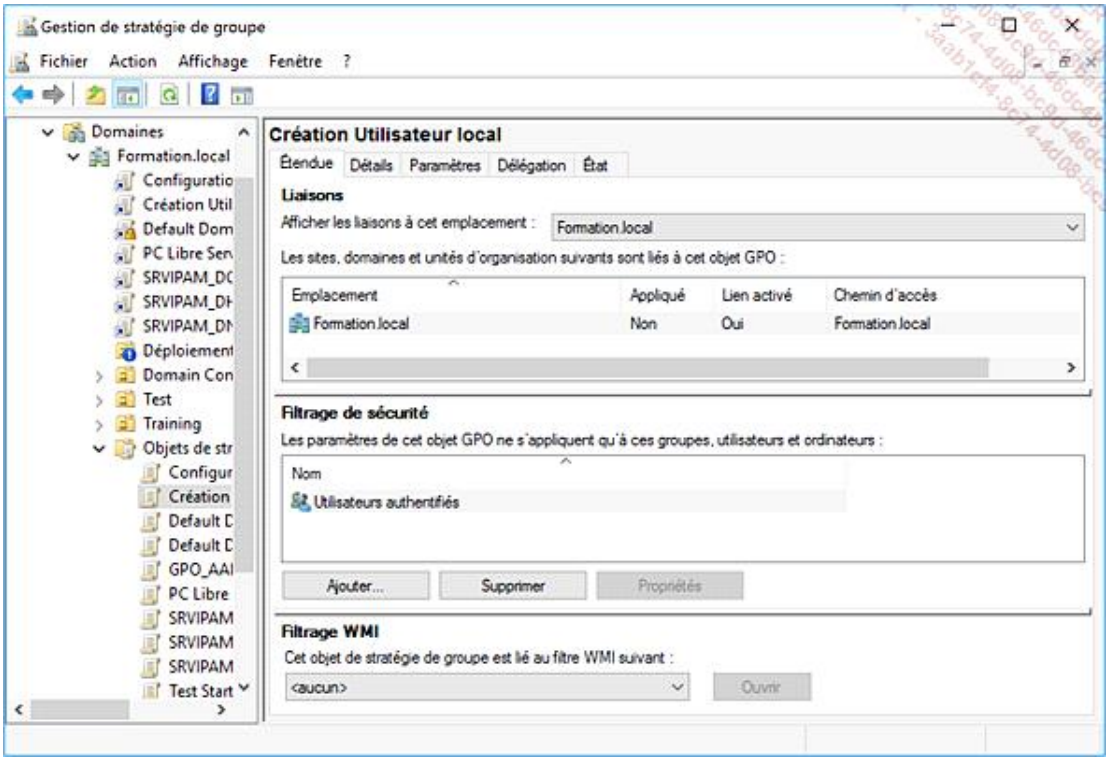
- Dans le champ **Requêtes**, saisissez la requête suivante :

```
Select * from win32_OperatingSystem Where ProductType="1"
```

Cela permet d'appliquer la GPO à des postes de travail uniquement.

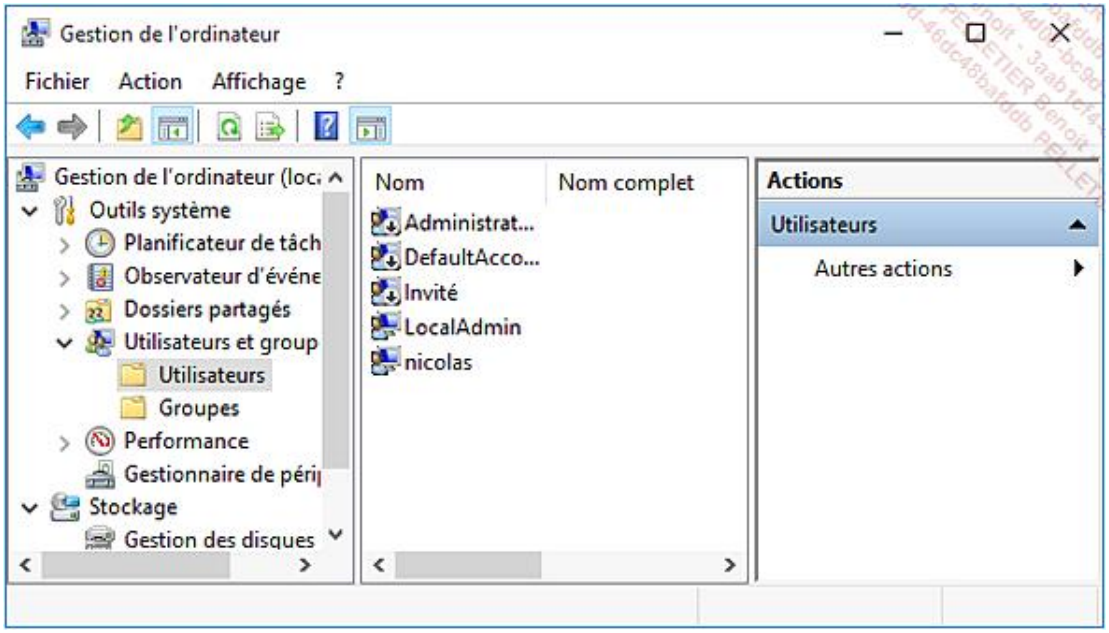


- Cliquez sur **OK**, puis validez le message d'avertissement en cliquant sur **OK**.
- Cliquez sur **Enregistrer** pour sauvegarder le filtre WMI.
- Sélectionnez la GPO puis, dans la liste déroulante **Filtrage WMI**, sélectionnez le filtre créé précédemment.
- Validez le message d'information et placez la GPO à la racine du domaine.



Sur **CL10-01** et **SV1**, exécutez la commande **gpupdate /force** puis redémarrez les deux serveurs.

Le compte est bien présent sur CL10-01.



Il est par contre absent du serveur **SV1**.

2. Modification du mot de passe

Comme pour la création du compte utilisateur local, il est nécessaire dans un premier temps d'élaborer le script PowerShell. Les différentes étapes sont détaillées ci-dessous, il est néanmoins possible de récupérer le script final (ModifMDP.ps1) depuis la page Informations générales.

Afin de ne réaliser la modification qu'une seule fois, nous allons tester si la clé _DeleteMe2 existe. Si cette dernière est présente le script a déjà été exécuté une première fois.

```
$RegKeyexiste = Test-Path HKLM:\Software\_DeleteMe2
```

La variable `$RegKeyexiste` est testée, si elle contient la valeur true, alors l'exécution du script est arrêtée car le mot de passe a déjà été modifié.

Dans le cas contraire, on récupère le mot de passe souhaité dans la variable `$pass` puis on effectue la modification. Par la suite on procède à la création de la clé.

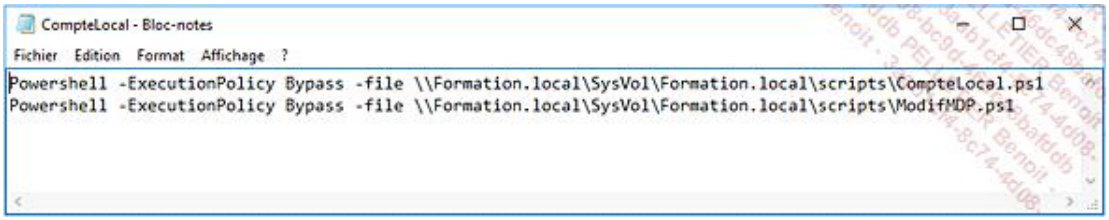
```
if($RegKeyexiste -eq $true)
{
   Exit
}
else
{
    $pass='Pa$$w0rd'
    $strComputer='localhost'

    $admin=[adsi]("WinNT://" + $strComputer + "/LocalAdmin, user")

    $admin.psbase.invoke("SetPassword", "Pa$$w0rd")
    New-Item -Path HKLM:\Software\_DeleteMe2
}
```

- Copiez le fichier **ModifMDP.ps1** dans **\\Formation.local\SysVol\Formation.local\scripts**.
- Modifiez le fichier bat présent au même emplacement afin qu'il comporte la ligne suivante :

```
Powershell -ExecutionPolicy Bypass -file
\\Formation.local\SysVol\Formation.local\scripts\ModifMDP.ps1
```



- Sur le poste **CL10-01**, exécutez la commande **gpupdate /force** puis redémarrer le poste.
- Au redémarrage, ouvrez une session en tant que **.\localadmin** avec le mot de passe **Pa$$w0rd** (sauf changement de votre part dans le script).

La session s'ouvre correctement.

Les stratégies par défaut

Lors de la création d'un domaine Active Directory, deux stratégies sont créées par défaut. Il est préférable de ne pas toucher à ces stratégies de groupe, préférez donc la création d'une nouvelle stratégie de groupe.

La Default Domain Policy est positionnée à la racine du domaine. Elle s'applique à l'ensemble des unités d'organisation du domaine et contient les paramètres de sécurité (paramètres de mot de passe et de verrouillage). Il est également possible de configurer des paramètres communs à tous les objets du domaine ou des paramètres d'audit.

La Default Domain Controller Policy est liée à l'unité d'organisation Domain Controllers. Elle s'applique uniquement aux serveurs ayant le rôle d'annuaire AD. Les paramètres contenus dans cette stratégie sont donc à destination des contrôleurs du domaine. Plusieurs types de paramètres peuvent être configurés :

- **Stratégie d'affectation des droits** : les paramètres permettent d'attribuer des droits supplémentaires à un utilisateur (Arrêter le système, Autoriser l'ouverture de session par les services Bureau à distance…).
- **Stratégie d'option de sécurité** : la configuration des paramètres d'Audit (modification effectuée dans le service d'annuaire…) ainsi que d'autres paramètres peut être effectuée.

Les stratégies d'audit

1. Introduction

L'audit permet l'enregistrement d'une entrée dans le journal d'événements lorsqu'un utilisateur effectue une action (accès à une ressource, etc.). Ainsi il est possible de voir l'action effectuée, le compte utilisateur associé ainsi que la date et l'heure de l'action. Il est possible d'auditer deux actions, celles ayant échoué ou celles ayant réussi.

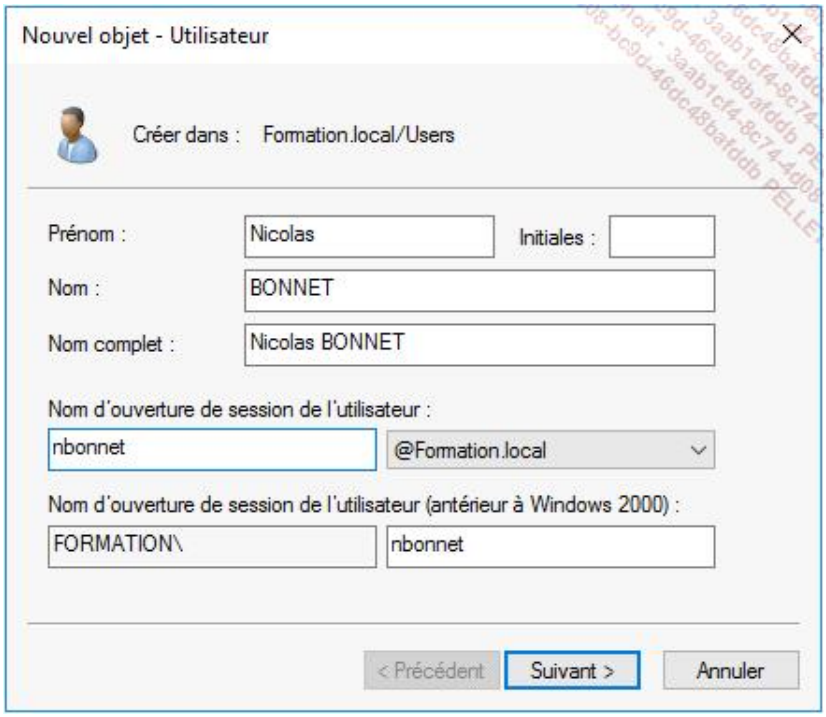
Les audits de sécurité ont un rôle important, les données qu'ils fournissent permettent de déceler une faille de sécurité potentielle (mauvaise ACL positionnée…).

Plusieurs événements peuvent être audités :

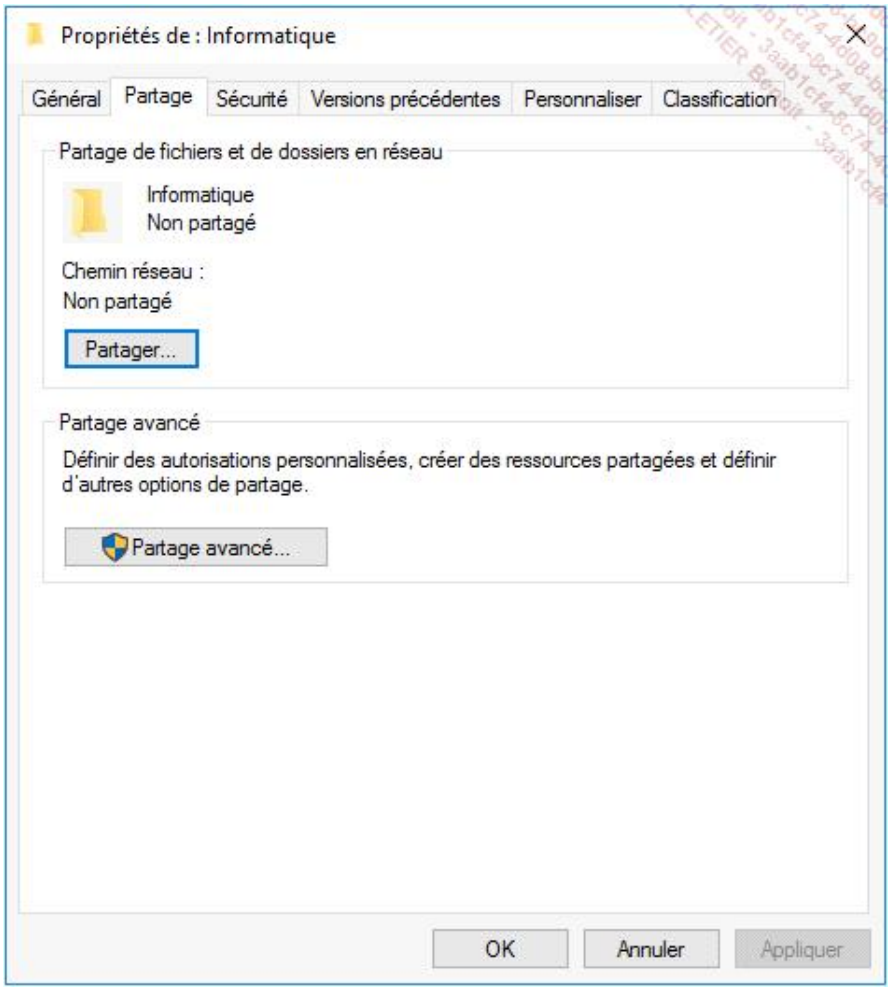
- **Événements de connexion aux comptes** : ce type d'audit permet de connaître chaque connexion et déconnexion d'un compte utilisateur ou ordinateur autre que celui qui enregistre l'événement et valide le compte. Lors de l'activation de l'audit des succès, une entrée est générée à chaque ouverture de session réussi. Ce paramètre permet d'effectuer des recherches après un incident. En cas d'audit des échecs, une entrée est cette fois générée lorsque la tentative d'ouverture de session du compte échoue. Ces informations sont utiles pour la détection des intrusions.
- **Auditer la gestion des comptes** : un événement est généré lorsqu'une modification est effectuée sur un compte (création, modification et suppression d'un compte utilisateur, compte utilisateur renommé, désactivé ou activé, mot de passe modifié…). Lors de l'activation des réussites, un événement est généré lorsqu'une modification a pu être effectuée. Il est donc plus aisé de trouver qui a effectué l'opération. L'audit des échecs permettra d'avoir connaissance d'éventuelles tentatives de modification infructueuses.
- **Auditer l'accès au service d'annuaire** : il est possible d'effectuer l'audit d'un objet AD (modification d'un objet utilisateur, …) à l'aide de ce paramètre. Pour cela, il faut modifier la liste de contrôle d'accès système (SACL) de l'objet à auditer. Cette dernière permet de déterminer les comptes dont les actions doivent être auditées.
- **Auditer les événements de connexion** : ce paramètre permet d'auditer chaque connexion ou déconnexion d'un utilisateur. Les tentatives de connexion vers l'ordinateur sur lequel l'audit est activé vont impliquer la création d'une entrée dans le journal. Lors de l'activation du paramètre sur le contrôleur de domaine, aucun audit de connexion n'est généré sur les postes du domaine lors des différentes tentatives d'ouverture de session. Pour cela, il est nécessaire d'effectuer une ouverture de session de type interactive ou via le réseau sur le contrôleur de domaine pour générer un événement. Les événements de connexion aux comptes sont générés sur le serveur d'annuaire. Les événements de connexion sont eux créés à l'endroit où la tentative est effectuée.
- **Auditer l'accès aux objets** : ce paramètre permet d'auditer l'accès à un objet (fichier, dossier…) qui contient une liste de contrôle d'accès système (SACL).

2. Auditer les accès aux dossiers partagés

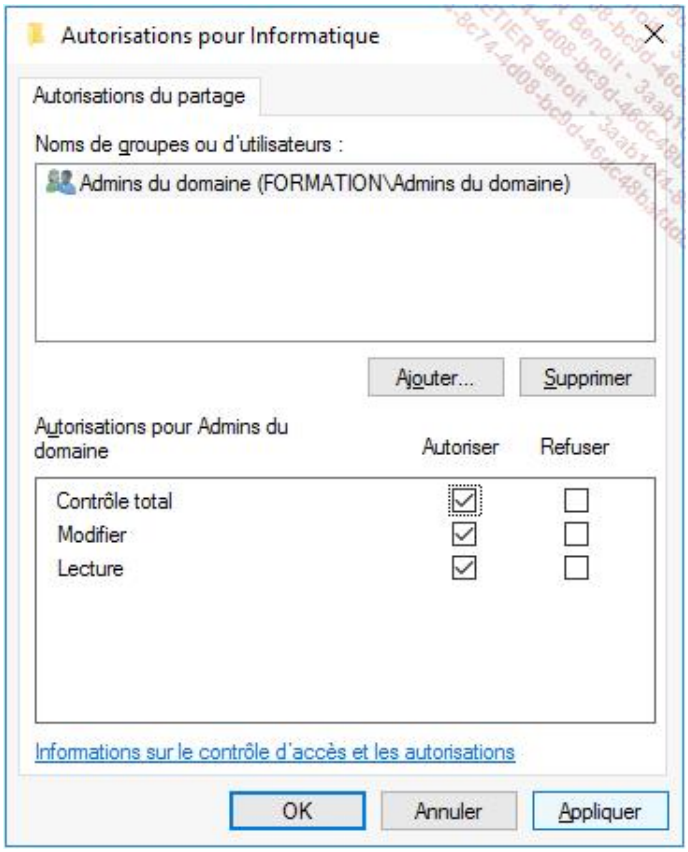
- Sur le serveur **AD1**, lancez la console **Utilisateurs et ordinateurs Active Directory**.
- Effectuez un clic droit sur l'unité d'organisation **Users** puis cliquez sur **Nouveau** -**Utilisateur**.
- Saisissez **Nicolas** dans le champ **Prénom**, **BONNET** dans le champ **Nom** et **nbonnet** dans **Nom d'ouverture de session**.



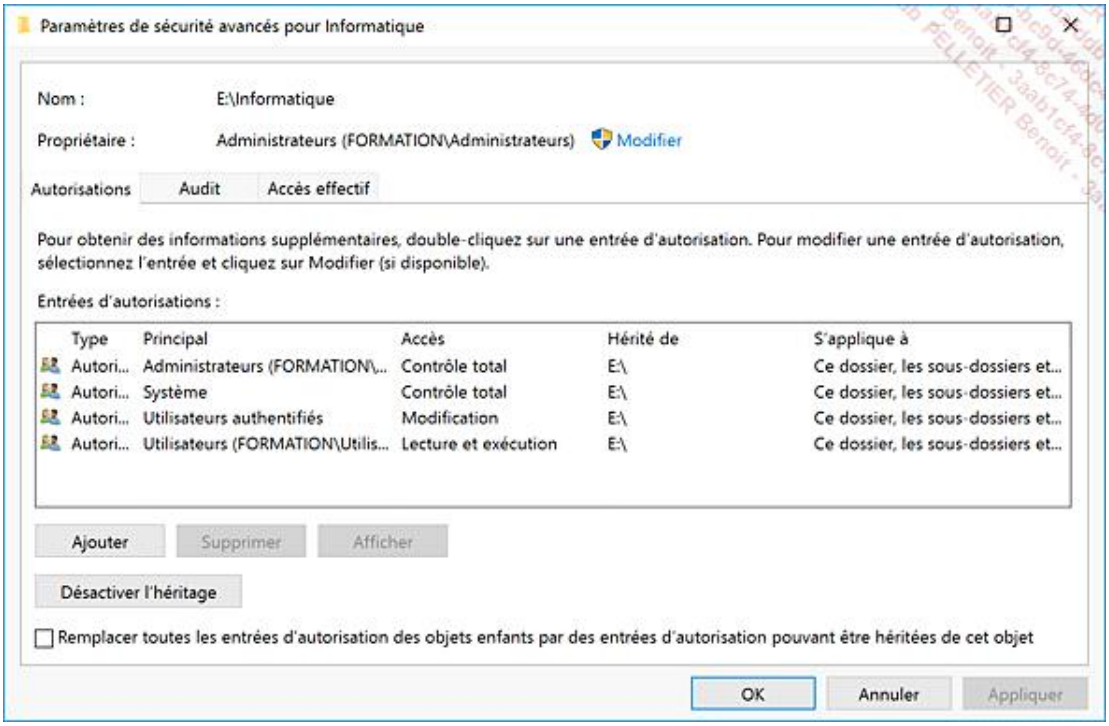
- Cliquez sur **Suivant**.
- Dans le champ **Mot de passe** saisissez **Pa$$w0rd** puis confirmez.
- Décochez la case **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**.
- Cochez la case **L'utilisateur ne peut pas changer de mot de passe**.
- Cliquez sur **Suivant** puis sur **Terminer**.
- Sur **SV1**, créez un dossier nommé **Informatique** sur la partition **E:**.
- Accédez aux **Propriétés** du dossier puis cliquez sur l'onglet **Partage**.



- Cliquez sur le bouton **Partage avancé**.
- Dans la fenêtre **Partage avancé**, cochez la case **Partager ce dossier**.
- Cliquez sur le bouton **Autorisations**, puis supprimez l'entrée **Tout le monde**.
- Ajoutez le compte **Admins du domaine** puis attribuez-lui le droit **Contrôle total**.

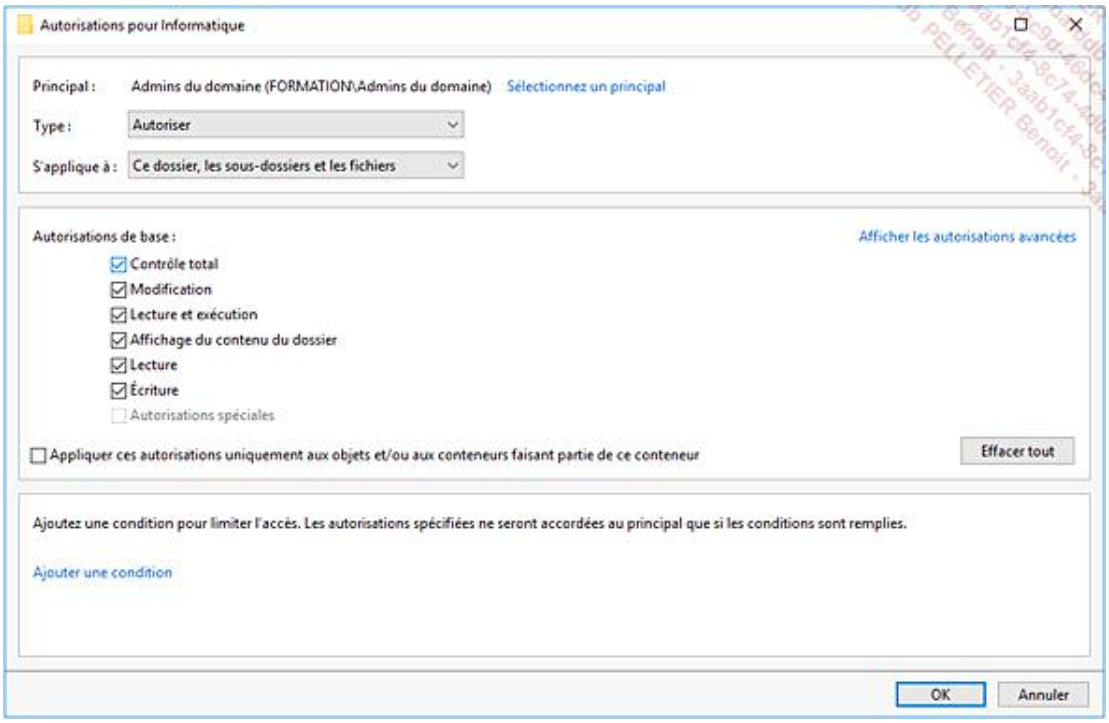


- Cliquez sur **Appliquer** puis deux fois sur **OK**.
- Dans la fenêtre des propriétés du dossier **Informatique**, cliquez sur l'onglet **Sécurité**.
- Cliquez sur le bouton **Avancé** puis sur **Désactiver l'héritage**.

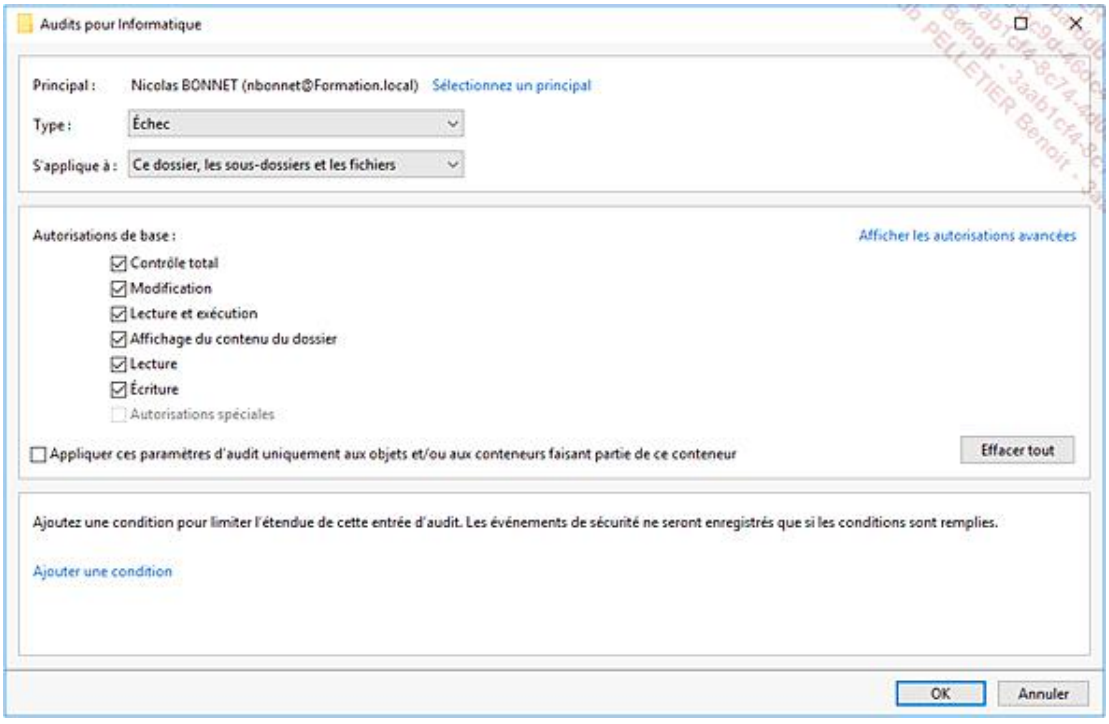


- Cliquez sur **Supprimer toutes les autorisations héritées de cet objet**.
- Cliquez sur **Ajouter** puis sur le lien **Sélectionner un principal**.

- Dans la fenêtre de sélection, saisissez **Admins du domaine** puis cliquez sur **Vérifier les noms**.
- Cliquez sur **OK** puis donnez à l'utilisateur le droit **Contrôle total**.



- Cliquez sur **OK** puis sur **Appliquer**.
- Dans l'onglet **Audit**, cliquez sur **Ajouter**.
- Cliquez sur le lien **Sélectionnez un principal** puis saisissez **nbonnet**.
- Cliquez sur **Vérifier les noms** puis sur **OK**.
- Dans la liste déroulante **Type**, sélectionnez **Échec** puis cliquez sur le droit **Contrôle total**.

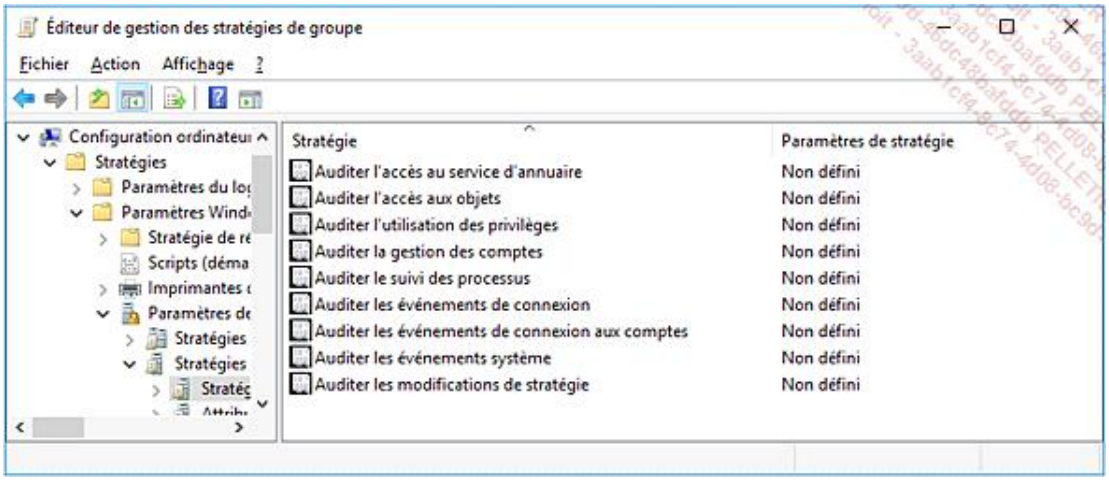


- Cliquez deux fois sur **OK** puis cliquez sur **Fermer**.

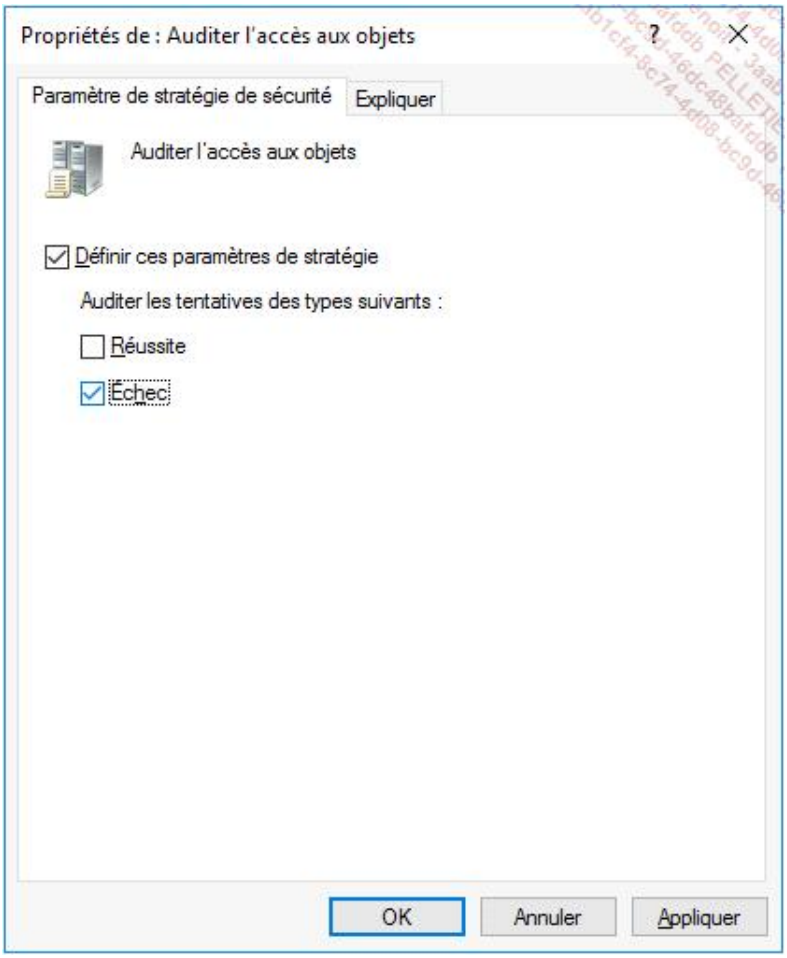
- Sur AD1, lancez la console **Gestion de stratégie de groupe** puis effectuez un clic droit sur **Objet de stratégie de groupe**.
- Dans le menu contextuel, choisissez l'option **Nouveau**.
- Saisissez **Audit dossier Informatique** dans le champ **Nom** puis cliquez sur **OK**.
- Effectuez un clic droit sur la stratégie puis sélectionnez l'option **Modifier**.

La console **Éditeur de gestion des stratégies de groupe** se lance.

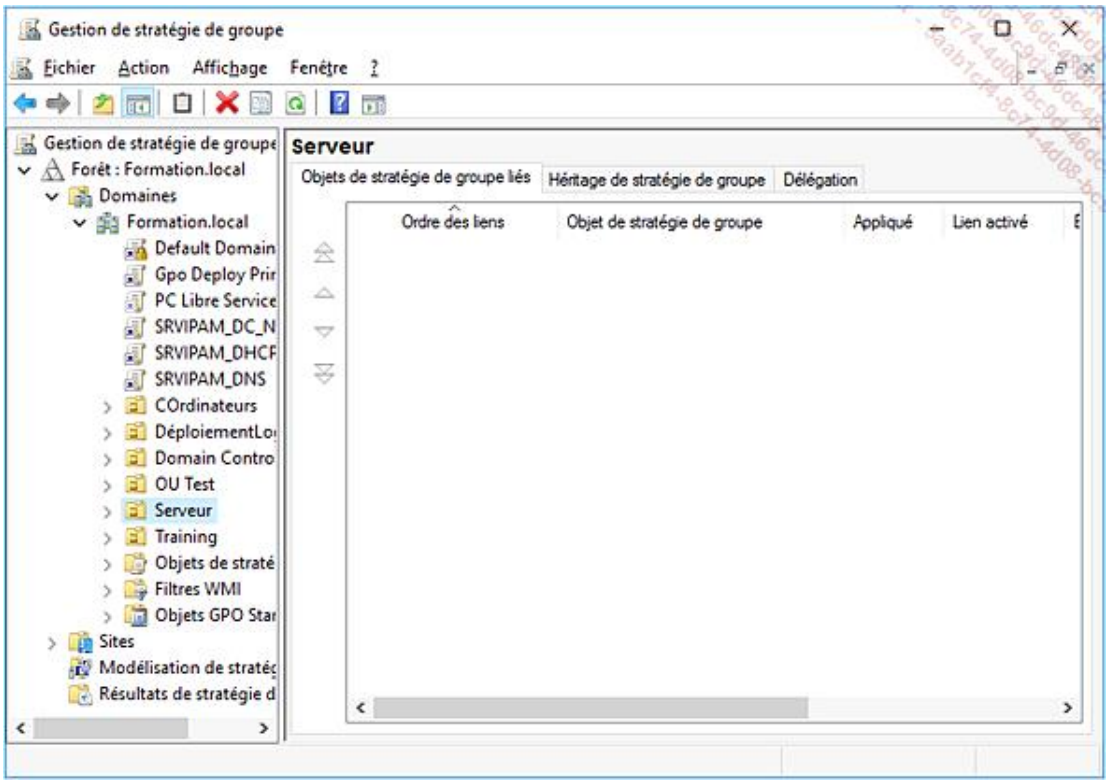
- Développez les nœuds **Configuration ordinateur**, **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, **Stratégies locales** et **Stratégie d'audit**.



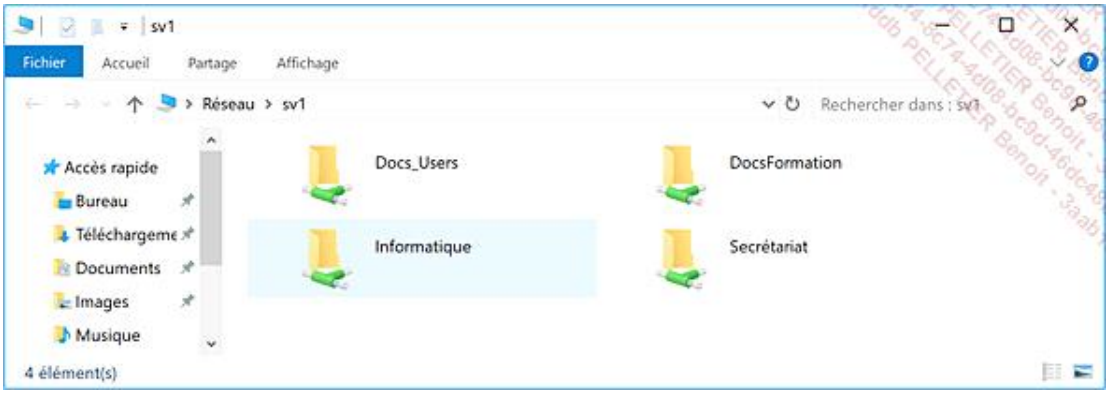
- Double cliquez sur **Auditer l'accès aux objets**, cochez **Définir ces paramètres de stratégie** et sélectionnez la case **Échec**.



- Cliquez sur **Appliquer** puis **OK**.
- Fermez la console **Éditeur de stratégie de groupe**.
- Depuis la console **Gestion de stratégie de groupe**, créez une unité d'organisation nommée **Serveur**.

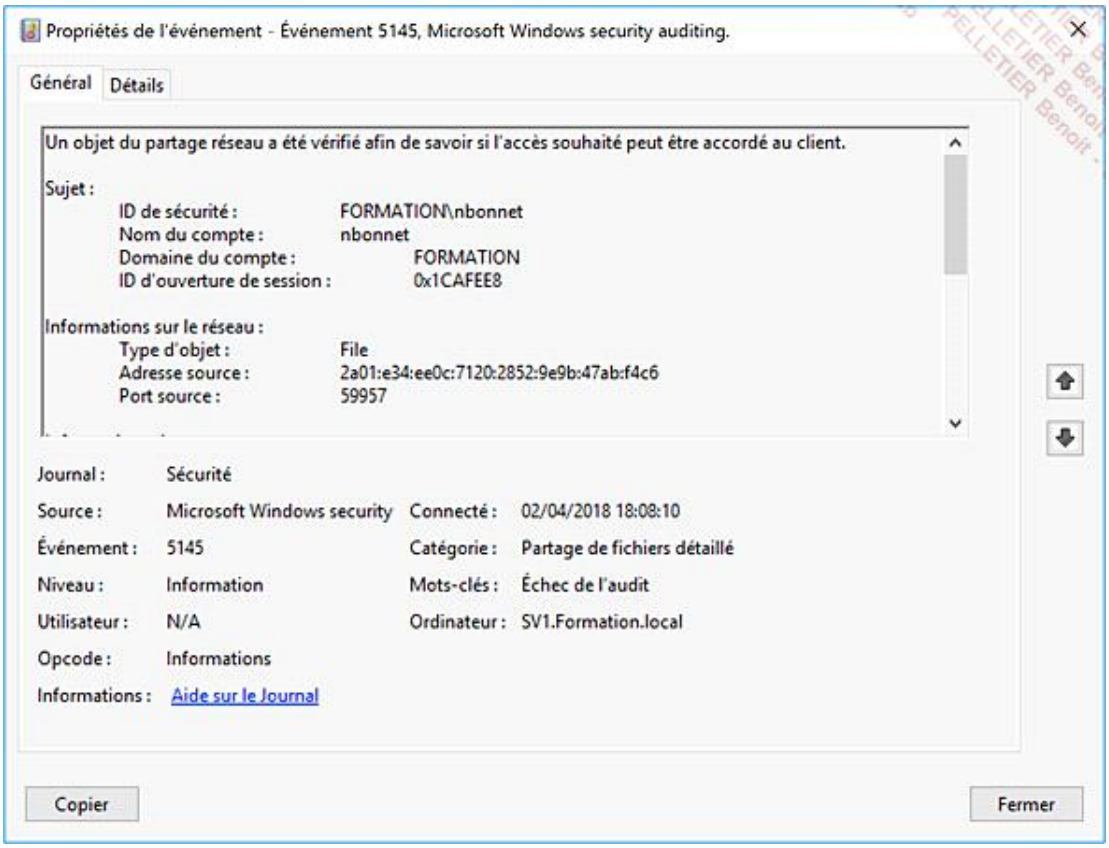


- Liez la stratégie **Audit dossier Informatique** à cette unité d'organisation.
- Déplacez le compte ordinateur de SV1 dans l'OU **Serveur**.
- Sur SV1, lancez une invite de commandes DOS et exécutez la commande `gpupdate /force`.
- Ouvrez une session en tant que **nbonnet** (mot de passe **Pa$$w0rd**) sur **CL10-01**.
- Essayez d'accéder au répertoire partagé **Informatique** présent sur SV1.



Un message d'avertissement informant d'un accès refusé s'affiche.

- Sur SV1, lancez la console **Gestion de l'ordinateur** puis développez les nœuds **Observateur d'événements** puis **Journaux Windows**.
- Visualisez le journal d'événements **Sécurité**.
- Ouvrez l'événement qui référence la tentative d'accès de **nbonnet** (**ID 5145**).



L’audit a fonctionné et les événements sont présents dans le journal.

Gestion de la sécurité

Une stratégie de sécurité englobe des paramètres concernant principalement la politique de mot de passe et de verrouillage. Ces paramètres sont configurés dans la **Default Domain Policy** afin que l'ensemble des objets du domaine AD reçoive cette politique.

La stratégie de mot de passe englobe les paramètres suivants :

- **Complexité du mot de passe** : si elle est activée, le mot de passe doit posséder au minimum trois des quatre catégories suivantes : des lettres minuscules, des lettres majuscules, des chiffres et des caractères spéciaux. En plus, le mot de passe ne doit pas contenir tout ou une partie du nom du compte utilisateur et compter un minimum de six caractères.
- **Durée de vie des mots de passe** : des durées de vie minimale et maximale sont configurées. Le temps minimum bloque le changement de mot de passe par l'utilisateur, ce dernier pourra donc effectuer l'action une fois la durée passée. La durée maximale permet de mettre une limite à l'utilisation du mot de passe : une fois le délai passé, il est nécessaire de le changer.

Si la durée minimale est de 1 jour et que l'utilisateur change son mot de passe, il ne pourra pas le modifier avant le lendemain.

- **Longueur du mot de passe** : ce paramètre permet de déterminer le nombre minimum de caractères du mot de passe. Si le nombre de caractères dans le mot de passe saisi par l'utilisateur est inférieur à celui défini dans le paramètre, le changement est refusé par le contrôleur de domaine.
- **Historique des mots de passe** : afin de s'assurer qu'un utilisateur ne saisit pas le même mot de passe que l'ancien lors du changement, l'historique des mots de passe doit être configuré. Il permet d'interdire les x derniers mots de passe de l'utilisateur. La valeur x est celle saisie par l'administrateur dans le paramètre de la stratégie.
- **Utilisation du chiffrement réversible** : ce paramètre permet l'enregistrement du mot de passe en utilisant un chiffrement réversible. Ce dernier est identique au stockage des versions des mots de passe en texte clair.

La stratégie de verrouillage englobe elle des paramètres différents :

- **Durée de verrouillage des comptes** : permet de déterminer le nombre de minutes pendant lesquelles le compte reste verrouillé. Ce délai passé, le déverrouillage est automatique si la valeur est différente de 0. Dans le cas contraire, un administrateur doit exécuter l'action manuellement.
- **Réinitialiser le compteur de verrouillage du compte après** : définit le temps en minutes après lequel le compteur d'échecs est mis à 0. La valeur doit être inférieure ou égale à la durée de verrouillage.
- **Seuil de verrouillage de comptes** : définit le nombre de tentatives infructueuses (au niveau de l'ouverture de session) au bout duquel le compte est verrouillé.

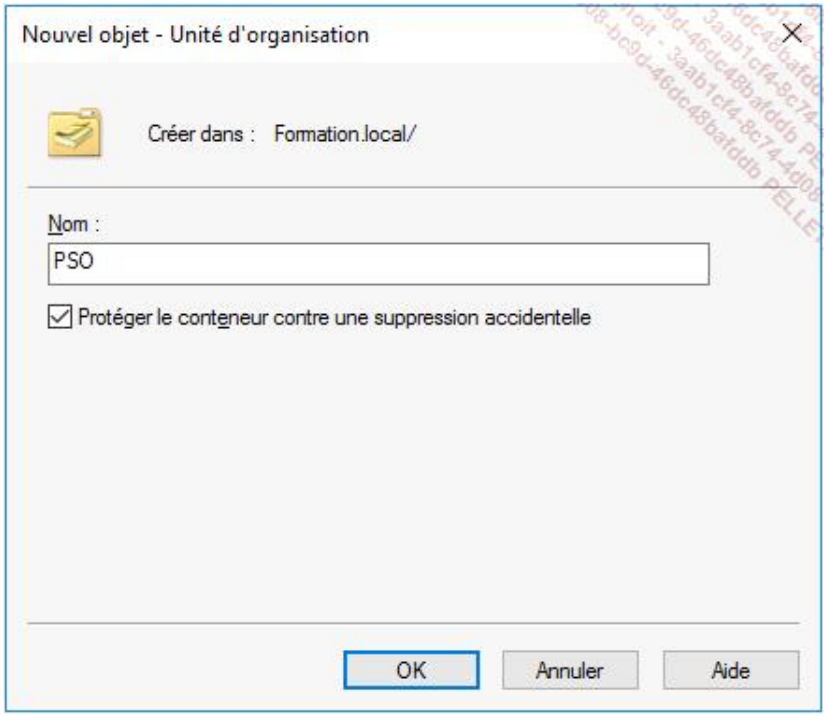
1. Stratégie de mot de passe affinée à l'aide de l'interface graphique

Depuis Windows Server 2012, la gestion et la création des stratégies de mot de passe affinées ont été améliorées. Une interface utilisateur a été ajoutée afin de rendre la création des différentes stratégies plus facile et visuelle. Cette interface est accessible par l'intermédiaire de la console **Centre d'administration Active Directory**.

La stratégie résultante d'un utilisateur peut maintenant être affichée par le biais de la console.

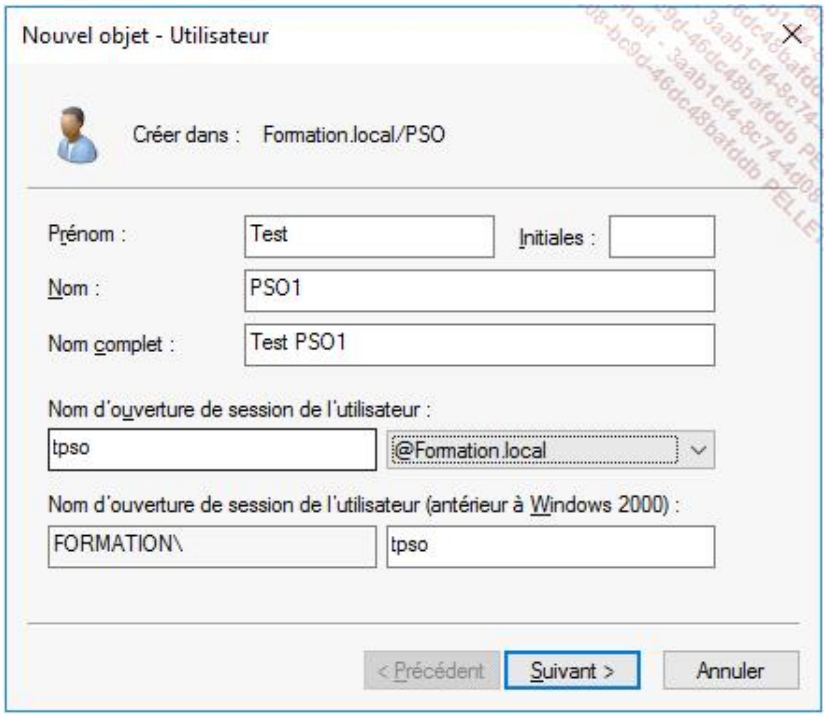
- Lancez la console **Utilisateurs et Ordinateurs Active Directory** par l'intermédiaire de l'interface Windows.
- Cliquez sur la racine du domaine **Formation.local** puis à l'aide de la barre d'outils, effectuez la création d'une nouvelle unité d'organisation.

- Dans le champ **Nom**, saisissez **PSO** puis cliquez sur **OK**.



- Cliquez sur l'unité d'organisation qui vient d'être créée puis cliquez sur le bouton permettant la création d'un nouvel utilisateur.
- Saisissez **Test** dans le champ **Prénom** puis **PSO1** dans **Nom**.

  Le **Nom d'ouverture de session** est **tpso**.

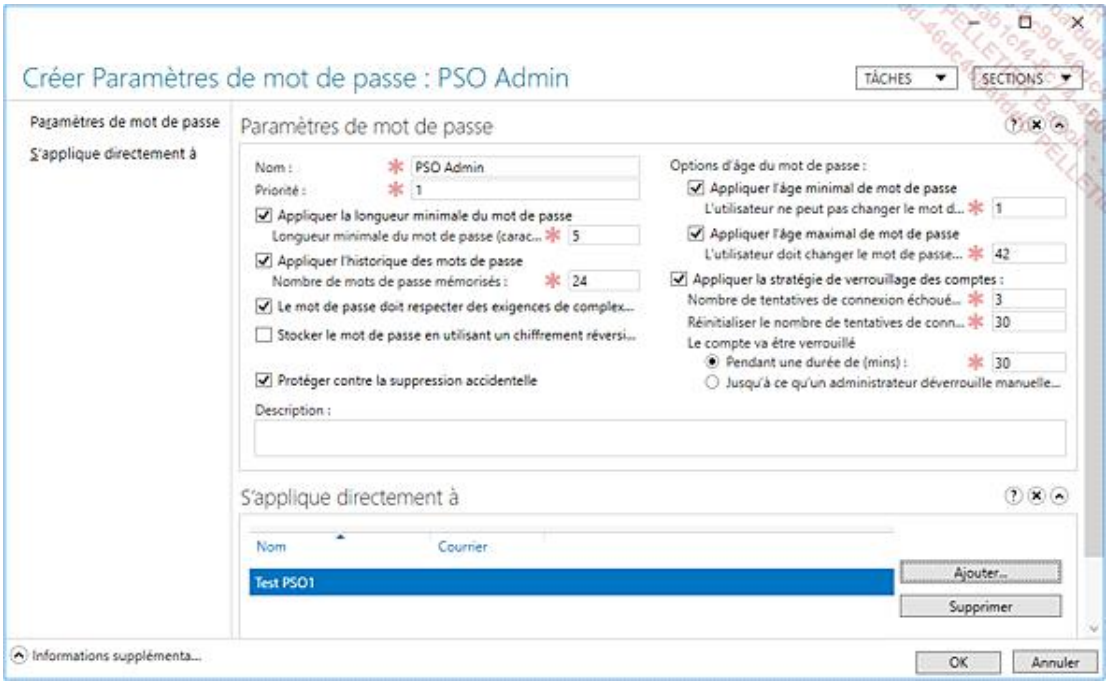


- Cliquez sur **Suivant**.
- Saisissez **Pa$$w0rd** dans le champ **Mot de passe** puis confirmez-le.
- Cochez l'option **Le mot de passe n'expire jamais**.

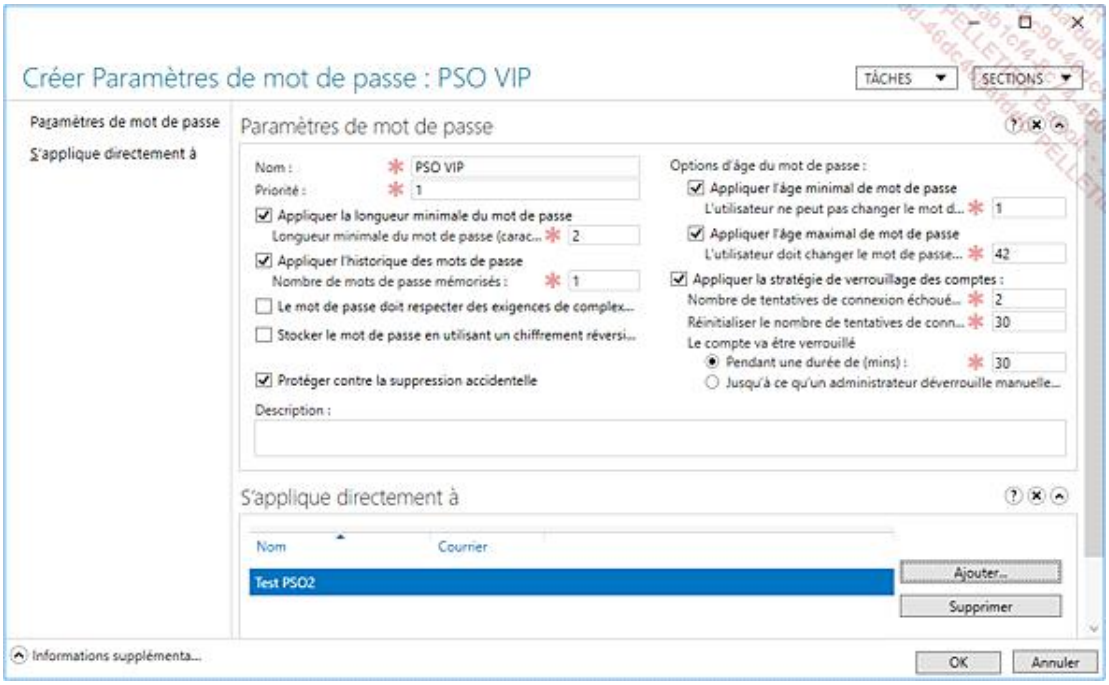
- Cliquez sur **Suivant**, puis **Terminer**.
- Recommencez les mêmes étapes pour la création de l'utilisateur **Test PSO2**.
- Depuis l'interface Windows, lancez la console **Centre d'administration Active Directory**.



- Dans le panneau de gauche, double cliquez sur la racine du domaine **Formation (local)**.
- Dans le volet de navigation, double cliquez sur le conteneur **Système** puis sur **Password Settings Container**.
- Cliquez sur **Nouveau** dans le bandeau **Tâches** puis sur **Paramètres de mot de passe**.
- Saisissez **PSO Admin** dans le champ **Nom** et **1** dans **Priorité**.
- Laissez cochée **Appliquer la longueur minimale du mot de passe** et saisissez dans le champ la valeur **5**.
- Dans le champ **Appliquer l'historique des mots de passe**, saisissez **24**.
- Cochez la case **Appliquer la stratégie de verrouillage des comptes** puis saisissez **3** dans le champ **Nombre de tentatives de connexion échoué**.
- Cliquez sur le bouton **Ajouter** puis saisissez **tpso** dans le champ.
- Cliquez sur **OK**.

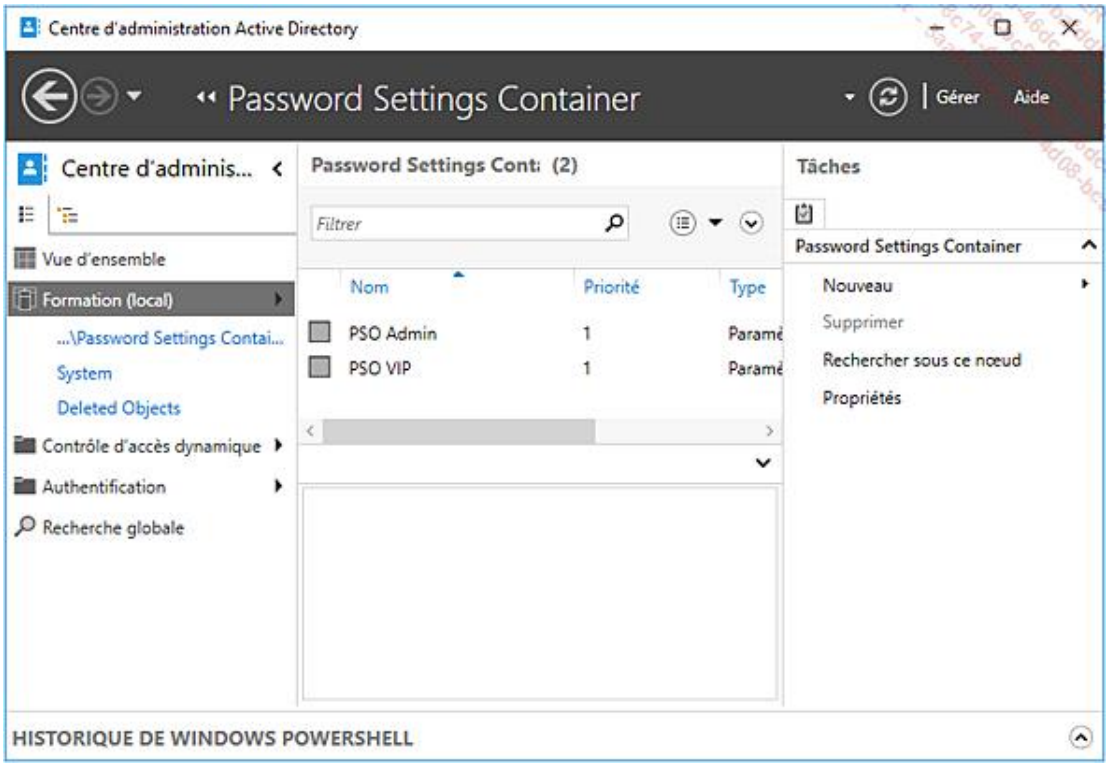


- Cliquez sur **OK** pour valider la création.
- Cliquez sur **Nouveau** dans le bandeau **Tâches** puis sur **Paramètres de mot de passe** afin de créer une nouvelle politique.
- Saisissez **PSO VIP** dans le champ **Nom** et **1** dans **Priorité**.
- Laissez cochée **Appliquer la longueur minimale du mot de passe** et saisissez dans le champ la valeur **2**.
- Dans le champ **Appliquer l'historique des mots de passe**, saisissez **1**.
- Décochez la case **Le mot de passe doit respecter de exigences de complexité**.
- Cochez la case **Appliquer la stratégie de verrouillage des comptes** puis **2** dans le champ **Nombre de tentatives de connexion échoué**.
- Cliquez sur le bouton **Ajouter** puis saisissez **tpso2** dans le champ.
- Cliquez sur **OK**.



Cliquez sur **OK**.

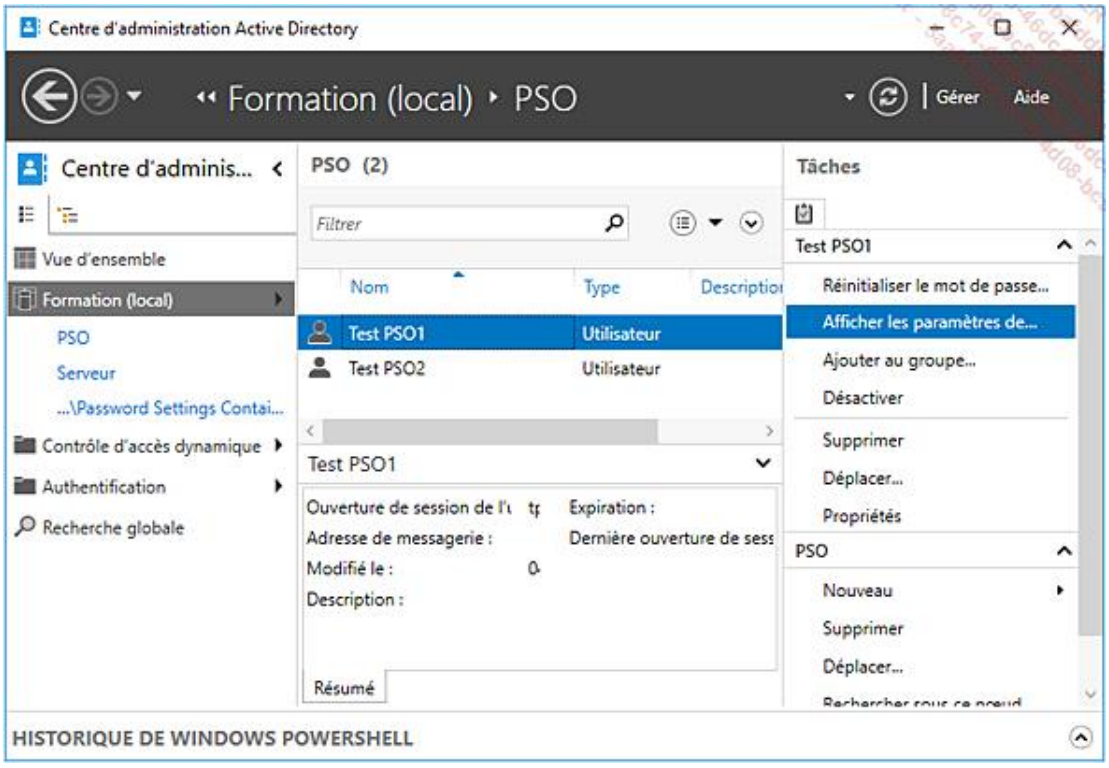
Les deux politiques de mot de passe affinées apparaissent dans la console.



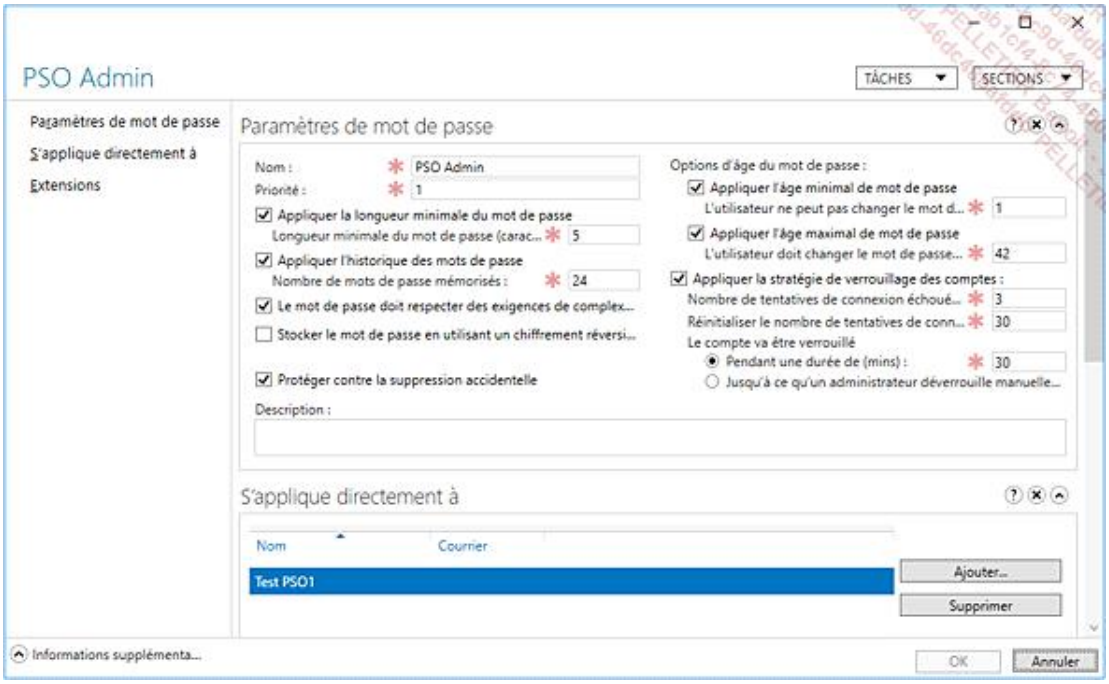
La console permet également de connaître les paramètres de mot de passe résultants pour un utilisateur.

Double cliquez sur la racine du domaine **Formation (local)** puis sur l'unité d'organisation **PSO**.

Cliquez sur **Test PSO1** puis dans le bandeau **Tâches**, cliquez sur **Afficher les paramètres de mots de passe résultants**.



La stratégie de mot de passe affinée qui lui est attribuée s'affiche.



Recommencez la même opération en sélectionnant cette fois **Test PSO2**.

La stratégie qui lui est appliquée est **PSO VIP**.

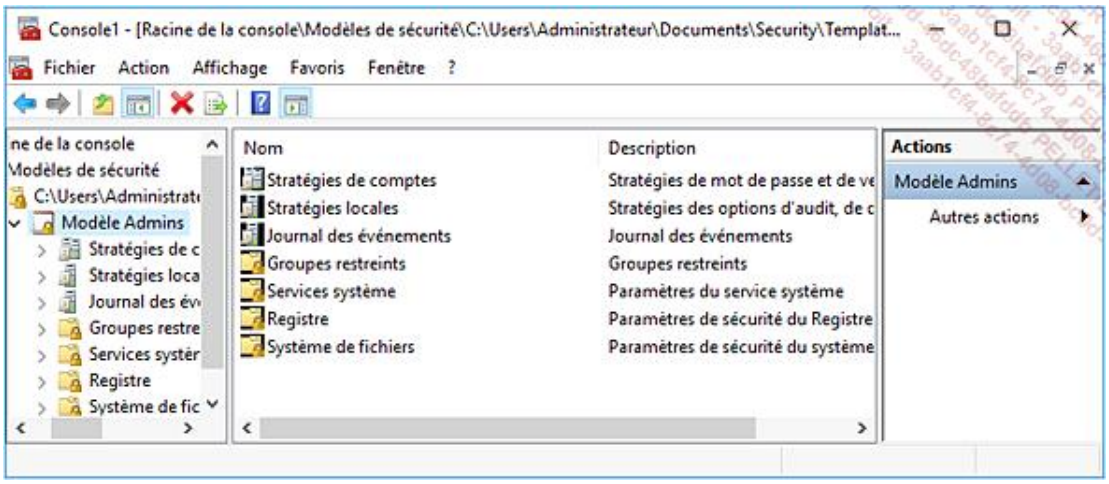
2. Création et importation d'un modèle de sécurité

Un modèle de sécurité est un fichier au format **INF** qui peut être importé dans une stratégie de groupe. Il a la particularité de pouvoir être créé sur n'importe quel poste. L'administrateur a ainsi le temps de travailler sur son

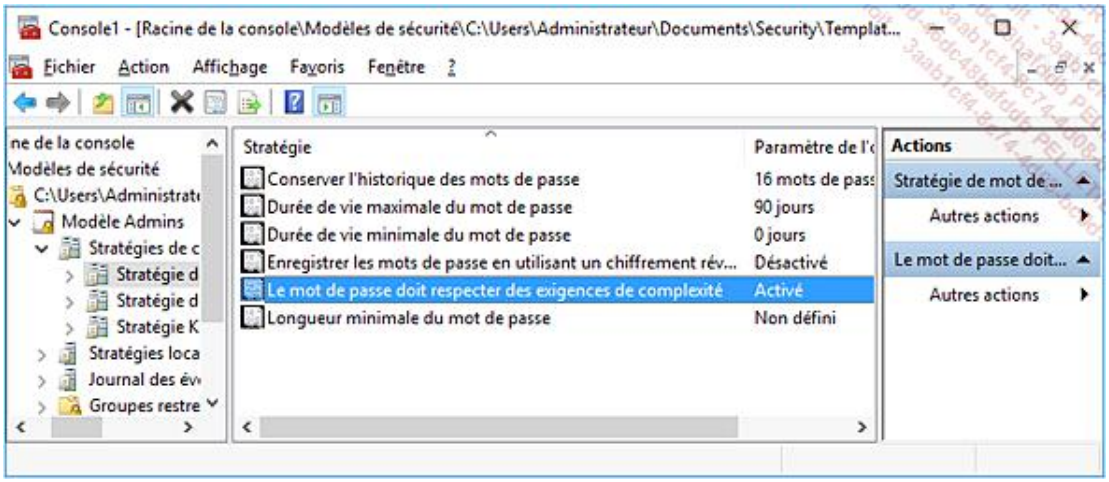
modèle. De plus, il permet d'homogénéiser la politique de sécurité dans toute l'entreprise en imposant aux succursales le modèle. Enfin, il peut facilement être réimporté.

- Sur AD1, lancez une **console MMC**.
- Cliquez sur **Fichier** puis sur **Ajouter/Supprimer un composant logiciel enfichable** puis cliquez sur **Modèles de sécurité**.
- Cliquez sur **Ajouter** puis sur **OK**.
- Développez le nœud **Modèles de sécurité** puis effectuez un clic droit sur le répertoire.
- Dans le menu contextuel, cliquez sur **Nouveau modèle**.
- Dans le champ **Nom du modèle**, saisissez **Modèle Admins** puis cliquez sur **OK**.
- Développez le nœud **Modèle Admins**.

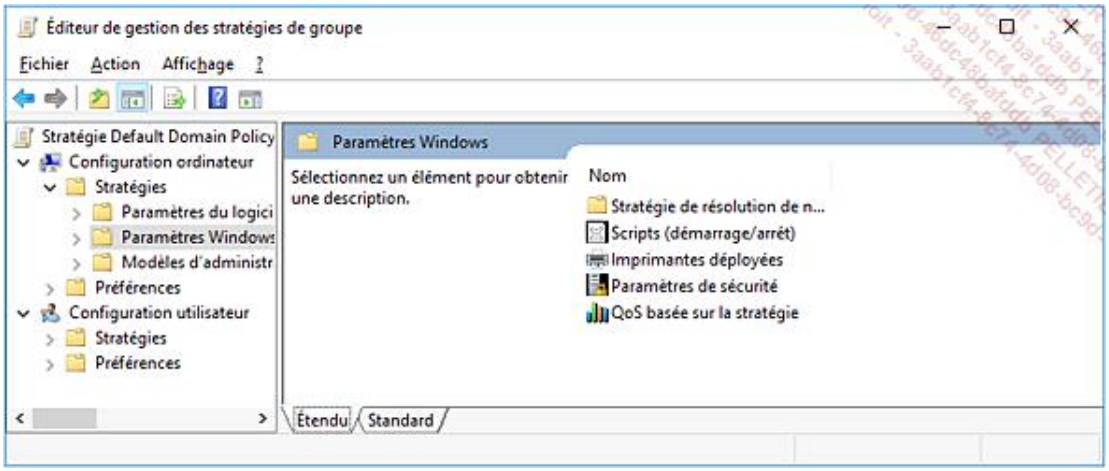
La console présente les différents paramètres.



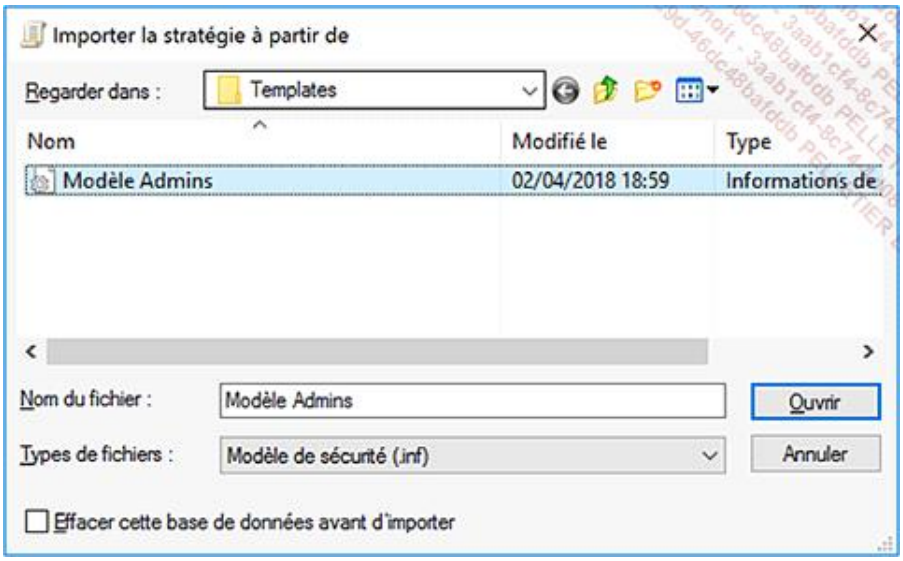
- Développez **Stratégies de compte** puis **Stratégie de mot de passe**.
- Configurez les paramètres comme ci-dessous :
  - Conserver l'historique des mots de passe : 16 mots de passe
  - Durée de vie minimale du mot de passe : 0 jour
  - Durée de vie maximale du mot de passe : 90 jours
  - Enregistrer les mots de passe en utilisant un chiffrement réversible : Désactivé
  - Le mot de passe doit respecter des exigences de complexité : Activé



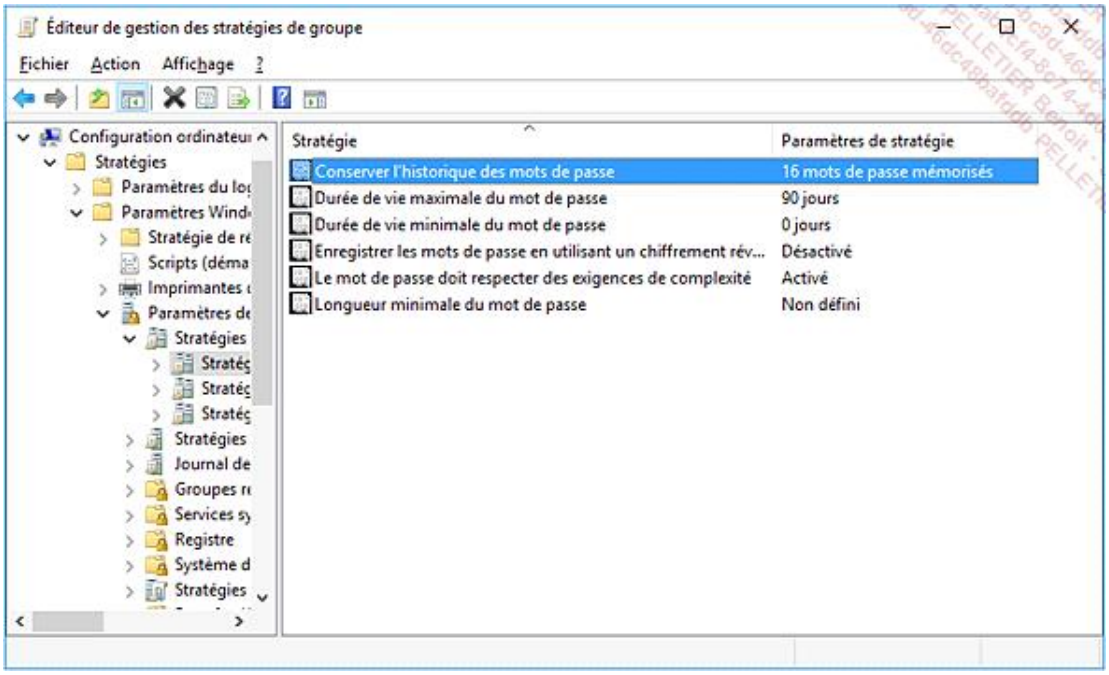
- Effectuez un clic droit sur **Modèle Admins** puis dans le menu contextuel, cliquez sur **Enregistrer**.
- Lancez la console **Gestion des stratégies de groupe** et développez les nœuds **Forêt** et **Domaines**.
- Effectuez un clic droit sur **Default Domain Policy** puis cliquez sur **Modifier**.
- Développez les nœuds **Configuration ordinateur**, **Stratégies** et **Paramètres Windows**.



- Effectuez un clic droit sur **Paramètres de sécurité** puis cliquez sur **Importer une stratégie**.
- Double cliquez sur le fichier **Modèle Admins**.



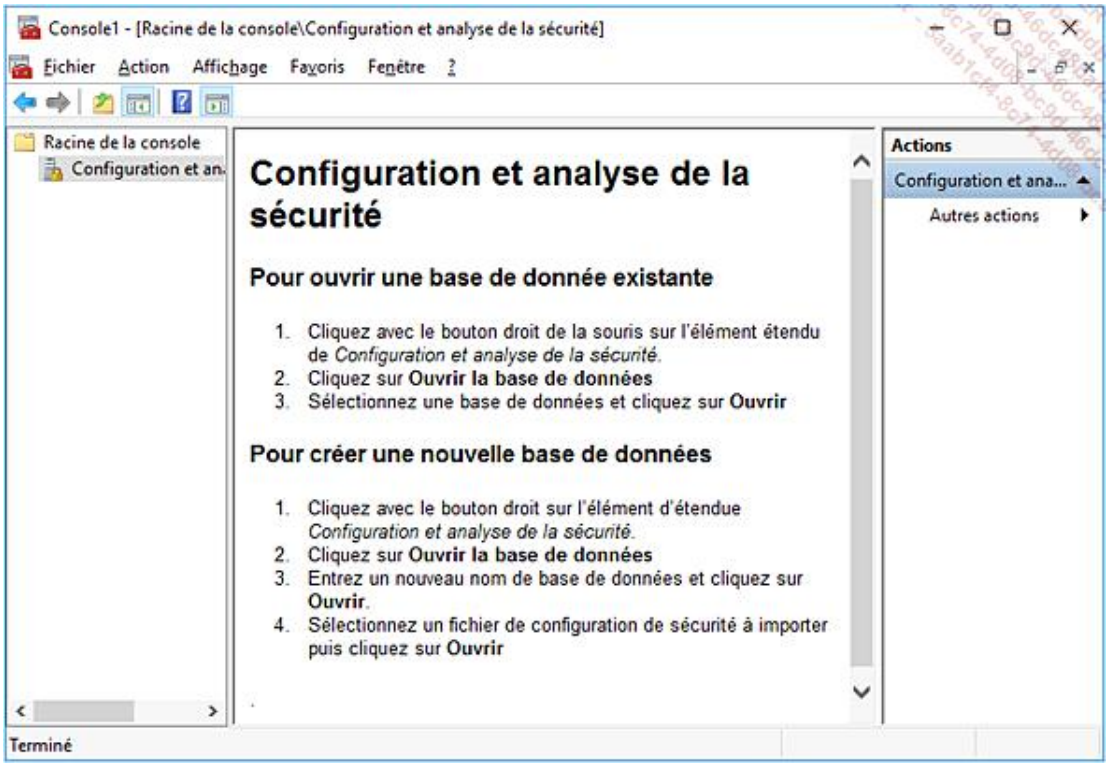
Les paramètres sont maintenant importés dans la Default Domain Policy.



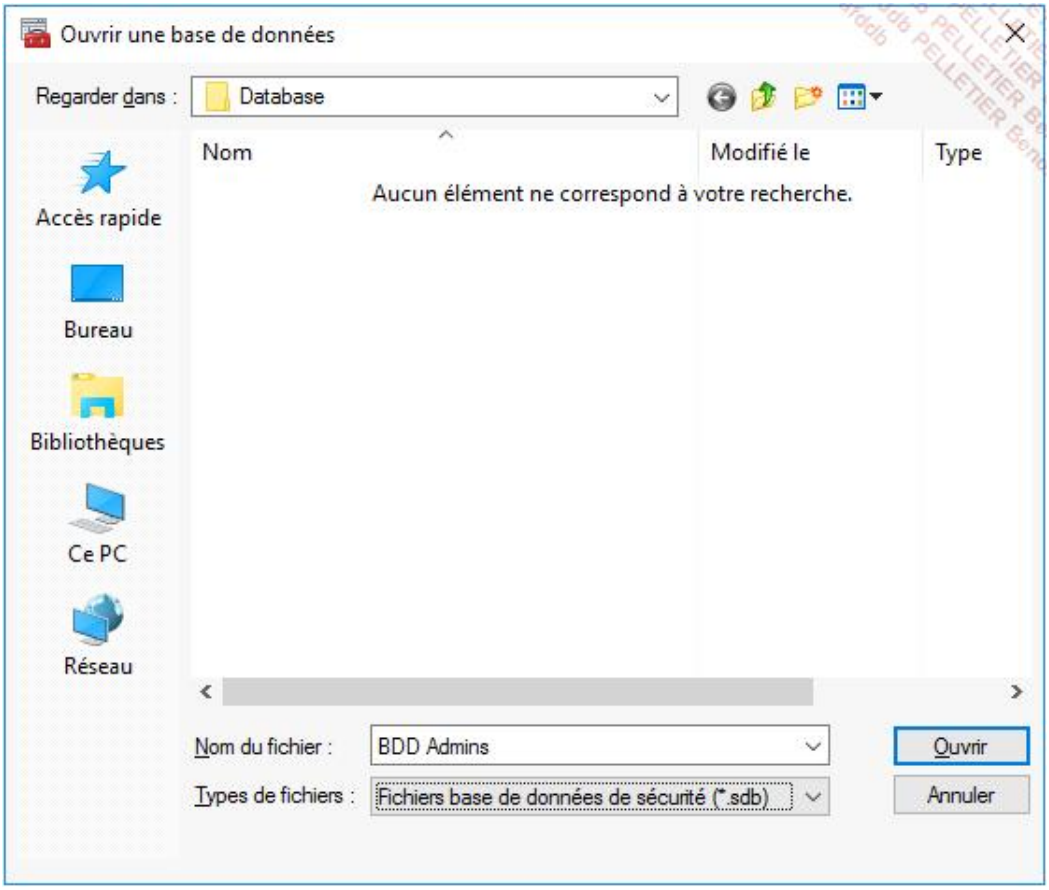
L'étape suivante consiste à modifier les paramètres dans la stratégie afin de voir des différences avec le modèle.

3. Comparaison des paramètres en cours et du modèle

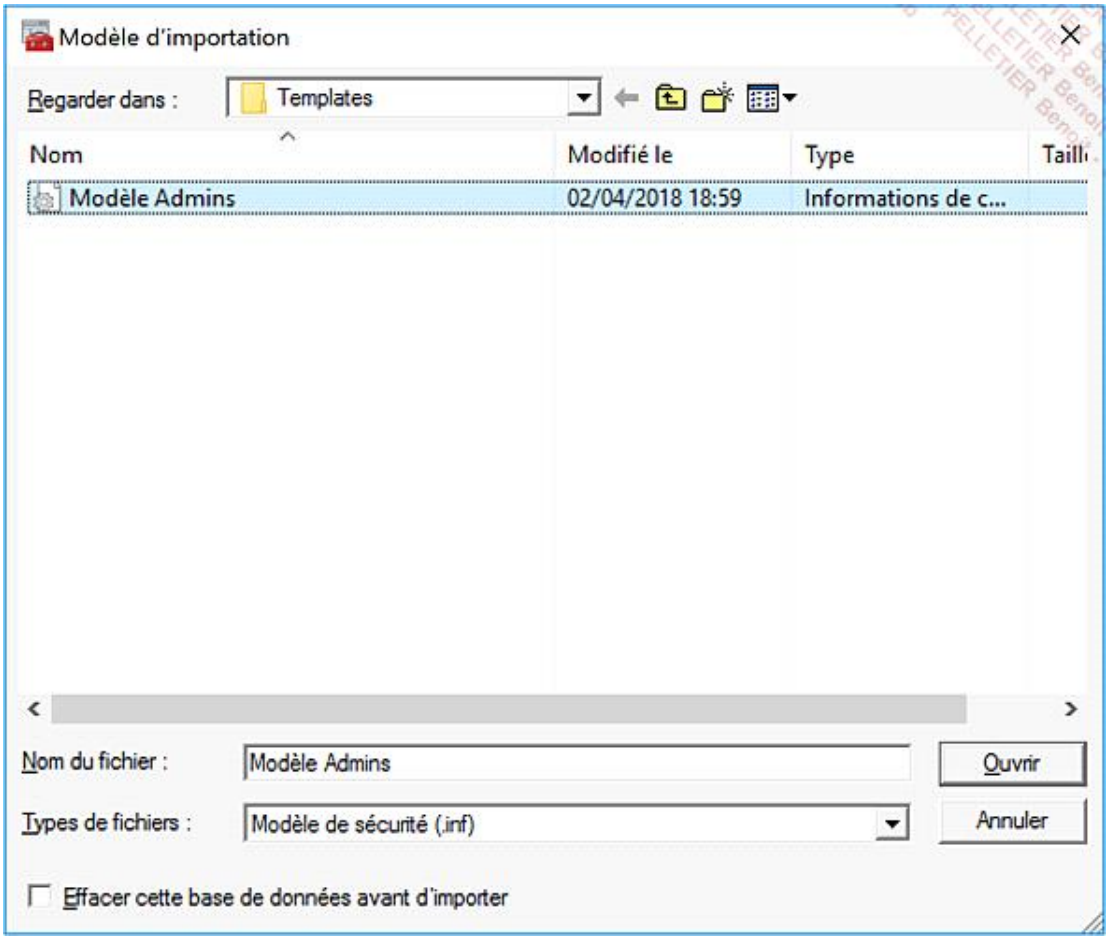
- Modifiez la stratégie de groupe **Default Domain Policy** comme ci-dessous :
  - Conserver l'historique des mots de passe : 1 mot de passe
  - Durée de vie minimale du mot de passe : 16 jours
  - Durée de vie maximale du mot de passe : 200 jours
  - Enregistrer les mots de passe en utilisant un chiffrement réversible : Désactivé
  - Le mot de passe doit respecter des exigences de complexité : Désactivé
- Sur AD1, lancez une **console MMC**.
- Cliquez sur **Fichier** puis sur **Ajouter/Supprimer des composants logiciels enfichables** puis cliquez sur **Configuration et analyse de la sécurité**.
- Cliquez sur le bouton **Ajouter** puis sur **OK**.



- Effectuez un clic droit sur **Configuration et analyse de la sécurité** puis sélectionnez **Ouvrir une base de données** dans le menu contextuel.
- Saisissez **BDD Admins** dans le champ **Nom du fichier** puis cliquez sur **Ouvrir**.

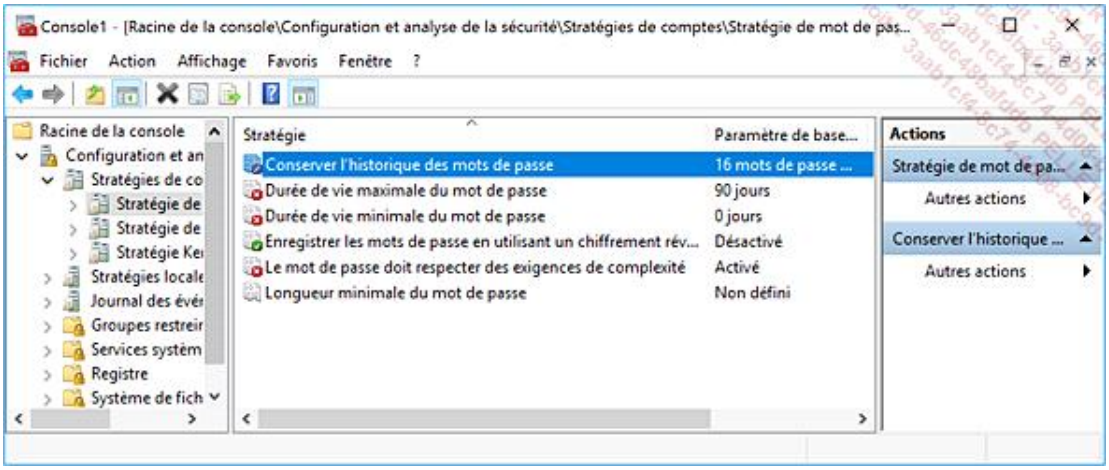


- Dans la fenêtre **Modèle d'importation**, cliquez sur **Modèle Admins** puis sur **Ouvrir**.



- Effectuez un clic droit sur **Configuration et analyse de la sécurité** puis sélectionnez **Analyser l'ordinateur maintenant** dans le menu contextuel.
- Dans la fenêtre **Effectuer l'analyse**, laissez le chemin par défaut puis cliquez sur **OK**.
- Développez les nœuds **Stratégies de compte** puis **Stratégie de mot de passe**.

La console centrale présente les différentes options et un éventuel conflit (vert : OK, rouge : conflit entre le modèle de sécurité et la GPO).



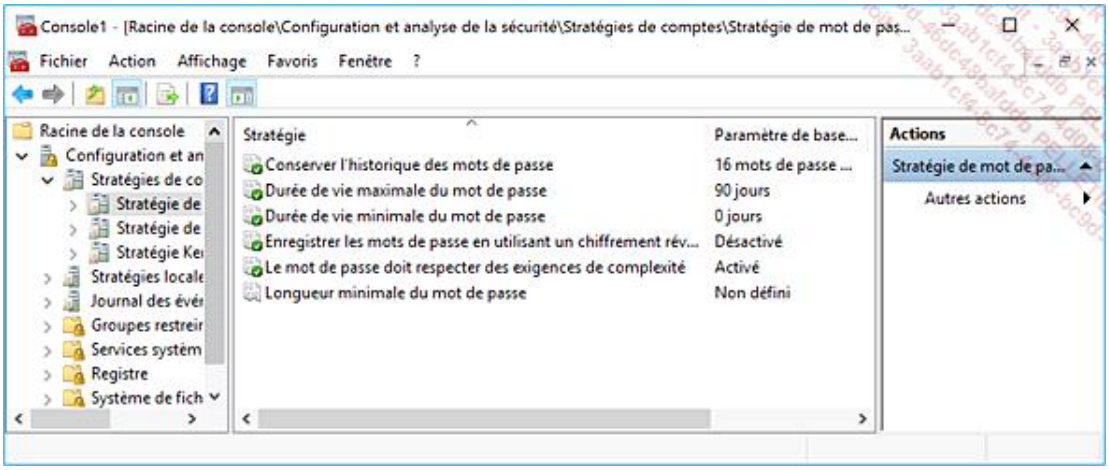
Le modèle de sécurité doit être réappliqué.

- Faites un clic droit sur **Configuration et analyse de la sécurité** puis dans le menu contextuel, sélectionnez

Configurer l'ordinateur maintenant.

Dans la fenêtre **Configuration du système**, laissez le chemin par défaut puis cliquez sur **OK**.

Les paramètres de la stratégie de groupe **Default Domain Policy** ont été modifiés par les paramètres du modèle.



Le modèle permet une réactualisation de l'ensemble des paramètres de façon très aisée.

Paramétrage de l'User Access Control

1. Introduction

Les comptes administrateurs sont généralement des comptes utilisateur sensibles. Principalement parce qu'ils fournissent à l'utilisateur qui ouvre une session des droits élevés (modification du registre, changement des paramètres Windows…). Une protection de ce type de compte est nécessaire afin d'assurer un bon fonctionnement du système d'exploitation ainsi que l'intégrité des données.

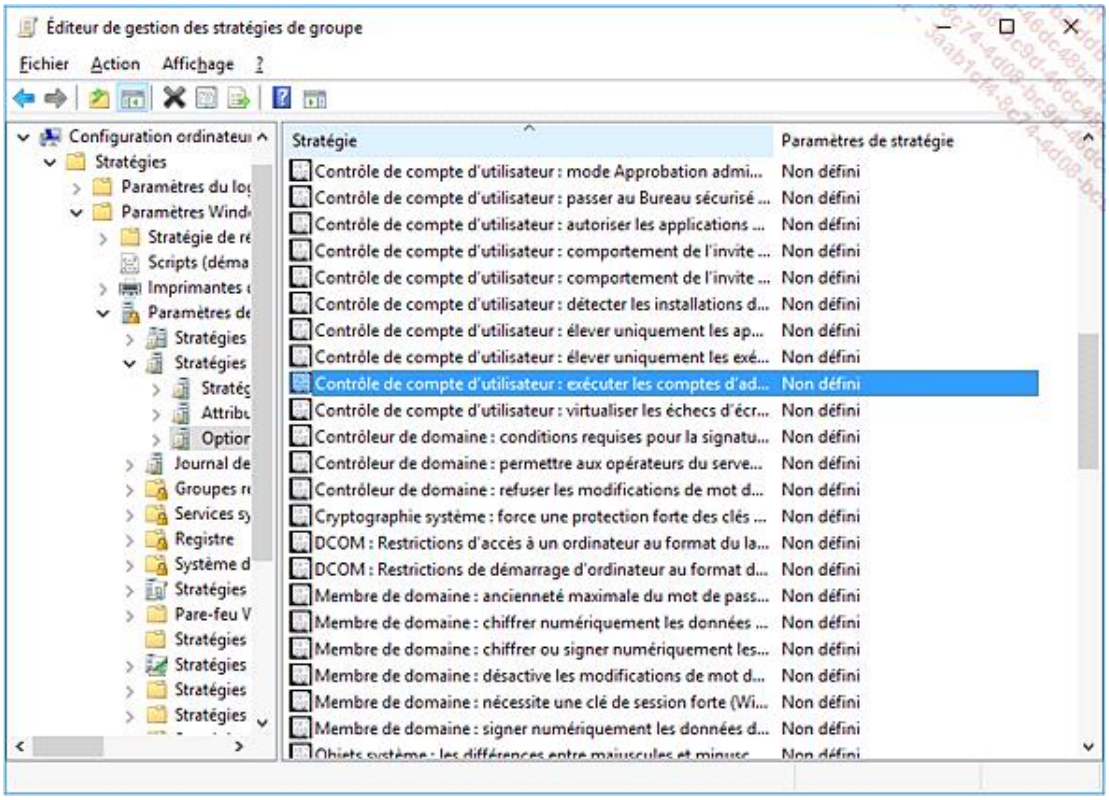
L'UAC (*User Access Control*) a fait son apparition avec Windows Vista et Windows Server 2008. Cette fonctionnalité permet de sécuriser l'utilisation des comptes sensibles. Pour cela une confirmation est demandée lorsqu'une élévation de privilèges est nécessaire. Si la personne connectée ne possède pas de droit d'administration, il est nécessaire de saisir les identifiants d'un compte d'administration. La commande Runas permet, comme l'UAC, le lancement d'un processus en utilisant les identifiants d'un autre compte.

Ainsi, les utilisateurs standards et les administrateurs se trouvent par défaut avec les mêmes droits sur le poste. Lorsque des droits plus élevés sont nécessaires, l'UAC effectue une élévation de privilège. Ainsi, seul le processus qui a demandé l'élévation fonctionne avec des droits d'administrateur. Deux actions sont possibles :

- **L'utilisateur est administrateur** : l'UAC demande à la personne connectée l'autorisation de continuer l'exécution du processus qui nécessite des droits d'administration.
- **L'utilisateur est un utilisateur standard** : la saisie des identifiants d'un compte possédant des droits d'administration doit être effectuée.

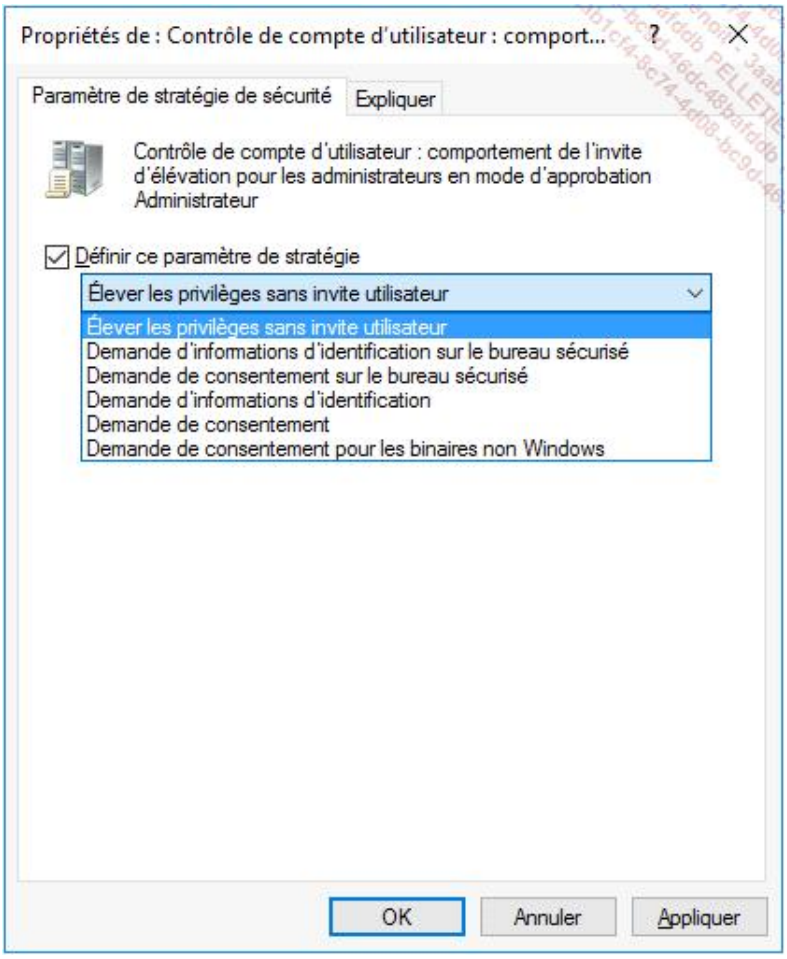
Le comportement de l'UAC peut être configuré pour ajuster la fréquence de notification.

Cette configuration peut être effectuée en accédant au nœud **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Options de sécurité**.

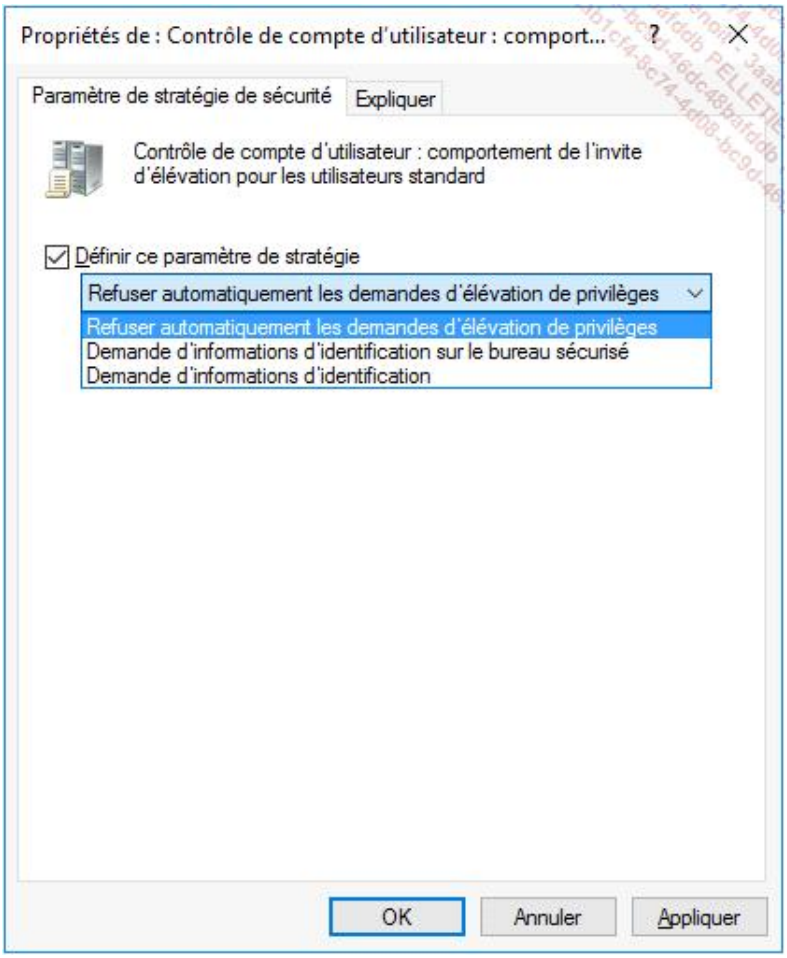


Parmi cette liste de paramètres, il est possible de trouver :

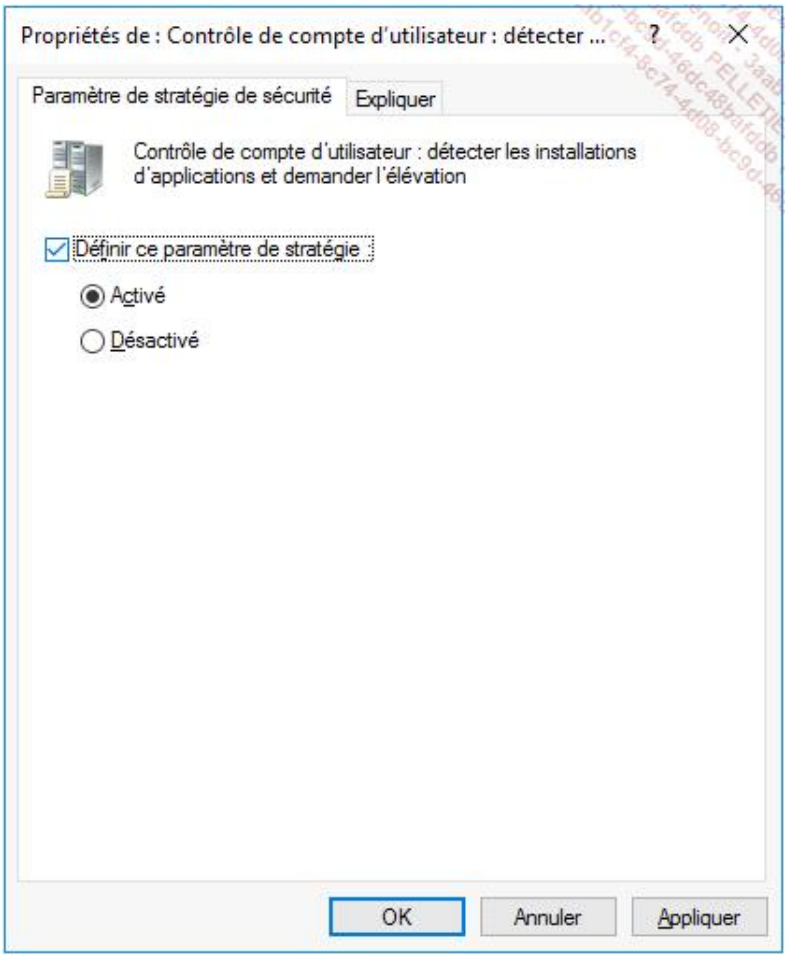
- **Contrôle de compte utilisateur : comportement de l'invite d'élévation pour les administrateurs en mode d'approbation** : permet de contrôler le comportement de l'invite d'élévation. Ce paramètre s'applique uniquement au compte Administrateur. Plusieurs options sont disponibles.



- **Contrôle de compte utilisateur : comportement de l'invite d'élévation pour les utilisateurs standard** : permet de gérer le comportement de l'invite d'élévation pour les comptes n'ayant pas de droits d'administration. Trois options sont disponibles.



- **Contrôle de compte utilisateur : détecter les installations d'applications et demander l'élévation** : permet d'autoriser la demande d'élévation lors de l'installation d'une application. Deux options sont disponibles.



Par défaut, l'UAC n'est pas activé sur un serveur installé en mode Core.

2. Utilisation d'AppLocker

AppLocker a été introduit dans les systèmes d'exploitation Windows Server 2008 R2 et Windows 7. Comme pour la restriction logicielle, il est possible de contrôler l'exécution d'une application. Elle permet aux administrateurs la mise en place plus aisée de règles et s'appuie également sur la mise en place de stratégies de groupe. La règle s'applique à un utilisateur ou à un groupe de sécurité Active Directory.

Il est possible d'appliquer une règle pour gérer son exécution mais également d'utiliser l'audit afin de pouvoir tester les règles avant leur application. Les administrateurs peuvent interdire plus simplement les applications dont les licences n'ont pas été achetées, seuls les logiciels validés par le service informatique sont autorisés à s'exécuter. Notez qu'il est préférable de ne pas activer AppLocker sur un contrôleur de domaine.

Trois types de fichiers sont gérés :

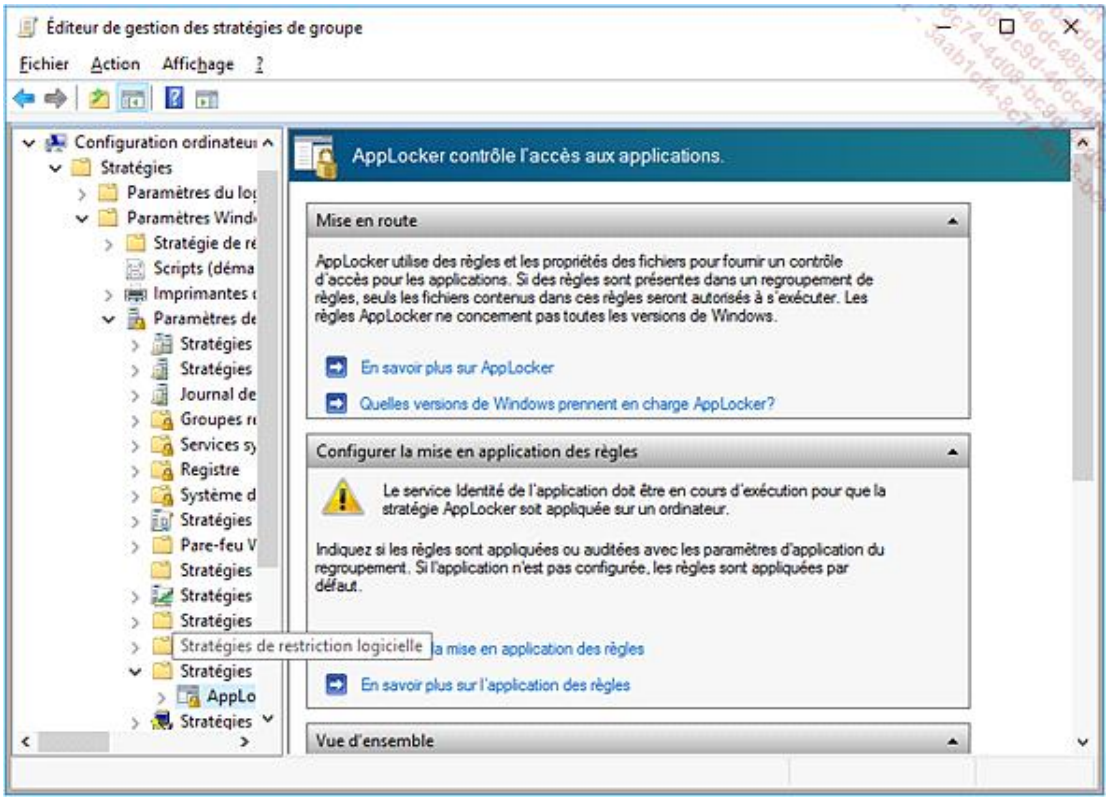
- Exécutable
- Script
- Windows Installer (msi)

Les règles AppLocker permettent d'empêcher une application et peuvent être utilisées dans plusieurs cas :

- Application interdite dans l'entreprise (MSN, etc.).

- Logiciel remplacé par une nouvelle version ou plus utilisé.
- Application réservée à un service spécifique.

Cette fonctionnalité est configurable par le biais du nœud **Configuration ordinateur \ Stratégies \ Paramètres Windows \ Paramètres de Sécurité \ Stratégie de contrôle de l'application**.



Le service **Identité de l'application** est utilisé pour le fonctionnement d'AppLocker. Si le service est arrêté, les règles ne sont pas appliquées.

Les règles utilisent plusieurs critères pour identifier l'application :

- **Éditeur** : s'appuie sur la signature numérique de l'éditeur.
- **Chemin d'accès** : autorise ou bloque tous les exécutables contenus dans le chemin d'accès donné.
- **Hash** : le hash est utilisé pour identifier l'application et gérer son exécution.

Le certificat numérique

1. Présentation

Un certificat numérique possède plusieurs fonctions (SSL, cryptage EFS…), généralement le choix du certificat est fait en fonction de son usage futur.

Ce certificat possède une clé privée et/ou une clé publique. En effet, deux types de cryptage sont présents dans le monde de la cryptographie :

- Le cryptage à l'aide de clés symétriques qui consiste à effectuer les opérations de cryptage et de décryptage avec la même clé.
- Le cryptage à l'aide de clés asymétriques qui utilise lui deux types de clé : une clé publique pour crypter et une clé privée pour décrypter.

La clé privée est normalement détenue uniquement par le propriétaire du certificat, les autres personnes utilisent sa clé publique pour effectuer le cryptage.

Le certificat peut être délivré par une entité publique (généralement en payant), celui-ci est reconnu sur Internet. Il est possible également d'installer dans son réseau une autorité de certification qui a pour rôle la gestion et la distribution de certificats numériques. Attention, ce dernier type de certificat ne peut être utilisé que dans le réseau local de l'entreprise. Néanmoins, les deux types de certificats (public ou privé) ont chacun une date de validité.

Il est possible d'annuler la validité d'un certificat avant que la date ne soit échue. On appelle cela révoquer un certificat. Une liste de révocation est gérée par le serveur et permet de référencer les certificats révoqués avant leur date d'expiration.

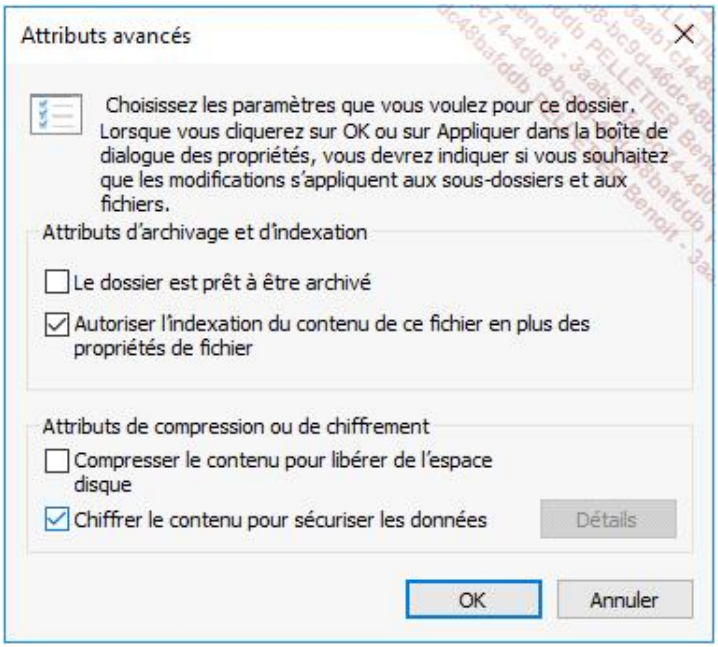
2. Cryptage à l'aide d'EFS

La fonctionnalité EFS est présente sur les systèmes d'exploitation clients et serveurs depuis de nombreuses années. Néanmoins, il est nécessaire de comprendre son mécanisme de fonctionnement avant de procéder à son implémentation. Ceci dans le but d'une implémentation correcte.

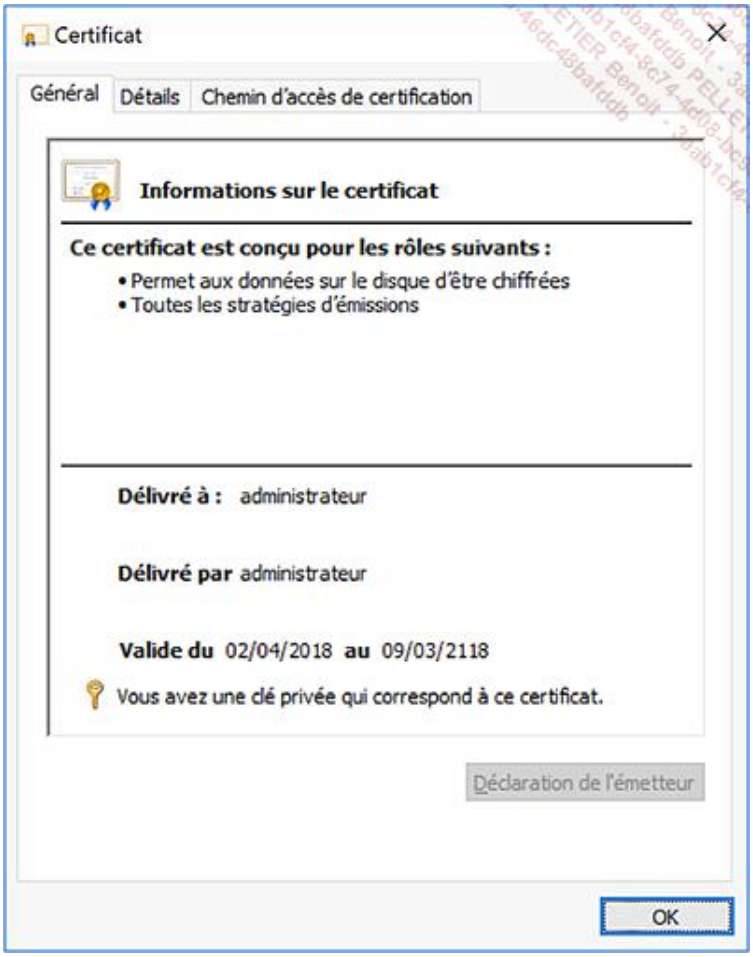
Fonctionnement d'EFS

EFS (*Encrypting File System*) permet de chiffrer un fichier afin d'en sécuriser l'accès. Il est néanmoins nécessaire de stocker le fichier sur une partition de type NTFS. Il n'est pas nécessaire de posséder des droits d'administration pour procéder au chiffrement, un simple utilisateur peut chiffrer ses fichiers locaux ou ceux présents sur un partage réseau sans action de l'administrateur.

Pour procéder au chiffrement, il faut accéder aux propriétés du répertoire ou fichier souhaité. Dans l'onglet **Général** des propriétés du dossier ou fichier, cliquez sur le bouton **Avancé** puis cochez l'option **Chiffrer le contenu pour sécuriser les données**.



Un certificat est utilisé pour le chiffrement et le déchiffrement des données.



Par la suite, seules les personnes autorisées ont la possibilité de déchiffrer et d'accéder au fichier ; dans le cas d'une personne non autorisée, le message **Accès refusé** apparaît.

En implémentant EFS, un utilisateur peut posséder des autorisations NTFS sur le fichier mais recevoir un message

Accès refusé. En effet il est nécessaire d'autoriser l'utilisateur à déchiffrer le fichier en plus de l'autorisation NTFS.

Par défaut, un certificat autosigné est attribué à l'utilisateur qui initie le chiffrement. Une paire de clés permettant d'effectuer le chiffrement et le déchiffrement lui est donnée sans que l'utilisateur ait besoin d'intervenir. Pour faciliter la gestion des certificats, il est possible d'utiliser ceux émis par une autorité de certification. Attention, cela nécessite une administration plus lourde car il est nécessaire d'administrer l'autorité de certification et de gérer la sauvegarde/restauration de ce serveur.

EFS utilise un système de chiffrement symétrique et asymétrique. Une clé symétrique est utilisée pour le chiffrement des fichiers et donc la protection de ces derniers contre toute attaque, la clé publique (chiffrement asymétrique) permet de chiffrer la clé symétrique nécessaire au déchiffrement du fichier. Il est donc impossible d'accéder aux fichiers sans détenir la clé privée de l'utilisateur.

Le chiffrement asymétrique utilise deux clés : une clé publique et une clé privée. La clé publique permet de chiffrer les fichiers alors que la clé privée permet le déchiffrement. Le chiffrement symétrique utilise pour sa part la même clé pour chiffrer et déchiffrer, et il est plus rapide que le chiffrement asymétrique. L'inconvénient majeur se situe au niveau de la sécurité, un pirate qui parvient à intercepter la clé symétrique pouvant déchiffrer le fichier. Ainsi avec le système EFS, l'utilisateur se voit octroyer un certificat possédant les clés privée et publique, et seuls les utilisateurs disposant du certificat auront la possibilité d'accéder au fichier.

Récupération d'un fichier crypté

La perte de la clé privée peut être problématique, en effet il est impossible pour l'utilisateur de déchiffrer son propre fichier. Il est donc nécessaire en amont du chiffrement de mettre en place les procédures adéquates pour répondre à ce genre de problématique.

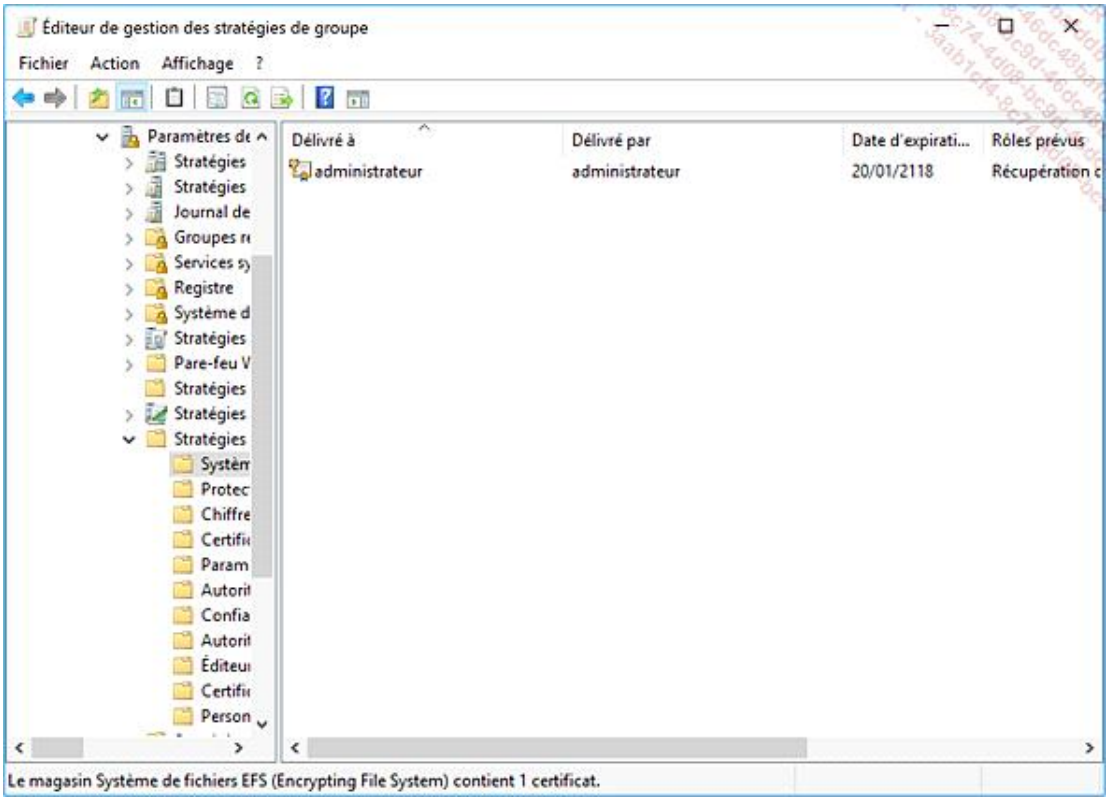
Plusieurs solutions s'offrent à nous pour éviter la perte de l'ensemble des données chiffrées :

- **Sauvegarder le certificat numérique**. En cas de perte du certificat suite à la réinstallation du poste, crash du système d'exploitation… il est possible de restaurer ce certificat. Il est également possible de restaurer le certificat sur le profil de l'administrateur, ce dernier peut ainsi effectuer le déchiffrement des données. Si de nombreux utilisateurs choisissent cette solution, cela peut devenir très vite assez compliqué à gérer.
- **Utilisation d'un agent de récupération**. Cet agent est un compte qui se voit octroyer le droit de déchiffrer tous les fichiers chiffrés à l'aide d'EFS. Par défaut le compte Administrateur du domaine possède ce rôle. Il est possible de déléguer ce rôle à un autre utilisateur par l'intermédiaire de la stratégie de groupe. Cet utilisateur est automatiquement ajouté avec les nouveaux fichiers chiffrés. Pour les fichiers existants, la mise à jour s'effectue lors d'un futur enregistrement du fichier (suite à une modification, etc.).

Pour sauvegarder le certificat, il est nécessaire de l'exporter avec la clé privée.

Le rôle Agent de récupération peut être donné à un utilisateur à l'aide de la stratégie de groupe, pour cela il faut accéder au chemin ci-dessous :

Configuration ordinateur \ Stratégies \ Paramètres Windows \ Paramètres de sécurité \ Stratégies de clé publique \ Système de fichiers EFS



L’administrateur est par défaut considéré comme un agent de récupération.

Mise en place de la délégation

La délégation est un point important, elle permet d'octroyer des droits supplémentaires à un ou plusieurs utilisateurs. Ces derniers ont la possibilité d'effectuer certaines actions sans pour autant posséder des droits d'administration.

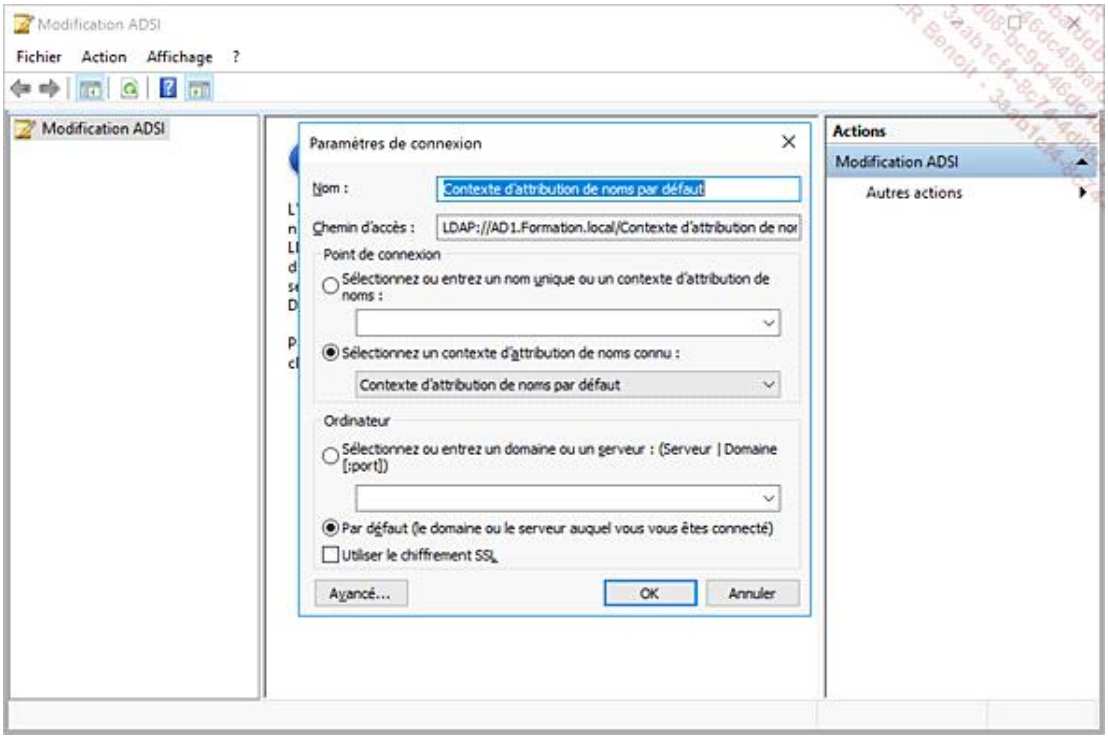
1. Délégation dans Active Directory

Il est possible de déléguer énormément de droits dans Active Directory. Les points suivants sont quelques exemples de délégation pouvant être mis en place.

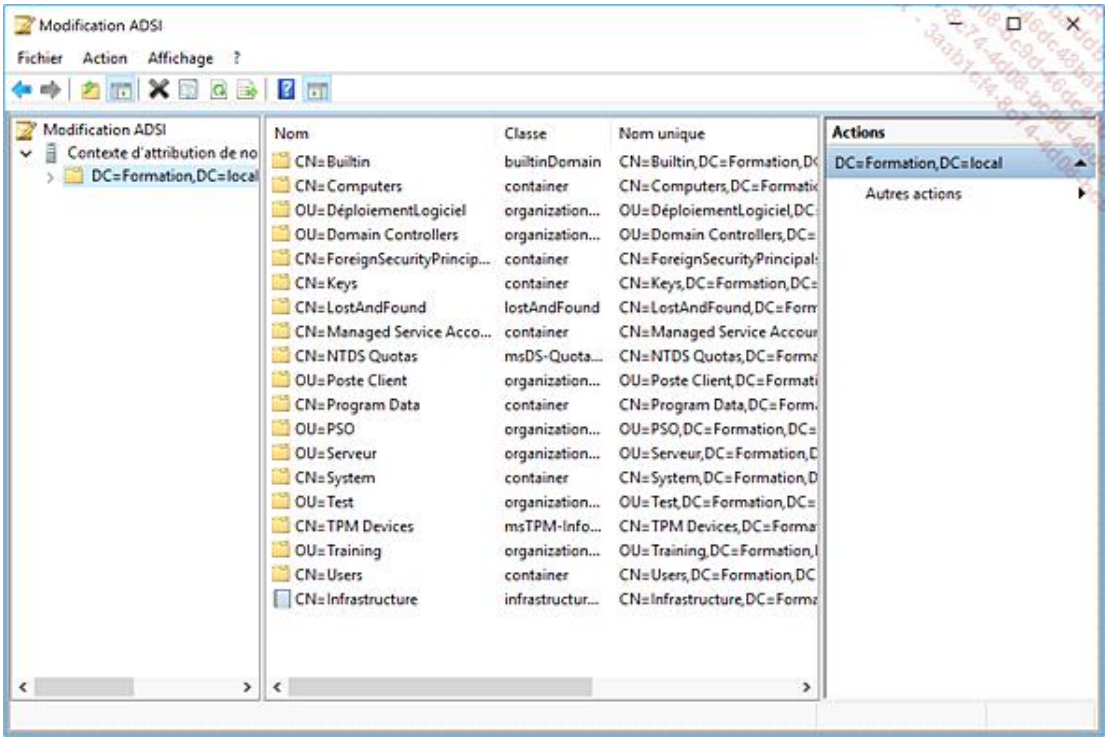
a. Déplacement d'utilisateur

Il peut être nécessaire pour un service de hotline, par exemple, de déléguer le déplacement d'un utilisateur d'une unité d'organisation à une autre. La mise en place de la délégation s'effectue au travers de la console **Modification ADSI** et **Utilisateurs et ordinateurs Active Directory**.

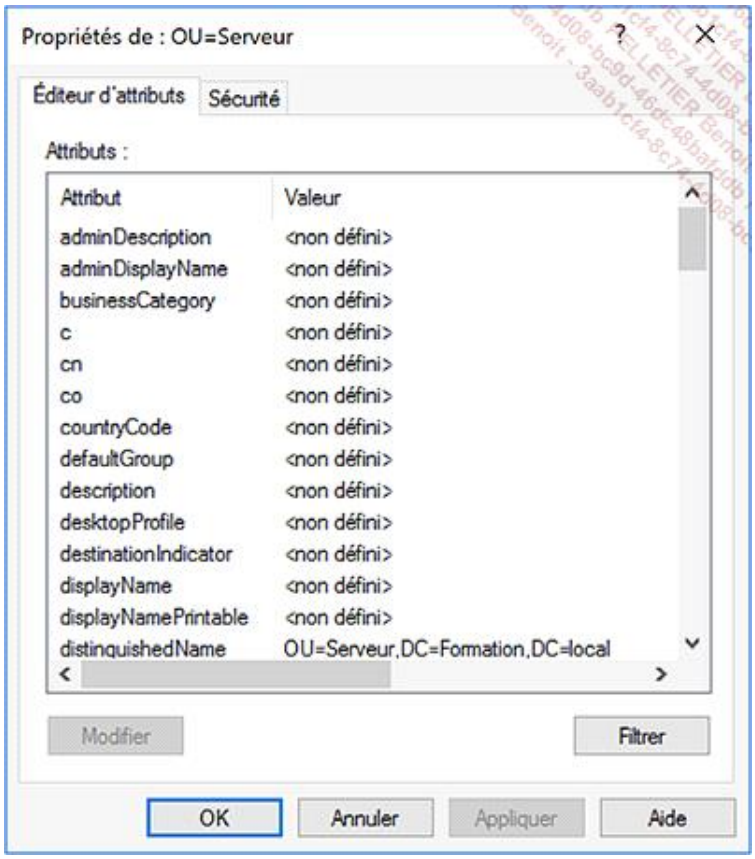
- Depuis le serveur **AD1**, accédez à la console **Modification ADSI** présente dans les outils d'administration.
- Sélectionnez l'unité d'organisation source (ou sur laquelle est présent l'utilisateur qui doit être déplacé).
- Effectuez un clic droit sur **Modification ADSI** puis, dans le menu contextuel, sélectionnez **Connexion**. Cliquez sur **OK** dans la fenêtre qui apparaît.



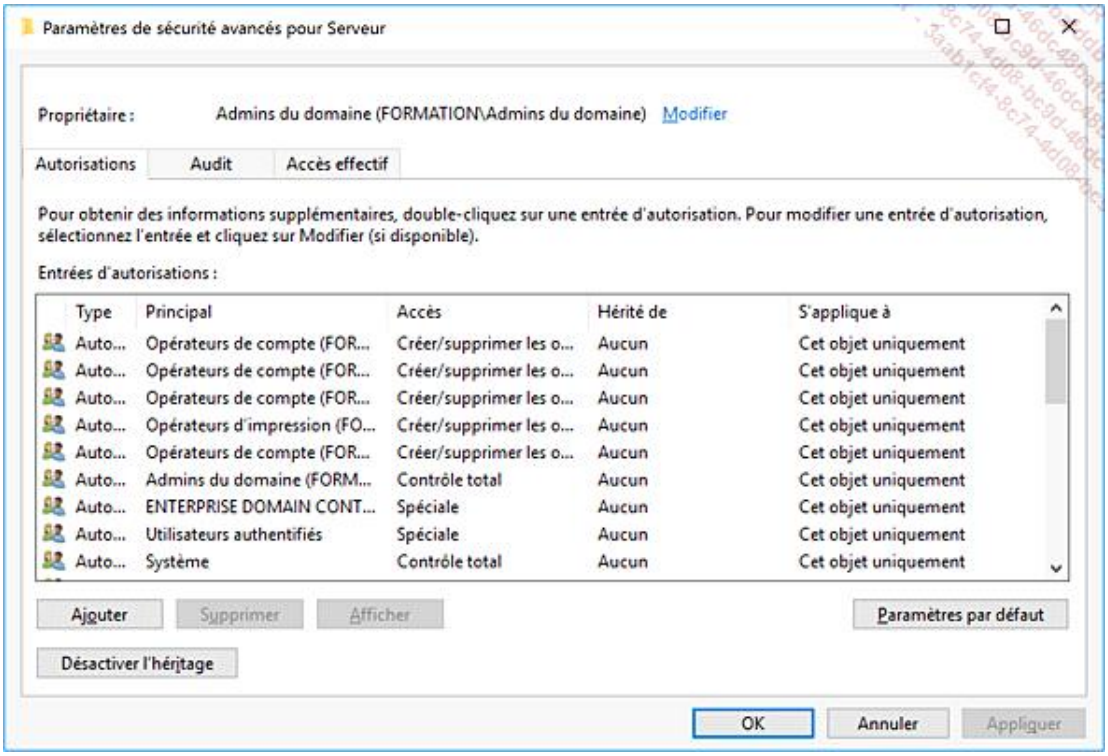
- Double cliquez sur **Contexte d'attribution de noms par défaut** puis sur **DC=Formation,DC=local**.



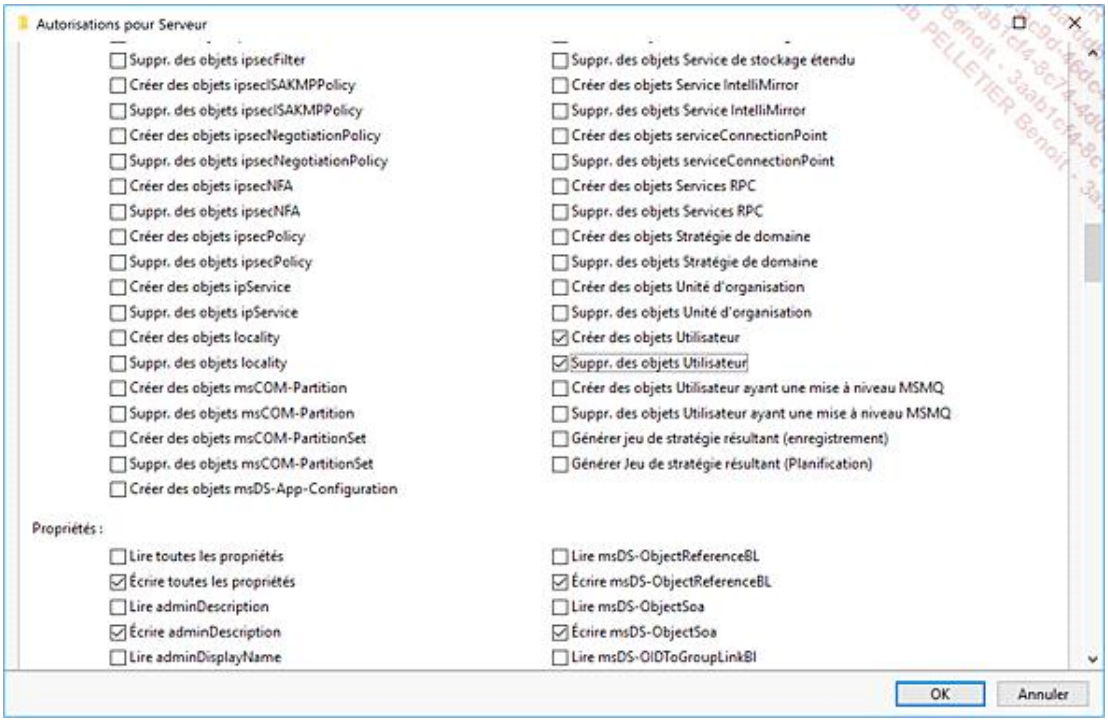
- Effectuez un clic droit sur l'unité d'organisation souhaitée puis, dans le menu contextuel, sélectionnez **Propriétés**.



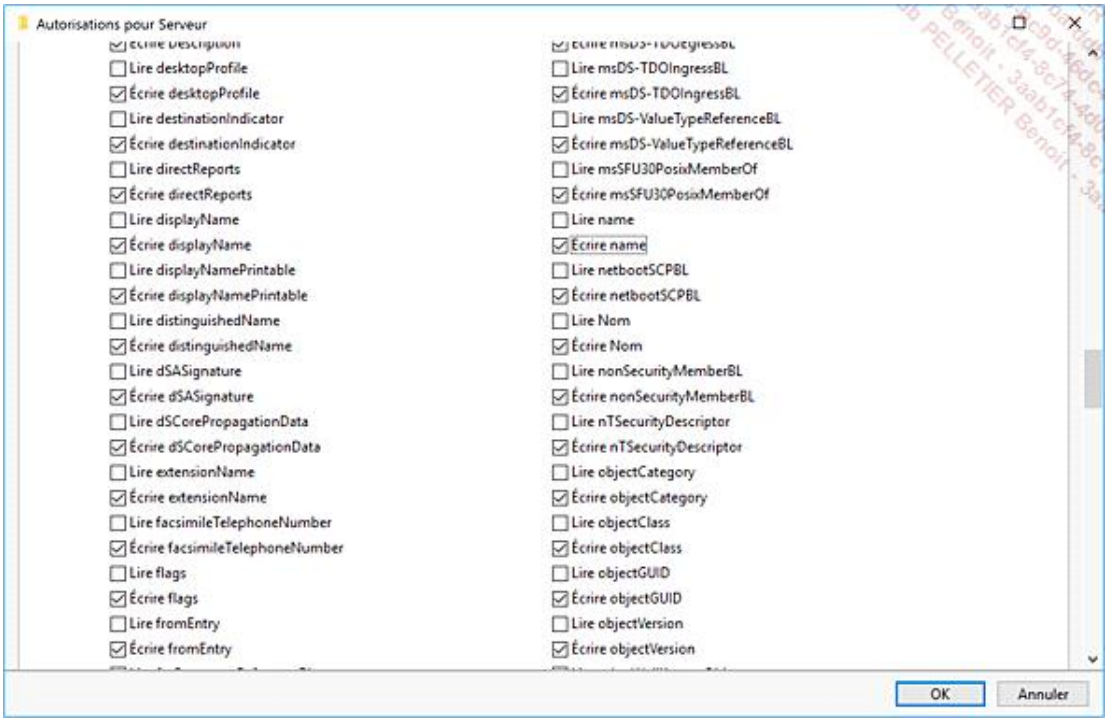
- Cliquez sur l'onglet **Sécurité** puis sur **Avancé**. Une nouvelle fenêtre s'affiche. Cliquez sur **Ajouter**.



- Cliquez sur le lien **Sélectionner un principal** puis ajoutez le compte utilisateur ou le groupe souhaité.
- Cochez les droits **Créer des objets Utilisateur** et **Supprimer des objets Utilisateur.**



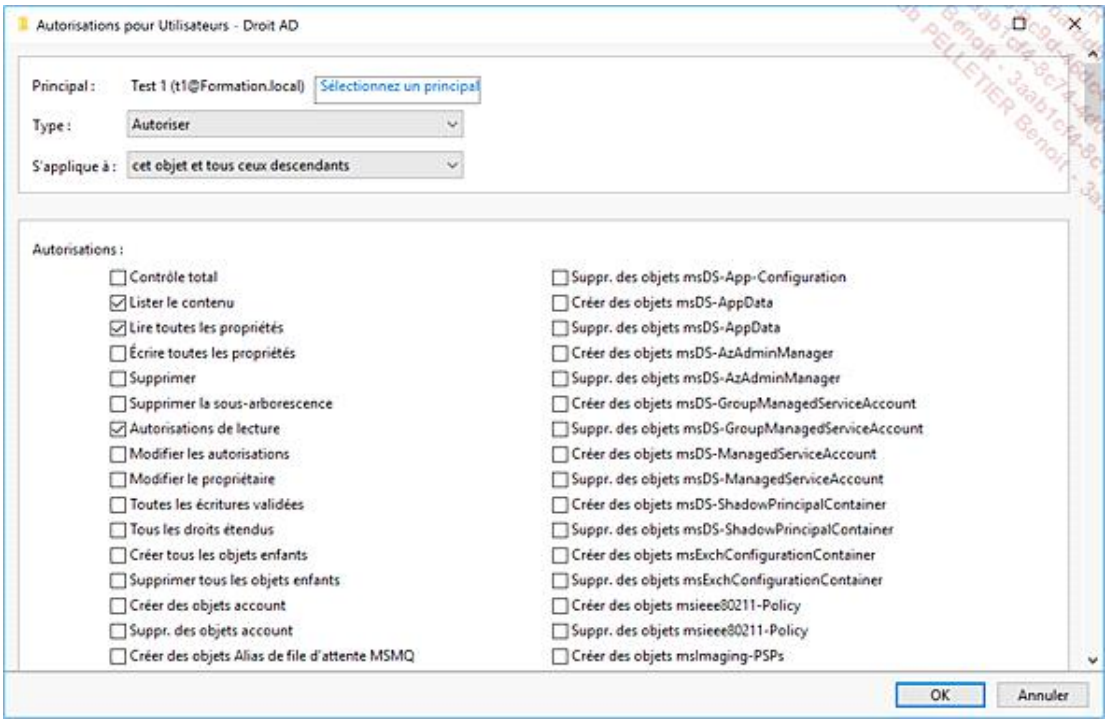
- Cochez les propriétés **Écrire name** et **Écrire Nom**. Cliquez sur **OK** pour valider.



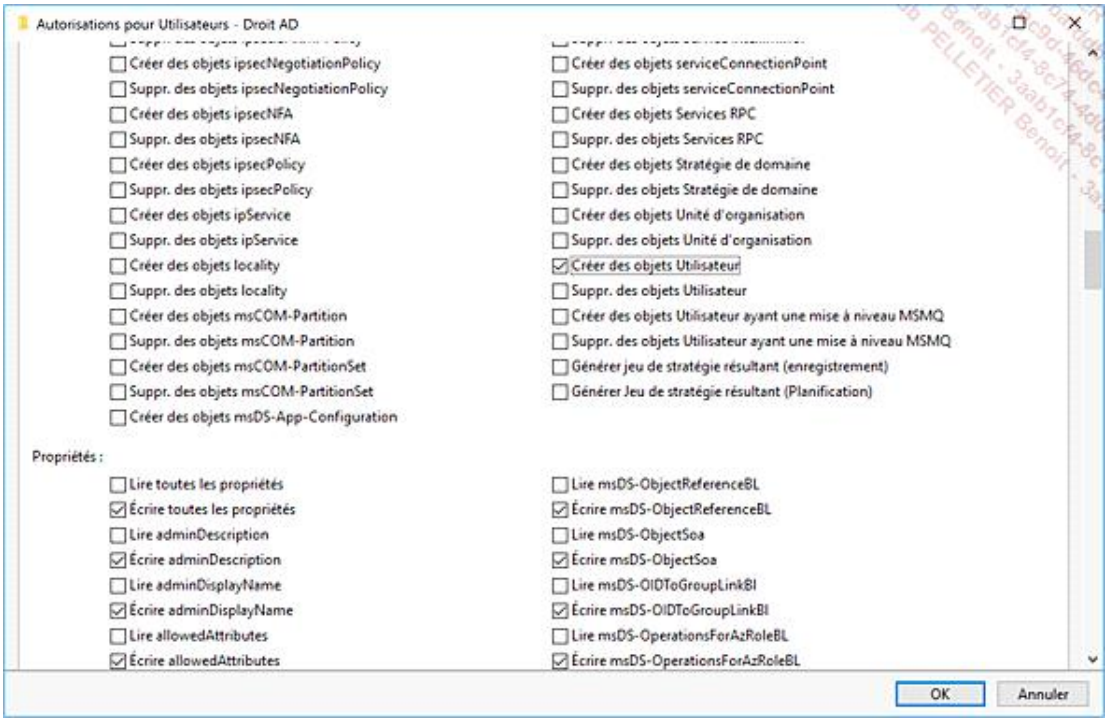
- Validez les différentes fenêtres en cliquant sur **OK**.

Il est maintenant nécessaire d'octroyer les droits adéquats sur l'unité d'organisation de destination.

- Depuis la console **Modification ADSI**, effectuez un clic droit sur l'unité d'organisation de destination. Dans le menu contextuel, cliquez sur **Propriétés**.
- Sélectionnez l'onglet **Sécurité** puis cliquez sur **Avancé**.
- Cliquez sur **Ajouter** dans la fenêtre qui s'affiche puis, à l'aide du lien **Sélectionner un principal**, sélectionnez l'utilisateur souhaité.



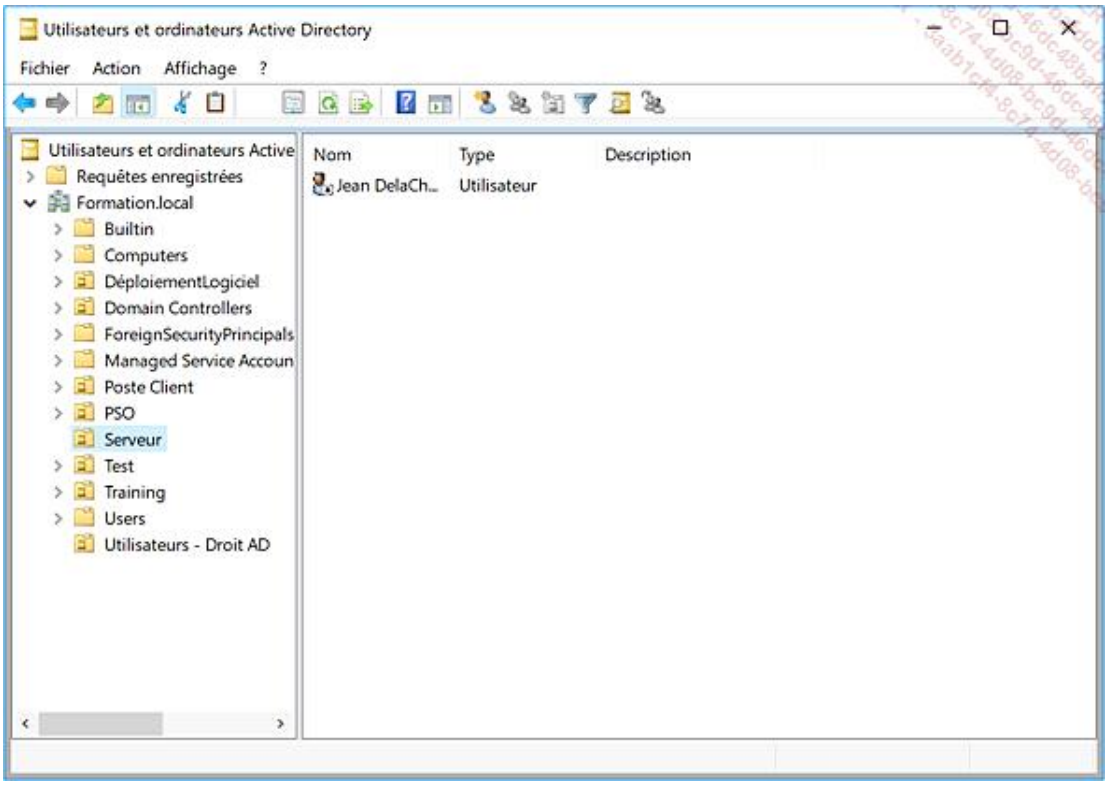
- Donnez à l'utilisateur le droit **Créer des objets Utilisateur** puis validez à l'aide du bouton **OK**.



Validez les fenêtres suivantes sans effectuer de modification.

Il est nécessaire d'installer, si cela n'est pas déjà fait, les outils RSAT sur le poste Windows 10. Par la suite, ouvrez une session en tant qu'utilisateur. Ce dernier ne doit pas avoir de droits d'administration sur le domaine (administrateur du poste au maximum).

En accédant à l'unité d'organisation **Serveur**, on peut s'apercevoir que les droits sont limités. L'utilisateur peut créer un autre utilisateur, mais ce dernier sera néanmoins désactivé. Il a également la possibilité de le déplacer dans l'unité d'organisation **Utilisateurs - Droit AD**.



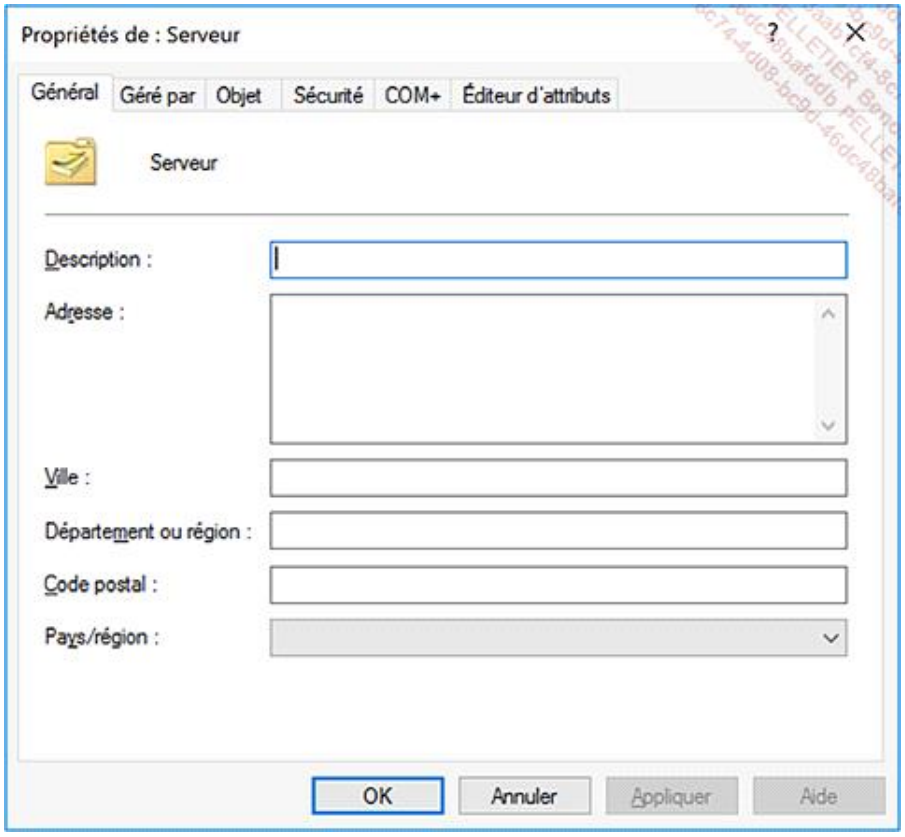
Aucun droit n'est accordé sur les autres unités d'organisation.

b. Activation de comptes utilisateurs

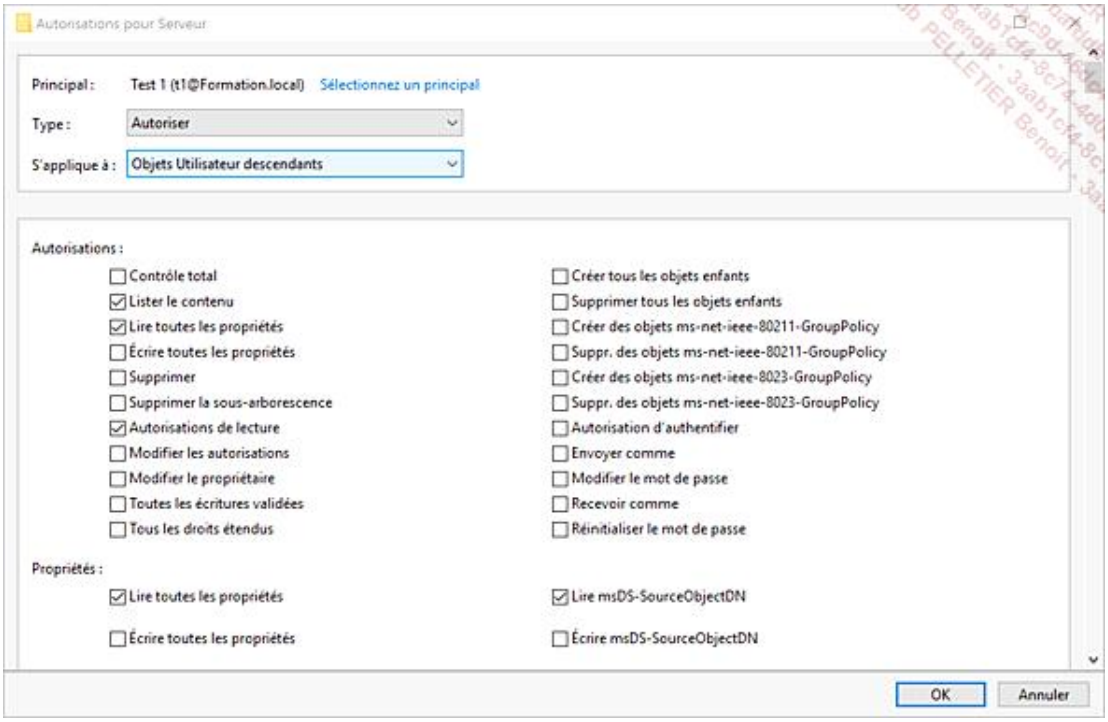
Nous avons vu avec la délégation précédente que l'utilisateur test 1 a la possibilité de créer des comptes utilisateurs dans certaines unités d'organisation. Néanmoins, le compte possédera un état désactivé.

Les opérations suivantes permettent de déléguer l'activation d'un compte utilisateur.

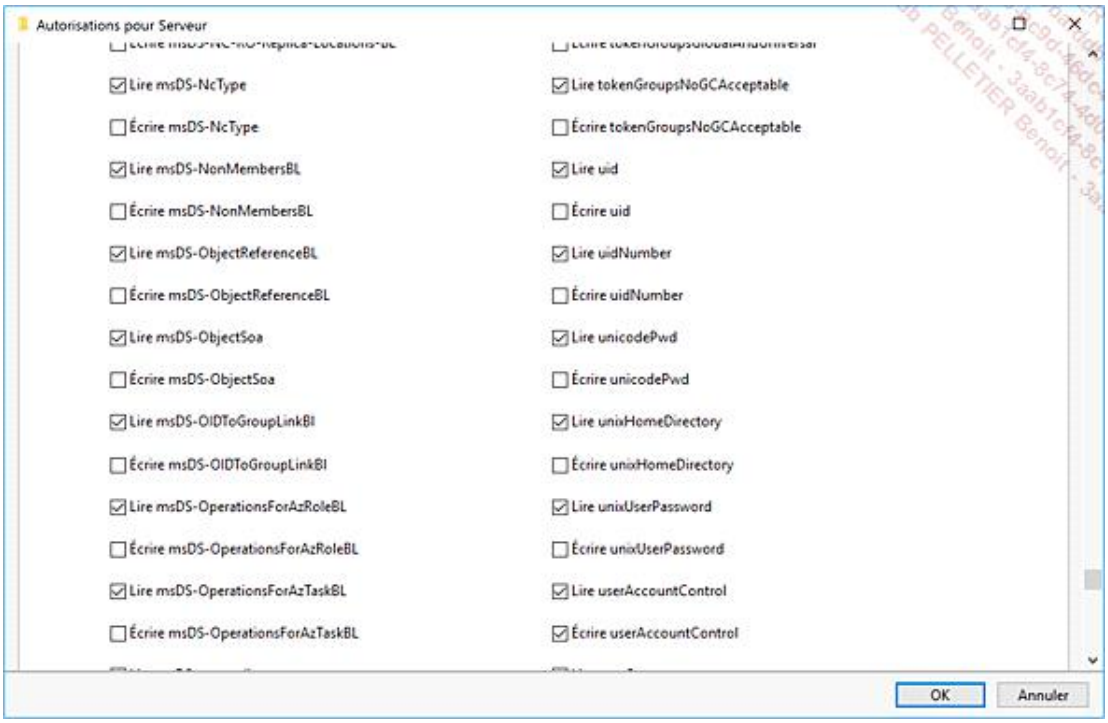
- Sur **AD1**, accédez à la console **Utilisateurs et ordinateurs Active Directory**.
- Cliquez sur **Affichage** dans la barre de menu puis sur **Fonctionnalités avancées**.
- Effectuez un clic droit sur l'unité d'organisation souhaitée puis, dans le menu contextuel, cliquez sur **Propriétés**.



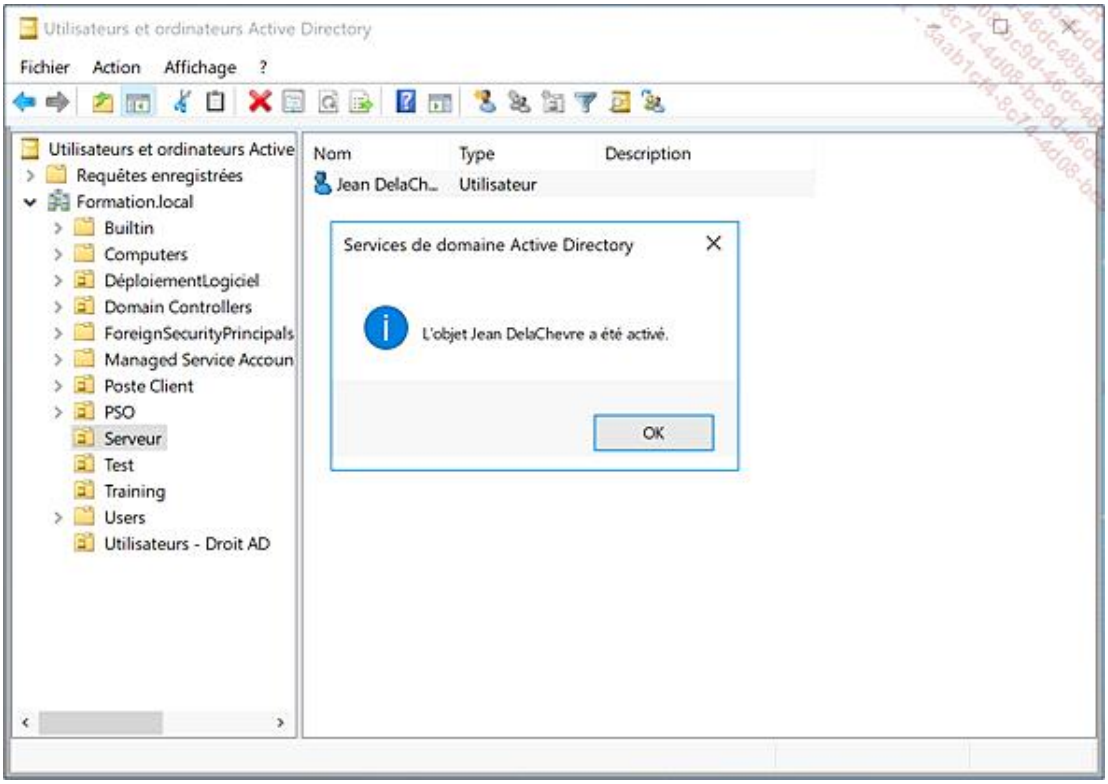
- Sélectionnez l'onglet **Sécurité** puis cliquez sur le bouton **Avancé**.
- Une fenêtre s'affiche, cliquez sur **Ajouter**.
- À l'aide du lien **Sélectionner le principal**, sélectionnez le compte utilisateur.
- Dans la liste déroulante **S'applique à**, sélectionnez **Objets Utilisateur descendants**.



- Donnez à l'utilisateur les droits **Lire userAccountControl** et **Écrire userAccountControl**.



- Cliquez sur **OK** afin de valider la modification.
- Sur **AD1**, procédez à la création d'un utilisateur dans l'unité d'organisation puis désactivez ce compte.
- Sur **CL10-01**, ouvrez une session avec le compte utilisateur à qui le droit a été délégué.
- Tentez de procéder à l'activation du compte. L'opération peut être effectuée pour les comptes présents dans l'unité d'organisation.

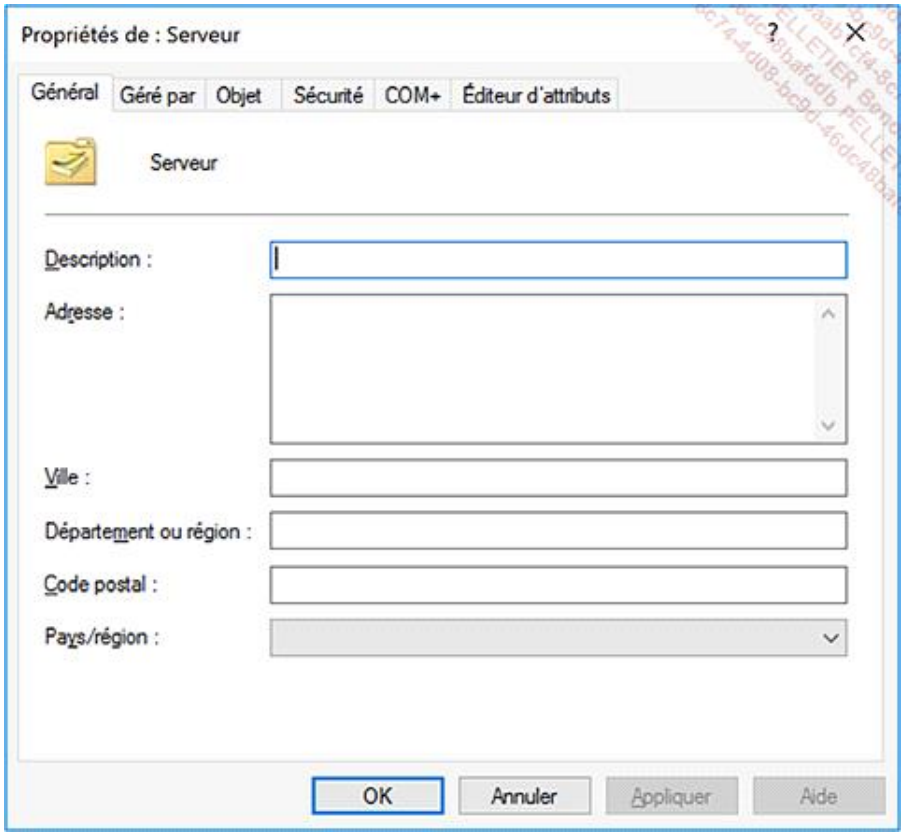


Le compte est correctement activé.

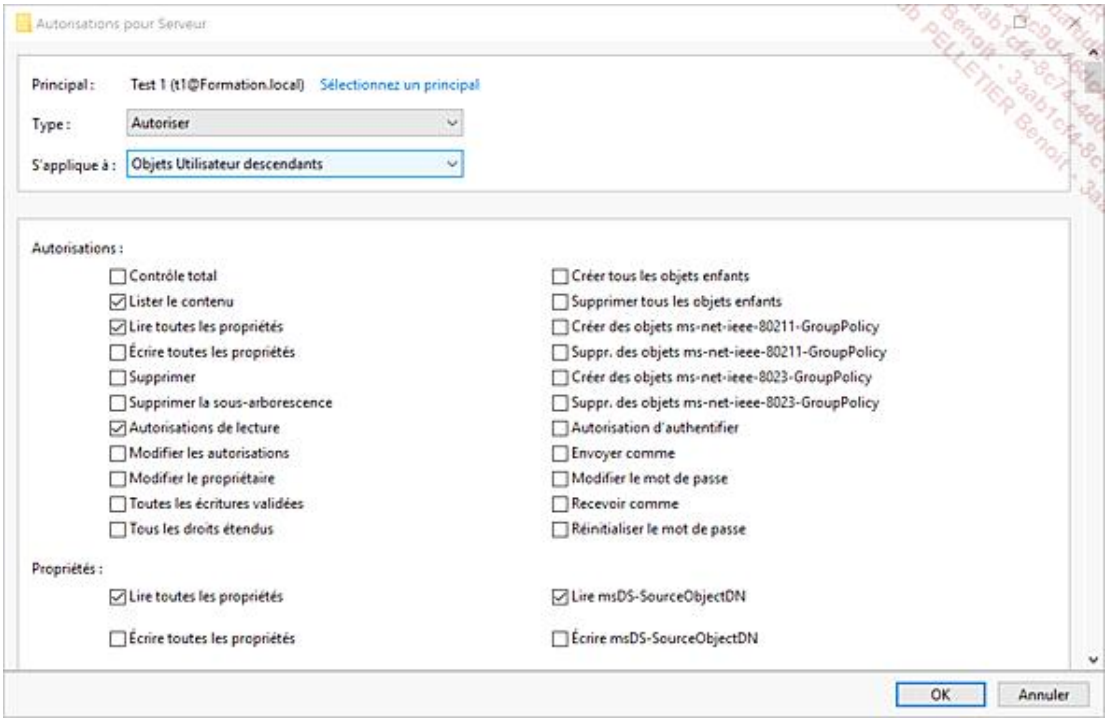
c. Réinitialisation de mot de passe

Il peut être nécessaire d'octroyer à une équipe support la réinitialisation d'un mot de passe d'un compte AD. Les opérations ci-dessous permettent de déléguer la réinitialisation du mot de passe sans pour autant posséder des droits d'admins du domaine.

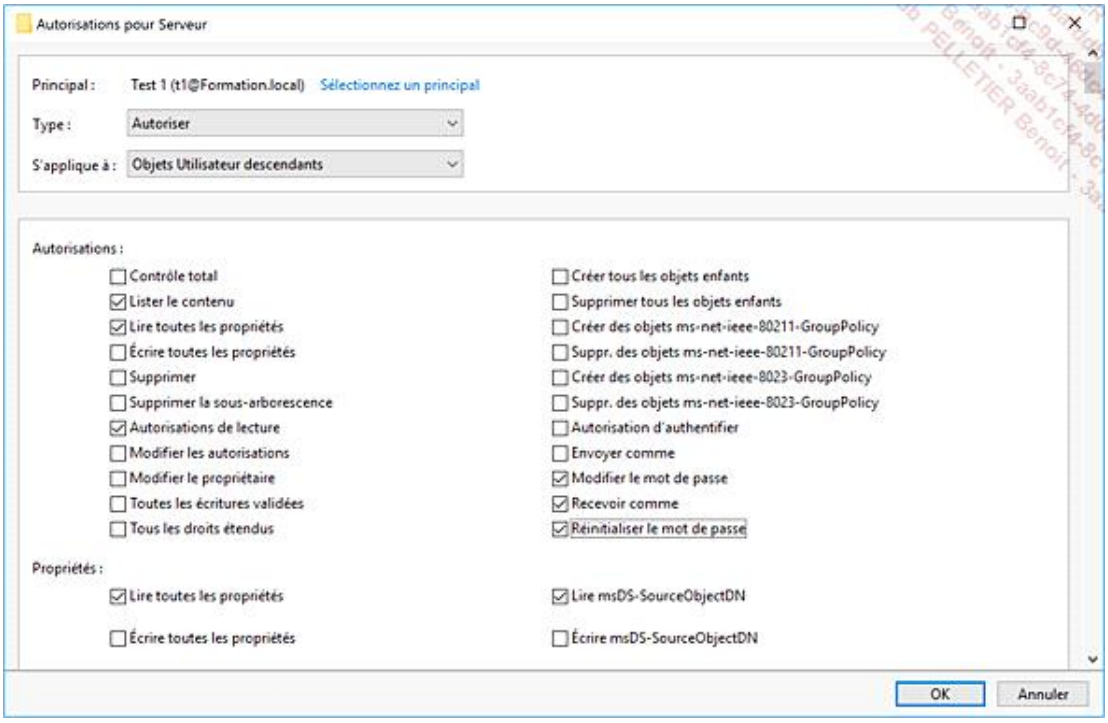
- Sur **AD1**, accédez à la console **Utilisateurs et ordinateurs Active Directory.**
- Cliquez sur **Affichage** dans la barre de menu puis sur **Fonctionnalités avancées**.
- Effectuez un clic droit sur l'unité d'organisation souhaitée puis, dans le menu contextuel, cliquez sur **Propriétés**.



- Sélectionnez l'onglet **Sécurité** puis cliquez sur le bouton **Avancé**.
- Une fenêtre s'affiche, cliquez sur **Ajouter**.
- À l'aide du lien **Sélectionner le principal**, sélectionnez le compte utilisateur.
- Dans la liste déroulante **S'applique à**, sélectionnez **Objets Utilisateur descendants**.



- Donnez à l'utilisateur les droits **Modifier le mot de passe**, **Recevoir comme** et **Réinitialiser le mot de passe**.



- Cliquez sur **OK** pour valider la modification.
- Depuis le poste Windows 10, tentez de modifier le mot de passe de l'utilisateur présent dans l'unité d'organisation Serveur.

2. Délégation du serveur d'impression

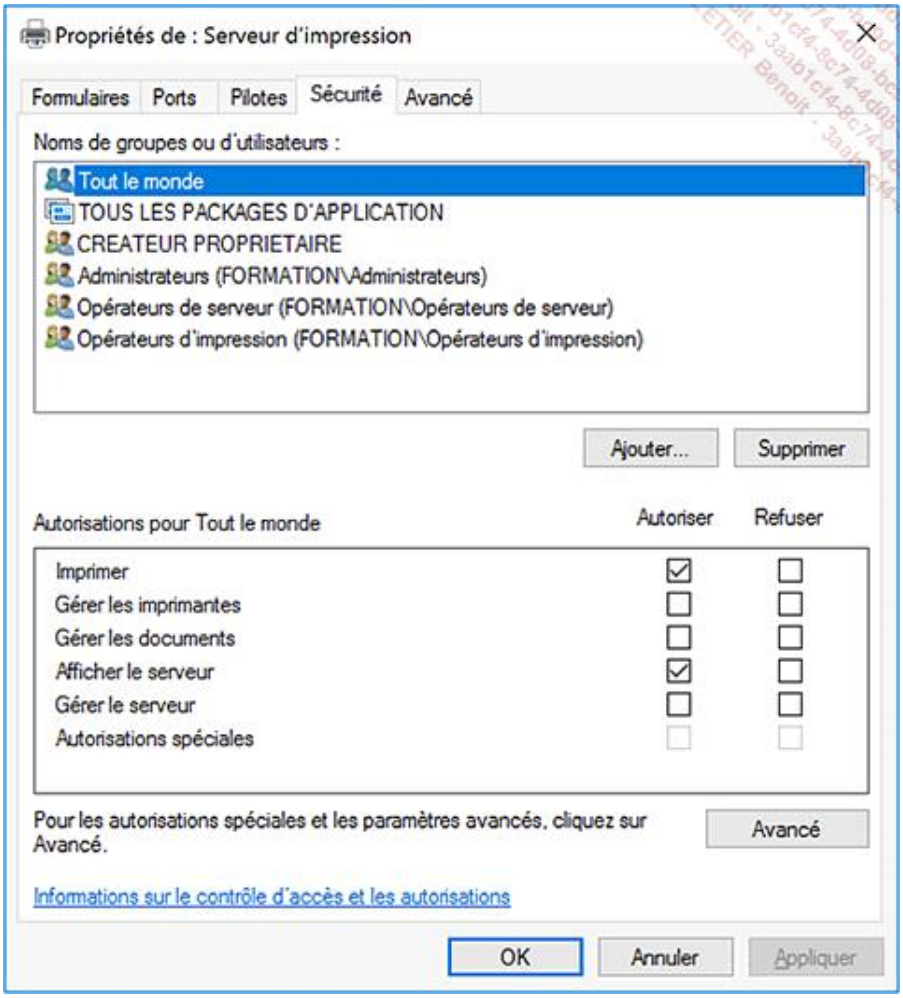
La délégation de l'administration du serveur d'impression peut être effectuée de plusieurs manières.

La première solution consiste à ajouter le compte de l'utilisateur en tant qu'administrateur local du serveur d'impression.

Il est néanmoins conseillé de définir des droits plus affinés. Cette solution nécessite d'accéder aux propriétés du serveur d'impression.



Des autorisations peuvent être données à un utilisateur depuis l'onglet **Sécurité**.


Propriétés de : Serveur d'impression
Formulaires
Ports
Pilotes
Sécurité
Avancé
Noms de groupes ou d'utilisateurs :
Tout le monde
TOUS LES PACKAGES D'APPLICATION
CREATEUR PROPRIETAIRE
Administrateurs (FORMATION\Administrateurs)
Opérateurs de serveur (FORMATION\Opérateurs de serveur)
Opérateurs d'impression (FORMATION\Opérateurs d'impression)
Ajouter...
Supprimer
Autorisations pour Tout le monde
Autoriser
Refuser
Imprimer
Gérer les imprimantes
Gérer les documents
Afficher le serveur
Gérer le serveur
Autorisations spéciales
Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé.
Avancé
Informations sur le contrôle d'accès et les autorisations
OK
Annuler
Appliquer

Conteneur des stratégies de groupe

Les différentes informations des stratégies de groupe sont réparties dans deux conteneurs :

- Le GPC (*Group Policy Container*) qui permet le stockage des propriétés comme le numéro de version, le statut ou les filtres WMI. Il est stocké dans l'annuaire Active Directory.
- Le GPT (*Group Policy Template*) contient les différents paramètres (sécurité, scripts et paramètres liés au registre). Ce container se trouve dans le dossier SYSVOL.

Les deux containers sont stockés dans deux endroits différents (AD et SYSVOL), la réplication utilise donc deux systèmes distincts. Le GPC stocké dans Active Directory est répliqué avec ce dernier. Le GPT utilise lui le système de réplication FRS (réplication de fichiers) pour effectuer la réplication. Des problèmes peuvent survenir sur un ou l'autre des systèmes de réplication, ce qui engendre éventuellement des données incohérentes entre les deux.

Utilisation de l'outil GPOTool

Cet outil, qui permet d'effectuer la vérification d'une stratégie de groupe, fonctionne depuis Windows 2000. La cohérence des GPO entre les conteneurs GPC et GPT peut être testée à l'aide de cet outil.

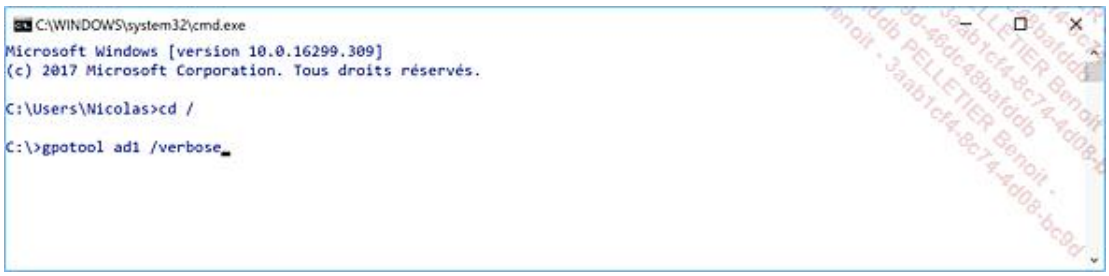
Ce dernier est gratuit et peut être téléchargé dans le Resource Kit Tools pour Windows Server 2003.

Néanmoins, si le système d'exploitation exécute Windows Server 2008 ou version supérieure, il est possible de récupérer l'exécutable de la commande en allant sur mon blog : http://www.nibonnet.fr/?p=272

- Téléchargez l'exécutable et insérez-le à la racine de la partition **C**.
- Lancez une invite de commandes DOS puis saisissez **cd /**.

L'instruction permet de sélectionner la racine de la partition.

- Saisissez la commande `gpotool ad1 /verbose`.



Il est donc plus facile de détecter un éventuel problème de réplication. Dans le cas d'une erreur dans la réplication, les journaux d'événements doivent être utilisés pour tenter de déceler la source du problème

Jeu de stratégie résultant

Le jeu de stratégie résultant (RSoP, *Resultant Set of Policy*) permet l'élaboration de rapports sur les différents paramètres de stratégie de groupe appliqués à un utilisateur ou un ordinateur. Ces rapports peuvent être créés à l'aide de la console **Gestion de la stratégie de groupe** (GPMC - *Group Policy Management Console*) ou par l'intermédiaire de la commande `gpresult`. Les données du jeu de stratégie résultant sont extraites de l'ordinateur cible puis présentées dans un rapport au format HTML.

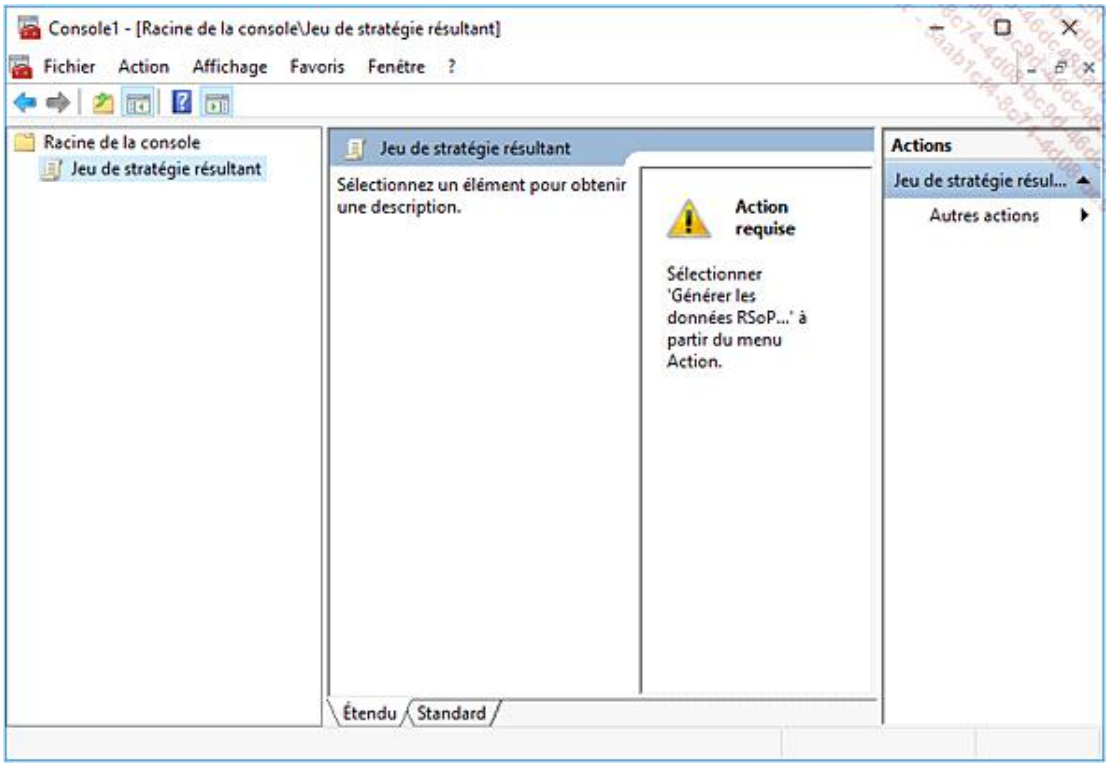
Plusieurs scénarios peuvent imposer un dépannage, comme une stratégie qui ne s'applique pas ou des paramètres qui s'appliquent mais sont complètement incohérents.

Dans un premier temps, il est important de vérifier la connectivité réseau à l'aide de la commande `ping`. Cette dernière permet de s'assurer de la réponse du contrôleur de domaine au niveau IP. Une fois cette étape validée, la résolution de noms DNS doit être testée à l'aide de la commande `nslookup`.

Si les deux outils ne remontent aucun problème, les journaux d'événements (journaux **Système**, **Application** et **Group Policy**) ainsi que le jeu de stratégie résultant doivent être utilisés.

1. Utilisation de la commande RSoP

- Sur le poste client CL10-01, ouvrez une session en tant que **nbonnet**.
- Ouvrez une console MMC et ajoutez le composant logiciel enfichable **Jeu de stratégie résultant**.



- Effectuez un clic droit sur le nœud **Jeu de stratégie résultant** puis sélectionnez **Générer les données RSoP**.
- L'assistant se lance. Cliquez sur **Suivant**.

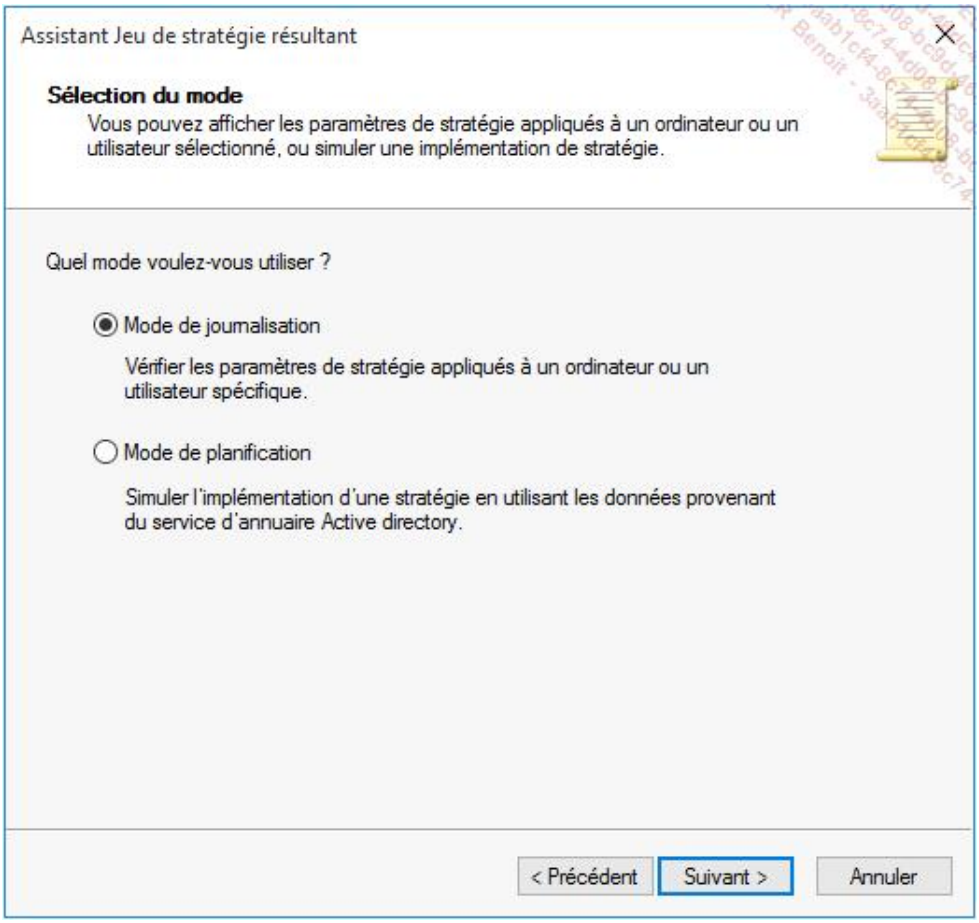
Deux modes sont utilisables :

- **Mode de journalisation**, qui permet de vérifier les paramètres de stratégie appliqués à un ordinateur ou un

utilisateur.

- **Mode de planification**, qui simule l'application d'une stratégie de groupe. Les données sont récupérées depuis Active Directory.

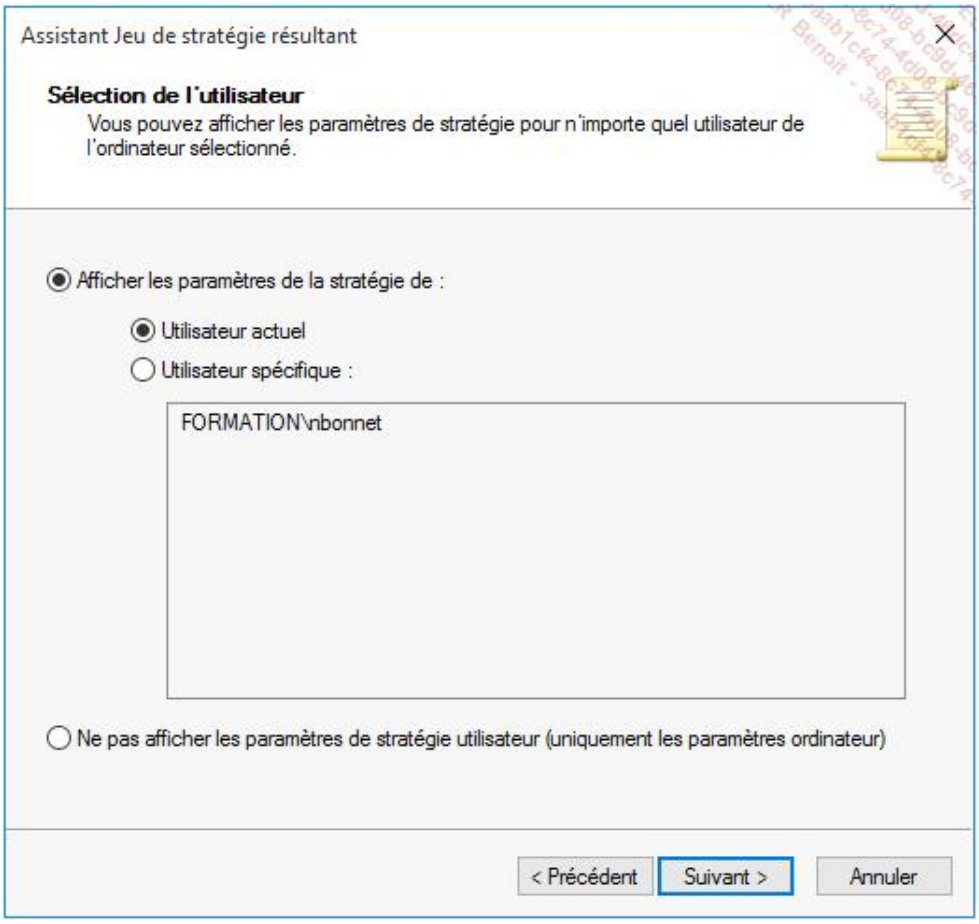
Sélectionnez **Mode de journalisation** puis cliquez sur **Suivant**.



Depuis l'assistant, il est possible de sélectionner l'ordinateur souhaité.

Laissez le choix sur **Cet ordinateur** puis cliquez sur **Suivant**.

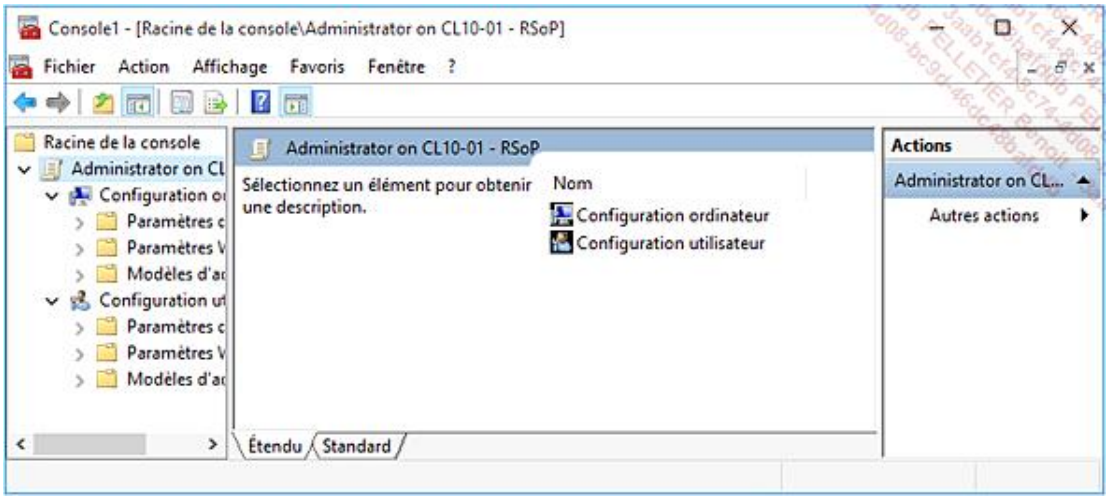
Les paramètres qui doivent être récupérés sont ceux de l'utilisateur en cours. Laissez le choix par défaut dans la fenêtre **Sélection de l'utilisateur** puis cliquez sur **Suivant**.



- Dans la fenêtre **Aperçu des sélections**, cliquez sur **Suivant** afin de lancer la récupération des paramètres.
- Cliquez sur **Terminer** pour fermer l'assistant.

La console MMC se lance et présente les paramètres qui sont appliqués pour les parties utilisateur et ordinateur.

Si le compte utilisateur n'est pas membre du groupe Admins du domaine, la partie ordinateur ne s'affiche pas.



Seuls les paramètres appliqués pour l'utilisateur et l'ordinateur s'affichent.

2. Utilisation de la commande gpresult

`gpresult` est un outil en ligne de commande qui permet l'affichage du jeu de stratégie résultant (RSoP, *Resultant Set Of Policy*). Ce dernier est valable pour les utilisateurs ou pour les ordinateurs. La commande permet également de résoudre d'éventuels problèmes ou de connaître les stratégies en vigueur.

Le rapport présente les stratégies de groupe qui sont appliquées et celles qui sont refusées.

La commande possède plusieurs commutateurs dont :

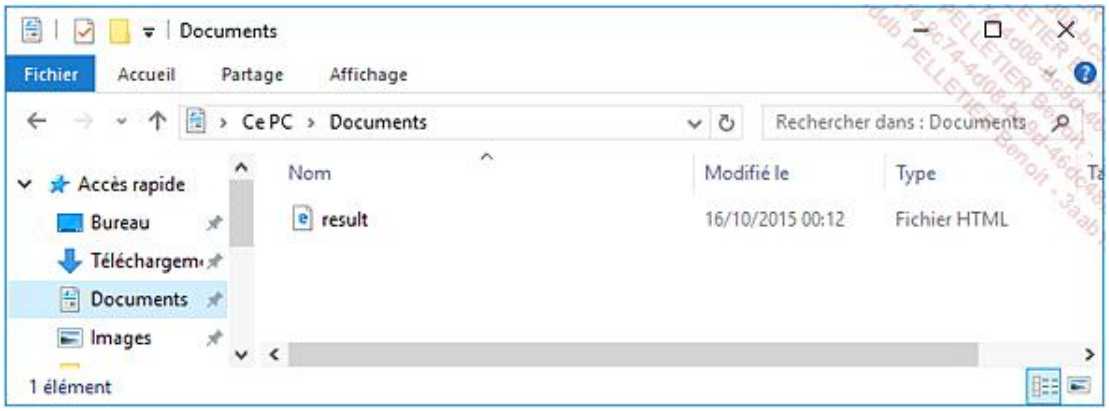
- `/s <computer>` : permet de spécifier l'adresse IP ou le nom du poste distant. Par défaut, l'ordinateur local est utilisé.
- `/u <username>` : spécifie les informations d'identification de l'utilisateur pour l'exécution de la commande. L'utilisateur par défaut est celui dont la session a été ouverte.
- `/p <password>` : le commutateur doit être utilisé si /u est présent dans la commande. Le mot de passe est demandé s'il n'est pas saisi dans la commande.
- `/User [<TARGETDOMAIN> \] <TARGETUSER>` : le nom d'utilisateur renseigné est utilisé pour l'élaboration des données RSoP.
- `/scope {utilisateur | ordinateur}` : permet de limiter les données RSoP affichées à l'utilisateur ou à l'ordinateur. Si le commutateur n'est pas utilisé, le rapport présente les données pour l'utilisateur et l'ordinateur.

La documentation de la commande `gpresult` est accessible à l'adresse : http://technet.microsoft.com/en-us/library/cc733160.aspx

- Sur le poste CL10-01, lancez une invite de commandes DOS.
- Saisissez la commande : `gpresult /H c:\Users\nbonnet\Documents\result.html`

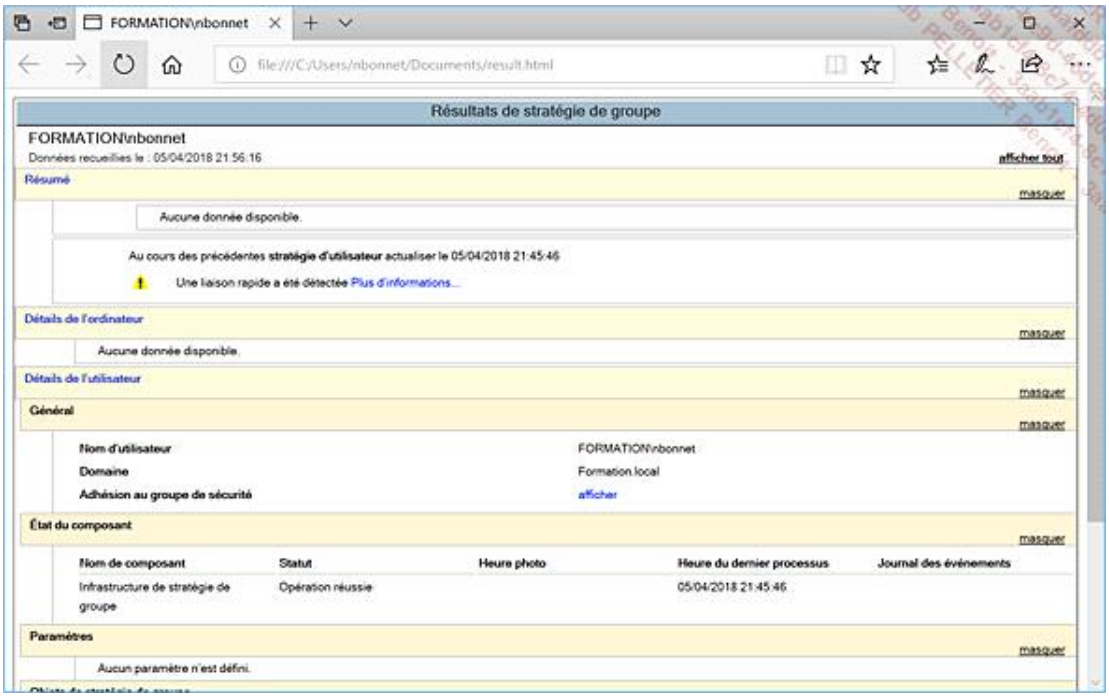


Le rapport est créé dans le dossier indiqué à l'aide du commutateur **/H** (**c:\users\nbonnet\Documents**).



- Double cliquez sur le fichier **result.html**.

Le rapport présente les stratégies appliquées et refusées, mais également les raisons de ces refus.

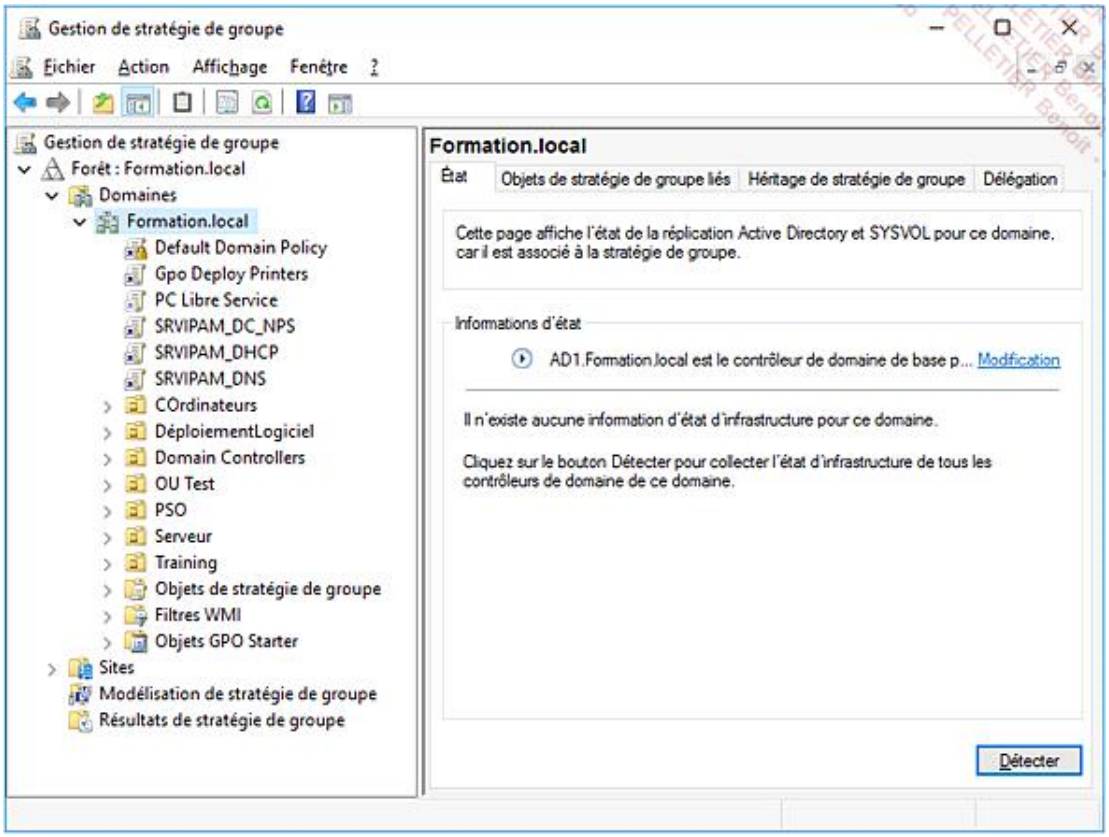


Il est donc plus aisé de comprendre la raison pour laquelle une stratégie de groupe n'est pas appliquée ou la raison de l'application de paramètres incohérents.

3. Résultat de stratégie de groupe

La console Gestion des stratégies de groupe intègre également un outil permettant la création de rapports sur la stratégie appliquée à un poste ou à un utilisateur. Un des avantages de cette console est de pouvoir centraliser la création de rapports. La relance de la requête y est également plus facile.

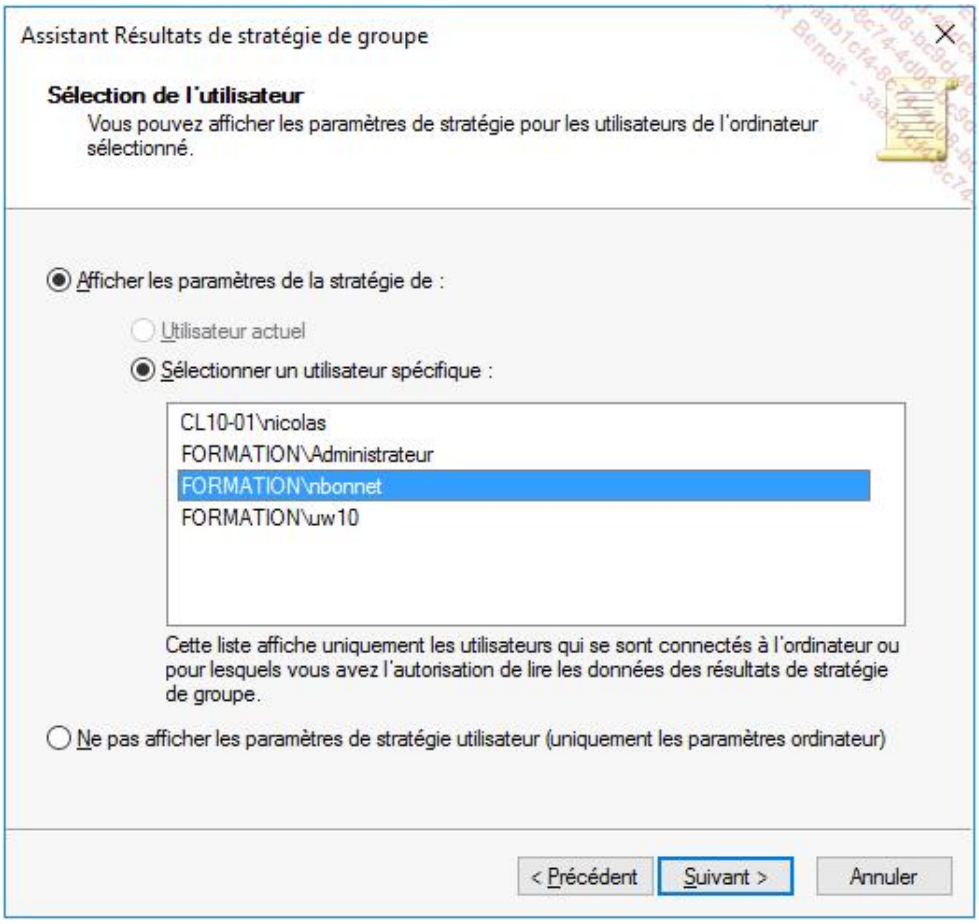
- Ouvrez une session sur AD1 en tant qu'administrateur.
- Lancez la console **Gestion de stratégie de groupe**.
- Effectuez un clic droit sur **Résultats de stratégie de groupe** puis sélectionnez **Assistant Résultats de stratégie de groupe**.



- L'assistant se lance, cliquez sur **Suivant**.
- Dans la fenêtre **Sélection des ordinateurs**, sélectionnez **Un autre ordinateur**.
- Cliquez sur le bouton **Parcourir** afin de sélectionner l'ordinateur.
- Saisissez **CL10-01** puis cliquez sur **Vérifier les noms**.
- Cliquez sur **OK** puis sur **Suivant**.

La console a besoin de se connecter au poste. Le pare-feu peut bloquer la connexion.

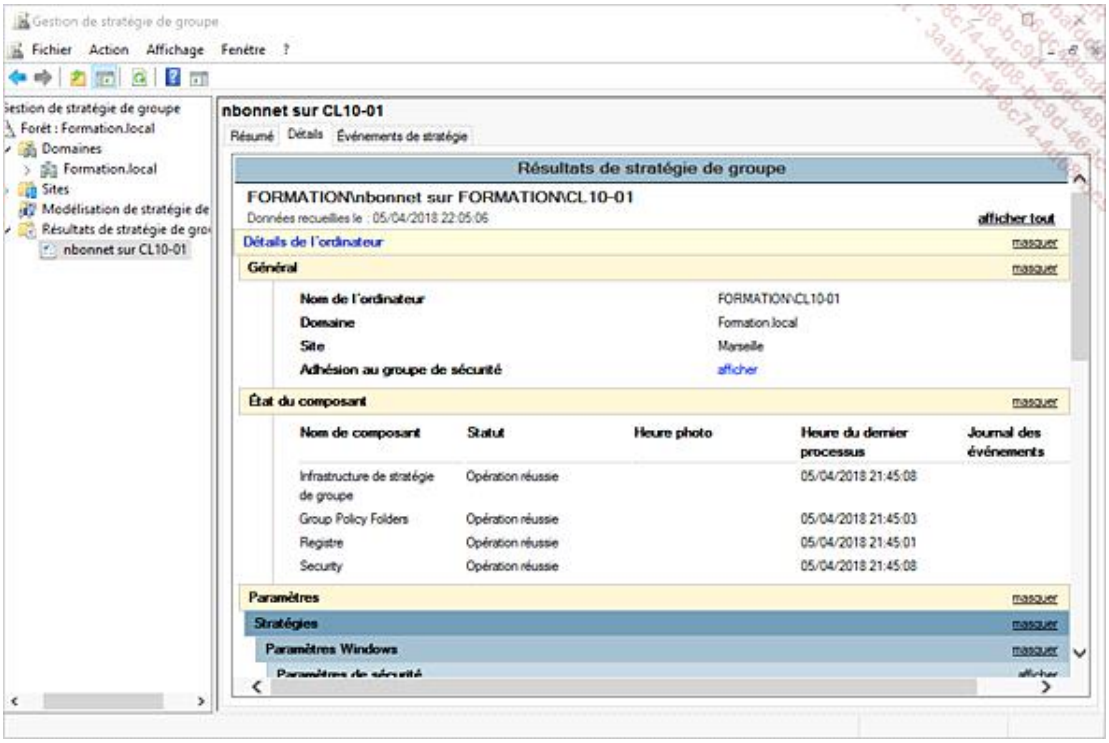
- Sélectionnez l'utilisateur souhaité puis cliquez sur **Suivant**.



Une session doit avoir été ouverte au moins une fois par l'utilisateur sur le poste.

Cliquez sur **Suivant** afin de lancer la création du rapport, puis sur **Terminer**.

Le rapport s'affiche.



Il est possible de relancer la requête et d'actualiser le rapport en effectuant un clic droit sur le rapport et en sélectionnant l'option **Relancer la requête**.

Opérations de maintenance sur l'infrastructure

Le paramétrage d'une stratégie de groupe peut prendre un certain temps. Il suffit malheureusement de quelques secondes pour supprimer et perdre l'ensemble des paramètres qu'elle contient.

Pour éviter ce problème, des solutions permettant la sauvegarde et la restauration des différentes stratégies sont mises en place depuis la console **Gestion de stratégie de groupe**. Elles permettent également l'exportation des stratégies vers un autre domaine.

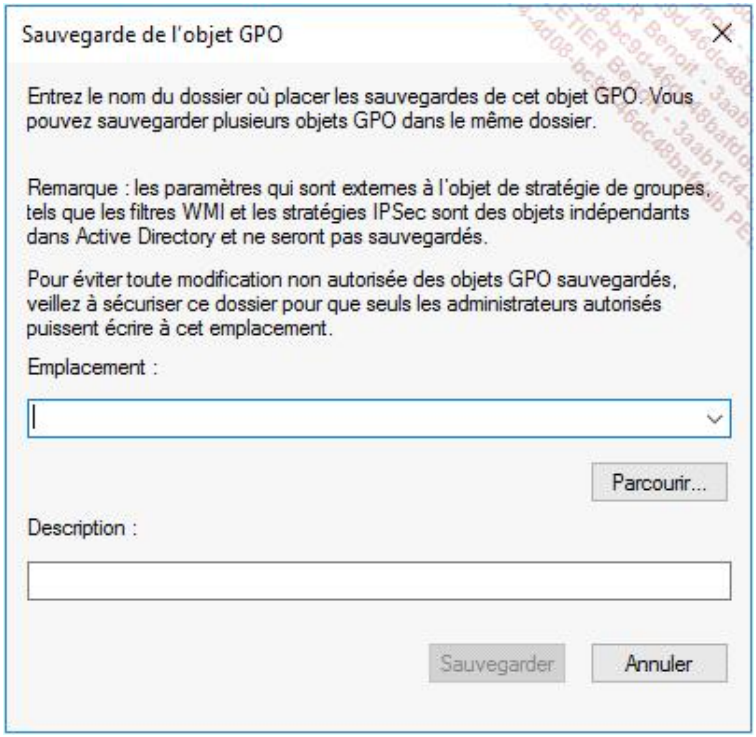
1. Sauvegarde d'une stratégie

La première étape est donc d'effectuer une sauvegarde de la stratégie de groupe afin de pouvoir effectuer une restauration des paramètres.

- Ouvrez une session sur AD1 en tant que **Formation\administrateur**.
- Lancez la console **Gestion de stratégie de groupe** puis développez les nœuds **Forêt : Formation.local**, **Domaines** puis **Formation.local**.
- Cliquez sur le conteneur **Objets de stratégie de groupe**.

Si vous effectuez un clic droit sur ce conteneur, le menu contextuel vous donne accès à l'option **Sauvegarder tout** qui permet la sauvegarde de l'ensemble des stratégies présentes.

- Effectuez un clic droit sur la stratégie **Audit dossier informatique** puis sélectionnez **Sauvegarder**.
- Dans la fenêtre **Sauvegarde de l'objet GPO**, cliquez sur le bouton **Parcourir**.



- Sélectionnez la partition **C:** puis créez un nouveau dossier nommé **Sauvegarde GPO**.
- Cliquez sur **OK** puis sur **Sauvegarder**.
- Cliquez sur **OK** à la fin de l'opération.

La stratégie peut désormais être restaurée très facilement.

2. Restauration et importation d'une stratégie

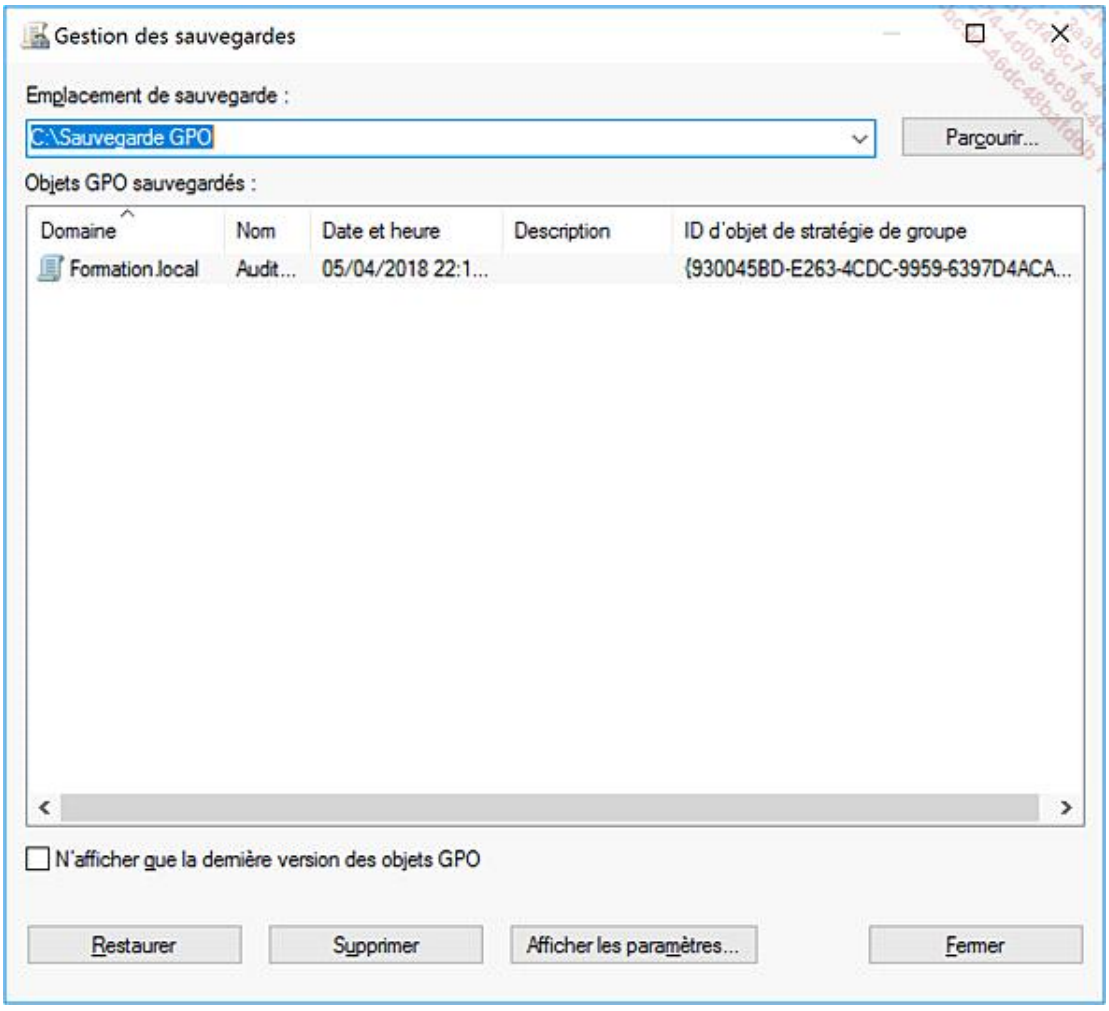
Le principe de la restauration est de recréer la stratégie telle qu'elle était au moment de la sauvegarde. Néanmoins, cette dernière n'est pas liée. Il convient donc d'effectuer par la suite la liaison à un conteneur.

- Dans la console **Gestion de stratégie de groupe**, supprimez la GPO **Audit dossier informatique**.
- Effectuez un clic droit sur le conteneur **Objets de stratégie de groupe** puis sélectionnez **Gérer les sauvegardes**.

La fenêtre est normalement redirigée dans le dossier de sauvegarde **C:\Sauvegarde GPO**.

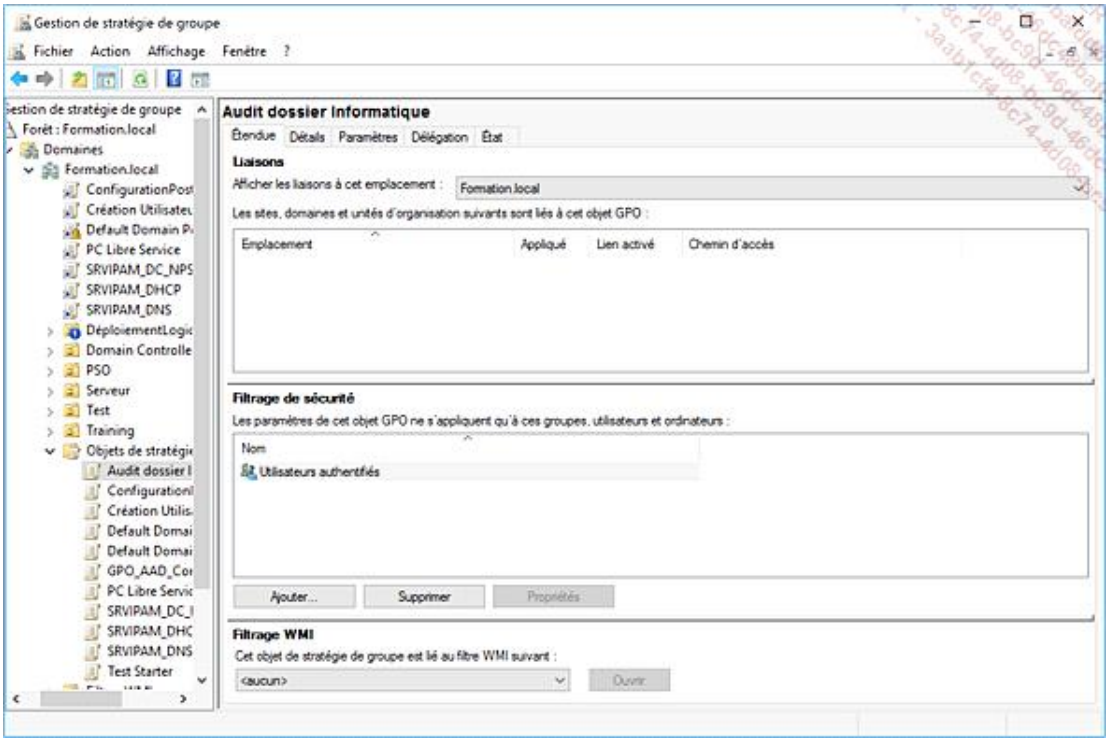
Il est possible de changer de répertoire à l'aide du bouton **Parcourir**.

- L'ensemble des stratégies sauvegardées dans ce dossier sont présentes. Cliquez sur **Audit dossier informatique** puis sur **Restaurer**.



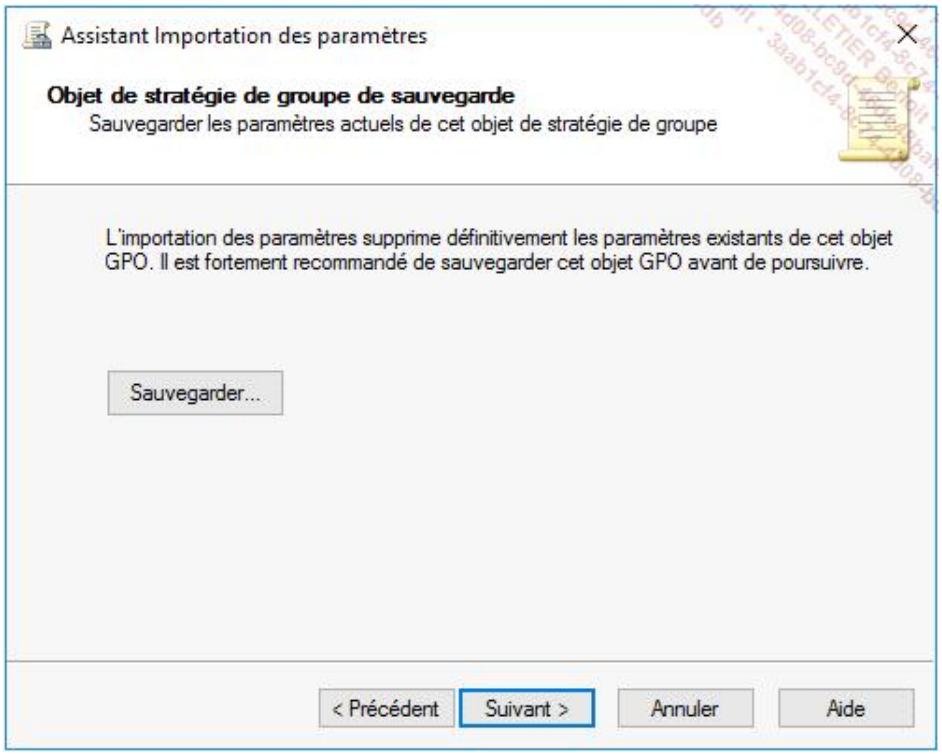
- Confirmez la restauration en cliquant sur **OK**.
- Cliquez sur **OK** puis sur **Fermer** afin de clôturer les fenêtres.

La stratégie apparaît désormais dans le conteneur **Objets de stratégie de groupe** mais n'est pas liée.

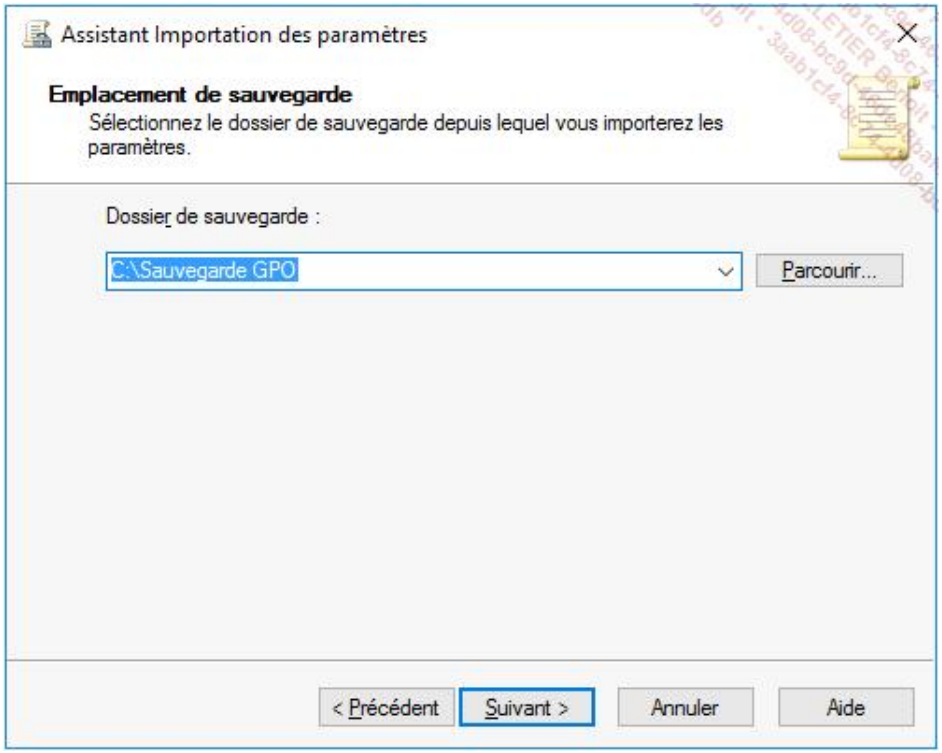


L'importation est une opération qui consiste à récupérer les paramètres d'une stratégie sauvegardée pour les insérer dans une stratégie nouvellement créée.

- Effectuez un clic droit sur **Objets de stratégie de groupe** puis sélectionnez **Nouveau**.
- Saisissez **GPO Test Import** dans le champ **Nom** puis cliquez sur **OK**.
- Effectuez un clic droit sur la stratégie nouvellement créée puis, dans le menu contextuel, sélectionnez **Importer des paramètres**.
- Cliquez sur **Suivant** dans la page de bienvenue de l'assistant.
- Aucune sauvegarde des paramètres actuels ne doit être lancée car la stratégie vient d'être créée. Cliquez sur **Suivant**.



- Le champ **Dossier de sauvegarde** doit contenir **C:\Sauvegarde GPO**, si ce n'est pas le cas, utilisez le bouton **Parcourir** afin de le sélectionner.



- L'ensemble des stratégies sauvegardées dans ce répertoire sont présentes dans la fenêtre **Objets de stratégie de groupe (GPO) source**. Sélectionnez **Audit dossier informatique** puis cliquez sur **Suivant**.
- Cliquez sur **Suivant** puis sur **Terminer**.
- Cliquez sur **OK** dans la fenêtre **Importer**.

La stratégie qui a été créée précédemment possède désormais des paramètres.

L’exportation de stratégie en est grandement facilitée. Si un chemin UNC compose votre GPO, une table de correspondance s’affiche permettant la modification des différents chemins.

Présentation du boot PXE

Le boot PXE (*Pre-boot eXecution Environment*) permet à une station de travail d'effectuer un démarrage depuis le réseau. L'installation du poste a lieu en récupérant l'image depuis le serveur PXE.

L'image peut être celle du système d'exploitation ou une image personnalisée contenant applications, pilotes…

Associée à un fichier de réponse, l'installation peut être effectuée de manière automatique. Seul le démarrage du poste et l'appui sur la touche [F12] (il est possible d'annuler l'obligation d'appuyer sur une touche) sont nécessaires.

L'amorce par la technologie PXE passe par plusieurs étapes :

- Demande d'une adresse IP à un serveur DHCP et recherche du fichier à amorcer.
- Téléchargement du fichier à l'aide du serveur TFTP (*Trivial File Transfer Protocol*).



Il est arrivé de ne pas pouvoir télécharger l'image depuis le serveur. La demande du poste client tourne sans aucune réponse avant d'afficher un time out. Dans ce cas, suivez la procédure présente sur ce blog : http://www.nibonnet.fr/?p=131

- Une fois l'étape de récupération terminée, l'exécution du fichier est démarrée.

Le boot PXE étant présenté, nous pouvons maintenant nous intéresser au serveur PXE. Présent dans les systèmes d'exploitation serveur de Microsoft, il apparaît dans la liste des rôles et porte le nom Windows Deployment Services (WDS).

Trois types d'images peuvent être utilisés, chacun ayant des avantages ou inconvénients.

- **Les images minces** : elles contiennent uniquement le système d'exploitation. Les applications doivent donc être installées par la suite. MDT (*Microsoft Deployment Toolkit*) ou une stratégie de groupe peuvent être utilisés. WDS (le service de déploiement de Windows) ne sait pas déployer une application.
- **Les images hybrides** : en plus du système d'exploitation, ces images contiennent également les applications communes (antivirus, Acrobat Reader…). Comme pour les images minces, les autres applications doivent être déployées par un autre moyen.
- **Les images volumiques** : ces images contiennent un système d'exploitation mais également l'ensemble des applications. Contrairement aux deux autres images, celle-ci ne peut être appliquée qu'à un nombre de postes limité (principalement à cause des applications présentes).

Les images hybrides et volumiques sont créées en capturant le poste (avec le système de déploiement Windows ou un autre outil - voir plus loin dans ce chapitre). Pour les images minces, il suffit d'importer le DVD de Windows 10 dans le serveur de déploiement.

Présentation et prérequis

Depuis Windows Server 2003 SP2, WDS (*Windows Deployment Services*) est présent sur les plateformes serveur. Depuis sa première version, il n'a cessé de connaître des améliorations.

1. WDS sous Windows Server 2008 R2

Présent en tant que rôle, il est possible de l'installer par l'intermédiaire de la console **Gestionnaire de serveur** en ajoutant le rôle **Services de déploiement Windows**.

Sous Windows Server 2008 R2 le rôle se voit ajouter plusieurs fonctionnalités :

- **Approvisionnement en pilotes dynamiques** : il est possible d'effectuer un déploiement de packages de pilotes sur un ordinateur client, ceci par l'intermédiaire d'une installation du poste. L'ajout de ces pilotes peut également s'effectuer sur les images de démarrage. Ainsi, l'administrateur n'a plus besoin d'importer les pilotes dans l'image de démarrage et la taille de celle-ci s'en trouve réduite. L'utilisation d'une image pour plusieurs configurations est donc plus facilement gérable.
- **Déploiement de disque dur virtuel** : le déploiement de fichiers portant l'extension VHD (*Virtual Hard Disk*) peut maintenant être effectué par le service de déploiement Windows. Ce type d'images est déployé de la même manière que les images de type WIM. Le format WIM est un format utilisé depuis Windows Vista. Il permet la mise en place d'un taux de compression de l'image, et l'imbrication de plusieurs images dans une seule. Il convient de noter que ce type de fichier peut être facilement modifié et ne détruit pas les données présentes sur le poste au moment de son application. Cette opération nécessite néanmoins d'utiliser la ligne de commande WDSUTIL.
- **Transmission en multicast** : la transmission en multicast permet d'économiser de la bande passante en effectuant le transfert des données au travers du réseau en multicast.

2. Les anciennes versions de WDS

- **Déploiement de disque dur virtuel** : la version d'Hyper-V présente dans Windows Server 2012 R2 et version supérieure utilise un nouveau format (VHDX) pour les disques durs virtuels. Depuis Windows Server 2012 R2, WDS peut donc déployer ce nouveau type de disques durs virtuels.
- **Approvisionnement en pilotes dynamiques** : les filtres des groupes de pilotes prennent désormais en charge le numéro de modèle et les groupes d'appareils du fabricant.
- **Interface EFI (*Extensible Firmware Interface*)** : les clients équipés de processeurs 32 bits avec UEFI (*Unified Extensible Firmware Interface*) sont pris en charge pour démarrer en réseau et effectuer un déploiement.

3. Prérequis nécessaires pour le rôle

Le bon fonctionnement de ce rôle nécessite des prérequis.

- **ADDS (*Active Directory Domain Services*)** : le serveur ayant le rôle de WDS doit être membre du domaine Active Directory. Depuis Windows Server 2012 R2, il est possible d'installer un serveur WDS sans Active Directory. Pour cela le mode Autonome doit être sélectionné.
- **DHCP (*Dynamic Host Configuration Protocol*)** : un serveur DHCP doit être présent afin de fournir une adresse IP aux postes pendant le boot PXE. Néanmoins, les serveurs WDS et DHCP utilisent le même port (UDP 67). Si les deux rôles sont installés sur le même serveur, il est nécessaire de cocher les options **Ne pas écouter sur le port 67** et **Configurer l'option 60 du DHCP** (cette option permet d'indiquer que ce serveur est également serveur PXE). Ces options peuvent être sélectionnées lors de la configuration du serveur.
- **Volume NTFS** : le magasin d'images requiert un volume NTFS, ceci afin de pouvoir assigner les autorisations NTFS

adéquates.

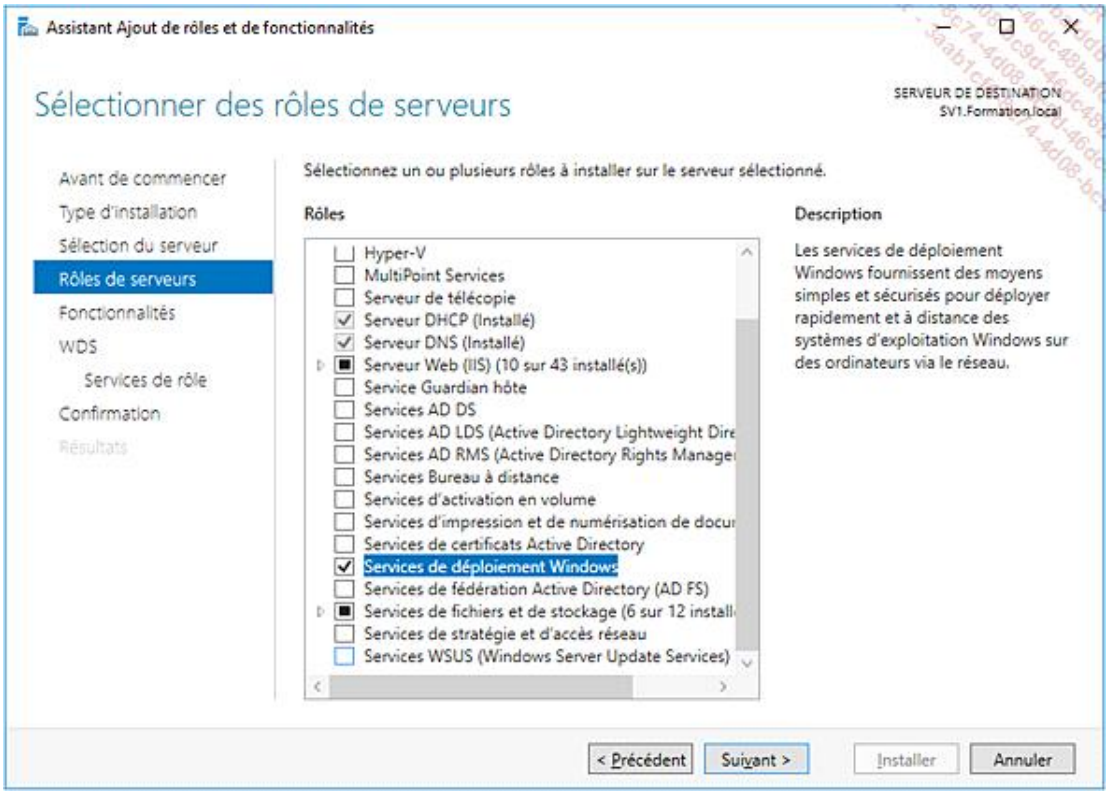
- **Credentials** : il est nécessaire de posséder un compte administrateur afin d'installer le rôle. Si ce dernier est installé sur un serveur membre, le compte doit uniquement être membre du groupe Administrateurs local de la machine.

Mise en place de WDS

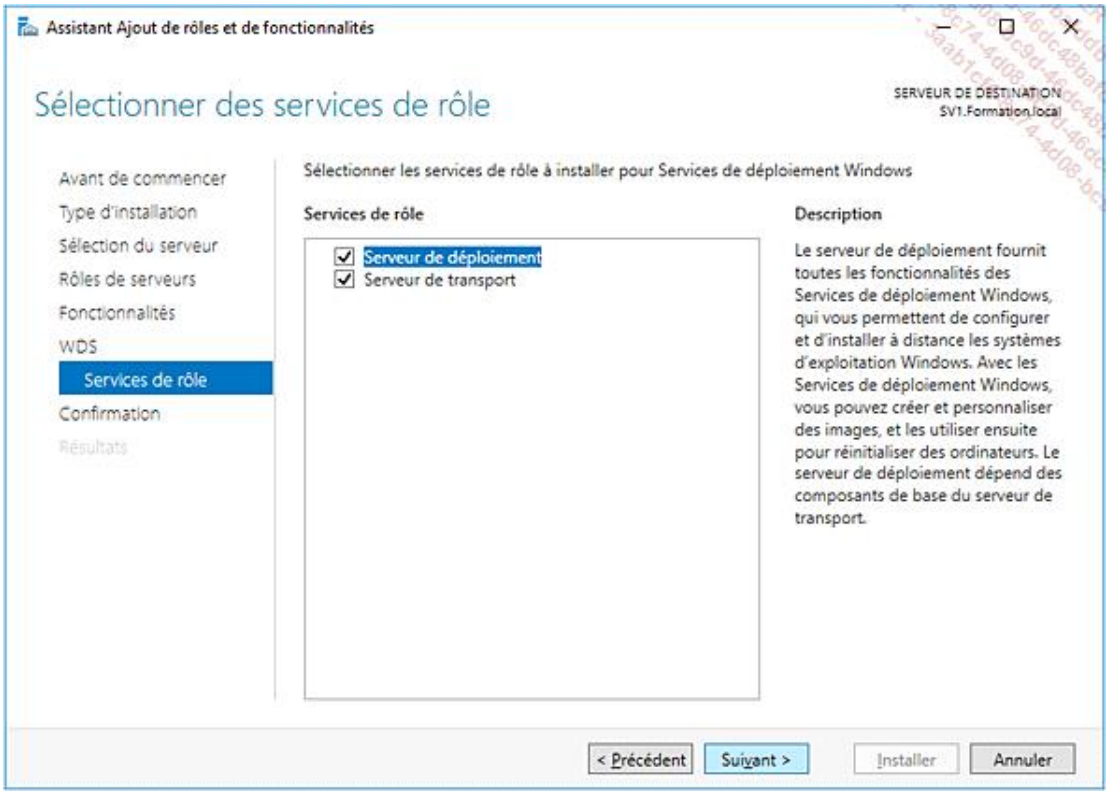
La mise en place du serveur nécessite de réfléchir à une architecture. En effet, il n'est pas conseillé d'effectuer un déploiement via une ligne WAN (ligne reliant deux sites distants). Il peut donc être nécessaire d'effectuer l'installation de plusieurs serveurs. Le deuxième élément de réflexion est le choix du serveur. N'oubliez pas que si le rôle DHCP est présent sur le même serveur, des manipulations sont nécessaires. Un oubli de ces dernières provoque le non-fonctionnement du service WDS.

1. Installation du serveur

- Démarrez la machine SV1 puis ouvrez une session en tant qu'administrateur.
- Lancez la console **Gestionnaire de serveur** puis cliquez sur **Ajouter des rôles et des fonctionnalités**.
- L'assistant se lance. Cliquez sur **Suivant** dans la fenêtre **Avant de commencer**.
- Dans la fenêtre **Sélectionner le type d'installation**, laissez cochée **Installation basée sur un rôle ou une fonctionnalité** puis cliquez sur **Suivant**.
- Cliquez sur **Suivant** dans la fenêtre **Sélectionner le serveur de destination**.
- Cochez **Services de déploiement Windows** puis cliquez sur le bouton **Ajouter des fonctionnalités** dans la fenêtre qui s'affiche.



- Cliquez sur **Suivant** afin de valider le choix.
- Cliquez sur **Suivant** dans la fenêtre **Sélectionner des fonctionnalités**.
- Dans la fenêtre **Sélectionner des services de rôle**, vérifiez que **Serveur de déploiement** et **Serveur de transport** sont bien cochés.



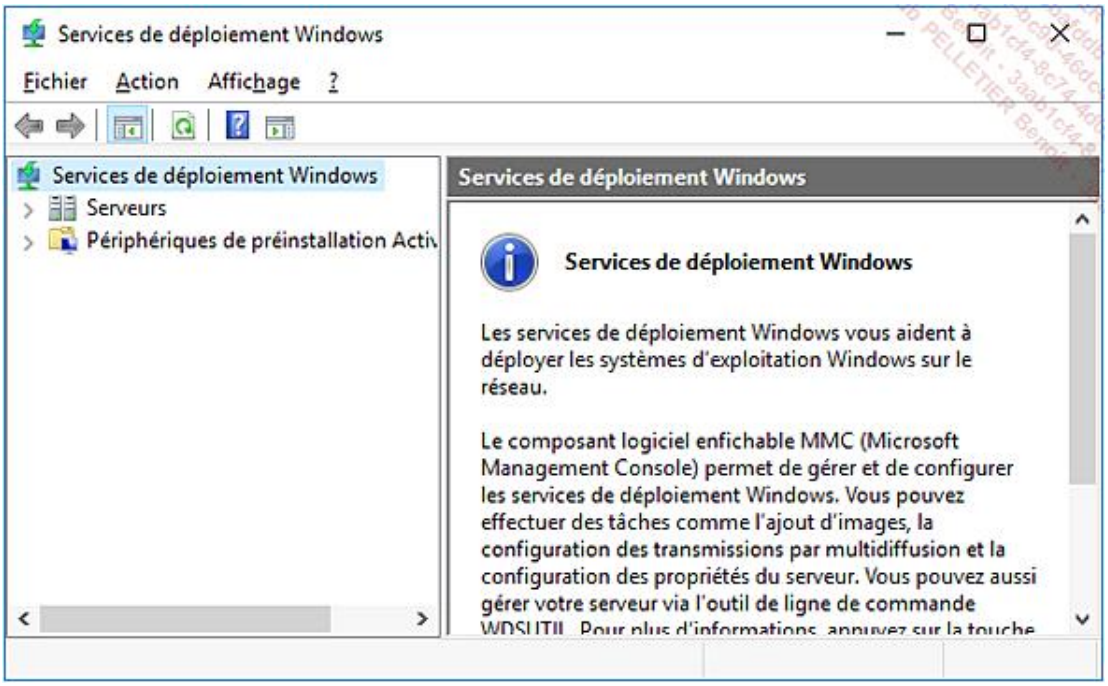
Le service de rôle **Serveur de déploiement** permet la fourniture de l'ensemble des fonctionnalités offertes par WDS. Il permet la configuration et l'installation des postes de travail présents sur le réseau ainsi que la gestion des images. Le service de rôle **Serveur de transport** est également nécessaire.

Il gère la partie transport des données. Il est utilisé par exemple lors de la transmission des données en multicast.

- Cliquez sur **Installer** afin de lancer l'installation.
- Cliquez sur **Fermer** à la fin de l'installation.

2. Configuration du serveur

- Lancez la console **Services de déploiement Windows**.

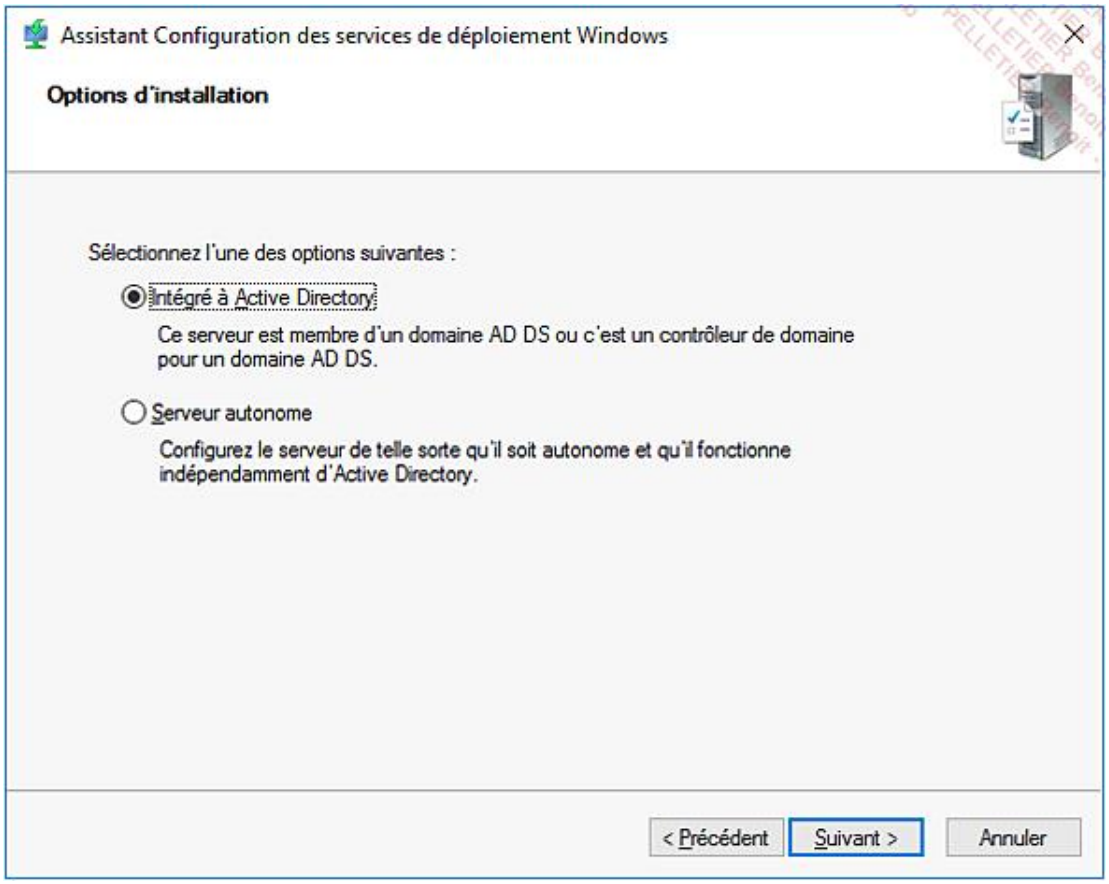


- Développez le nœud **Serveurs** puis effectuez un clic droit sur **SV1.formation.local**.
- Cliquez sur **Configurer le serveur**.
- L'assistant se lance. Cliquez sur **Suivant** dans la fenêtre **Avant de commencer**.

Deux options d'installation sont présentes, l'option **Intégré à Active Directory** et l'option **Serveur autonome**.

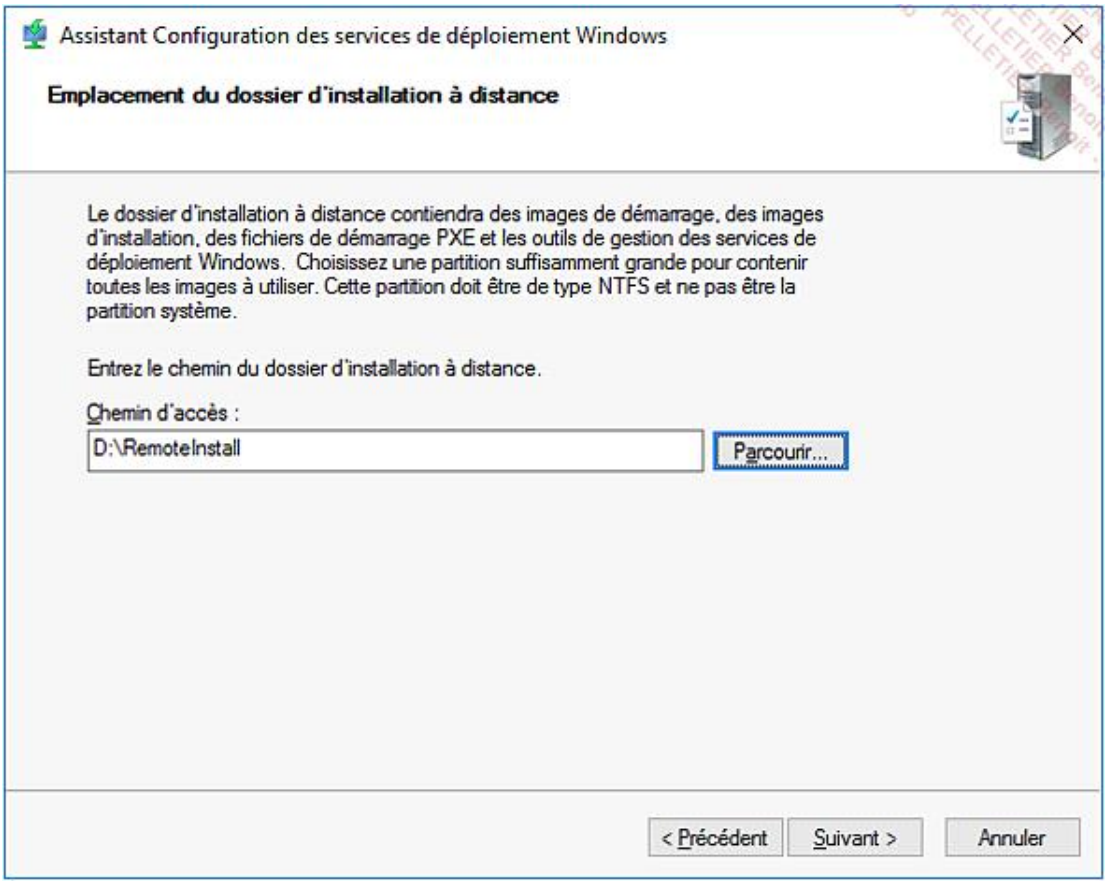
- L'option **Intégré à Active Directory** nécessite que le serveur soit membre du domaine. En effet le serveur s'appuie sur Active Directory pour son fonctionnement.
- L'option **Serveur autonome** permet de posséder un serveur dont le fonctionnement n'est pas lié à Active Directory. Le serveur possède donc dans ce cas un magasin local qui est utilisé afin de stocker les informations sur les périphériques de préinstallation.

- Laissez l'option **Intégré à Active Directory** sélectionnée puis cliquez sur **Suivant**.

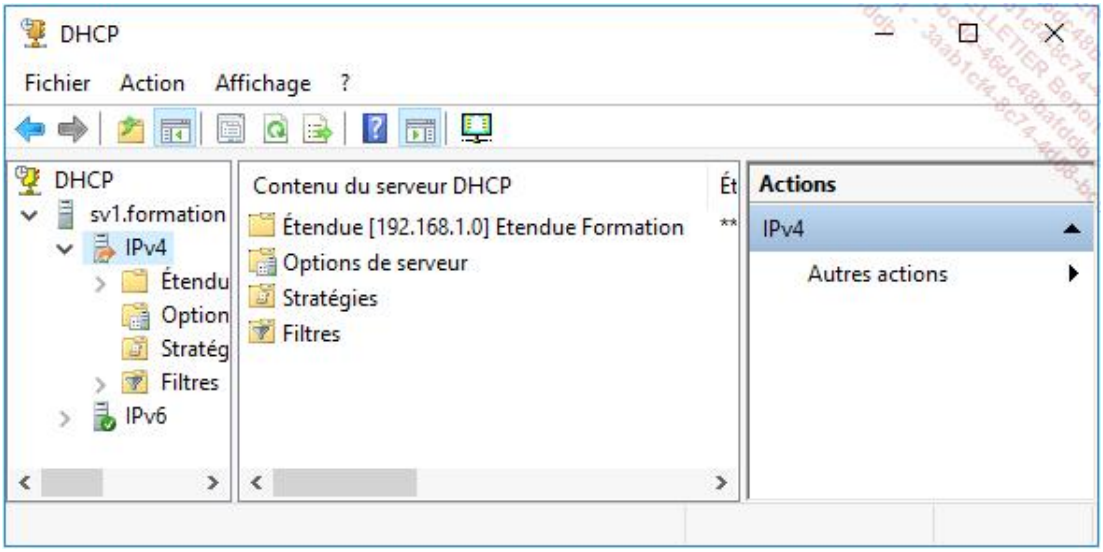


Le dossier d'installation à distance permet le stockage des différentes images, des pilotes et des fichiers de réponse mais également de la configuration du serveur. Il est recommandé de ne pas le stocker sur la partition système afin de ne pas avoir à le recréer suite à une réinstallation du système d'exploitation.

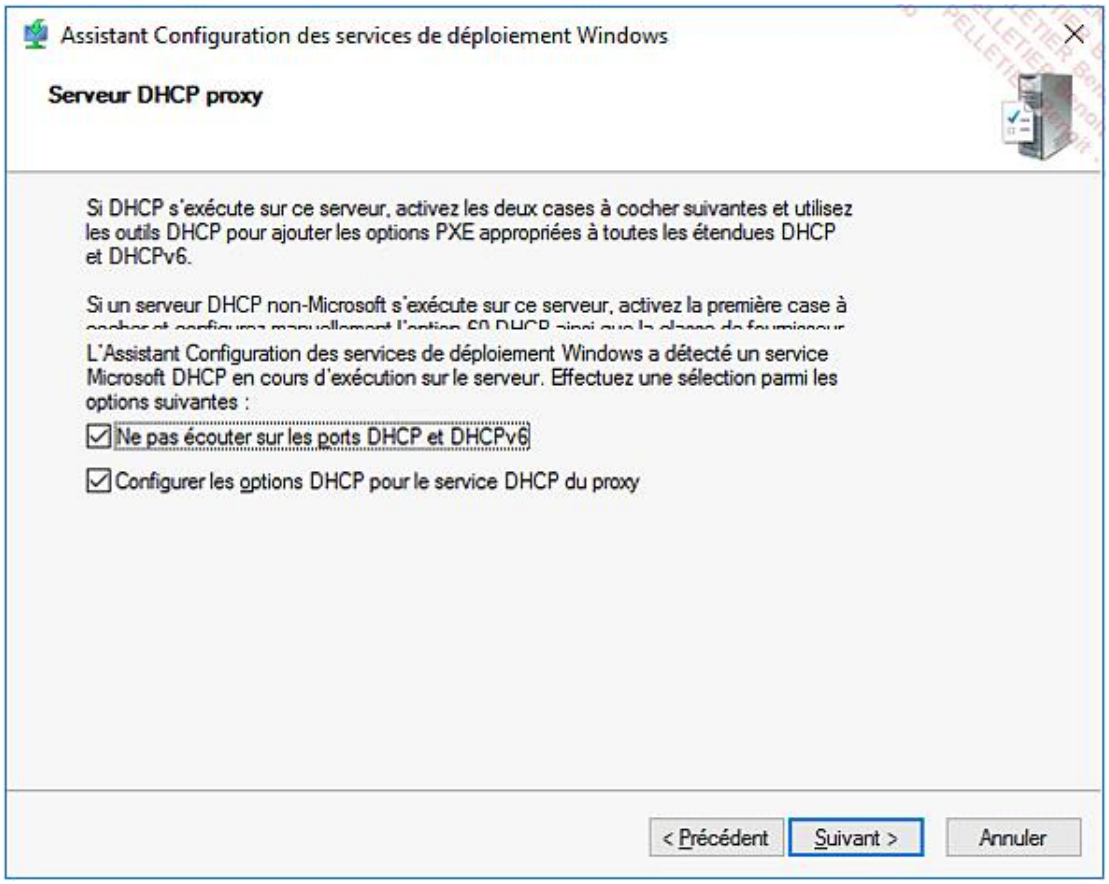
- Dans la fenêtre **Emplacement du dossier d'installation à distance**, stockez le dossier **RemoteInstall** dans la partition **D** puis cliquez sur **Suivant**.



Les serveurs DHCP et WDS cohabitant sur le même serveur, le service de déploiement ne doit pas écouter sur les mêmes ports que le serveur DHCP.



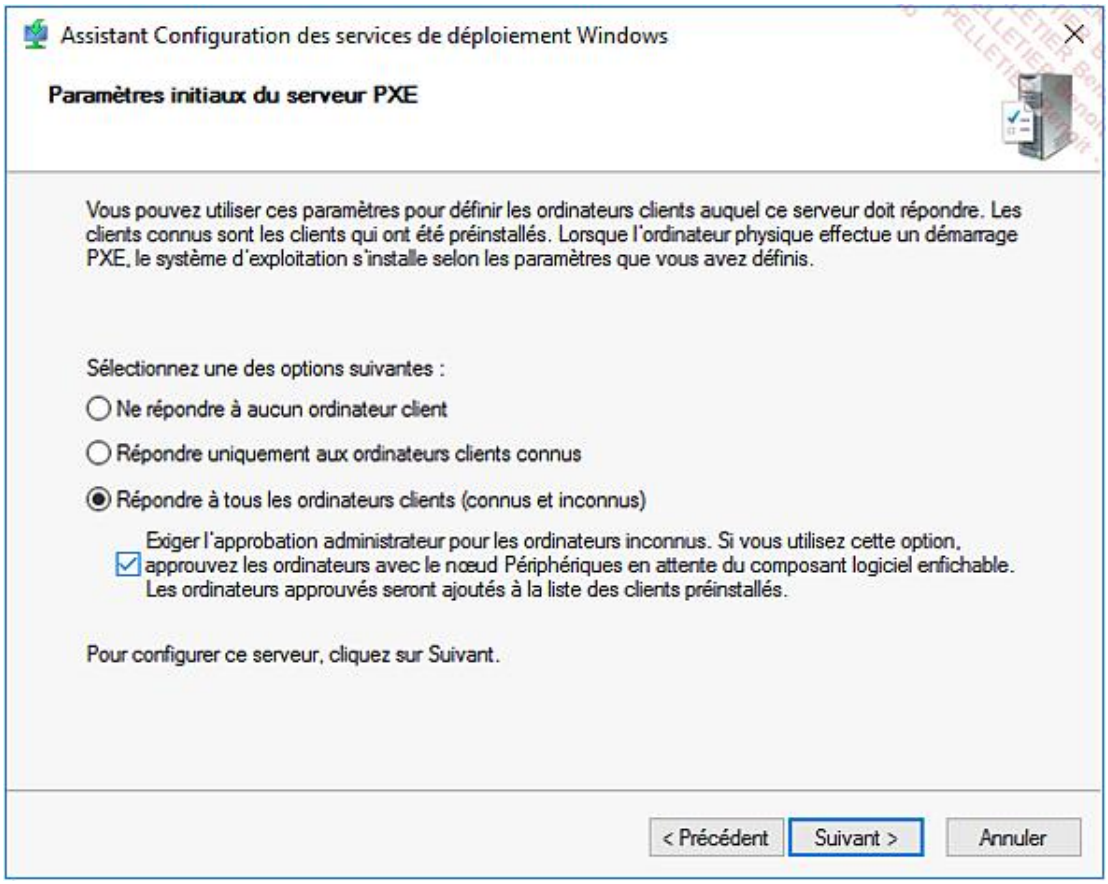
Cochez les deux options puis cliquez sur **Suivant**.



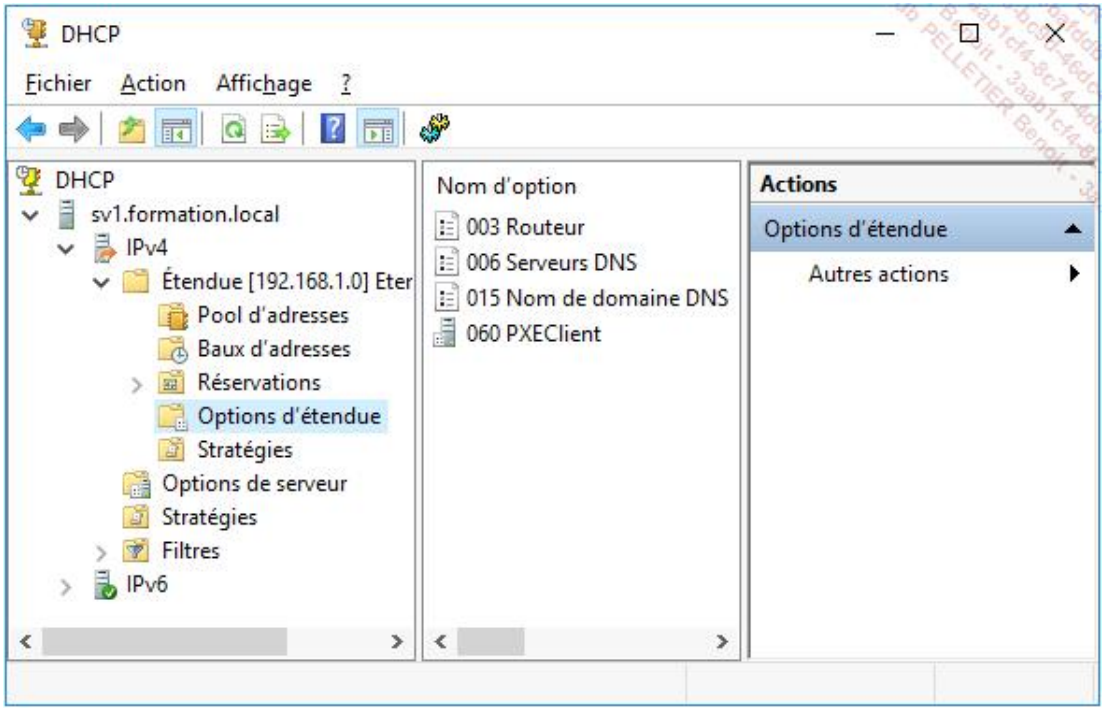
Plusieurs types de réponses sont configurables :

- **Ne répondre à aucun client** : le serveur ne répond à aucune demande de sollicitation qui lui est transmise.
- **Répondre uniquement aux ordinateurs clients connus** : une réponse est apportée uniquement aux postes clients qui sont connus dans Active Directory ou la base locale pour les serveurs autonomes. En cas de nouveau poste, il est nécessaire de procéder à la création du compte en amont pour les deux modes.
- **Répondre à tous les ordinateurs clients (connus et inconnus)** : une réponse est apportée à tous les postes qui viennent solliciter le serveur. Afin de s'assurer qu'aucun déploiement n'est effectué sans l'aval de l'administrateur, il convient de cocher la case **Exiger l'approbation administrateur pour les ordinateurs inconnus**.

Cochez **Répondre à tous les ordinateurs clients (connus et inconnus)** puis la case **Exiger l'approbation administrateur pour les ordinateurs inconnus**.



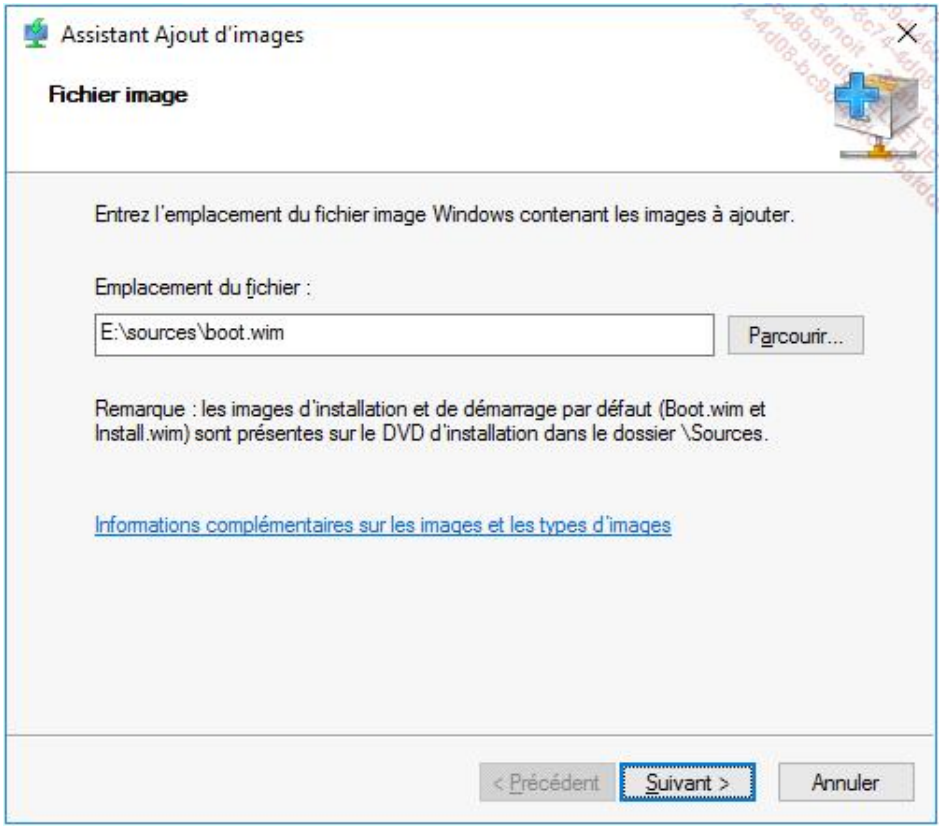
- Cliquez sur **Suivant**, puis sur **Terminer** à la fin de l'installation.
- Lancez la console DHCP.
- Développez les nœuds **SV1.formation.local**, **IPv4** puis **Étendue**.
- Cliquez sur le nœud **Options d'étendue** et vérifiez que l'option **060 PXEClient** est présente.



Le serveur étant maintenant configuré, les images doivent être ajoutées.

3. Ajout d'une image de démarrage et d'installation

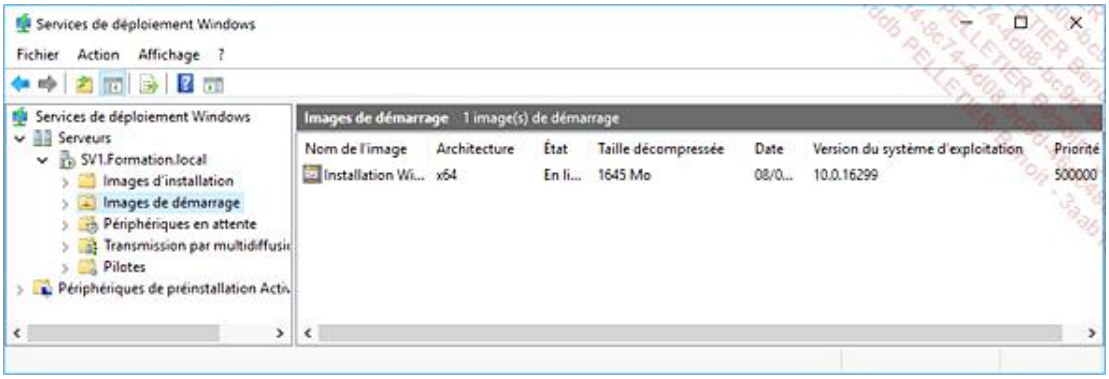
- Connectez l'ISO de Windows 10 à la machine virtuelle SV1.
- Dans la console du rôle **Services de déploiement Windows**, sur le serveur **SV1**, effectuez un clic droit dans **Boot Images** puis sélectionnez **Ajouter une image de démarrage**.
- Cliquez sur **Parcourir** puis sélectionnez le fichier **boot.wim** présent dans le dossier **sources** du DVD puis cliquez sur **Suivant**.



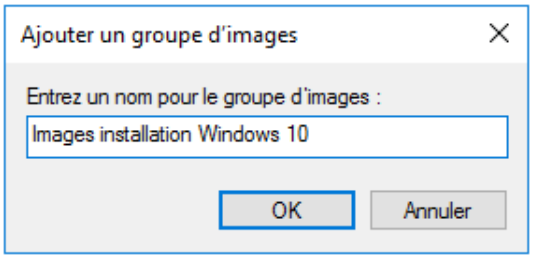
Le fichier **boot.wim** est une image WinPE qui permet l'installation du système d'exploitation.

- Dans les champs **Nom de l'image** et **Description de l'image**, saisissez **Installation Windows 10 - x64** puis cliquez sur **Suivant**.
- Cliquez sur **Suivant** dans la page **Résumé** puis, une fois l'importation terminée, cliquez sur **Terminer**.

L'image est maintenant présente dans la console.



- Effectuez un clic droit sur le dossier **Images d'installation** puis sélectionnez **Ajouter un groupe d'images**.
- Dans le champ texte, saisissez **Images installation Windows 10** puis cliquez sur **OK**.



- Effectuez un clic droit sur le groupe précédemment créé puis sélectionnez **Ajouter une image d'installation**.
- À l'aide du bouton **Parcourir**, sélectionnez l'image **install.wim** présente dans le dossier sources du DVD puis cliquez sur **Suivant**.

Cette image contient les fichiers système des différentes éditions de Windows 10.

- Cliquez sur **Suivant** dans la fenêtre **Images disponibles**.

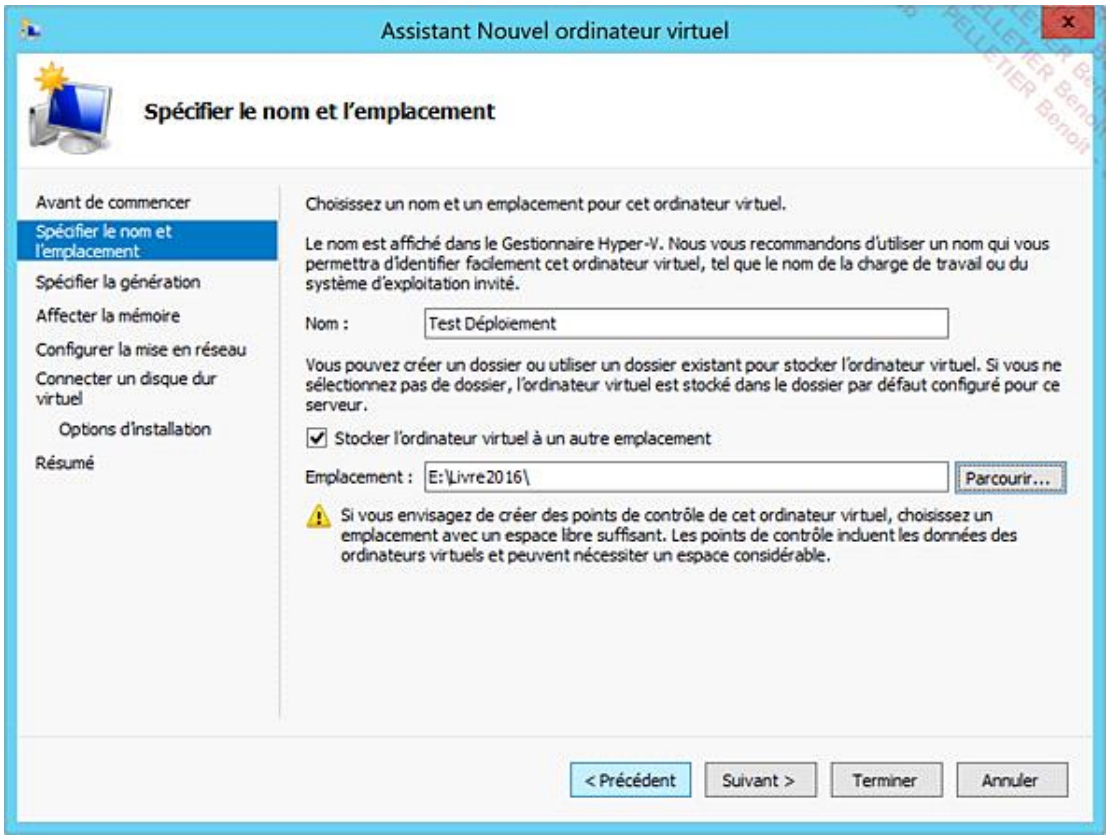
Si le fichier **install.wim** contient plusieurs éditions, il est possible de sélectionner celle souhaitée dans cette fenêtre.

- Cliquez sur **Suivant** dans la page **Résumé** puis, une fois l'importation terminée, cliquez sur **Terminer**.

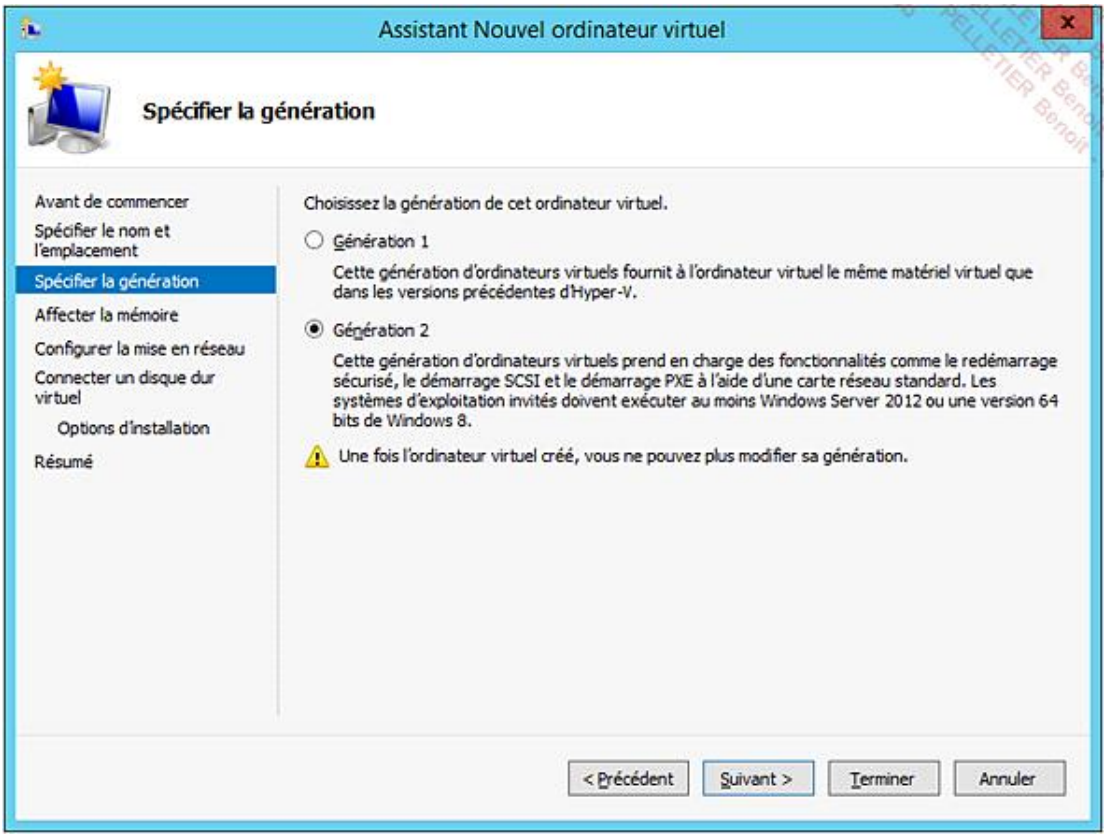
Déploiement d’un système d’exploitation

Le déploiement effectué sur le poste de travail n’est pas automatisé. Il est possible d’ajouter un fichier de réponse afin d’automatiser toutes les opérations. Ce dernier point sera abordé plus loin dans ce chapitre.

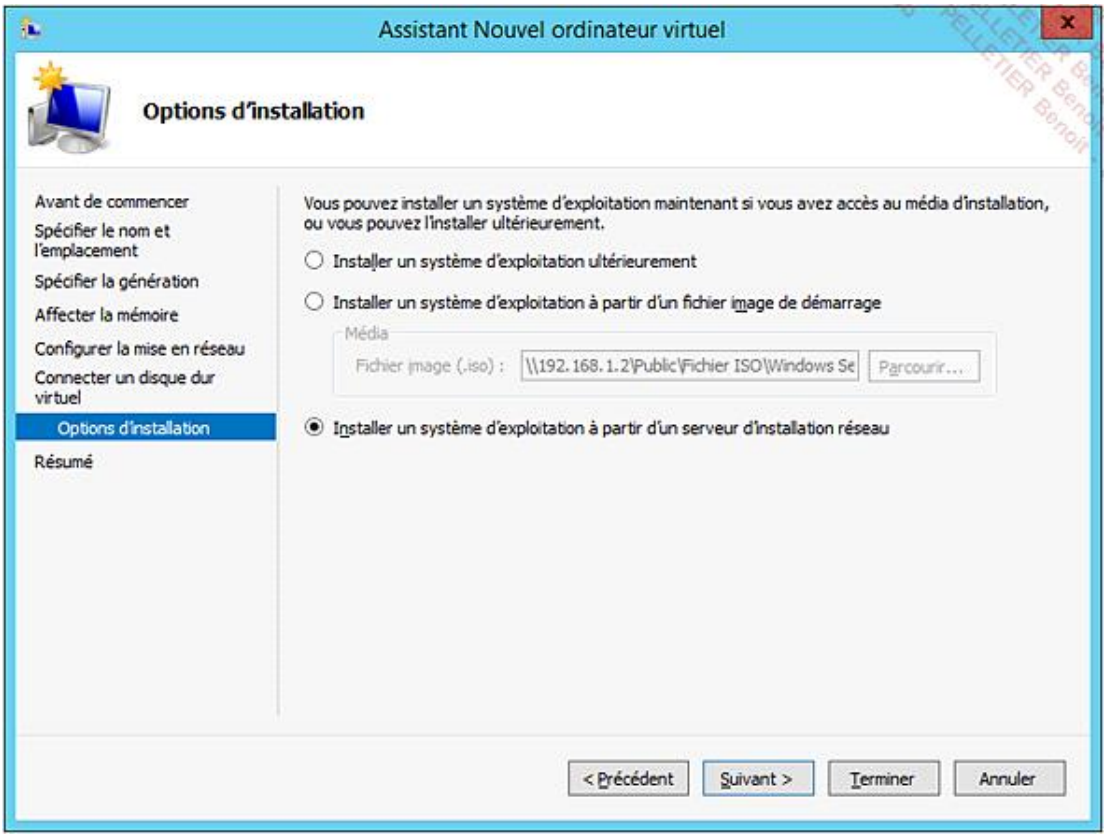
- Ouvrez la console **Hyper-V** sur la machine physique.
- Cliquez sur **Nouveau** dans le bandeau **Actions** puis sur **Ordinateur virtuel**.
- Dans la fenêtre **Avant de commencer** cliquez sur **Suivant**.
- Dans le champ **Nom**, saisissez **Test Déploiement** puis cliquez sur **Suivant**.



- Dans la fenêtre **Spécifier la génération**, sélectionnez **Génération 2** puis cliquez sur **Suivant**.

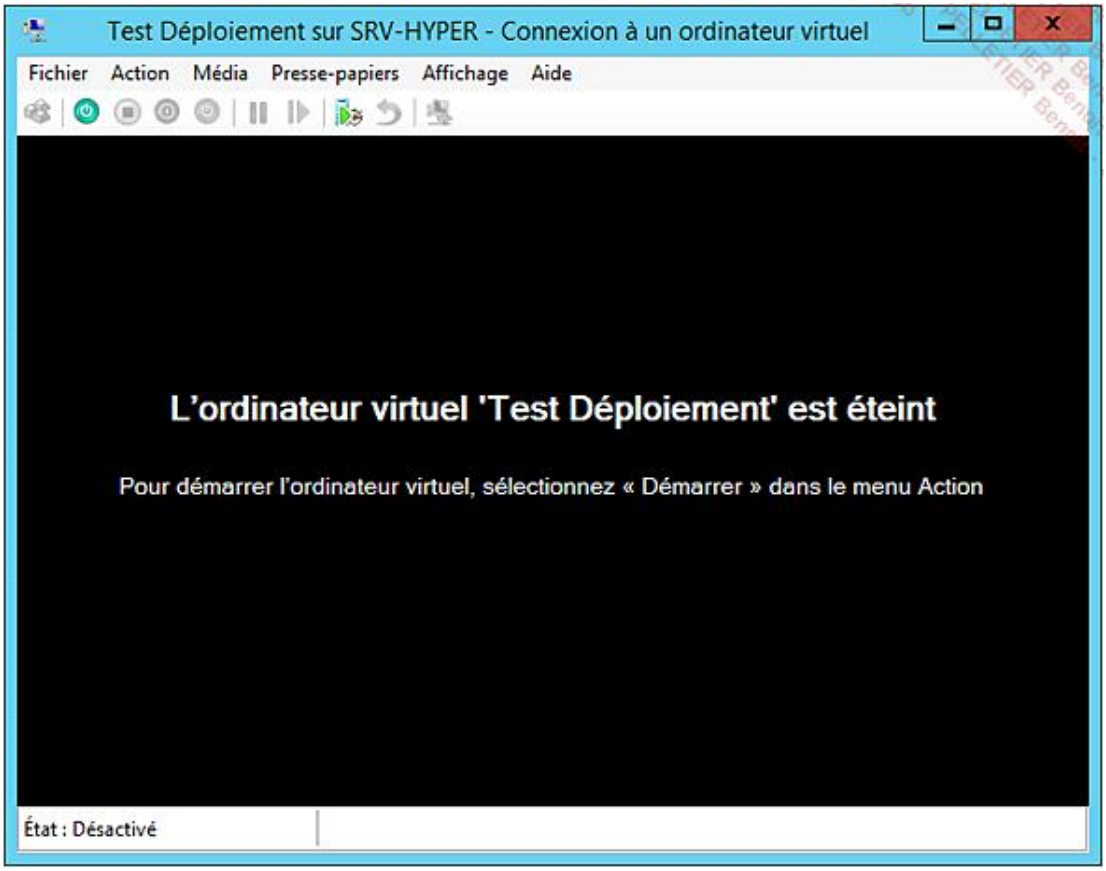


- Dans la fenêtre **Affecter la mémoire**, saisissez 2048 puis cliquez sur **Suivant**.
- Sélectionnez dans la liste déroulante la même carte réseau que les autres machines virtuelles puis cliquez sur **Suivant**.
- Dans la fenêtre **Connecter un disque dur virtuel**, cliquez sur **Suivant**.
- Dans la fenêtre **Options d'installation**, cochez **Installer un système d'exploitation à partir d'un serveur d'installation réseau** puis cliquez sur **Suivant**.



Une fois créée, la machine virtuelle apparaît dans la console.

Double cliquez sur la nouvelle machine puis cliquez sur le bouton **Démarrer** (bouton vert).



La machine démarre et tente de récupérer une adresse IP auprès d'un serveur DHCP.

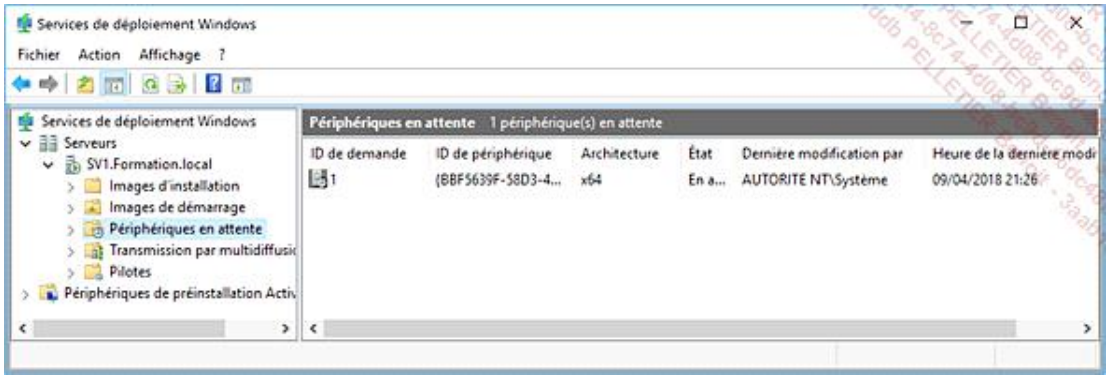
- Appuyez sur [F12] quand la machine tente de démarrer sur WDS (un message vous demande d'appuyer sur cette touche).

L'approbation doit être effectuée sur le serveur afin que celui-ci réponde au client.



- Sur SV1, lancez la console WDS puis cliquez sur le nœud **Périphériques en attente**.

Pensez à cliquer sur **Actualiser** si aucune ligne n'apparaît.

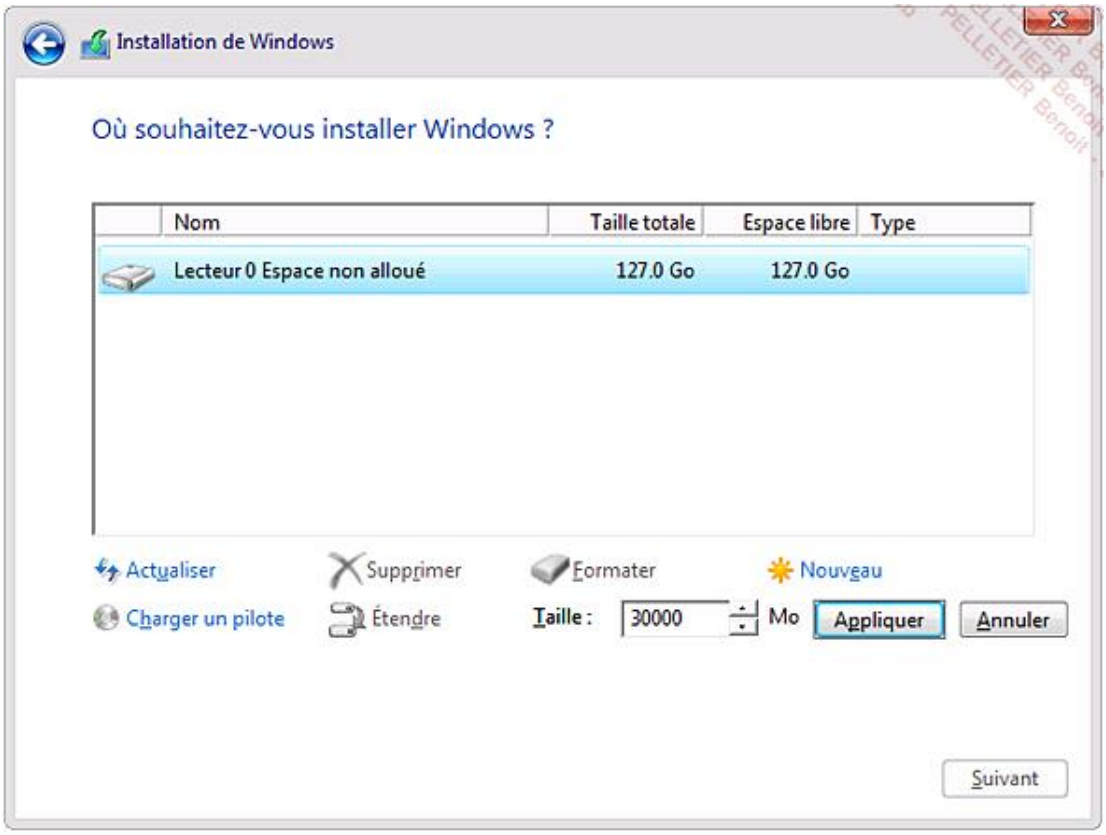


- Effectuez un clic sur la ligne de la demande à accepter puis sélectionnez **Approuver**.

Un message confirme l'approbation.

L'installation se déroule sur la machine cliente.

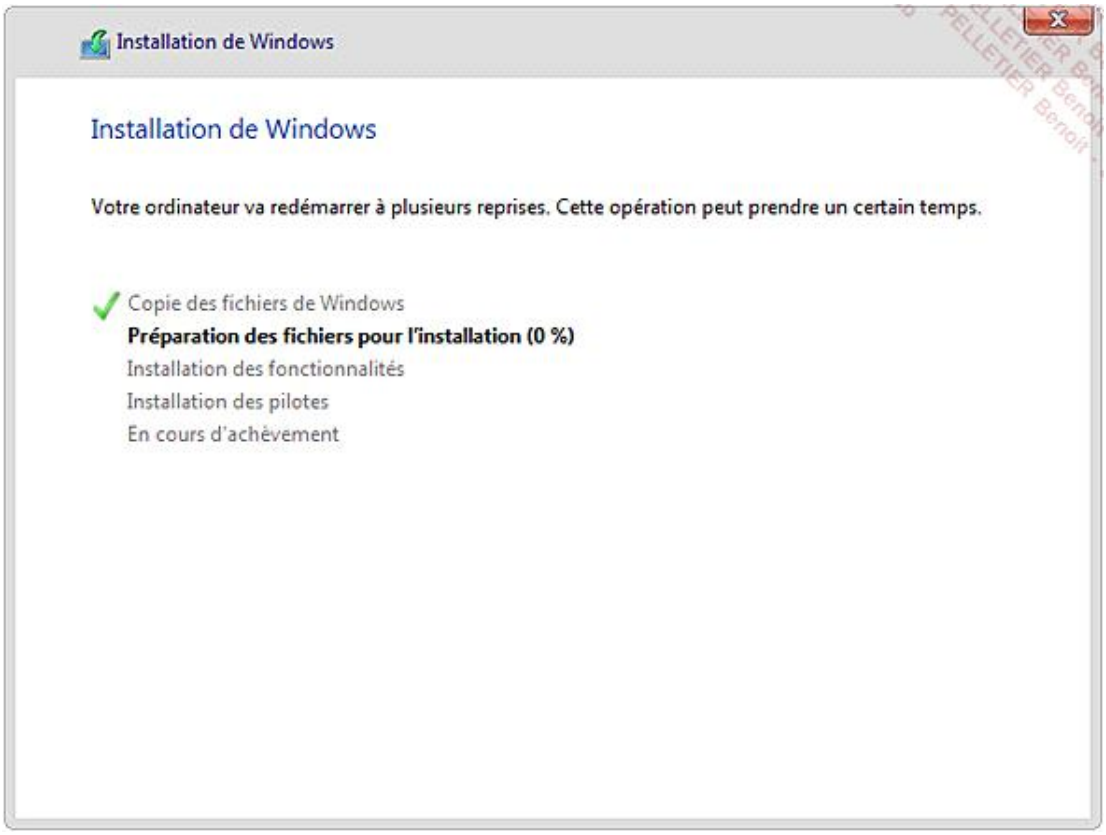
- Sélectionnez les paramètres régionaux et le clavier souhaités sur l'ordinateur en cours de déploiement, puis cliquez sur **Suivant**.
- Authentifiez-vous en tant qu'**administrateur@formation.local** dans la fenêtre **Connexion à SV1.formation.local** puis cliquez sur **OK**.
- Dans la fenêtre de sélection du système d'exploitation, cliquez sur **Suivant**.
- Cliquez sur **Options de lecteur (avancées)** puis sur **Nouveau**. Dans le champ **Taille**, insérez la valeur **30 000**.



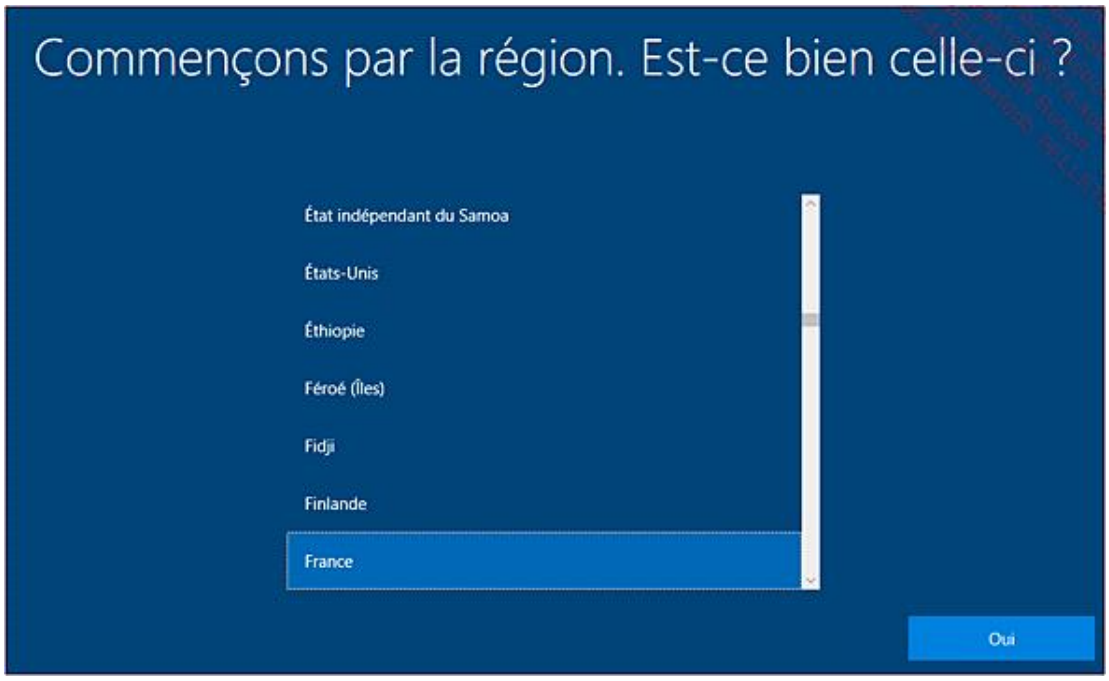
- Cliquez sur **Appliquer** puis sur **OK**. Une fois les partitions créées, cliquez sur **Suivant**.

Plusieurs partitions sont créées.

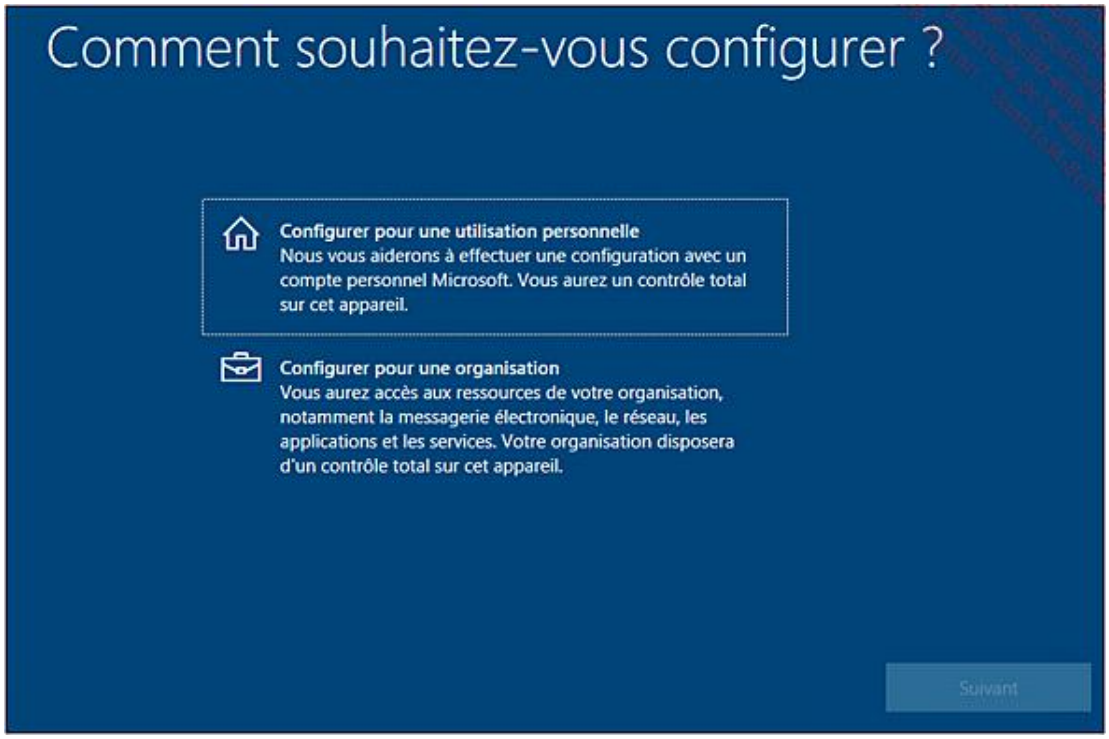
L'installation démarre…



- Après le redémarrage du poste, vérifiez les langues puis cliquez sur **Oui**.



- Dans la fenêtre **Termes du contrat de licence**, cliquez sur **Accepter**.
- Dans la fenêtre **Choisissez votre mode de connexion**, choisissez **Configurer pour une utilisation personnelle** puis cliquez sur **Suivant**.



- Afin de créer l'utilisateur, cliquez sur **Compte hors connexion** puis saisissez le nom et mot de passe souhaités.

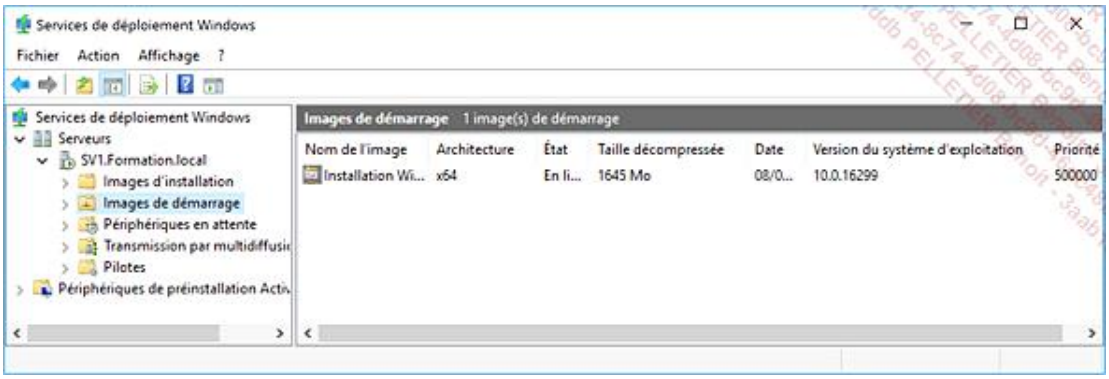
La session s'ouvre par la suite avec l'utilisateur qui vient d'être créé.

1. Création d'une image de capture

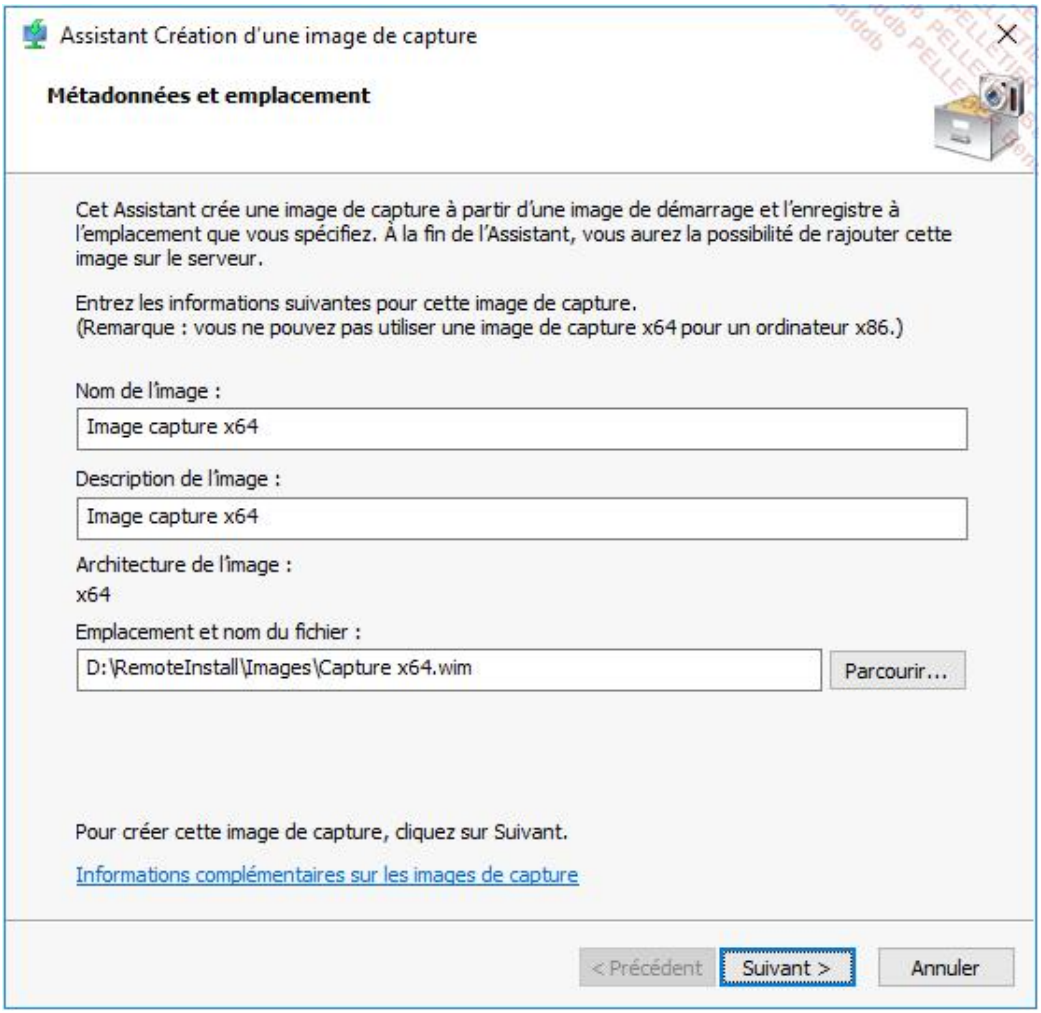
Une image de capture se construit à l'aide de la console **Services de déploiement Windows**. Après le démarrage du poste sur cette image, un assistant s'affiche afin de permettre la capture de la partition système. Néanmoins, il est nécessaire d'avoir lancé sur le poste un **sysprep** afin de généraliser l'image. Sans ce sysprep, il est impossible de procéder à la capture de l'image.

Un fichier WIM est donc créé. Ce dernier contient l'ensemble des métadonnées capturées. Il est par la suite possible de déployer cette image sur les autres postes du réseau.

- Sur SV1, ouvrez la console **Services de déploiement Windows**.
- Développez les nœuds **Serveurs** puis **SV1.Formation.local**.
- Cliquez sur **Images de démarrage** afin d'afficher le contenu du dossier.



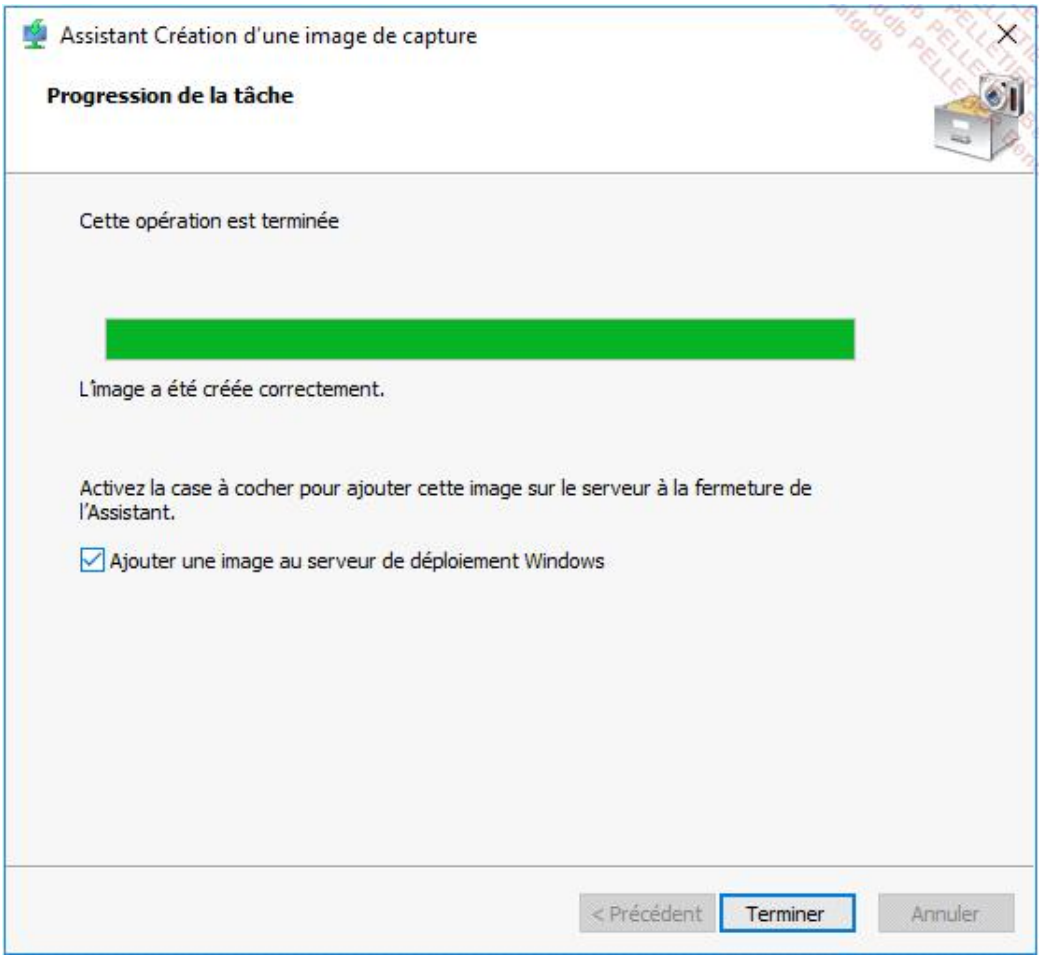
- Effectuez un clic droit sur l'image **Installation Windows 10** puis dans le menu contextuel, cliquez sur **Créer une image de capture**.
- Saisissez **Image capture x64** dans les champs **Nom de l'image** et **Description de l'image**.
- À l'aide du bouton **Parcourir**, sélectionnez le répertoire **D:\RemoteInstall\Images**, saisissez **Capture x64** dans le champ **Nom du fichier** puis cliquez sur **Ouvrir**.



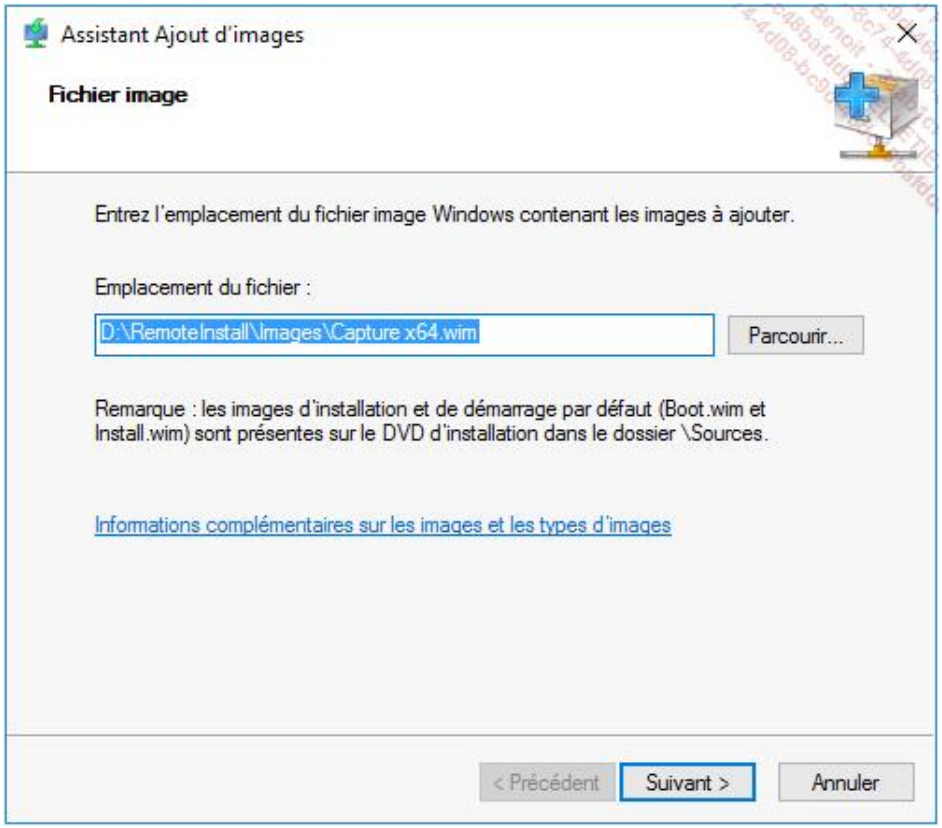
- Cliquez sur **Suivant**.

La création de l'image est en cours.

- Une fois celle-ci terminée, cochez **Ajouter une image au serveur de déploiement Windows** et cliquez sur **Terminer**.



- Vérifiez le chemin dans la fenêtre **Assistant Ajout d'images** puis cliquez sur **Suivant**.



- Dans la fenêtre **Métadonnées d'image**, laissez les valeurs par défaut et cliquez sur **Suivant**.

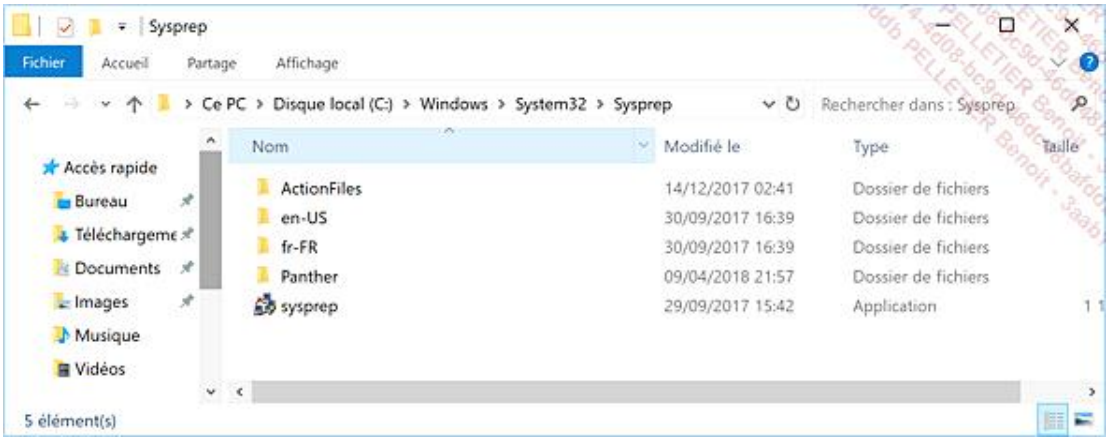
Cliquez sur **Suivant** dans la fenêtre **Résumé** puis sur **Terminer** à la fin de l'opération.

Deux images sont maintenant présentes dans le conteneur **Images de démarrage**.

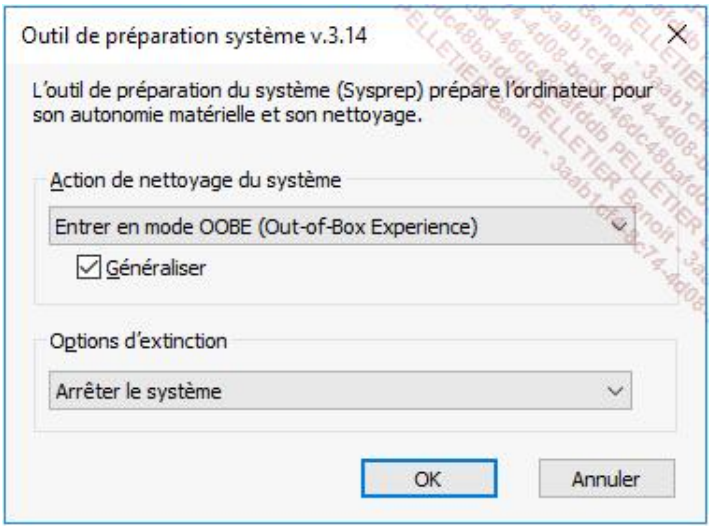
2. Capture d'un poste de référence

Sur le poste **Test Déploiement**, lancez l'Explorateur Windows.

Ouvrez le répertoire **Sysprep** présent dans **C:\Windows\System32**.



Exécutez le fichier **sysprep.exe**, cochez la case **Généraliser** et sélectionnez **Arrêter le système** dans la liste déroulante **Options d'extinction**.



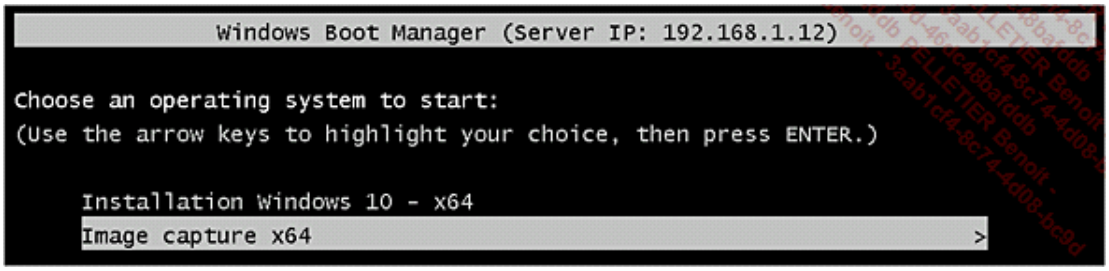
Cliquez sur **OK**.

Si un message d'erreur s'affiche lors de l'exécution du sysprep, vous pouvez utiliser cet article présent sur le blog de l'auteur.

https://www.nibonnet.fr/sysprep-fails/

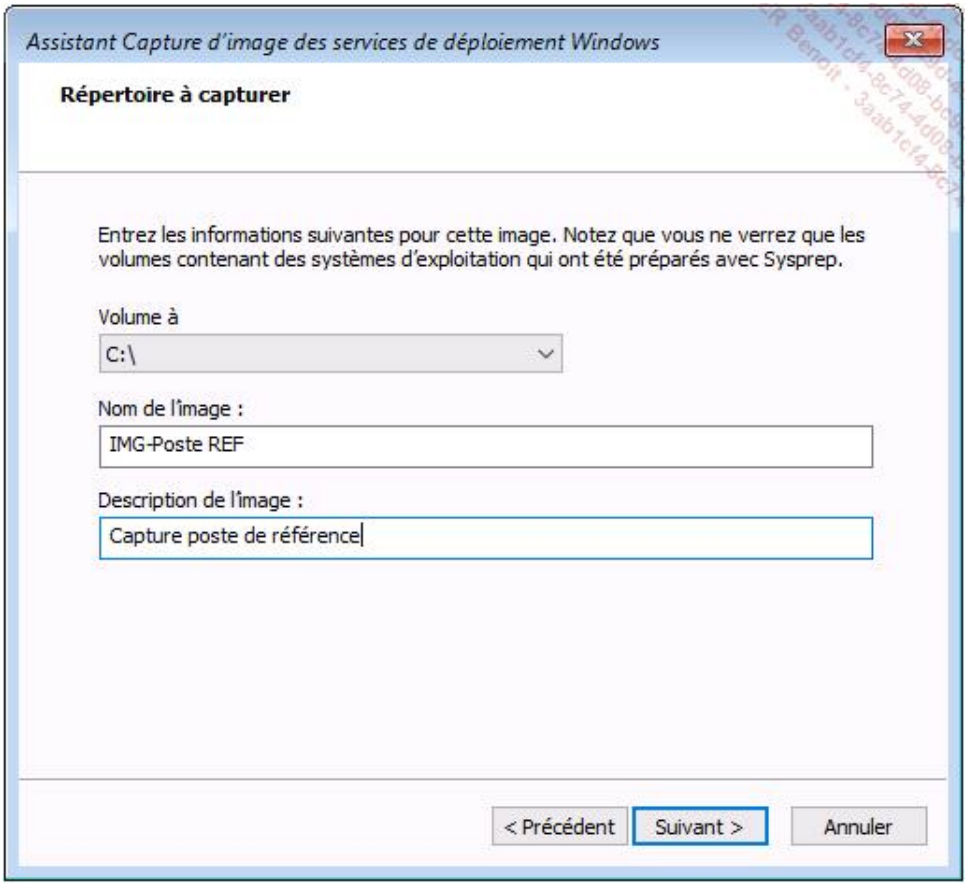
Redémarrez le poste et appuyez sur la touche [F12] afin d'effectuer un démarrage PXE.

Sélectionnez l'image **Image capture x64** et appuyez sur la touche [Entrée].



L'image **Capture x64.wim** se charge.

- Dans la fenêtre de bienvenue de l'assistant, cliquez sur **Suivant**.
- Dans la fenêtre **Répertoire à capturer**, configurez la fenêtre comme ci-dessous :
  - **Volume à** : sélectionnez la partition système dans la liste déroulante.
  - **Nom de l'image** : **IMG-Poste REF**.
  - **Description de l'image** : **Capture poste de référence**.



L'image est stockée en local avant d'être téléchargée sur le serveur.

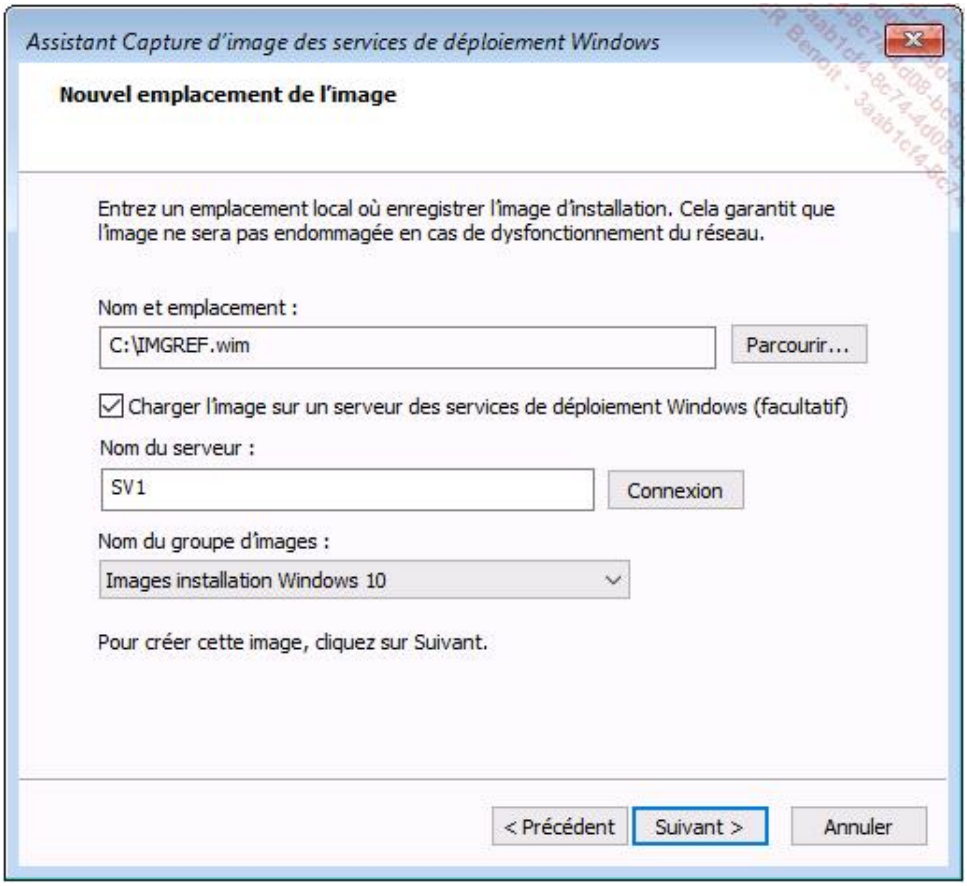
- À l'aide du bouton **Parcourir**, sélectionnez la partition D puis dans le champ **Nom du fichier**, saisissez **IMGREF**.

Remplacez D par la lettre de votre partition.

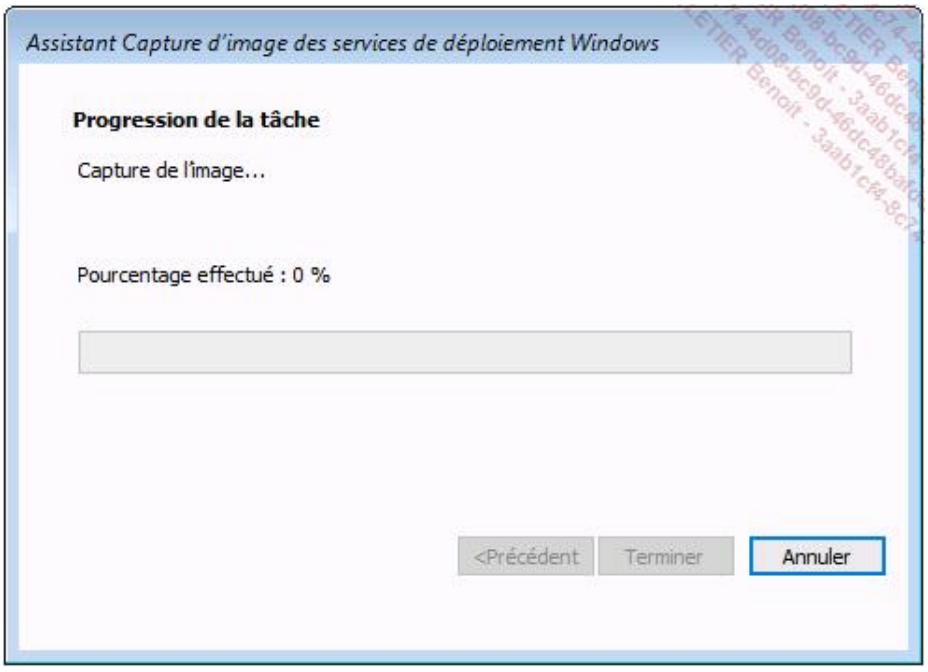
- Cochez la case **Charger l'image sur un serveur des services de déploiement Windows**, saisissez **SV1**

dans le champ **Nom du serveur** puis cliquez sur **Connexion**.

- Authentifiez-vous en tant que **formation\administrateur**, mot de passe **Pa$$w0rd**.
- Dans la liste déroulante **Nom du groupe d'images**, sélectionnez **Images installation Windows 10** et cliquez sur **Suivant**.



La capture est en cours.

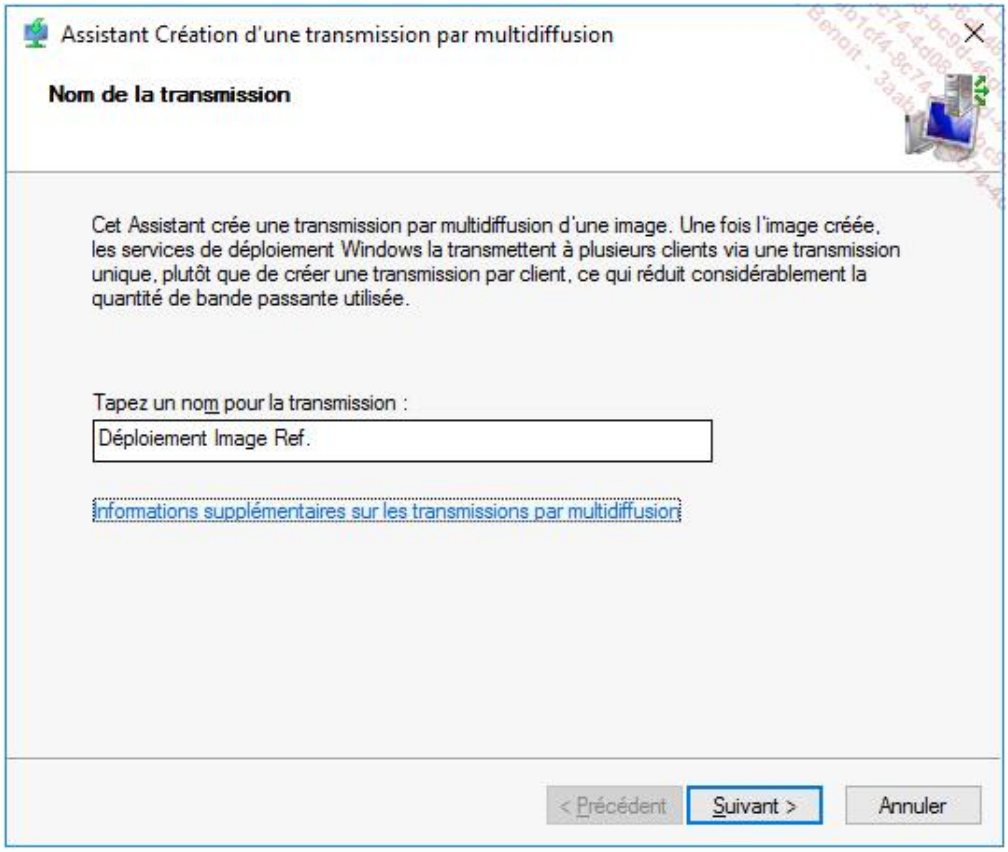


- Cliquez sur **Terminer** à la fin de la capture.
- Sur SV1, cliquez sur le groupe **Images installation Windows 10**. L'image capturée est présente.

L'image peut maintenant être déployée.

3. Déploiement en multicast

- Effectuez un clic droit sur **Transmission par multidiffusion** dans la console **Services de déploiement Windows**.
- Cliquez sur **Créer une transmission par multidiffusion**.
- Dans la fenêtre **Nom de la transmission**, saisissez **Déploiement Image Ref.**, puis cliquez sur **Suivant**.

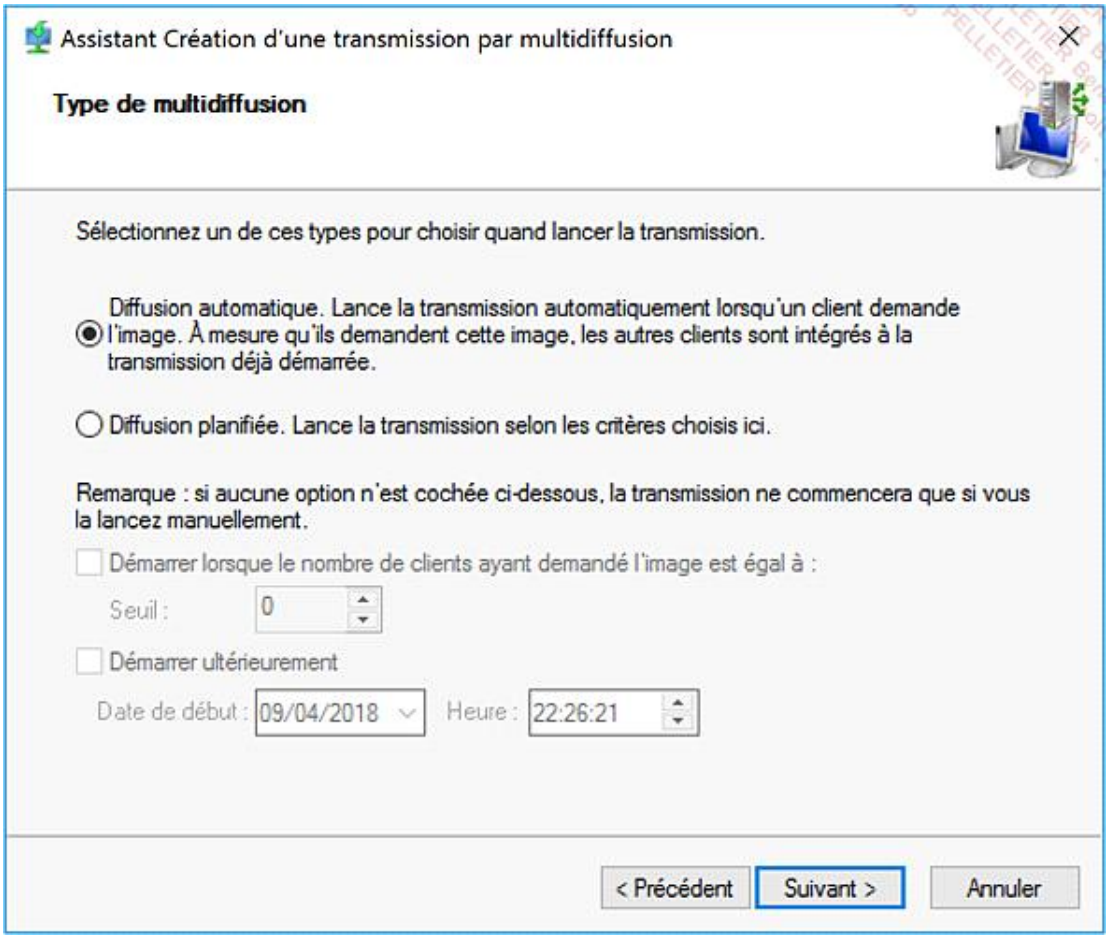


- Sélectionnez **IMG-Poste REF** puis cliquez sur **Suivant**.

Deux types de transmission sont possibles :

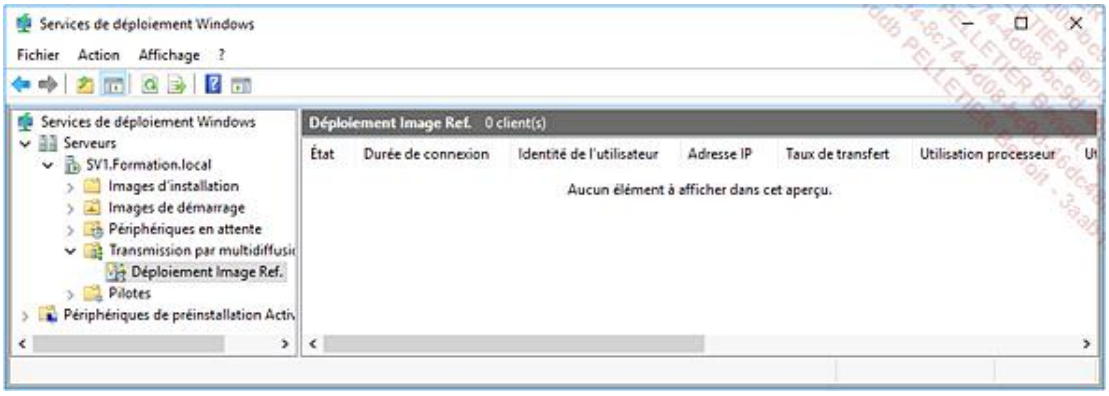
- **Diffusion automatique** : la transmission démarre lorsque le premier poste en fait la demande.
- **Diffusion planifiée** : la transmission est démarrée en fonction d'un critère. Le premier critère est le nombre de postes qui font la demande et la transmission ne démarre pas tant que le nombre minimum de postes n'est pas atteint. Le deuxième critère est un critère de temps. Ainsi, il est possible de faire débuter une transmission à une date et une heure spécifiques.

- Laissez **Diffusion automatique** coché puis cliquez sur **Suivant**.

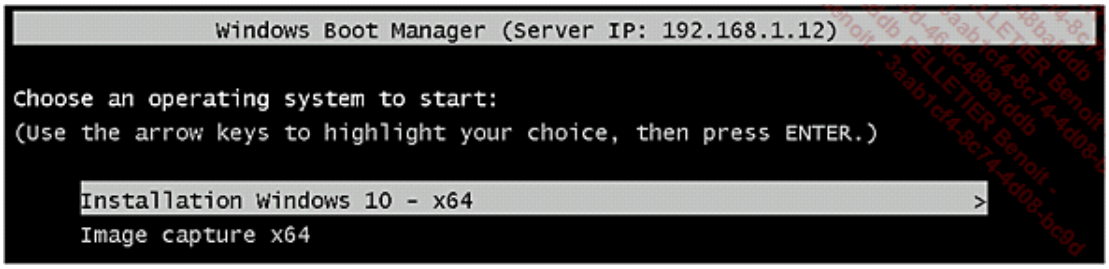


- Cliquez sur **Terminer** pour valider les différents choix.

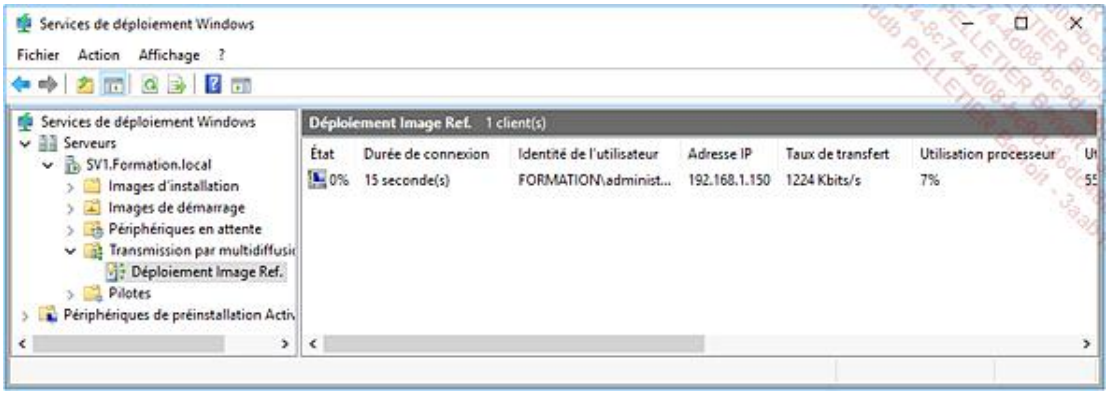
La transmission par multidiffusion ainsi créée a le statut **Actif**.



- Redémarrez la machine virtuelle **Test Déploiement** et effectuez un démarrage PXE.
- Sélectionnez l'image **Installation Windows 10 - x64** puis appuyez sur la touche [Entrée] afin de lancer le chargement de l'image.



- Laissez les **Paramètres régionaux** et le **Clavier** en **Français** puis cliquez sur **Suivant**.
- Dans la fenêtre de connexion, identifiez-vous en tant que administrateur@formation.local (mot de passe : Pa$$w0rd).
- Sélectionnez l'image **IMG-Poste REF** puis cliquez sur **Suivant**.
- Cliquez sur **Options de lecteur (avancées)** puis supprimez l'ensemble des partitions à l'aide du bouton **Supprimer**.
- Cliquez sur **Suivant** pour lancer le déploiement.
- Double cliquez sur **Déploiement Image Ref.**. Des informations sur la transmission sont données (**État**, **Durée de connexion**, **Identité de l'utilisateur**, **Taux de transfert**…).

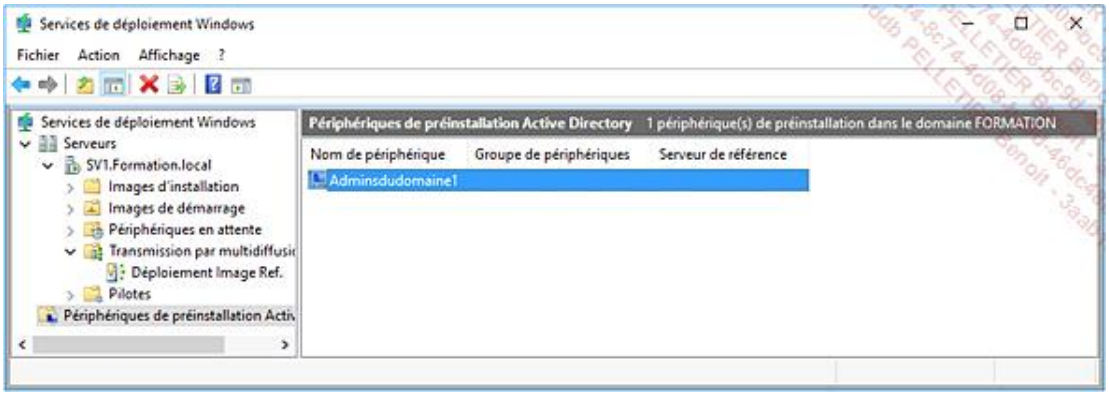


4. Périphériques de préinstallation Active Directory

Les périphériques de préinstallation Active Directory permettent de déterminer les paramètres à appliquer à un périphérique. Il est possible d'effectuer la création d'un nouvel élément de façon manuelle.

L'onglet **Général** permet la saisie de l'ID du périphérique (GUID du poste), mais également du nom unique du poste. L'onglet **Démarrage** permet de déterminer le serveur de référence ainsi que la stratégie du démarrage (**Toujours continuer le démarrage pxe**,…). L'image de démarrage à utiliser peut également être définie. L'onglet **Installation sans assistance client** permet d'indiquer un fichier de réponse à utiliser pour le périphérique. Si ce dernier n'existe pas, la création d'un nouveau fichier est possible. Enfin, les **Droits de jointure** permettent d'effectuer la configuration pour autoriser la jonction du poste au domaine.

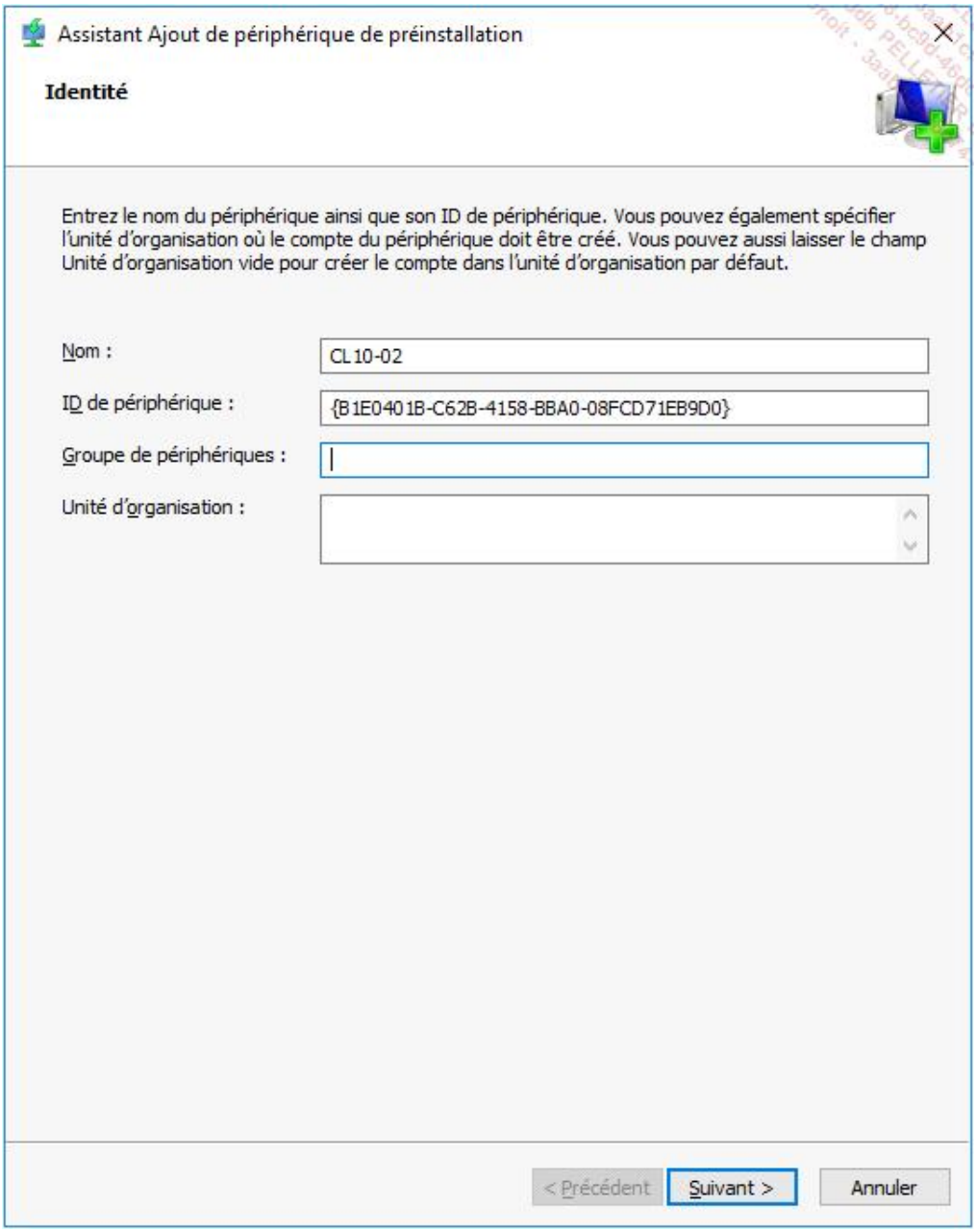
- Cliquez sur **Périphériques de préinstallation Active Directory**.



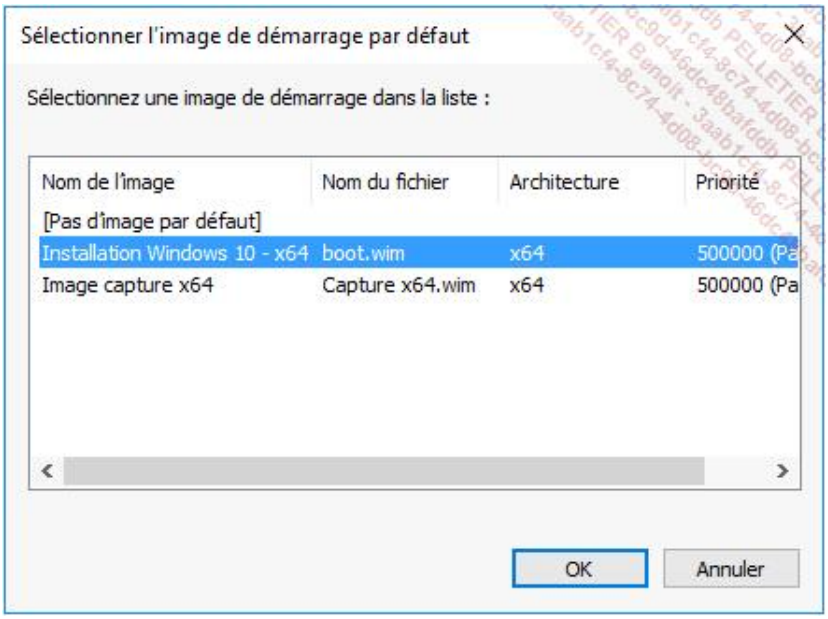
- Effectuez un double clic sur le périphérique déjà présent.
- Sélectionnez l'**ID de périphérique** puis copiez-le avec la séquence de touches [Ctrl] **C**.

Les accolades sont également à récupérer.

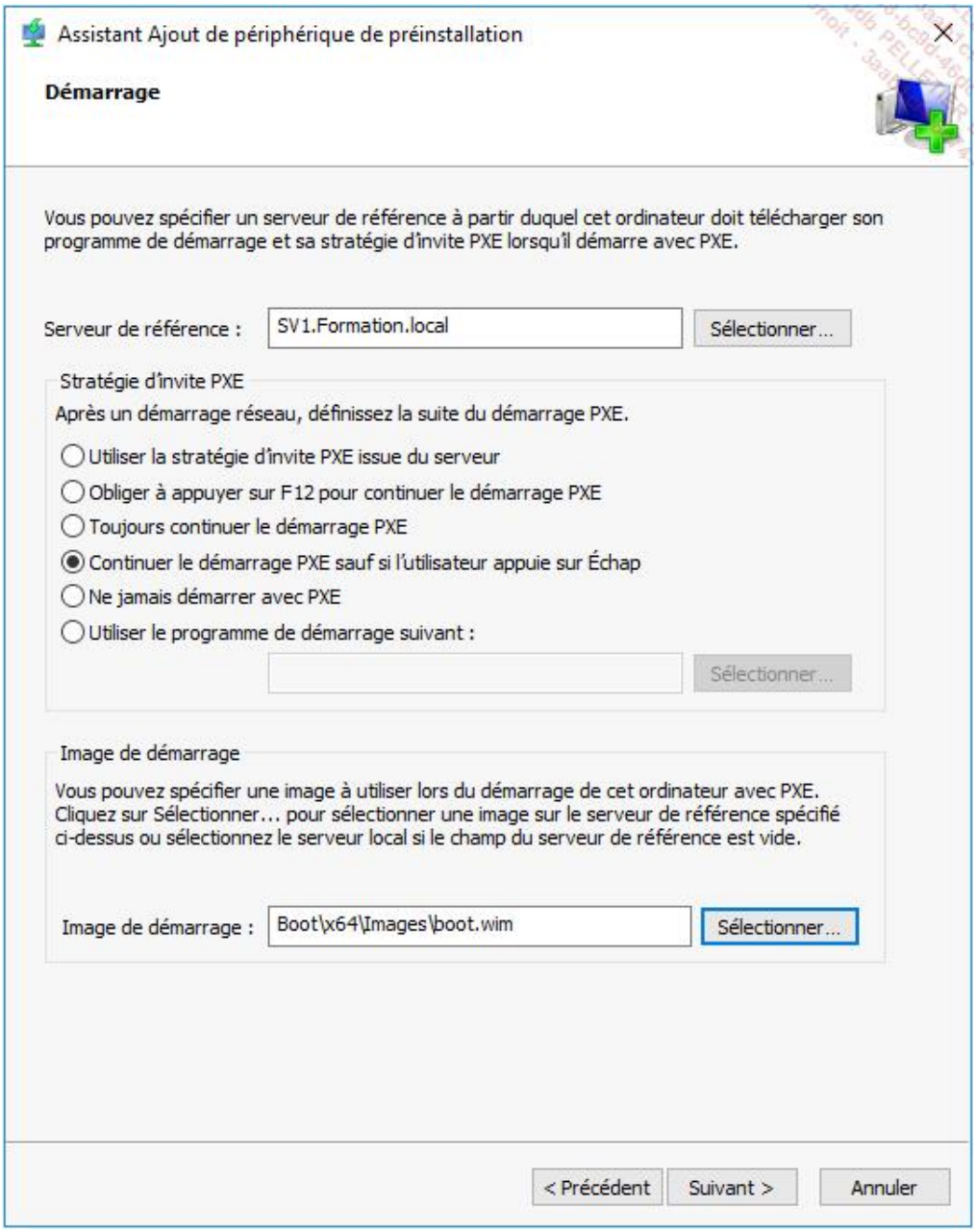
- Assurez-vous que la copie a fonctionné (effectuez un coller dans le **Bloc-notes**) puis supprimez le compte présent.
- Effectuez un clic droit sur **Périphériques de préinstallation Active Directory** puis dans le menu contextuel, cliquez sur **Ajouter**.
- Dans le champ **Nom**, saisissez **CL10-02**, puis collez l'ID précédemment copié dans le champ **ID de périphérique**.



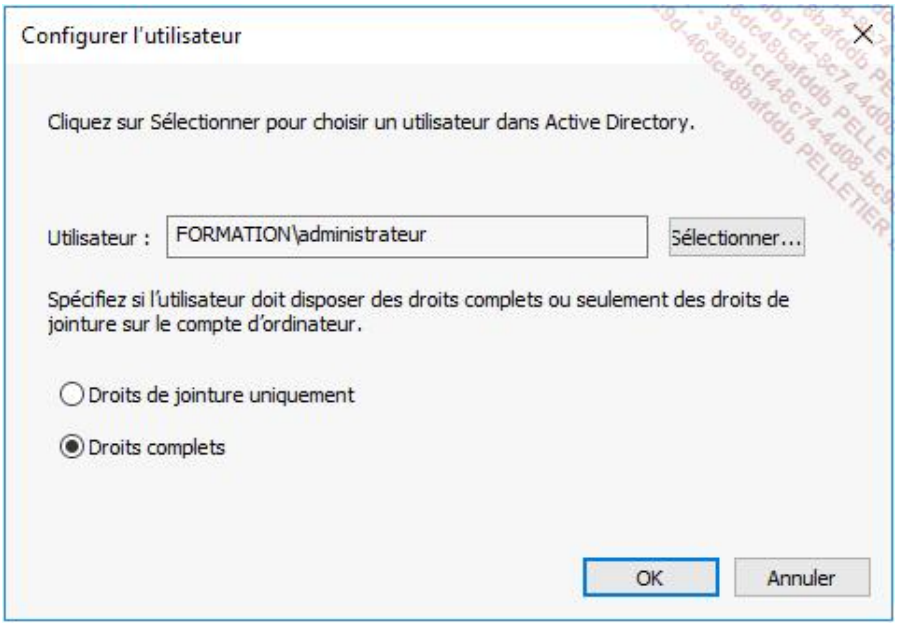
- Cliquez sur **Suivant**.
- Cliquez sur le bouton **Sélectionner** pour choisir le **Serveur de référence** souhaité.
- Saisissez **SV1** dans la nouvelle fenêtre, cliquez sur **Vérifier les noms** et sur **OK**.
- Dans la **Stratégie d'invite PXE**, sélectionnez le choix **Continuer le démarrage PXE sauf si l'utilisateur appuie sur Echap**.
- Cliquez sur le bouton **Sélectionner** à droite du champ **Image de démarrage**, choisissez **Installation Windows 10 - x64** dans la nouvelle fenêtre puis cliquez sur **OK**.



La fenêtre **Démarrage** est maintenant configuré.



- Cliquez sur le bouton **Suivant**.
- Dans la fenêtre **Installation sans assistance**, cliquez sur **Suivant**.
- Cliquez sur **Configurer l'utilisateur** dans la fenêtre **Droits de jointure**.
- Cliquez sur le bouton **Sélectionner** dans la fenêtre **Configurer l'utilisateur**.
- Saisissez **administrateur** dans la fenêtre du choix de l'utilisateur puis cliquez sur les boutons **Vérifier les noms** et **Suivant**.
- Cliquez sur le bouton radio **Droits complets** puis sur **OK**.



- Cliquez sur le bouton **Terminer**.

Un message apparaît confirmant l'ajout du périphérique.

- Démarrez la machine **Test Déploiement**.

La station démarre sur le réseau et charge l'image sans que l'utilisateur ait besoin d'effectuer une manipulation. Avec l'aide d'un fichier de réponse, il est possible d'automatiser complètement le déploiement des postes.

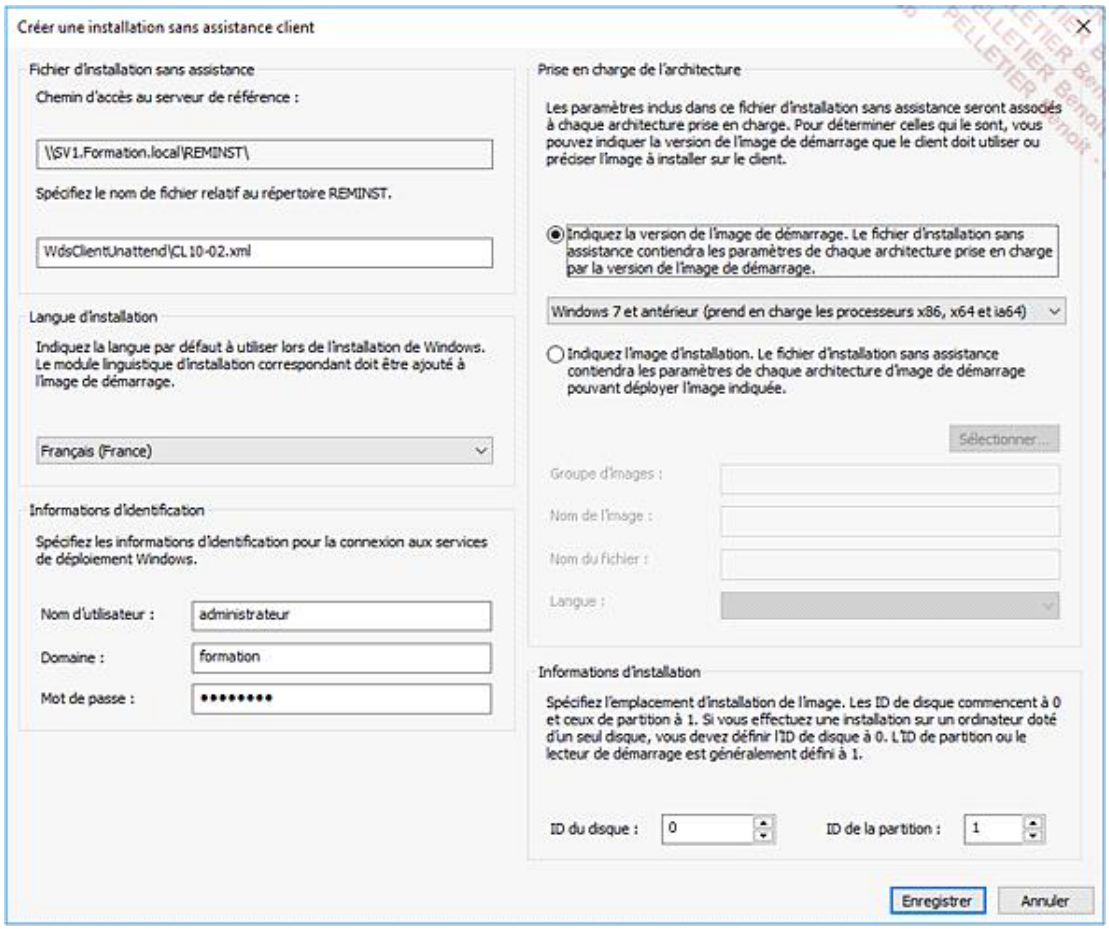
Création d'un fichier de réponse

L'utilisation d'un fichier de réponse permet l'automatisation du déploiement. Le fichier va contenir les informations d'identification, l'image souhaitée…

- Sur SV1, lancez la console **Services de déploiement Windows** par l'intermédiaire des **outils d'administration**.
- Cliquez sur **Périphériques de préinstallation Active Directory**.
- Effectuez un double clic sur le périphérique déjà présent.
- Dans la fenêtre **Installation sans assistance client**, cliquez sur **Créer un nouveau fichier**.

Le fichier XML qui permet l'automatisation des étapes d'installation est stocké dans le répertoire **WdsClientUnattend** et porte le nom du poste.

- Dans la liste déroulante **Langue d'installation**, sélectionnez **Français (France)**.
- Saisissez les informations d'authentification :
  - **Nom d'utilisateur** : administrateur
  - **Domaine** : formation
  - **Mot de passe** : Pa$$w0rd



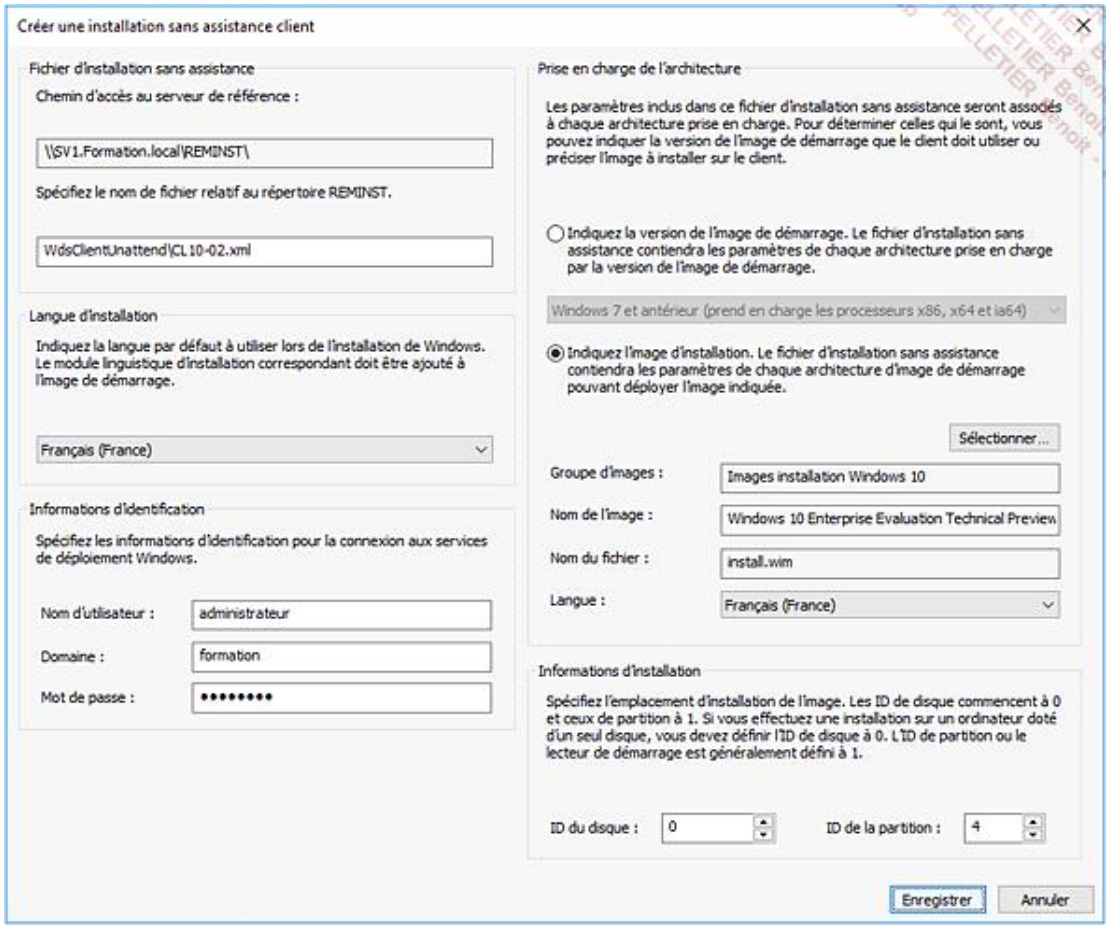
- Cochez **Indiquer l'image d'installation** puis cliquez sur le bouton **Sélectionner**.
- Sélectionnez dans la liste déroulante le groupe d'images **Images Installation Windows 10** puis cochez

Windows 10 Enterprise.

- Cliquez sur **OK** pour valider le choix.
- Sélectionnez **Français (France)** dans la liste déroulante **Langue**.

Le poste est composé d'un disque et de plusieurs partitions : les partitions système et la partition hébergeant les fichiers du système d'exploitation ayant l'ID 4.

- À l'aide des boutons, sélectionnez le chiffre **4** dans **ID de la partition**.



- Cliquez sur le bouton **Enregistrer** puis sur **OK**.
- Démarrez la machine **Test Déploiement**.

La station démarre sur le réseau et charge l'image sans que l'utilisateur ait besoin d'effectuer une manipulation. L'installation se poursuit mais il est nécessaire de créer un autre fichier pour automatiser la configuration des écrans d'accueil Windows.

Présentation de WSUS

Le service WSUS (*Windows Server Update Services*) permet aux administrateurs d'effectuer la gestion et la distribution des mises à jour par le biais d'une console MMC. Il est possible de monter un serveur WSUS en cascade : le premier serveur (appelé serveur en amont) servira de source aux autres serveurs de l'organisation. Il lui est nécessaire de se connecter à Microsoft Update afin de récupérer les mises à jour disponibles.

Le principal atout de ce service est la gestion centralisée des mises à jour. Il est possible de procéder à l'administration de ces serveurs en utilisant des applets de commande PowerShell. Avant d'implémenter ce rôle, il faut s'assurer d'avoir assez d'espace disque.

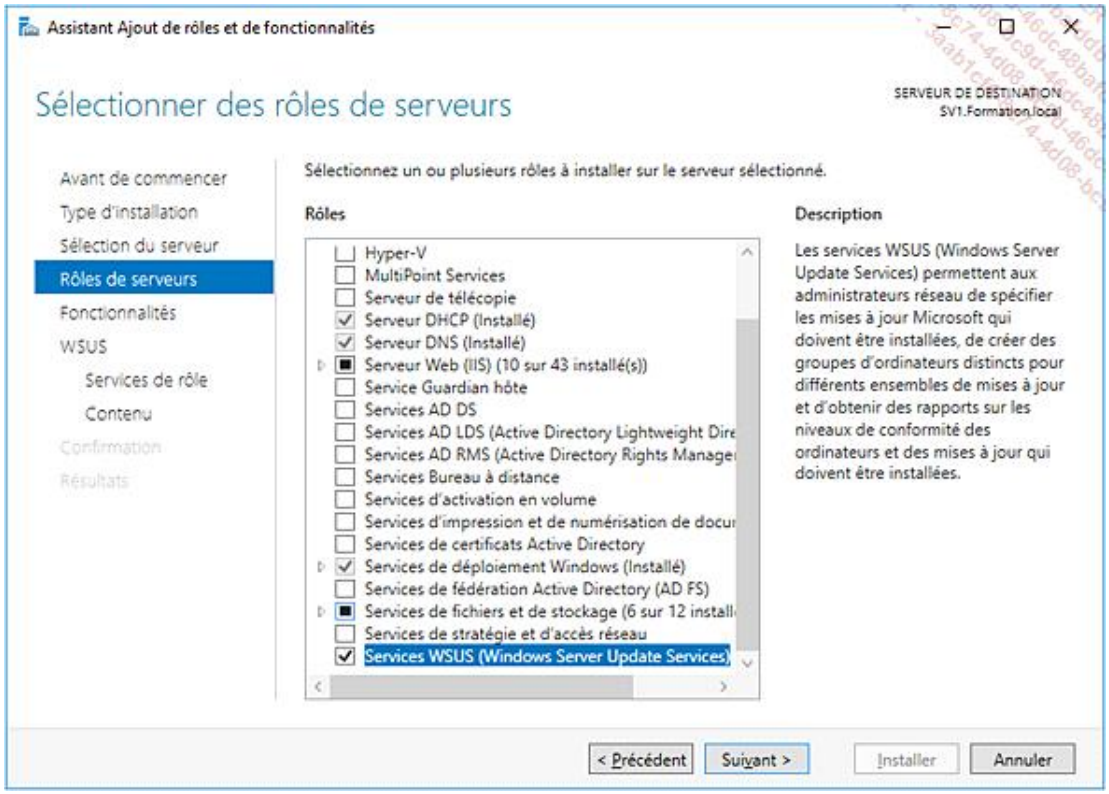
Un serveur IIS doit être présent, ainsi qu'un serveur de base de données (SQL 2008 R2, 2012, base de données interne à Windows).

Mise en place du serveur de mise à jour

L'installation de WSUS nécessite uniquement l'ajout d'un rôle. Il est conseillé de s'assurer de posséder assez d'espace disque.

Une connexion à Internet est nécessaire pour la récupération de la liste des correctifs et du téléchargement de ces derniers. Il est nécessaire de vérifier les commutateurs des machines virtuelles utilisées ainsi que leurs adresses IP.

- Sur SV1, lancez la console **Gestionnaire de serveur**.
- Cliquez sur **Ajouter des rôles et des fonctionnalités**.
- Dans la fenêtre **Avant de commencer**, cliquez sur **Suivant**.
- Laissez cochée **Installation basée sur un rôle ou une fonctionnalité** dans la fenêtre **Sélectionner le type d'installation**.
- Cliquez sur **Suivant** pour valider la destination.
- Cochez le rôle **Services WSUS (Windows Server Update Services)** puis cliquez sur le bouton **Ajouter les fonctionnalités** dans la fenêtre qui s'affiche.



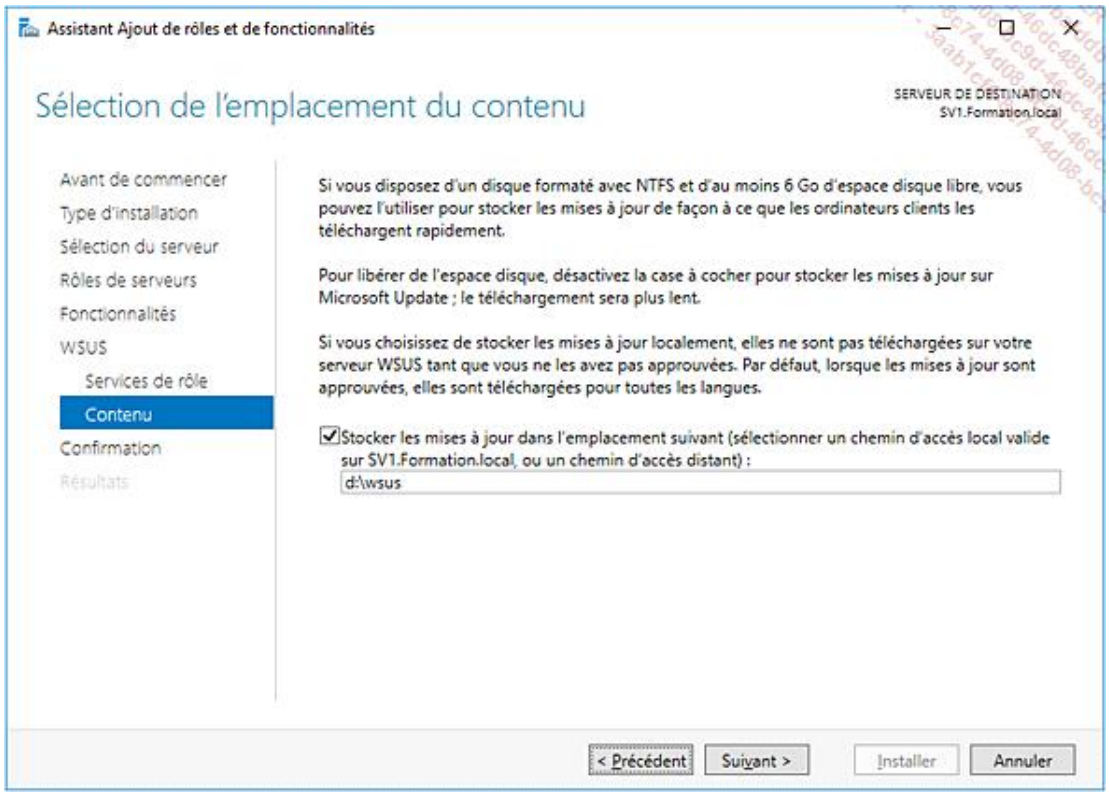
- Laissez les **Services de rôles** par défaut et cliquez sur **Suivant**.

On trouve les services suivants :

- **WID Connectivity** : le rôle WSUS utilise la base de données interne à Windows.
- **WSUS Services** : installe les services utilisés par les services WSUS (service de mise à jour, de création de rapport…).
- **SQL Server Connectivity** : permet à WSUS d'utiliser un serveur SQL à la place d'une base de données interne.

Les services de rôle WID Database et Base de données ne peuvent pas être utilisés simultanément. Il est nécessaire de faire un choix entre les deux.

- Créez un répertoire nommé **WSUS**. Ce dernier contiendra les mises à jour téléchargées depuis Microsoft Update.
- Dans le champ, saisissez **D:\WSUS** (remplacer la lettre par celle attribuée à la partition).



- Cliquez deux fois sur **Suivant** puis sur **Installer**.

Une fois installé, il faut vérifier que le pare-feu de l'entreprise contient la règle qui autorise WSUS à se connecter au serveur Microsoft Update. La liste ci-dessous présente les URL sur lesquelles le serveur WSUS est susceptible de se connecter :

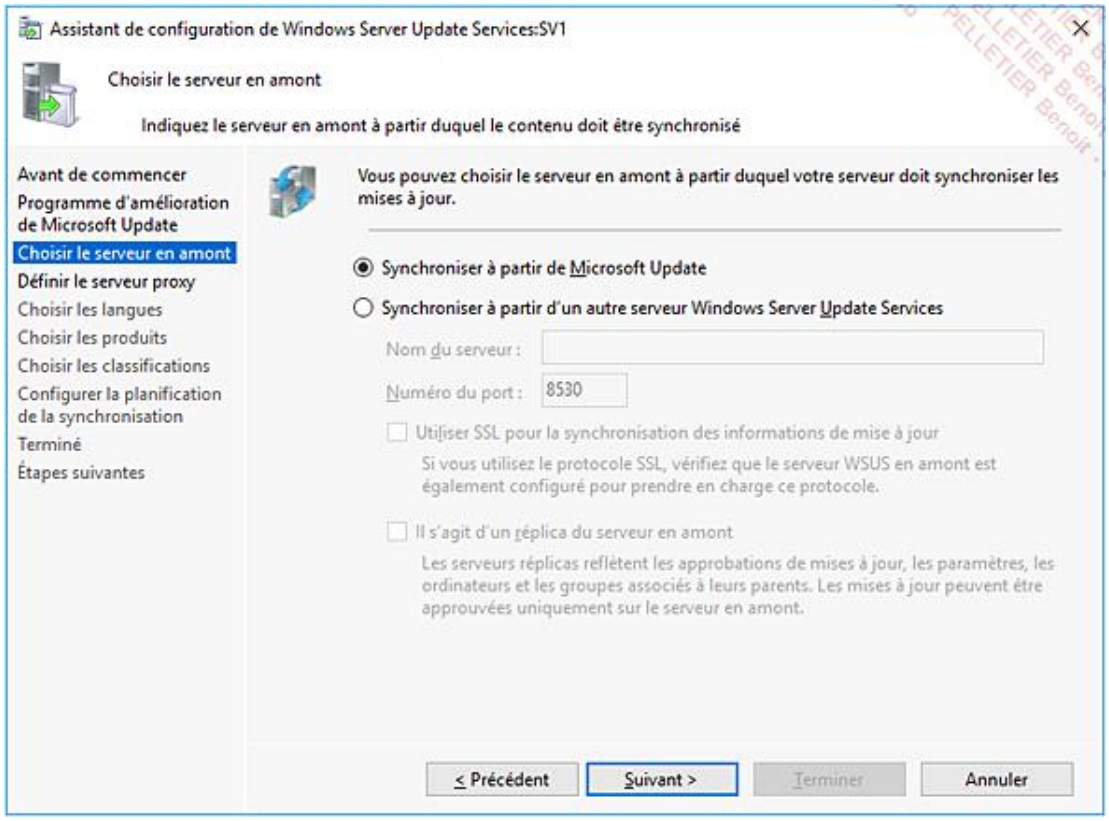
- http://windowsupdate.microsoft.com
- http://*.windowsupdate.microsoft.com
- https://*.windowsupdate.microsoft.com
- http://*.update.microsoft.com
- https://*.update.microsoft.com
- http://*.windowsupdate.com
- http://download.windowsupdate.com
- http://download.microsoft.com
- http://*.download.windowsupdate.com
- http://wustat.windows.com
- http://ntservicepack.microsoft.com

- Depuis le menu **Démarrer**, accédez à la console **Windows Server Update Services** depuis **Outils d'administration Windows**.

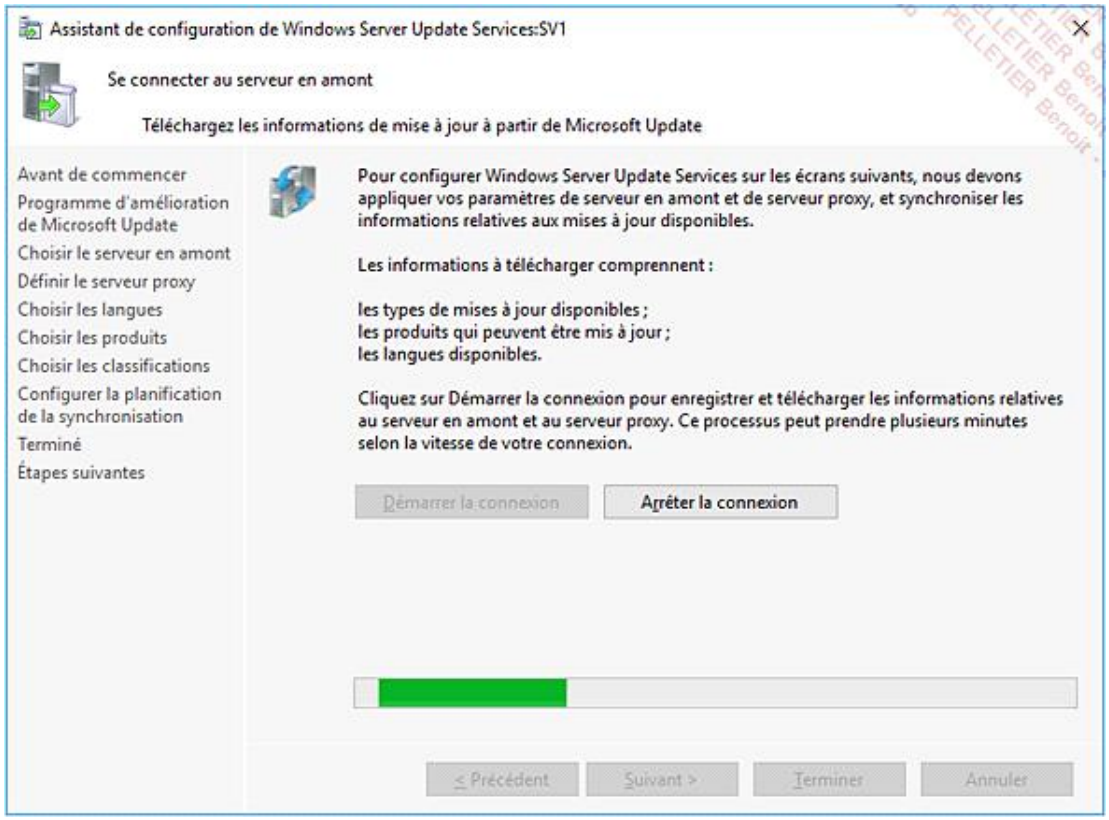
L'assistant des **Services WSUS** (*Windows Server Update Services*) s'affiche.

- Dans la fenêtre **Terminer l'installation de WSUS**, validez le chemin du répertoire de stockage des mises à jour et cliquez sur **Exécuter**.
- Cliquez sur **Terminer**. Un deuxième assistant se lance.
- Cliquez sur **Suivant** dans la fenêtre **Avant de commencer**.
- Le serveur étant en amont, cliquez sur **Suivant** dans la fenêtre **Choisir le serveur en amont**.

Il est possible de configurer le serveur comme serveur en aval. Indiquez alors au serveur son serveur en amont.



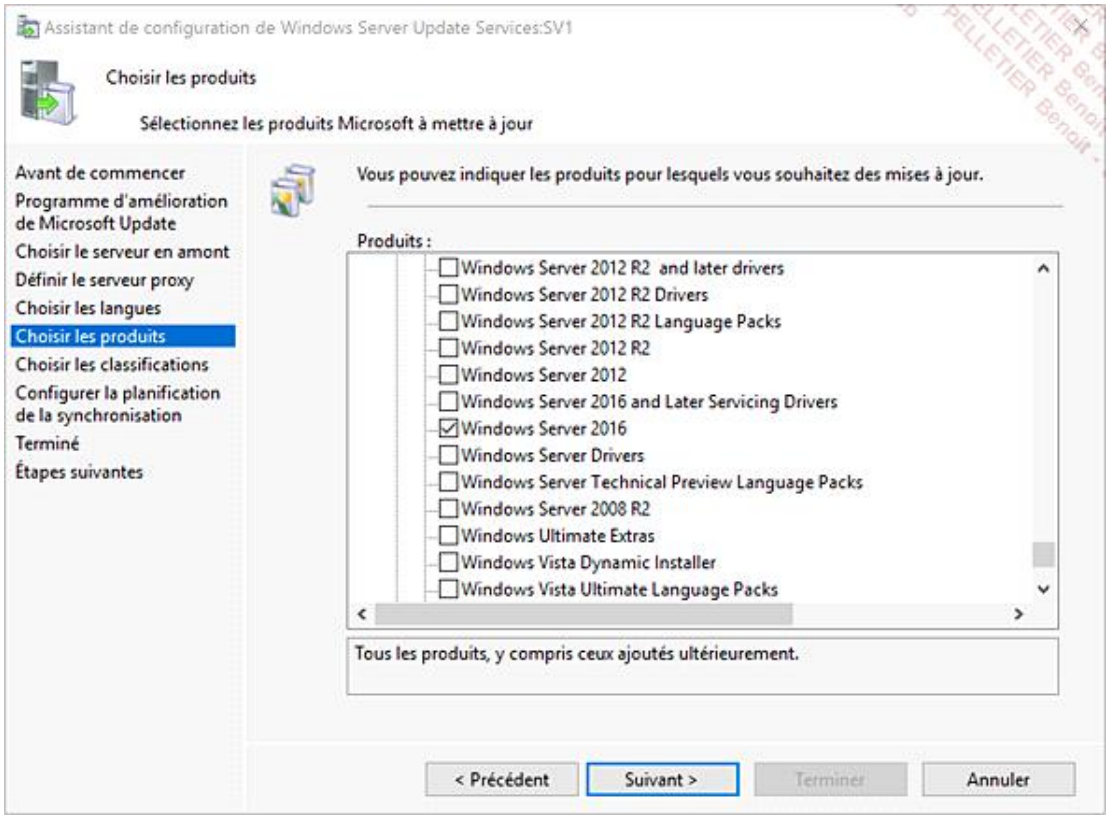
- Aucun serveur proxy n'étant utilisé pour accéder à Internet, laissez les choix par défaut dans la fenêtre **Définir le serveur proxy**.
- Cliquez sur **Démarrer la connexion** pour récupérer depuis le serveur Microsoft Update :
  - Les types de mises à jour disponibles.
  - Les produits qui peuvent être mis à jour.
  - Les langues disponibles.



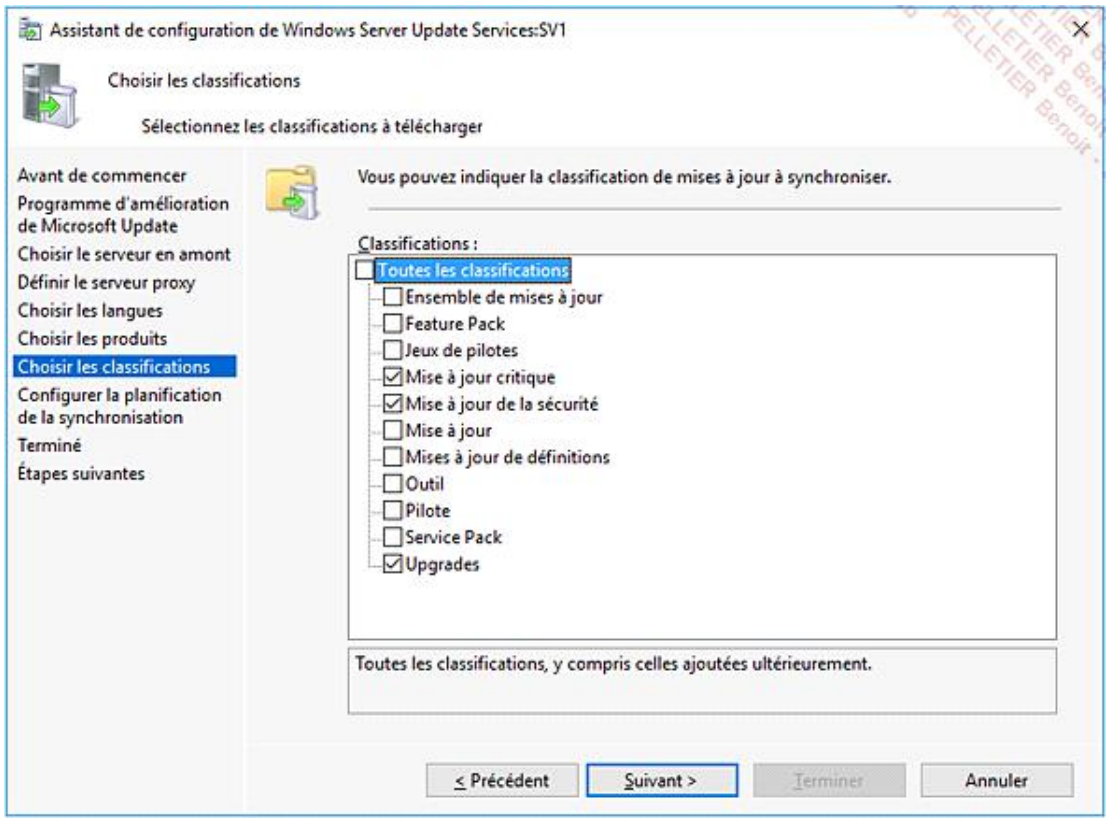
- Une fois la connexion établie, cliquez sur **Suivant** pour continuer.
- Sélectionnez les langues souhaitées puis cliquez sur **Suivant**.

Les produits qui doivent être mis à jour sont **Windows Server 2016** et **Windows 10**.

- Sélectionnez dans la liste, les produits qui doivent être mis à jour.

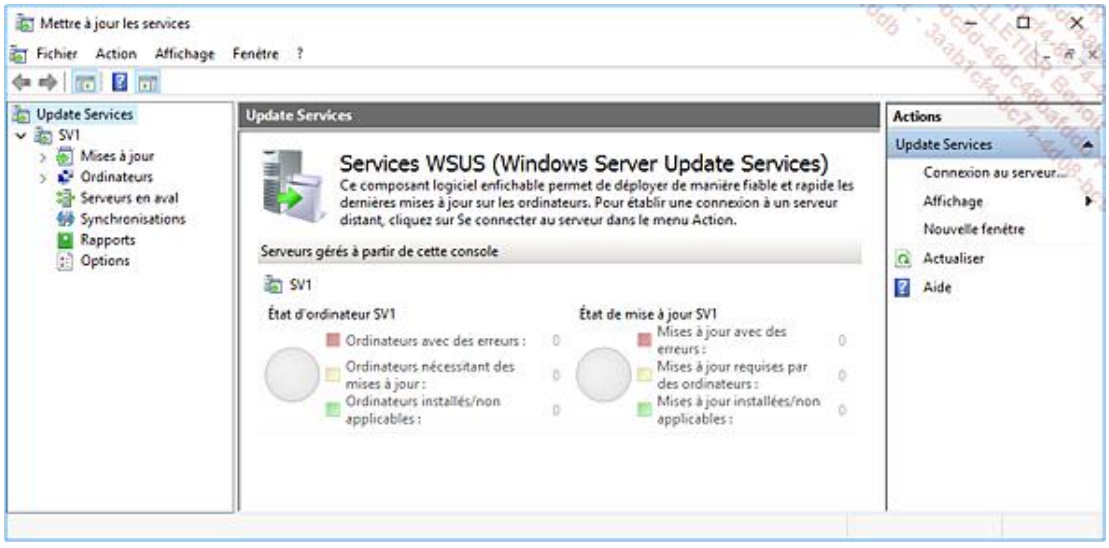


- Cochez **Mise à jour critique**, **Mise à jour de la sécurité** et **Upgrades** puis cliquez sur **Suivant**.



La synchronisation du serveur WSUS avec le serveur Microsoft Update peut être planifiée ou lancée manuellement.

- Cochez le bouton radio **Synchroniser manuellement**.
- Cliquez sur **Suivant** puis sur **Terminer**.
- La console se lance, développez le nœud **SV1**.



- Sélectionnez le nœud **Synchronisations** puis cliquez sur **Synchroniser maintenant**.

La synchronisation est en cours…

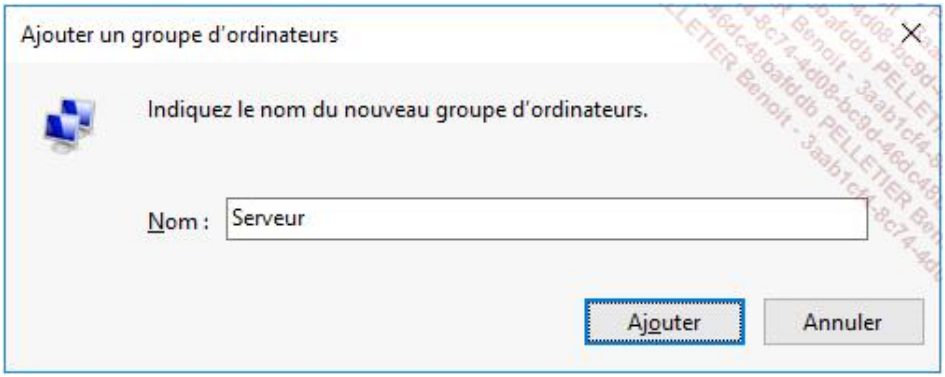
Avant d’approuver les mises à jour, les postes clients et les autres serveurs doivent être connectés aux serveurs WSUS.

Gestion de WSUS

Le serveur est maintenant configuré, néanmoins aucun poste client n'est relié. Le ciblage s'effectue au niveau du client. Pour effectuer cette opération, il est nécessaire d'utiliser une stratégie de groupe qui configure Windows Update sur le poste. L'utilisation d'un fichier REG peut également être envisagée.

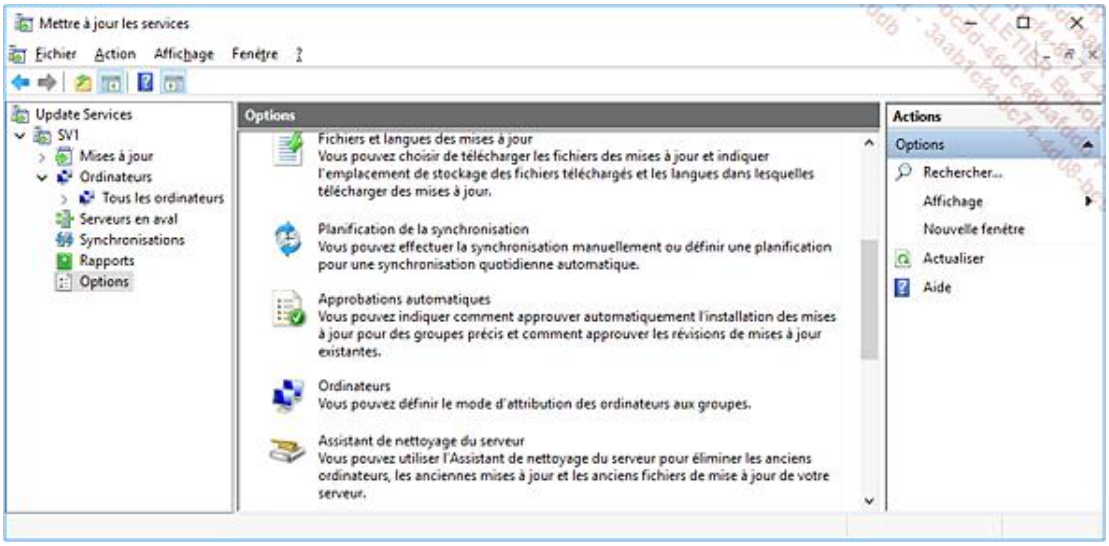
1. Création des groupes d'ordinateurs

- Lancez la console **Windows Server Update Services** sur **SV1**.
- Développez le nœud **Ordinateurs** et effectuez un clic droit sur **Tous les ordinateurs** puis sélectionnez **Ajouter un groupe d'ordinateurs**.
- Dans le champ **Nom**, saisissez **Poste Client** et cliquez sur **Ajouter**.
- Effectuez un clic droit sur **Tous les ordinateurs** puis sélectionnez **Ajouter un groupe d'ordinateurs**.
- Dans le champ **Nom**, saisissez **Serveur** et cliquez sur **Ajouter**.

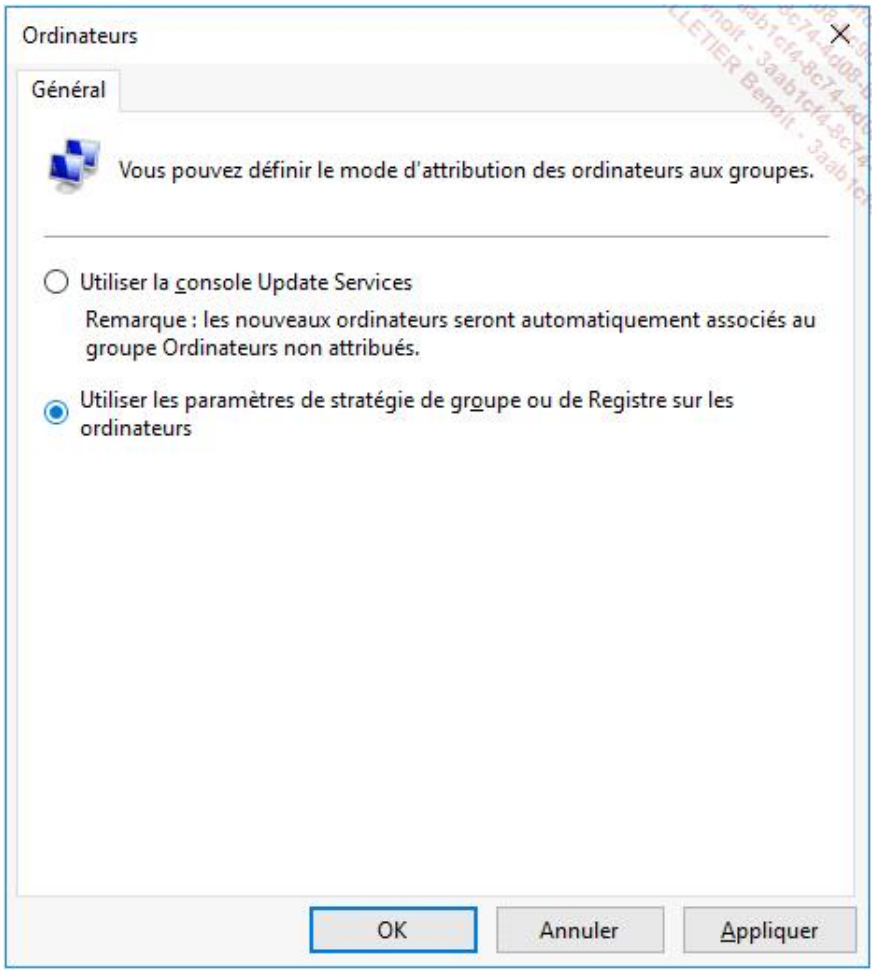


Les groupes sont maintenant créés.

- Cliquez sur **Options** puis sur **Ordinateurs**.



- Cochez **Utiliser les paramètres de stratégie de groupe ou de Registre sur les ordinateurs** puis cliquez sur **OK**.

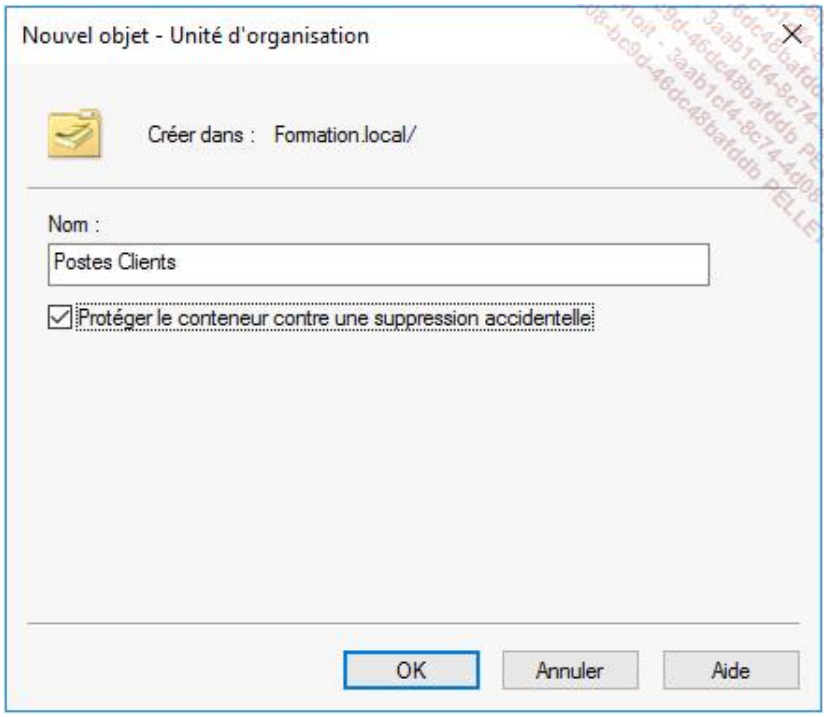


La configuration des clients Windows Update peut désormais être effectuée.

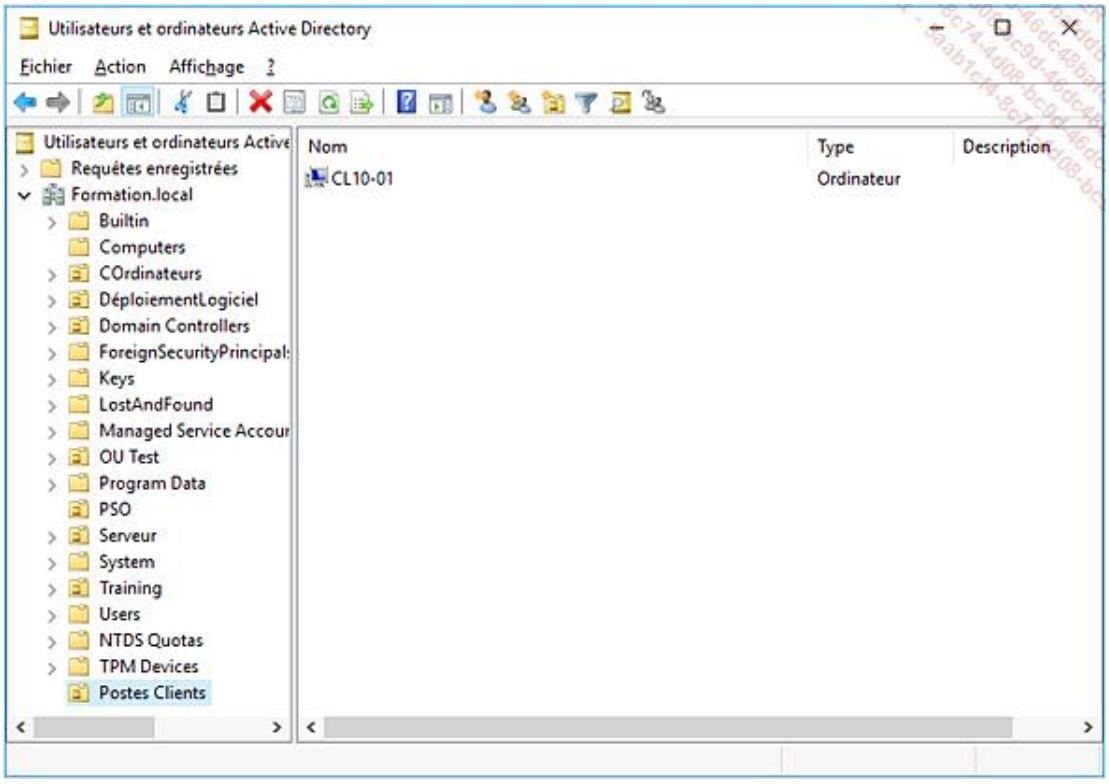
2. Configuration des postes clients

La stratégie de groupe qui va être appliquée aux postes permet de configurer l'adresse IP du serveur à contacter mais également le groupe d'ordinateurs à joindre.

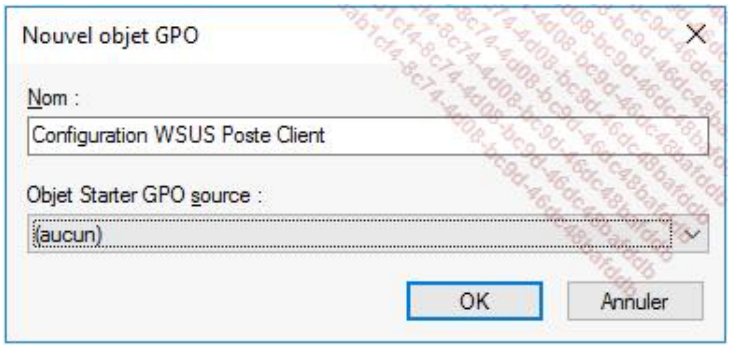
- Sur AD1, lancez la console **Utilisateurs et ordinateurs Active Directory**.
- Effectuez un clic droit sur **Formation.local** puis sélectionnez **Nouveau**, **Unité d'organisation**.
- Saisissez **Postes Clients** dans le champ **Nom** puis cliquez sur **OK**.



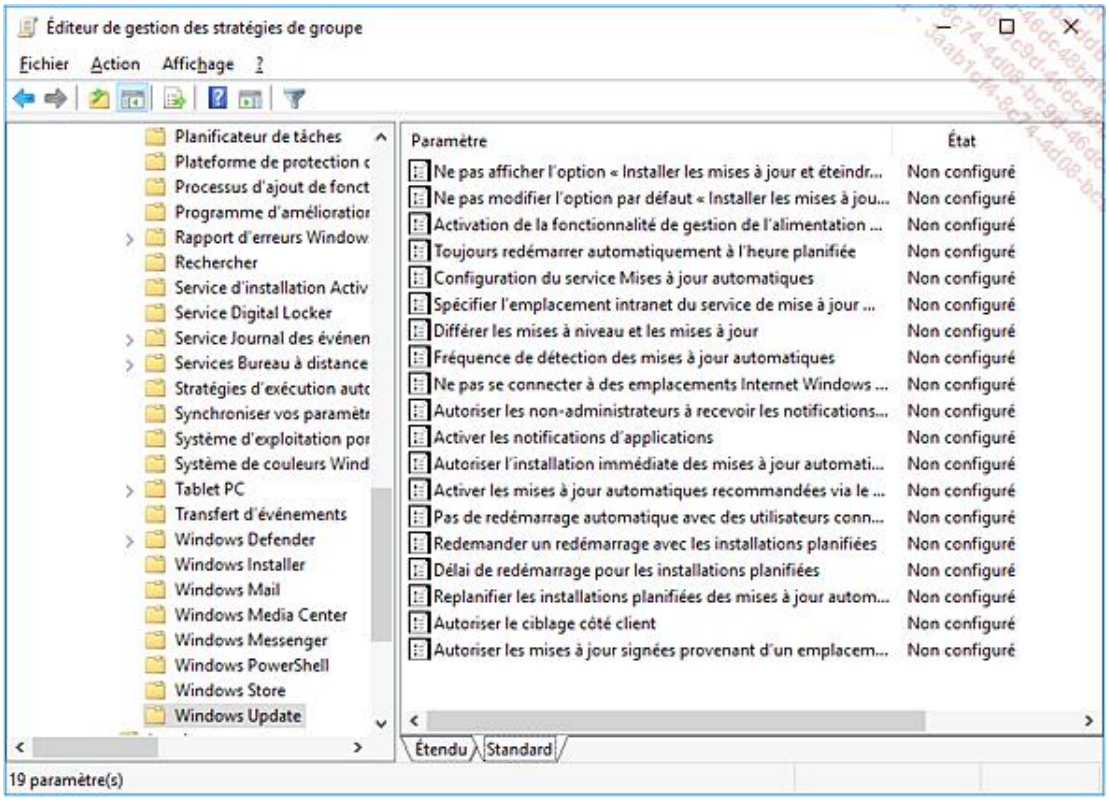
- Déplacez le compte ordinateur de **CL10-01** dans l'OU **Postes Clients**.



- Vérifiez la présence du compte ordinateur de **SV1** dans l'OU **Serveur**.
- Lancez la console **Gestion de stratégie de groupe**.
- Effectuez un clic droit sur **Objets de stratégie de groupe** puis sélectionnez **Nouveau**.
- Saisissez **Configuration WSUS Poste Client** dans le champ **Nom**.



- Effectuez un clic droit sur **Configuration WSUS Poste Client** puis dans le menu contextuel, sélectionnez **Modifier**.
- Développez les nœuds **Configuration ordinateur**, **Stratégies**, **Modèles d'administration**, **Composants Windows** puis sélectionnez **Windows Update**.



- Double cliquez sur **Configuration du service Mises à jour automatique**.
- Cochez le bouton radio **Activé**.
- Dans la liste déroulante **Configuration du service Mises à jour automatique**, sélectionnez **Téléchargement automatique et notifications des installations**.

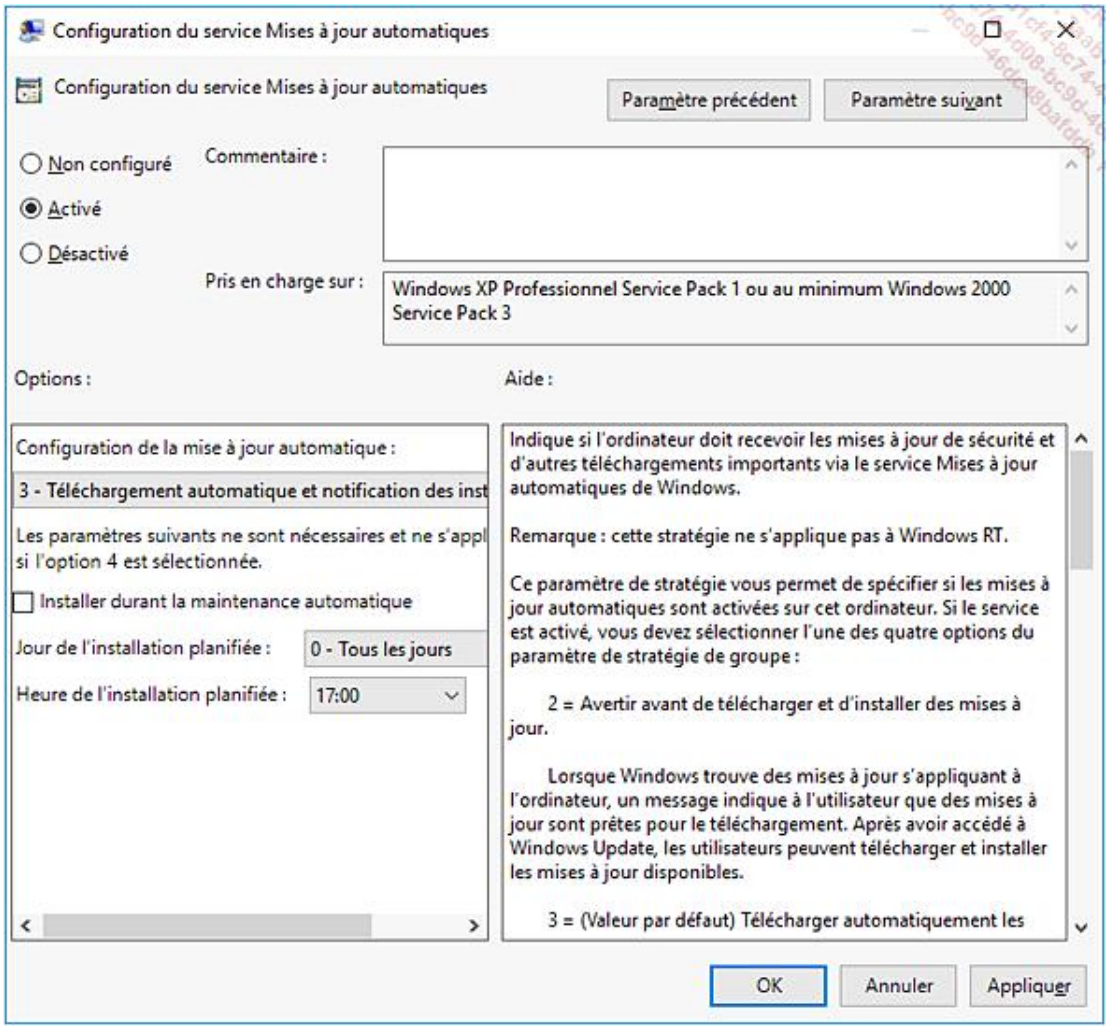
  Quatre options sont possibles :

  - **Notification des téléchargements et des installations**. L'administrateur connecté est averti avant le téléchargement et l'installation des mises à jour.
  - **Téléchargement automatique et notifications des installations**. Le téléchargement est automatiquement lancé et par la suite, l'administrateur connecté reçoit un avertissement avant l'installation de la mise à jour.
  - **Téléchargement automatique et planification des installations**. Le téléchargement des mises à jour est automatique avec cette option. Par la suite, les mises à jour sont installées en fonction des jour et heure

spécifiés.

- **Autoriser l'administrateur local à choisir les paramètres**. Cette option laisse la possibilité à un utilisateur membre du groupe Administrateurs de modifier des options configurées de l'applet Mises à jour automatique présentes dans le panneau de configuration.

- Sélectionnez **17:00** dans la liste déroulante **Heure de l'installation planifiée**.

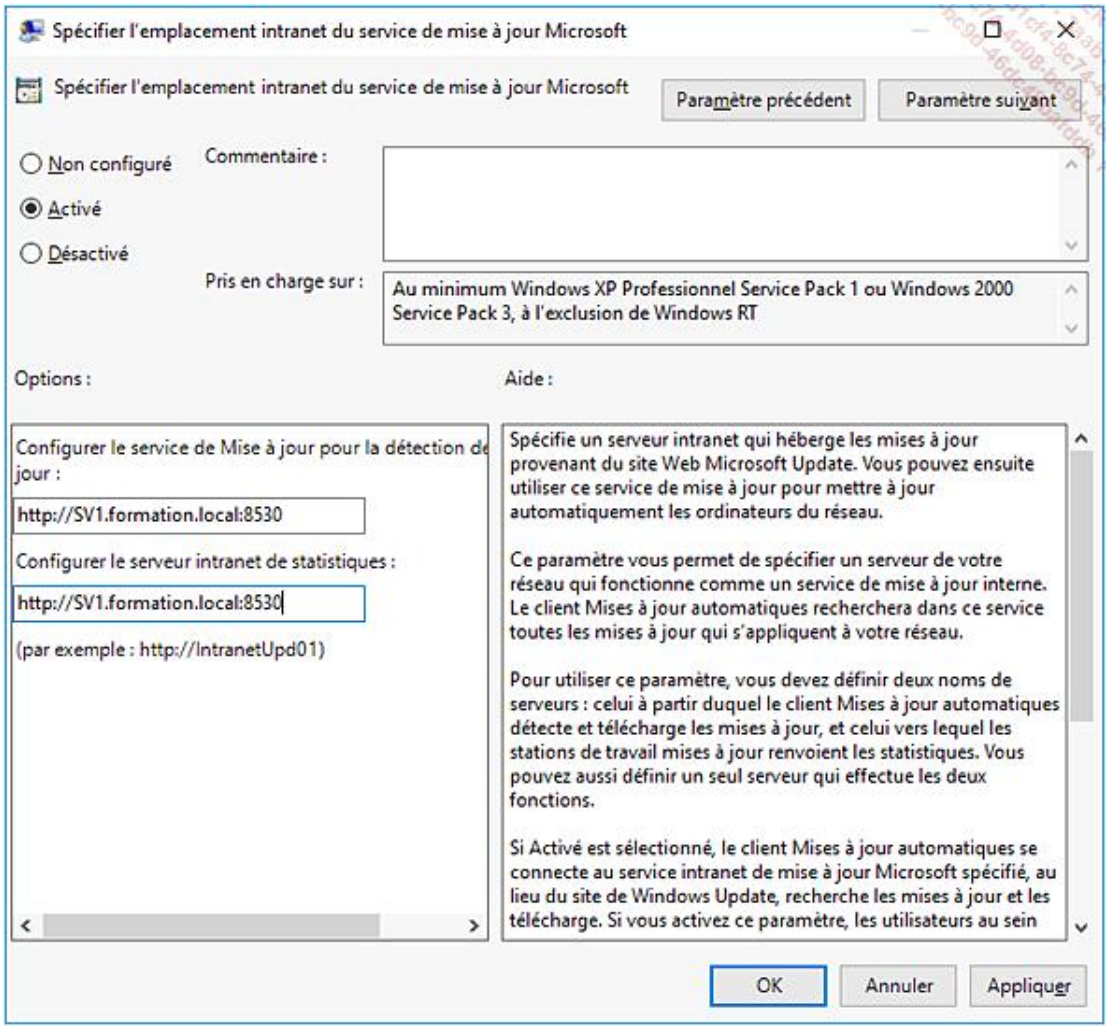


- Cliquez sur **Appliquer** puis sur **OK**.

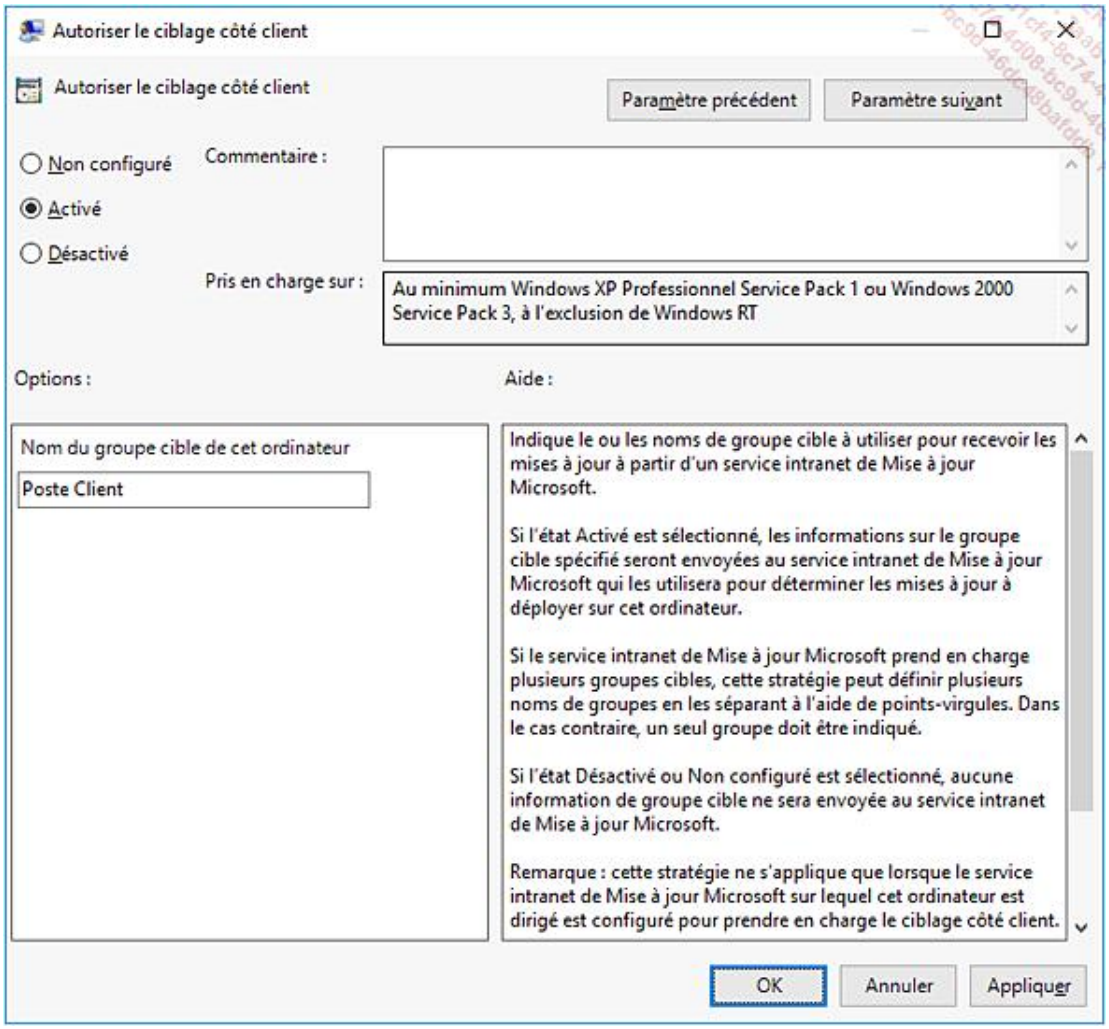
- Double cliquez sur **Spécifier l'emplacement intranet du service de mise à jour Microsoft**.

- Saisissez **http://SV1.formation.local:8530** dans les champs **Configurer le service de mise à jour pour la détection des mises à jour** et **Configurer le serveur intranet de statistiques**.

Le port utilisé par défaut par le serveur WSUS est le port 8530.



- Cliquez sur **Appliquer** puis sur **OK**.
- Double cliquez sur **Autoriser le ciblage côté client**.
- Sélectionnez **Activer** puis saisissez **Poste Client** dans le champ **Nom du groupe cible de cet ordinateur**.



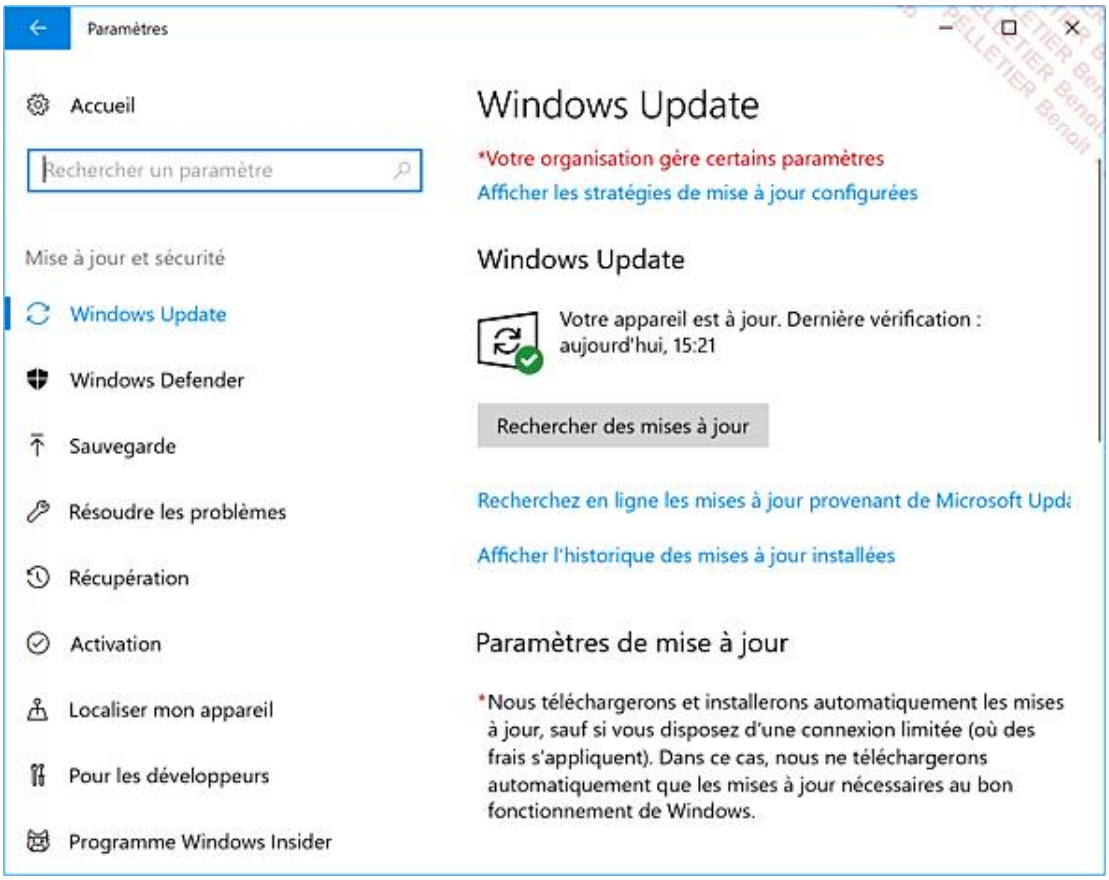
- Cliquez sur **Appliquer** puis **OK**.
- Fermez la fenêtre **Éditeur de gestion de stratégie de groupe**.
- Dans la console **Gestion de stratégies de groupe**, effectuez un clic droit sur l'OU **Postes Clients** puis sélectionnez **Lier un objet de stratégie de groupe existant**.
- Sélectionnez **Configuration WSUS Poste Client** puis cliquez sur **OK**.

La précédente stratégie de groupe est destinée aux postes de travail. Il faut donc maintenant créer une stratégie similaire pour les serveurs.

- Effectuez un clic droit sur **Objets de stratégie de groupe** puis sélectionnez **Nouveau**.
- Saisissez **Configuration WSUS Serveur** dans le champ **Nom**.
- Développez les nœuds **Configuration ordinateur**, **Stratégies**, **Modèles d'administration**, **Composants** puis sélectionnez **Windows Update**.
- Double cliquez sur **Configuration du service Mises à jour automatique**.
- Cochez le bouton radio **Activé**.
- Dans la liste déroulante **Configuration du service Mises à jour automatique**, sélectionnez **Téléchargement automatique et notifications des installations**.
- Sélectionnez **17:00** dans la liste déroulante **Heure de l'installation planifiée**.
- Cliquez sur **Appliquer** puis sur **OK**.

- Double cliquez sur **Spécifier l'emplacement intranet du service de mise à jour Microsoft**.
- Saisissez **http://SV1.formation.local:8530** dans les champs **Configurer le service de mise à jour pour la détection des mises à jour** et **Configurer le serveur intranet de statistiques**.
- Cliquez sur **Appliquer** puis sur **OK**.
- Double cliquez sur **Autoriser le ciblage côté client**.
- Sélectionnez **Activer** puis saisissez **Serveur** dans le champ **Nom du groupe de ciblage**.
- Fermez la fenêtre **Éditeur de gestion des stratégies de groupe**.
- Dans la console **Gestion de stratégie de groupe**, effectuez un clic droit sur l'OU **Serveur** puis sélectionnez **Lier un objet de stratégie de groupe existant**.
- Sélectionnez **Configuration WSUS Serveur** puis cliquez sur **OK**.
- Lancez une invite de commandes DOS sur **CL10-01** et saisissez la commande `gpupdate /force`.
- Recommencez l'étape précédente sur **SV1**.

Les paramètres dans Windows Update sont grisés car les paramètres de la stratégie de groupe ont été pris en compte.



Les machines clientes et serveurs sont maintenant reliées aux serveurs WSUS.

3. Approbation et déploiement des mises à jour

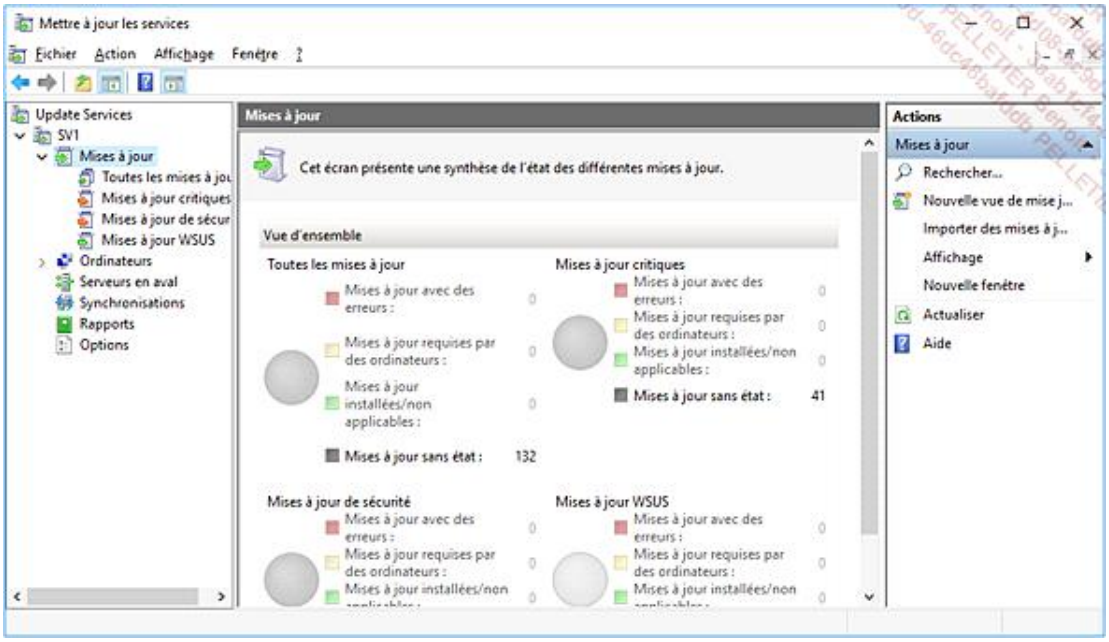
Un ordinateur présent dans un groupe d'ordinateurs va contacter automatiquement le serveur WSUS afin de récupérer les mises à jour. Il est préférable de déployer dans un premier temps les mises à jour dans un groupe

d'ordinateurs de test. Cette étape permet de s'assurer du bon fonctionnement du déploiement, mais principalement de l'état des applications après l'installation de la mise à jour. Il peut arriver qu'une application ne fonctionne plus suite à l'application d'un correctif.

Une fois les tests effectués sur une plateforme (de préférence la plus représentative de la production), il est nécessaire d'approuver les mises à jour pour les groupes d'ordinateurs de la production. Le fait de scinder les ordinateurs clients et les serveurs permet de restreindre l'application du correctif au bon groupe (application des correctifs Windows 10 au groupe **Poste Client** et application des mises à jour Windows Server 2016 au groupe **Serveur**).

- Dans la **console Updates Services**, cliquez sur le nœud **Mises à jour**.

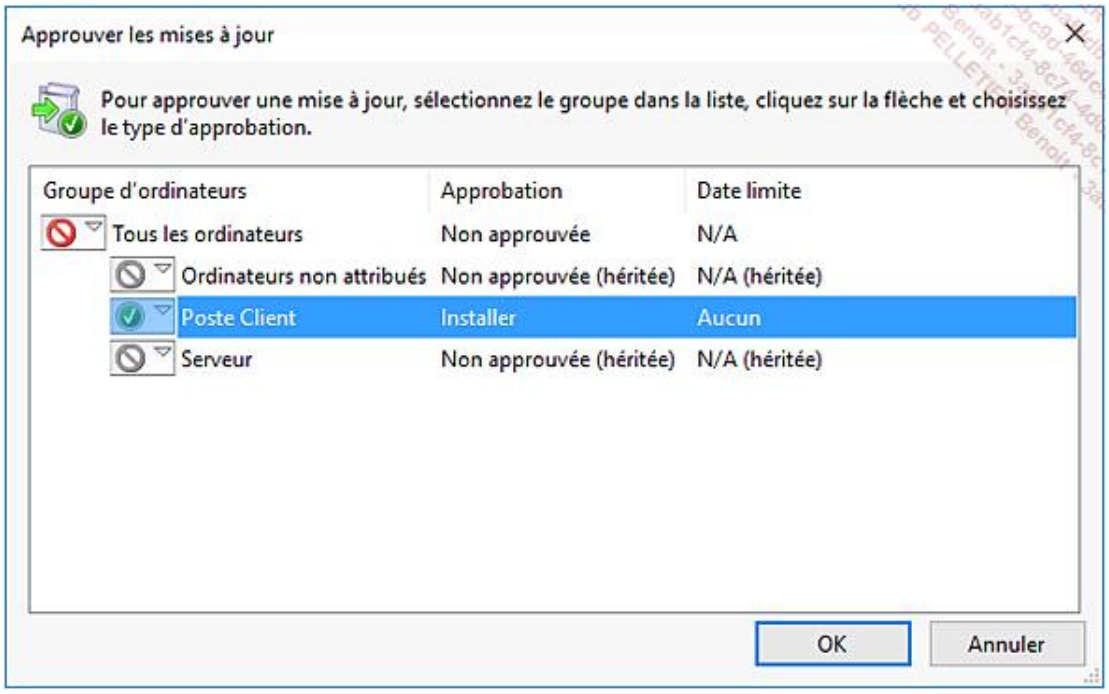
Une synthèse des mises à jour s'affiche. Un graphique est présent pour les catégories **Toutes les mises à jour**, **Mises à jour critiques**, **Mises à jour de sécurité** et **Mises à jour WSUS**.



- Dans la section **Toutes les mises à jour**, sélectionnez **Toutes** dans la liste déroulante **État**. Cliquez sur **Actualiser**.
- Sélectionnez la ou les mises à jour souhaitées.

Sélectionnez uniquement les mises à jour serveur ou uniquement les mises à jour clientes souhaitées.

- Effectuez un clic droit sur les mises à jour souhaitées et cliquez sur **Approuver**.
- Cliquez sur le groupe **Serveur ou Poste Client** et sélectionnez **Approuvée pour l'installation** dans la liste déroulante.



L'approbation est en cours…

Cliquez sur **OK**.

Dans le menu contextuel utilisé pour approuver un correctif, d'autres options sont disponibles.

- **Approuvée pour la suppression** : si le correctif cause des défaillances sur le poste après son installation, il est nécessaire de le désinstaller. Afin de ne pas avoir à passer sur tous les postes, il suffira d'approuver cette mise à jour pour suppression, **si le correctif le supporte**.
- **Date limite** : la date limite permet de déterminer la date et l'heure limites pour l'installation de la mise à jour. Pour accélérer le traitement de la mise à jour, insérez une date passée (le 1e septembre si l'approbation est faite le 2 septembre).

Une fois la mise à jour téléchargée par le serveur WSUS, les clients Windows Update sur les postes et le serveur pourront récupérer les mises à jour.

4. Gestion de WSUS en ligne de commande

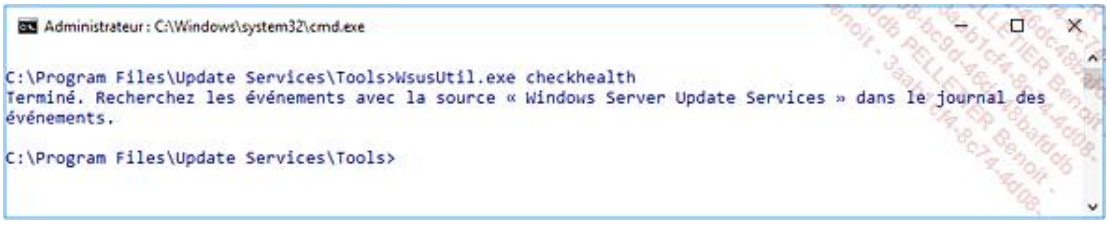
WSUS peut être administré à l'aide de l'interface graphique néanmoins certaines opérations ne peuvent s'effectuer qu'en ligne de commande.

Wsusutil checkhealth

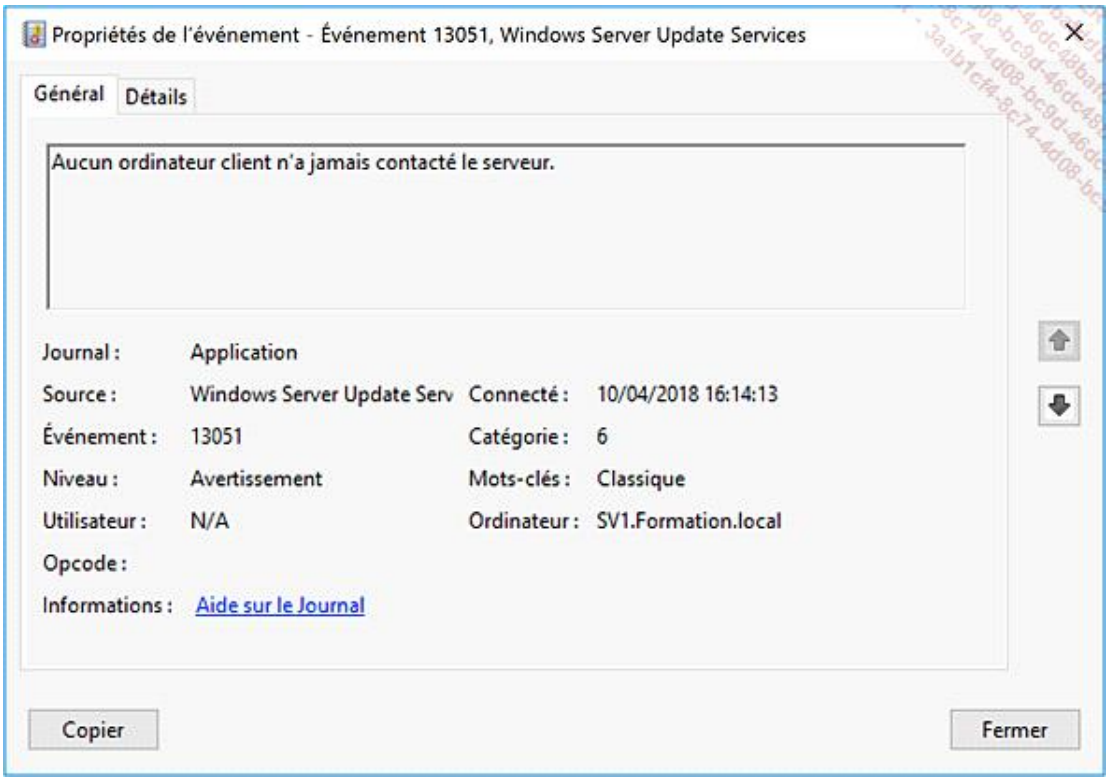
Cette commande permet de connaitre très rapidement l'état de santé du serveur WSUS. À la sortie de la commande, un événement dans le journal est créé. Si un événement possédant l'ID 1000 est présent, le serveur est en bonne santé.

La commande Wsusutil est de type externe, il est donc nécessaire de placer le prompt dans le répertoire adéquat.

Ainsi en accédant aux dossier C:\Program Files\Update Services\Tools, il est possible d'utiliser la commande.



Un événement est présent dans le journal Application du serveur. Celui-ci indique qu'aucun client n'a contacté le serveur pour l'instant.



Il est donc facile de réaliser un premier diagnostic de l'état de santé du serveur.

Wsusutil configuressl

Un serveur WSUS utilise par défaut le protocole HTTP, néanmoins il est fréquent de voir pour des raisons de sécurité des serveurs utilisant le protocole HTTPS. Ce sujet est détaillé dans le point suivant.

Wsusutil reset

Après la restauration de la base de données du serveur WSUS, il peut être utile d'exécuter la commande wsusutil suivi du commutateur reset. Ce dernier vérifie que chaque mise à jour présente dans la base de données correspond à un correctif dans le répertoire partagé. Dans le cas d'une absence de correctif ou si ce dernier était corrompu, un nouveau téléchargement sera opéré.

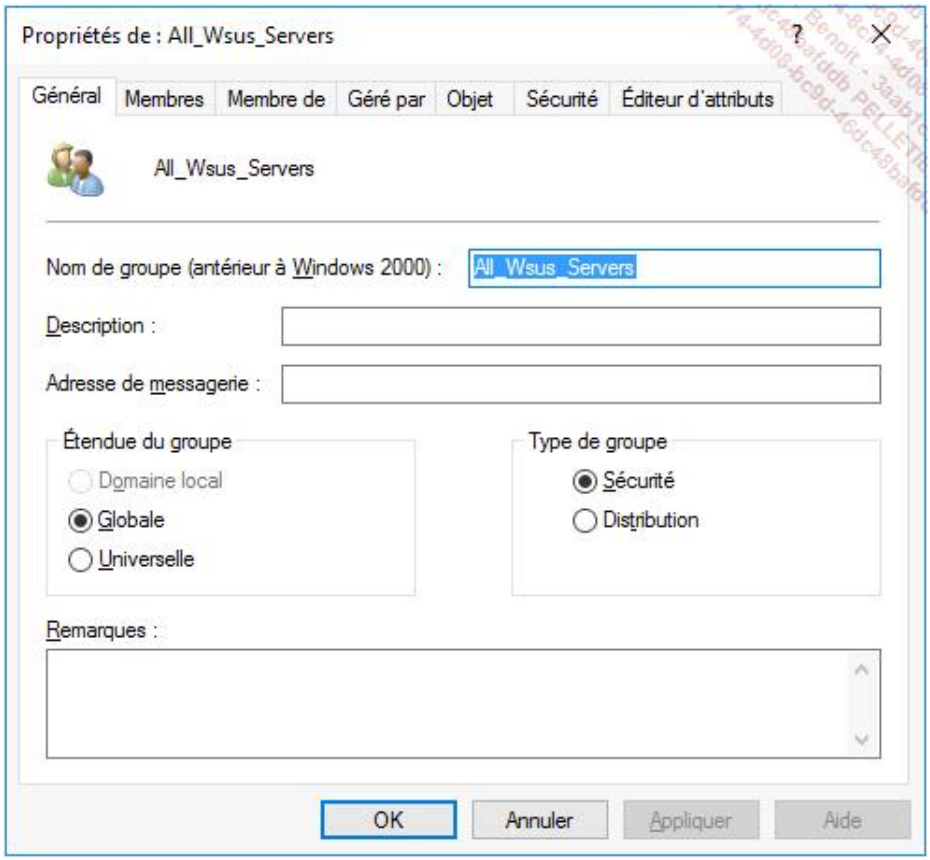
5. Mise en place de SSL pour WSUS

La mise en place du protocole SSL nécessite d'avoir une autorité de certification d'entreprise sur le réseau local. Un certificat autosigné peut également fonctionner, il est néanmoins préférable d'utiliser une autorité de certification.

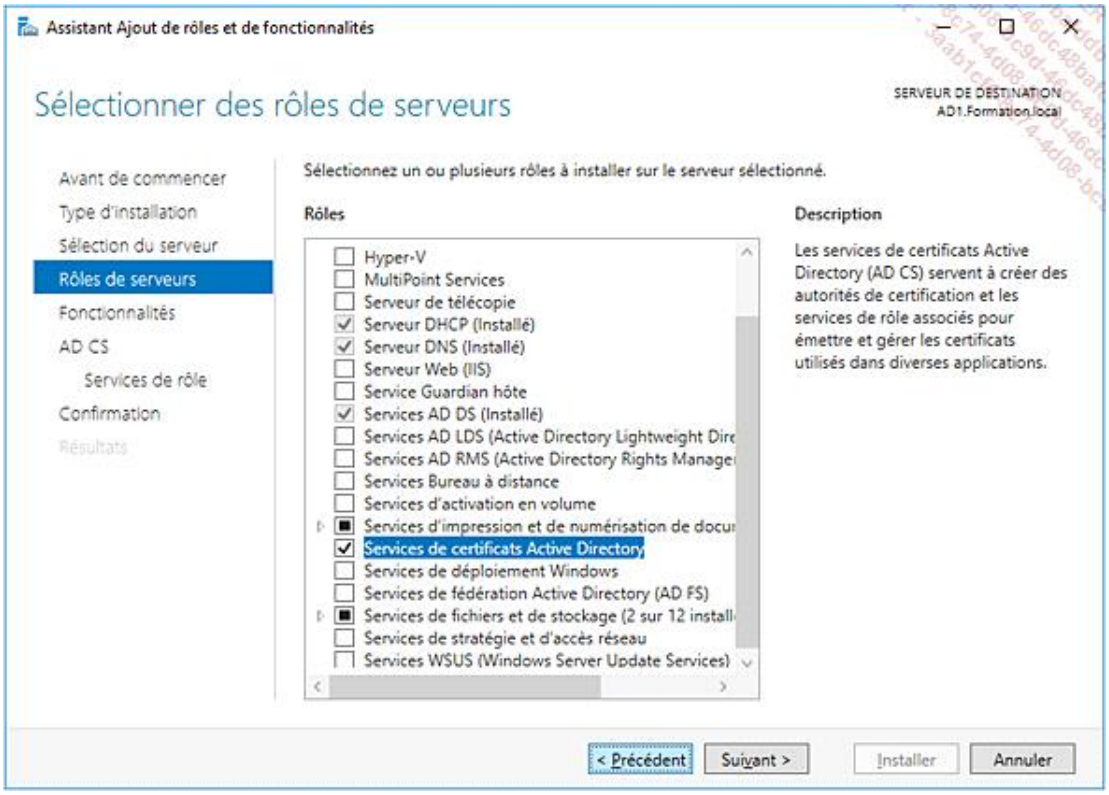
Une fois le certificat obtenu, il est nécessaire de procéder à la configuration du serveur à l'aide de la commande wsusutil.

L'installation de l'autorité de certification va dans un premier temps être effectuée. Le serveur qui aura ce rôle est AD1. Attention, en production, il est préférable d'installer le rôle sur un serveur qui n'est pas contrôleur de domaine. Les futures mises à niveau des contrôleurs de domaine s'en trouveront plus aisées.

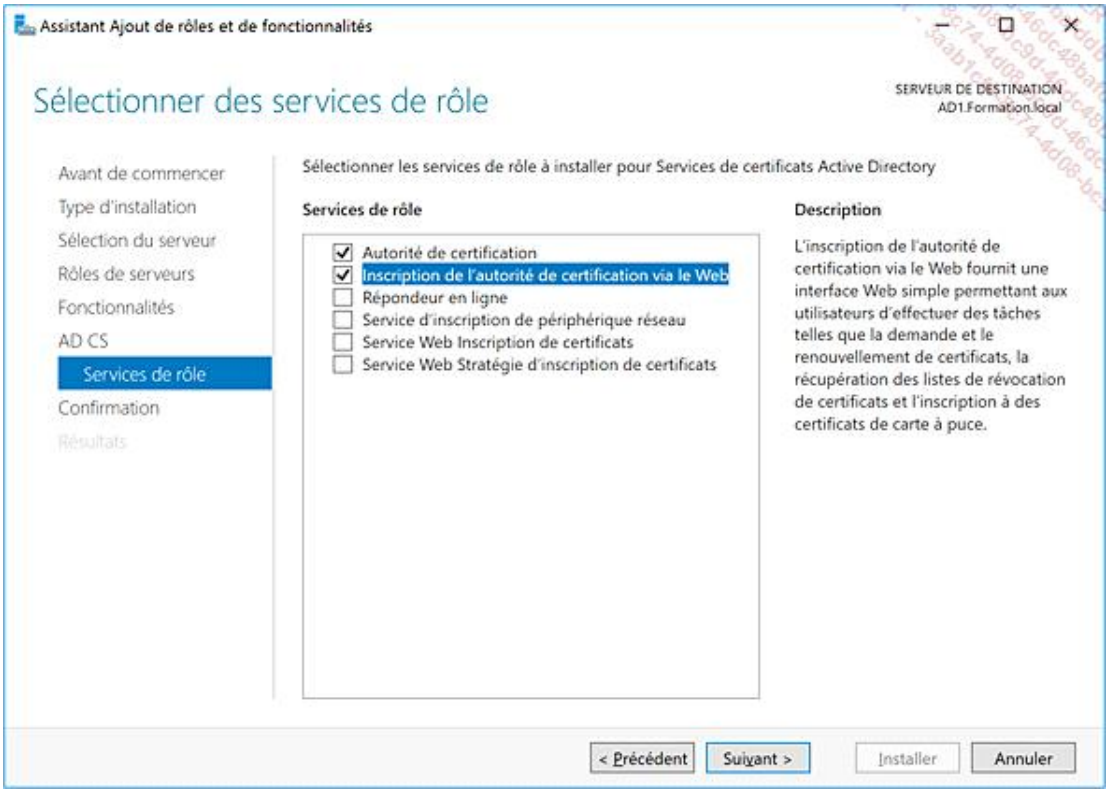
- Depuis la console Active Directory, créez un groupe de sécurité global nommée **All_Wsus_Servers**. Le nom de ce groupe n'a pas d'importance pour la suite de l'atelier.



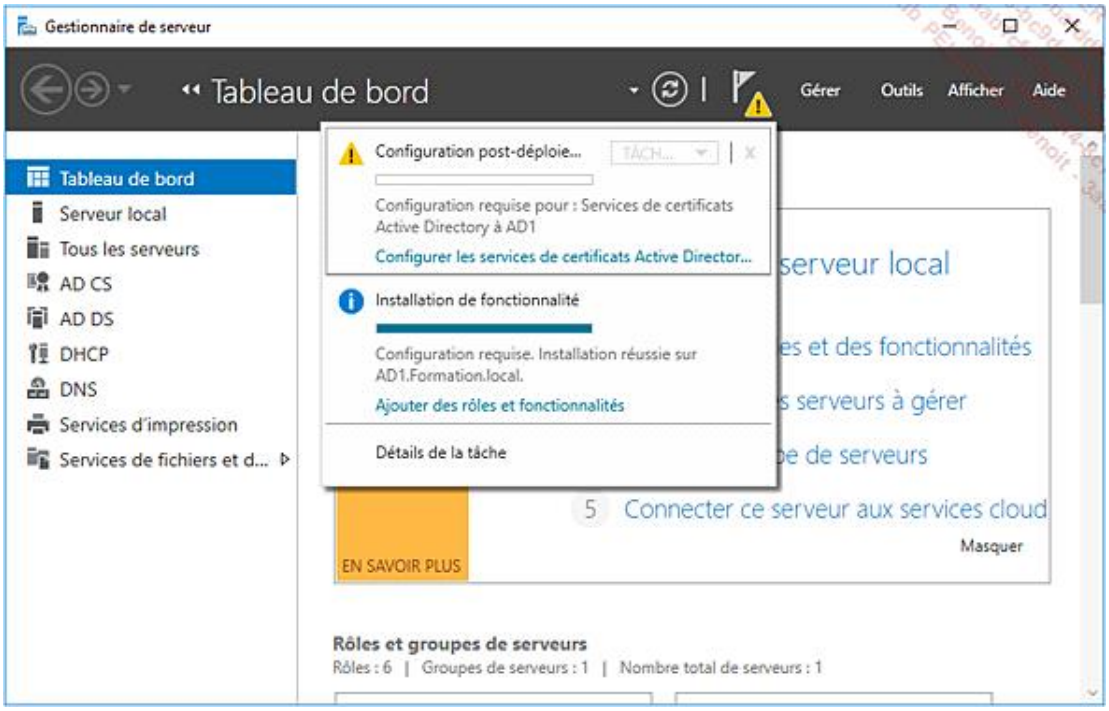
- Rajoutez SV1 en tant que membre de ce groupe.
- Sur le serveur AD1, ouvrez la console **Gestionnaire de serveur**.
- Ajoutez le rôle **Services de certificats Active Directory** puis cliquez sur **Suivant**.



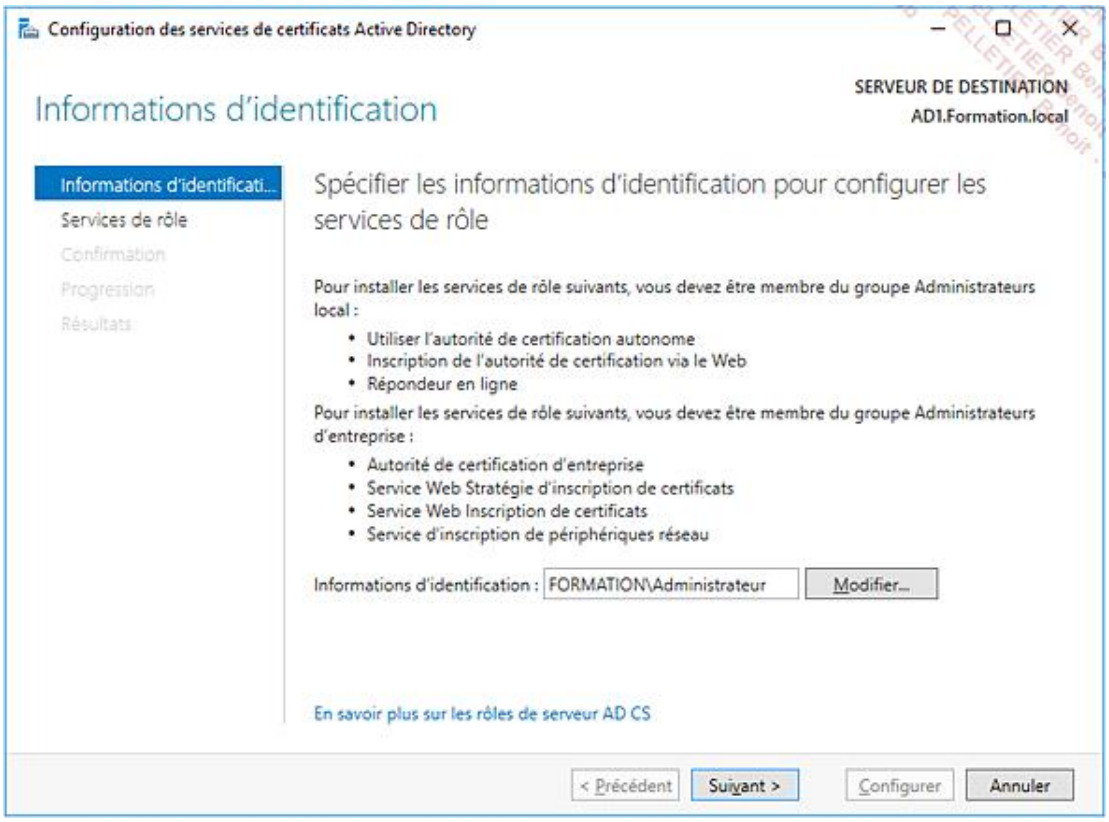
- Dans la fenêtre de sélection des services de rôle, cochez **Autorité de certification** et **Inscription de l'autorité de certification via le Web** puis cliquez sur **Suivant**.



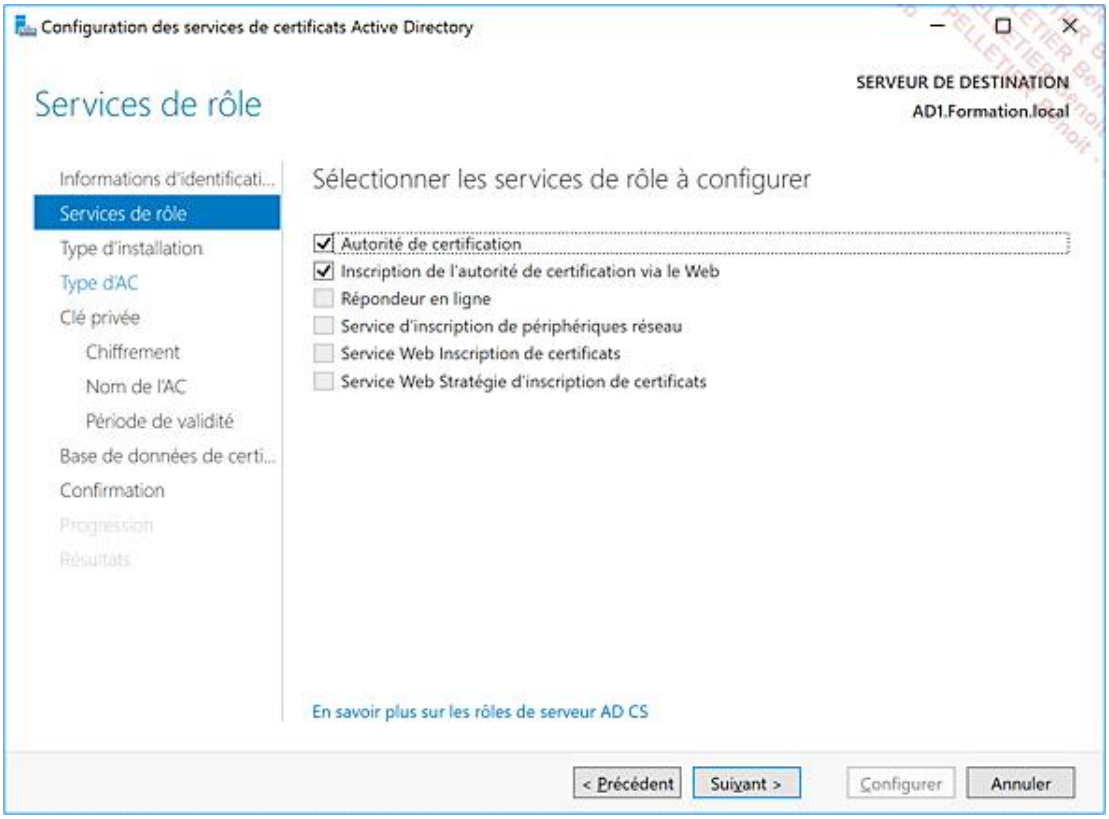
- Une fois l'installation réalisée, une nouvelle notification est présente dans la console **Gestionnaire de serveur**. Cliquez sur **Configurer les services de certificats Active Directory**.



- Dans la fenêtre **Informations d'identification**, cliquez sur **Suivant**.

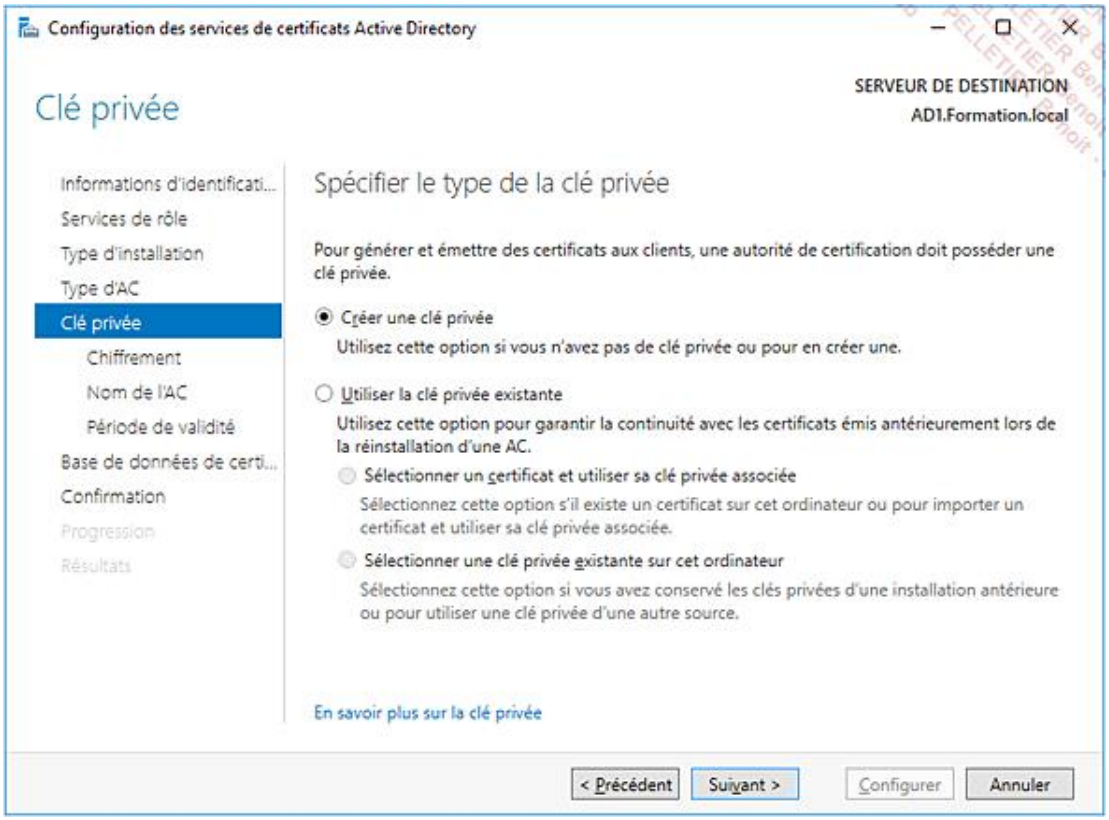


- Cochez **Autorité de certification** et **Inscription de l'autorité de certification via le Web** puis cliquez sur **Suivant**.

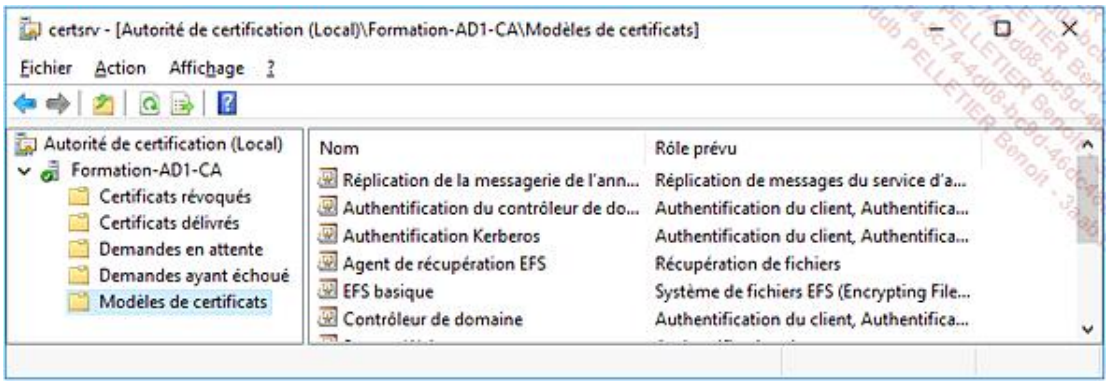


- Cliquez sur **Suivant** sans apporter de modification dans la fenêtre **Spécifier le type d'installation de l'AC** et **Spécifier le type de l'AC**.

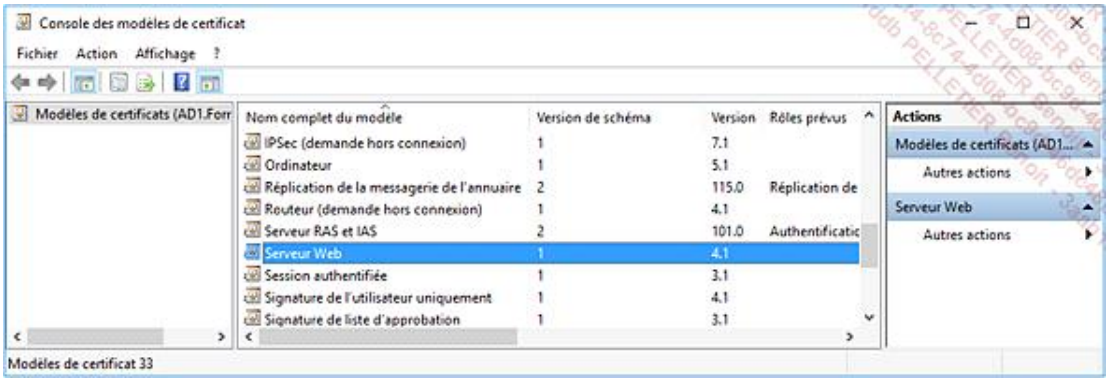
Une nouvelle clé va être générée, il n'est pas nécessaire d'apporter de modification à la fenêtre **Spécifier le type de la clé privée**.



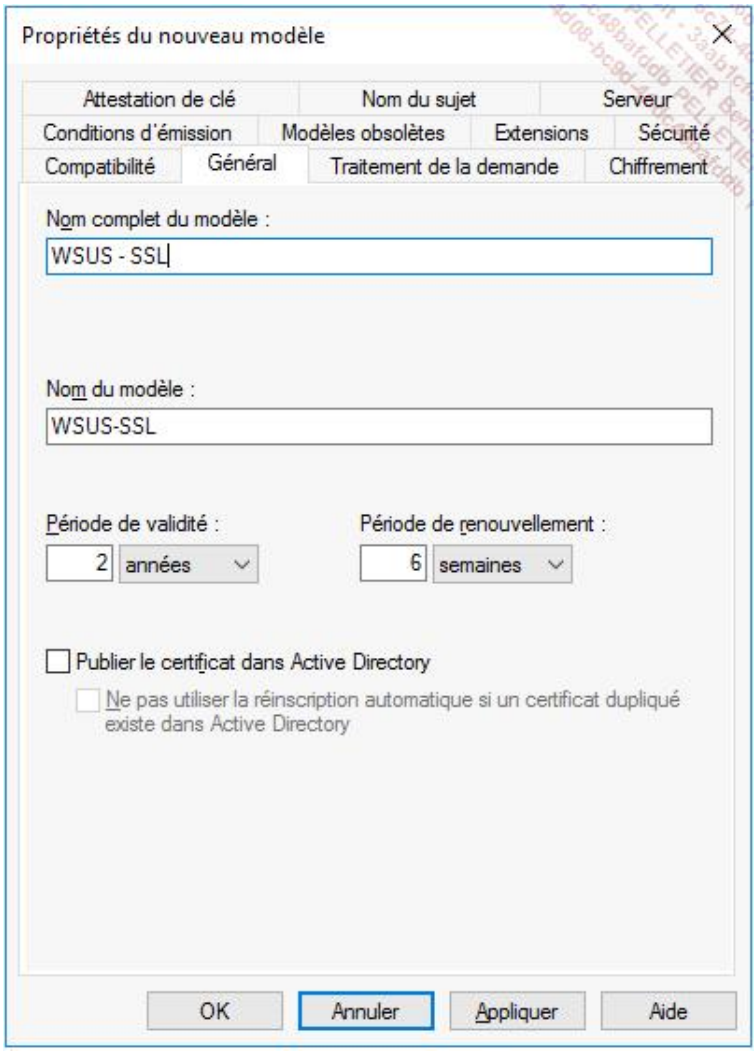
- Les fenêtres suivantes peuvent être validées sans apporter de modification. Par la suite, cliquez sur **Configurer**. Une fois l'opération de configuration terminée, cliquez sur **Fermer**.
- Ouvrez la console **Autorité de certification** depuis la liste déroulante **Outils** dans la console **Gestionnaire de serveur**.
- Déroulez le nœud **Formation-AD1-CA** puis effectuez un clic droit sur **Modèles de certificats**. Dans le menu contextuel, cliquez sur **Gérer**.



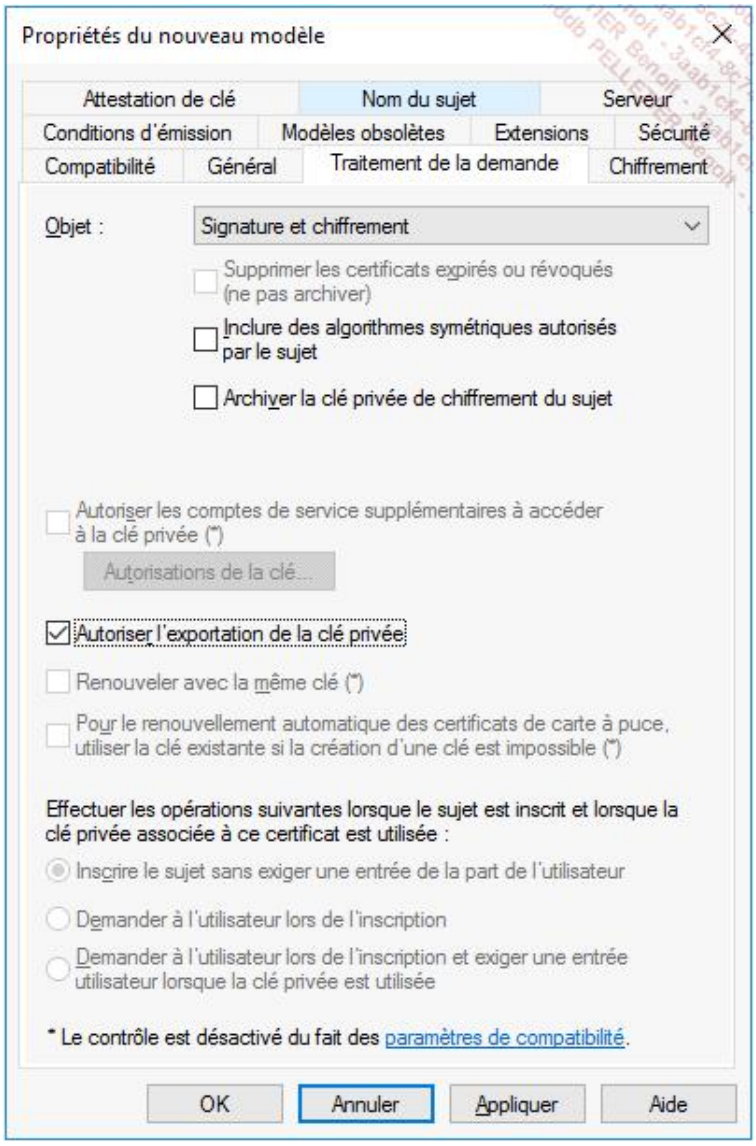
- Dans la console qui s'affiche, effectuez un clic droit sur **Serveur Web** puis sélectionnez **Dupliquer le modèle**.



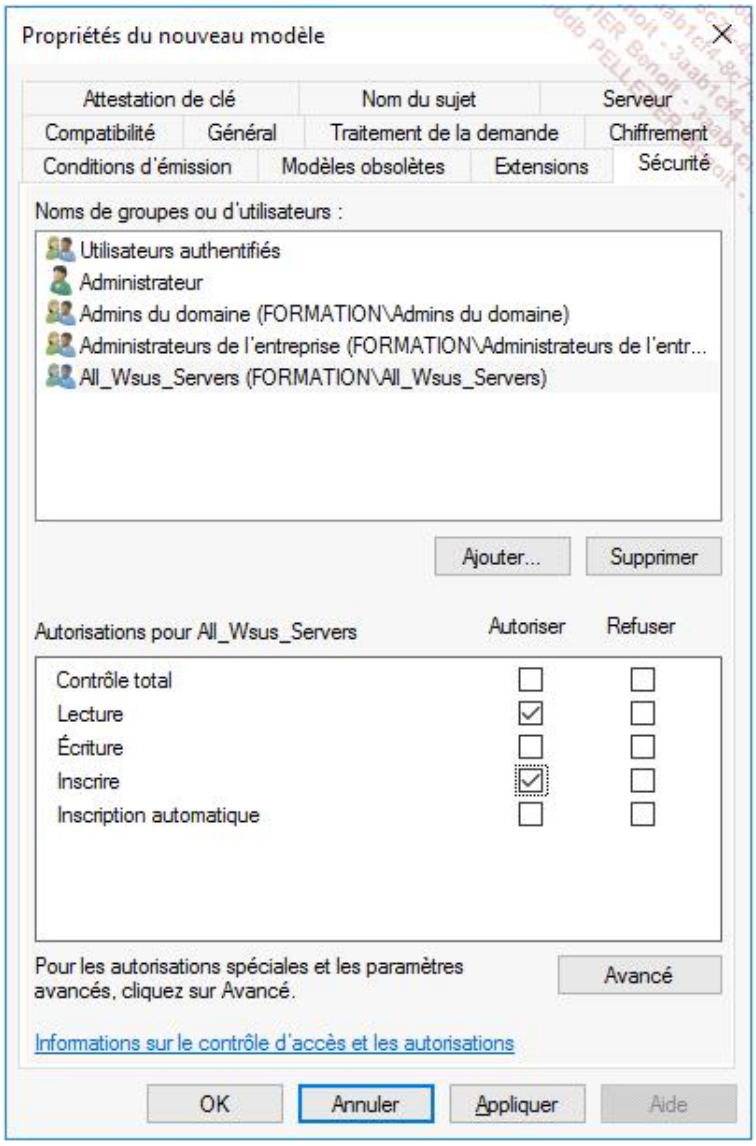
- Dans l'onglet **Général**, saisissez **WSUS - SSL** dans les champs **Nom complet du modèle** et **Nom du modèle**. Pour permettre un renouvellement plus aisée, il est nécessaire en production de cocher **Publier le certificat dans Active Directory**.



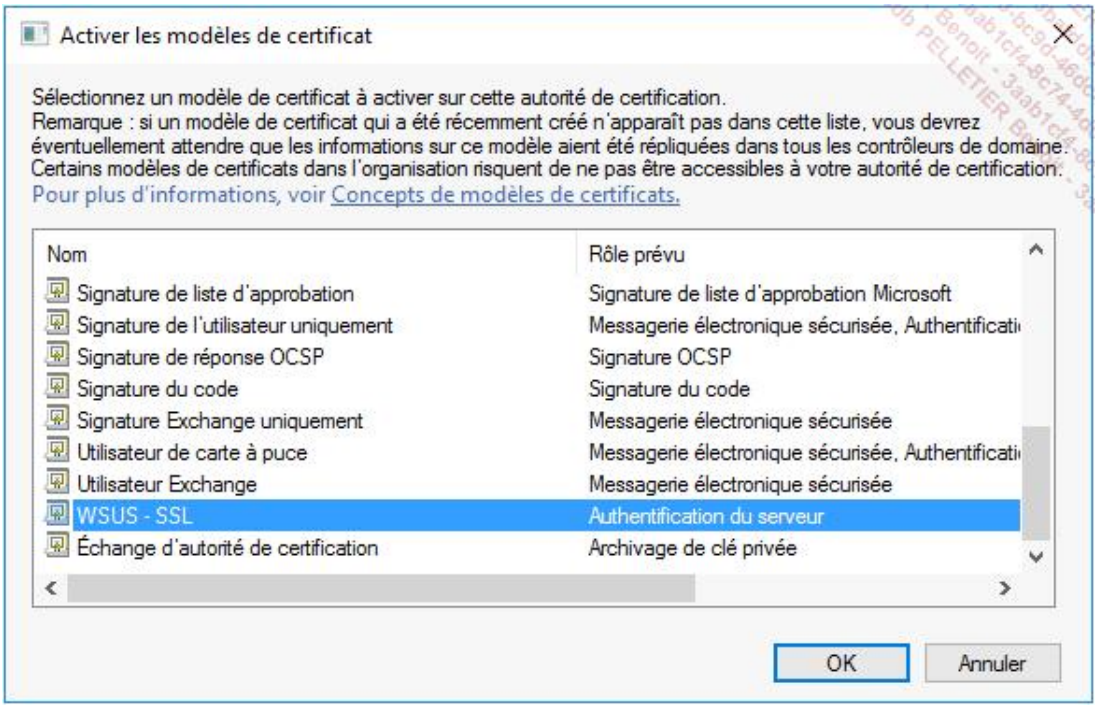
- Cliquez sur l'onglet **Traitement de la demande** puis cochez **Autoriser l'exportation de la clé privée**.



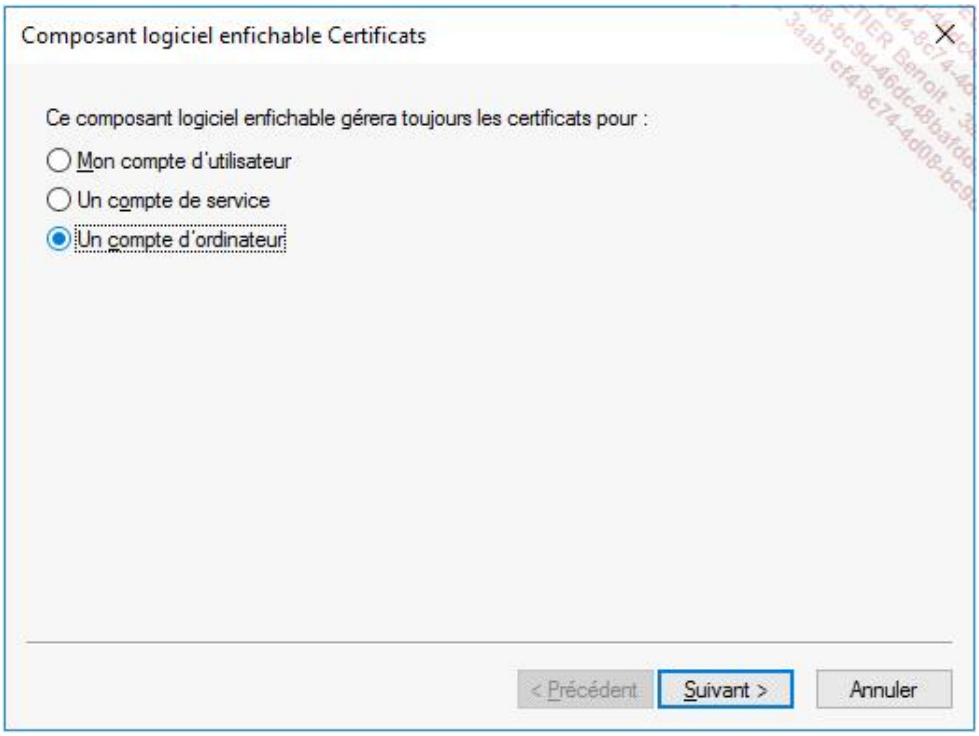
- Dans l'onglet **Sécurité**, attribuez au groupe **All_Wsus_Servers**, le droit **Inscrire**.



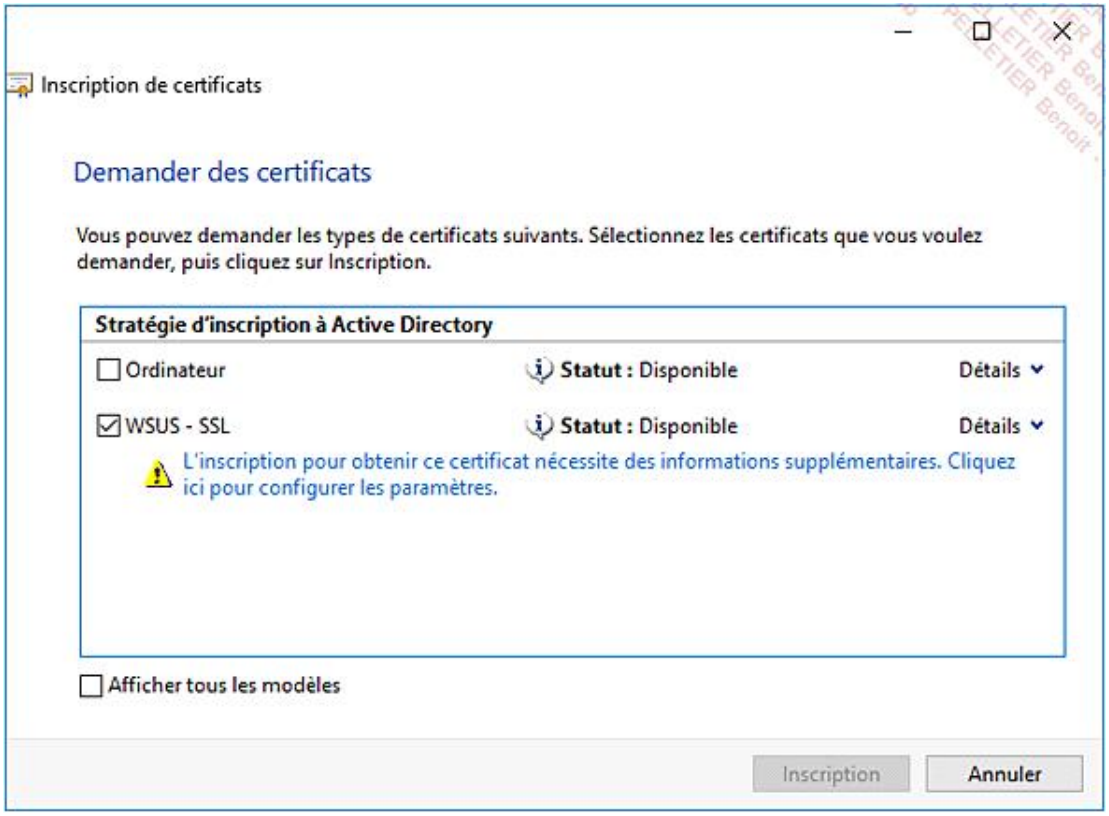
- Cliquez sur **OK** puis fermer la fenêtre **Console des modèles de certificats**.
- Dans la console **Autorité de certification**, effectuez un clic droit sur **Modèles de certificats**.
- Dans le menu contextuel, cliquez sur **Nouveau** puis **Modèle de certificat à délivrer**.
- Sélectionnez le certificat précédemment créé puis cliquez sur **OK**.



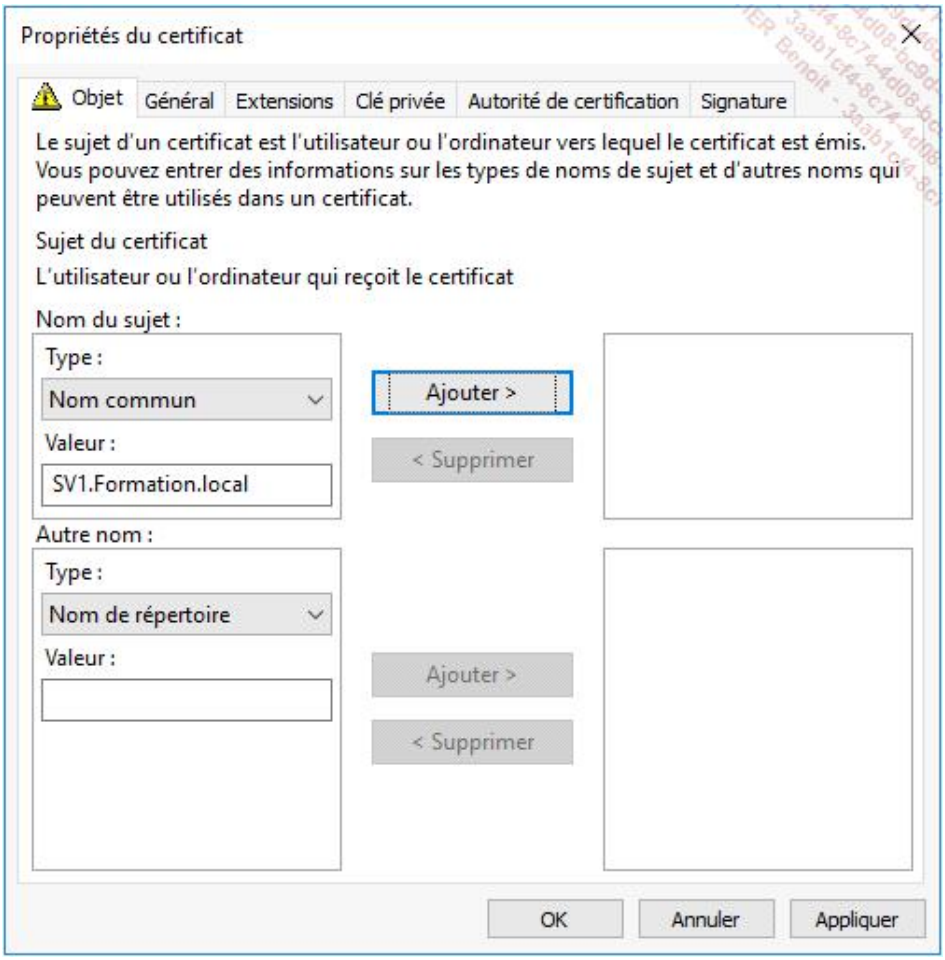
- Sur SV1, ouvrez une session en tant qu'administrateur du domaine puis lancez une console **MMC**.
- Ajoutez le snap-in **Certificats**, dans l'assistant sélectionnez **Un compte d'ordinateur**.



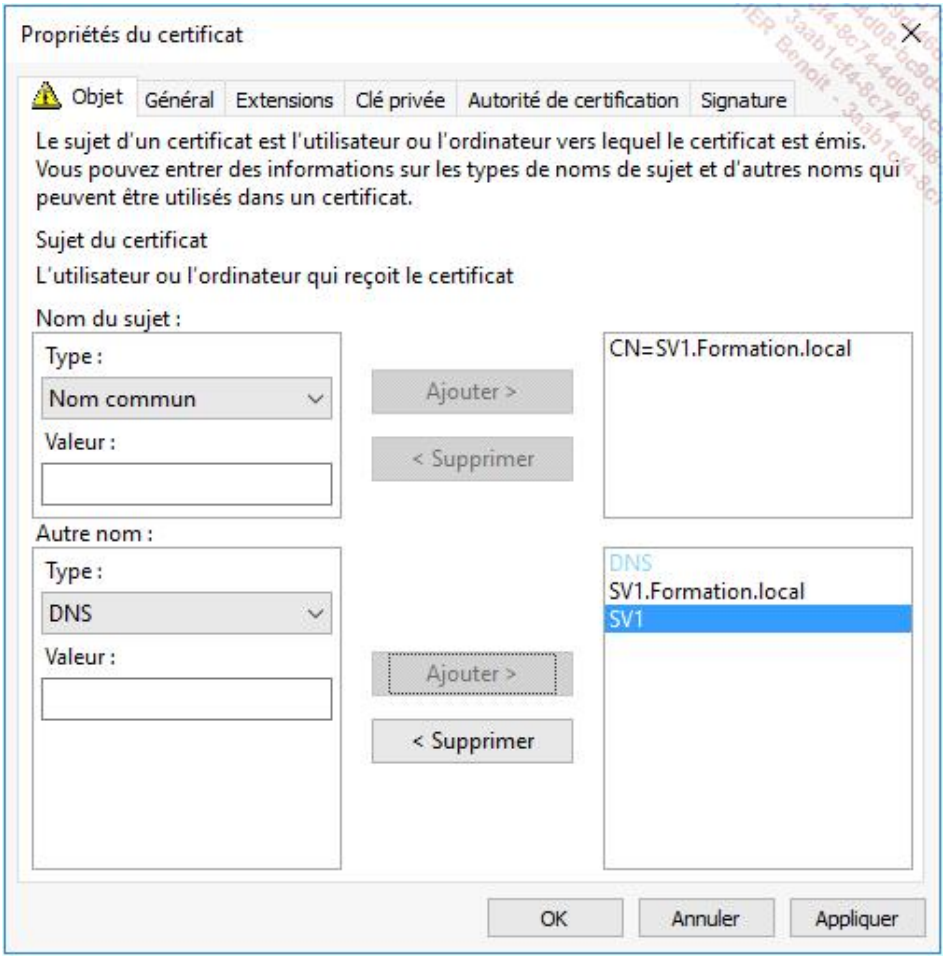
- Déroulez **Certificats (Ordinateur local)** puis cliquez sur le magasin **Personnel**.
- Effectuez un clic droit sur **Personnel** puis dans le menu contextuel sélectionnez **Toutes les tâches**, **Demander un nouveau certificat**.
- Cliquez sur **Suivant** dans les fenêtres **Avant de commencer** et **Sélectionner la stratégie d'inscription de certificat**.
- Cochez le certificat portant le nom WSUS - SSL. Pour valider la demande, il est nécessaire de cliquer sur le lien **L'inscription pour obtenir ce certificat nécessite des informations supplémentaires**.



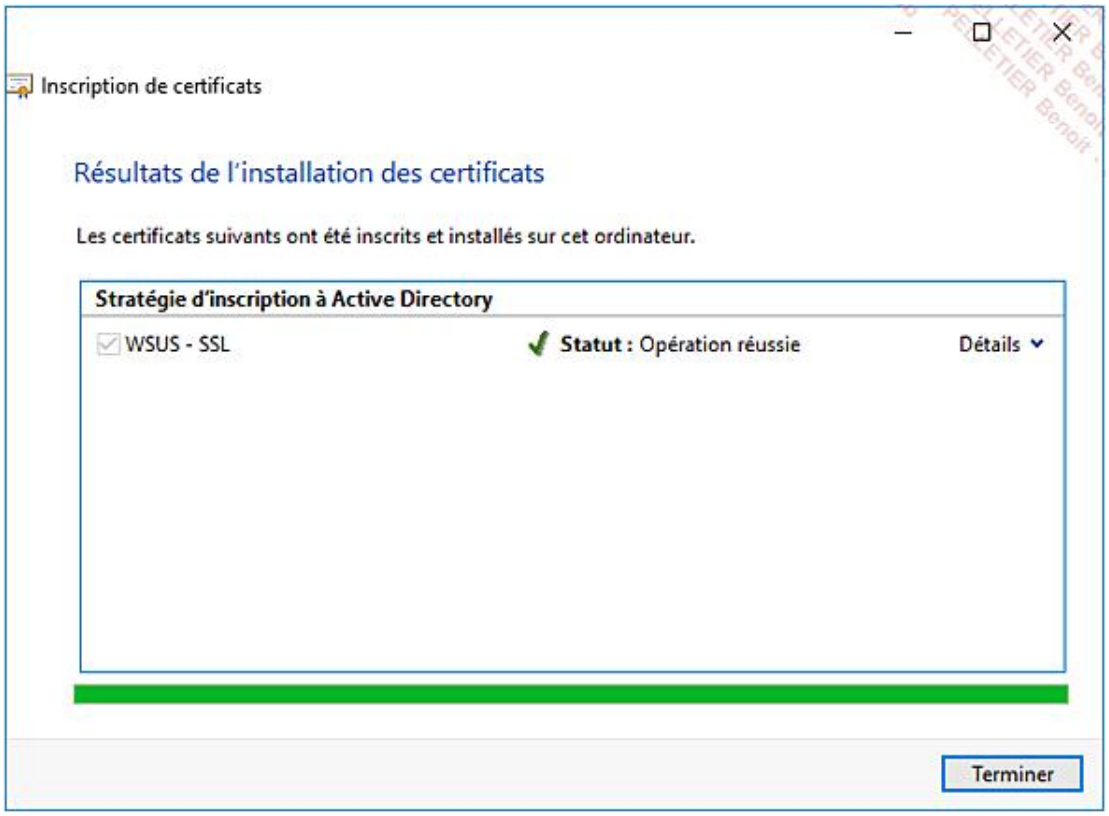
- Dans la liste déroulante **Type (Nom du sujet)** choisissez **Nom Commun**, saisissez **SV1.Formation.local** dans le champs **Valeur**. Validez le tout à l'aide du bouton **Ajouter**.



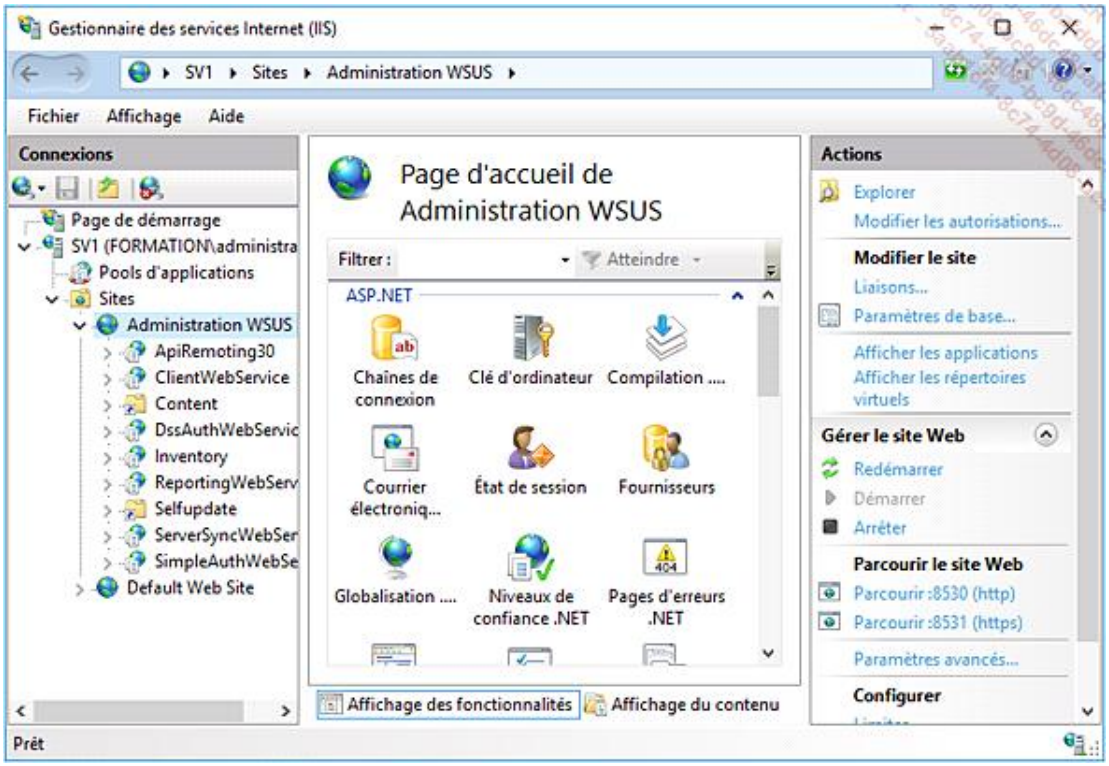
- Dans la liste déroulante **Type (Autre nom)** choisissez **DNS**, saisissez **SV1.Formation.local** dans le champ **Valeur**. Validez le tout à l'aide du bouton **Ajouter**. La même opération doit être effectuée pour la valeur **SV1**.



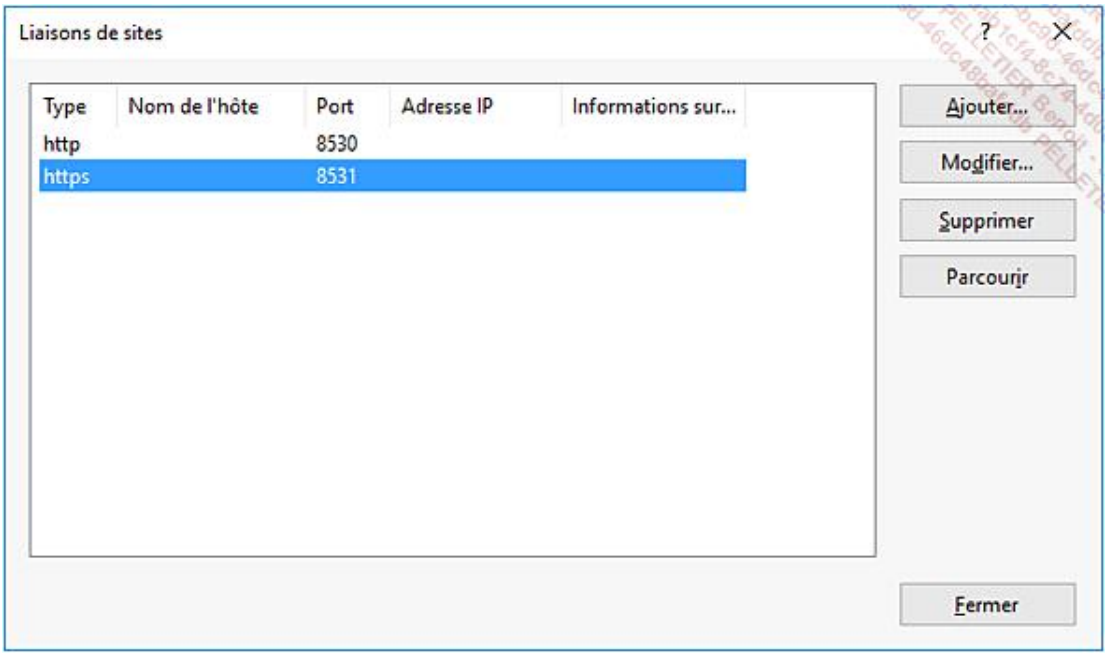
- Cliquez sur **OK** puis sur **Inscription** pour procéder à l'inscription.
- Une fois terminée, cliquez sur **Terminer**.



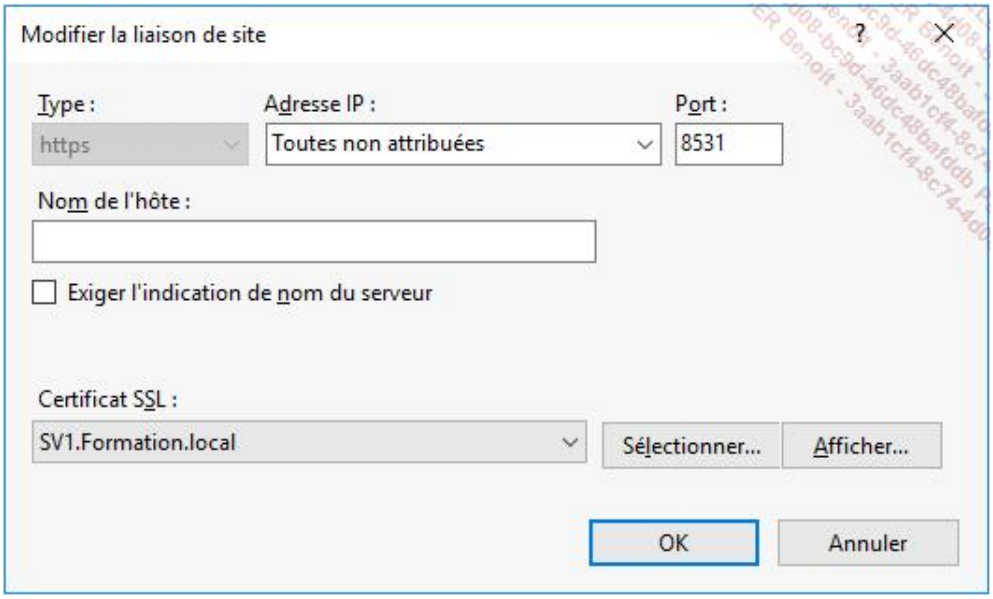
- Le serveur IIS peut désormais être configuré. Pour cela lancez la console sur le serveur SV1.
- Déroulez **SV1**, **Sites** puis **Administration WSUS**.



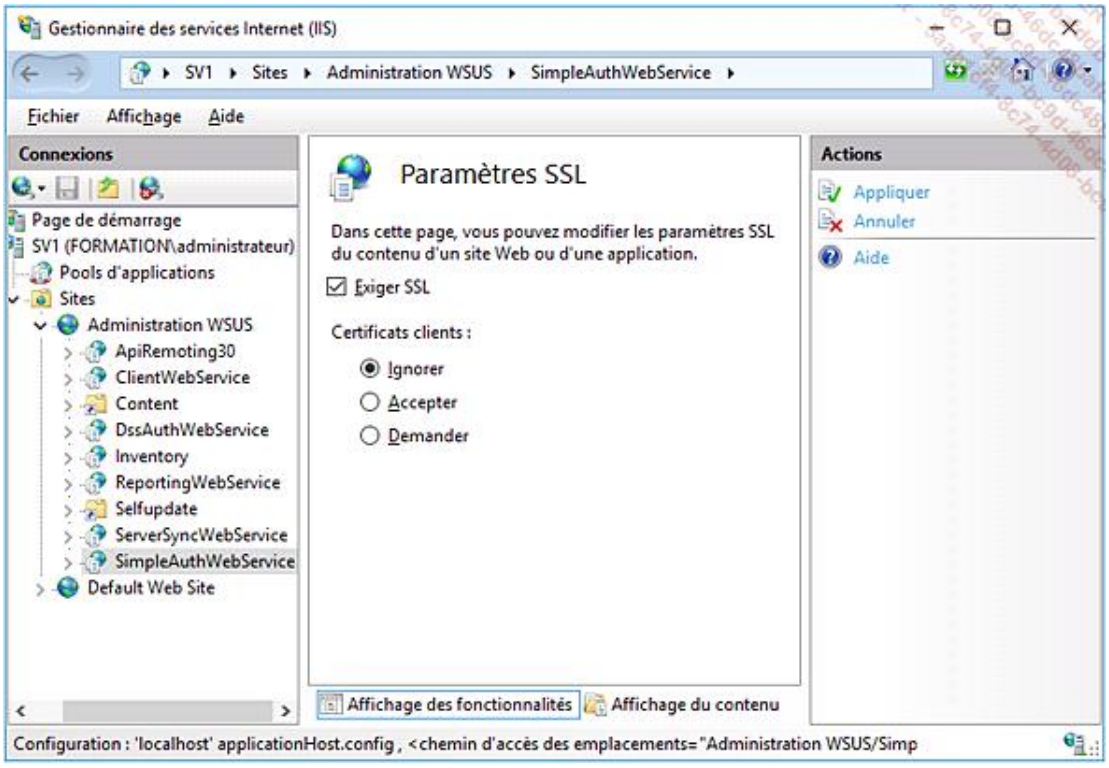
- Dans le menu **Actions**, cliquez sur **Liaisons**.
- Sélectionnez la ligne **https** puis cliquez sur **Modifier**.



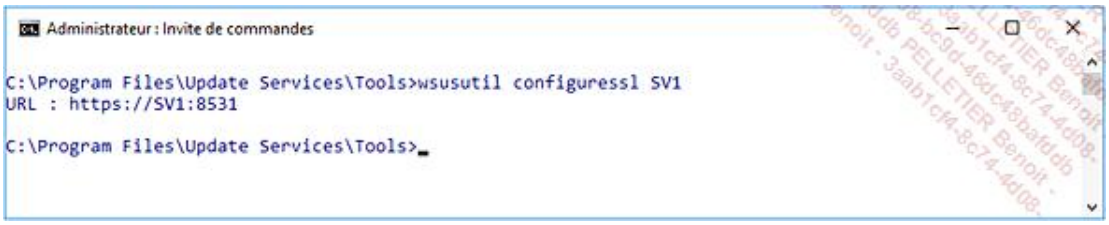
- Sélectionnez dans la liste déroulante le certificat précédemment généré.



- Cliquez sur **OK** puis sur **Fermer**.
- Le protocole SSL peut maintenant être activé sur les dossiers WSUS. Pour cela, cliquez sur l'application **SimpleAuthWebService** puis dans le panneau central, cliquez sur **Paramètres SSL**. Sélectionnez les options **Exiger SSL** puis **Ignorer**.

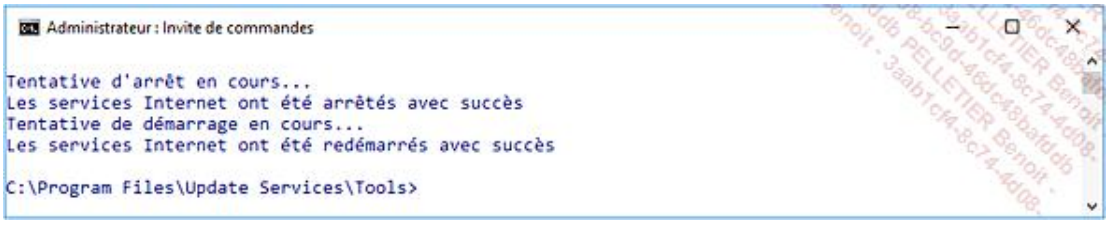


- Cliquez sur **Appliquer** puis effectuez la même opération pour les répertoires suivants :
  - ServerSyncWebService
  - DssAuthWebService
  - ClientWebService
  - ApiRemoting30
- Ouvrez une invite de commandes DOS puis accédez aux répertoires C:\Program Files\Update Services\Tools. Exécutez par la suite la commande `wsusutil configuressl SV1`.



Le protocole SSL est maintenant activé.

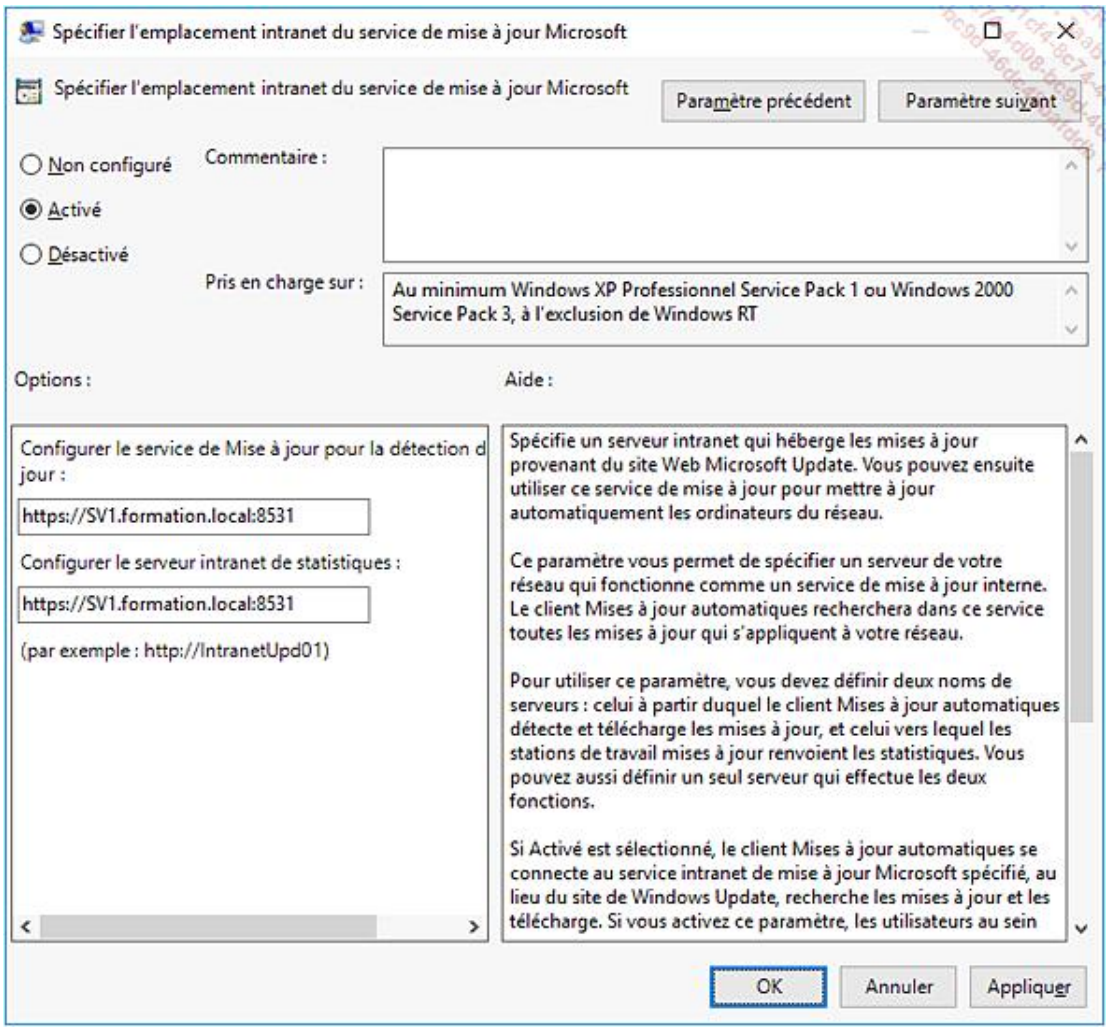
- Saisissez la commande `iisreset /noforce` afin de redémarrer les services IIS.



- Redémarrez le serveur puis exécutez la commande `wsusutil checkhealth`. L'événement avec l'ID

1000 doit s'afficher.

Il est maintenant nécessaire de modifier les stratégies de groupe afin de configurer les clients pour qu'ils utilisent l'URL https://SV1.Formation.local:8531.



Les communications du serveur WSUS sont maintenant chiffrés.

6. Gestion des builds Windows 10 avec WSUS

Avec Windows 10, une nouvelle gestion des "versions majeures" est apparue. Microsoft a mis en place une gestion par branche.

Ainsi, lors de la validation d'une nouvelle build, celle-ci est positionnée dans la branche Semi-Annual Channel. Les différents postes de travail Windows 10 peuvent alors la récupérer et l'installer. Pour les entreprises utilisant WSUS ou SCCM, il est possible de retarder de quelques semaines/mois cette installation. Il est important de noter que Microsoft ne supportera plus les anciennes builds, il est donc recommandé de ne pas sauter plus de deux build (chaque build a une durée de validité de 18 mois suite à sa publication).

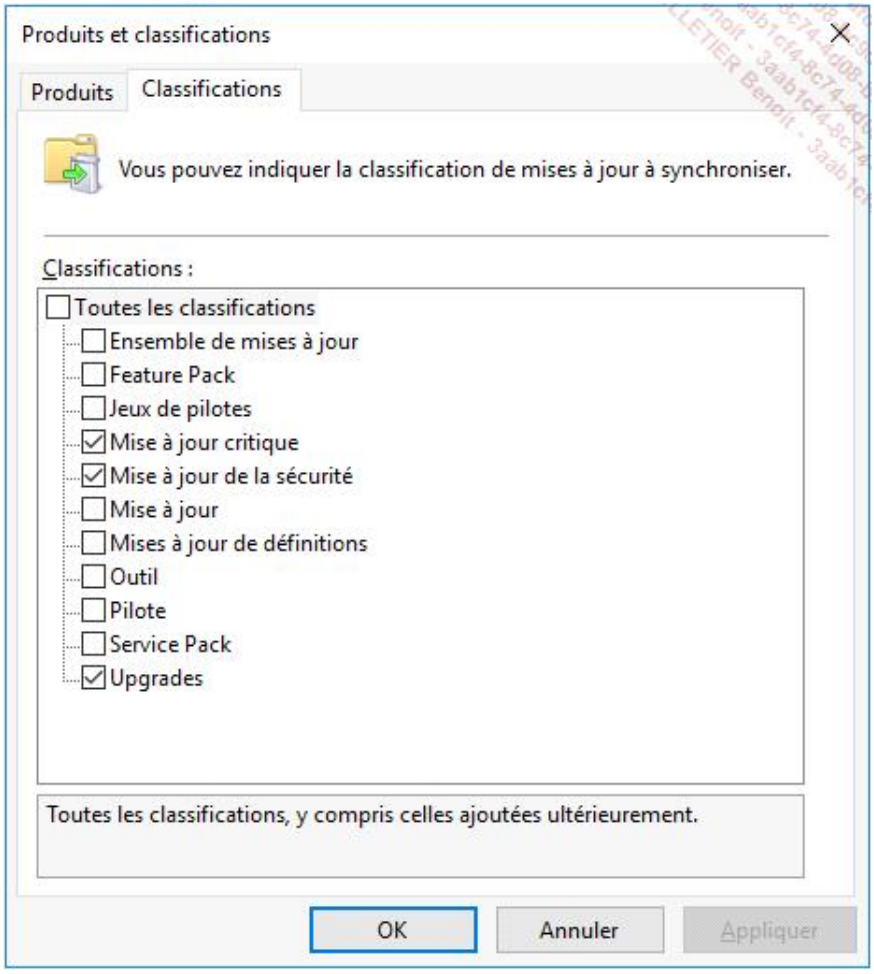
Pour cela, il est possible de distribuer ces builds par l'intermédiaire de WSUS. Néanmoins cela ne peut être effectué qu'en respectant les prérequis suivants :

- WSUS sous 2012/2012 R2 ainsi que l'installation de la KB 3095113 et KB3159706.

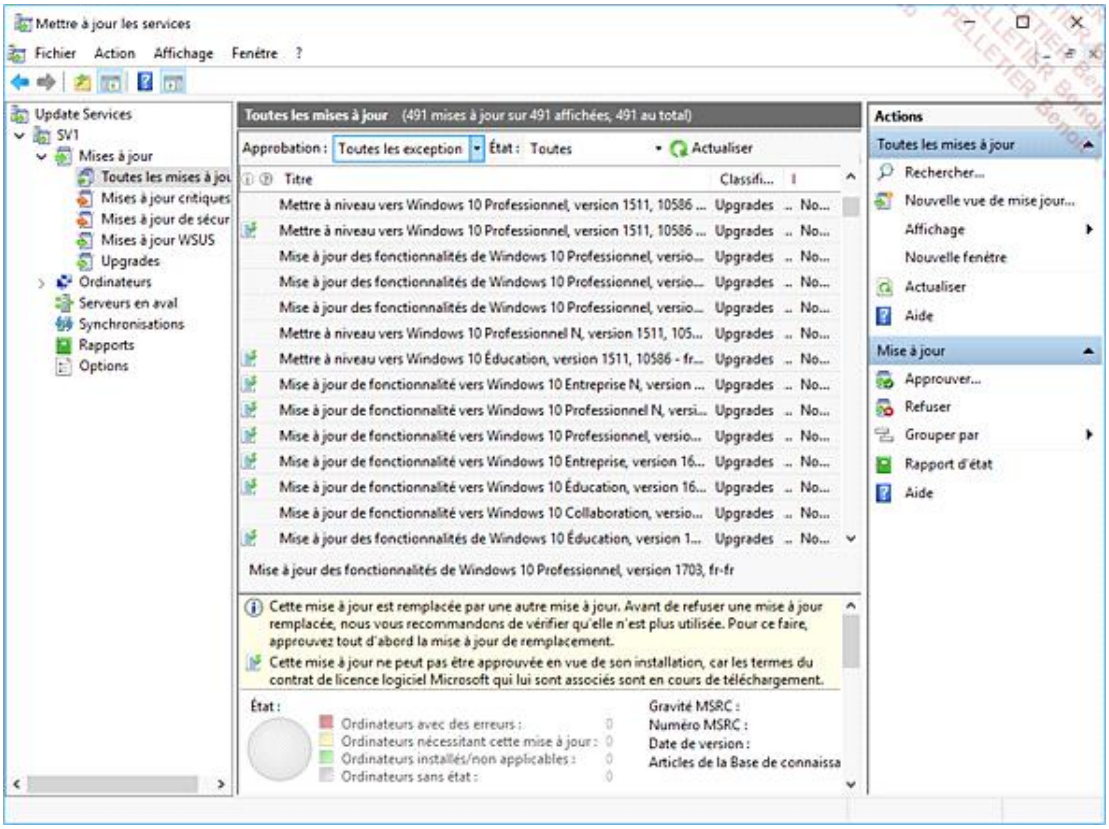
- WSUS sous Windows Server 2016.

WSUS 3.0 (Windows Server 2008 R2) n'est pas supportée.

Une nouvelle catégorie est présente dans **Classifications**, nommée **Upgrades**. Elle permet de récupérer et déployer les différentes builds Windows 10.



Après avoir procédé à la synchronisation du serveur WSUS, les différentes Upgrades apparaissent dans WSUS.



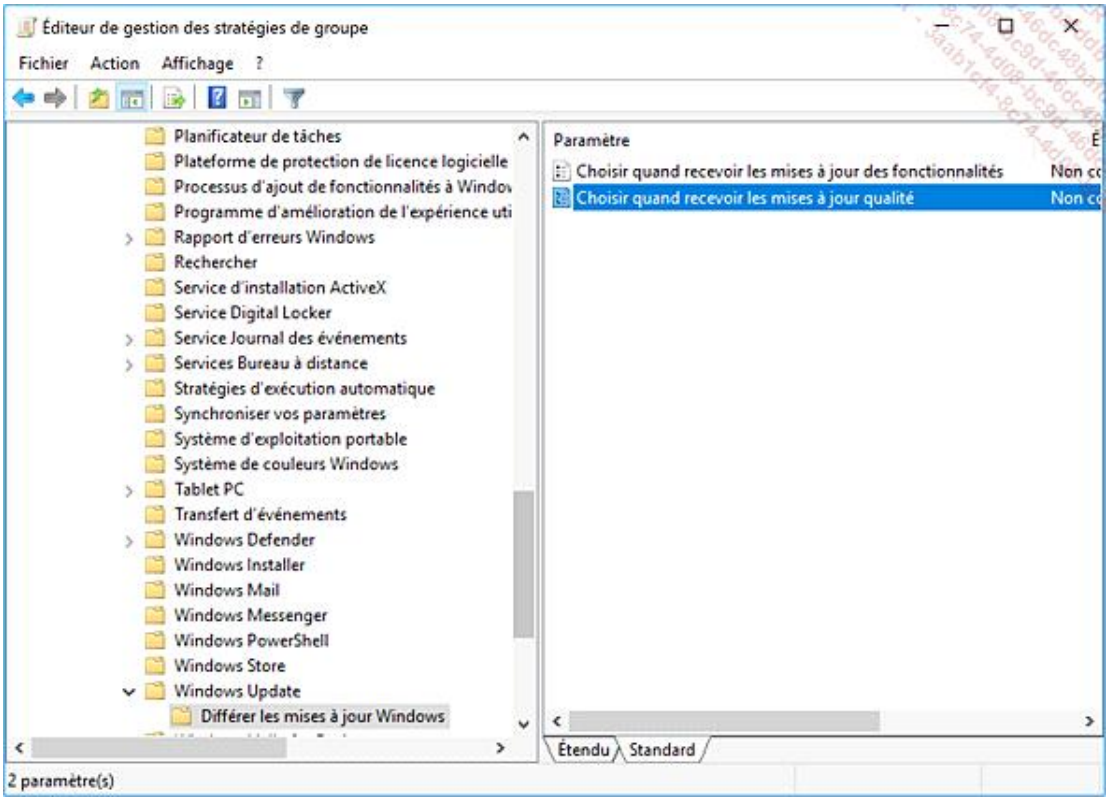
Le déploiement s'effectue comme toute mise à jour en l'approuvant sur un groupe d'ordinateurs.

Windows for Business

Dans le cas où le poste Windows 10 n'utilise pas WSUS pour se mettre à jour, il est possible d'utiliser Windows for Business. Cette fonctionnalité permet le paramétrage du client Windows update afin de retarder l'installation d'une nouvelle build ou de mise à jour.

Cela s'opère par l'intermédiaire d'une stratégie de groupe :

- Chemin du paramètre : **Configuration ordinateur - Modèles d'administration - Composants Windows - Windows Update - Différer les mises à jour Windows**.
- Nom du paramètre : **Choisir quand recevoir les mises à jour qualité** et **Choisir quand recevoir les mises à jour des fonctionnalités**.



Il est ainsi plus aisé de gérer l'installation des différentes builds et autres mises à jour si le poste n'est pas intégré à une infrastructure WSUS.

Les rapports dans WSUS

Le nœud **Rapports** permet la création et l'affichage de rapports permettant la gestion du serveur. Les informations sur les mises à jour, les ordinateurs et les synchronisations peuvent être analysées à l'aide des rapports.

Néanmoins, pour profiter de cette fonctionnalité, le composant **Report Viewer** doit être installé sur le poste.



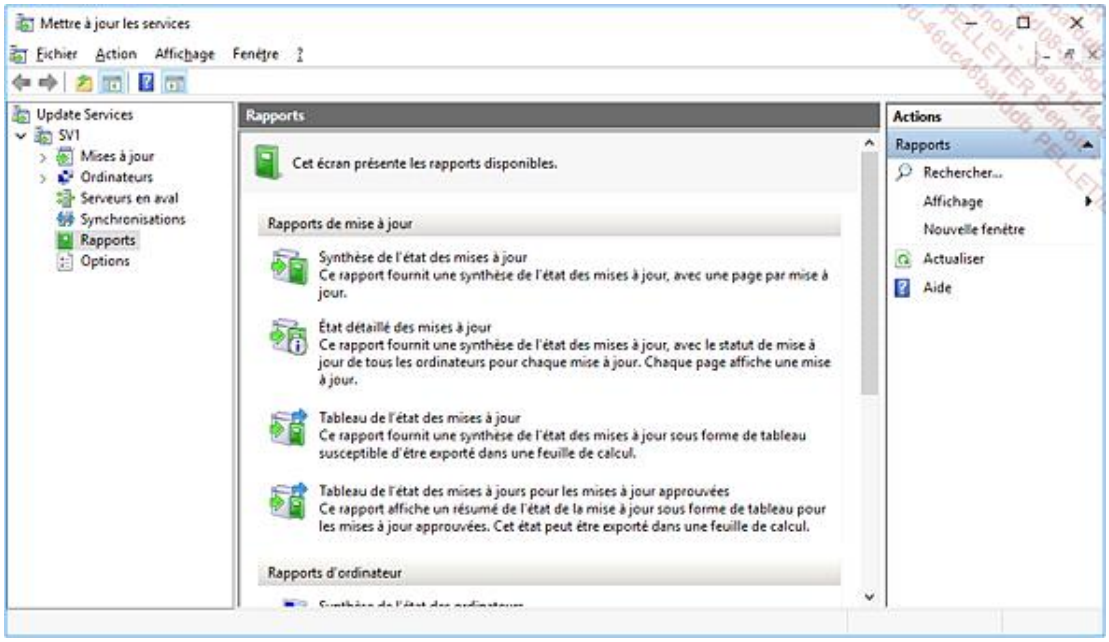
Il est nécessaire d'installer la fonctionnalité **.NET Framework 3.5** si cela n'est pas déjà fait. Si l'installation échoue, spécifiez une source alternative lors de l'installation et indiquez le chemin suivant : D:\sources\sxs, D: étant la lettre du lecteur DVD. L'installation de Report Viewer 2012 nécessite également l'installation de SQL 2012 Feature Pack.

- Pour installer **SQL 2012 Feature Pack**, rendez-vous à l'adresse :http://www.microsoft.com/en-us/download/details.aspx?id=29065
- Développez le nœud **Install Instructions** puis téléchargez le composant **Microsoft System CLR Types pour Microsoft SQL Server 2012**.



L'installation de Report Viewer peut maintenant être effectuée.

- Cliquez sur le nœud **Rapports**.



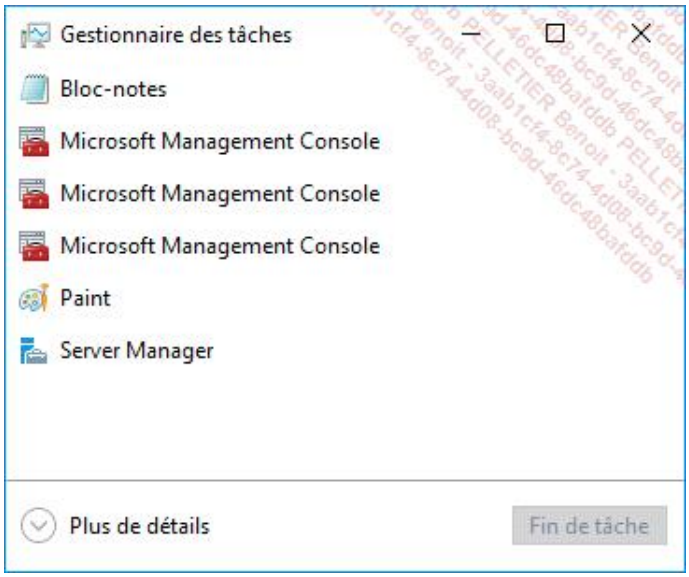
Plusieurs types de rapports concernant les mises à jour, les ordinateurs ou les synchronisations peuvent être utilisés.

Gestionnaire des tâches

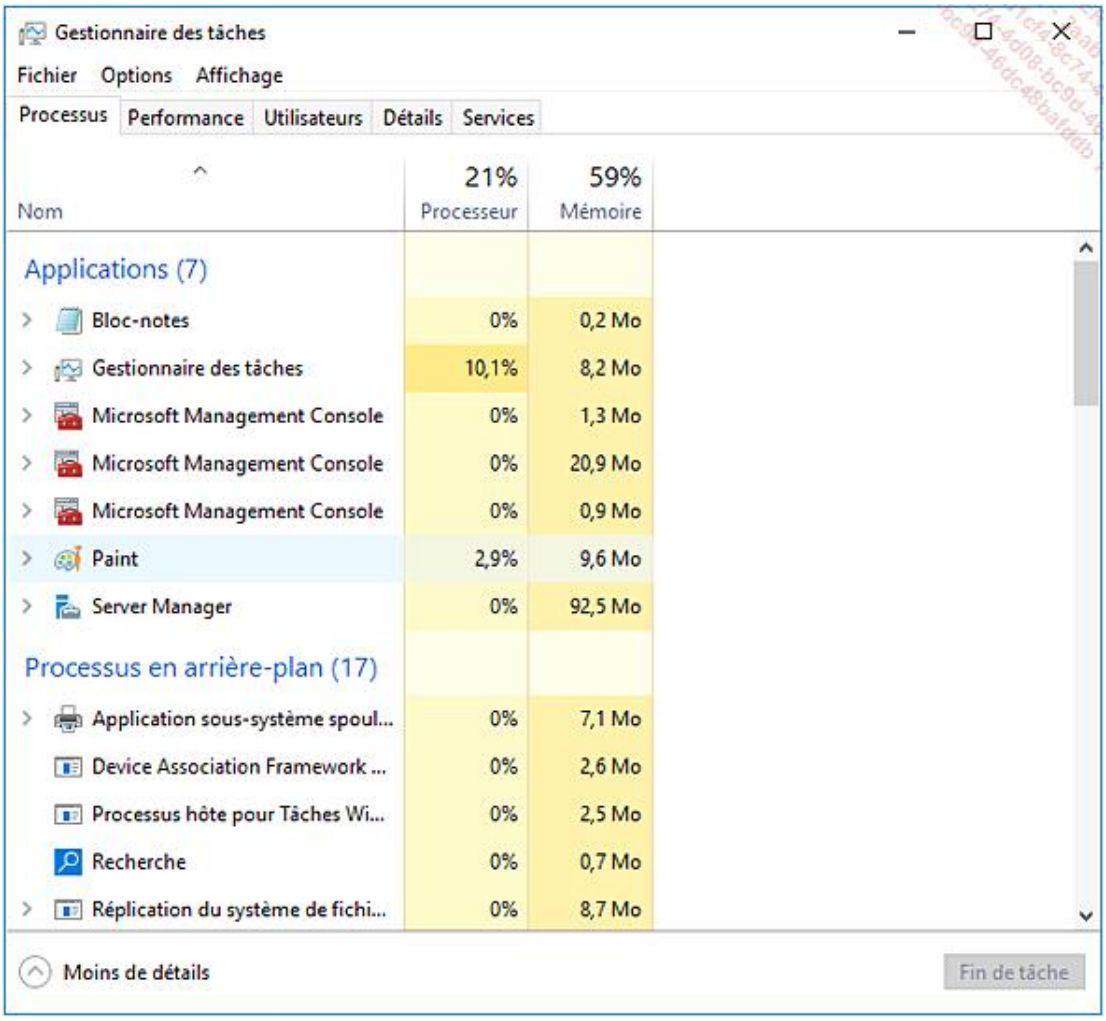
Le **Gestionnaire des tâches** offre à l'utilisateur plusieurs fonctionnalités (fermer des applications, fournir des informations sur les processus, effectuer une opération sur un service…). Depuis Windows Server 2012 R2, le gestionnaire a été optimisé afin de répondre à plusieurs scénarios :

- **Arrêter un processus de manière rapide et efficace** : l'ergonomie de la console a été modifiée afin de proposer une vue plus claire des différents processus actifs de l'utilisateur. L'opération visant à arrêter une application ou autres a été également simplifiée. Un simple clic sur le bouton **Fin de tâche** arrête le processus.

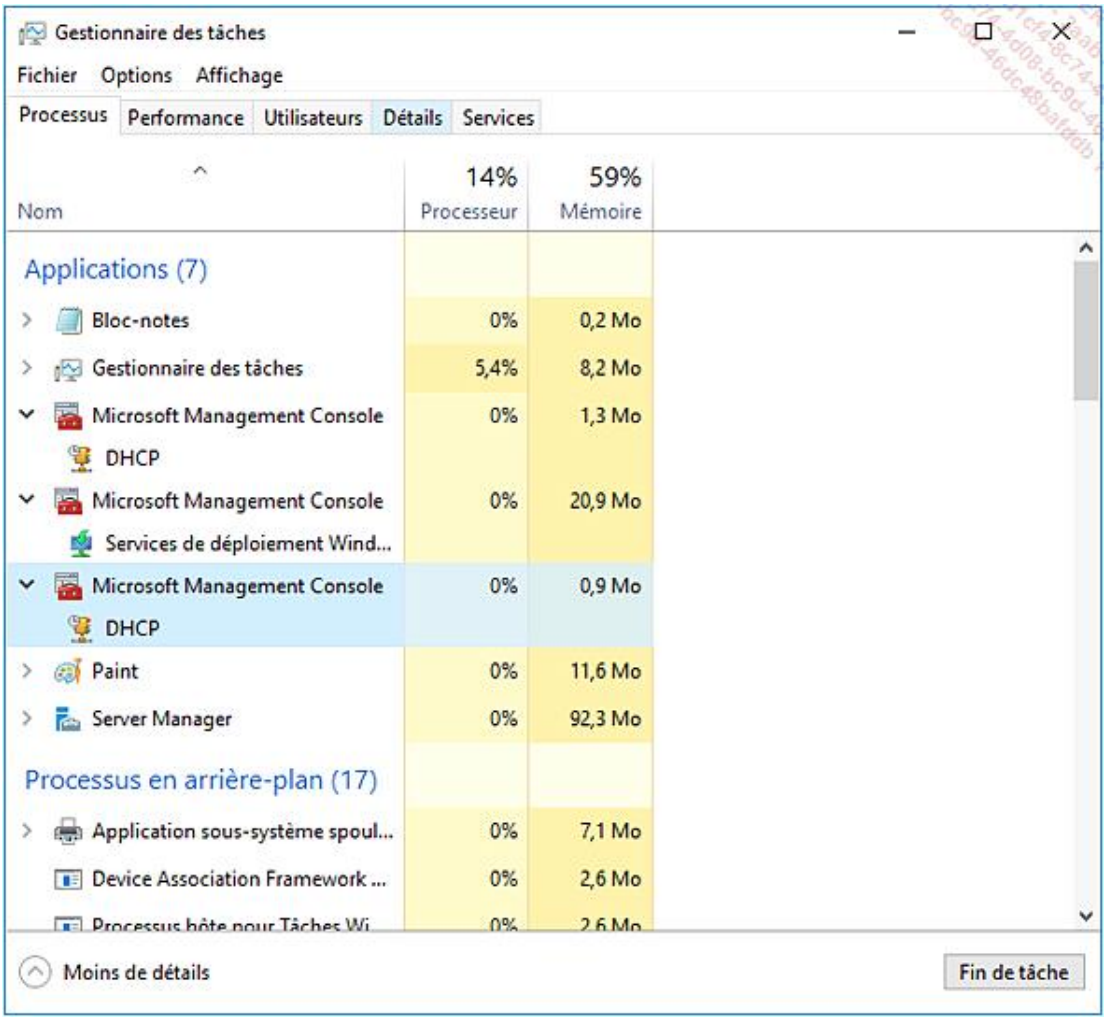
  Une vue plus détaillée peut également être activée à l'aide du bouton **Plus de détails**.



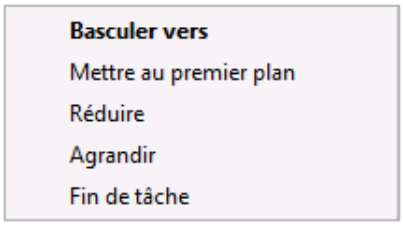
- **Diagnostiquer un problème de performance** : en activant la vue **Plus de détails**, les différentes fenêtres du gestionnaire des tâches apparaissent. Il est plus aisé pour un utilisateur averti de diagnostiquer un problème de performance. Il est possible de voir très rapidement l'utilisation totale du processeur et de la mémoire. Ces valeurs en pourcentage donnent une première indication sur un problème potentiel. Il est par la suite intéressant d'examiner en détail chaque processus.



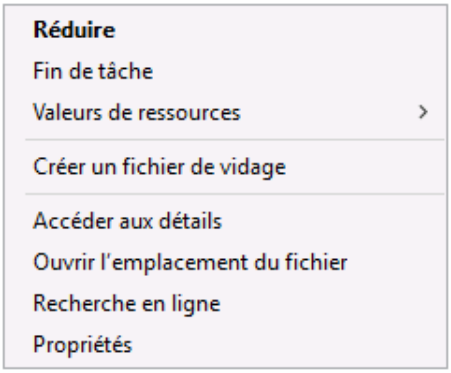
Il est possible de développer chaque entrée en cliquant sur la petite flèche à gauche de chaque ligne. On peut voir à quelles applications appartient le processus. Ainsi, si **Microsoft Management Console** est développé, les noms des différents logiciels enfichables présents dans chaque console s'affichent.



Un clic droit sur **Services de déploiement Windows** donne accès à un menu contextuel qui, en plus de proposer l'action **Fin de tâches**, permet également la réduction/agrandissement de la console ou sa mise au premier plan.

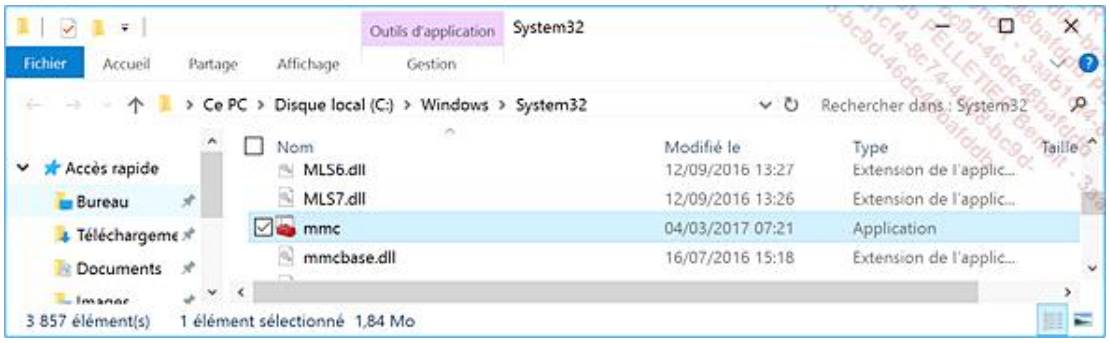


En cliquant cette fois sur **Microsoft Management Console**, d'autres options sont disponibles.

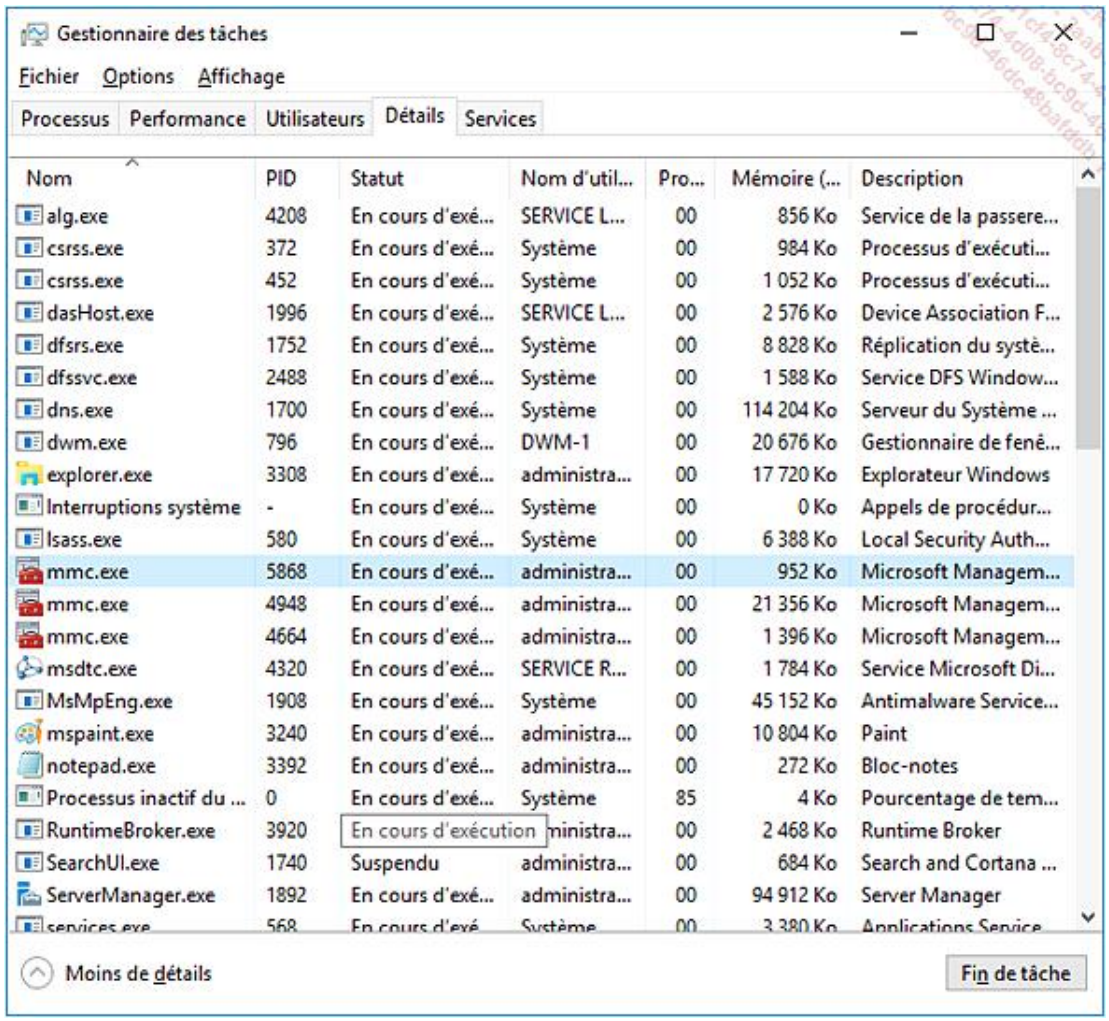


Il est ainsi possible de faire une recherche en ligne. Cette fonctionnalité peut être très utile si vous souhaitez obtenir des informations sur un processus présent dans la console. L'option **Valeurs de ressources** permet quant à elle de changer l'unité de la colonne **Mémoire** afin d'afficher des pourcentages à la place de valeurs et inversement.

L'exécutable peut être stocké dans n'importe quel dossier de votre système de fichiers. Afin de pouvoir accéder au répertoire contenant l'exécutable du processus sans effectuer de recherche, choisissez l'option **Ouvrir l'emplacement du fichier**. Le dossier contenant le fichier s'affiche.



Il est dans certains cas nécessaire d'avoir plus d'informations sur un processus. Pour cela, cliquez sur **Accéder aux détails**. L'onglet **Détails** s'affiche et le processus en question est sélectionné.

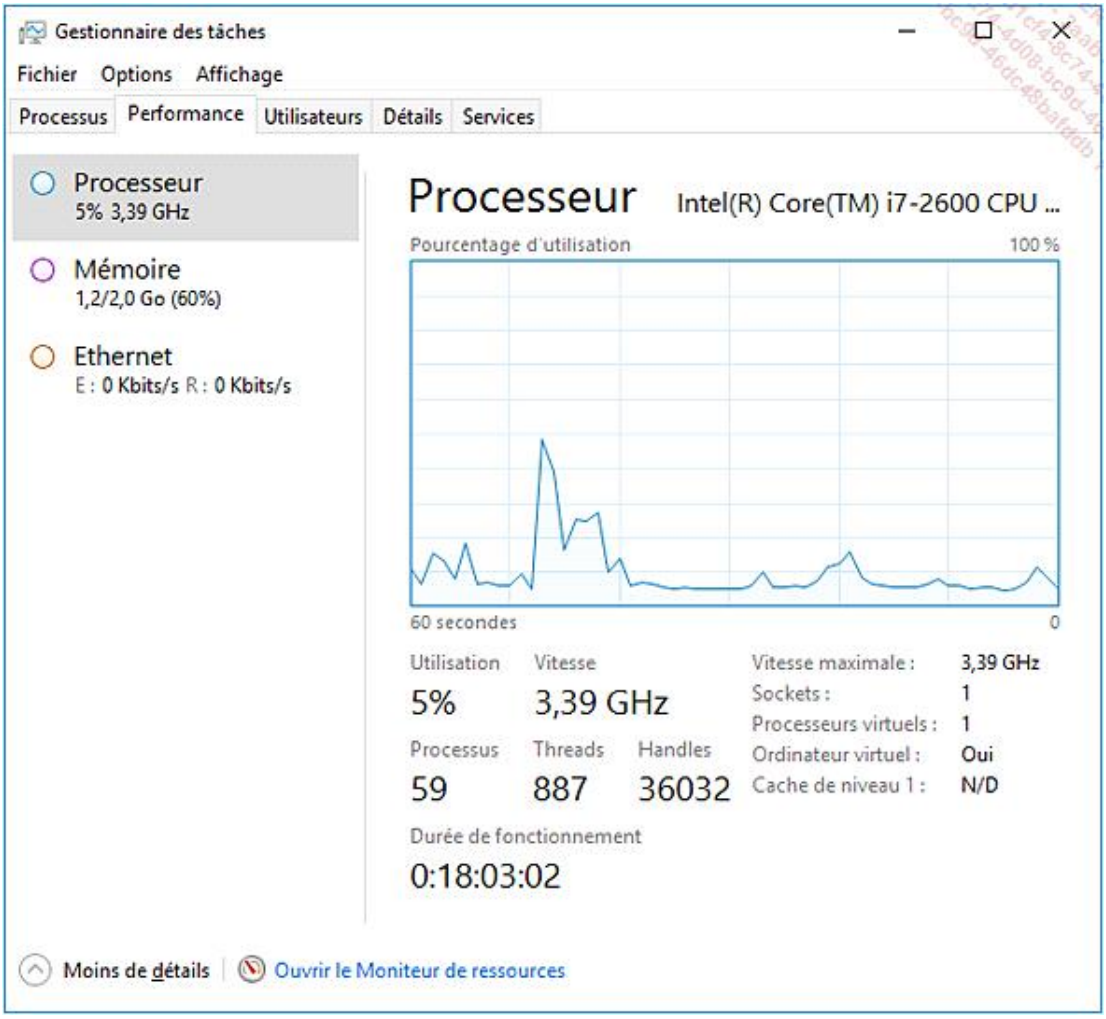


Cette vue donne accès au nom du fichier exécutable mais également à l'ID du processus (**PID**) ainsi qu'à son **Statut**. -

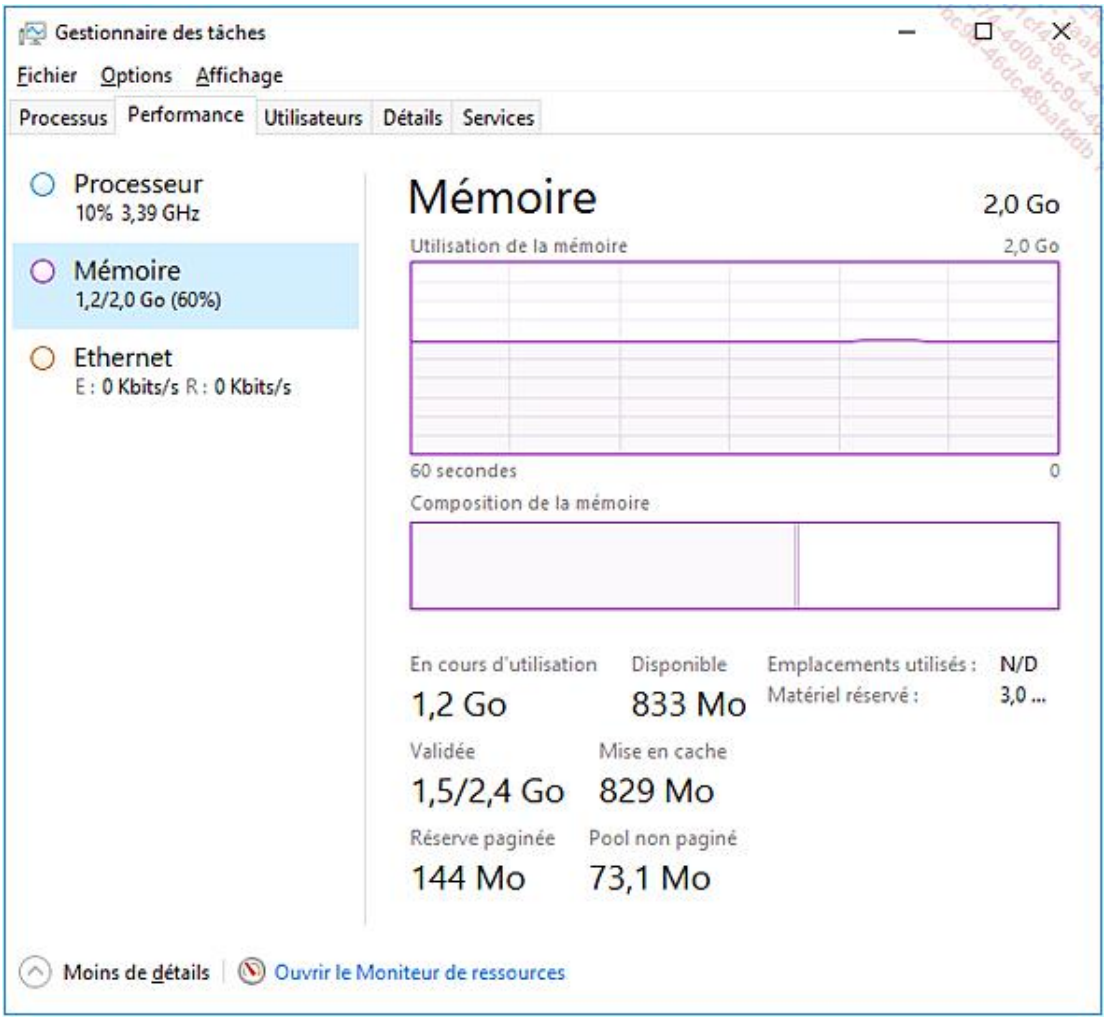
Le nom du compte qui a lancé le processus ainsi que l'utilisation du processeur et de la mémoire sont également affichés.

L'onglet **Performance** permet la visualisation de graphiques sur trois éléments essentiels :

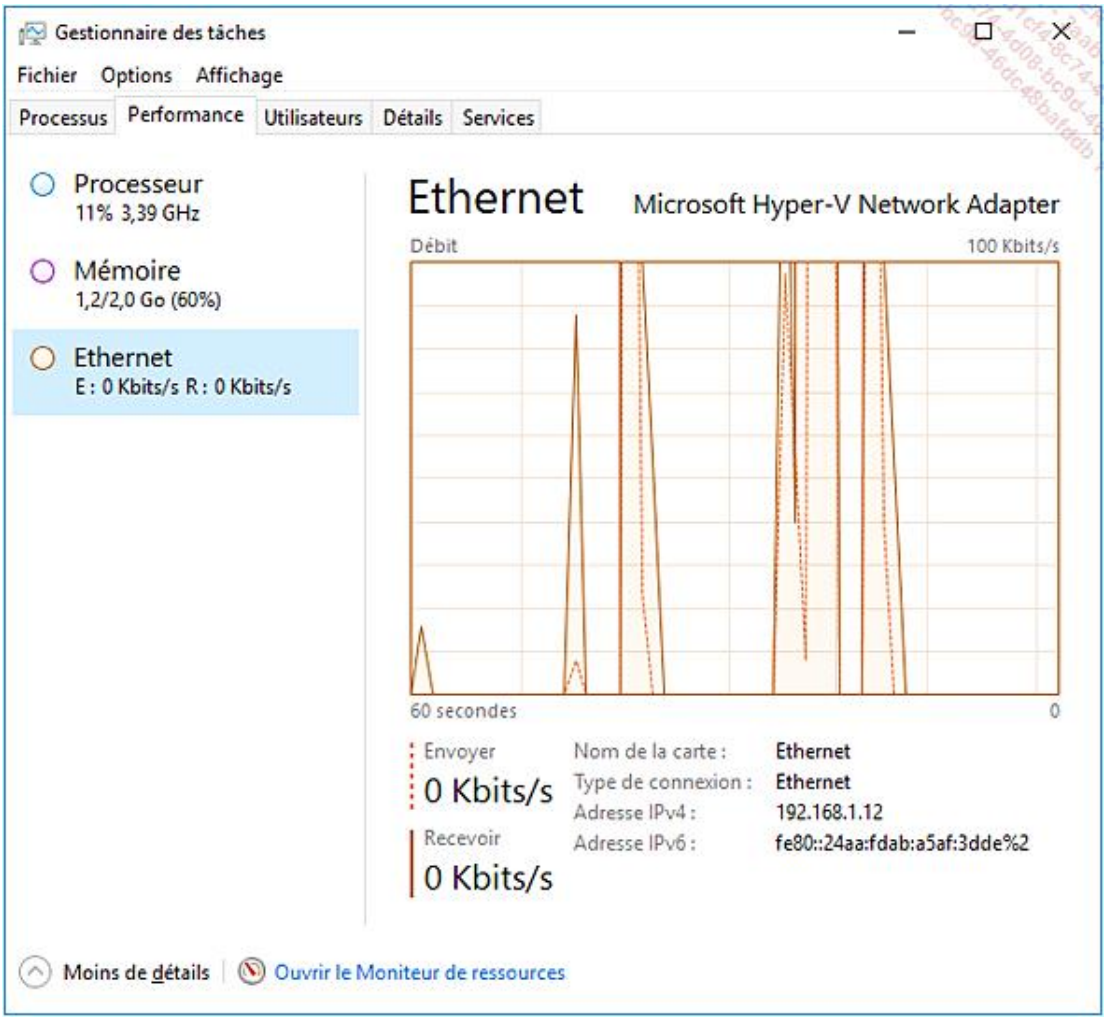
- **Le processeur** : accompagnés de la courbe, différents champs donnent des informations telles que le pourcentage d'utilisation et le nombre de processus.



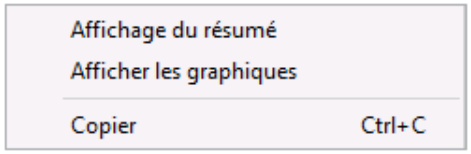
- **La mémoire** : comme pour le processeur, des informations liées à la mémoire s'affichent et sont mises à jour automatiquement. Il est donc très aisé de voir la quantité de mémoire utilisée et celle qui est libre.



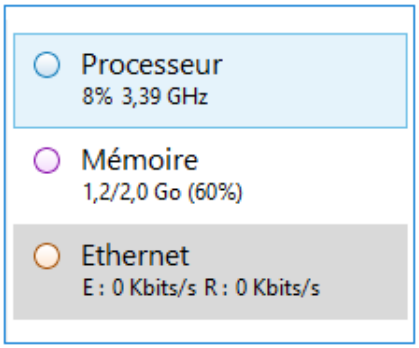
- **Le réseau** : en plus du graphique qui montre l'activité, les informations **Envoyer** et **Recevoir** permettent de connaître très facilement la vitesse d'envoi et de réception.



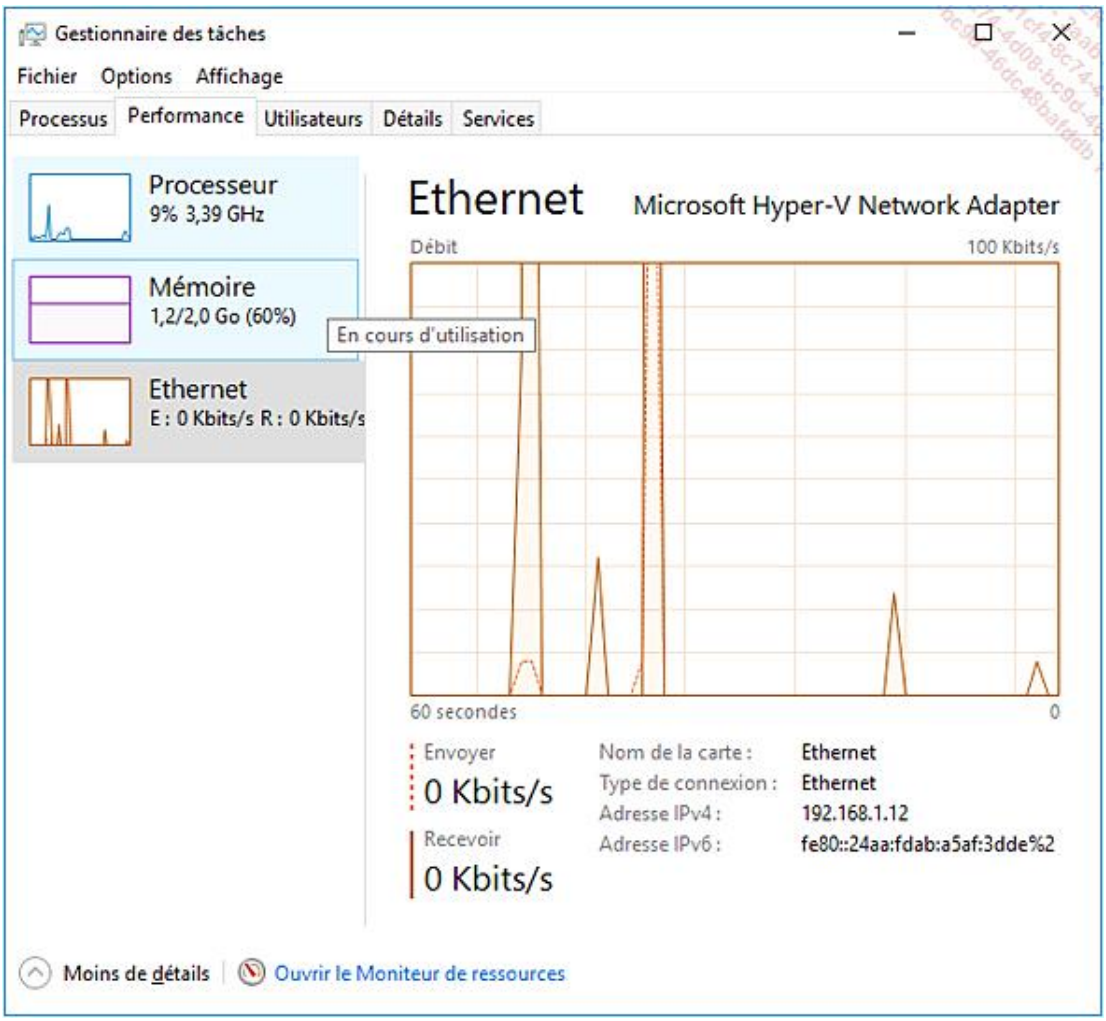
Un clic droit sur la console donne accès à un menu contextuel possédant trois options.



Affichage du résumé permet de réduire la fenêtre en affichant uniquement les valeurs des trois graphiques. Décochez l'option pour revenir au format initial.

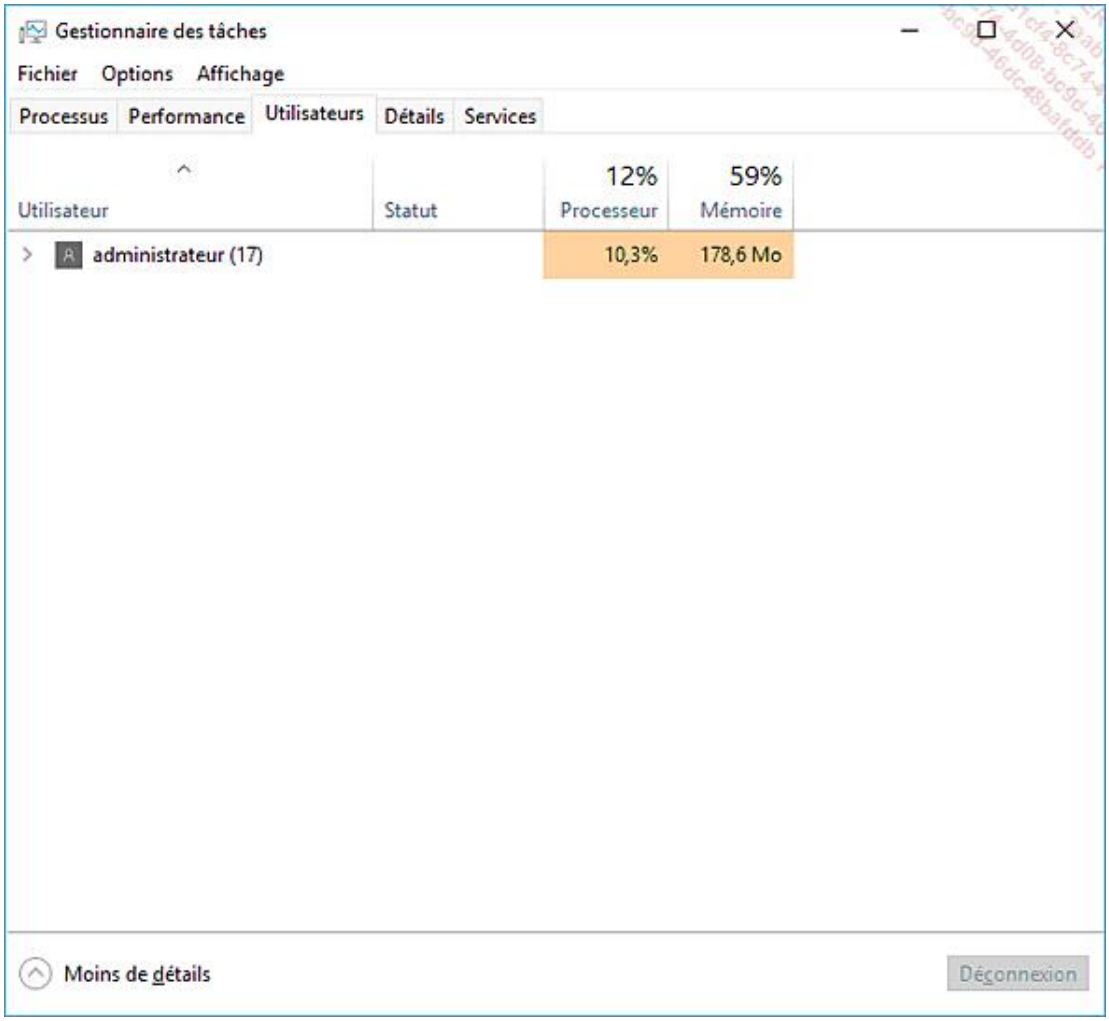


Afficher les graphiques remplace les boutons de couleurs par les graphiques en cours. Sélectionnez **Cacher les graphiques** dans le menu contextuel pour annuler l'affichage en cours.



Copier insère les données présentes sous le graphique dans le presse-papiers.

L'onglet **Utilisateurs** facilite la gestion des utilisateurs connectés.



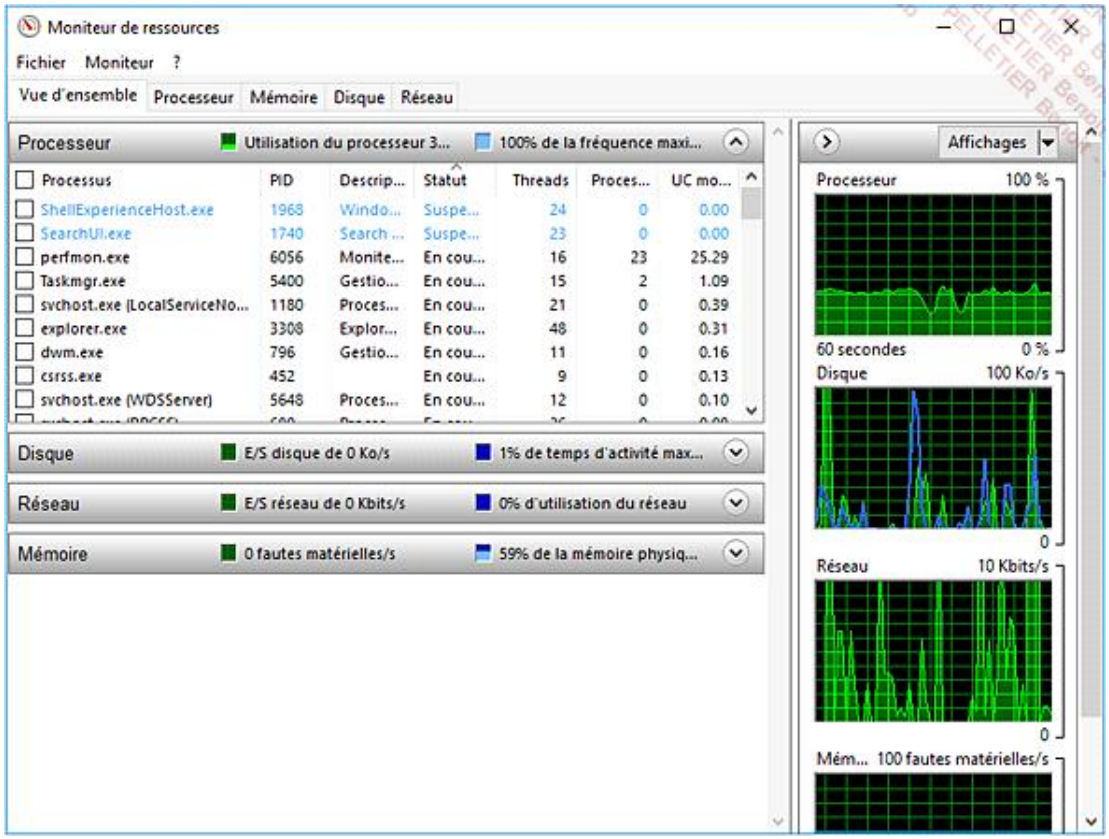
La déconnexion de la session de l'utilisateur est toujours possible mais il est maintenant plus aisé de le faire. En effet, en développant la ligne de la personne concernée, on peut très facilement voir les processus qui lui appartiennent. De plus on peut maintenant connaître l'utilisation processeur et mémoire de chacun des processus.

Enfin, le dernier onglet, **Services**, donne accès à la gestion des services. Il est possible de connaître leur statut ainsi que leurs différents paramètres (PID, etc.). L'accès à la console **Services.msc** est possible en effectuant un clic sur le lien **Ouvrir les services**.

Moniteur de ressources

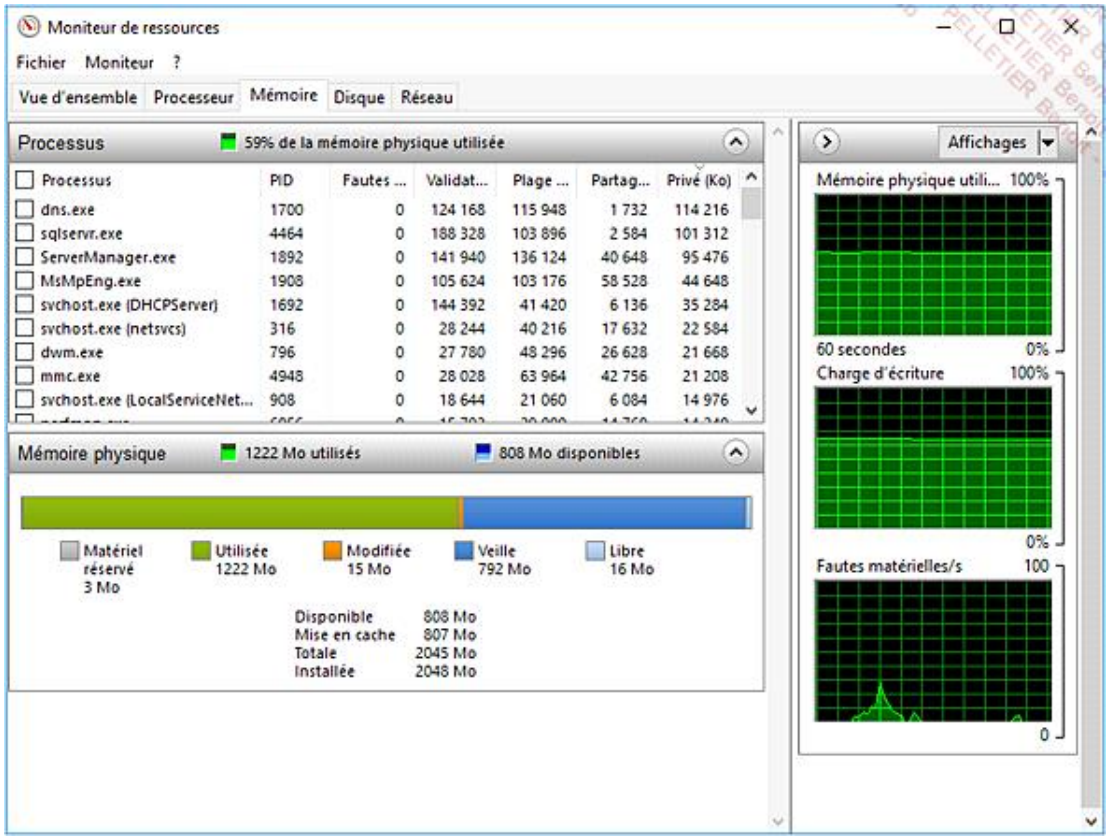
Le moniteur de ressources permet le contrôle des ressources d'un poste de travail ou d'un serveur. Cet outil permet donc d'effectuer la surveillance du processeur, des processus, de la mémoire vive ainsi que de l'activité sur les disques et le réseau.

La console est composée de plusieurs onglets. Le premier, **Vues d'ensemble**, permet d'avoir une vue sur l'ensemble des composants qui peuvent causer un goulet d'étranglement. En plus des catégories **Mémoire**, **Réseau**, **Processeur** et **Disque** présents dans l'onglet **Vues d'ensemble**, des graphiques sont affichés et actualisés en temps réel.

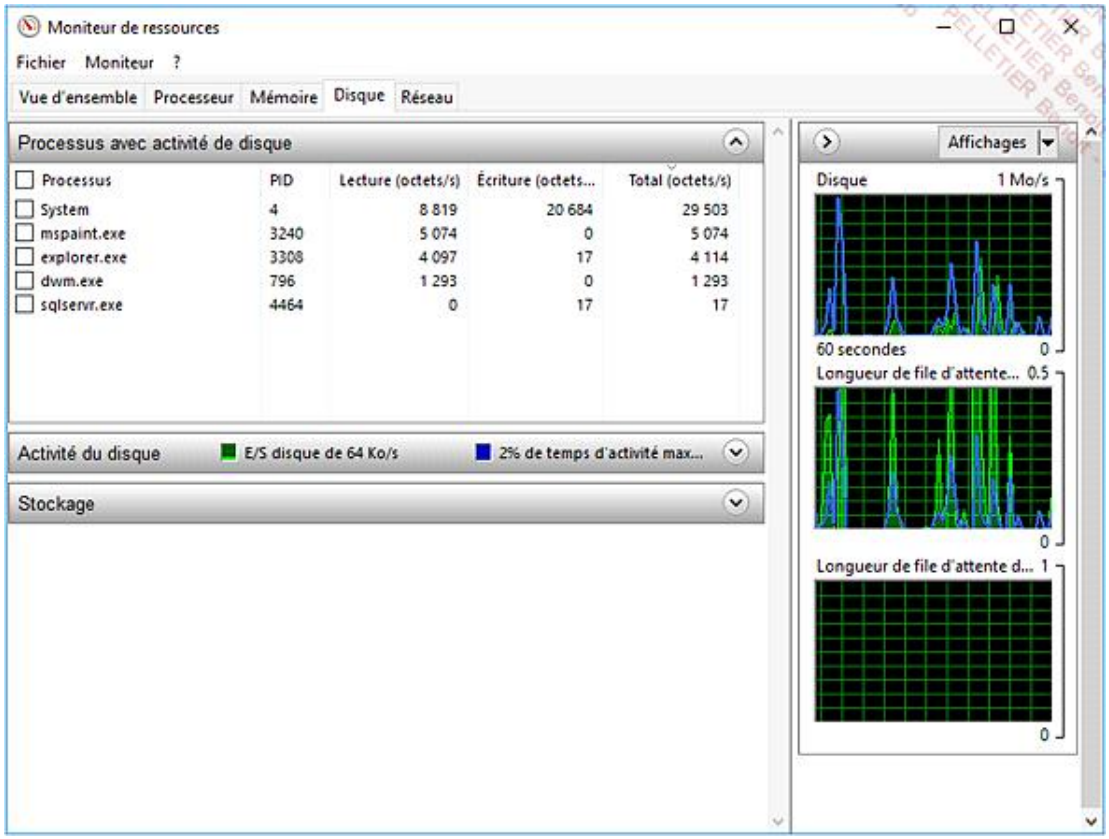


L'onglet **Processeur** reprend les différentes informations de chaque processus. En sélectionnant un processus, les différents services et descripteurs associés sont affichés. On peut également voir un graphique représentant l'activité pour chaque processeur ou chaque cœur présent dans un processeur.

La répartition de l'utilisation de la mémoire du serveur peut être visualisée par l'intermédiaire de l'onglet **Mémoire**. Trois graphiques présentent la mémoire physique utilisée, la charge d'écriture et les fautes matérielles.

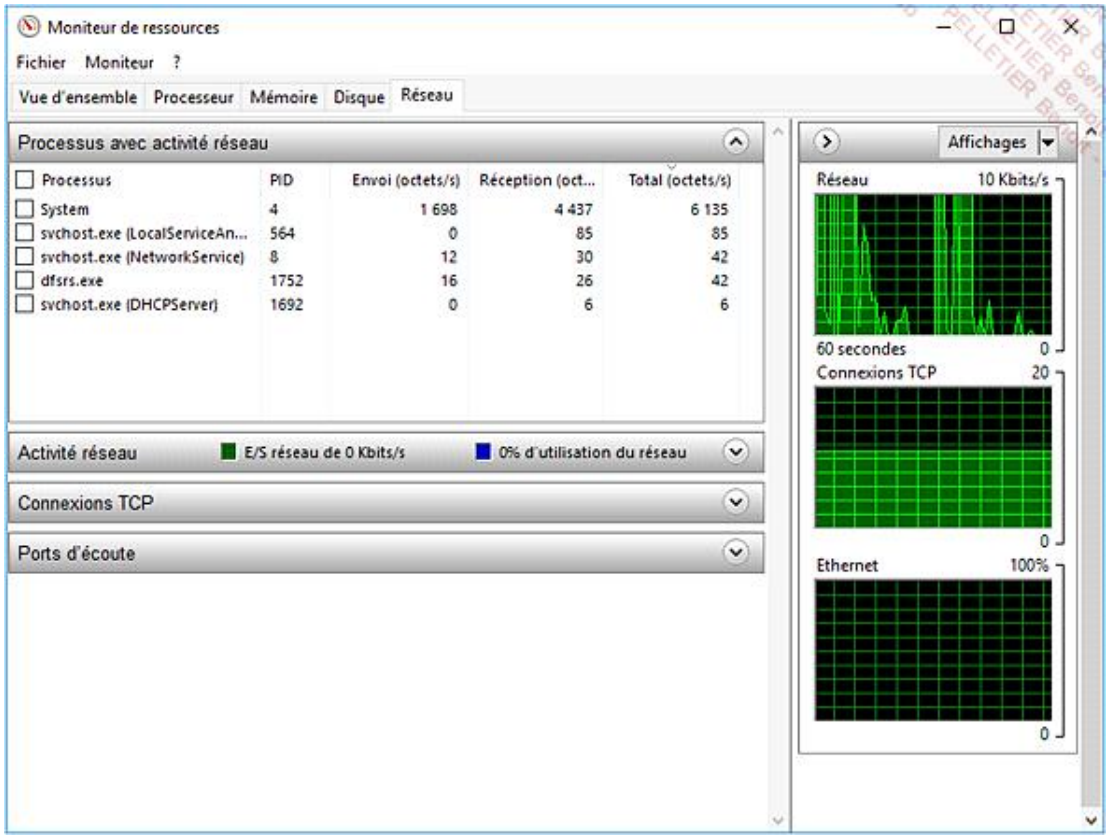


L'onglet **Disque** présente les processus effectuant une opération sur le disque. Il est une fois de plus possible de filtrer sur un processus afin de l'isoler. Les graphiques montrent une courbe représentant l'activité sur le disque.



Enfin, l'onglet **Réseau** présente les différents processus ayant une activité réseau. Cet outil est également utile pour -

voir les connexions TCP et les ports d'écoute. L'outil va permettre d'analyser les différents composants afin de donner une explication à un ralentissement du poste.



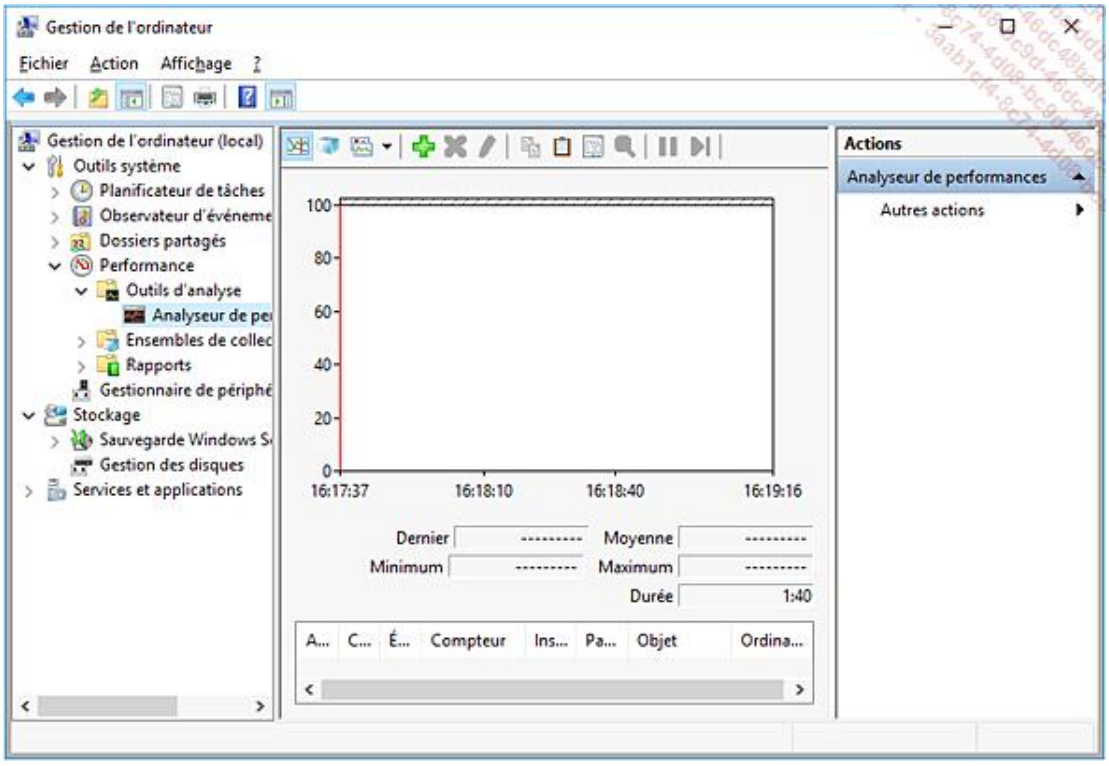
Analyseur de performances

L'**Analyseur de performances** permet la surveillance de l'activité d'un poste de travail. L'opération peut se faire par le biais d'un graphique et de rapports. L'outil possède plusieurs types de compteurs qui permettent de surveiller les parties matérielle ou logicielle. Le compteur **Processeur** permet de surveiller le temps d'interruption, le temps processeur…

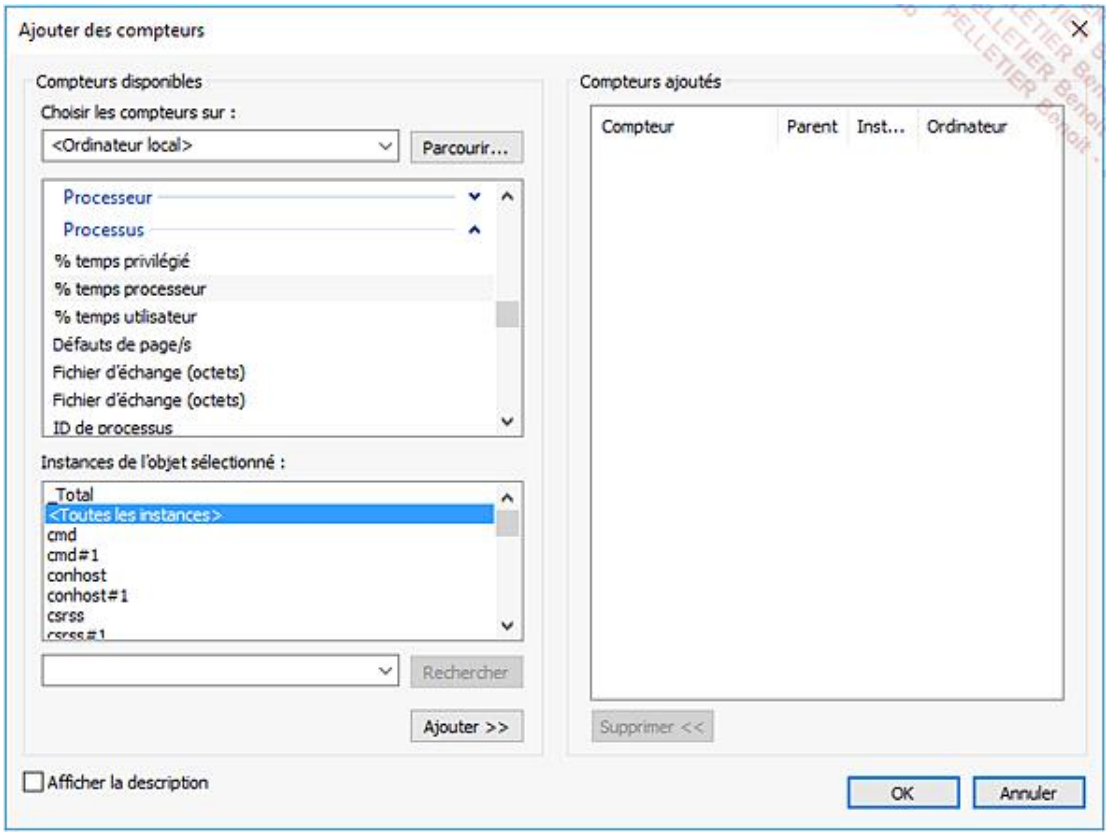
L'analyse peut être réalisée en temps réel, ce qui oblige l'administrateur à être devant le poste. De plus, la lecture des données n'est pas optimale. Une deuxième manière est l'exécution d'un collecteur de données qui permet l'enregistrement des informations récupérées par les différents compteurs.

1. Ajout d'un compteur

- Lancez la console **Gestionnaire de serveur** sur AD1.
- Cliquez sur **Outils** puis sélectionnez dans le menu contextuel **Gestion de l'ordinateur**.
- Développez les nœuds **Performance** puis **Outils d'analyse**.
- Cliquez sur **Analyseur de performances** puis sur la croix verte afin d'ajouter les compteurs.

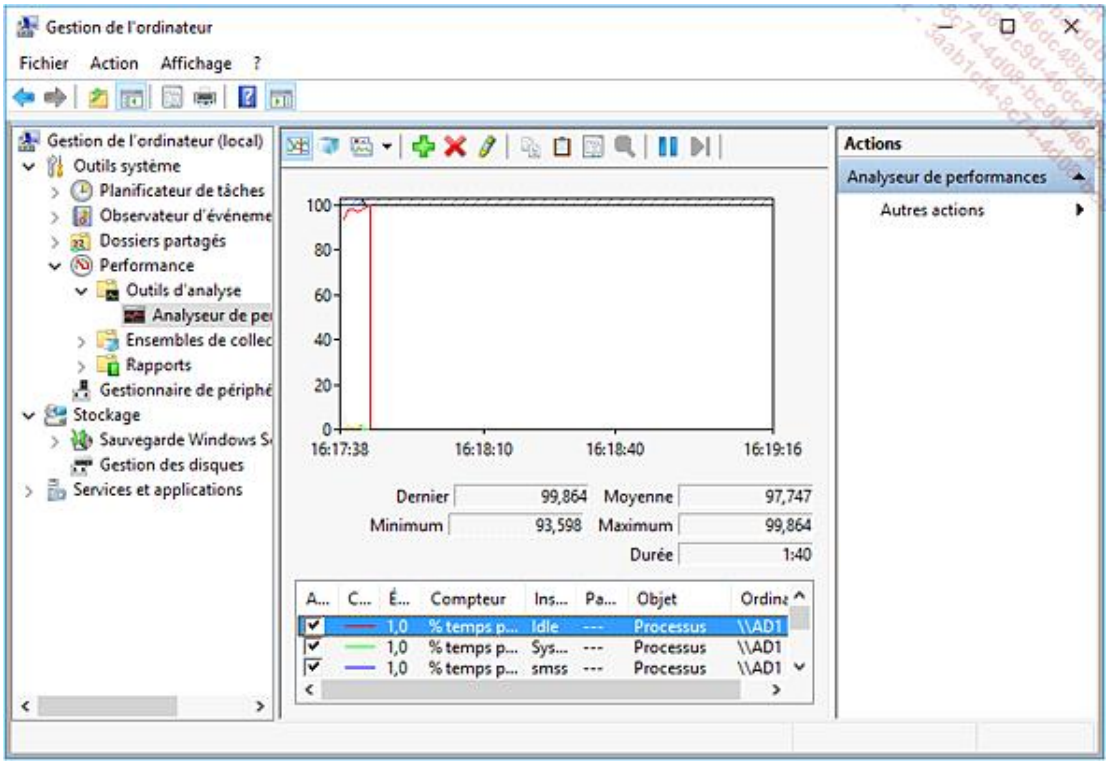


- Développez **Processus** puis cliquez sur **% temps processeur** et **<Toutes les instances>**.

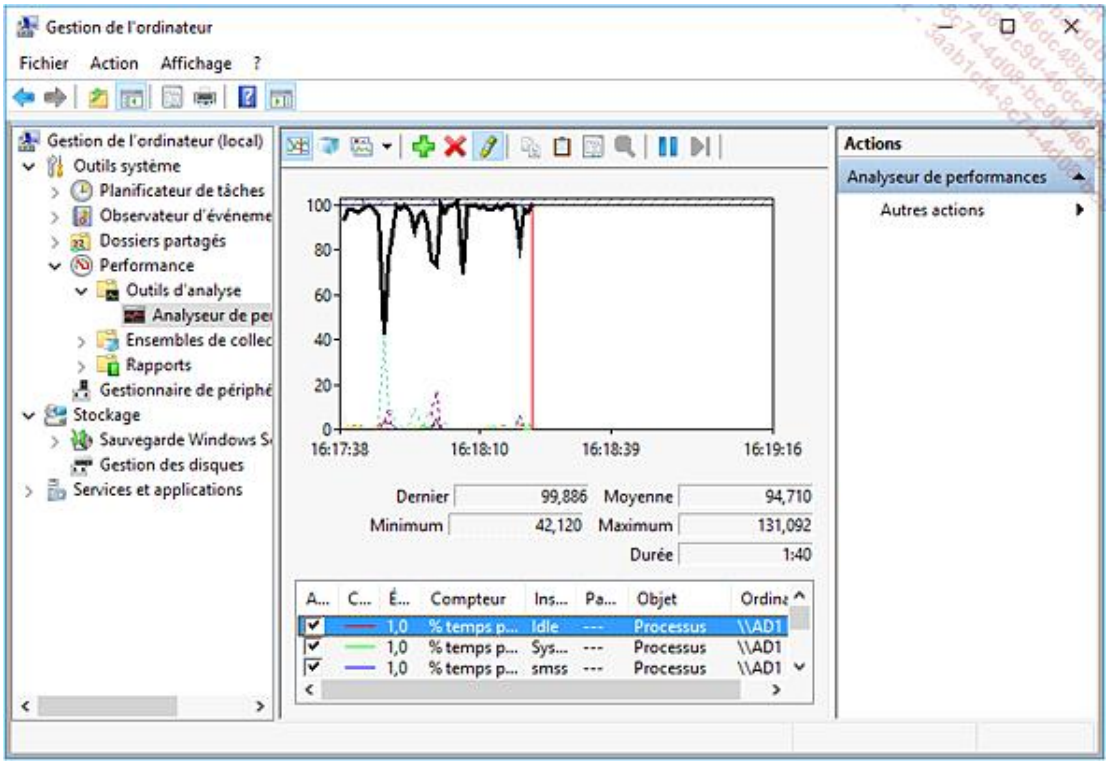


Cliquez sur **Ajouter** puis sur **OK**.

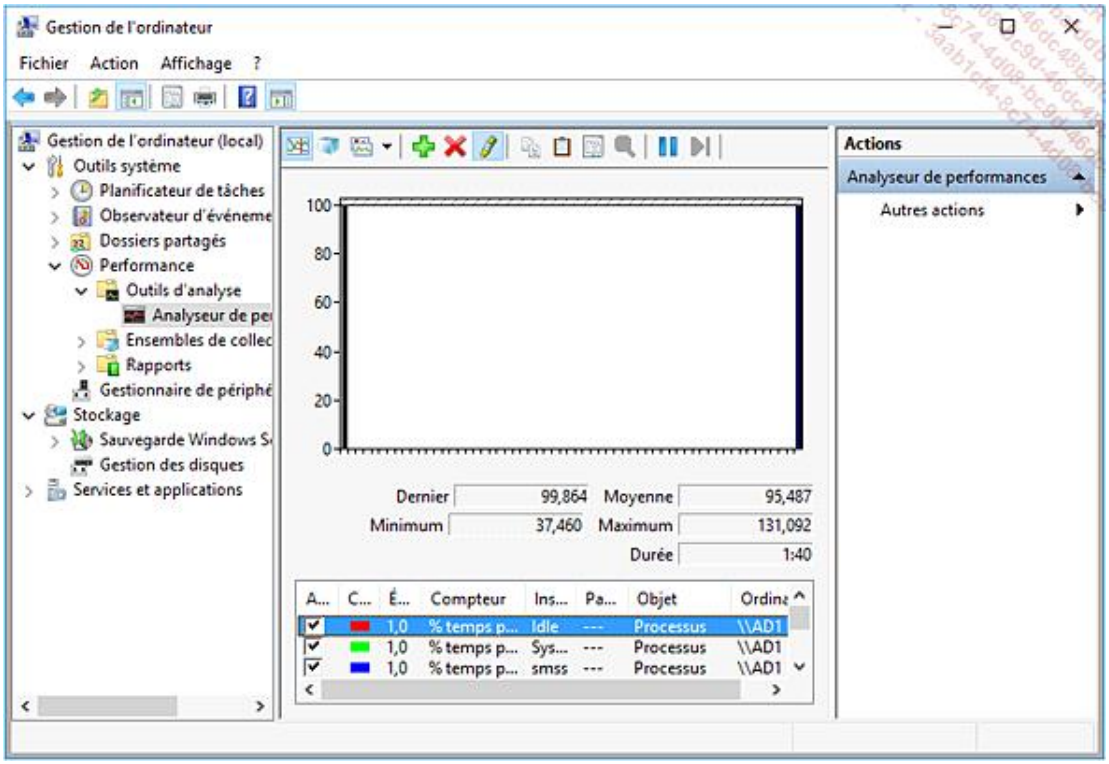
Les courbes affichées présentent les différents paramètres récupérés.



Dans la barre d'outils, cliquez sur l'icône représentant un stylo. Lors de la sélection d'un compteur, la courbe qui lui est associée se met en gras (raccourci-clavier [Ctrl] **H**).



Cliquez sur le bouton **Changer le type de graphique** puis sélectionnez dans le menu contextuel **barre d'histogramme**.



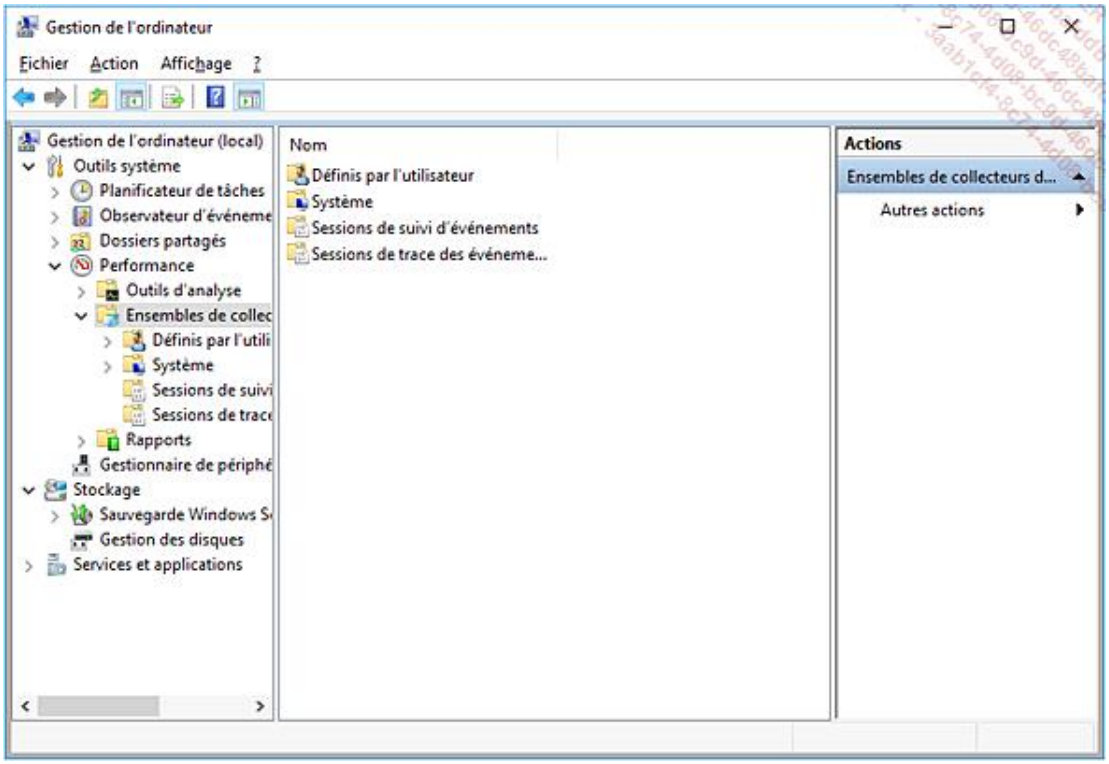
Le graphique apparaît désormais sous forme d'histogramme.

Le type de graphique peut également être présenté sous forme de rapport.

2. Création d'un ensemble de collecteurs de données

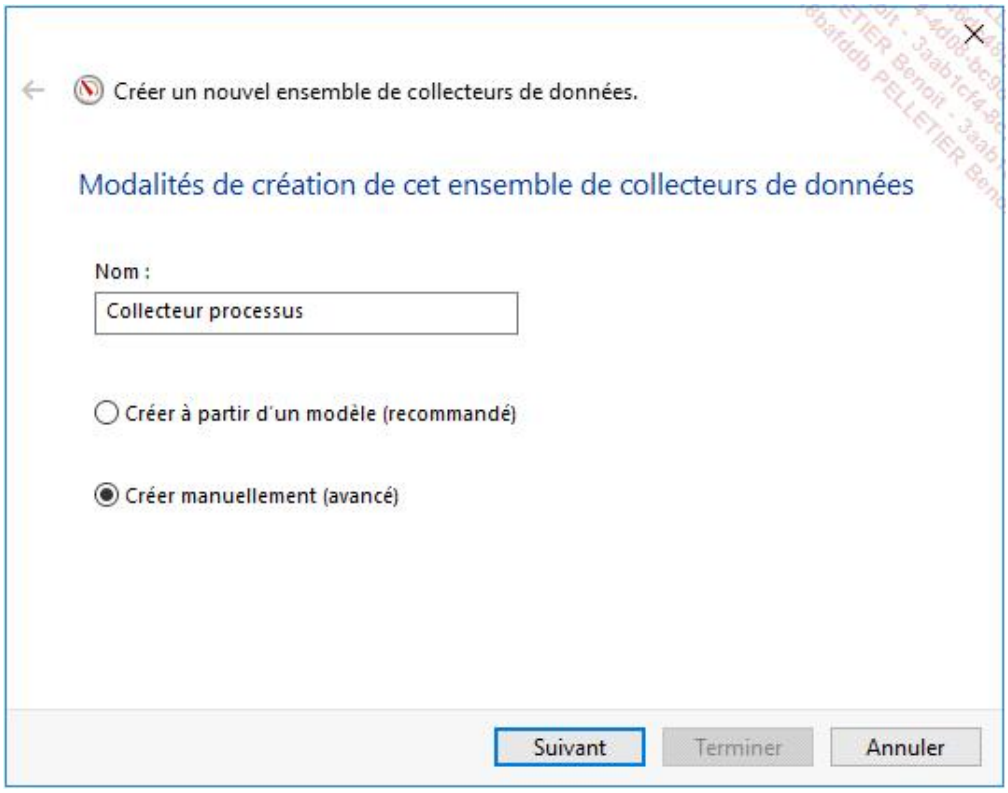
L'inconvénient de l'analyseur de performances est que l'analyse a lieu en temps réel. Cela oblige à rester devant la machine analysée. Afin d'enregistrer les données dans le but de les visualiser dans un second temps, il est recommandé d'utiliser des collecteurs de données.

- Dans la console **Gestion de l'ordinateur**, développez **Ensemble de collecteurs de données**.

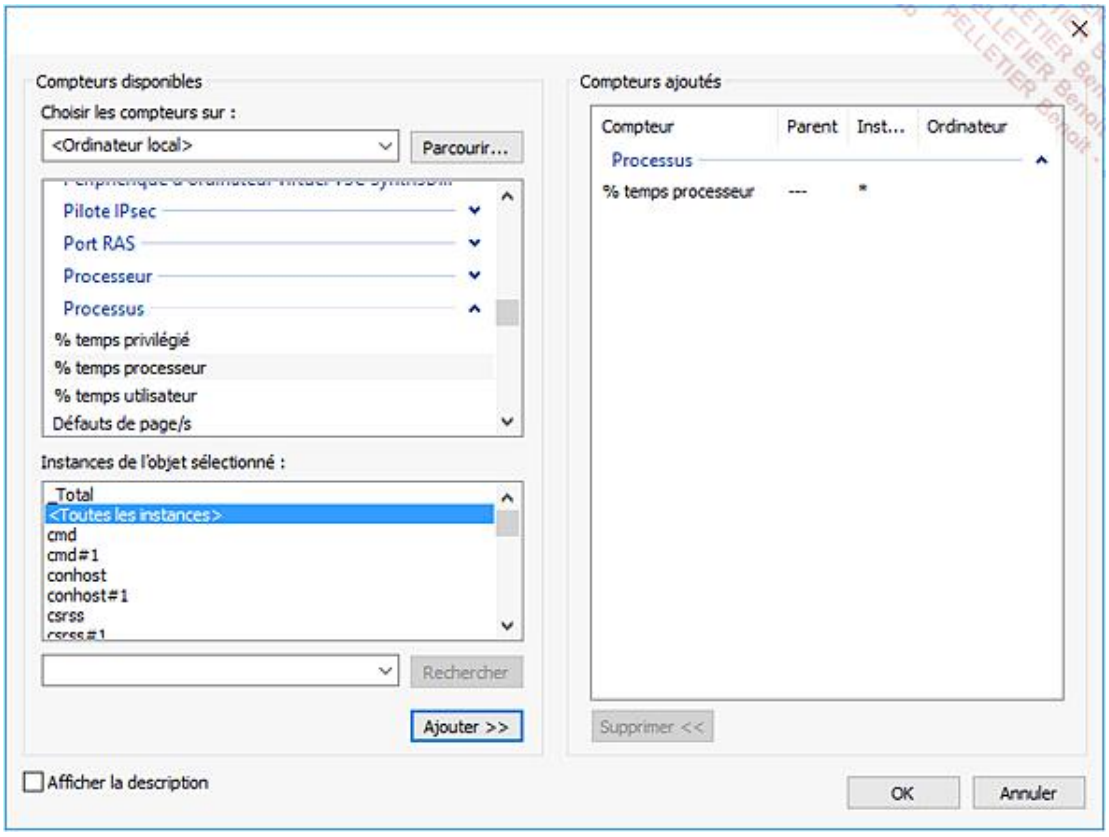


Des collecteurs sont créés en fonction des rôles présents sur la machine analysée. Cette dernière est un contrôleur de domaine. Le compteur pour le diagnostic d'Active Directory est donc présent dans **Système**. Le conteneur défini par l'utilisateur permet la création de nouveaux collecteurs de données.

- Effectuez un clic droit sur **Définis par l'utilisateur** puis dans le menu contextuel sélectionnez **Nouveau** et **Ensemble de collecteurs de données**.
- Saisissez **Collecteur processus** dans le champ **Nom** puis cochez le bouton radio **Créer manuellement (avancé)** puis cliquez sur **Suivant**.

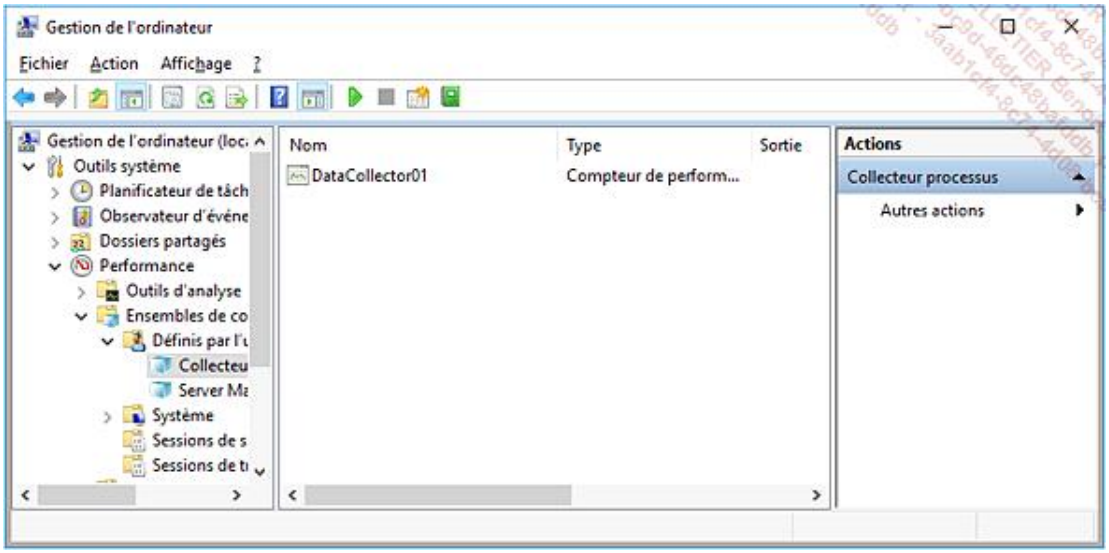


- Dans la fenêtre de choix des types de données, cochez **Compteur de performance** puis cliquez sur **Suivant**.
- Dans la fenêtre des choix des compteurs, cliquez sur **Ajouter**.
- Développez **Processus** puis cliquez sur **% temps processeur** et **<Toutes les instances>**.
- Cliquez sur le bouton **Ajouter** puis **OK**.



- Configurez **Intervalle d'échantillonnage** à 2 secondes.
- Cliquez deux fois sur **Suivant** puis sur **Terminer**.

Le collecteur de données est maintenant présent dans la console.



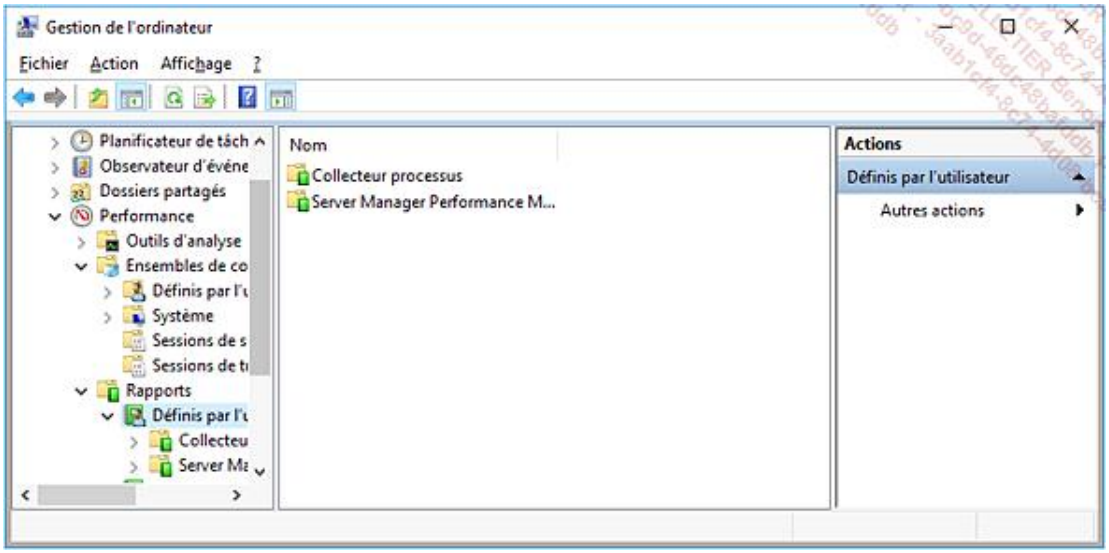
- Effectuez un clic droit sur **Collecteur processus** puis sélectionnez **Démarrer**.

Laissez le collecteur sur l'état **En cours d'exécution** quelques secondes afin qu'il recueille un minimum d'informations.

- Effectuez un clic droit sur **Collecteur processus** puis sélectionnez **Arrêter**.

Lors du démarrage du collecteur, un rapport est créé afin de présenter les données récupérées.

- Développez les nœuds **Rapports** puis **Définis par l'utilisateur**.



Un conteneur portant le même nom que le collecteur de données est présent.

- Développez **Collecteur processus** puis cliquez sur le rapport.

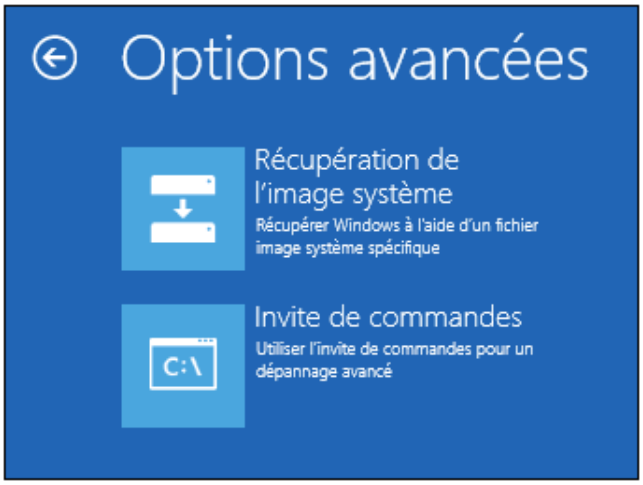
Comme pour l’analyseur de performances, il est possible de surligner la courbe du compteur sélectionné ou de changer le type de graphique.

L'environnement WinRE

Apparu avec Windows Vista, l'environnement WinRE (*Windows Recovery Environment*) permet de charger une image dans le but d'effectuer une maintenance. Cette image intègre une multitude d'outils dont une invite de commandes DOS permettant d'accéder aux disques et aux différents outils en ligne de commande. Il est également possible d'avoir un accès à l'outil d'analyse du démarrage afin d'analyser et réparer un problème dans la séquence de boot.

D'autres comme l'analyse de la mémoire, la récupération de l'image système ou encore la restauration du système en utilisant un point de restauration sont autant d'outils présents dans l'environnement. Depuis Windows 8.1 l'environnement WinRE permet l'accès à plus d'outils.

Environnement sous Windows Server 2016 :



Environnement sous Windows 10 :



Le démarrage de cet environnement peut se faire par le biais du **DVD d'installation** ou tout simplement lorsque le système ne peut pas démarrer.

1. Commande bcdedit

Les fichiers BCD (*Boot Configuration Data*) fournissent un magasin qui permet la description des paramètres de démarrage. Le BCD remplace le fichier boot.ini depuis Windows Vista.

Afin de gérer ce magasin de données, la commande `bcdedit` peut être utilisée. Elle permet la création d'un nouveau magasin ou la modification d'un magasin existant. L'ajout d'une option de démarrage s'effectue également à l'aide de cette commande. Cette dernière peut être utilisée directement dans une invite de commandes ou par l'intermédiaire d'un script.

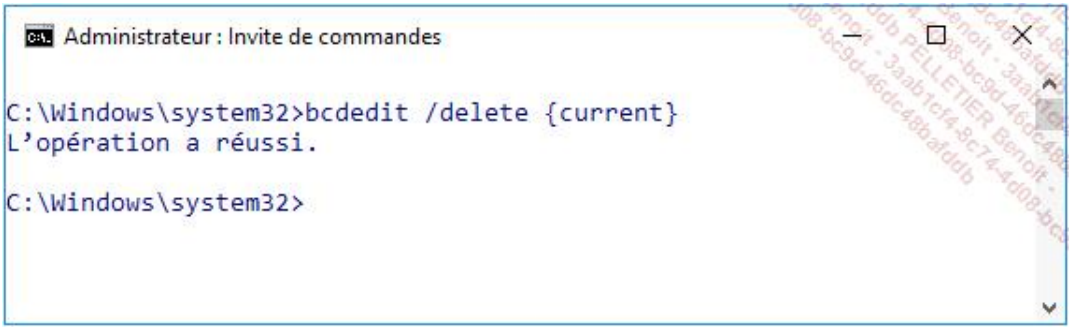
- Saisissez la commande `bcdedit` dans l'invite de commandes.



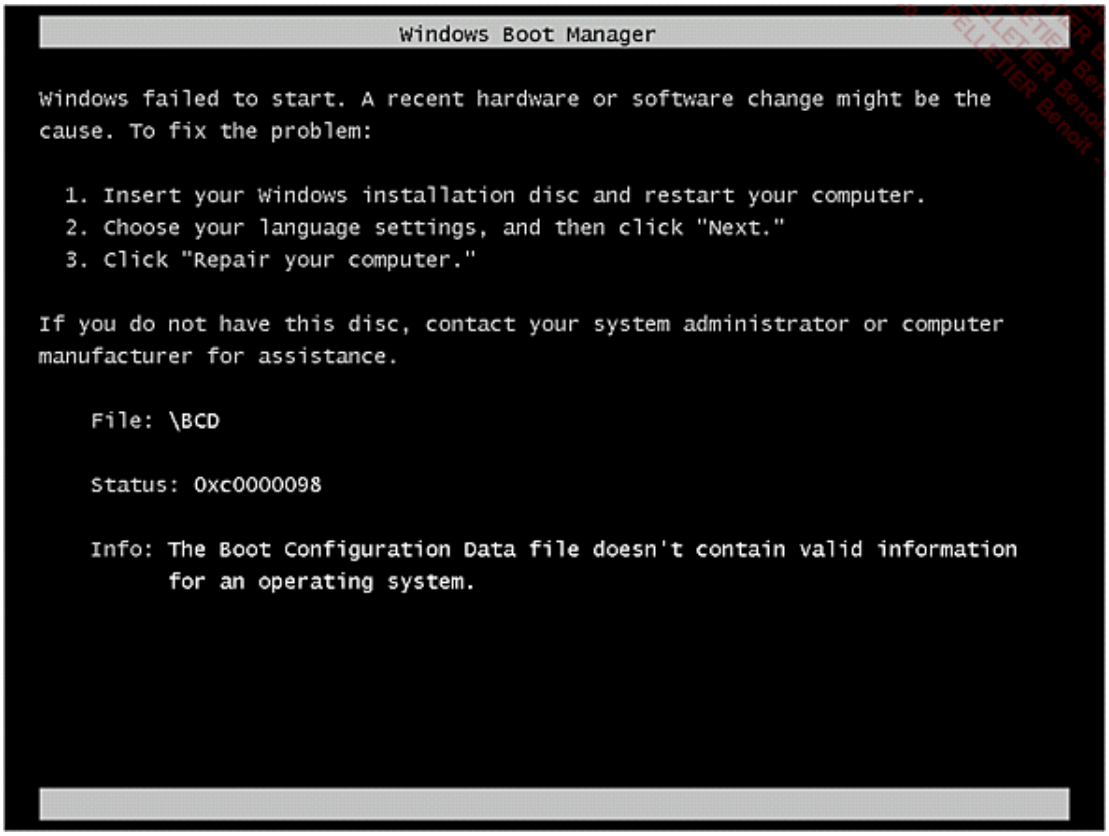
identificateur {current} indique le magasin qui est chargé actuellement. Les champs **device** et **path** indiquent la lettre de la partition ainsi que le chemin du fichier **winload**.

La description permet de donner un renseignement sur le système qui est chargé.

- Sur AD1, saisissez `bcdedit /delete {current}`, afin de supprimer l'entrée **{current}** du magasin.



L'ordinateur ne peut désormais plus démarrer.

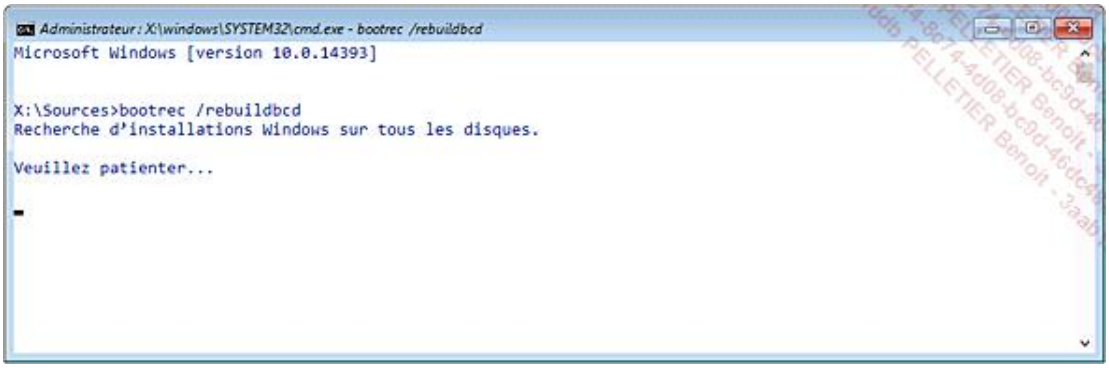


Le système ne trouve pas d'entrée dans le magasin de données, il lui est donc impossible de charger un système d'exploitation.

2. Réparer la séquence de démarrage

La séquence de boot peut être réparée depuis l'invite de commandes en utilisant la commande `bootrec`.

- Connectez l'ISO de Windows Server 2016 sur la machine virtuelle AD1.
- Démarrez la machine puis appuyez sur une touche pour démarrer sur le DVD.
- À la fin du chargement de l'image, cliquez sur **Suivant** dans la fenêtre de bienvenue.
- Cliquez sur **Réparer l'ordinateur** afin de lancer l'environnement WinRE.
- Sélectionnez **Dépannage** puis **Invite de commandes**.
- Saisissez la commande `bootrec /rebuildbcd` dans l'invite de commandes DOS.



Le système a identifié une ou plusieurs installations de Windows. Il est donc nécessaire de les ajouter.

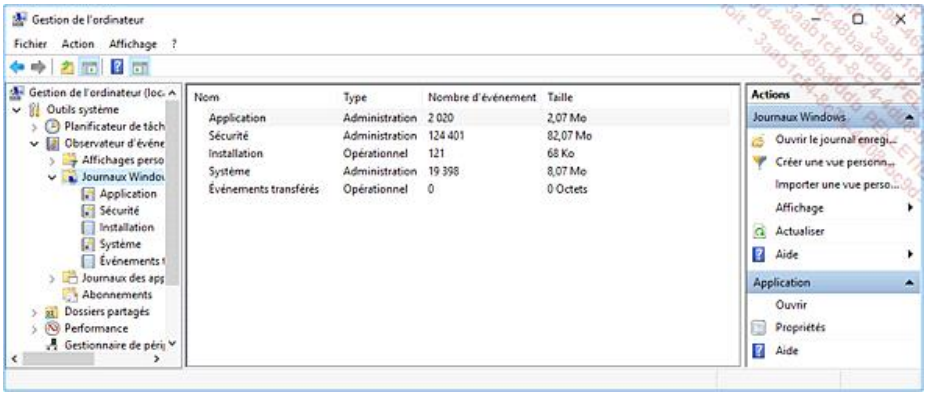
- Saisissez **o** puis appuyez sur la touche [Entrée].
- Redémarrez la machine AD1. Celle-ci doit démarrer correctement.

L'Observateur d'événements

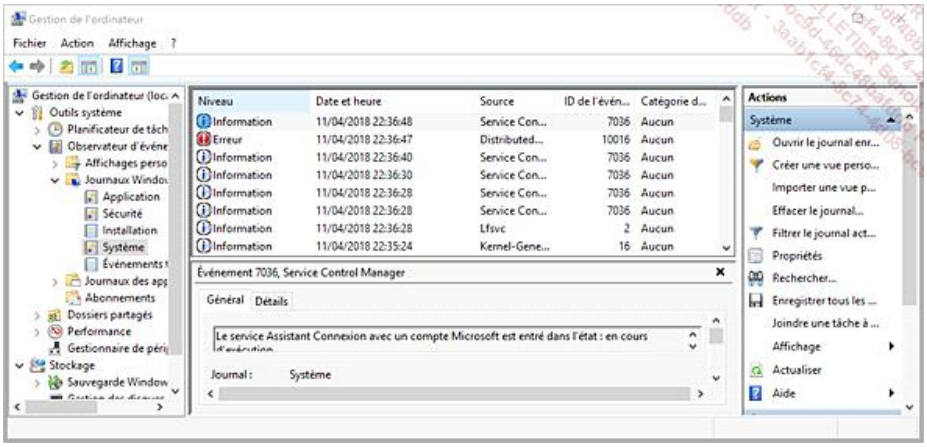
L'observateur d'événements contient plusieurs journaux utiles pour diagnostiquer une panne ou une incohérence dans le système. Il est composé de plusieurs journaux dont **Application**, **Système** ou **Sécurité**. Le journal **Application** permet aux développeurs d'applications d'inscrire des événements retournés par leurs applications. Le journal **Système** permet de récupérer les informations retournées par le système (par exemple, un problème DHCP). Le journal **Sécurité** contient un retour des audits configurés.

Les différents journaux au format **EVTX** sont présents dans le dossier **C:\windows\system32\winevt\Logs**.

- Sur AD1, lancez la console **Gestionnaire de serveur** puis à l'aide du menu **Outils**, sélectionnez **Gestion de l'ordinateur**.
- Développez **Observateur d'événements** puis **Journaux Windows**.



- Cliquez sur le journal **Système**. Il contient plusieurs types d'événements.



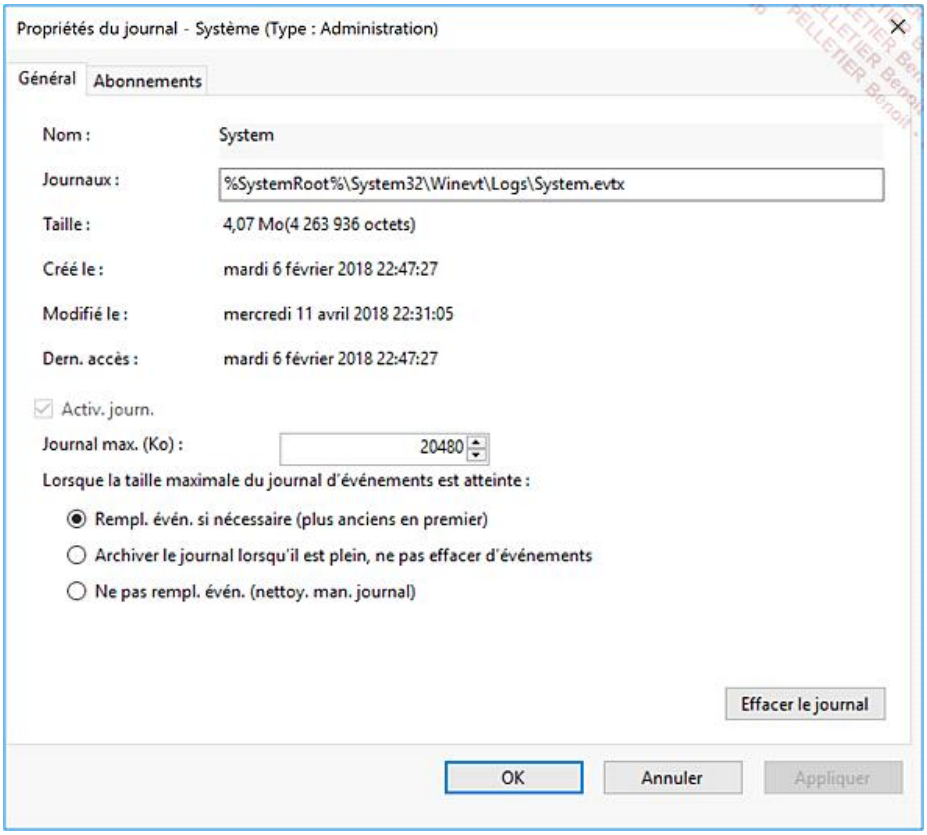
On peut trouver dans un journal plusieurs niveaux d'avertissement :

- Information
- Avertissement
- Erreur
- Critique

De plus, un événement possède plusieurs informations importantes dont le numéro ID (**ID de l'événement**), l'application source (**Source**) et le message.

- Effectuez un clic droit sur le journal **Système** puis sélectionnez **Propriétés**.

La fenêtre présente le chemin du journal et son nom mais également sa taille actuelle et sa taille maximale. Le bouton **Effacer le journal** permet de vider un journal de tous ses événements.



Cliquez sur **OK**.

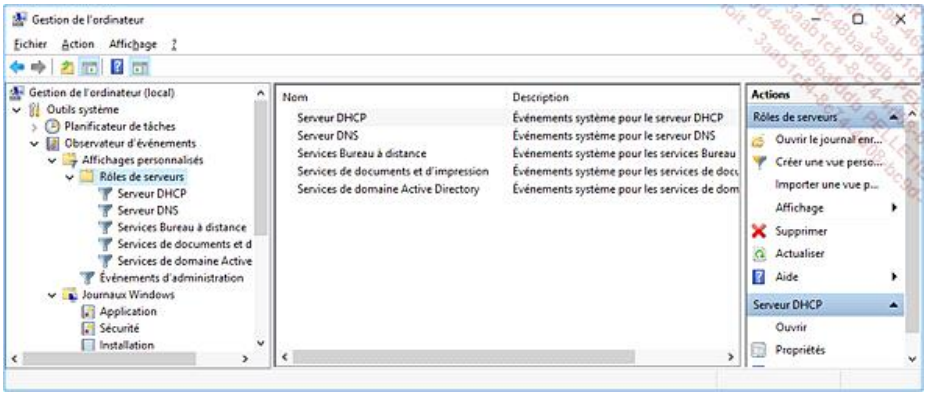
L'action à effectuer lorsque la taille maximale est atteinte est également à déterminer. Trois actions sont possibles :

- **Rempl. éven. si nécessaire (plus anciens en premier)**. Les événements les plus anciens sont supprimés.
- **Archiver le journal lorsqu'il est plein, ne pas effacer d'événements**. Un archivage automatique est effectué.
- **Ne pas rempl. évén. (nettoy. Man. Journal)**. Un nettoyage manuel doit être effectué.

1. Création d'une vue personnalisée

Très vite, le journal peut contenir un nombre important d'événements, ce qui complique la recherche d'un événement particulier. Depuis Windows Server 2008, il est possible de créer une vue afin de positionner un filtre sur un ou plusieurs journaux.

Déroulez les nœuds **Affichages personnalisés** puis **Rôles de serveurs**.



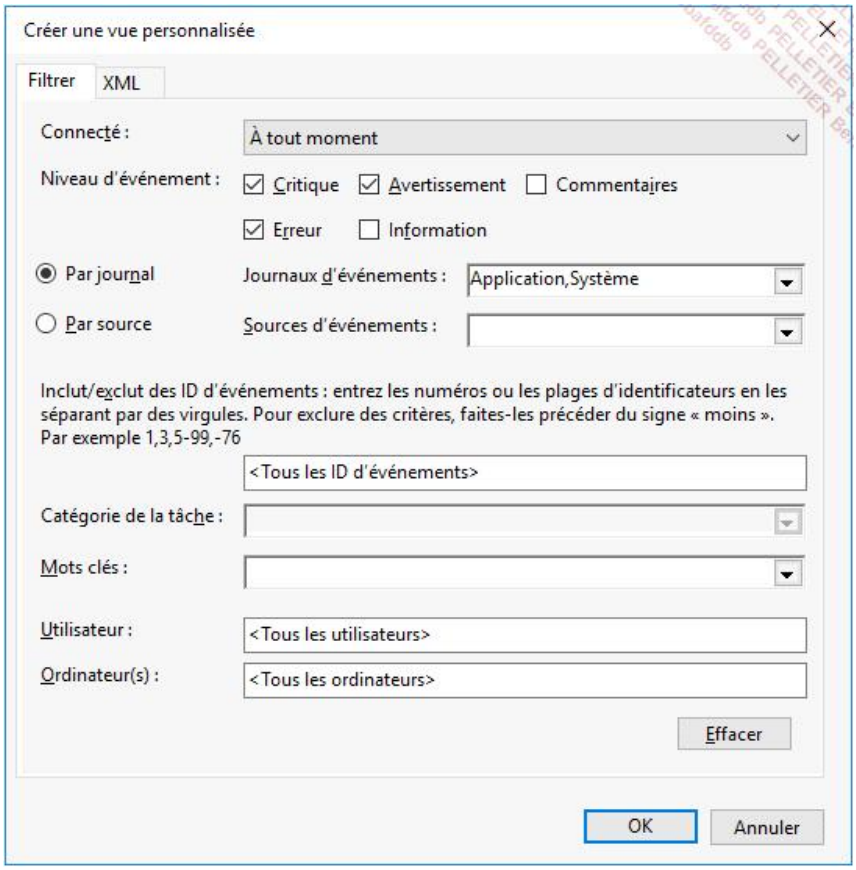
Des filtres ont été créés afin de récupérer les événements d'un rôle particulier.

Effectuez un clic droit sur **Affichages personnalisés** puis sélectionnez **Créer une vue personnalisée**.

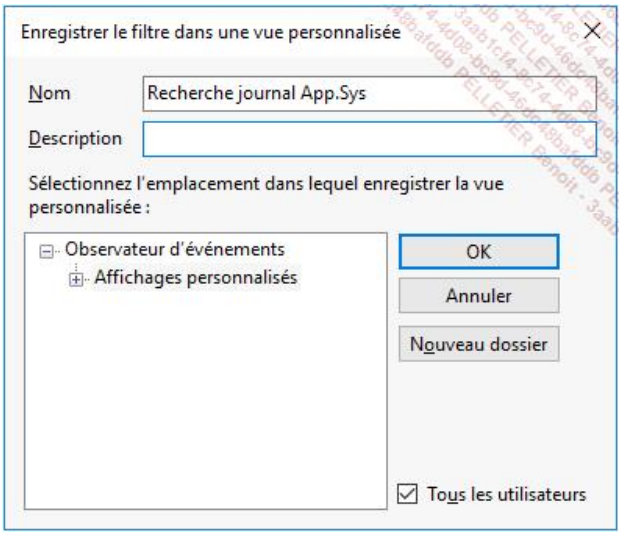
La liste déroulante **Connecté** permet de donner aux systèmes une constante de temps à prendre en compte dans le filtre.

- Laissez la valeur **À tout moment** dans la liste déroulante **Connecté**.
- Cochez **Erreur**, **Avertissement** et **Critique** afin de limiter les journaux filtrés à ces niveaux.
- Dans la liste déroulante **Journaux d'événements**, sélectionnez les journaux **Système** et **Application**.

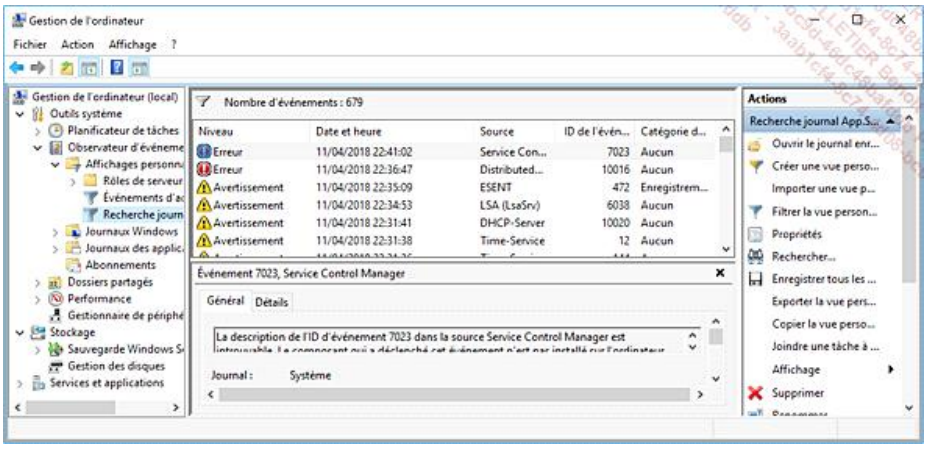
Le filtre est positionné sur les journaux ci-dessus. Il est également possible de filtrer par source en cochant le bouton radio **Par source** et en sélectionnant dans la liste déroulante une ou plusieurs sources. Il est également possible de filtrer en fonction d'un nom d'ordinateur, d'utilisateur ou de mots-clés, voire d'un ID.



- Cliquez sur **OK** puis dans le champ **Nom**, saisissez **Recherche journal App.Sys**.



Le filtre est appliqué sur l'ensemble des journaux sélectionnés.



Il est maintenant plus aisé de retrouver une information dans un journal.

2. Association d'une tâche à un événement

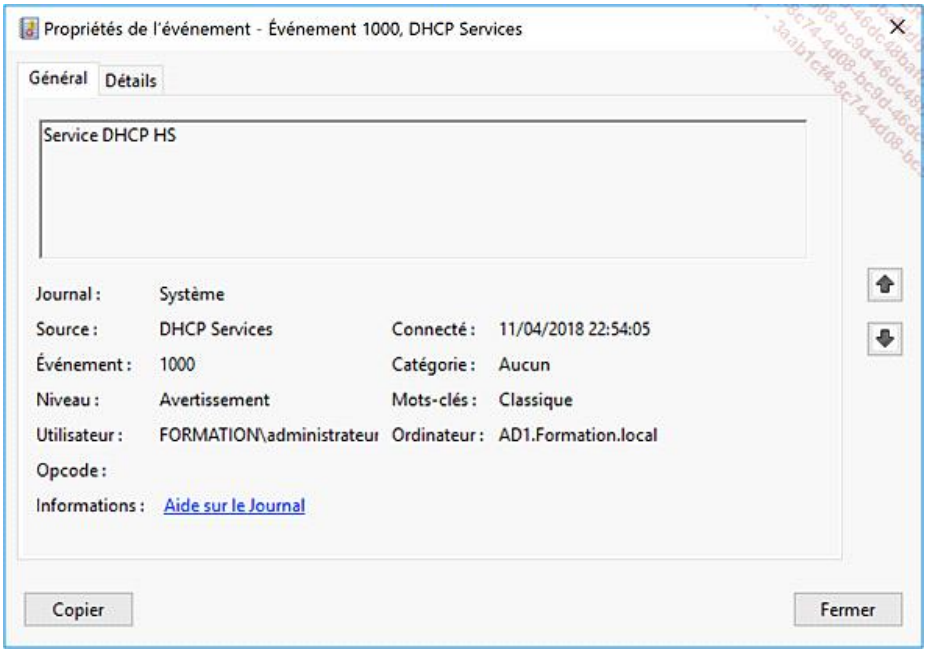
L'association d'une tâche à un événement permet l'exécution d'une action lorsque l'événement est généré. Il est possible de lancer l'exécution d'un programme, l'envoi d'un mail ou simplement l'affichage d'un message. Une fois l'association validée, une entrée est inscrite dans le planificateur de tâches. C'est depuis ce dernier qu'il est possible de modifier l'action ou de suspendre la tâche.

- Sur AD1, accédez aux **Outils d'administration** puis cliquez sur **DHCP**.
- Développez le nœud **AD1.Formation.local** puis effectuez un clic droit sur ce dernier.
- Dans le menu contextuel, sélectionnez **Toutes les tâches** puis **Arrêter**.
- Créez et exécutez le fichier **Script-Evenement.ps1**.

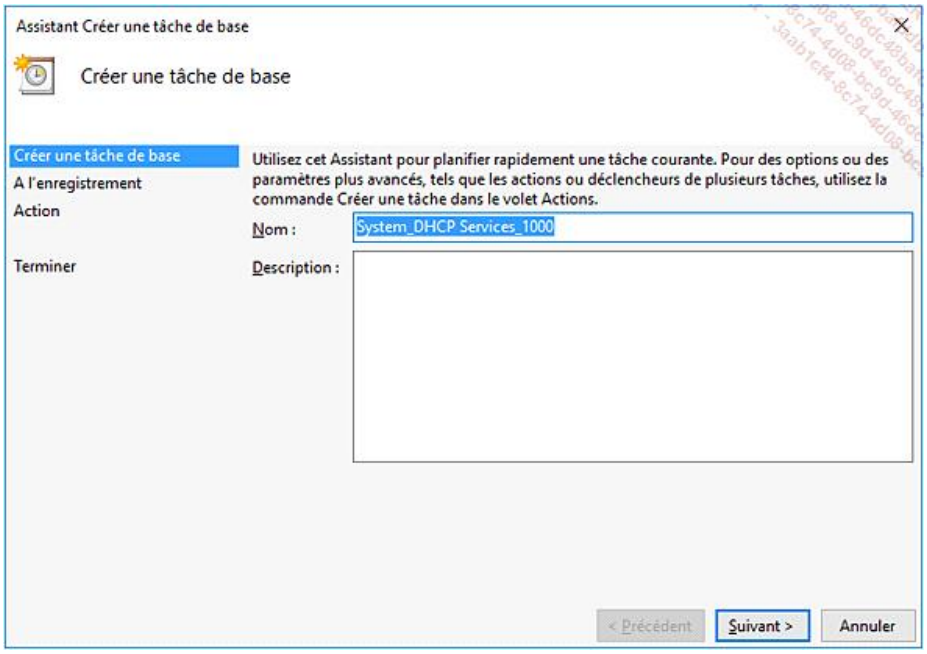


Le fichier peut être téléchargé depuis la page Informations générales.

- Dans le journal **Système**, sélectionnez l'avertissement qui a été créé.



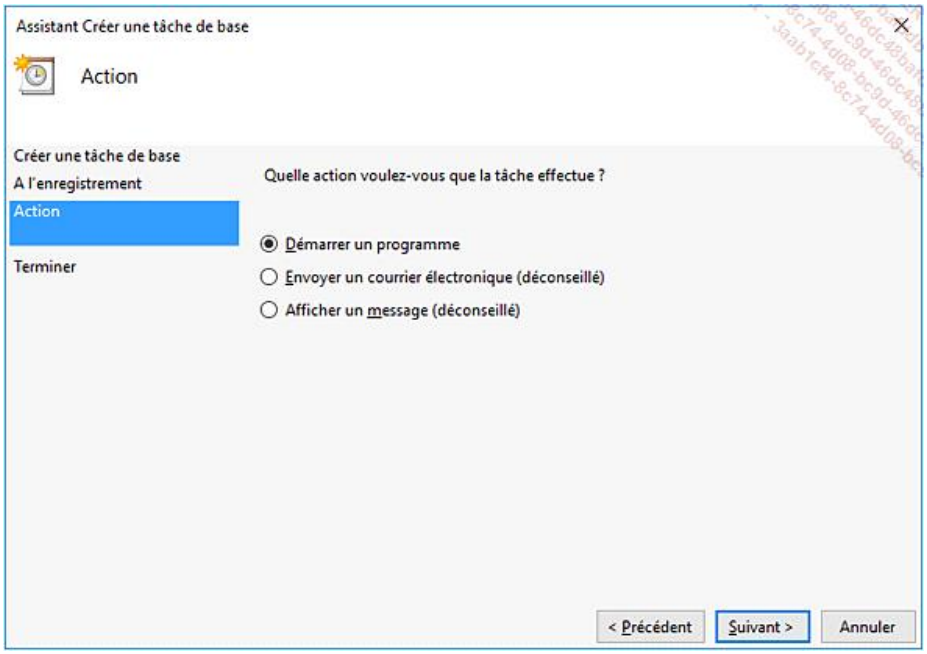
- Effectuez un clic droit sur l'avertissement puis sélectionnez **Joindre une tâche à cet événement**.
- Cliquez sur **Suivant** dans la fenêtre **Créer une tâche de base** en laissant les paramètres par défaut.



- Les champs **Journal**, **Source** et **ID de l'événement** sont grisés et contiennent déjà les valeurs adéquates. Cliquez sur **Suivant** afin de valider la fenêtre **Si un événement spécifique est enregistré**.

Il est préférable d'exécuter un script ou un programme qui effectue une tâche plutôt que d'afficher un message qui ne sera pas obligatoirement vu par l'administrateur.

- Cochez le bouton radio **Démarrer un programme** puis cliquez sur **Suivant**.



Créez le fichier **Reset-Services.ps1**.

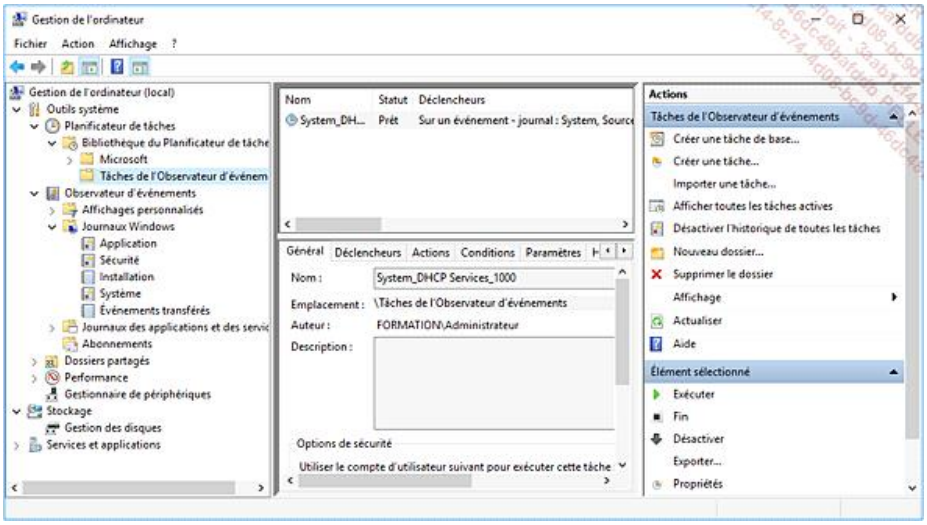
Le fichier peut être téléchargé depuis la page Informations générales.



Cliquez sur **Parcourir** puis sélectionnez le script et validez votre choix à l'aide du bouton **Suivant**.

Cliquez sur **Terminer** puis sur **OK** dans le message d'information.

Une nouvelle entrée est présente dans le planificateur de tâches.



Exécutez une nouvelle fois le fichier **Script-Evenement.ps1**.

Une nouvelle entrée est présente dans le journal Système et le fichier **Reset-Services** est exécuté. Attention à vérifier la politique d'exécution. Si besoin, pensez à modifier cette politique afin d'autoriser les scripts non signés (set-executionpolicy).

Le service DHCP a bien été redémarré.

Certaines actions peuvent donc être facilement automatisées.

3. Récupération des événements à l'aide de WinRMS

Depuis de nombreuses années, il est possible de récupérer les journaux d'événements d'un poste ou serveur sur un serveur central. Cette section aborde la récupération d'événements depuis des serveurs à l'aide de WinRMS (WinRM et SSL pour le chiffrement du trafic). Notez qu'il est possible d'effectuer la même opération sur un poste de travail.

Pour procédez au chiffrement, un certificat numérique est requis. Les ports utilisés par WinRM (port par défaut) sont les suivants :

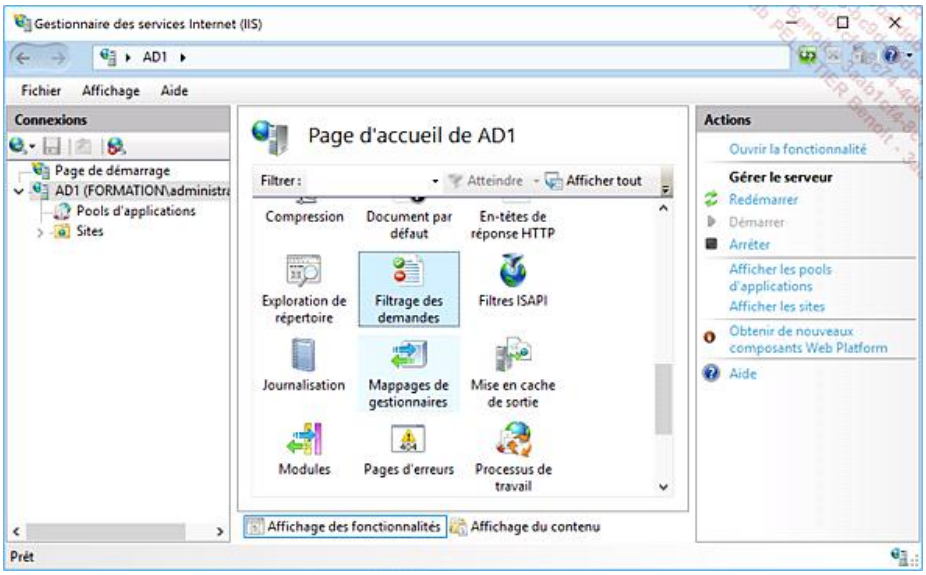
- 5985 pour WinRM,
- 5986 pour WinRMS.

Dans le cas où le serveur collecteur (serveur qui est en charge de récupérer les différents événements) fonctionne sous Windows Server 2012 R2, la KB2919355 doit être installée : https://www.microsoft.com/fr-FR/download/details.aspx?id=42334

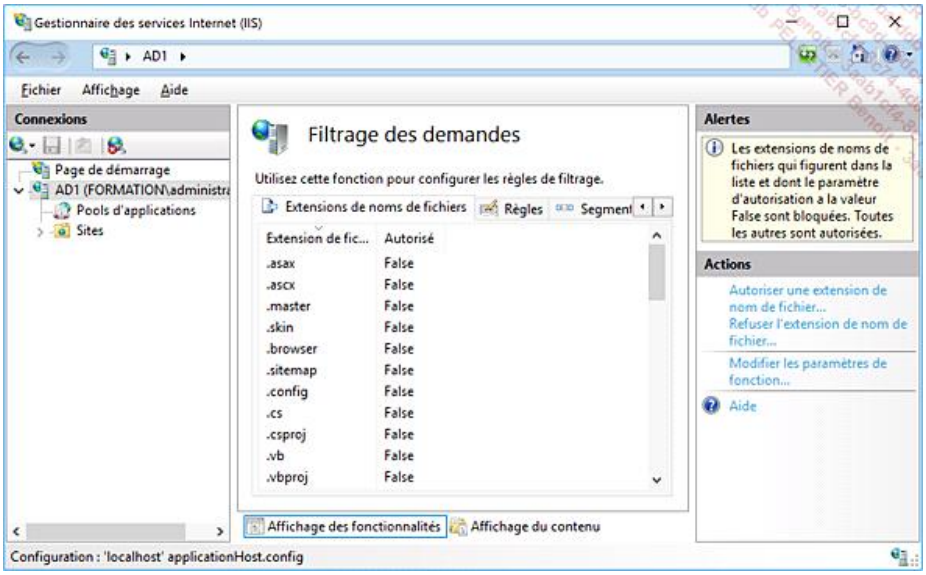
a. Configuration des prérequis pour le chiffrement

Avant toute chose, nous allons procéder à l'activation de WinRM. L'autorité de certification a été installée sur AD1 dans le précédent chapitre. La même autorité de certification va être utilisée.

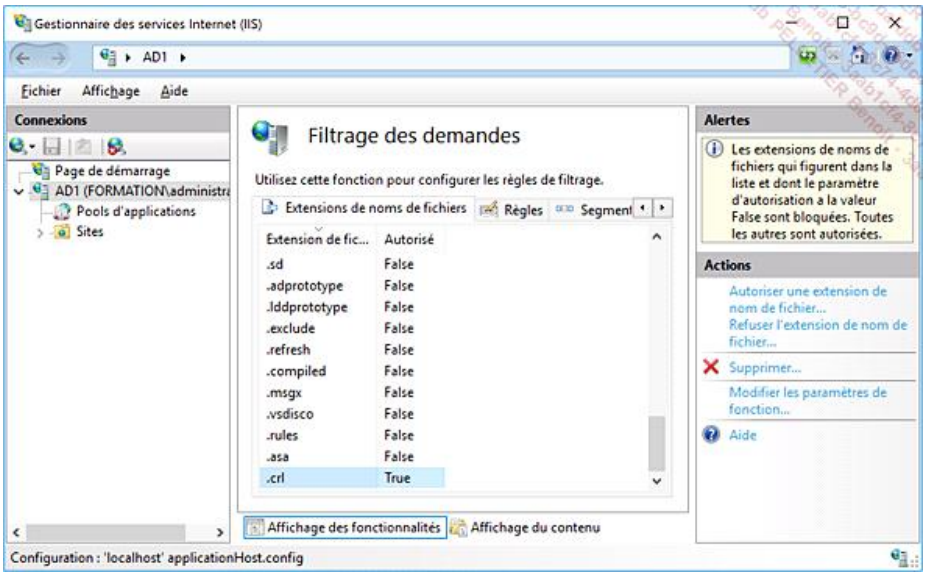
- Sur AD1, accédez à la console **Internet Information Services (IIS) Manager**, sélectionnez le serveur puis double cliquez sur **Filtrage des demandes** dans le panneau central.



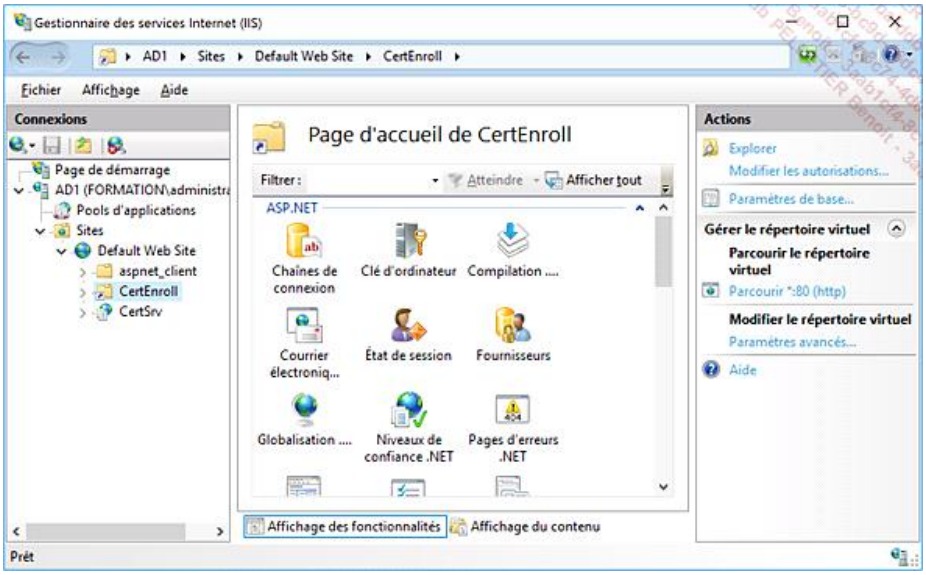
- Dans le bandeau **Actions**, cliquez sur **Autoriser une extension de nom de fichier**.



Saisissez **.crl** dans le champ puis cliquez sur **OK**.

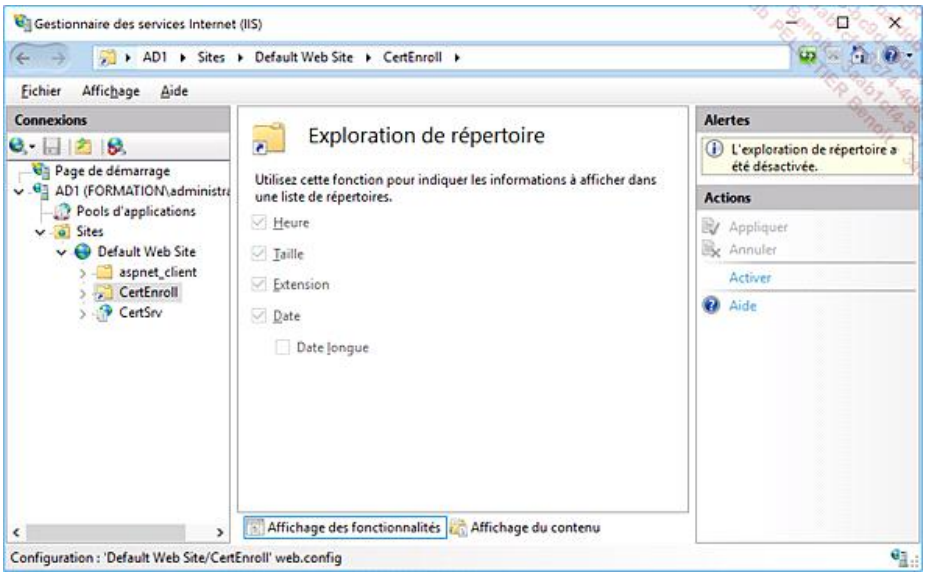


Développez le nœud **Sites** puis **Default Web Site** et cliquez sur **CertEnroll**.



Dans le panneau central, cliquez sur **Exploration de répertoire** puis sur **Activer** dans le panneau

Actions.

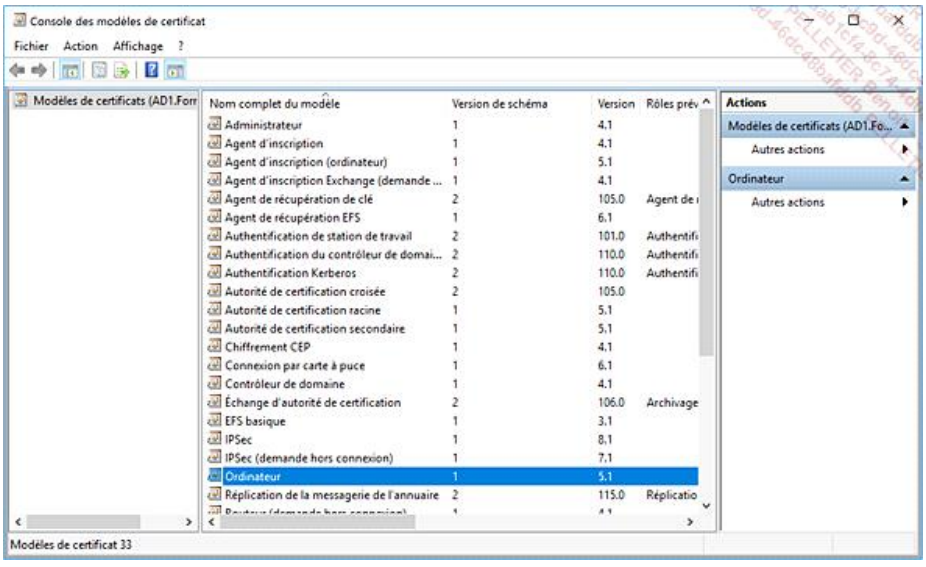


- Dans une invite de commandes DOS, exécutez la commande `IISRESET` afin que les modifications soient prises en compte.

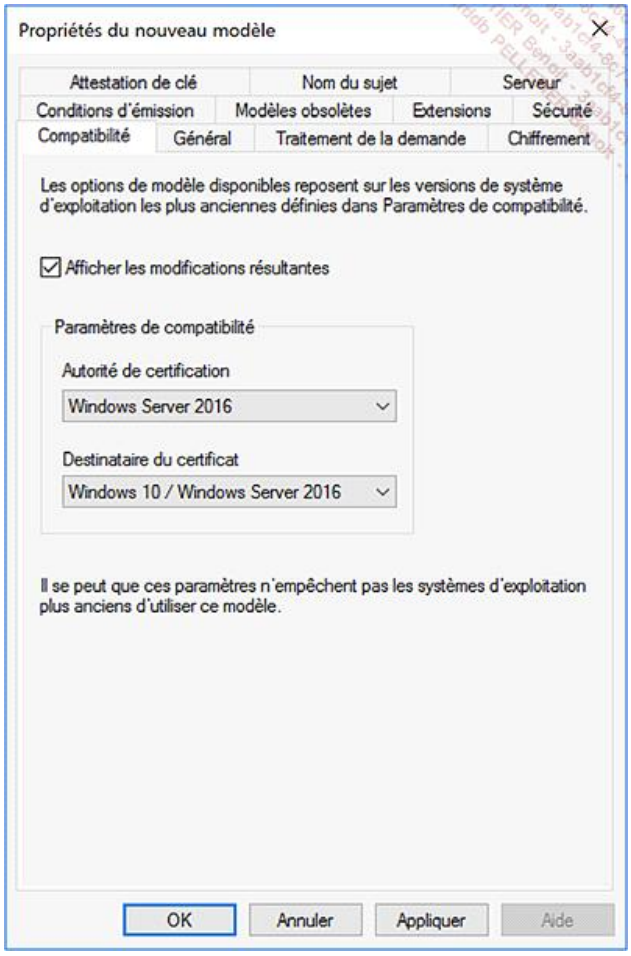
La création du modèle de certificat peut maintenant être effectuée.

b. Création du modèle de certificat

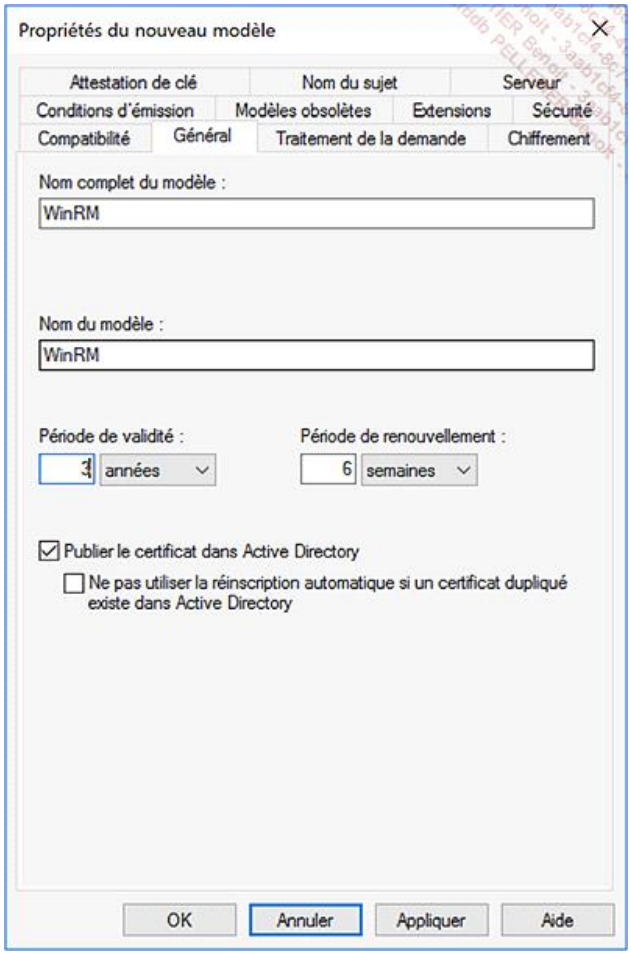
- Depuis l'autorité de certification présente sur **AD1**, accédez à la console **Autorité de certification**. Effectuez un clic droit sur **Modèles de certificat** puis cliquez sur **Gérer** dans le menu contextuel.
- Sélectionnez le modèle **Ordinateur** puis effectuez un clic droit sur ce dernier. Dans le menu contextuel, sélectionnez **Dupliquer le modèle**.



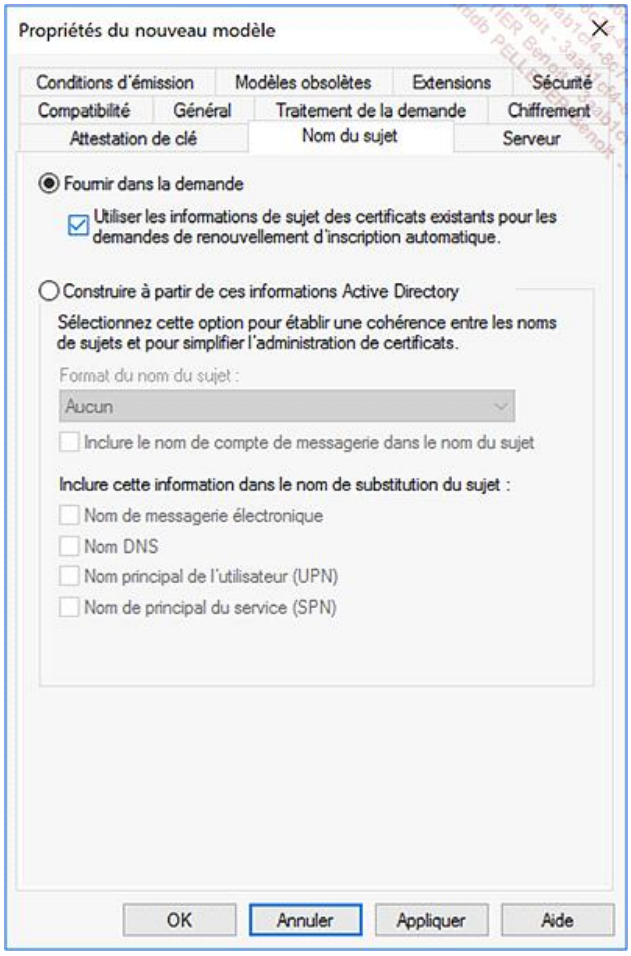
- Dans l'onglet **Compatibilité**, configurez les paramètres de compatibilité comme souhaité.



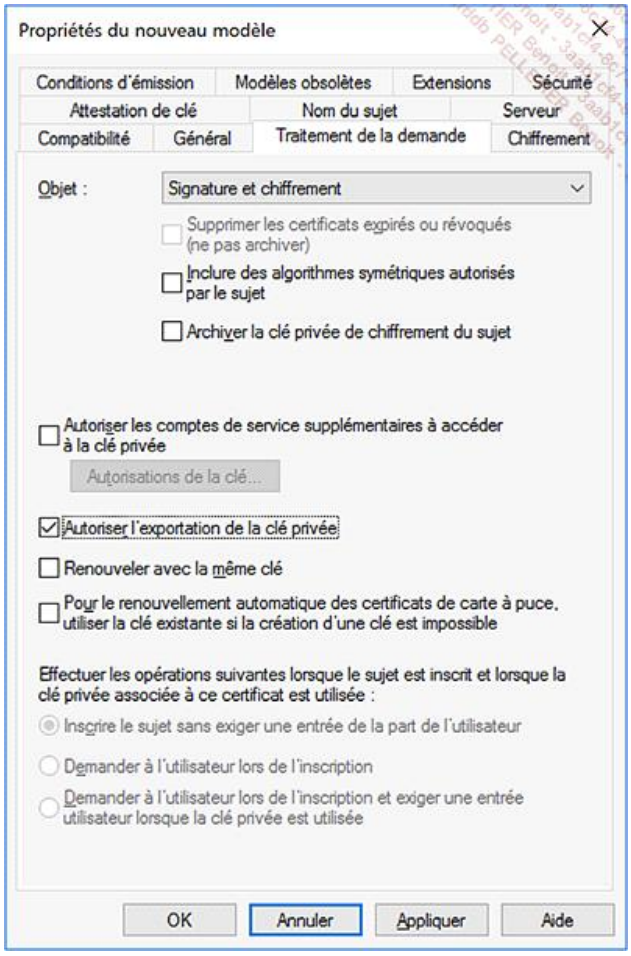
- Dans l'onglet **Général**, saisissez le nom du modèle puis cochez la case **Publier le certificat dans Active Directory**, et saisissez la période de validité souhaitée.



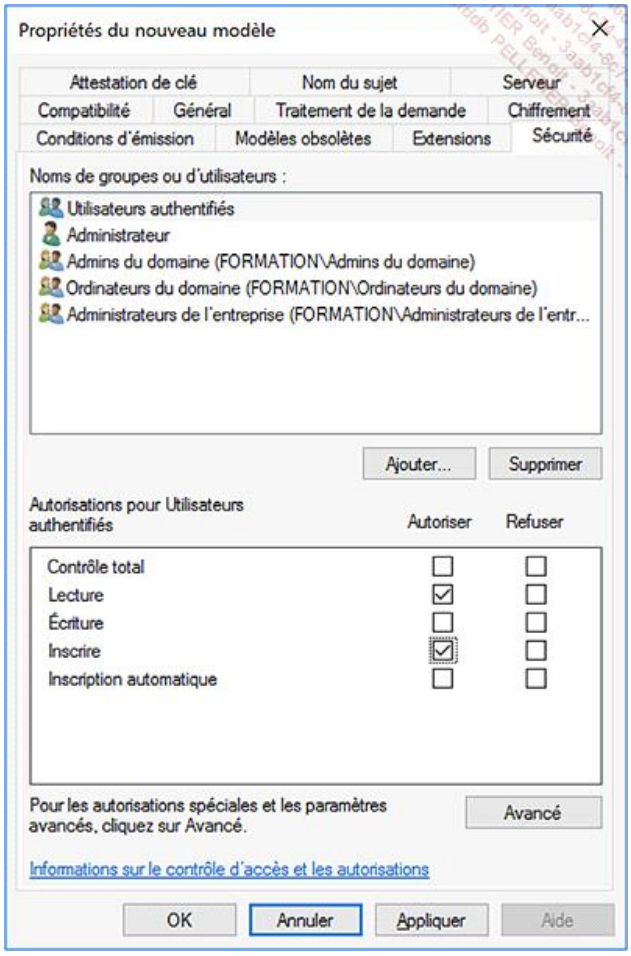
- Dans l'onglet **Nom du sujet**, cochez le bouton radio **Fournir dans la demande** puis cochez **Utiliser les informations de sujet des certificats existants pour les demandes de renouvellement d'inscription automatique**.



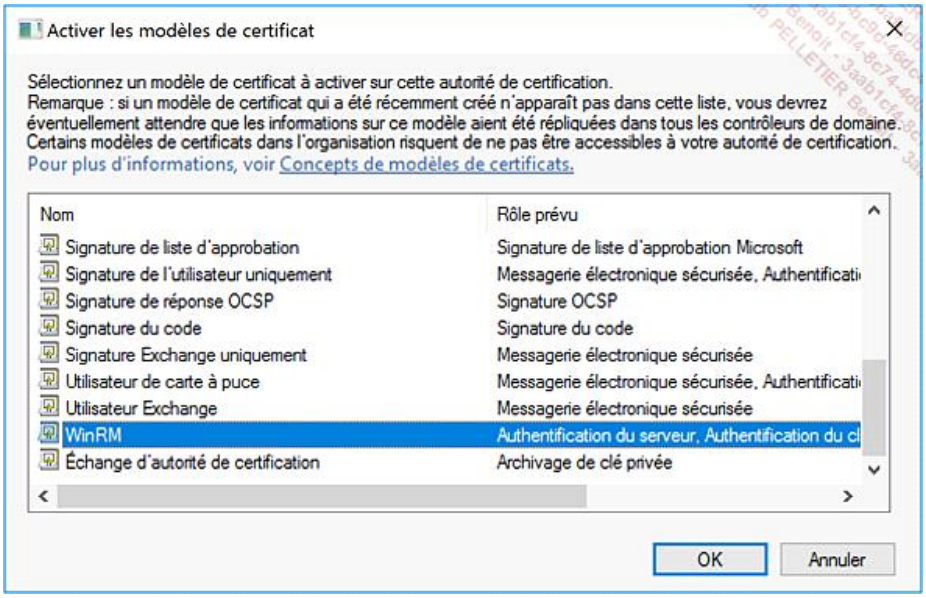
- Dans l'onglet **Traitement de la demande**, cochez **Autoriser l'exportation de la clé privée**.



- Dans l'onglet **Sécurité**, ajoutez le droit **Inscrire** au groupe **Utilisateurs authentifiés**.

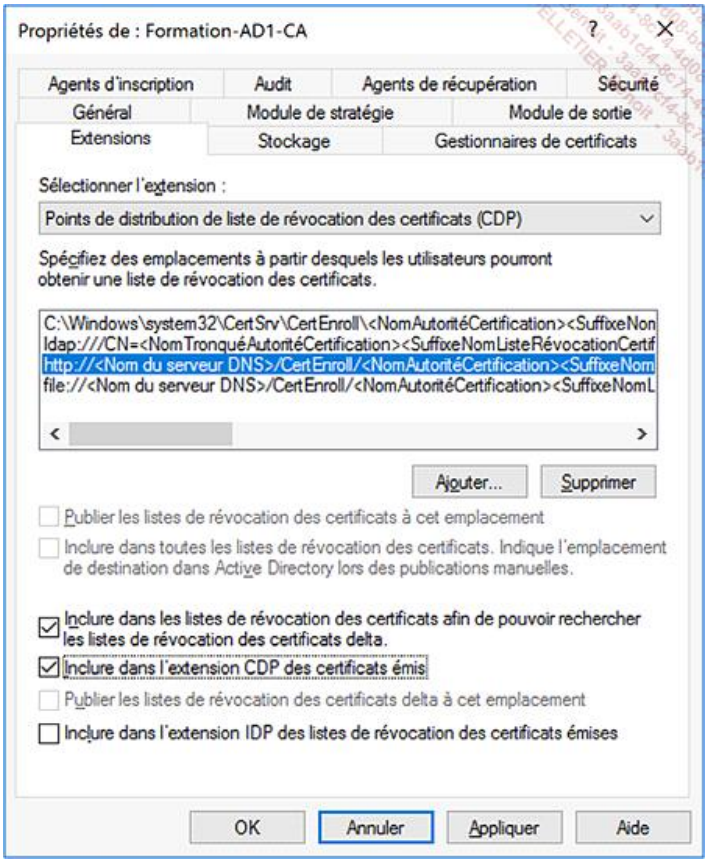


- Cliquez sur **OK** puis fermez la fenêtre **Console des modèles de certificat**. Effectuez un clic droit sur **Modèles de certificat** puis, dans le menu contextuel, cliquez sur **Nouveau** et **Modèle de certificat à délivrer**. Sélectionnez le modèle **WinRM** puis cliquez sur **OK**.

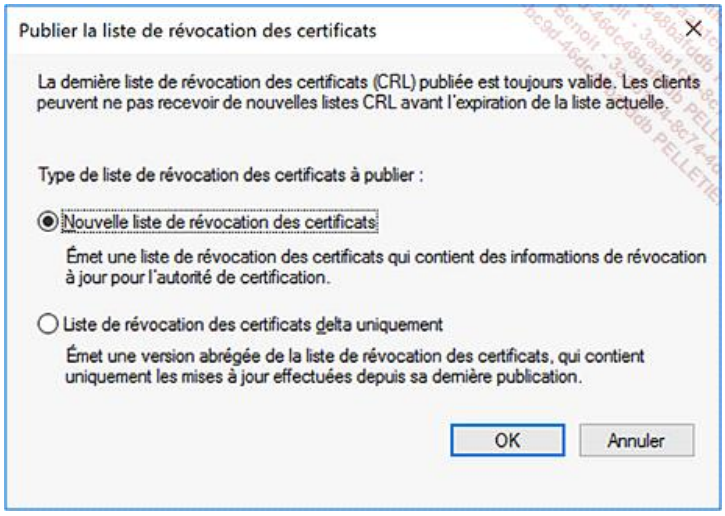


- La configuration de l'autorité de certification est quasiment terminée. Effectuez un clic droit sur le serveur puis, dans le menu contextuel, sélectionnez **Propriétés**. Une fenêtre s'affiche, cliquez sur **Extensions**.

- Sélectionnez la ligne **http** puis cochez les cases **Inclure dans les listes de révocation des certificats afin de pouvoir rechercher les listes de révocation des certificats delta** et **Inclure dans l'extension CDP des certificats émis**.



Cliquez sur **Appliquer** puis sur **OK** puis redémarrez les services. Dans la console **Autorité de certification**, effectuez un clic droit sur le dossier **Certificats révoqués** puis cliquez sur **Toutes les tâches** - **Publier**. Dans l'assistant, sélectionnez **Nouvelle liste de révocation des certificats**.



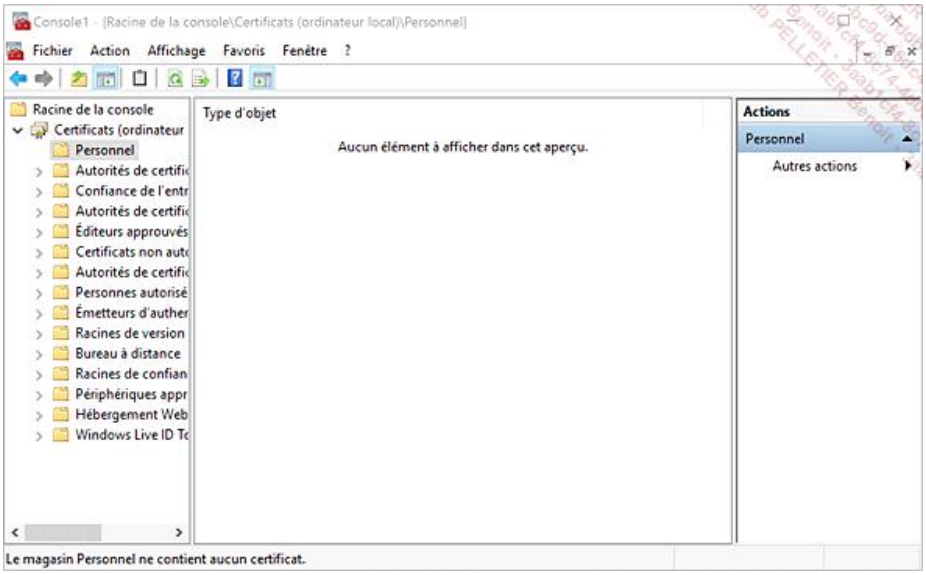
c. Mise en place des certificats

La configuration de l'autorité de certification est maintenant effectuée. Nous pouvons désormais débuter la mise en place des certificats. Notez que si vous souhaitez récupérer des événements sur des postes et serveurs en Workgroup, la demande de certificats devra être effectuée depuis un serveur membre du domaine puis exportée. Il est également nécessaire d'importer le certificat Root dans le bon magasin.

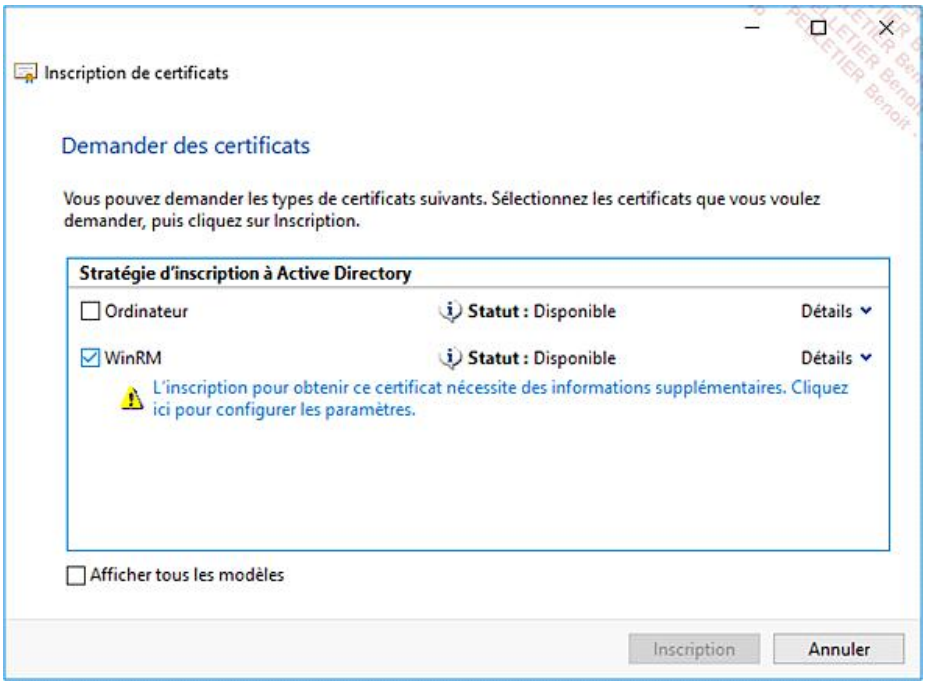
Dans notre cas, l'ensemble des serveurs sont membres de l'AD, il n'est donc pas nécessaire de procéder à la demande du certificat sur un autre serveur.

SV1 possède le rôle de collecteur, le serveur AD2 est, lui, le serveur collecté.

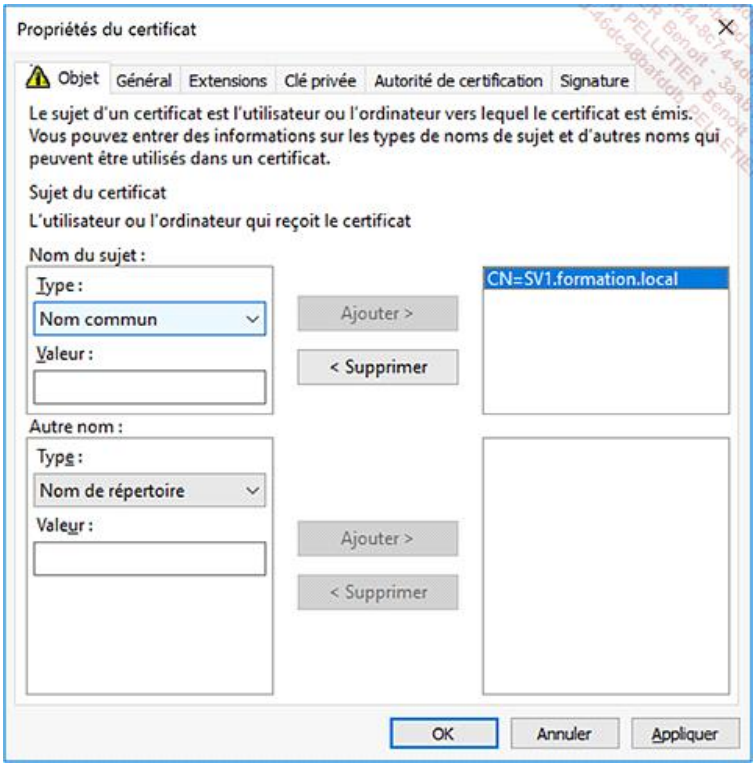
- Depuis le serveur **SV1**, accédez à la console **mmc** puis ajoutez le logiciel enfichable **Certificats**. Dans l'assistant, sélectionnez **Compte ordinateur** puis cliquez sur **OK**.



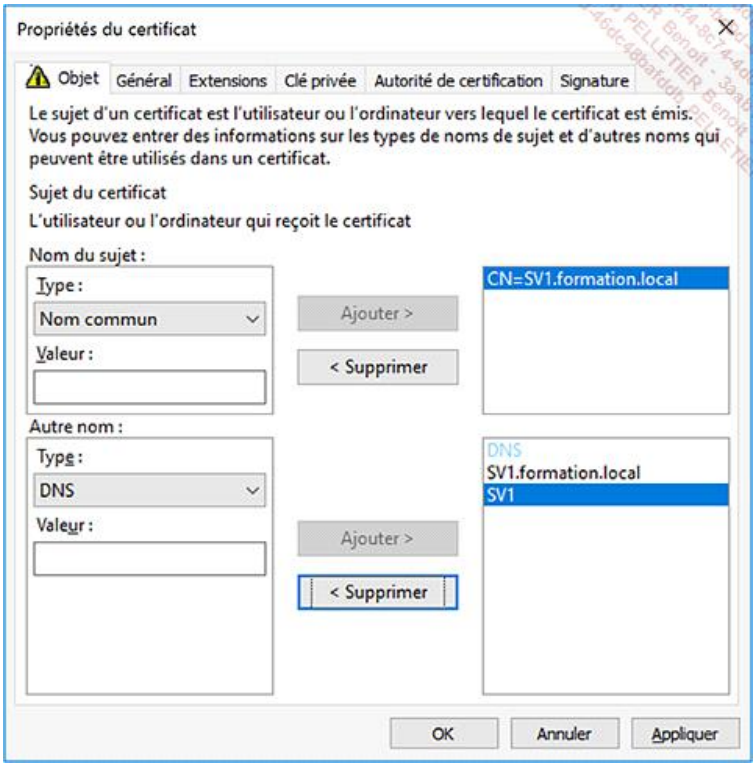
- Accédez au dossier **Personnel** puis effectuez un clic droit. Dans le menu contextuel, cliquez sur **Toutes les tâches** et **Demander un nouveau certificat**.
- Cliquez deux fois sur **Suivant** puis sélectionnez le modèle créé précédemment.



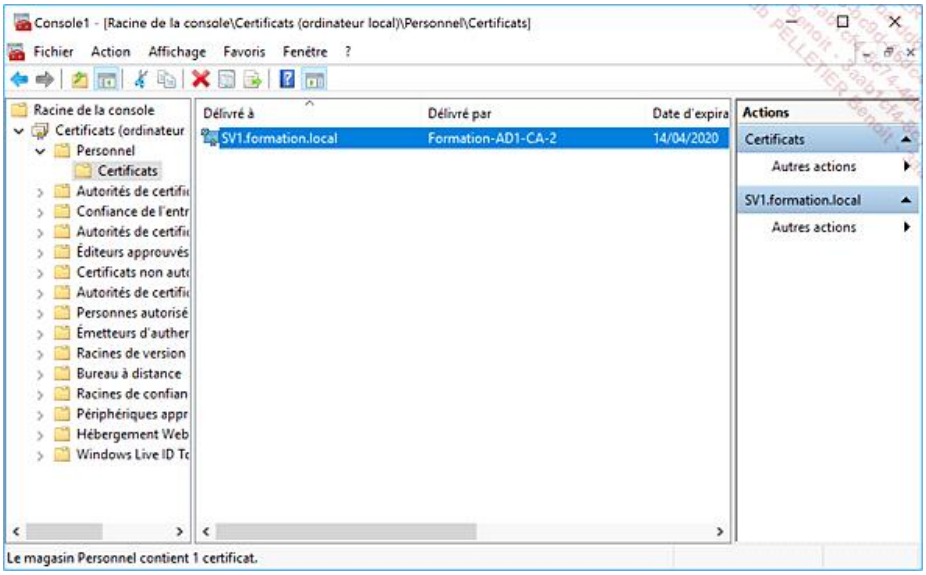
- Cliquez sur **L'inscription pour obtenir ce certificat nécessite des informations supplémentaires**.
- Dans la liste déroulante **Nom du sujet**, sélectionnez **Nom commun** puis insérez le FQDN du serveur (srv.domain.local). Cliquez sur **Ajouter** pour insérer la valeur.



- Dans la liste déroulante **Autre nom**, sélectionnez **DNS** puis insérez le nom FQDN et NetBIOS du serveur. Cliquez sur **Ajouter** entre chaque.



- Cliquez sur **OK** puis sur **Inscription**. Après avoir cliqué sur **Terminer**, le certificat est présent dans la console.

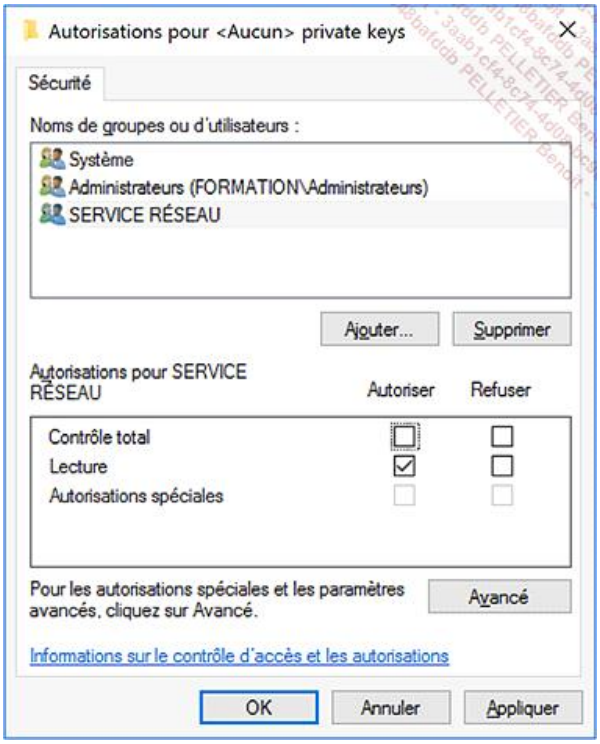


Recommencez la même opération sur le serveur AD2. Attention à bien changer le nom.

d. Autorisation de gestion des clés privées

L'opération suivante doit être effectuée uniquement sur les postes/serveurs sources exécutant Windows 7/Windows Server 2008 R2 ou version ultérieure. Aucun événement ne sera envoyé tant que le droit n'aura pas été accordé.

- Sur le serveur **AD2**, sélectionnez le dossier **Certificats** présent dans **Personnel** puis effectuez un clic droit sur le certificat précédemment importé.
- Dans le menu contextuel, cliquez sur **Toutes les tâches** puis sur **Gérer les clés privées**.
- Accordez le droit **Lecture** au compte **SERVICE RÉSEAU** puis cliquez sur **OK**.



L'opération doit être effectuée sur l'ensemble des serveurs sources.

e. Configuration du listener WinRM

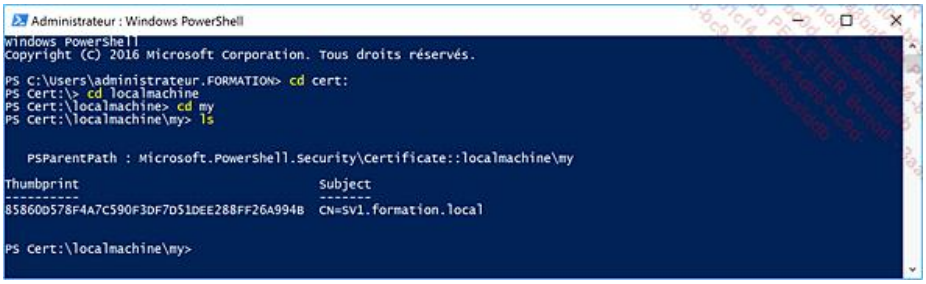
Le listener WinRM utilisé par le collecteur et les machines collectées doit être configuré afin d'utiliser le protocole HTTPS.

- Sur **SV1**, ouvrez une invite de commandes DOS puis exécutez la commande `WinRM qc` puis la commande `wecutil qc`.



- Exécutez une invite de commandes PowerShell ou saisissez PowerShell dans la console DOS. L'invite de commandes DOS est nécessaire après l'exécution des commandes ci-dessous.
- Saisissez les commandes suivantes afin de récupérer l'empreinte numérique du certificat. Le but de ces commandes est d'accéder au magasin de certificats ordinateur puis d'afficher les propriétés du certificat.

```
cd cert:
cd localmachine
cd my
ls
```



- L'empreinte numérique du certificat (thumbprint) apparaît. Copiez la valeur, elle est nécessaire par la suite.
- Depuis l'invite de commandes DOS, exécutez la commande suivante afin de procéder à la création du listener HTTPS. Remplacez "serverfqdn" par le nom FQDN du serveur et "EmpreinteNumérique" par l'empreinte numérique du certificat.

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="serverfqdn";CertificateThumbprint="EmpreinteNumérique"}
```

La commande peut être téléchargée depuis la page Informations générales.



- Supprimez le listener HTTP à l'aide de la commande `winrm delete winrm/config/Listener?Address=*+Transport=http`

La commande peut être téléchargée depuis la page Informations générales.



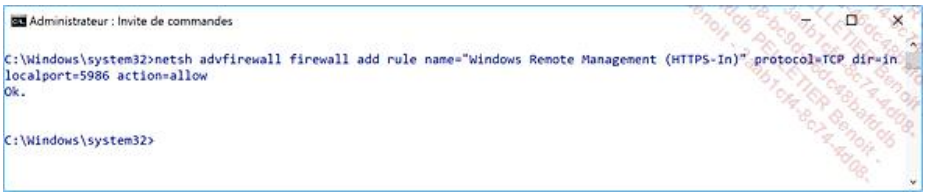
Le listener HTTPS est le seul listener qui peut être utilisé.



Dans le cas où le pare-feu est actif, il est nécessaire d'activer l'exception adéquate.

- Depuis l'invite de commandes DOS, exécutez la commande `netsh advfirewall firewall add rule name="Windows Remote Management (HTTPS-In)" protocol=TCP dir=in localport=5986 action=allow`

La commande peut être téléchargée depuis la page Informations générales.

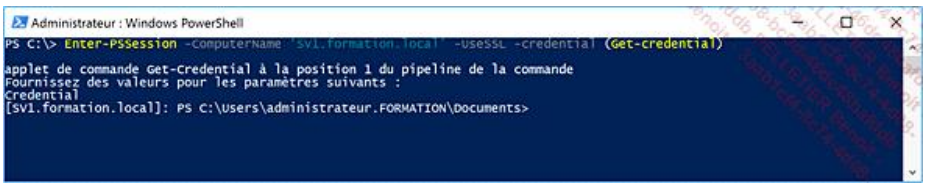


Exécutez les mêmes opérations sur AD2 afin de procéder à la création du listener HTTPS. Suite à la configuration de AD2 et afin de vérifier la bonne configuration, il est nécessaire de procéder à l'établissement d'une connexion WinRMs.

- Depuis le serveur SV1, lancez une invite de commandes PowerShell puis saisissez la commande `Enter-PSSession -ComputerName 'AD2.formation.local' -UseSSL -credential (Get-credential)`

La commande peut être téléchargée depuis la page Informations générales.

La connexion est bien établie sur le serveur.



L'abonnement peut maintenant être créé et configuré.

f. Configuration de l'abonnement

Après avoir configuré les listeners HTTPS, il est nécessaire de procéder à la configuration de l'abonnement.

- Depuis le serveur SV1, accédez à la base de registre puis procédez à la création de la clé DWORD ClientAuthTrustMode afin qu'elle ait la valeur 2. Cette clé DWORD est présente dans

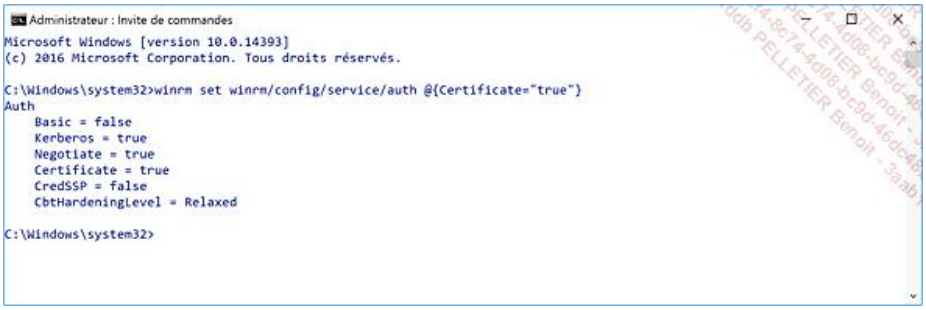
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL.



Le listener doit être configuré pour prendre en charge l'authentification basée sur un certificat.

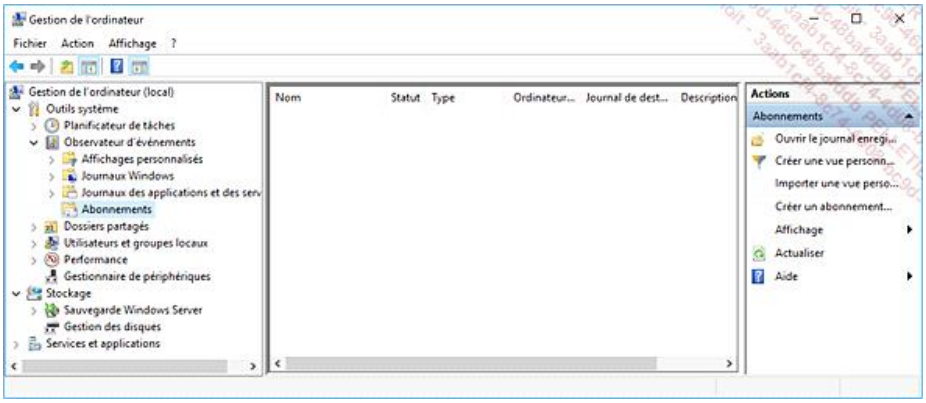
- Lancez une invite de commandes puis exécutez la commande `winrm set winrm/config/service/auth @{Certificate="true"}`

  Recommencez la même opération sur le serveur AD2.

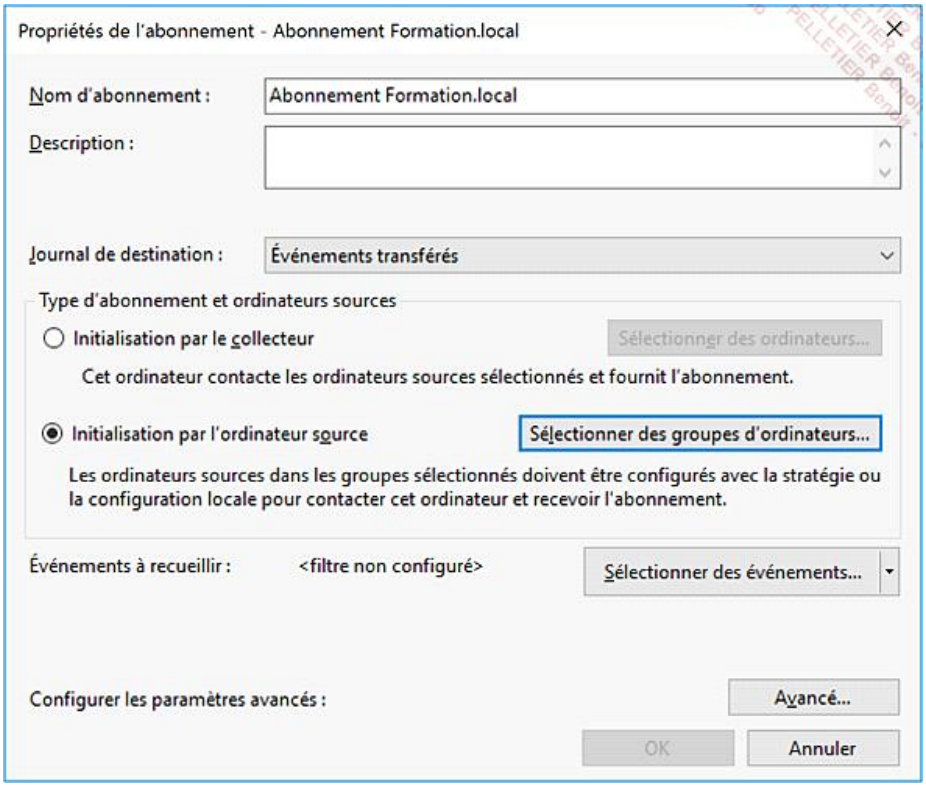


Nous pouvons procéder à la création de l'abonnement.

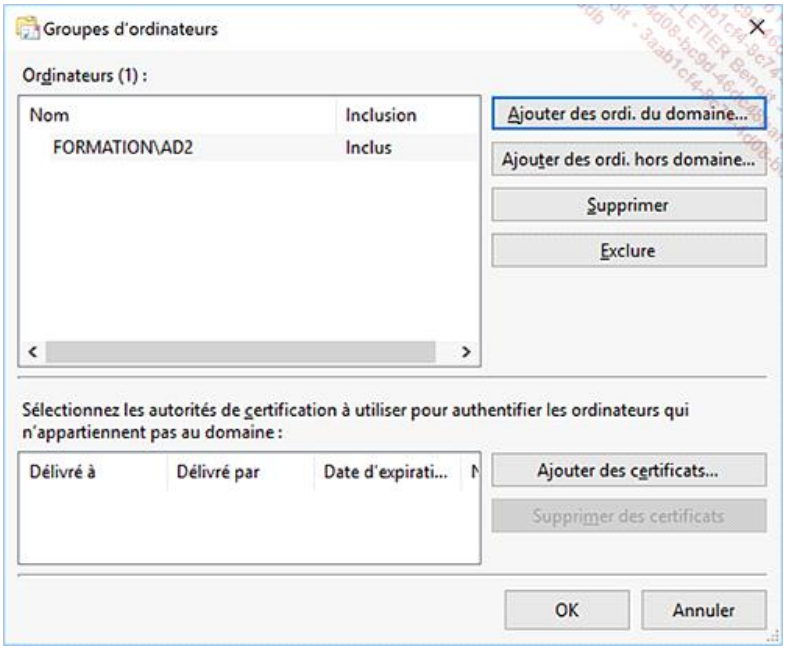
- Sur **SV1**, accédez à la console **Gestion de l'ordinateur** puis, dans le noeud **Observateur d'événements**, sélectionnez **Abonnements**.



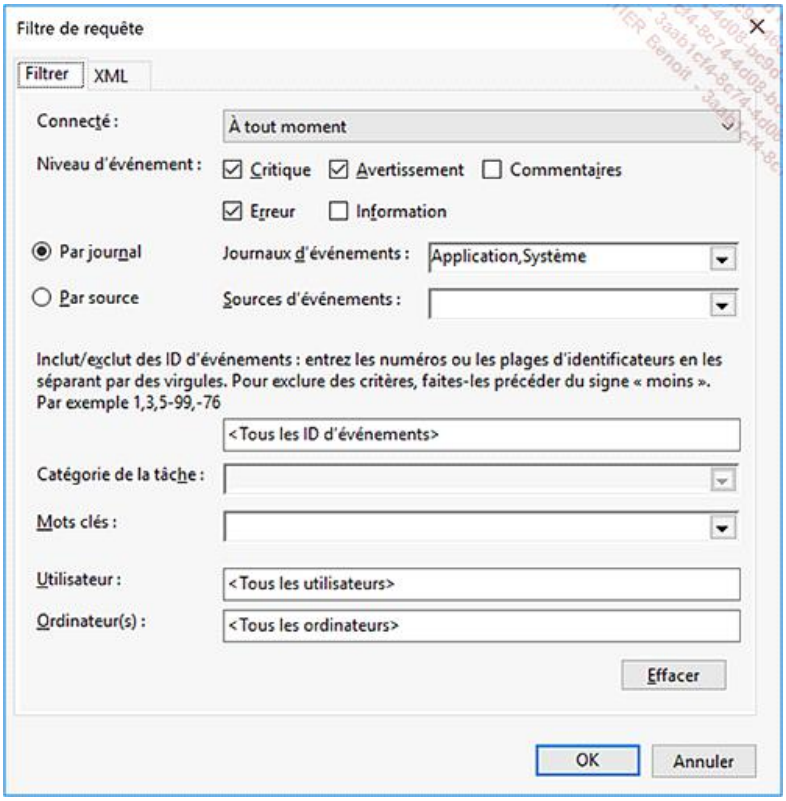
- Cliquez sur **Créer un abonnement** et saisissez le nom de l'abonnement.
- Cochez le bouton radio **Initialisation par l'ordinateur source** puis cliquez sur **Sélectionner des groupes d'ordinateurs...**.



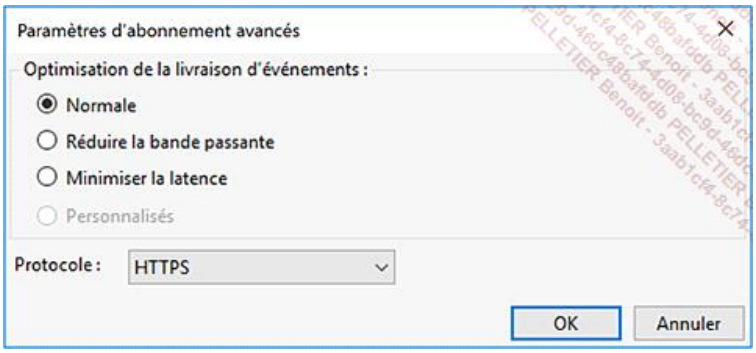
- Cliquez sur le bouton **Ajouter des ordi. du domaine...** puis saisissez **AD2**.



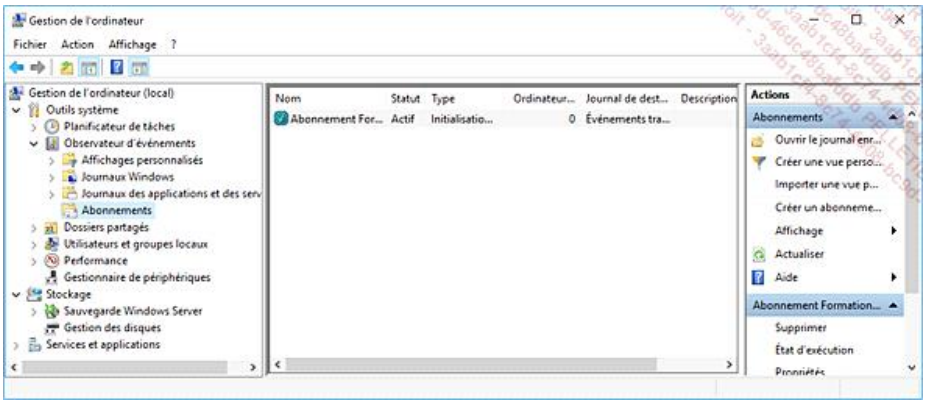
- Cliquez sur **OK** puis, dans les propriétés de l'abonnement, cliquez sur **Sélectionner des événements**.
- Configurez le filtre de requête comme souhaité puis cliquez sur **OK**.



Cliquez sur **Avancé** puis sélectionnez dans la liste déroulante le protocole **HTTPS**.



Validez les différentes fenêtres, l'abonnement est correctement créé.

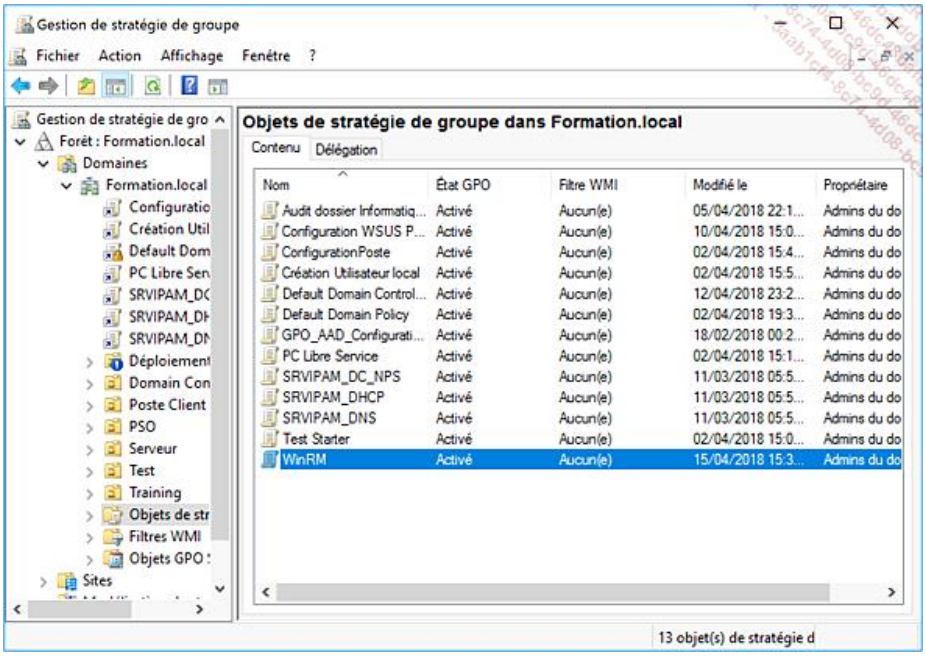


g. Configuration des postes/serveurs

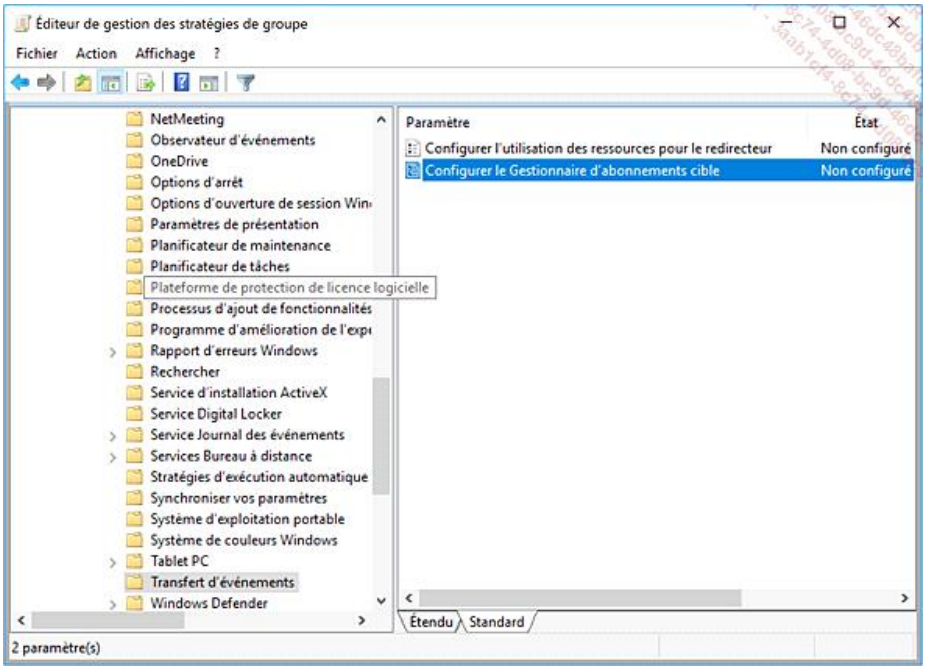
Les postes de travail et/ou serveurs peuvent maintenant être configurés pour être rattachés à l'abonnement. Cette configuration s'effectue par le biais d'une stratégie de groupe.

Sur **AD1**, ouvrez la console **Gestion des stratégies de groupe** depuis les outils d'administration.

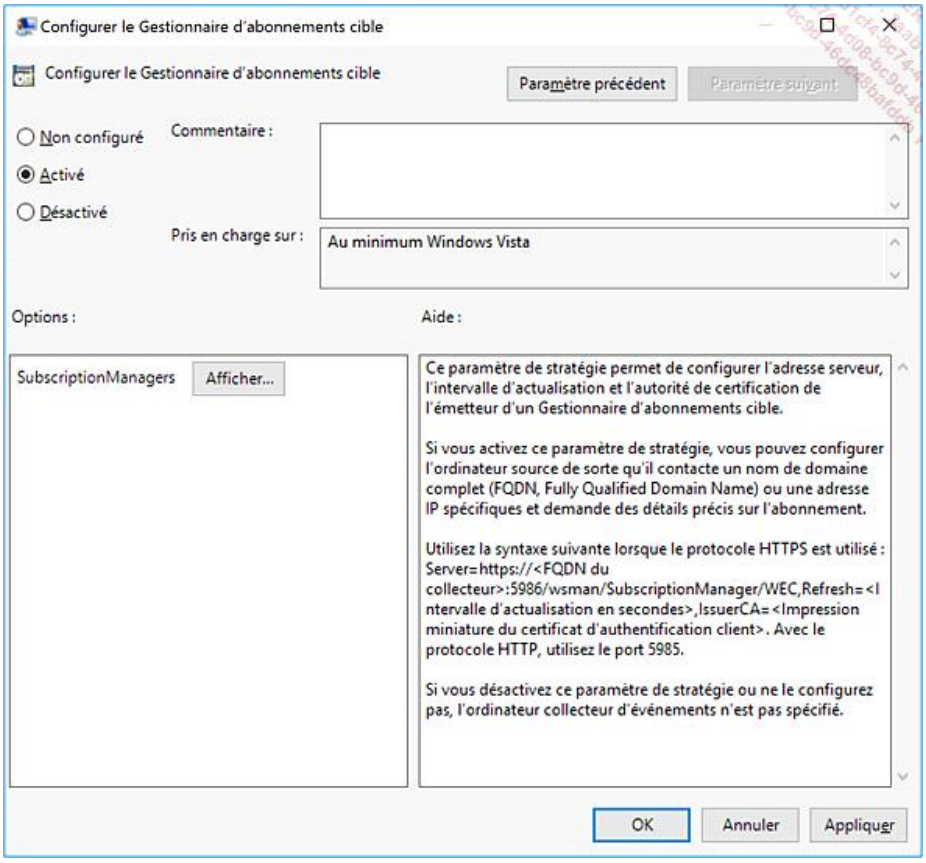
- Effectuez un clic droit sur **Objets de stratégie de groupe** puis cliquez sur **Nouveau**. Saisissez **WinRM** dans la fenêtre qui s'affiche puis cliquez sur **OK**.



- Effectuez un clic droit sur la stratégie de groupe puis cliquez sur **Modifier**.
- Développez les nœuds **Configuration ordinateur** - **Modèles d'administration** - **Composants Windows** - **Transfert d'événements**, puis double cliquez sur **Configurer le Gestionnaire d'abonnements cible**.

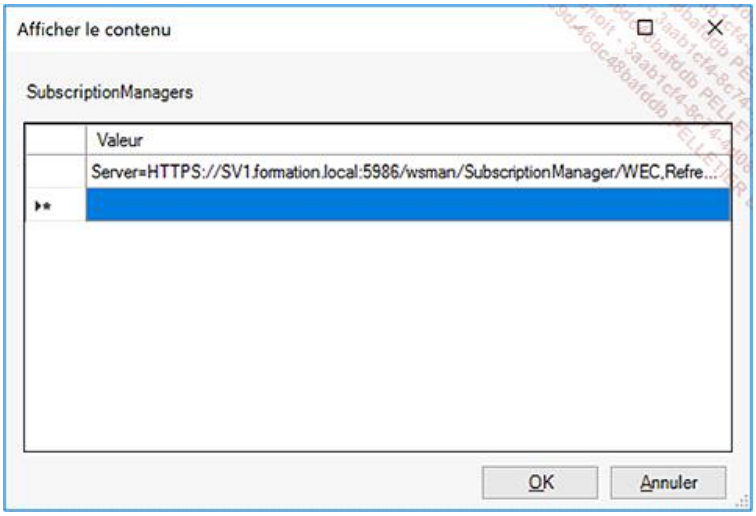


- Cochez le bouton radio **Activé** puis cliquez sur le bouton **Afficher**.

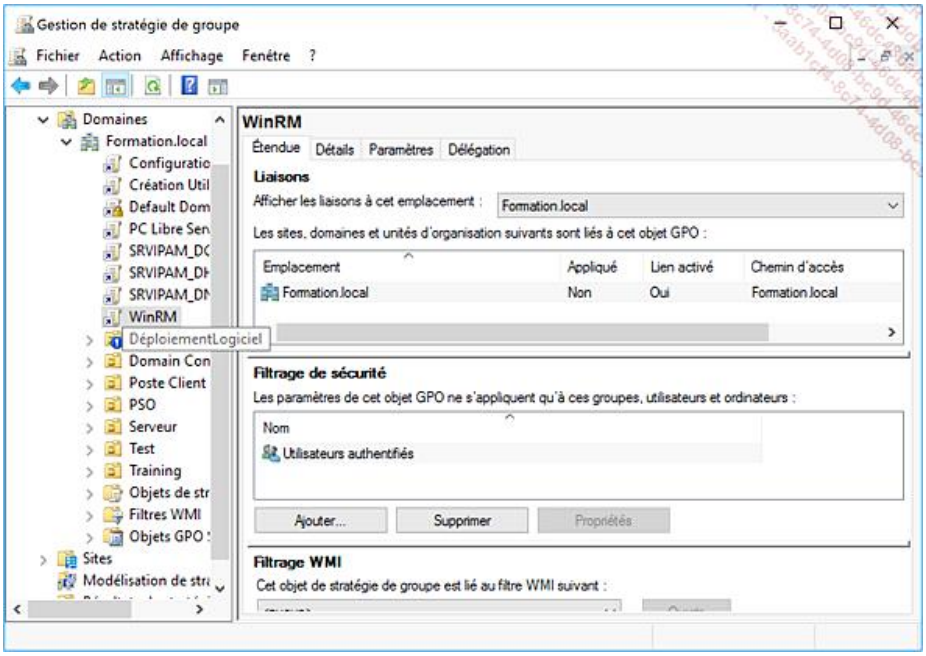


- La valeur du paramètre est la suivante. Remplacez <FQDN du serveur> par le nom FQDN du serveur qui a le rôle de collecteur, <Temps de rafraîchissement en secondes> par le temps de rafraîchissement souhaité (en secondes / minimum 10 secondes).

```
Server=HTTPS://<FQDN du serveur>:5986/wsman/SubscriptionManager/
WEC,Refresh=<Temps de rafraîchissement en secondes>
```

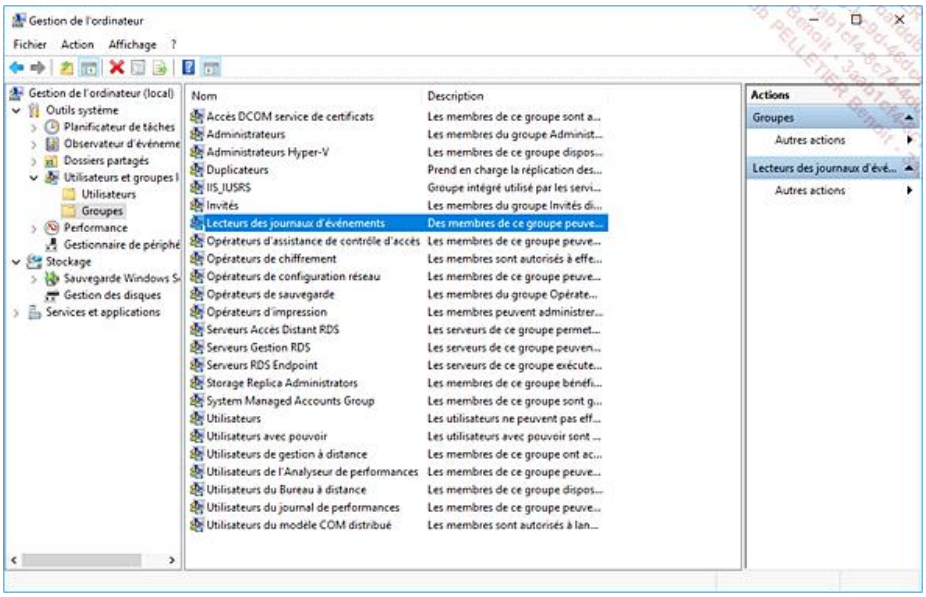


- Cliquez deux fois sur **OK** puis fermez l'éditeur de stratégie de groupe. Liez la stratégie de groupe à l'unité d'organisation ou la racine du domaine afin que **AD2** récupère la stratégie de groupe.

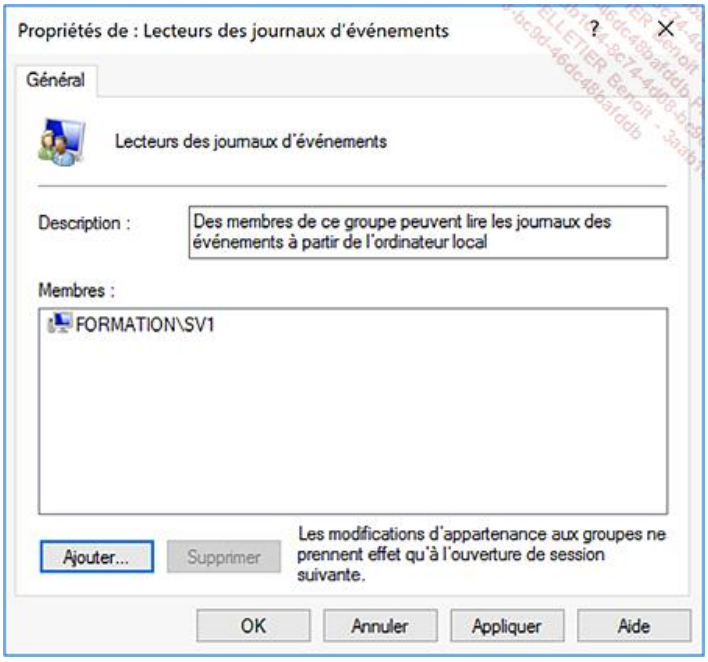


Il est nécessaire de rajouter le compte ordinateur du collecteur dans le groupe local Lecteurs des journaux d'événements. Ce dernier est présent avec les autres groupes locaux. Les contrôleurs de domaine ne possédant pas de groupes locaux, il est nécessaire de procéder à cette opération depuis la console **Utilisateurs et ordinateurs Active Directory**.

- Sur **AD2**, accédez à la console **Gestion de l'ordinateur** puis développez le nœud **Utilisateurs et groupes locaux**. Cliquez sur le dossier **Groupes** puis effectuez un double clic sur le groupe **Lecteurs des journaux d'événements**.

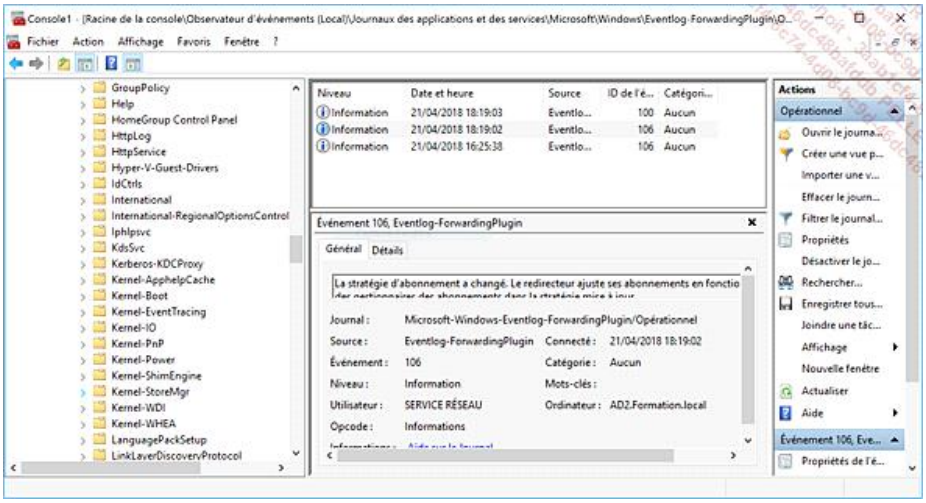


- Dans le groupe, ajoutez le compte ordinateur de SV1.

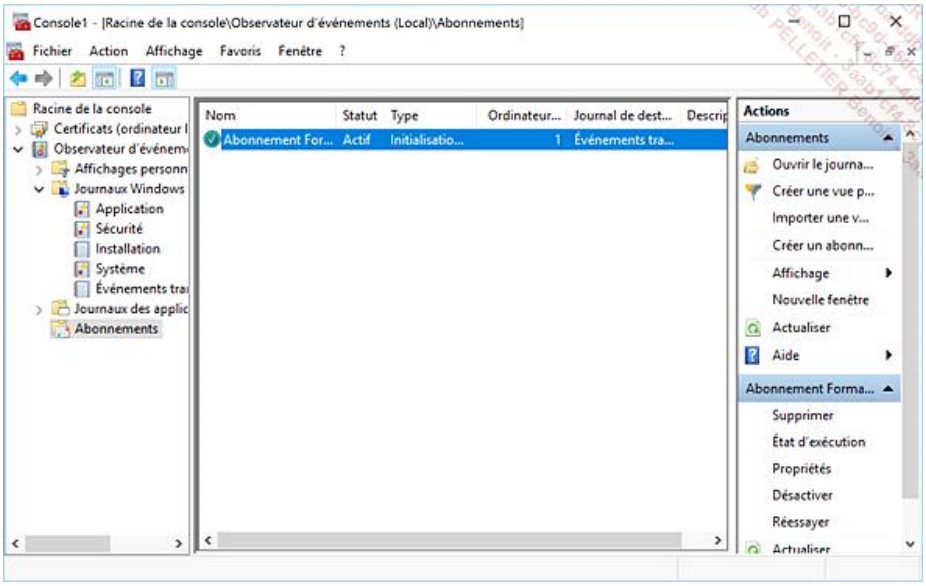


- Exécutez la commande `gpupdate /force` afin de forcer l'application des paramètres de stratégie de groupe.
- Sur le serveur **AD2**, accédez à **l'Observateur d'événements** puis développez les nœuds **Journaux des applications et des services** puis **Microsoft**, **Windows** et **Eventlog-ForwardingPlugin**.

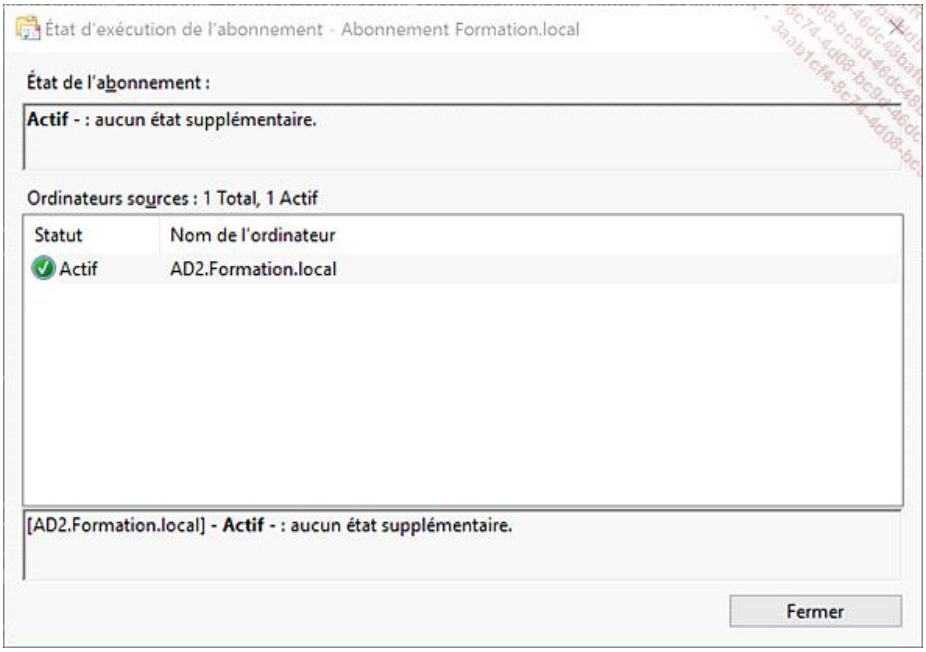
Dans le journal Opérationnel, les événements possédant l'ID 106 et 100 sont bien présents. Ces événements permettent de valider la configuration de l'abonnement.



- Sur le serveur **SV1**, accédez à l'**Observateur d'événements** puis au noeud **Abonnements**. Le chiffre **1** est maintenant présent dans **Ordinateur**.



Effectuez un clic droit sur l'abonnement puis, dans le menu contextuel, sélectionnez **État d'exécution**. Une fenêtre s'affiche et permet de visualiser les ordinateurs raccordés.



Les événements vont maintenant être envoyés au journal **Événements transférés**.

Le pare-feu sous Windows Server

Depuis Windows XP SP2, les systèmes d'exploitation Microsoft contiennent un pare-feu qui permet de filtrer le trafic en entrée et en sortie du poste.

1. Profil réseau

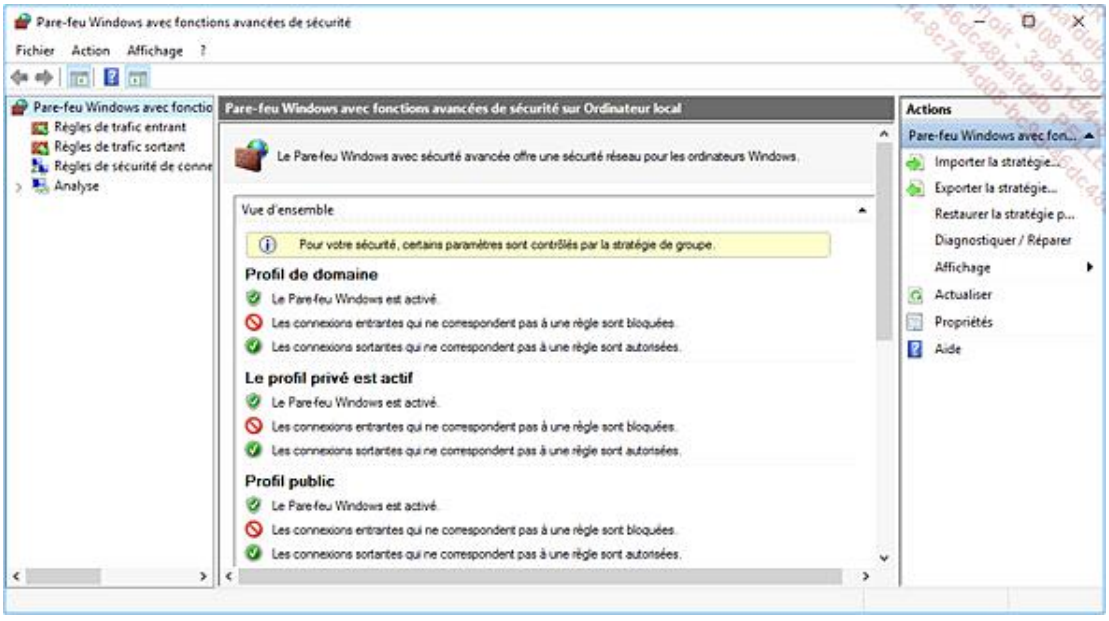
Lors de la première connexion à un réseau, il est nécessaire de choisir le profil réseau souhaité. Les profils sont au nombre de trois. Les règles s'appliquent en fonction du profil (le choix des profils sur lesquels elles s'appliquent se configure dans les propriétés de la règle).

- **Bureau ou réseau avec domaine** : utilisé dans un réseau d'entreprise ou un réseau contenant un contrôleur de domaine. Par défaut, la découverte réseau est désactivée. Le partage de fichiers et d'imprimantes est activé si un partage est présent.
- **Réseau domestique** : principalement utilisé dans de très petits réseaux ou au domicile de l'utilisateur. Ce profil permet d'utiliser la découverte réseau et d'effectuer la création d'un groupe résidentiel.
- **Réseau public** : utilisé lors de la connexion à des hotspots ou simplement sur un réseau dans lequel l'ordinateur ne doit pas être visible. Il est impossible de créer un groupe résidentiel et la découverte réseau est désactivée.

2. Configuration du pare-feu

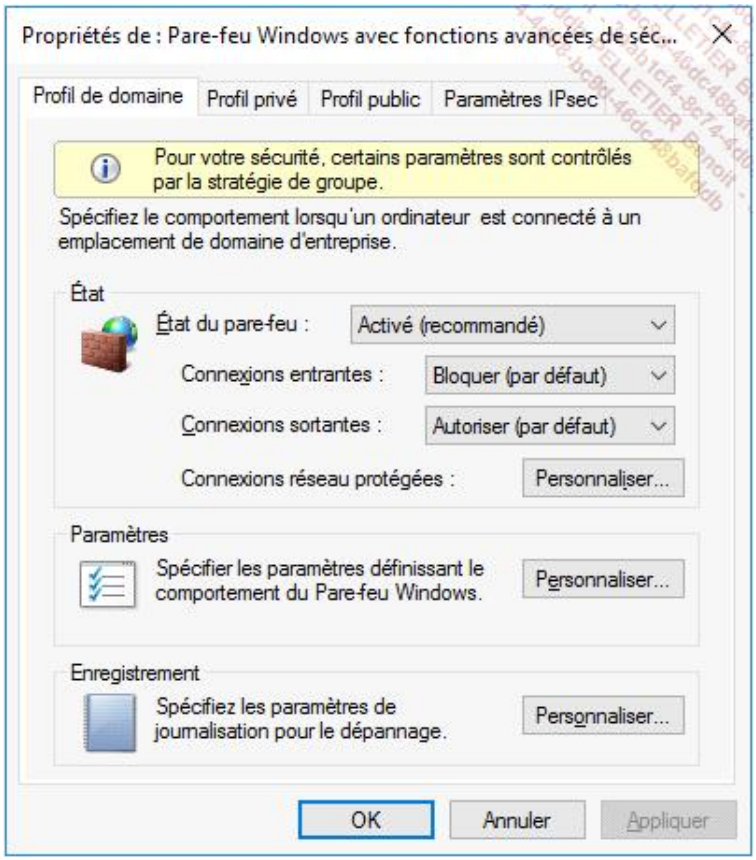
Présente dans le **Panneau de configuration** (catégorie **Système et sécurité** puis **Pare-feu Windows**), la console permet de visualiser les notifications ou d'activer/désactiver le pare-feu. L'activation/désactivation du pare-feu se configure pour chaque profil réseau.

- Sur AD1, affichez le menu Démarrer puis accédez aux **Outils d'administration**.
- Double cliquez sur **Pare-feu Windows avec fonctions avancées de sécurité**.



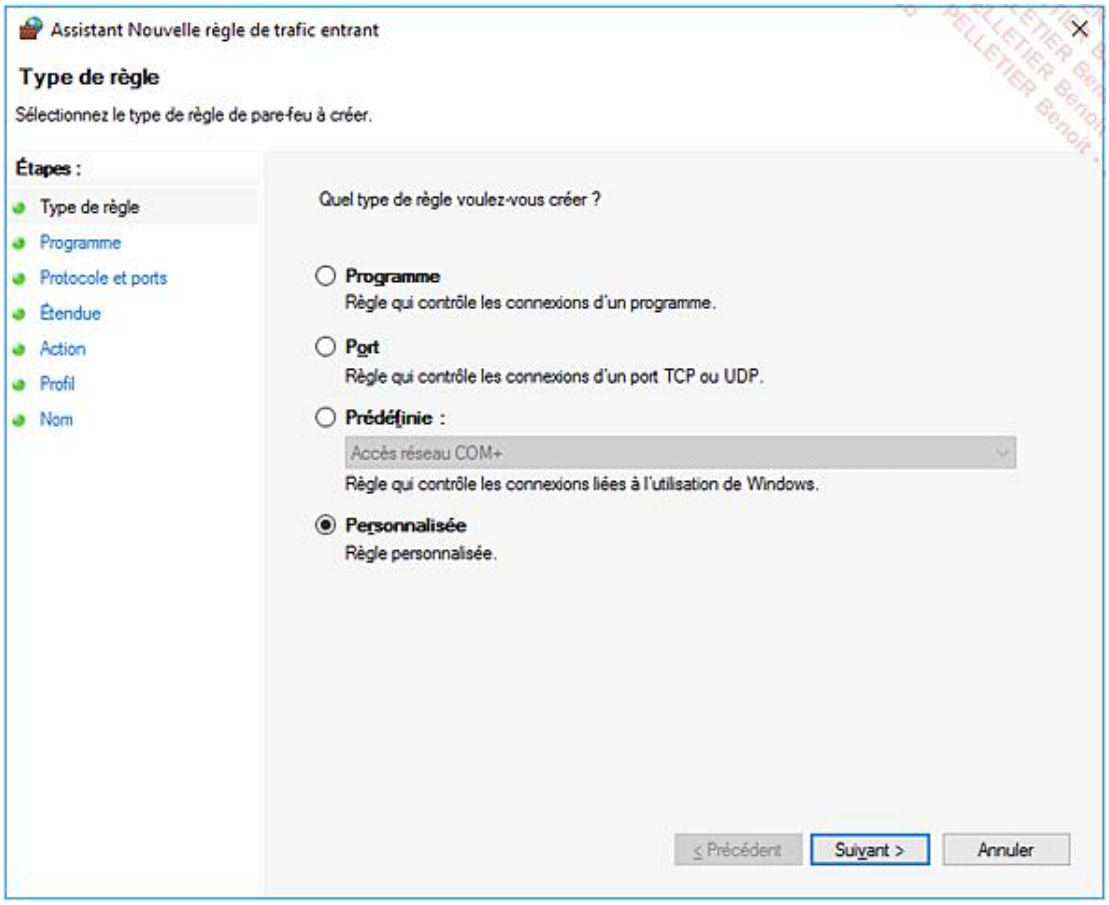
- Cliquez sur **Propriétés** dans le bandeau **Actions**.

Pour chaque profil, il est donc possible de configurer le comportement du pare-feu. Il est maintenant plus simple de le configurer en fonction du réseau sur lequel la machine est branchée.



La console permet la création de règles entrantes, sortantes ou de règles de connexion. Il est également possible d'effectuer des paramétrages avancés (règles par défaut, analyse des règles…).

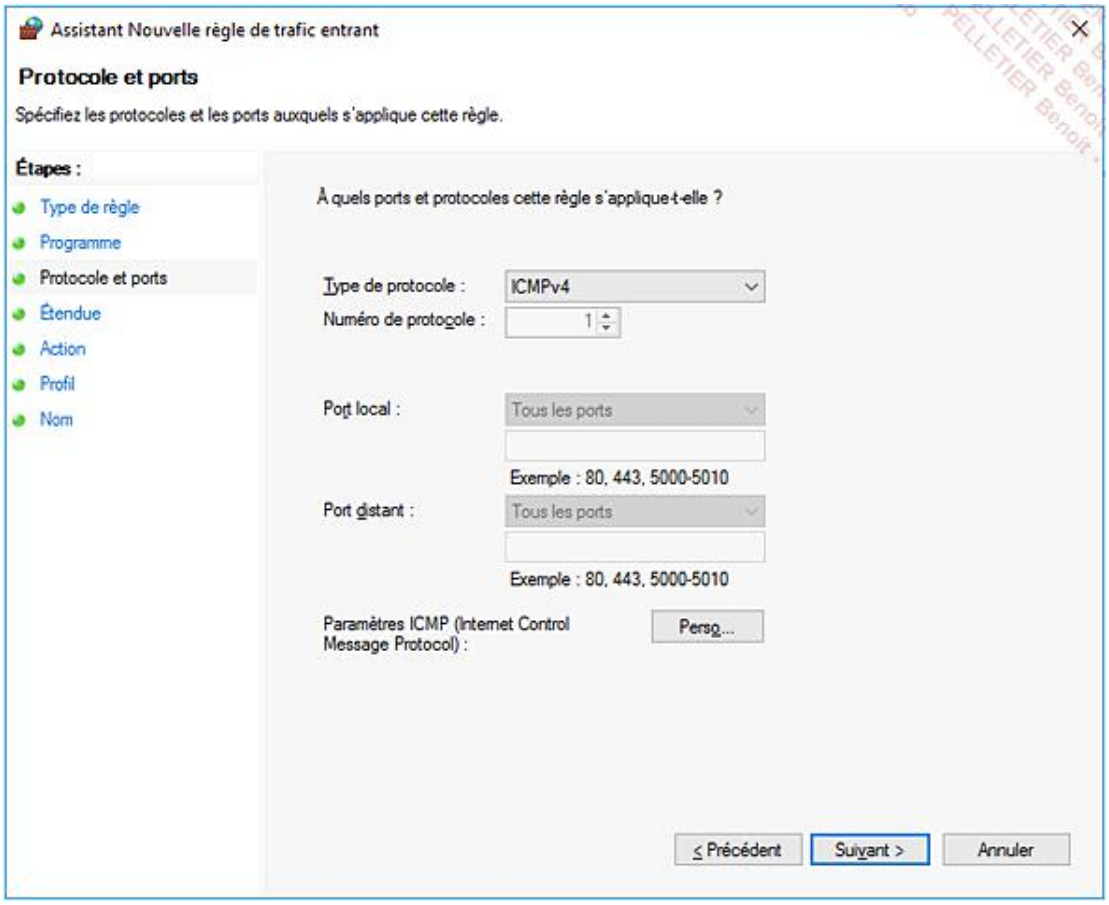
- Cliquez sur **Règles de trafic entrantes** puis sur **Nouvelle règle** dans le menu **Actions**.
- Sélectionnez le bouton radio **Personnalisée** puis cliquez sur le bouton **Suivant**.



- La règle s'applique à tous les programmes. Laissez le choix par défaut dans la fenêtre **Programme** puis cliquez sur **Suivant**.

Le protocole concerné par la règle est **ICMPv4**.

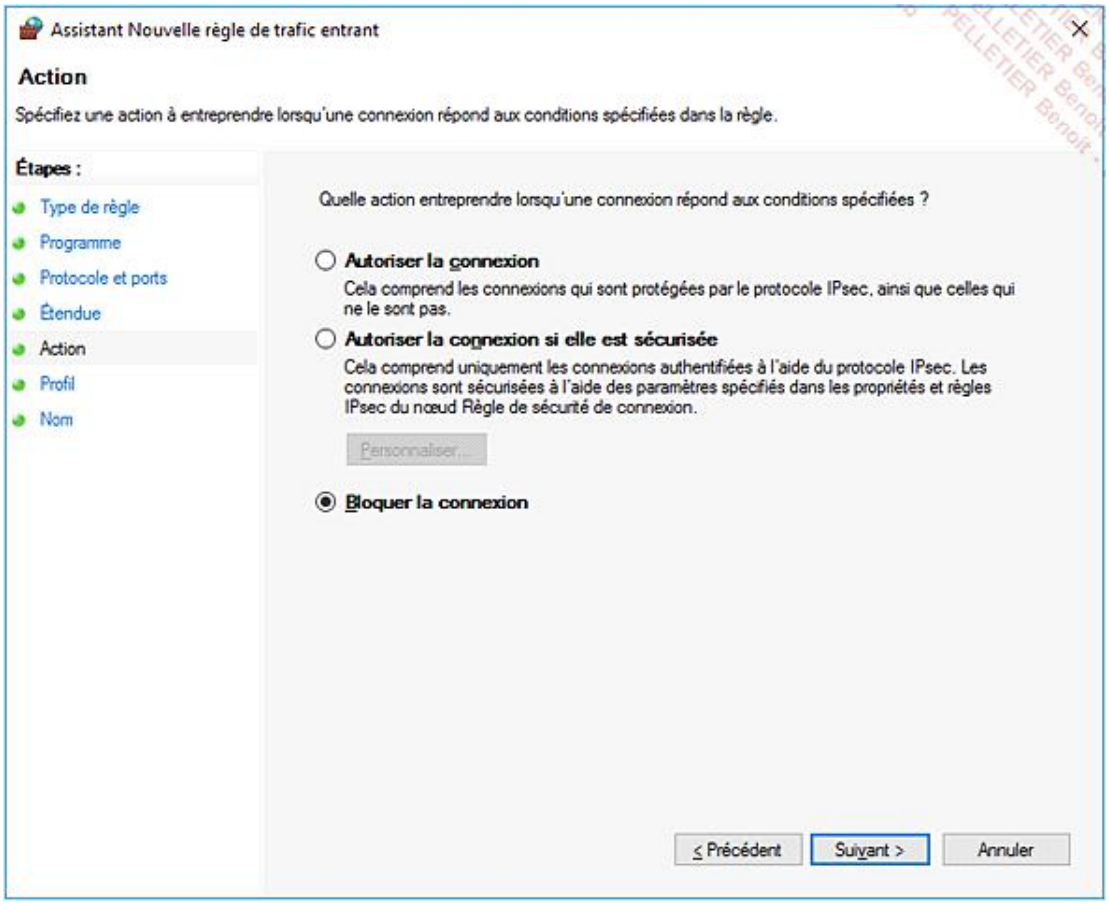
- Sélectionnez dans la liste déroulante le protocole **ICMPv4**.



- Dans la fenêtre **Étendue**, laissez coché **Toute adresse IP** puis cliquez sur **Suivant**.
- Cochez le bouton radio **Bloquer la connexion**.

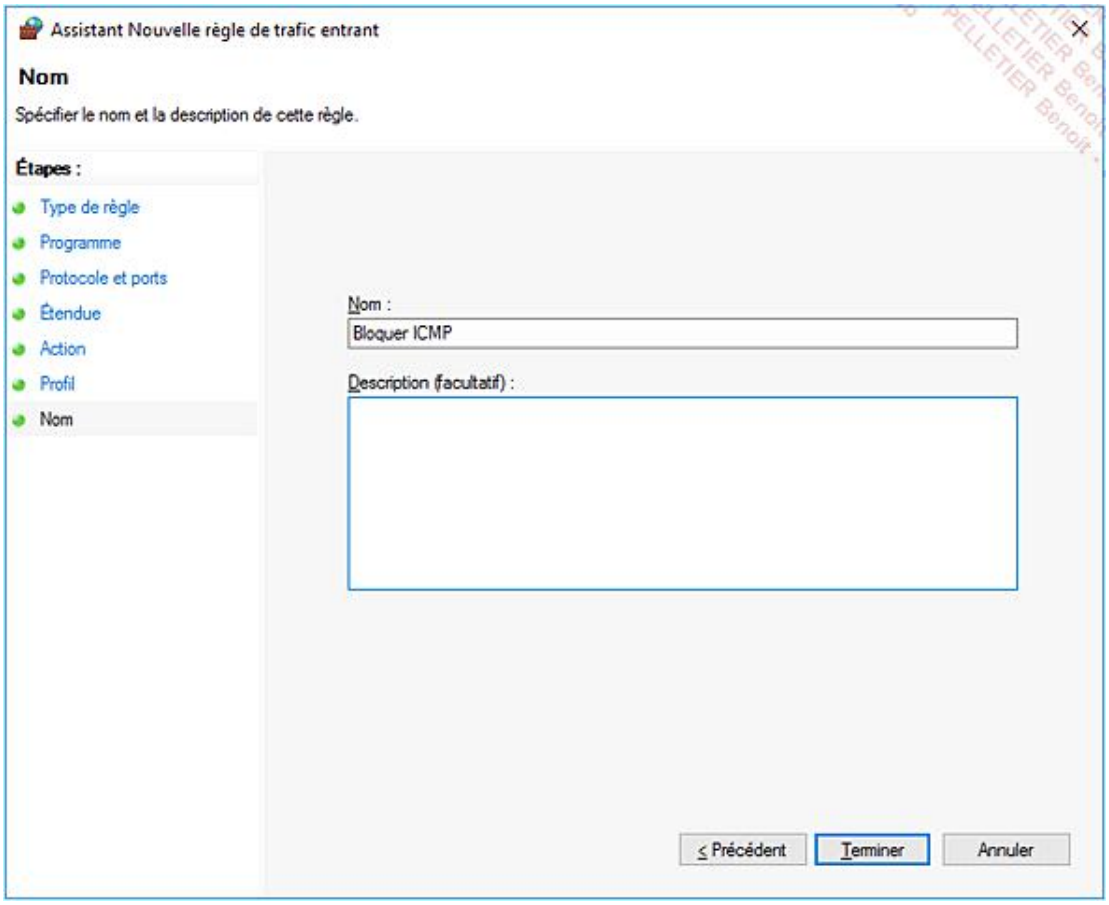
Trois actions sont possibles :

- **Autoriser la connexion** : l'application ou la fonctionnalité qui utilise cette connexion obtient le droit de passer le pare-feu.
- **Autoriser la connexion si elle est sécurisée** : la connexion est autorisée uniquement si le protocole IPsec est utilisé.
- **Bloquer la connexion** : l'application ne peut pas traverser le pare-feu.



La règle va s'appliquer aux trois profils réseau.

- Laissez le choix par défaut dans la fenêtre **Profil** puis cliquez sur **Suivant**.
- Dans le champ **Nom**, saisissez **Bloquer ICMP** puis cliquez sur **Suivant**.



- Cliquez sur **Terminer**.

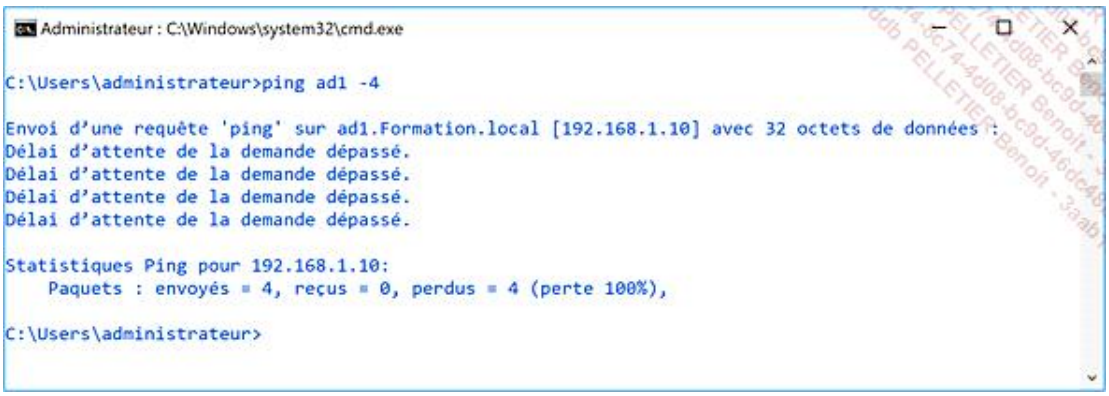
La règle apparaît avec un rond rouge barré. L'icône permet très rapidement de s'apercevoir que le trafic est bloqué. L'icône composée d'un rond vert et d'une coche blanche est attribuée aux règles dont l'action est autorisée.

3. Test de la règle

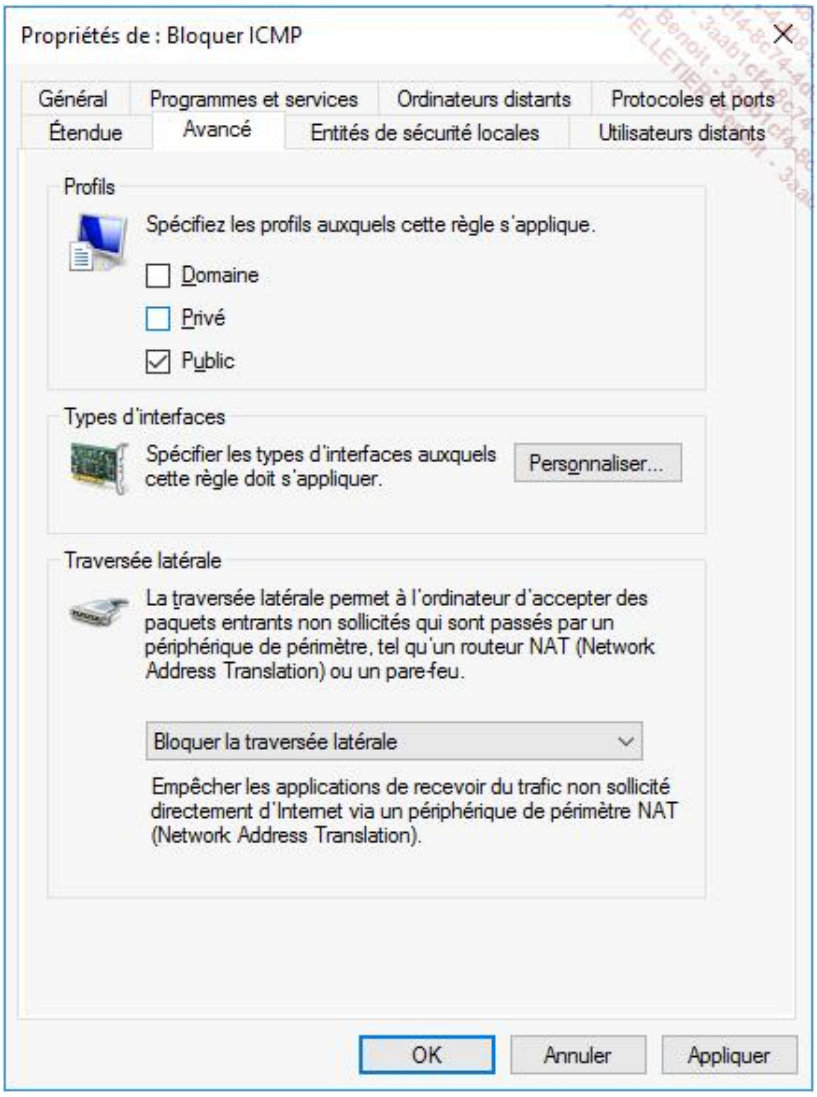
Il est maintenant nécessaire de vérifier le bon fonctionnement de la règle.

- Sur CL10-01, lancez une invite de commandes DOS.
- Saisissez la commande `ping AD1` puis validez à l'aide de la touche [Entrée].

Le protocole ICMPv4 étant bloqué, aucune réponse n'est envoyée. Si le protocole IPv6 vous répond, ajoutez le commutateur `-4` à la commande `ping`.



- Sur AD1, double cliquez sur la règle **Bloquer ICMP** dans la console du Pare-feu Windows.
- Sélectionnez l'onglet **Avancé** et décochez **Domaine**.



- Cliquez sur **Appliquer** puis sur **OK**.

Ainsi la règle ne s'applique plus au profil **Domaine**.

- Sur CL10-01, relancez la commande `ping AD1`.

Le ping est maintenant possible car le serveur est un contrôleur de domaine et le profil réseau configuré est **Domaine**.

Sauvegarde avec Windows Server

Une sauvegarde est nécessaire dans un réseau informatique. Elle permet d'assurer la restauration d'un document supprimé ou altéré ainsi que la restauration de l'ensemble du système d'exploitation et de ses paramètres. Depuis Windows Server 2008, la commande `wbadmin` permet de gérer les sauvegardes. Dans certains cas, il est nécessaire d'y dédier un disque dur. Ce dernier peut être un disque interne ou simplement un disque branché en USB (seule la fonctionnalité de sauvegarde peut écrire dessus).

Les utilitaires de sauvegarde des versions précédentes ne sont pas compatibles avec celui utilisé depuis Windows Server 2008.

1. Installation de la fonctionnalité de sauvegarde

- Sur SV1, lancez la console **Gestionnaire de serveur**.
- Cliquez sur **Ajouter des rôles et des fonctionnalités**.
- Dans la fenêtre **Avant de commencer**, cliquez sur **Suivant**.
- Cochez le bouton radio **Installation basée sur un rôle ou une fonctionnalité** puis cliquez **Suivant**.
- Dans la fenêtre du choix du serveur de distribution, cliquez sur **Suivant** en laissant la sélection par défaut.
- Cochez **Sauvegarde Windows Server** dans la fenêtre de sélection des fonctionnalités à installer puis cliquez sur **Suivant**.
- Cliquez sur **Installer**.

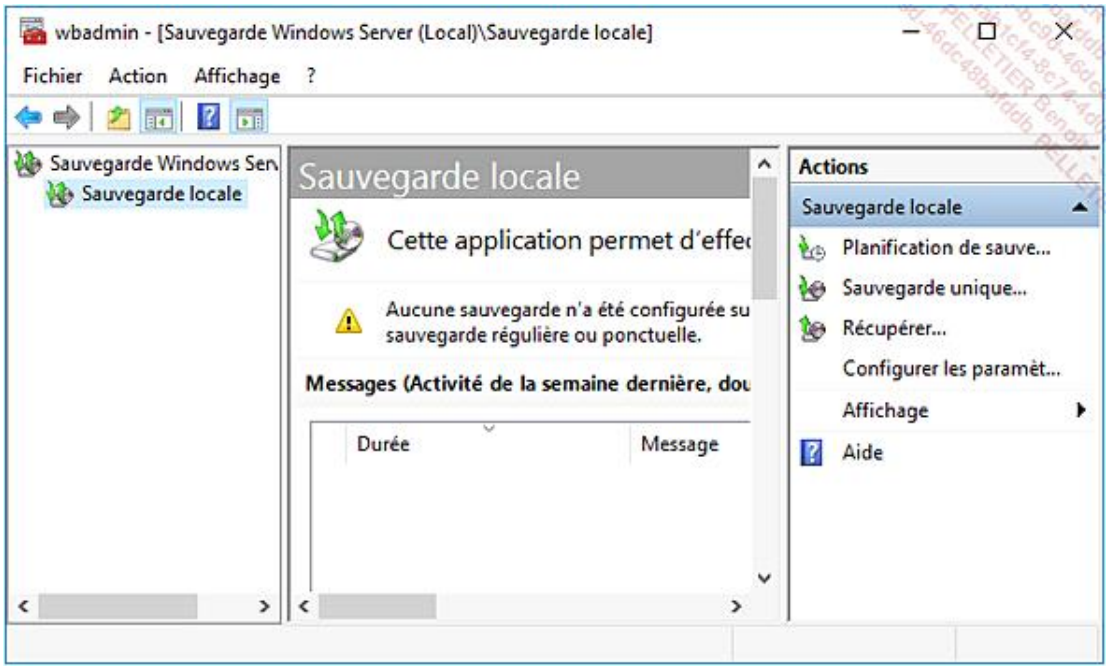
Une fois l'installation terminée, une nouvelle console est présente parmi les outils d'administration.

2. Création d'une sauvegarde manuelle unique

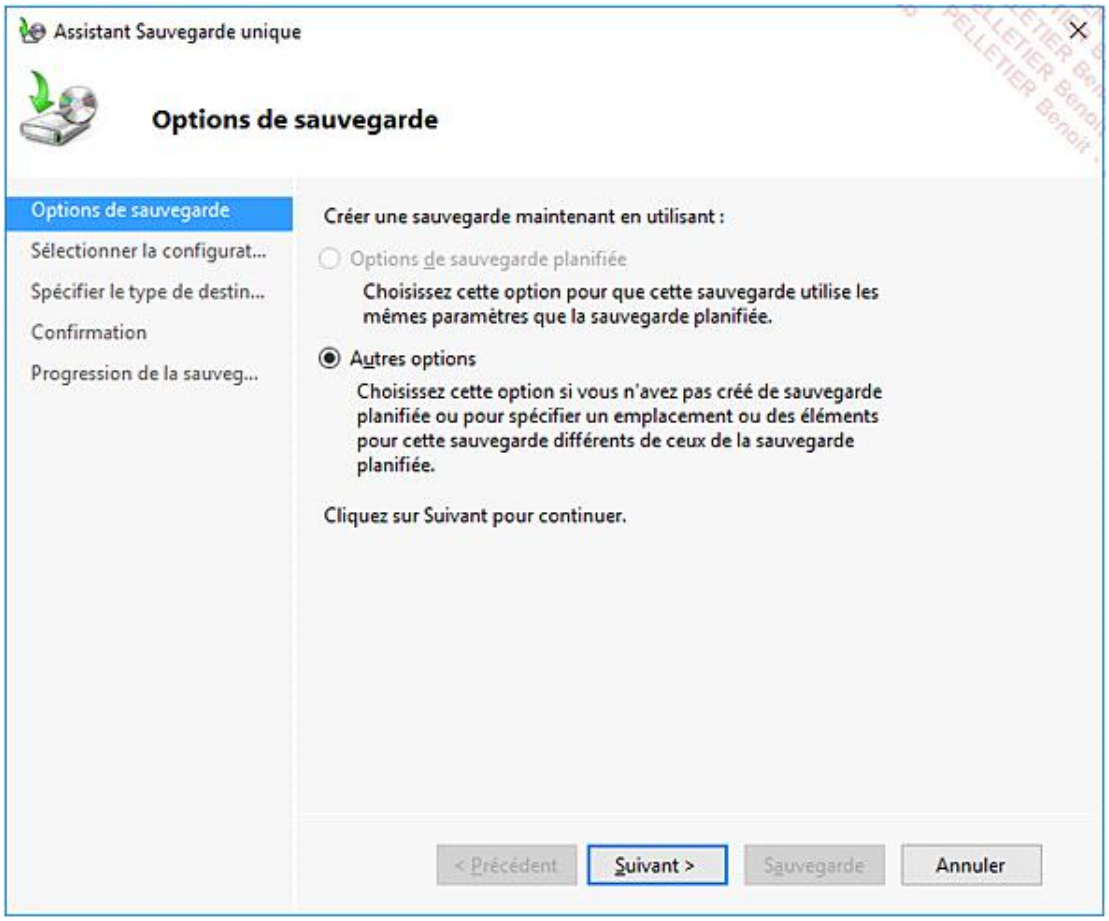
Une deuxième partition est nécessaire pour l'élaboration des manipulations ci-dessous. Il est possible d'ajouter un deuxième disque VHD au serveur SV1.

Contrairement à la sauvegarde planifiée, la sauvegarde manuelle ne nécessite pas de disque dédié.

- Effectuez un clic droit sur le menu Démarrer puis sélectionnez l'option **Exécuter**.
- Saisissez **wbadmin.msc** puis cliquez sur **OK**.
- Dans le dossier **Documents**, créez un répertoire nommé **Important** et insérez des documents ou images à l'intérieur.
- Dans la console, cliquez sur **Sauvegarde locale** puis sur **Sauvegarde unique** dans le bandeau **Actions**.



Dans la fenêtre **Options de sauvegarde**, cliquez sur **Suivant**.

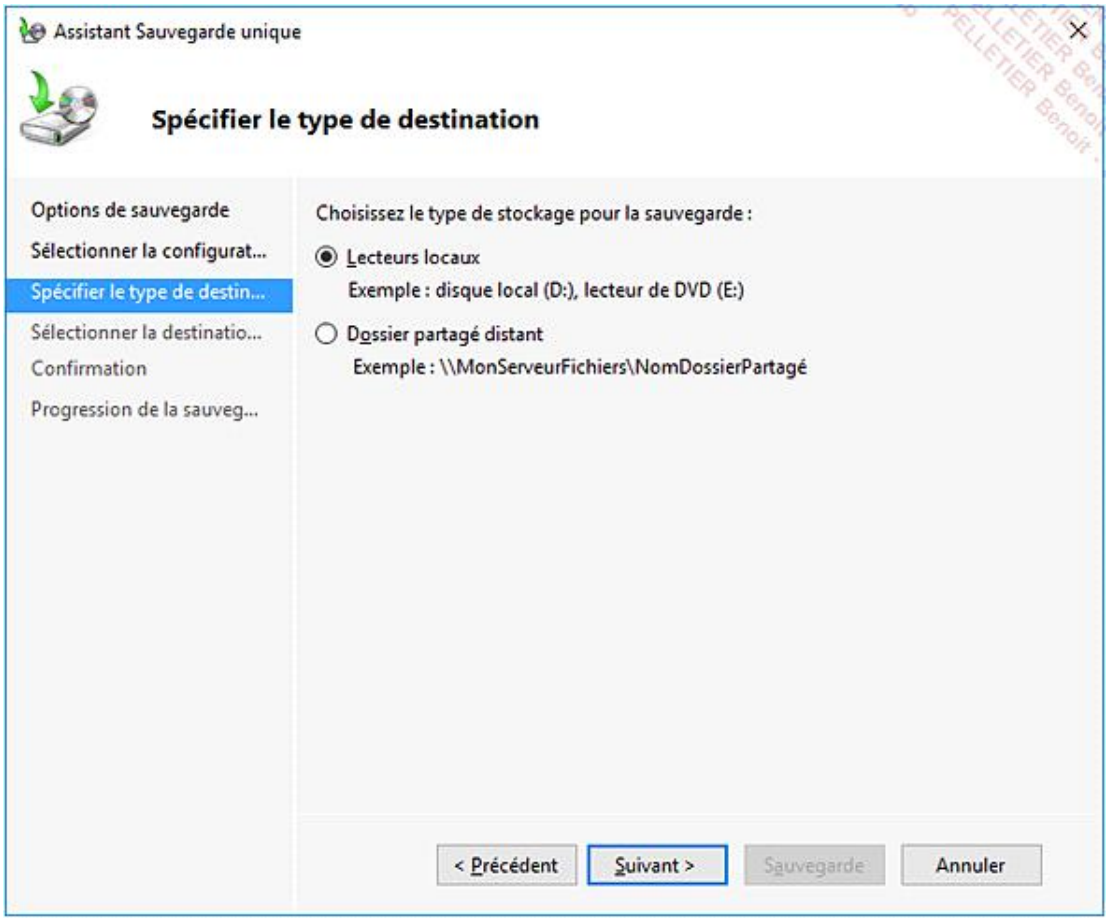


La sauvegarde peut être configurée pour sauvegarder l'ensemble du système ou une sélection faite par l'administrateur.

Laissez coché **Serveur complet (recommandé)** puis cliquez sur **Suivant**.

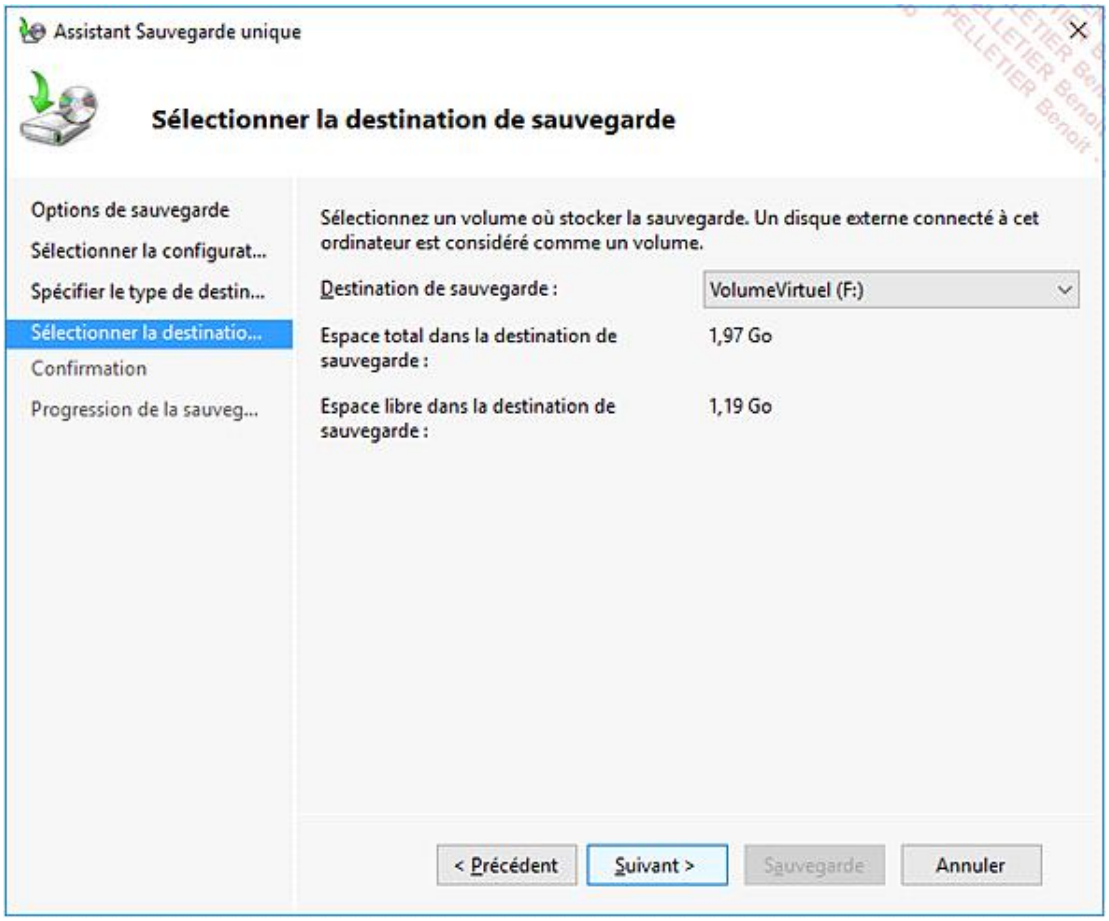
Ainsi il est possible de restaurer l'ensemble de la configuration, et des rôles (Active Directory, etc.) du serveur.

La sauvegarde est stockée sur les disques locaux. Cliquez sur **Suivant** dans la fenêtre de destination.



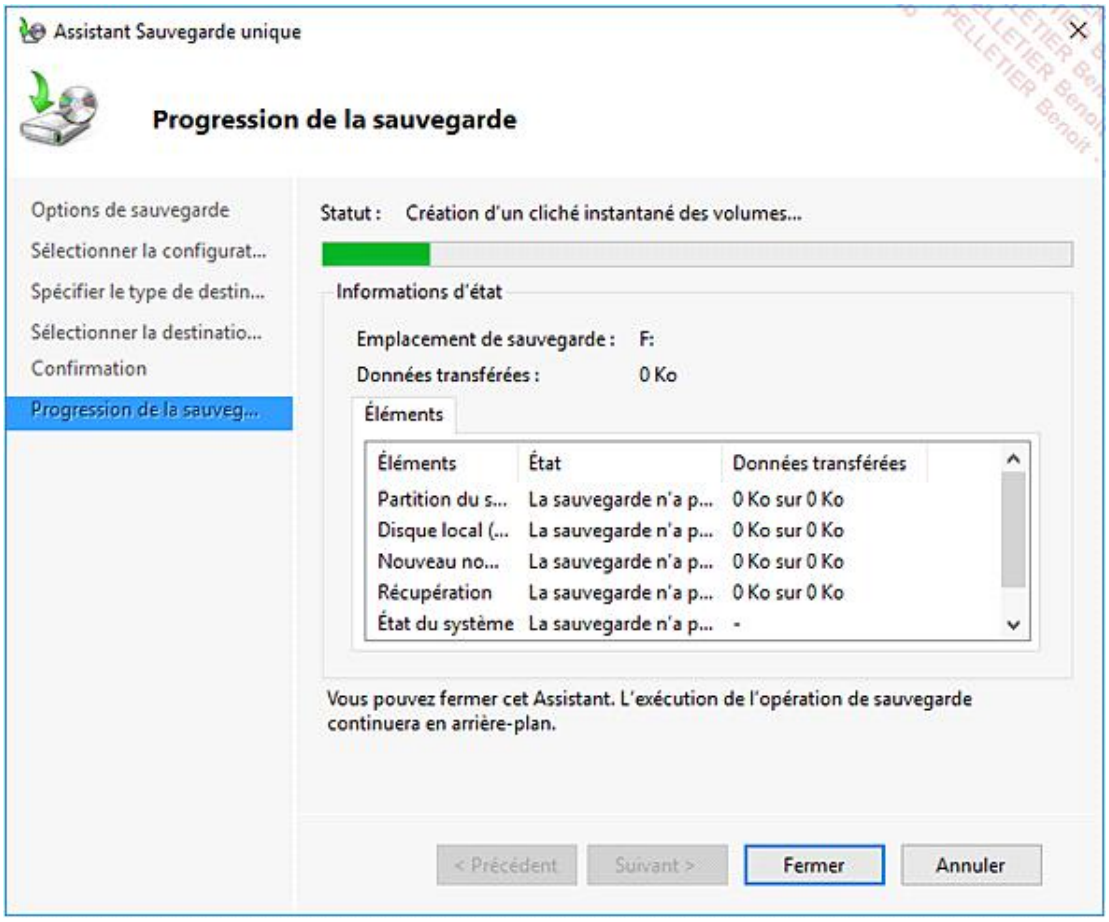
Une deuxième partition est nécessaire et un message d'erreur s'affiche si une partition supplémentaire n'est pas présente.

Sélectionnez la destination de la sauvegarde puis cliquez sur **Suivant**.



- Cliquez sur **OK** dans la fenêtre d'avertissement afin d'exclure la destination de la sauvegarde.
- Cliquez sur **Sauvegarder** afin de lancer la sauvegarde.

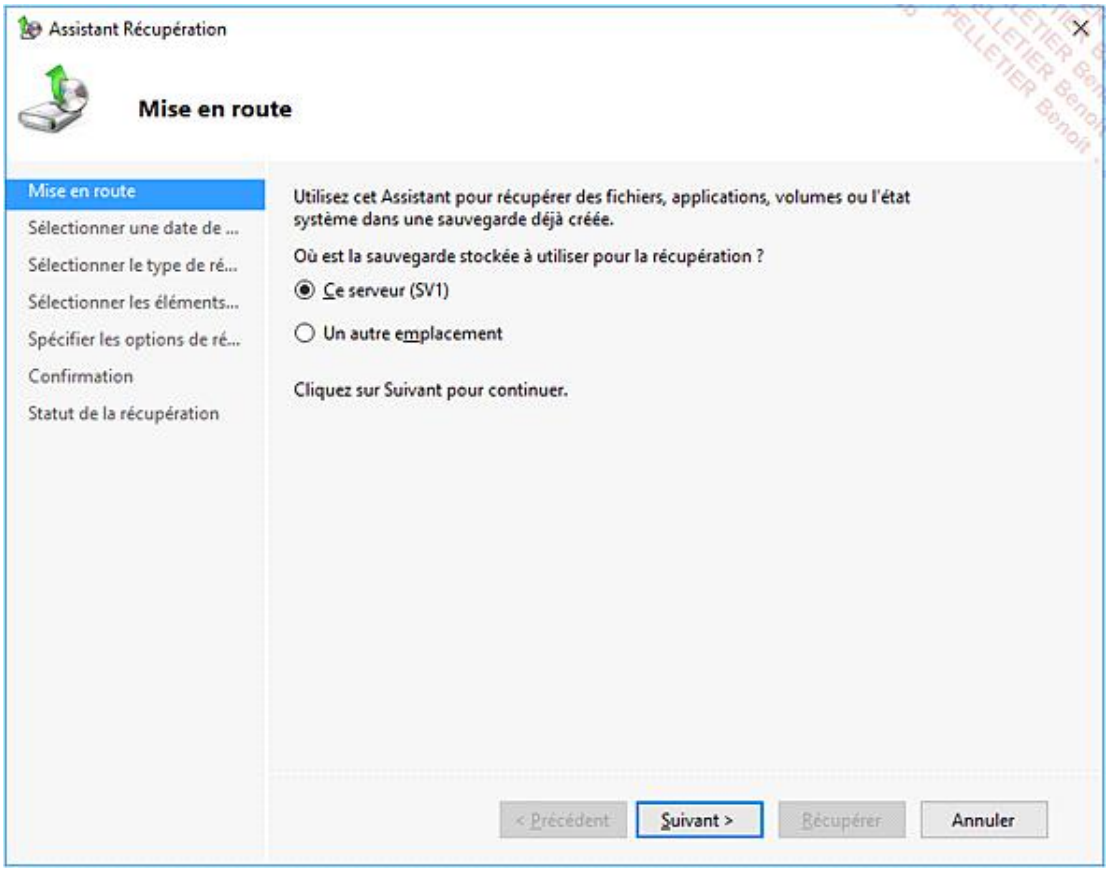
La sauvegarde est en cours…



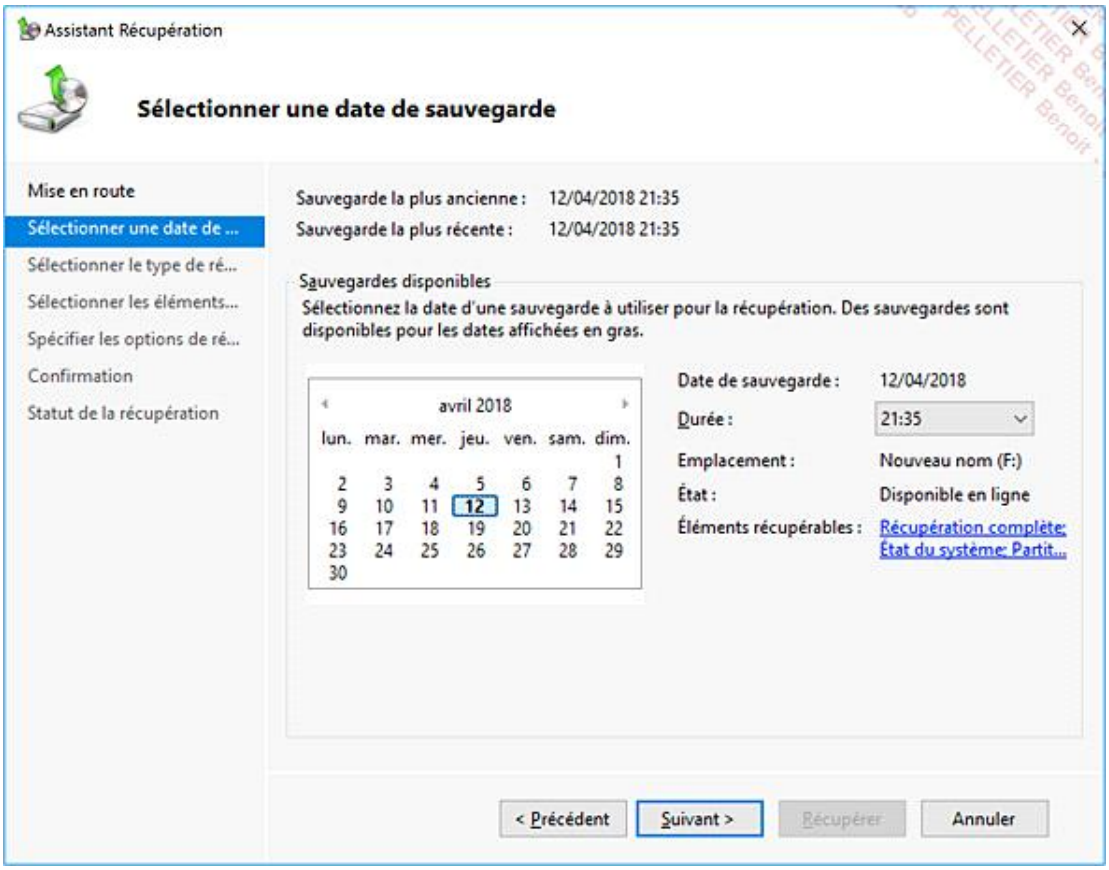
Un dossier est créé dans la partition de destination.

3. Restauration d'un fichier ou dossier

- Sur SV1, supprimez le dossier **Important** présent dans **Documents**.
- Lancez la console **Sauvegarde Windows Server** (**wbadmin.msc**).
- Sélectionnez **Sauvegarde locale** puis **Récupérer** dans le bandeau **Actions**.
- La sauvegarde est stockée sur ce serveur. Cliquez sur **Suivant** dans la fenêtre **Mise en route**.

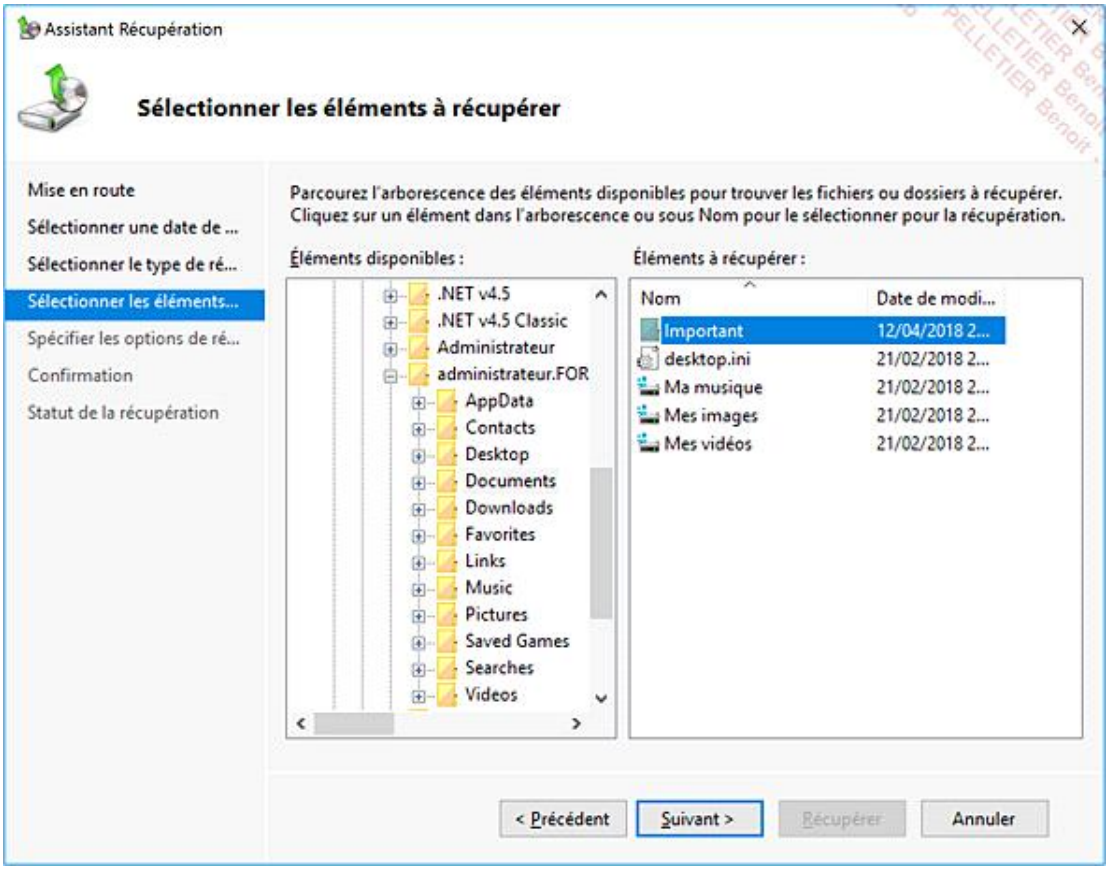


- Sélectionnez la date à laquelle la sauvegarde a été effectuée puis cliquez sur **Suivant**.



- Cochez le bouton radio **Fichiers et dossiers** dans la fenêtre du choix du type de récupération puis cliquez sur **Suivant**.

- Développez **SV1**, **Disque local (C:)**, **Users**, **Administrateur.formation.local** puis **Documents**.
- Sélectionnez **Important** puis cliquez sur **Suivant**.



Les documents doivent être replacés à l'emplacement d'origine. Nous pouvons remplacer sans problème les versions existantes car le dossier a été supprimé.

- Cochez **Remplacer les versions existantes par les versions récupérées** puis cliquez sur **Suivant**.
- Cliquez sur le bouton **Récupérer**.

À la fin de la récupération, les fichiers sont présents dans **Documents**.

Introduction à PowerShell

PowerShell est une plateforme permettant l'exécution de scripts, il a également la fonction d'interpréteur de commandes.

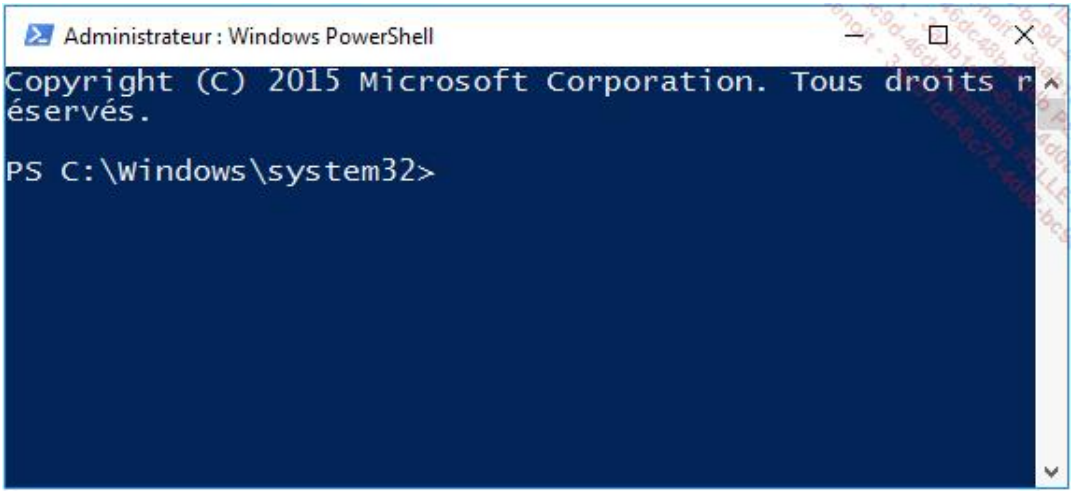
1. Présentation de PowerShell

Cette plateforme n'a cessé de s'enrichir et offre une multitude de jeux de commandes. Les commandes DOS peuvent également être utilisées avec la console PowerShell et ce à l'aide des alias (**get-alias** pour avoir la correspondance).

Depuis Windows Server 2008 R2 et Windows 7, PowerShell est directement intégré au système d'exploitation. Pour les plus anciens (Windows Vista, XP, 2008…), il est nécessaire de procéder à une installation. Notons également que certaines applications (par exemple : Microsoft Deployment Toolkit) nécessitent obligatoirement la présence de la plateforme PowerShell pour fonctionner.

2. La console PowerShell

La saisie des différentes commandes s'effectue par le biais de la console PowerShell. Cette dernière a un aspect graphique très proche d'une invite de commandes DOS.



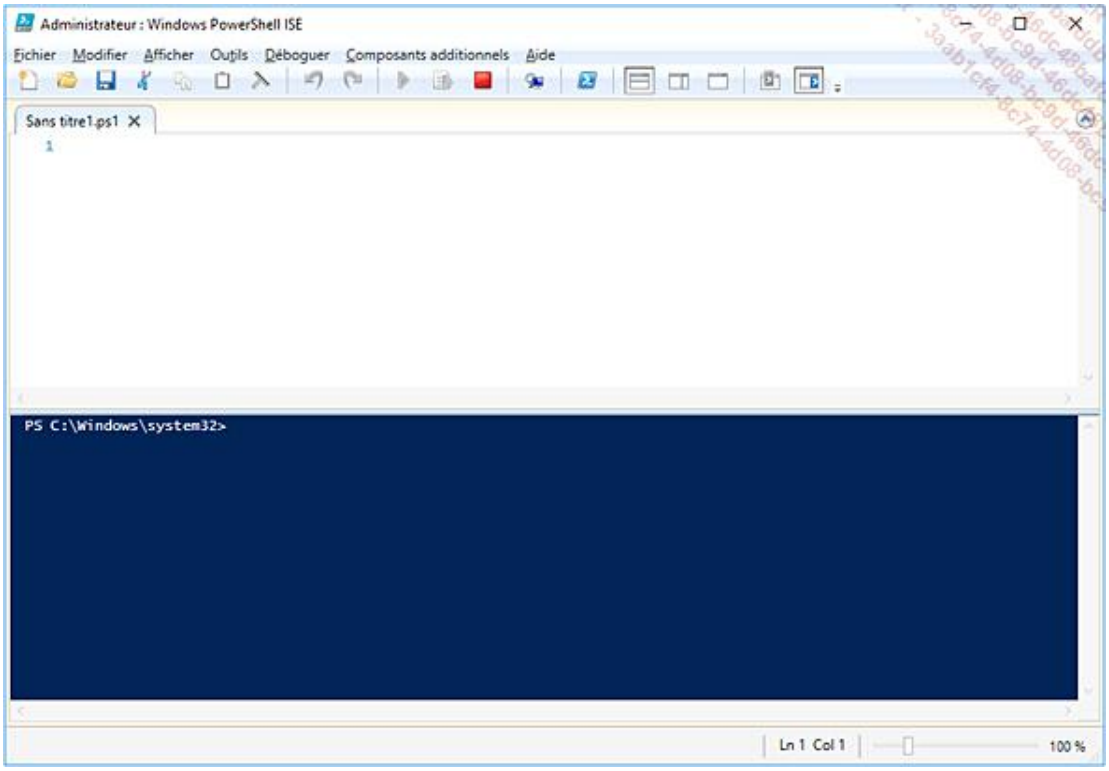
L'autocomplétion d'un chemin, d'un nom de commande, etc. peut s'effectuer à l'aide de la touche [Tab]. Pour rappel, l'autocomplétion consiste à saisir le début d'une commande ou d'un chemin, le système tente de compléter la suite.

Enfin, la combinaison [Ctrl] **C** ou [Ctrl][Pause] permet de mettre fin à l'exécution de l'instruction courante pour la première combinaison et de mettre fin à l'exécution de la console pour la seconde.

3. La console Windows PowerShell ISE

Cette console facilite la création de scripts PowerShell. Il est donc possible pour ceux qui le souhaitent et d'effectuer la création de scripts à l'aide de cet outil.

De plus, il offre plusieurs fonctionnalités intéressantes (coloration syntaxique, affichage des numéros de ligne...) mais également un débogueur.

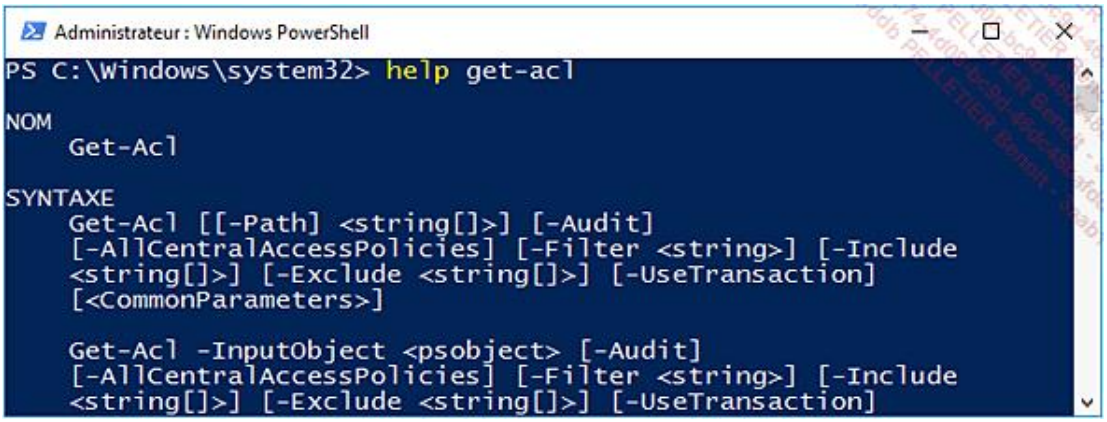


Il est possible d'ouvrir plusieurs scripts en même temps (chacun est ouvert dans un onglet différent). Enfin, nous pouvons noter également la possibilité de tester les scripts et l'accès aux différents modules (Active Directory...). En effet, cette dernière fonctionnalité permet d'avoir accès aux différents paramètres obligatoires ou facultatifs des commandes.

Aide avec PowerShell

Nous avons tous à un moment donné saisi le fameux /? dans une console DOS, ceci nous permettant de récupérer la syntaxe de la commande et un descriptif des différents commutateurs.

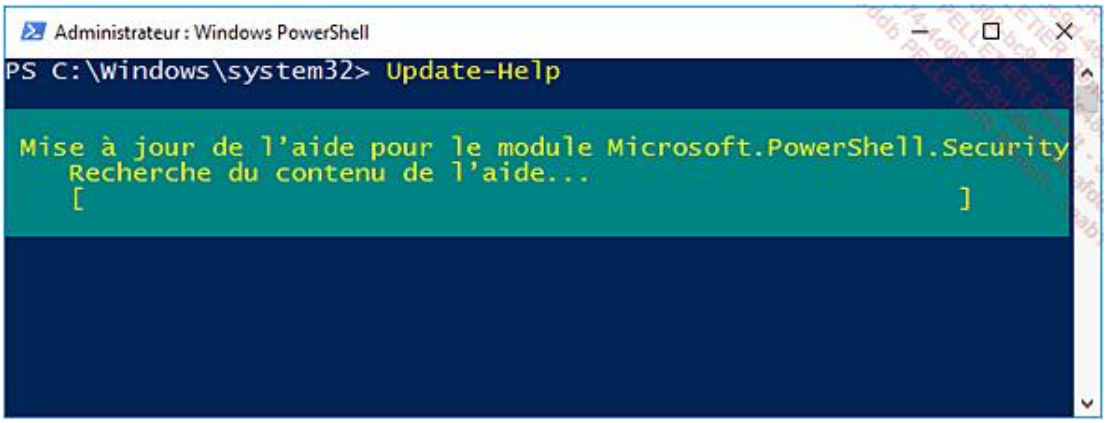
Avec PowerShell, la syntaxe est quelque peu différente. En effet, l'aide s'affiche en saisissant l'instruction **help *commande***.



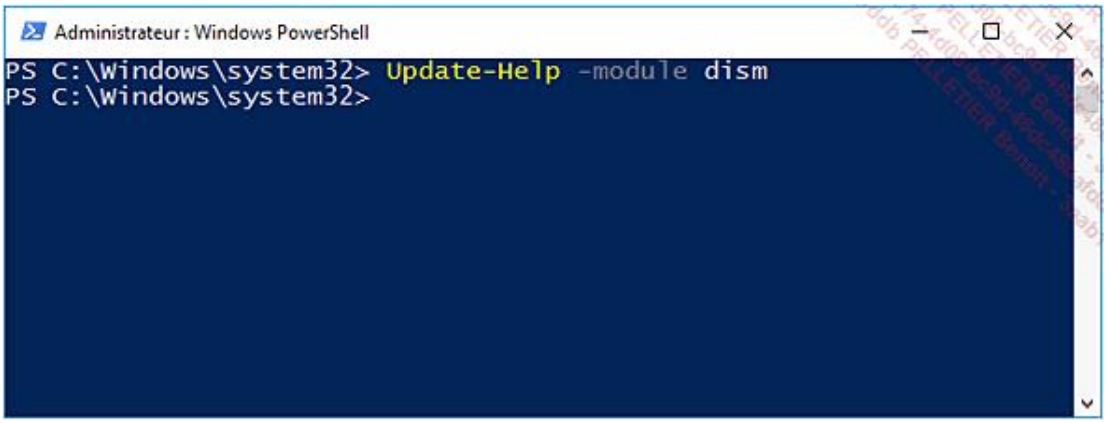
Les fichiers d'aide peuvent aisément être mis à jour. Il est néanmoins nécessaire d'avoir des droits d'administrateur et de lancer la console en tant qu'administrateur.

Une connexion Internet est également nécessaire.

Cette opération s'effectue avec la commande `update-help`.



Cette mise à jour concerne uniquement les fichiers de la langue utilisée et du module actif. Si vous souhaitez mettre à jour le module dism alors que le module actif est AppLocker, il faut rajouter à la commande précédente le commutateur `-Module dism`.



Il est possible de déposer les fichiers d'aide sur un partage réseau afin que les postes qui ne sont pas raccordés à Internet puissent profiter de la mise à jour. L'opération va cette fois être scindée en deux parties (copie des fichiers sur un partage réseau et mise à jour des postes depuis ce partage réseau).

Pour effectuer cette opération, l'instruction suivante doit être utilisée : `Save-Help -DestinationPath CheminUNC -Force`

Enfin, il est nécessaire d'exécuter sur les postes la commande suivante : `Update-Help -SourcePath "CheminUNC" -force`

La syntaxe PowerShell

Une commande est constituée d'un verbe et d'un nom séparés par un tiret (-). Le verbe a pour but de décrire l'action effectuée :

- Get (obtenir une information)
- Set (effectuer une action)
- Add...

Le verbe est complété par un nom (Acl, etc.). Ce dernier constitue la commande.

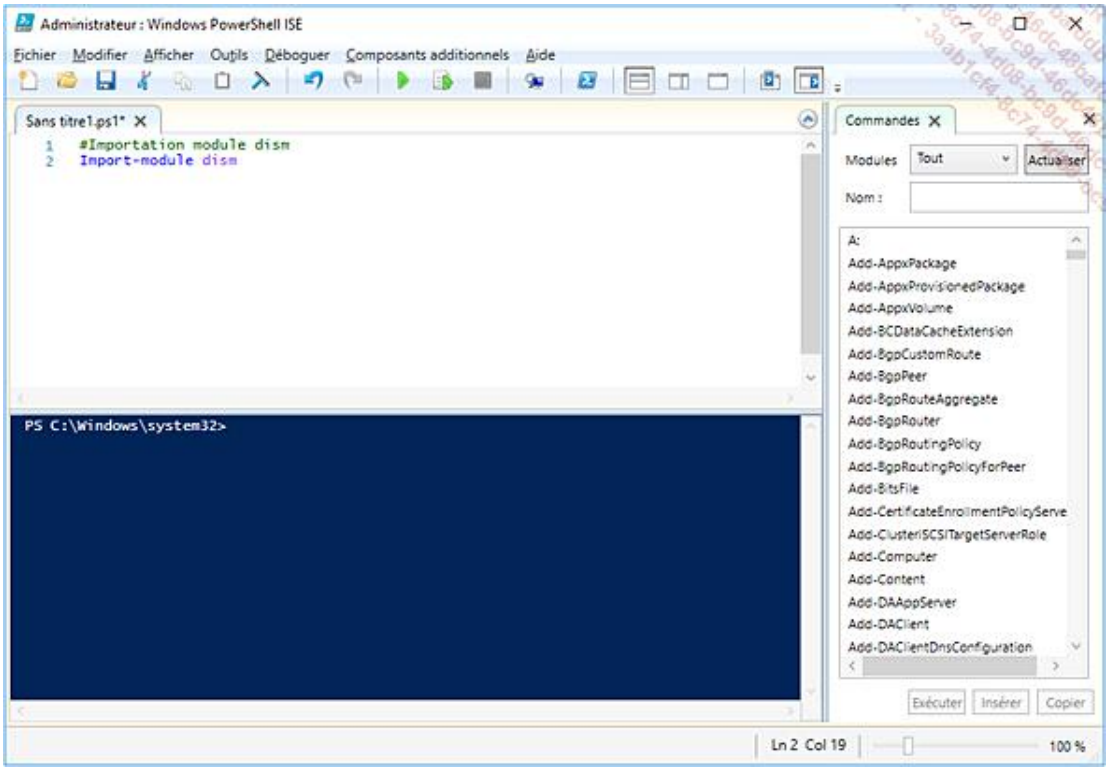
Comme pour les commandes DOS, l'analyse de la syntaxe PowerShell n'est pas sensible à la casse.

1. Les commentaires

Comme dans tous langages de programmation, il est possible de placer des commentaires dans les scripts.

Pour différencier une instruction d'un commentaire, il faut utiliser le caractère dièse "#" en début de ligne. Ainsi la ligne est considérée comme commentaire.

De plus, l'ajout de commentaire après l'instruction peut être effectué.

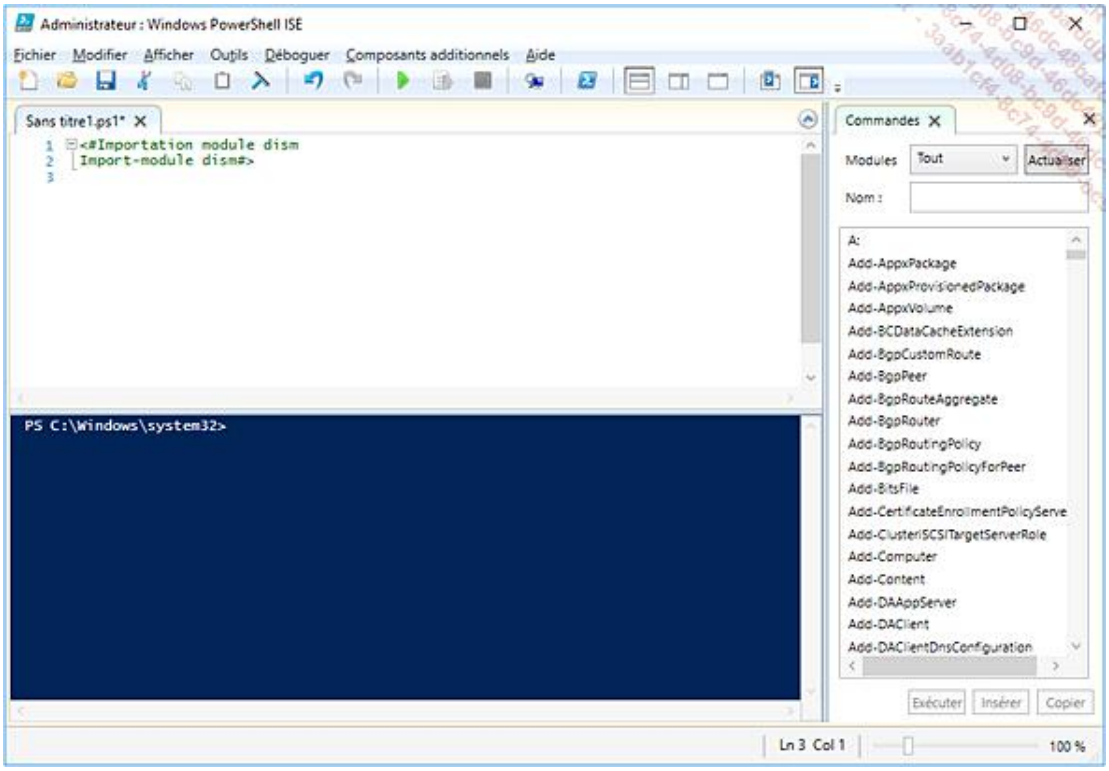


Pour commenter un bloc entier, une syntaxe particulière doit être utilisée.

Cela ne fonctionne que depuis PowerShell v2.0.

Les caractères **<#** doivent être insérés au début du bloc de commentaire puis, afin d'en marquer la fin, on insère les

caractères **#>**.



La ligne mise en commentaire ne sera pas prise en compte par l'interpréteur de commandes.

2. Les guillemets

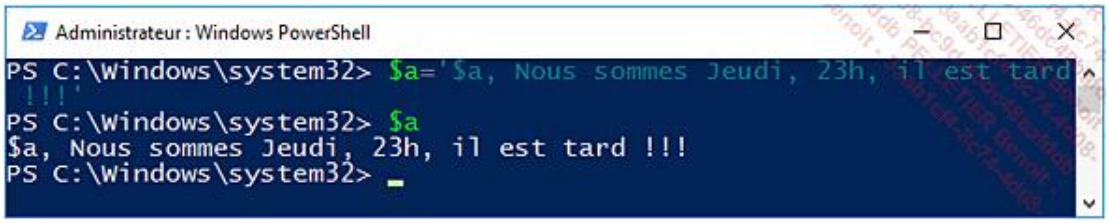
Il est nécessaire de délimiter les chaînes de caractères, ceci afin d'aider la compréhension de la syntaxe par l'analyseur syntaxique. Les guillemets (") sont généralement utilisés pour effectuer cette opération. Cette règle s'applique également à PowerShell.

Néanmoins, deux méthodes peuvent être utilisées pour délimiter une chaîne de caractères.

- Les guillemets doubles " " qui permettent la substitution de variable.



- Les guillemets simples " laissent le texte tel quel.
- Reprenons la variable $a utilisée ci-dessus et ajoutons-lui le texte : 23h, il est tard!!!



La chaîne de caractères $a n'a pas été prise comme variable mais comme chaîne de caractères.

3. Les variables

PowerShell utilise des variables comme tous les autres langages informatiques. Néanmoins, la déclaration avant l'utilisation n'est pas nécessaire. Le système va déterminer automatiquement le type de variable nécessaire (chaîne de caractère, entier…).

Par la suite ces variables peuvent être utilisées à n'importe quel endroit du script. Afin de stocker une valeur, il est nécessaire de faire suivre la variable par un égale.

Exemple : `$a= "Bonjour !"`



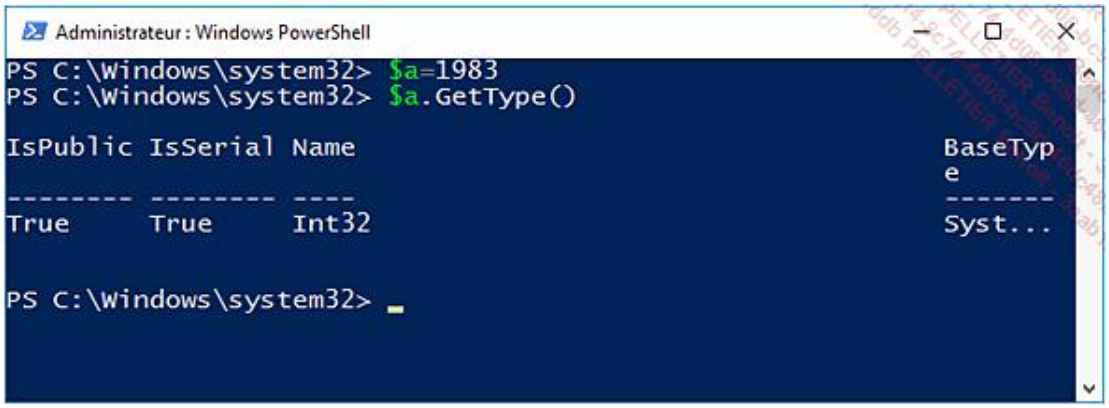
Dans l'exemple précédent, le type de la variable n'a pas été défini.

Il est possible de transformer le type de la variable (transformer une variable de type entier en chaîne de caractères).

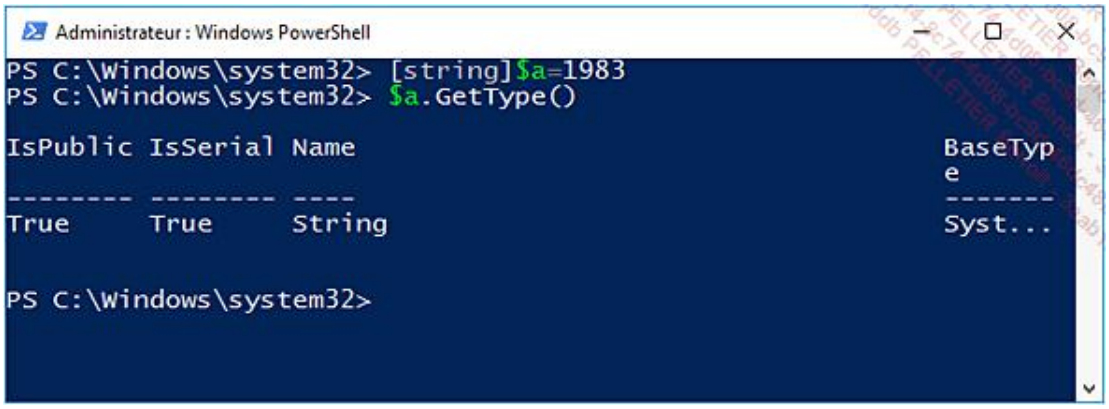
Cette opération s'effectue de la manière suivante :

```
$a=1983
```

La variable est de type entier.



En définissant le type de variable, la même valeur est cette fois considérée comme chaîne de caractère.



En saisissant dans la console $a, nous appelons cette fois la variable et le contenu de cette dernière sera affichée.

Il est préférable d'éviter les variables contenant des caractères spéciaux afin d'éviter les problèmes.

Les boucles avec PowerShell

Les boucles sont très utiles dans un langage de programmation pour exécuter x fois une même action.

1. La boucle While

Ce type de boucle permet de répéter les instructions présentes dans la boucle tant que la condition est vérifiée (vraie).

Cette boucle s'écrit de la manière suivante :

```
While condition
{
Instruction1
Instruction 2
...
}
```

2. La boucle Do-While

Ce type de boucle est identique à la précédente, néanmoins le test est effectué à la fin.

La syntaxe est la suivante :

```
Do
{
Instruction1
Instruction 2
...
}
While condition
```

La boucle est obligatoirement exécutée au moins une fois, le test s'effectuant à la fin.

3. La boucle For

Ce type de boucle offre l'avantage de pouvoir déterminer le nombre de fois où le bloc d'instructions doit être exécuté. L'exécution est effectuée tant que la valeur indiquée au départ n'est pas atteinte. Le pas d'incrémentation est également déclaré.

La syntaxe de ce type de boucle est la suivante :

```
For (<Valeur Initiale> ; <Condition> ; <Increment>)
{
Instruction 1
Instruction 2
}
```

PowerShell V5

Avec l'arrivée de Windows Server 2016, une nouvelle version de PowerShell a vu le jour. Cette section présente quelques-unes de ces nouveautés.

Une nouvelle cmdlet, Write-Information, a été ajoutée. Elle permet de spécifier comment les flux d'information pour une commande sont traités. Les paramètres InformationVariable et InformationAction permettent de déterminer la manière dont les flux d'information sont affichés.

Il est maintenant possible de gérer les archives. En effet, un nouveau module le permettant a été intégré à la plateforme. Les mêmes opérations pouvaient être effectuées sur les anciennes versions mais nécessitaient l'ajout de modules développés par la communauté Microsoft.

Il est donc possible, et cela de manière native, de générer une archive (compress-archive) ou d'effectuer une extraction (expand-archive). Attention néanmoins, il est important de noter que seules les extensions zip sont gérées. L'opération de mise à jour (ajout d'un fichier dans l'archive) ainsi que le taux de compression peuvent être définis au moment de la génération.

La commande New-item a été enrichie, elle offre désormais la possibilité de créer des raccourcis. Pour cela, le type symboliclink doit être utilisé.

Comme pour Office, PowerShell est maintenant "gérable" par l'intermédiaire de stratégies de groupe. Un fichier ADMX est présent dans le système d'exploitation et donne accès à quelques paramètres.