

Objectifs pédagogiques

À la fin de ce cours, vous saurez :

- Installer et administrer la version pertinente, selon votre contexte, de Windows Server.
- Installer et configurer les rôles Windows Server et leurs fonctionnalités associées.
- Gérer les services avancés.
- Mettre en place Windows Server dans un contexte professionnel.

Un peu de contexte

Microsoft Windows Server est le système d'exploitation serveur de Microsoft. En quelque sorte, il s'agit d'une version améliorée du système Windows que vous connaissez sûrement, installé par défaut sur une grande majorité des ordinateurs du commerce !

Pourquoi différencier le système utilisateur d'un système pour les serveurs ?

Eh bien, tout simplement pour permettre de **simplifier la gestion** de services applicatifs et réseau. Avec Windows Server, l'objectif est de fournir des services à de nombreux autres équipements.

Pour cela, Microsoft a choisi de segmenter ses différents systèmes en plusieurs grandes familles. En 1985, Microsoft sort **Windows 1.0** ; ce nom fait référence au système de fenêtres qui permet de simplifier l'utilisation d'un ordinateur, qui à l'époque se faisait uniquement au travers d'un **shell**, une interface en ligne de commande (chez Microsoft, ce système se nommait DOS – Disk Operating System).

Rapidement, ce système à base de fenêtres s'est trouvé très pratique et a vite évolué. Durant les années 1990, la nécessité de concurrencer les systèmes serveur de l'époque pousse Microsoft à concevoir un système orienté services et non plus bureautique. La naissance de **Windows Server** est en marche avec les versions NT.

La popularité de cette nouvelle version de Windows (Windows NT) dans le domaine de l'entreprise pousse Microsoft à continuer d'investir dans ce domaine. En 2003 arrive enfin la première version de Windows Server (Windows Server 2003). Cette version marque un tournant dans la conquête de l'entreprise par Microsoft. Ce sera une version **massivement** adoptée en entreprise. Se suivent alors, régulièrement, de nouvelles versions de ce système : 2008, 2012, 2016, 2019 et 2022.

La version 2022 est sortie en été 2021. Cependant, comme les nouvelles versions sont généralement suivies par beaucoup de correctifs, et qu'il n'est pas encore totalement déployé dans les entreprises, il est plus sage pour le moment de rester sur la version 2019.

Distinguez les différentes éditions de Windows Server

À ce jour, il n'existe pas qu'une seule édition de Windows Server 2019, ce serait bien trop simple. Microsoft étant une société commerciale, elle se doit de commercialiser différentes versions d'un même produit ! Pour cette mouture 2019, il existe donc **trois éditions de Windows** avec des cibles différentes :

- **Windows Server 2019 Essentials**

Cette édition se destine aux petites entreprises et organisations jusqu'à 25 utilisateurs et 50 équipements. Cette licence permet de faire fonctionner, à moindre coût (aux environs de 500 €) tous les services que vous allez maîtriser d'ici les prochains chapitres. Il suffit de faire l'acquisition du matériel, tel qu'un serveur et des postes de travail disposant d'une licence Windows Professionnel, et le tour est joué !

Si jamais vous passez la barre des 25 utilisateurs, vous ne pouvez pas mettre à jour vers une édition Standard. Il convient donc d'anticiper au mieux vos besoins.

- **Windows Server 2019 Standard**

Cette édition se destine à toute entité n'ayant pas de forts besoins de virtualisation, ou à faible densité (peu de serveurs). Sa tarification se base sur le nombre de cœurs sur le serveur physique (aux environs de 900 €). Il sera nécessaire de faire l'acquisition de licences d'accès clients en plus de l'acquisition d'un poste disposant d'une licence Windows Pro.

- **Windows Server 2019 Datacenter**

Cette dernière édition est haut de gamme. Avec cette édition, vous pouvez créer autant de machines virtuelles que vous le souhaitez sous Windows Server. Elle se destine aux entités ayant de forts besoins de virtualisation, pour la mise en œuvre de centres de données totalement gérés logiciellement. Sa tarification se base elle aussi sur le nombre de cœurs des serveurs physiques (aux environs de 6 500 €), et nécessite également une licence d'accès client pour chaque machine cliente (toujours en supplément d'une licence Windows Pro).

Comme vous le voyez, il conviendra de bien définir ses besoins pour choisir la bonne édition de Windows Server 2019.

Ajoutez à cela les différents "packs" que les revendeurs de licences peuvent fournir (pack Windows Server 2019 Standard + 16 licences d'accès, par exemple), et vous avez **un écosystème complet** mais tout de même complexe en termes de tarification et de licences.

Prenez en main Windows Server Standard

Ce serait trop beau que cela s'arrête à un choix d'édition. Je vous propose de nous attarder sur l'édition Standard. Prenons le scénario fictif, mais réaliste, suivant :

Vous êtes nouvellement embauché dans une société, Gift S.A. La direction vous demande de prévoir la mise en œuvre d'un Active Directory, qui permet de gérer les identités et les droits d'accès au sein d'un réseau d'ordinateurs Microsoft, ainsi qu'un serveur de fichiers.

Vous avez donc décidé d'opter pour Windows Server Standard, car il y a plus de 25 utilisateurs à gérer au sein de la société Gift, et bien plus de 50 équipements (1 ordinateur sous Windows par personne + des ordinateurs en libre service pour le service logistique, et des tablettes sous Windows pour la gestion des stocks).

Vous pensiez en avoir terminé et vous vous êtes rendu sur le site de Microsoft pour [récupérer l'ISO de Windows Server 2019 Standard](#).

Comme vous êtes un administrateur consciencieux, vous décidez, à raison, de tester et qualifier votre choix via l'installation de la version d'évaluation, sur une machine virtuelle sous VirtualBox.

Vous allez donc suivre les étapes suivantes :

- 1. Récupérer**[l'ISO de Windows Server 2019 Standard](#).
- 2. Créer** une machine virtuelle :
 - **spécifier** une quantité d'espace mémoire (RAM) ;
 - **créer** un disque dur virtuel.
- 3. Démarrer** la machine virtuelle.
- 4. Lancer** l'installation de Windows Server 2019 Standard.

C'est parti !

Sur le site de Microsoft, vous avez choisi **le format ISO** et rempli consciencieusement le formulaire de contact de Microsoft :

Evaluations | 180 jours

Commencer l'évaluation

Veuillez remplir le formulaire pour continuer :

* Prénom

* Nom

* Nom de la société

* Taille de l'entreprise

En sélectionner une

* Fonction

En sélectionner une

* Adresse de messagerie professionnelle

* Numéro de téléphone professionnel

* Pays

En sélectionner une

« * » indique un champ obligatoire

Précédent

Continuer

+ Description

+ Informations préalables à l'installation

+ Exploration

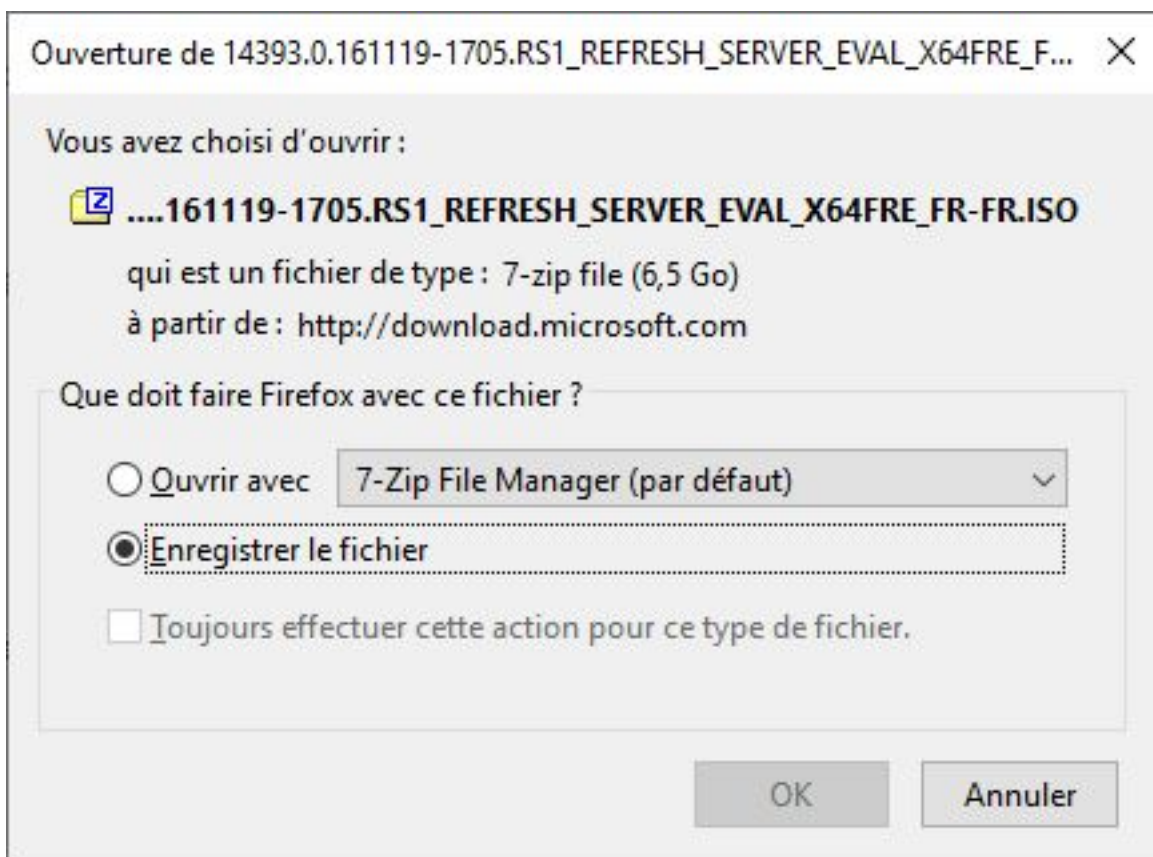
+ Test

+ Formation

Veillez sélectionner votre téléchargement de Windows Server 2019

Anglais (États-Unis)	Téléchargement ISO Édition 64 bits >	Téléchargement VHD Édition 64 bits >	Windows Server sur Azure Essayez maintenant >
Chinois (simplifié)	Téléchargement ISO Édition 64 bits >		
Français	Téléchargement ISO Édition 64 bits >		

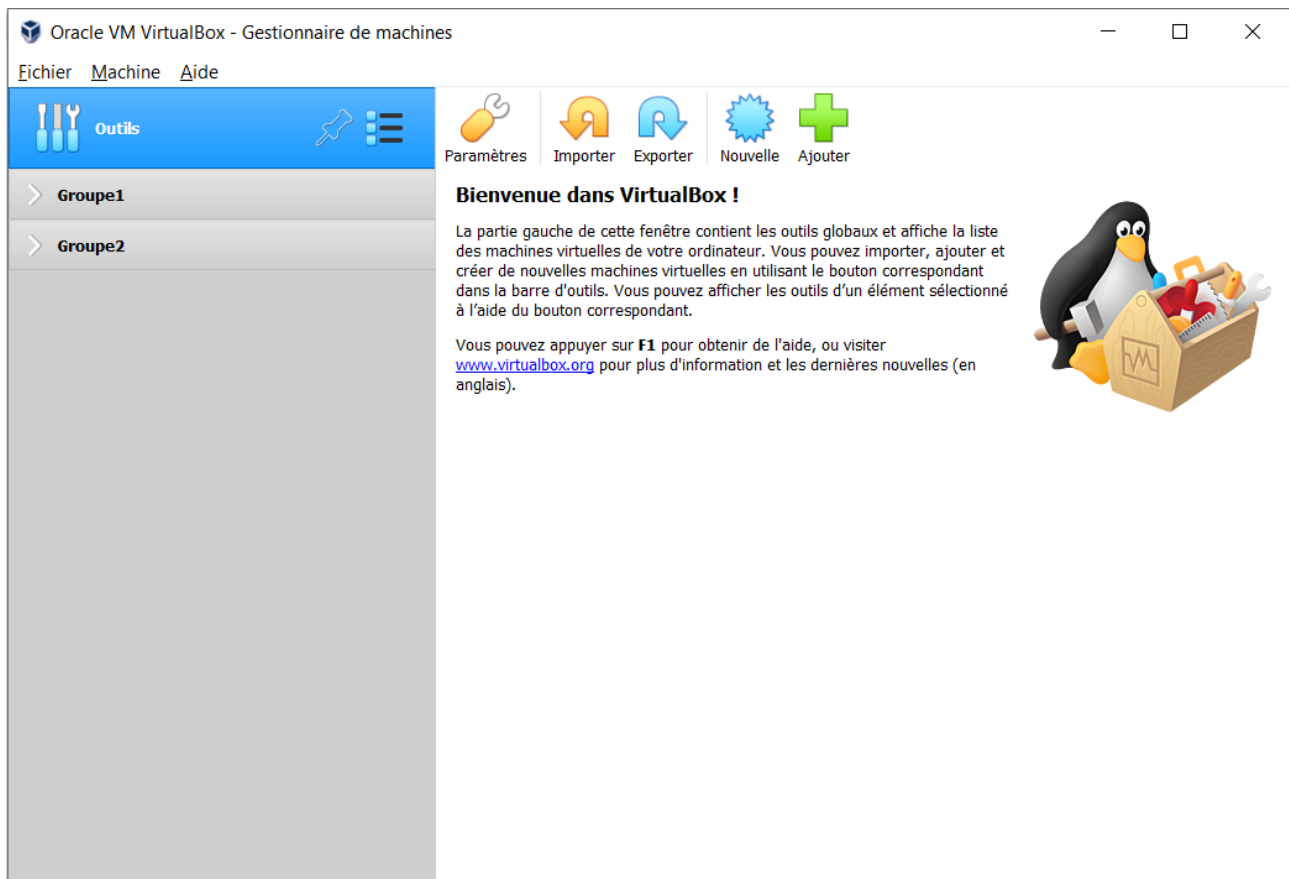
Choisissez la langue de Windows Server
Puis, le téléchargement démarre :



Téléchargement de l'ISO de Windows Server 2016 Standard

Vous avez téléchargé votre ISO et vous allez maintenant l'installer sur une machine. Si vous disposez d'un serveur physique prévu à cet effet, c'est le moment de l'utiliser ! Sinon, pas de panique, vous allez installer Windows Server sur une machine virtuelle. Si nous ne savez pas ce que c'est ni comment faire, je vous invite à lire le cours [Virtualisez votre architecture et vos environnements de travail](#), puis à installer VirtualBox.

La première chose à faire est de créer une nouvelle machine virtuelle. Si vous maîtrisez cette étape, passez directement au paragraphe suivant ; sinon, lancez VirtualBox :



Interface de VirtualBox

Choisissez “Nouvelle” et entrez le **nom de votre système** : Windows Server 2019 Standard. Si tout se passe bien, cela aura pour effet de sélectionner le type “Microsoft Windows” et la version “Windows 2019 (64 bits)”.

← Crée une machine virtuelle

Nom et système d'exploitation

Veillez choisir un nom et un dossier pour la nouvelle machine virtuelle et sélectionner le type de système d'exploitation que vous envisagez d'y installer. Le nom que vous choisirez sera repris au travers de VirtualBox pour identifier cette machine.

Nom :

Dossier de la machine :  ▾

Type : ▾

Version : ▾



Mode expert

Suivant >

Annuler

Nom et système d'exploitation de la machine virtuelle

Ensuite, vous devez affecter une certaine quantité de mémoire vive à votre machine virtuelle pour qu'elle puisse fonctionner correctement. Plus vous allez en affecter, plus votre machine virtuelle aura de l'espace en mémoire pour gérer ses services. Pour le moment, restez sur **2048 Mio** :

← Crée une machine virtuelle

Taille de la mémoire

Choisissez la quantité de mémoire vive en méga-octets alloués à la machine virtuelle.
La quantité recommandée est de **2048 Mo**.

4 MB 16384 MB

2048 MB

Suivant > Annuler

Affectation de la taille de mémoire vive à la machine virtuelle

Maintenant, vous devez spécifier **un espace de stockage**, qui représente le disque dur de la machine virtuelle. Attention, cet espace doit être disponible sur votre ordinateur (celui sur lequel vous exécutez VirtualBox). Pour éviter d'avoir à modifier ce paramètre plus tard, il est possible d'affecter un espace assez élevé (100 Gio), mais de ne pas l'affecter directement en totalité !

Ensemble des étapes nécessaires à la création du disque virtuel de 100 Gio avec allocation de l'espace dynamiquement



← Crée une machine virtuelle

Disque dur

SI vous le souhaitez, vous pouvez ajouter un disque dur virtuel à la nouvelle machine. Vous pouvez soit créer un nouveau disque, soit en choisir un de la liste ou d'un autre emplacement en utilisant l'icône dossier.

Si vous avez besoin d'une configuration de stockage plus complexe, vous pouvez sauter cette étape et modifier les réglages de la machine une fois celle-ci créée.

La taille du disque dur recommandée est de **50,00 Gio**.

- ☐ Ne pas ajouter de disque dur virtuel
- ☒ Créer un disque dur virtuel maintenant
- ☐ Utiliser un fichier de disque dur virtuel existant

Windows 10_1.vdi (Normal, 50,10 Gio)



Créer

Annuler

Créer un nouveau disque

← Créer un disque dur virtuel

Type de fichier de disque dur

Choisissez le type de fichier que vous désirez utiliser pour le nouveau disque virtuel. Si vous n'avez pas besoin de l'utiliser avec d'autres logiciels de virtualisation vous pouvez laisser ce paramètre inchangé.

- ☒ VDI (VirtualBox Disk Image)
- ☐ VHD (Disque dur Virtuel)
- ☐ VMDK (Virtual Machine Disk)

Mode expert

Suivant >

Annuler

Sélectionner le type de format de stockage

← Créer un disque dur virtuel

Stockage sur disque dur physique

Veillez choisir si le nouveau fichier de disque dur virtuel doit croître au fur et à mesure (allocation dynamique) ou bien s'il doit être créé à sa taille maximale (taille fixe).

Un fichier de disque dur **alloué dynamiquement** n'utilisera d'espace sur votre disque dur physique qu'au fur et à mesure qu'il se remplira (jusqu'à une **taille fixe maximale**), **cependant il ne se réduira pas automatiquement lorsque de l'espace sur celui-ci sera libéré.**

Un fichier de disque dur à **taille fixe** sera plus long à créer sur certains systèmes mais sera souvent plus rapide à utiliser.

☒ Dynamiquement alloué

☐ Taille fixe

Suivant >

Annuler

Spécifier le type d'allocation de l'espace disque

← Créer un disque dur virtuel

Emplacement du fichier et taille

Veuillez saisir un nom pour le nouveau fichier de disque dur virtuel dans la boîte ci-dessous ou cliquez sur l'icône dossier pour choisir un autre dossier dans lequel le créer.

C:\Users\Dam\VirtualBox VMs\Windows Server 2019 Standard\Windows Server 2019 Standard.vdi 

Choisissez la taille du disque dur virtuel en mégaoctets. Cette taille est la limite de la quantité de données de fichiers qu'une machine virtuelle sera capable de stocker sur le disque dur.

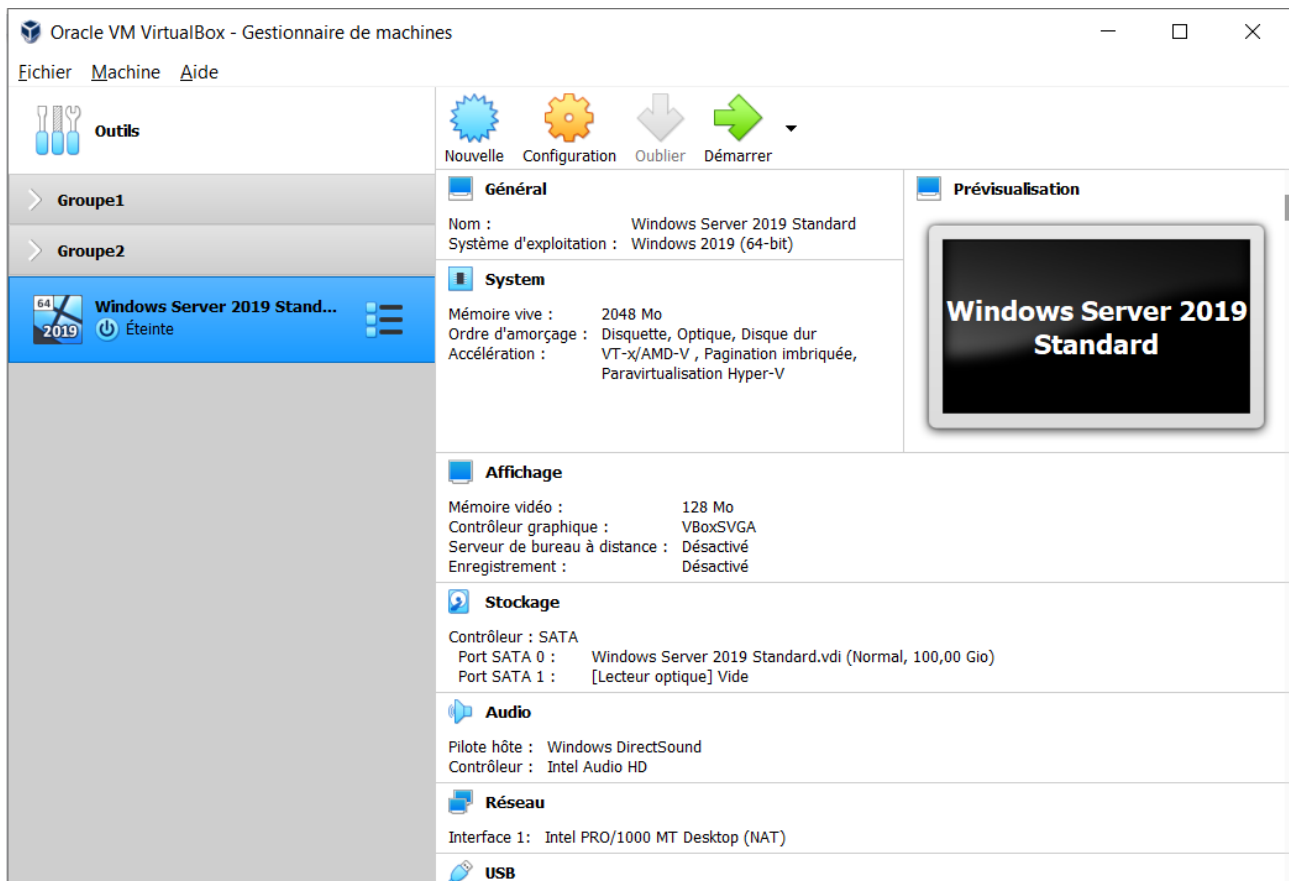


Créer

Annuler

Nommer le disque et déclarer l'emplacement du fichier de stockage

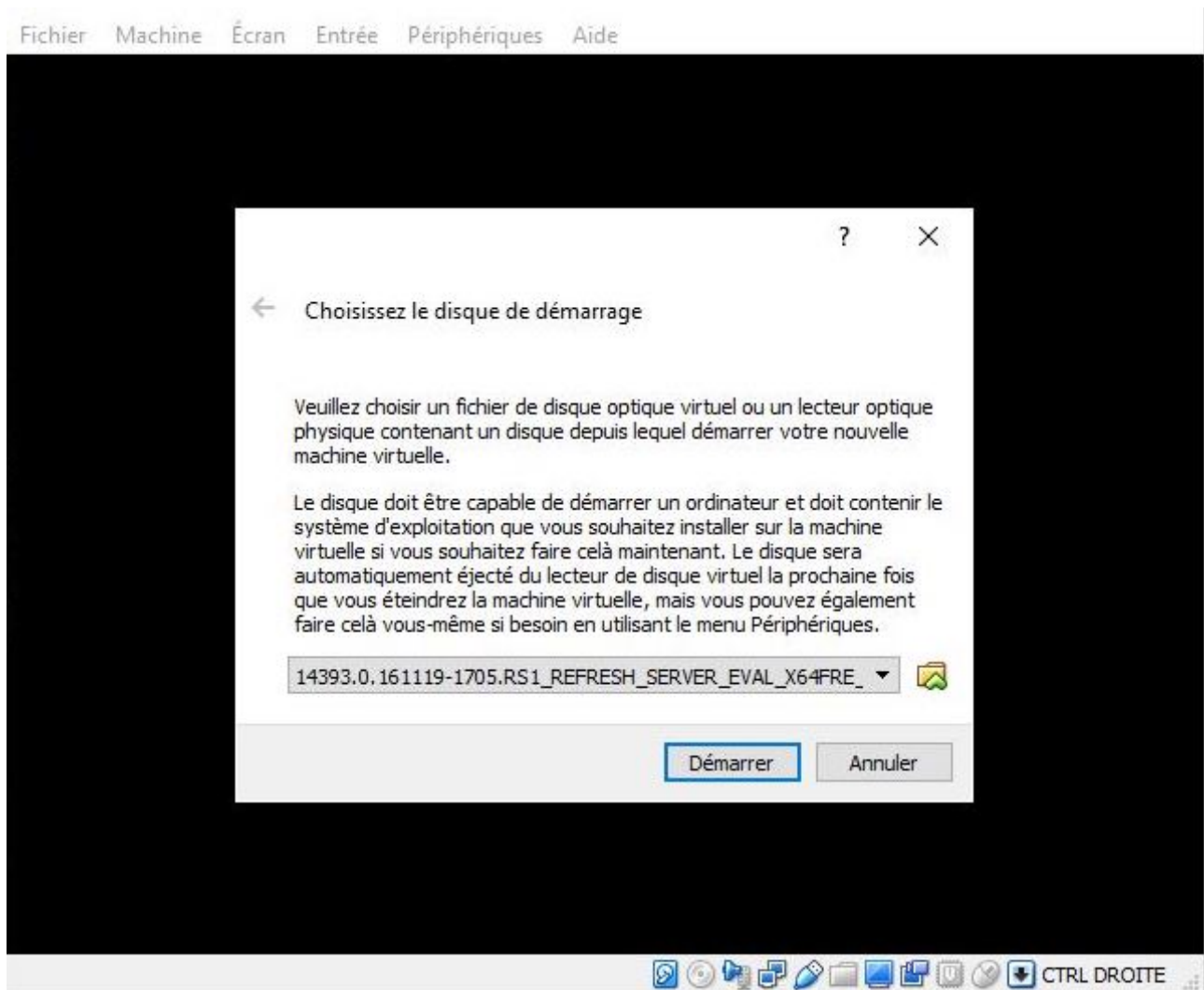
Voilà, une fois cette dernière étape terminée, votre machine est prête à démarrer et vous voyez la configuration matérielle dont elle dispose :



Machine virtuelle créée et prête à démarrer

Par défaut, votre machine virtuelle est normalement équipée d'un disque dur utilisant un contrôleur SATA. Vous pouvez vérifier cela dans la partie "Stockage". Ce n'est pas obligatoire, mais un disque SATA rendra votre machine virtuelle bien plus rapide notamment lors de l'installation.

Une fois la configuration matérielle vérifiée, cliquez sur "Démarrer", et la première chose qui vous sera demandée est le fichier ISO que vous avez téléchargé précédemment :



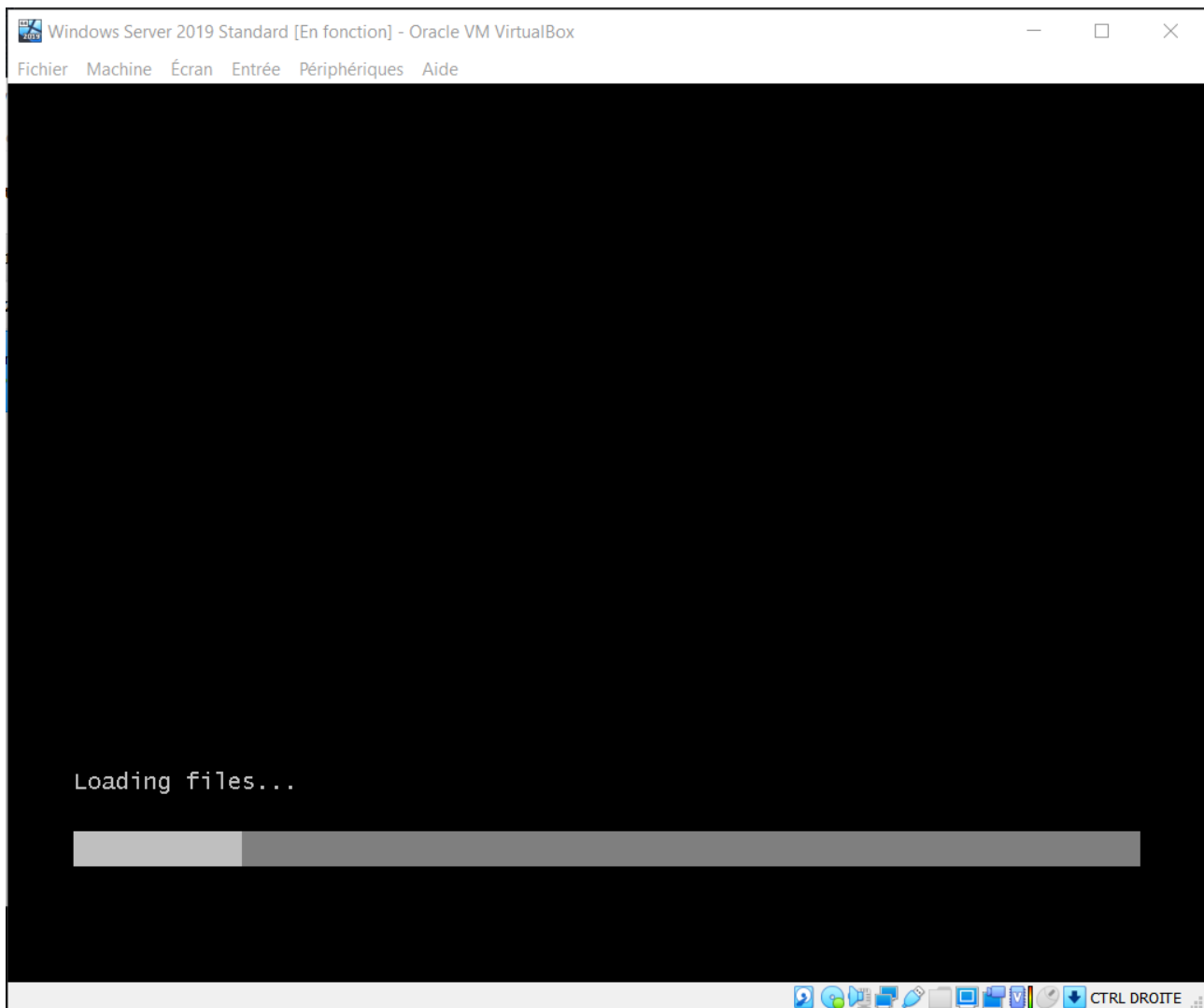
Premier écran de démarrage de votre machine virtuelle

Si toutefois vous n'arrivez pas à cet écran, vous avez la possibilité de **sélectionner** votre ISO via le menu "Périphériques" puis "Lecteurs optiques", et d'**insérer** votre ISO dans le lecteur CD virtuel de votre machine !

Bravo, vous avez préparé votre machine virtuelle ! Maintenant, je vous propose d'installer votre tout premier Windows Server 2019 Standard !

Maîtrisez l'installation de Windows Server

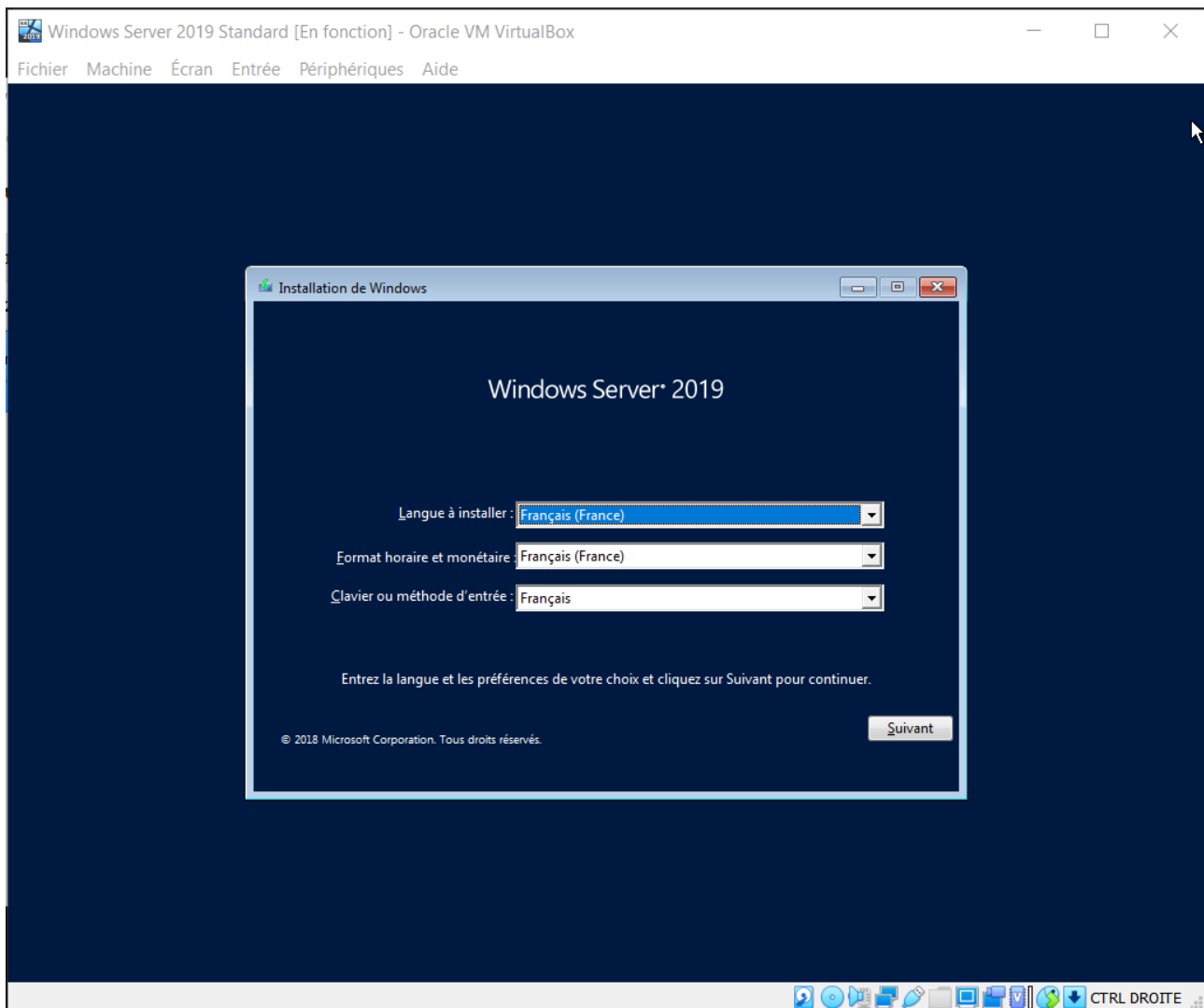
Si vous avez suivi les différentes étapes précédentes, vous devriez arriver sur l'écran suivant :



Écran de démarrage de la machine virtuelle chargeant l'ISO Windows Server

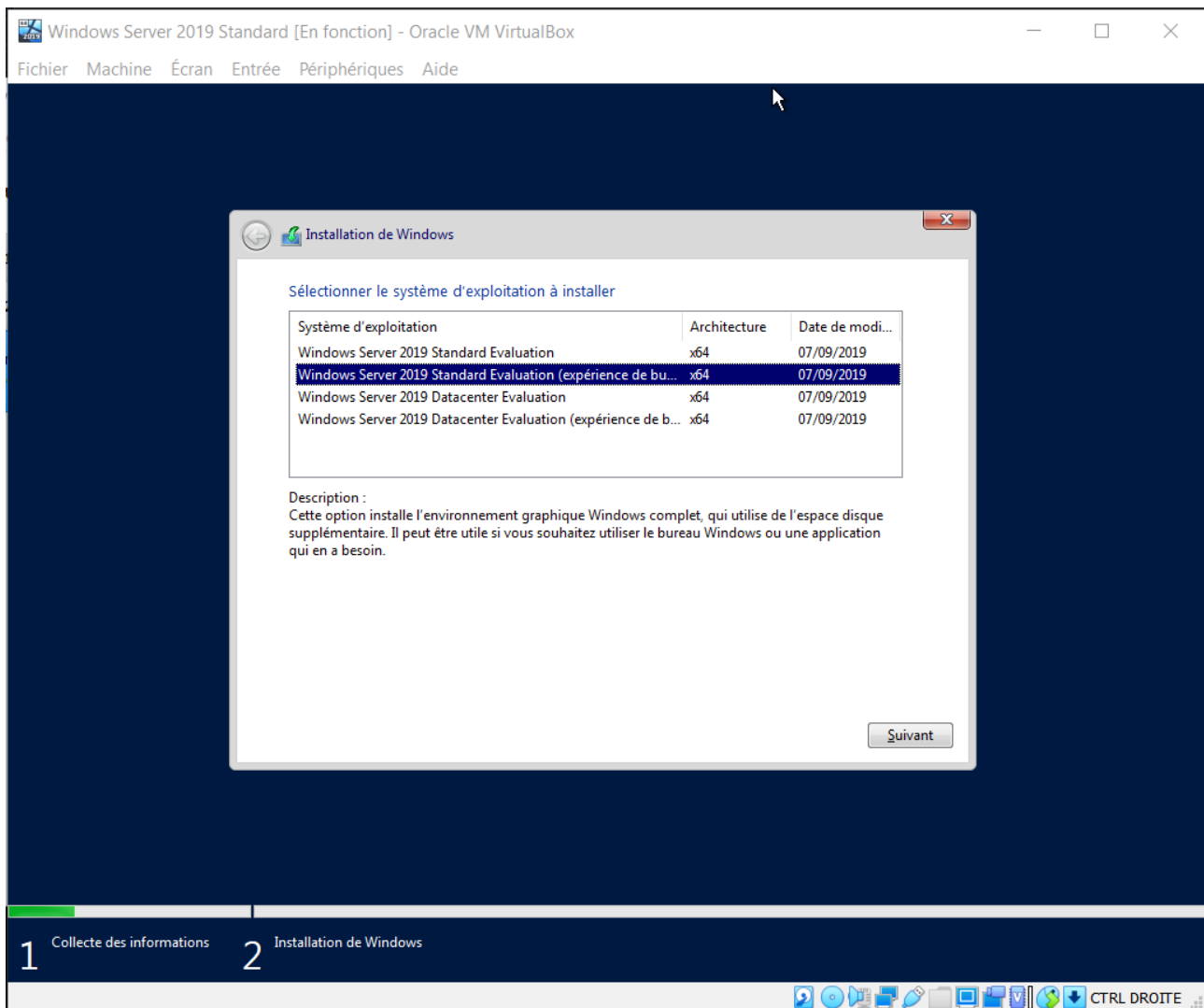
Vous connaissez sûrement la réputation de Microsoft : le “**cliquodrome**”, car, du fait de son interface graphique, tout se fait en quelques clics ! Eh bien, c’est toujours très vrai, notamment pour les installations de systèmes d’exploitation. Microsoft aime simplifier la vie des utilisateurs et administrateurs.

Après ce premier chargement, vous tombez sur un écran vous demandant de cliquer sur “**Suivant**”.



Écran de validation de la langue de Windows

En cliquant sur **“Suivant”**, vous avez enfin la possibilité de lancer l’installation, via le bouton **“Installer maintenant”**. Vous arrivez ensuite sur un écran de choix assez étrange :



Écran de choix du système d'exploitation

Ici, vous avez la possibilité de choisir l'édition Standard ou Datacenter (un média identique pour les deux éditions, c'est plus simple) ; par contre, il vous est fait mention d'une expérience utilisateur, qu'est-ce donc que cette histoire d'expérience ?

Si vous sélectionnez le premier choix, "Windows Server 2019 Standard Evaluation", vous serez bien étonné de découvrir que cette option **ne vous donne pas** accès à des fenêtres (dommage pour un produit qui s'appelle "Windows" : "Fenêtres", en anglais). Vous installez la version "Core" de Windows Server 2019 Standard. Cette version permet de **réduire** les éléments "superflus" chargés au démarrage du serveur. Parmi ces éléments, se trouvent :

- **L'interface graphique !**
- L'explorateur (pour afficher les fichiers).
- Edge.
- L'observateur d'événements.
- ...

Je m'arrêterai ici car la liste est assez longue !

Pourquoi avoir une édition de Windows sans *windows* (fenêtres) ? Eh bien, pour réduire les ressources nécessaires **pour faire fonctionner** le serveur, afin que ce dernier puisse concentrer ses ressources sur les services, rôles et fonctionnalités qu'il va fournir aux utilisateurs et clients.

À titre de comparaison, il est nécessaire d'avoir au minimum 2 048 Mio (2 Gio) pour pouvoir lancer Windows Server 2019 Standard avec son interface graphique (très similaire à Windows 10, qui plus est), alors que Windows 2019 Core ne nécessite que 512 Mio de RAM. Oui, vous avez bien lu, seulement 512 Mio.

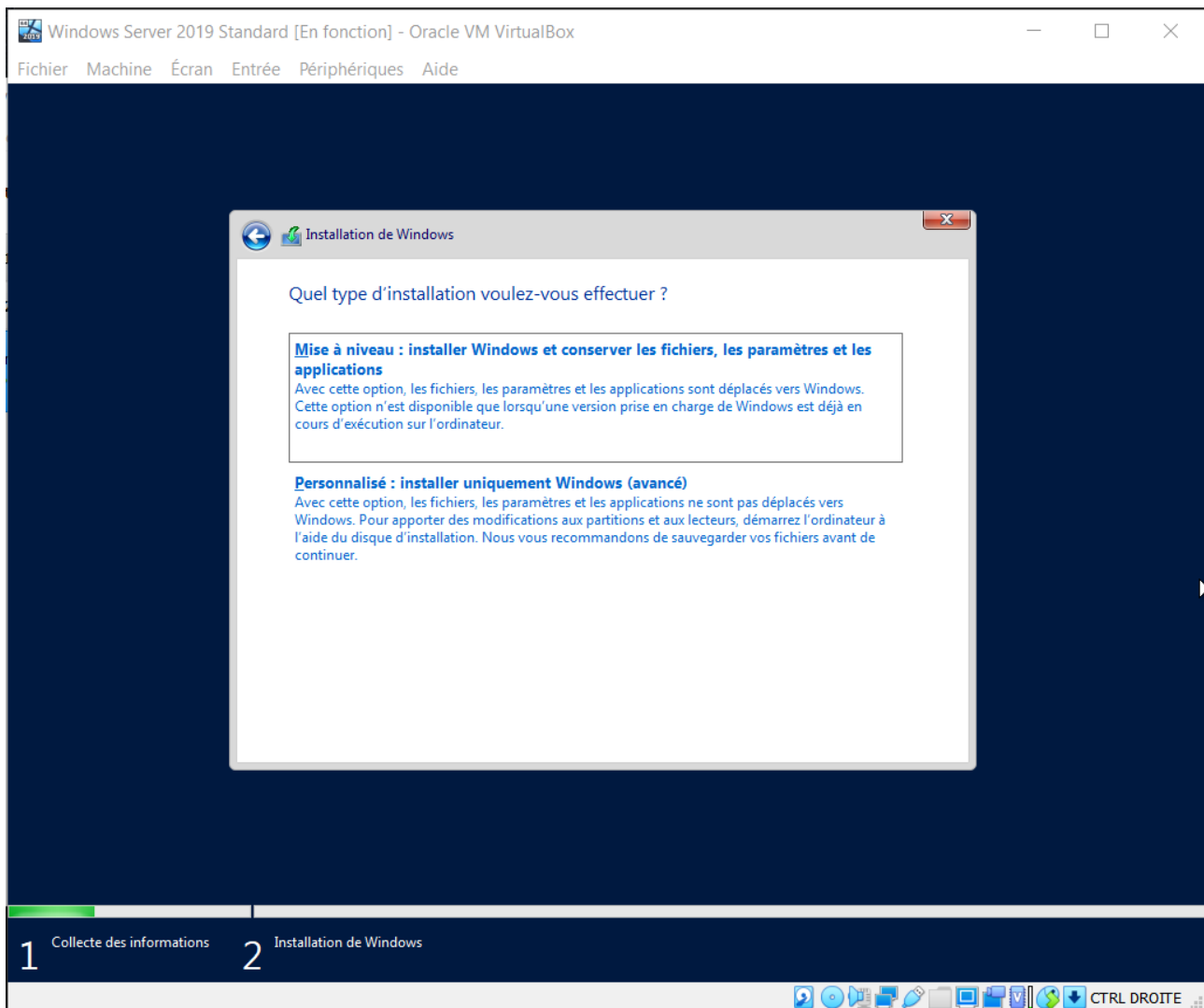
Comment effectuer une administration sans interface graphique ?

Eh bien comme sous Linux, en ligne de commande ! PowerShell permet de lancer toutes les commandes utiles, et de reproduire tout ce qui peut être fait graphiquement en ligne de commande.

Si vous le souhaitez, vous avez également la possibilité de mettre en place de l'administration à distance, via la console d'administration à distance de Windows 10 ; ainsi vous retrouverez les outils graphiques habituels, mais via un poste d'administration (dédié).

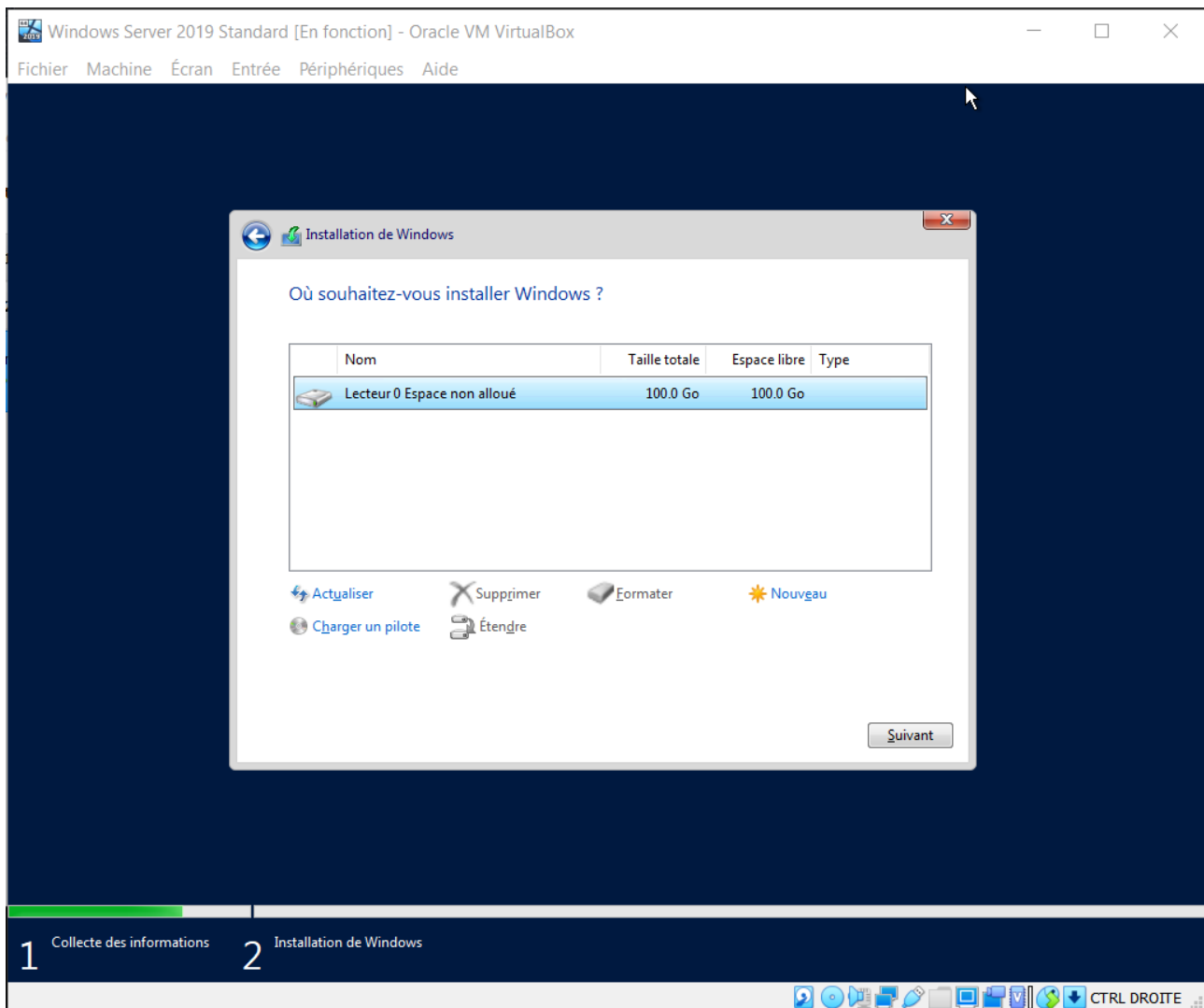
Cette mise en place d'administration à distance de Windows 10 est possible depuis un gestionnaire de serveur venant d'un autre serveur (si présent dans un domaine), qui dispose également d'une interface graphique.

Je vous propose de rester sur **une expérience utilisateur** "à la Microsoft" avec un **environnement graphique simple** ; sélectionnez donc "Windows Server 2019 Standard Evaluation (Expérience utilisateur...)". Après avoir fait ce choix et validé les avis et conditions du contrat de licence, vous arrivez sur l'écran de choix du type d'installation :



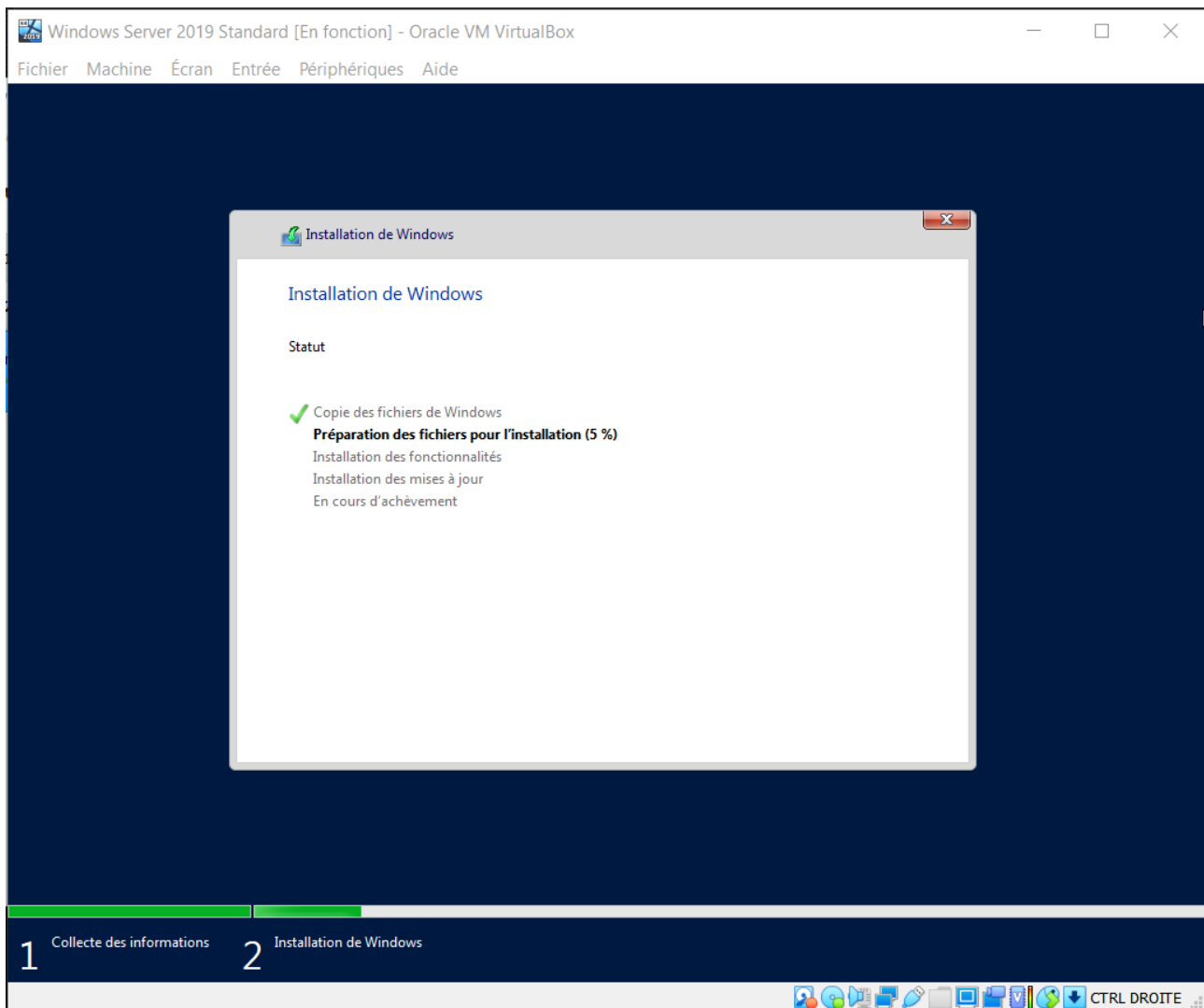
Écran de choix du type d'installation

Choisissez l'option "Personnalisé", afin de maîtriser toutes les configurations de cette installation :



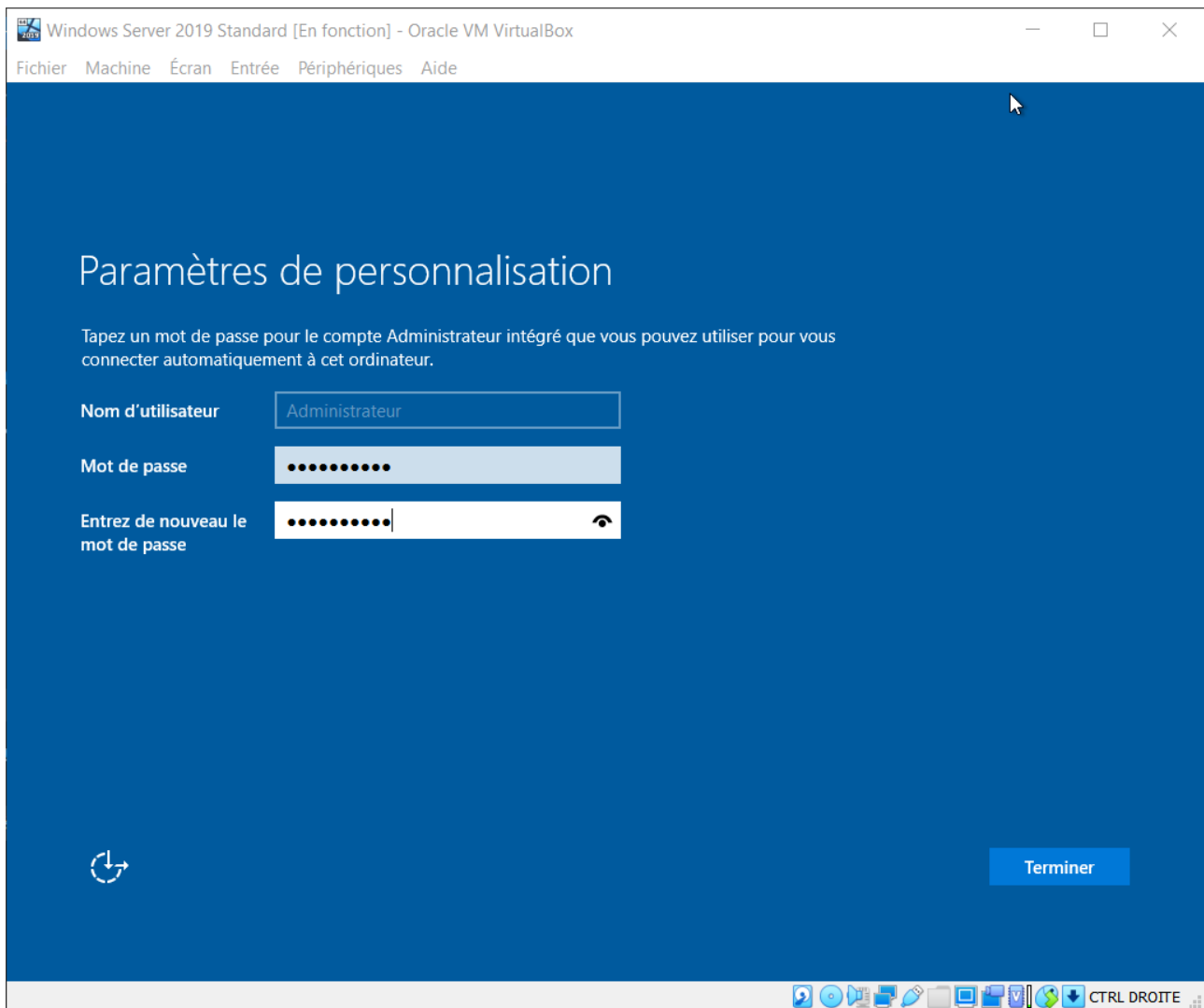
Sélection du disque d'installation

Vous retrouverez votre disque de 100 Gio. Cliquez sur **"Suivant"** et... c'est tout ! Vous avez remarqué ? Hormis quelques clics, rien de spécial pour le moment. Merci Microsoft !



Installation de Windows Server 2019

Une fois cette *looongue* étape (qui peut ne durer que quelques minutes si votre ISO et le disque dur de la machine virtuelle utilisent un contrôleur SATA), Windows Server vous demandera de personnaliser votre installation. Première personnalisation, le mot de passe du compte Administrateur local :

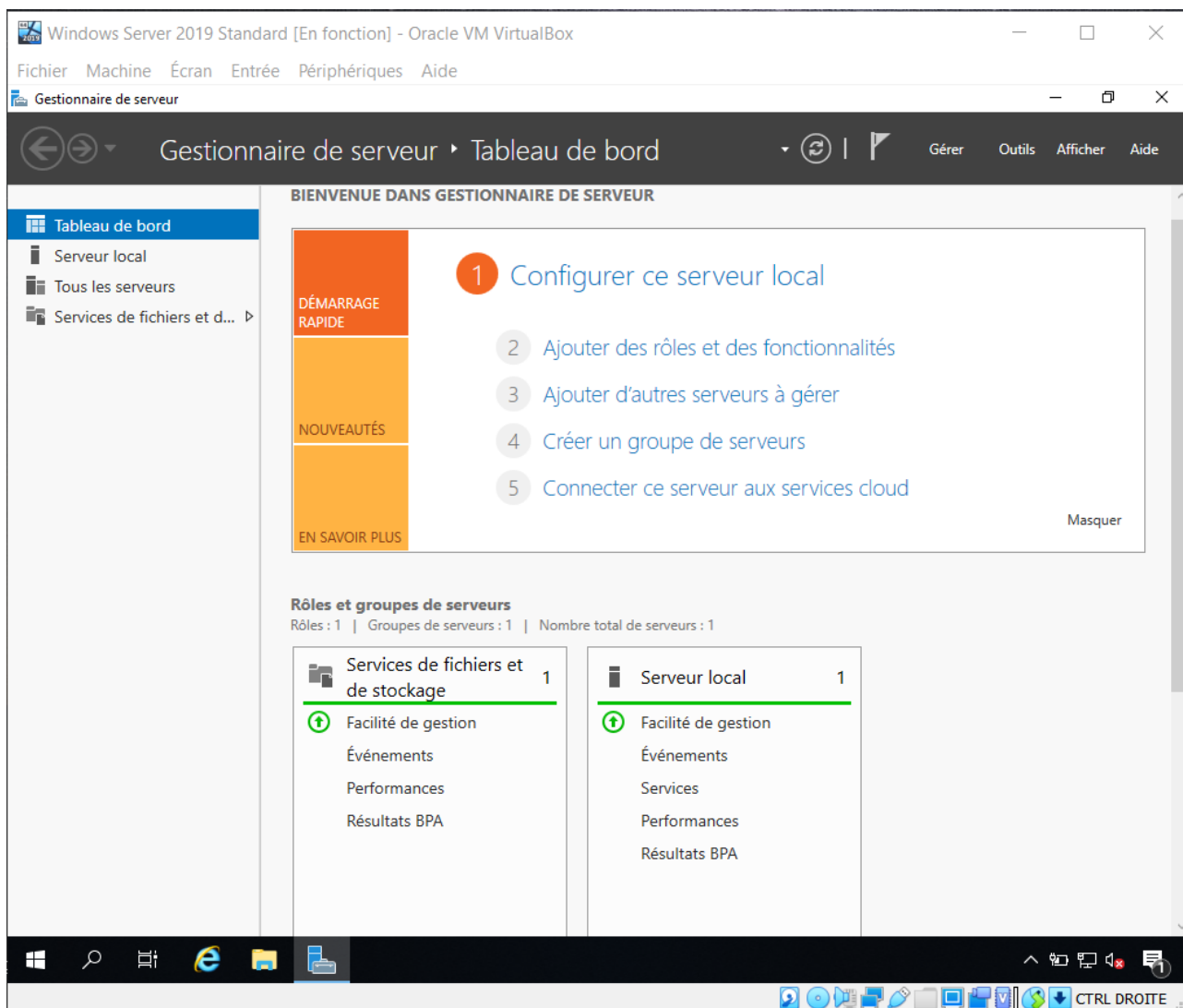


Personnalisation du mot de passe

Une fois cette personnalisation terminée (c'était long !), vous voici **devant l'écran de connexion** de Windows Server. **Identifiez-vous** sur le serveur avec le mot de passe **Administrateur** (il n'y a actuellement que ce compte de disponible).

Le profil local du compte Administrateur local est en cours de création, ce qui rend la première authentification un peu longue.

Une fois terminé, vous devriez arriver sur le bureau de votre serveur. Vous remarquez que le chargement n'est pas totalement terminé, Windows Server va lancer **automatiquement** le gestionnaire de serveur :



Gestionnaire de serveur lancé automatiquement à l'ouverture de session

Voilà, vous avez installé votre premier Windows Server Standard avec interface graphique. Je vous propose d'en rester là pour ce chapitre, car vous allez prendre en main le gestionnaire de serveur dès le chapitre suivant !

Pourquoi une version récente de Windows Server ?

Attendez, avant de passer à la suite, quelques informations annexes qui pourraient vous intéresser. Lorsque vous devrez prendre vos marques dans une entreprise déjà existante, vous trouverez d'autres versions de Windows Server.

Pourquoi ?

Tout simplement parce que l'entreprise dans laquelle vous arrivez dispose d'une histoire informatique en plus de son histoire propre. La mise à jour d'un serveur existant vers une nouvelle version est une étape **complexe**, car elle nécessite l'arrêt des serveurs. La sécurité des données étant au cœur des préoccupations, il devient de plus en plus **compliqué** d'éteindre des services. Cela aurait pour conséquences de rendre les données indisponibles en rendant les services indisponibles. Quel rapport avec la sécurité ? Eh bien l'un des critères de sécurité des données est la **disponibilité** !

Alors une question se pose :

Pourquoi travailler à changer de version de Windows Server pour une plus récente ?

Eh bien, les dernières versions de Windows apportent toujours de nombreuses fonctionnalités et correctifs. Par exemple, par rapport aux anciennes versions, Windows Server 2019 apporte entre autres :

- Le cryptage des machines virtuelles ;
- L'amélioration de la protection avancée de Windows Defender ;
- Le cloud hybride ;
- Les évolutions de la plateforme d'applications...

Windows Server 2022 apportera quant à lui :

- La virtualisation imbriquée (créer une machine virtuelle dans une machine virtuelle) ;
- Le navigateur Edge qui remplace définitivement Internet Explorer ;
- La compression automatique des fichiers avant leur transfert sur le réseau.

Vous l'avez compris, même si la mise à jour d'un système d'exploitation est complexe, les nouvelles fonctionnalités peuvent apporter un réel avantage et vous permettre d'augmenter la sécurité de votre système informatique, et donc plus généralement de votre système d'information !

Découvrez des ressources additionnelles

Si vous êtes à l'aise avec la langue de Shakespeare, voici quelques liens utiles qui compléteront parfaitement ce chapitre :

- [Site Microsoft Windows Server](#) (quelques ressources en français) ;
- Des [labs virtuels pour s'exercer sur les services/rôles/versions de Windows Server](#).

Vous voulez découvrir en profondeur les possibilités offertes par une installation sans interface graphique, rendez-vous ici :

- [Documentation en ligne sur Windows Server Core](#).

Si vous voulez en savoir plus sur l'administration à distance d'un Windows Server Core, rendez-vous ici :

- [Outils d'administration à distance de Windows Server](#).

Pour en savoir plus, rendez-vous à l'adresse suivante pour comparer les versions de Windows Server :

- [Comparaison des éditions de Windows Server](#).

En résumé

- **Windows Server** est un système d'exploitation **dédié aux services et à la mise en réseau**.

- Il existe de **nombreuses** éditions et distributions de **Windows Server 2019** (tout comme pour toutes les autres versions).
- Il convient de correctement **choisir la licence en fonction de ses besoins**, et surtout **d'anticiper** ses besoins futurs.
- Les différentes versions de Windows Server apportent avec le temps de **nouvelles fonctionnalités**, une meilleure prise en charge des rôles critiques, et souvent une meilleure compatibilité avec les **nouvelles technologies**.
- Il existe une version **sans interface graphique** de Windows Server, fonctionnant sur le principe de Linux/Unix (via des **lignes de commande**).
- La version 2022 de Windows Server est déjà sortie mais ne sera pas utilisée dans ce cours pour éviter certains problèmes de compatibilité.

Dans le prochain chapitre, vous apprendrez à mettre en réseau votre système Windows Server. C'est parti !

- <#>

Dans ce chapitre, vous allez préparer votre Windows Server à la mise en réseau. **Pourquoi un chapitre dédié ?** Eh bien, parce que la plupart des erreurs arrivent à ce moment. Il convient de bien savoir ce que l'on fait et peut faire, car Microsoft a **automatisé** de nombreux points.

Si vous ne préparez pas votre système, vous allez créer de belles vulnérabilités pouvant porter préjudice à la sécurité de votre réseau et, pire, offrant un **accès non désiré** à votre serveur et donc aux données qu'il héberge ou gère !

Préparez votre machine virtuelle

Cette première étape sur votre machine virtuelle correspond au raccordement d'un câble réseau sur un serveur physique. Pour le moment et par défaut, sous VirtualBox votre machine est à peu près protégée de l'extérieur. Elle n'a accès qu'au réseau NAT géré par VirtualBox.

En résumé, votre serveur n'est pas accessible d'Internet, mais il peut y avoir accès !

Allez voir la configuration du réseau ; si votre VirtualBox est correctement configurée, vous devriez avoir **une adresse IP, un masque, une passerelle et un serveur DNS** par défaut !

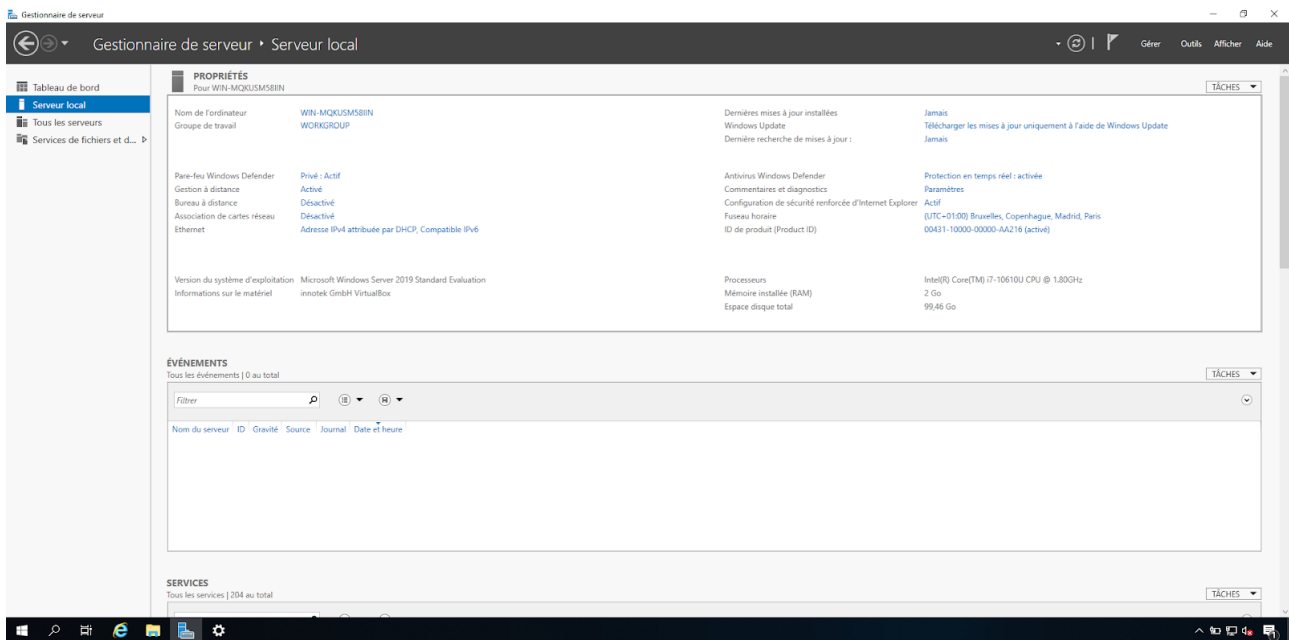
Maintenant que j'ai tout ça, par quoi je commence ? Quelle est la première chose à faire ?

Tout comme sur une distribution Linux où vous lanceriez un `sudo apt update` (ou `sudo apt-get update`) suivi d'un `sudo apt upgrade` (ou `sudo apt-get upgrade`), eh bien vous allez lancer une **vérification des correctifs disponibles** pour vos édition, version et option d'installation de Windows auprès des serveurs de Microsoft !

Vous devriez obtenir un résultat plus ou moins satisfaisant ; je vous laisse effectuer ces mises à jour tranquillement, et on se retrouve tout de suite après !

Comment faire ?

Eh bien rendez-vous sur le gestionnaire de serveur, dans la partie “Serveur local” :



Gestionnaire de serveur -> Serveur Local

Vous avez ici toutes les informations nécessaires à la mise en réseau :

Le nom de votre serveur, ici **WIN-1HOJWCE0IT**, le groupe de travail, ici **WORKGROUP**, et sur la même ligne les dernières mises à jour installées, le mode de mise à jour ("Télécharger les mises à jours uniquement à l'aide de...") et la date de la dernière recherche ! Il vous suffit donc de cliquer sur “**Télécharger les mises à jours uniquement à l'aide de...**” :

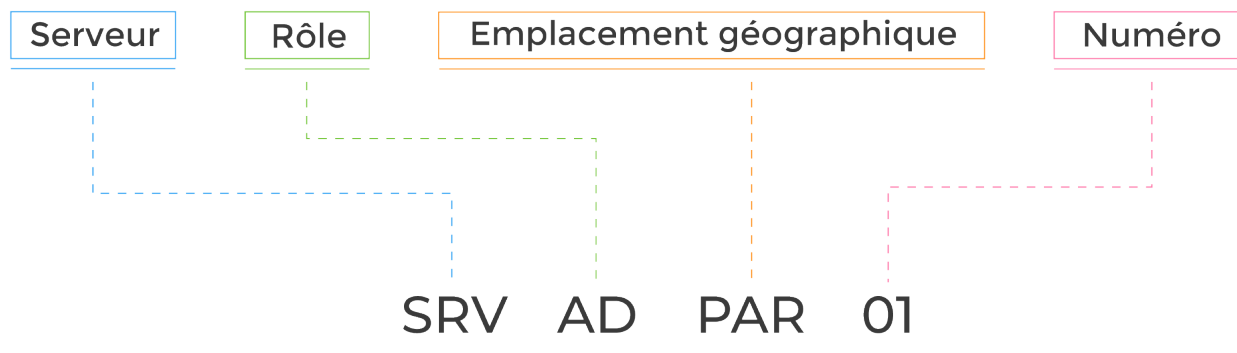
Très bien, votre Windows Server est maintenant fin prêt ! Occupez-vous maintenant de lui donner un nom qui soit plus intéressant que le nom généré aléatoirement par Microsoft !

Nommez un serveur

Si vous avez déjà suivi le cours sur [Active Directory](#), vous savez que la nomenclature est une activité à ne pas prendre à la légère. En effet, nommer correctement un équipement, dans le cas présent, votre serveur, permettra de suivre son cycle de vie.

Aussi, il est important de ne pas nommer le serveur en fonction de son rôle ou de son nom public, mais d'opter pour une nomenclature cohérente, logique et simple. Sachez que, de toute façon, il sera possible de donner d'autres noms au serveur via le protocole DNS !

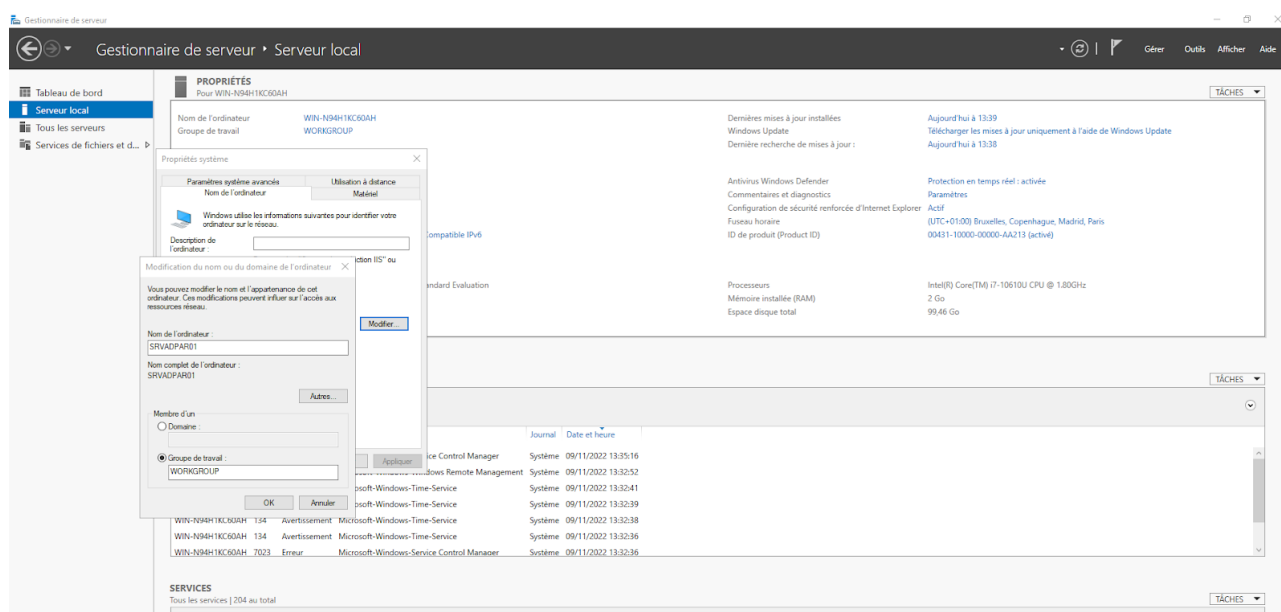
Ainsi, pour nommer vos serveurs, vous pouvez par exemple adopter une codification telle que **SRVADPAR01** pour un serveur (**SRV**) ayant le rôle **ADDS** situé à Paris (**PAR**) et étant le premier serveur de ce type (**01**).



Exemple de nommage

Ainsi, il sera simple de retrouver tous les serveurs hébergés à Paris, en effectuant une recherche sur **"*PAR*"**, ou de rechercher tous les serveurs Active Directory en effectuant la recherche **"*AD*"**. Je vous laisse réfléchir à une convention qui soit cohérente !

Pour renommer le serveur, cliquez simplement sur son nom dans le tableau de bord :



Renommer un serveur

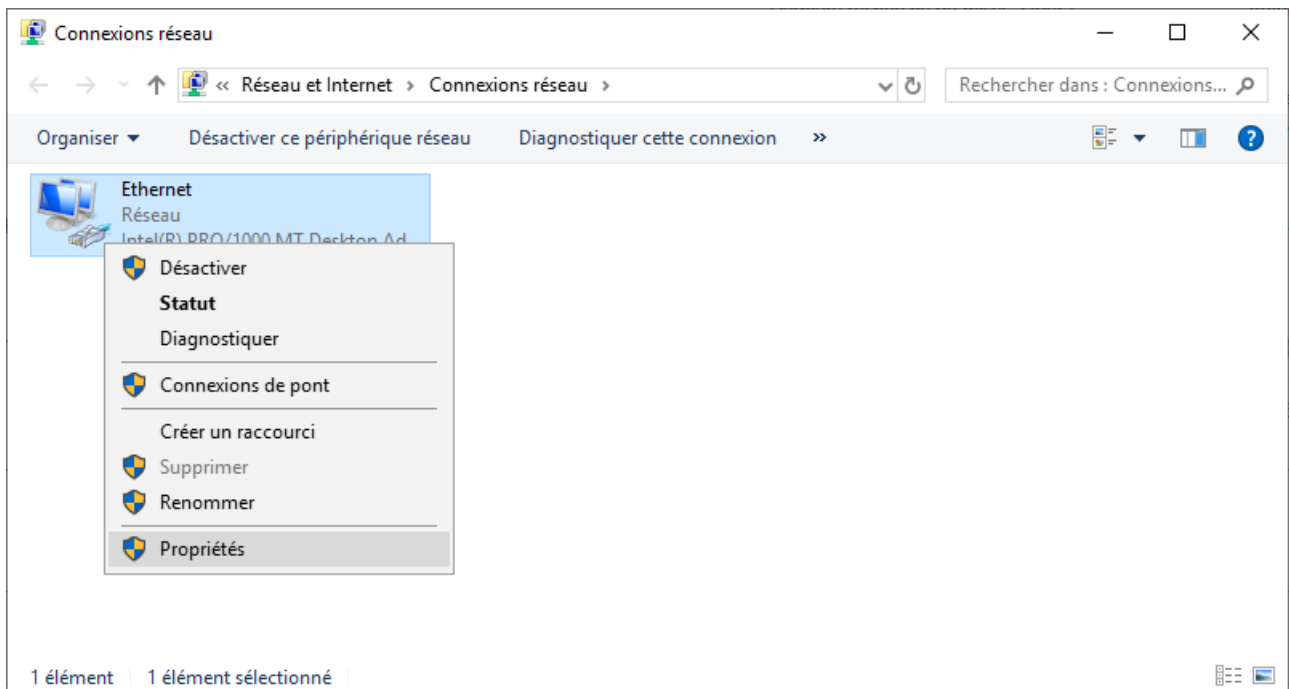
Il vous faudra redémarrer pour prendre en compte le changement de nom. Ensuite, il vous faut imaginer l'adresse IP de votre serveur au sein de votre réseau.

Configurez la couche TCP/IP de votre serveur

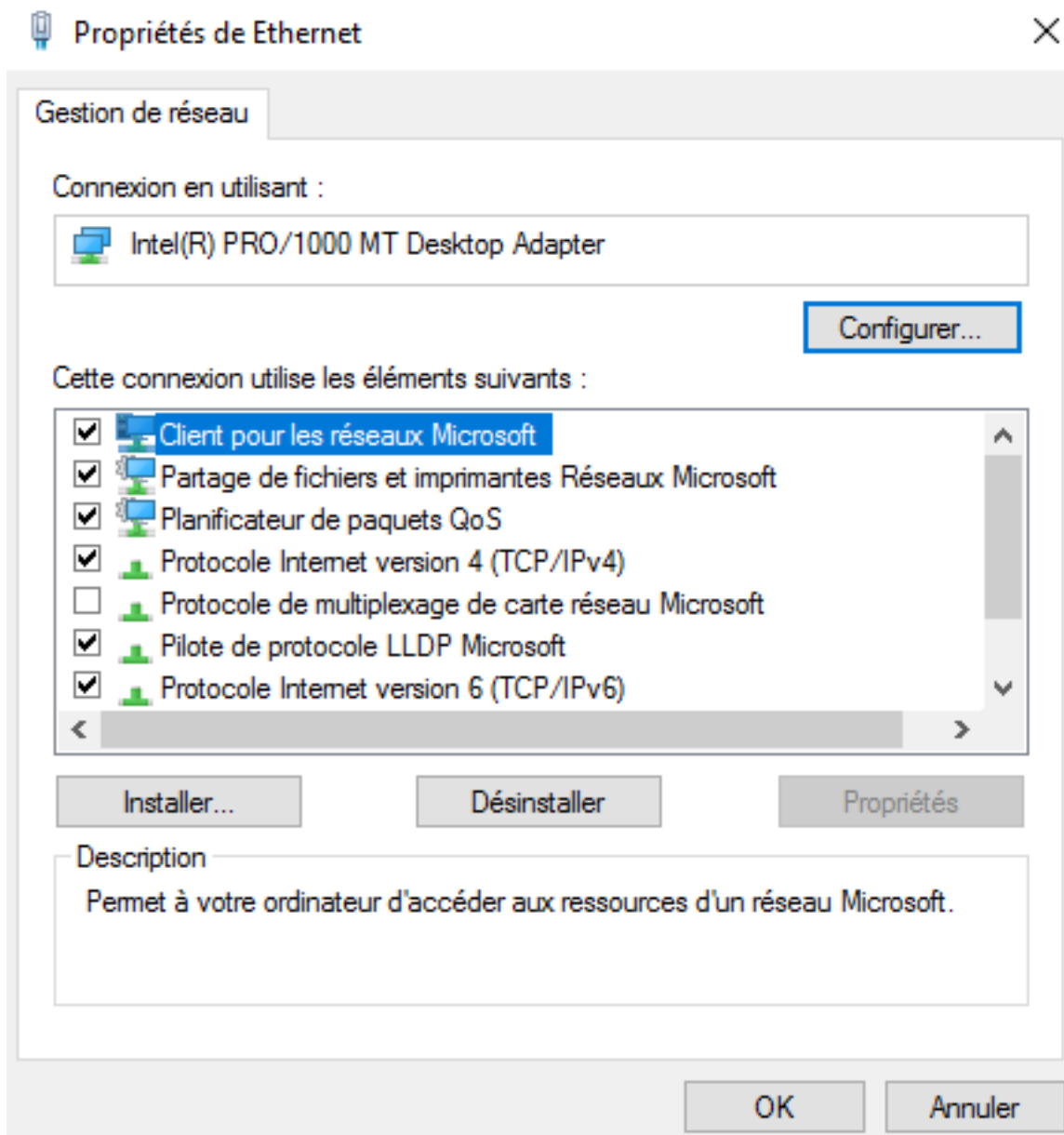
Cette étape dépendra de votre réseau, des éventuels sous-réseaux et de la stratégie d'adressage mise en œuvre !

Ici votre serveur se trouve derrière un routeur effectuant de la translation d'adresse ; il doit donc être (tant qu'il est dans ce mode de fonctionnement) configuré avec une adresse de ce réseau bien spécifique à VirtualBox.

Toujours sur le tableau de bord, si vous cliquez sur "**Adresse IPv4 attribuée par DHCP, compatible IPv6**", vous arrivez sur la configuration de vos interfaces réseaux. Si vous connaissez Windows en tant que système bureautique, vous ne serez pas perdu. Faites un clic droit sur la carte réseau active puis "Propriétés" :



Cartes réseau disponibles sur le serveur



Configuration d'une interface réseau sous Windows

Vous remarquerez que Microsoft active de nombreux services par défaut sur une interface :

- Client pour les réseaux Microsoft ;
- Partage de fichiers et imprimantes réseaux Microsoft ;
- Planificateur de paquets QoS ;
- Protocole Internet version 4 (TCP/IPv4) ;
- Pilote de protocole LLDP Microsoft ;
- Protocole Internet version 6 (TCP/IPv6) ;
- Répondeur de découverte de la topologie de la couche liaison ;
- Pilote E/S de mappage de découverte de topologie de la couche de liaison.

Par défaut, l'IPv6 est actif. Si votre réseau n'en a pas l'utilité, je vous invite à le **désactiver**.

Attention toutefois, certains rôles Microsoft utilisent ce protocole. Il peut être plus judicieux d'étudier le rôle en détail (ce que vous allez faire dans ce cours) pour comprendre comment il fonctionne, et ensuite décider de la pertinence de conserver IPv6 ou pas.

Ce n'est pas encore terminé ; sélectionnez les propriétés de "**Protocole Internet version 4 (TCP/IPv4)**" puis cliquez sur "**Avancés**" :

Paramètres TCP/IP avancés

Paramètres IP DNS WINS

Adresses IP

Adresse IP	Masque de sous-réseau
DHCP activé	

Ajouter... Modifier... Supprimer

Passerelles par défaut :

Passerelle	Métrique
------------	----------

Ajouter... Modifier... Supprimer

☒ Métrique automatique

Métrique de l'interface :

OK Annuler

Configuration avancée des paramètres TCP/IPv4

Le premier onglet vous permet de configurer toute la partie IP : adresse, masque, alias, passerelle(s).

Le second onglet, DNS, permet de configurer **tout ce qui se rapporte à la gestion des noms**. Une première zone permet de configurer les adresses des serveurs DNS :

Paramètres TCP/IP avancés



Paramètres IP **DNS** WINS

Adresses des serveurs DNS, dans l'ordre d'utilisation :




Les trois paramètres suivants sont appliqués à toutes les connexions pour lesquelles TCP/IP est activé. Pour la résolution des noms non qualifiés :

☒ Ajouter des suffixes DNS principaux et spécifiques aux connexions
 ☒ Ajouter des suffixes parents du suffixe DNS principal

☐ Ajouter ces suffixes DNS (dans l'ordre) :




Suffixe DNS pour cette connexion :

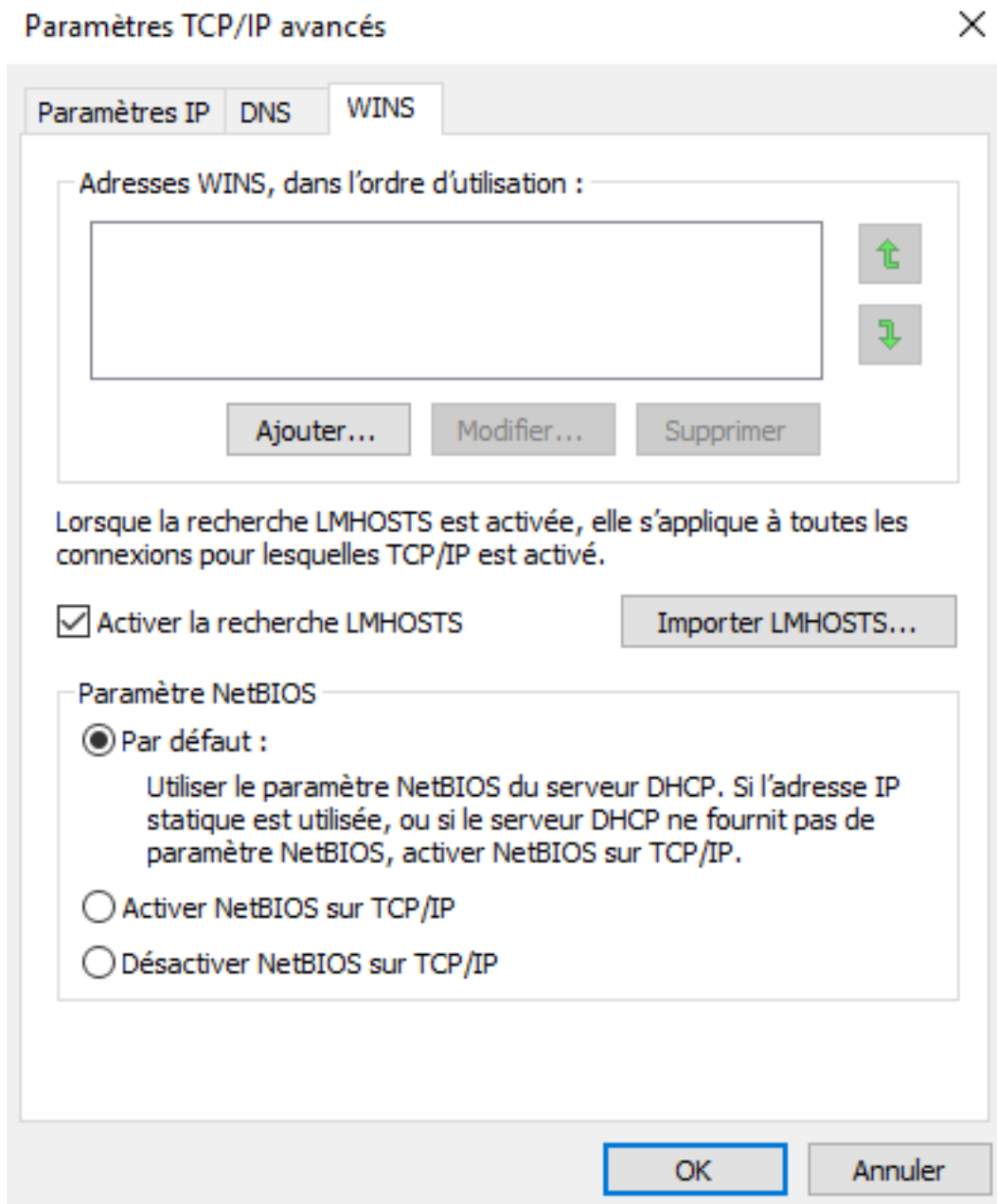
☒ Enregistrer les adresses de cette connexion dans le système DNS
☐ Utiliser le suffixe DNS de cette connexion pour l'enregistrement DNS

Paramètres DNS

Pour les connaisseurs de Linux, il s'agit de l'équivalent au fichier "resolv.conf". Dans la partie "Suffixes", vous allez pouvoir spécifier comment les requêtes DNS vont être faites au serveur, soit en direct, soit en ajoutant un suffixe.

À noter que vous pouvez aussi gérer l'enregistrement du nom de la machine et de son adresse dans votre DNS interne. Pas d'inquiétude, vous rentrerez en détail dans le rôle DNS dans les chapitres suivants.

Enfin, un dernier onglet, **WINS**, est présent. Il s'agit d'un protocole similaire au **DNS** mais propre à Microsoft et Windows (**Windows Internet Naming Service**). Il était très utilisé, voire obligatoire avant les années 2000 et la démocratisation de l'**Active Directory** (qui utilise le DNS). Il permettait de retrouver une adresse IP à partir d'un nom NetBIOS :



Paramètres WINS

Qu'est ce que NetBIOS ? En plus il est activé par défaut ?!

NetBIOS n'est **pas** un protocole ! C'est un système de nommage et une interface logicielle permettant d'établir des sessions entre différents ordinateurs d'un réseau. Ce programme de communication tend à disparaître au profit du protocole DNS. Il est cependant utilisé par Microsoft (toujours aujourd'hui) sur TCP/IP, notamment pour une compatibilité avec les systèmes Windows NT et XP.

Vous avez remarqué la case "Activer la recherche LMHOSTS". LMHOSTS est à NetBIOS ce que le fichier HOSTS est à DNS. Il permet de faire une association manuelle entre nom NetBIOS et adresse IP ! Là encore, c'est intéressant de le désactiver si vous n'avez plus besoin de NetBIOS.

Une fois que vous avez terminé ces configurations IP et plus généralement TCP/IP, votre serveur est prêt à être mis en réseau.

À moins qu'il ne reste un paramétrage à faire...

Paramétrez le pare-feu Windows

Windows intègre un pare-feu. À la manière de Linux et Iptables, cela permet de **verrouiller les flux** réseaux entrants et sortants de votre serveur ! Une sécurité supplémentaire indispensable aujourd'hui ! Pourquoi laisser le port 80 ouvert sur un serveur ne disposant pas du rôle Serveur Web ?

Encore une fois, rendez-vous sur le tableau de bord de votre serveur local :

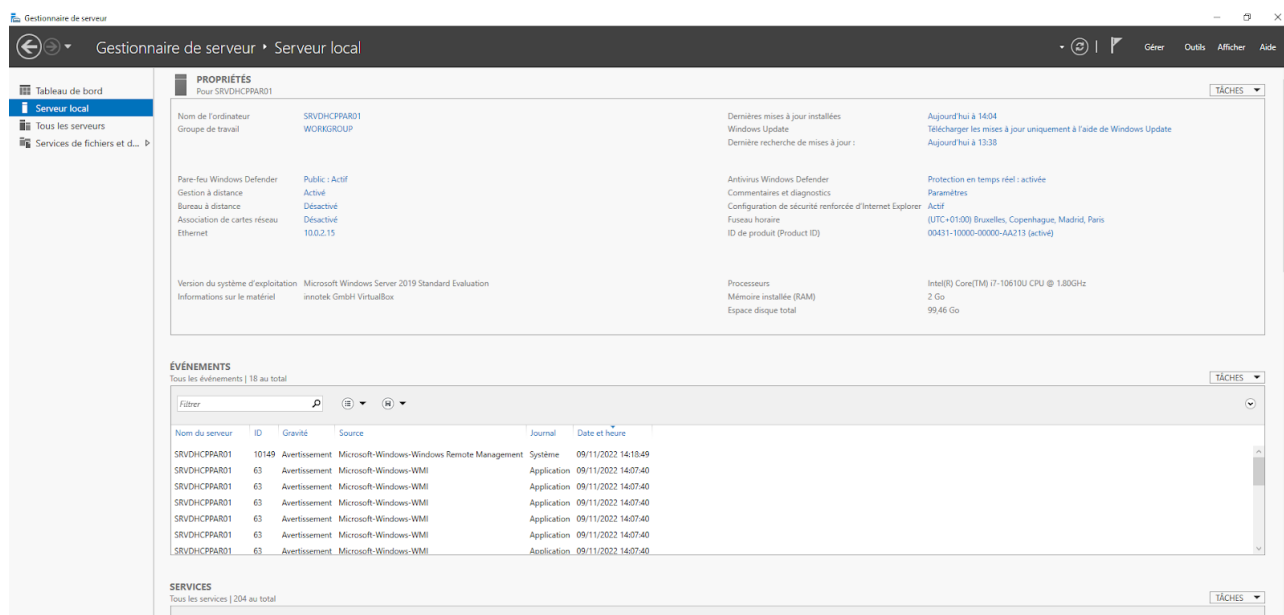


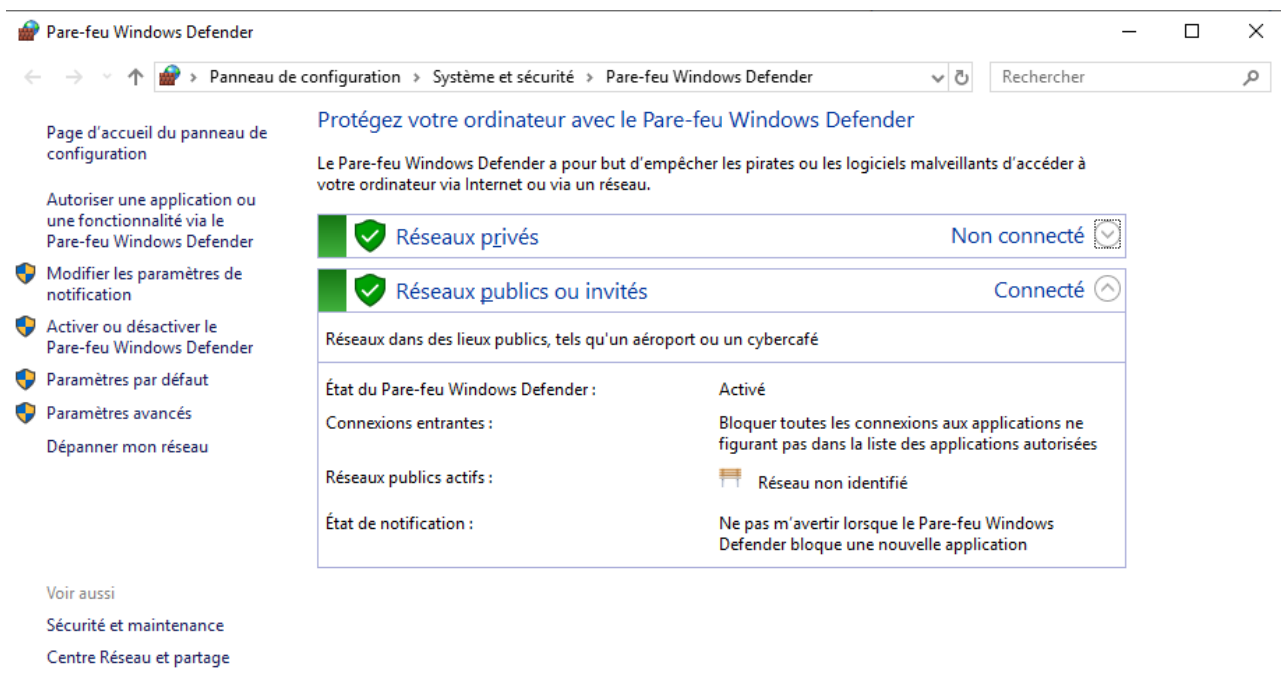
Tableau de bord

Comme vous le voyez, j'ai choisi de configurer un premier serveur DHCP à Paris SRVDHCPPAR01. J'ai maintenant uniquement de l'IPv4 avec une **adresse**, un **masque**, une **passerelle** et un **serveur** DNS (pas de NetBIOS et pas d'autres services réseaux Microsoft). Mon serveur est opérationnel.

Pour configurer le pare-feu vous avez plusieurs solutions:

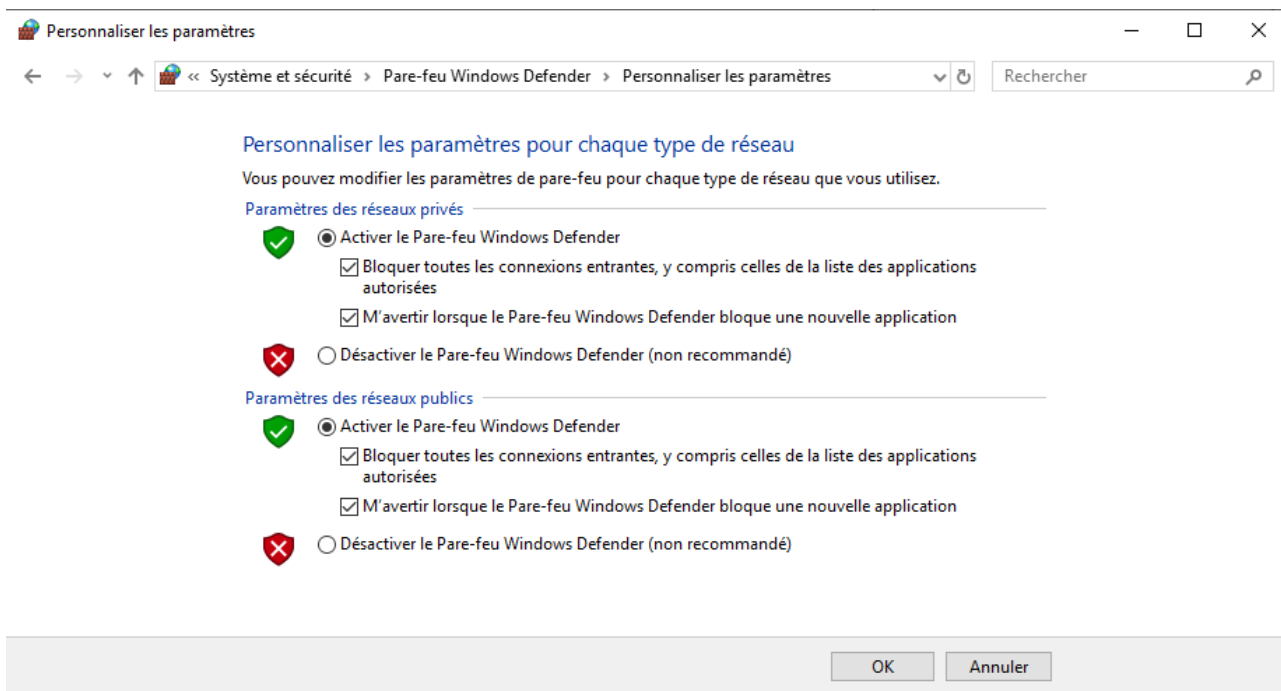
- Cliquez sur la ligne où est inscrit "**Pare-feu Windows : Privé Actif**" ;
- Entrez "Defender" (le nom du pare-feu Windows) dans la barre de recherche.

La première méthode permet d'accéder à une fenêtre de configuration simplifiée du pare-feu. Personnellement, j'utilise la deuxième méthode car elle ouvre une fenêtre offrant plus de paramètres de configurations.



Pare-feu Microsoft

Plutôt pas mal comme configuration par défaut : il bloque **toutes les connexions** aux applications ne figurant pas dans une liste ! Pour être serein, je vous propose de cliquer sur “**Modifier les paramètres de notification**” et de sélectionner les options “**Bloquer toutes les connexions et m’avertir en cas d’accès**” :



Pare-feu avec options renforcées

Ainsi, votre serveur pourra sortir sur le réseau (pratique pour configurer les rôles, fonctionnalités et services), mais ne sera pas accessible sur le réseau !

À noter que cette partie pare-feu peut être faite en premier. Le fait d’être derrière le mécanisme de NAT de VirtualBox permet de faire cet écart.

Vous avez remarqué que Windows classe automatiquement vos réseaux dans 2 profils de connexion : les connexions privées et les connexions publiques. Cela permet notamment de créer 2 profils de configuration sur votre pare-feu : un profil avec des règles très restrictives lorsque vous utilisez un réseau public et un profil un peu plus souple lorsque que vous utilisez un réseau privé.

Voilà, votre serveur est prêt à être connecté à un réseau.

En résumé

- Un **serveur Windows doit être configuré** avant d'être connecté à un réseau (surtout si c'est un réseau de production !).
- Par défaut, un serveur Windows dispose de **nombreux paramètres à changer** en priorité (nom, IP, DNS, NetBIOS...).
- Le **pare-feu Windows intégré** permet de sécuriser les accès en bloquant tous les ports !
- La **mise en réseau** doit être **une action maîtrisée** !

Dans le prochain chapitre, vous apprendrez à maîtriser les différentes configurations (rôles, fonctionnalités, services...). Allons-y !

Dans ce troisième chapitre, je vous propose de prendre en main les différents rôles et fonctionnalités disponibles sous Windows Server. Attention, à ce stade je vous propose de comprendre le fonctionnement des rôles et fonctionnalités, pas encore de les mettre en œuvre. Si vous pensez déjà disposer de ces connaissances et compétences, rendez-vous au chapitre suivant, sinon, accrochez-vous.

Comprenez ce que sont un rôle, une fonctionnalité et un service

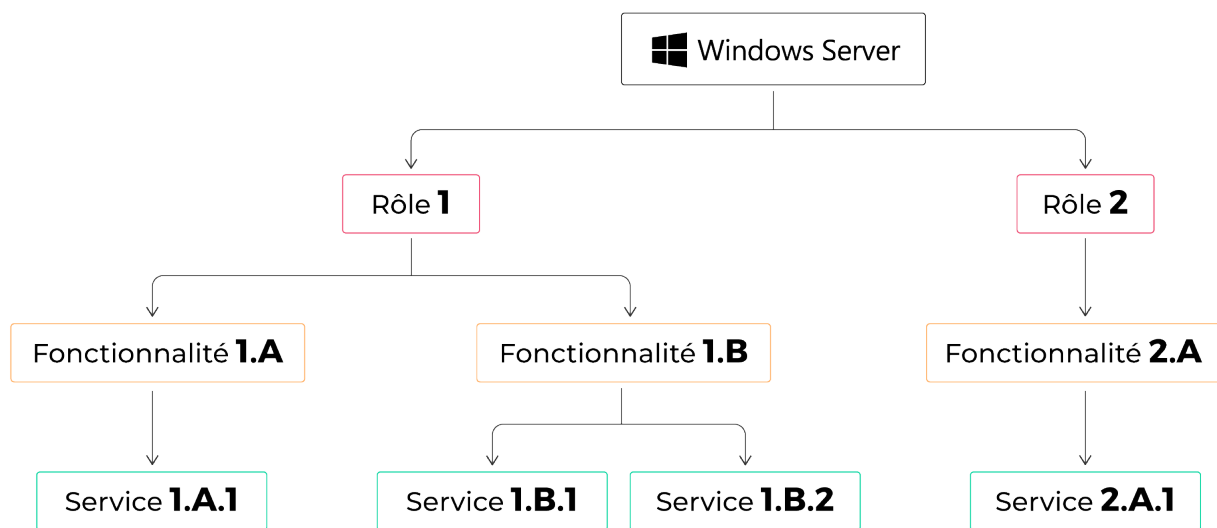
Rôle, fonctionnalité, service... Qu'est-ce qui se cache derrière ces termes ?

Eh bien, un serveur Windows va avoir dans une entreprise un (ou plusieurs) **rôle(s)**. Ce(s) rôle(s) peu(ven)t être de fournir/héberger des fichiers, gérer un annuaire (AD DS), gérer des certificats (AD CS), la configuration réseau (DHCP)...

Chacun de ces rôles, pour fonctionner, va s'appuyer sur des **services** (l'équivalent des démons sous Linux/Unix). Par exemple, le service `srvcost.exe` avec l'option "`-k DHCPServer`" est nécessaire au fonctionnement du rôle DHCP.

Enfin, pour être efficace, un rôle peut avoir besoin de **fonctionnalités**. Le rôle Serveur Web qui va héberger vos pages web peut avoir besoin d'une fonctionnalité .Net si vous avez besoin de développer votre application web à l'aide d'un langage dynamique.

Si l'on remet tout cela en perspective, on a donc :



Organisation d'un serveur Windows en rôles, fonctionnalités et services

N'est-ce pas plus clair maintenant ? Pas totalement, très bien, on continue alors !

Découvrez les rôles d'un serveur sous Windows

Depuis Windows Server 2008, les rôles n'ont pas beaucoup changé, la liste s'est précisée sans avoir été fondamentalement bouleversée. Voici la liste des rôles que vous **pouvez** installer sur un serveur Windows 2019 Standard :

- Accès à distance ;
- Attestation d'intégrité de l'appareil ;
- Hyper-V ;
- Serveur de télécopie ;
- Serveur DHCP ;
- Serveur DNS ;
- Serveur Web (IIS) ;
- Service Guardian hôte ;
- Services AD DS ;
- Services AD LDS ;
- Services AD RMS ;
- Services Bureau à distance ;

- Services d'activation en volume ;
- Services d'impression et de numérisation de documents ;
- Services de certificats Active Directory ;
- Services de déploiement Windows ;
- Services de fédération Active Directory (AD FS) ;
- Service de fichiers et de stockage ;
- Service de stratégie et d'accès réseau ;
- Service WSUS (Windows Server Update Services).

Il y a de quoi faire ! Vous avez remarqué comme la nomenclature des rôles fait appel aux termes "Services" et "Service"... Du coup, on pourrait croire qu'il s'agit de services, mais non, il s'agit bien des rôles que vos serveurs peuvent prendre au sein de votre réseau !

La liste étant longue, dans ce cours nous ne verrons que quelques-uns de ces rôles en détail.

Dans la partie 2, vous prendrez en main les rôles suivants :

- Serveur DHCP ;
- Serveur DNS ;
- Service de fichiers et de stockage (fonctionnalités de base) ;
- Service de stratégie et d'accès réseau.

Dans la partie 3, vous prendrez en main les rôles :

- Service WDS ;
- Service de fichiers et de stockage (fonctionnalité avancés) ;
- Service WSUS.

Dans la partie 4, les rôles suivants :

- Hyper-V ;
- Serveur Web.

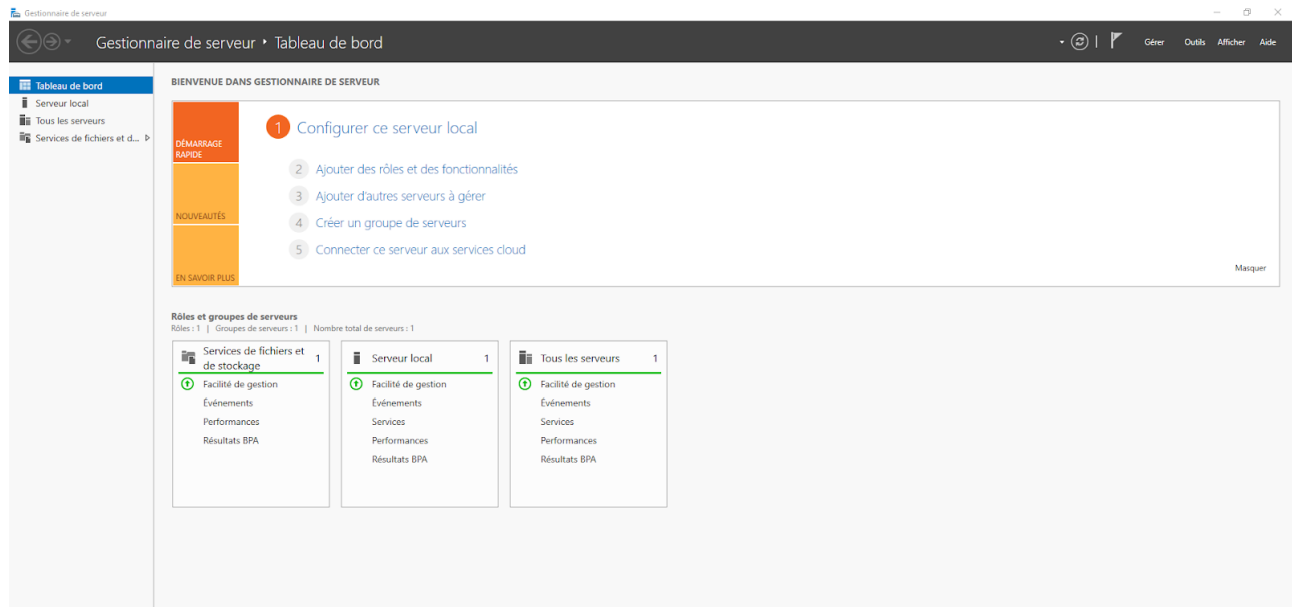
Tout un programme.

Gérez les rôles, fonctionnalités et services

Microsoft a travaillé l'interface graphique de son serveur (sauf pour sa version Core), afin de donner rapidement accès à la gestion des rôles et fonctionnalités, ainsi qu'aux différents services.

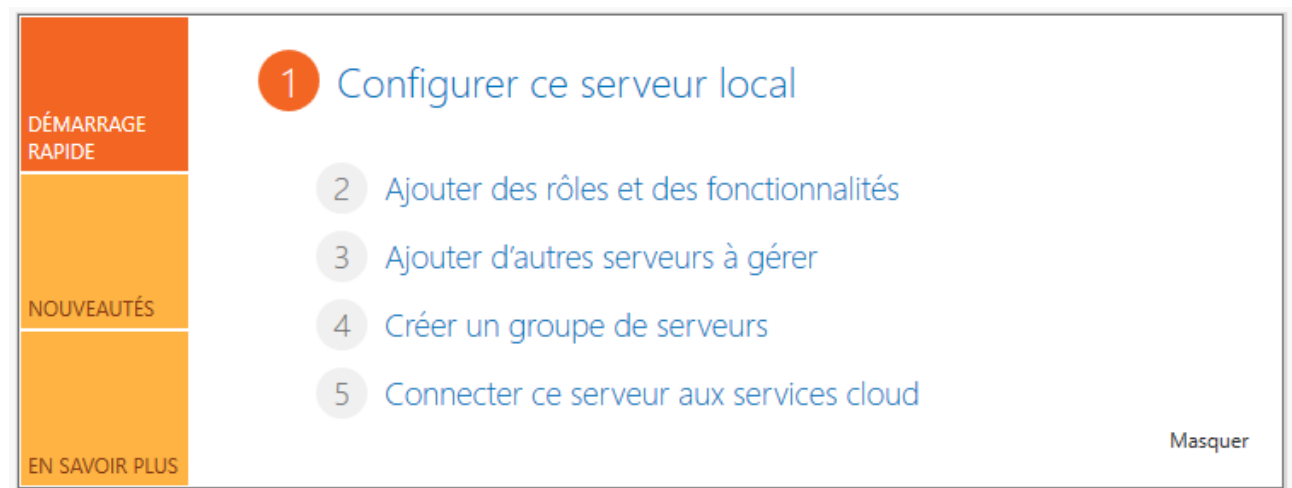
Pour cela, rien de spécifique à mettre en œuvre, laissez votre serveur démarrer, si vous n'avez rien modifié ou configuré de particulier, au démarrage, le gestionnaire de serveur devrait se lancer ! Si tout va bien, c'est à cette étape que vous avez terminé le premier chapitre de ce cours.

Si vous avez éteint votre serveur, vous n'avez qu'à le redémarrer et vous authentifier, le gestionnaire de serveur apparaîtra tout seul à l'ouverture de la session :



Gestionnaire de serveur

Cet outil permet d'avoir un tableau de bord permettant d'avoir rapidement l'état de santé général de votre service. Avant de voir en détail ce tableau de bord, remarquez la zone de démarrage rapide de l'outil :



Zone de démarrage rapide

Avec cette zone vous pouvez directement :

- **Ajouter des rôles et des fonctionnalités** (comme c'est écrit) ;
- **Ajouter d'autres serveurs à gérer** (comme des serveurs Core sans interface graphique) ;
- **Regrouper vos serveurs en groupe** permettant de simplifier l'administration ;

- Et, depuis la version 2016, **gérer des services Cloud** directement depuis cet espace !

Sous cette zone de démarrage rapide se trouve le tableau de bord. Ici, et c'est généralement le cas systématiquement à l'installation "par défaut" d'un serveur Windows, vous avez le rôle "**Services de fichiers et de stockage**" installé, et l'état de santé de votre serveur local affiche des alertes :

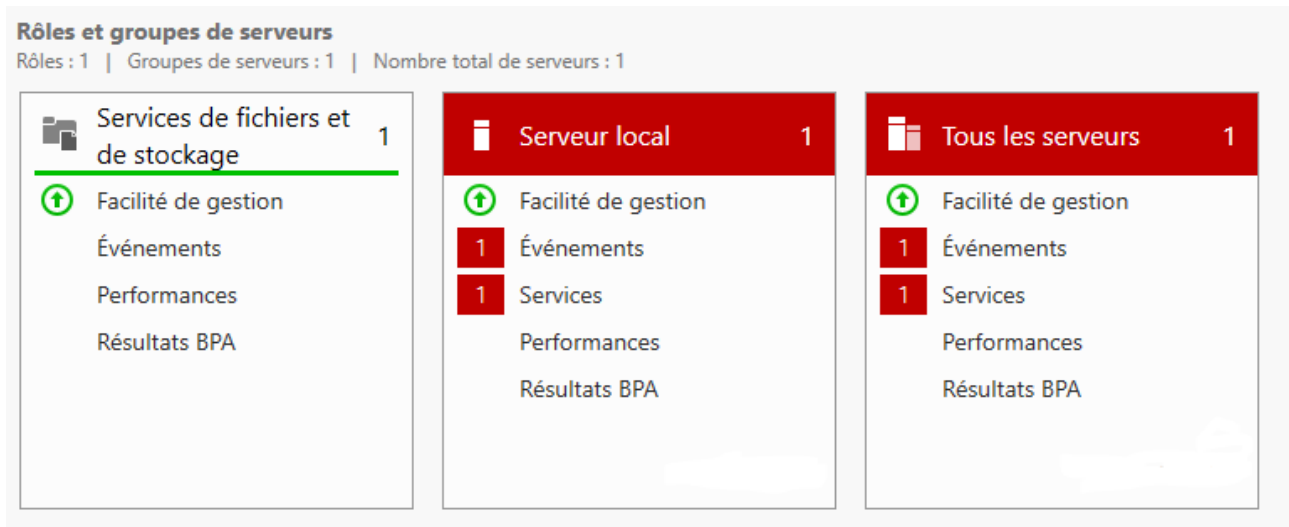
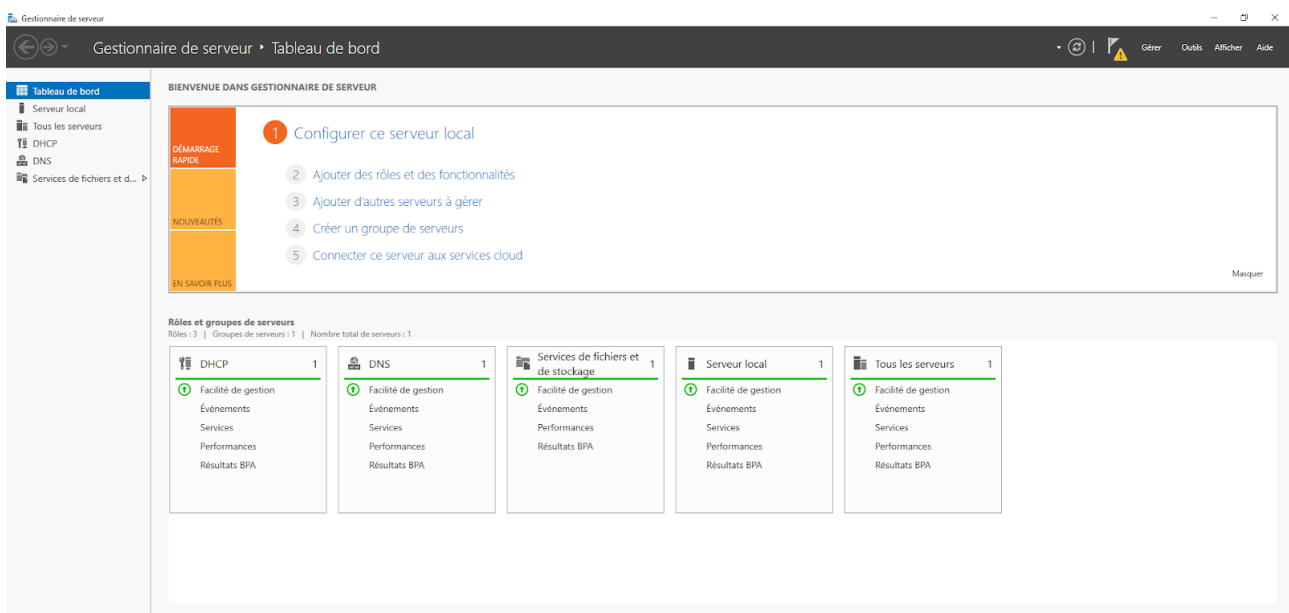


Tableau de bord d'un serveur juste installé

Certains éléments apparaissent en rouge mais pas de panique ça ne veut pas dire que votre serveur n'est pas fonctionnel ! Il s'agit souvent d'informations indiquant l'état de certains services liés à la configuration par défaut de Windows Server.

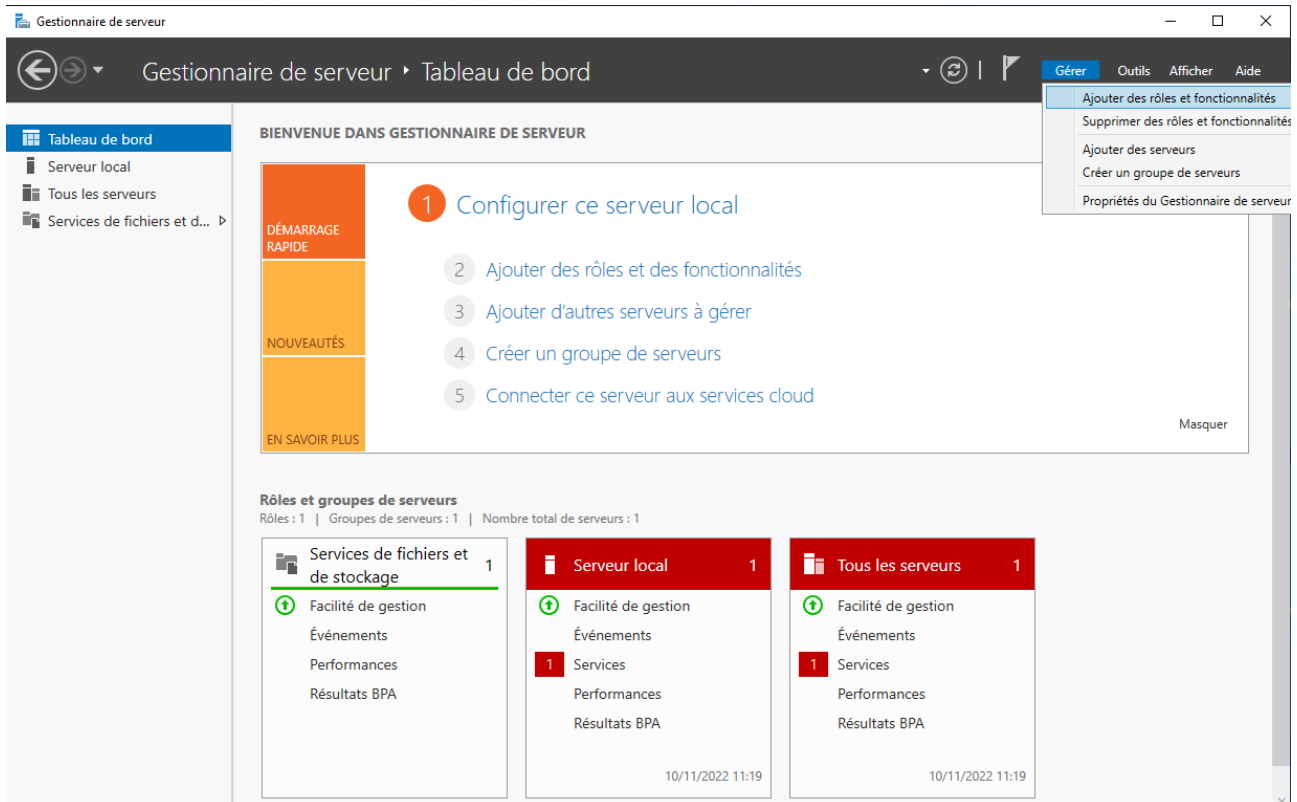
Au départ un serveur Windows n'a qu'un seul rôle, et le groupe de serveur ne contient qu'un seul serveur (lui-même)

Si vous ajoutez un ou plusieurs rôles, ils seront présents dans le volet à gauche comme c'est le cas ici :



Les rôles DHCP et DNS ont été ajoutés au serveur

Comment ajouter un rôle ? Rien de plus simple : soit en utilisant le démarrage rapide et donc en cliquant sur le 2e item “**Ajouter des rôles et des fonctionnalités**”, soit en cliquant sur “**Gérer**” (en haut à droite), puis sur “**Ajouter des rôles et fonctionnalités**” :



Ajouter un rôle

Ensuite, sélectionnez le rôle qui vous intéresse parmi la liste des rôles proposés. Avant de vous afficher la liste, le **Gestionnaire de serveur** va vous donner de l'information et vous poser quelques questions, à savoir :

- Quelques informations sur le fonctionnement de l'assistant ;
- Le mode/type d'installation (basée sur un rôle, ou bureau à distance) ;
- Le serveur ou groupe de serveurs de destination.

Bien entendu, pour le moment pas d'histoire de bureau à distance ou d'architecture de bureaux virtuels (VDI), mais simplement une installation basée sur des rôles sur votre serveur local ! Vous devriez arriver ici :

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION
SRVDHCPPAR01

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

- ☐ Accès à distance
- ☐ Attestation d'intégrité de l'appareil
- ☐ Hyper-V
- ☐ Serveur de télécopie
- ☐ Serveur DHCP
- ☐ Serveur DNS
- ☐ Serveur Web (IIS)
- ☐ Service Guardian hôte
- ☐ Services AD DS
- ☐ Services AD LDS (Active Directory Lightweight Directory Services)
- ☐ Services AD RMS (Active Directory Rights Management Services)
- ☐ Services Bureau à distance
- ☐ Services d'activation en volume
- ☐ Services d'impression et de numérisation de documents
- ☐ Services de certificats Active Directory
- ☐ Services de déploiement Windows
- ☐ Services de fédération Active Directory (AD FS)
- ☒ Services de fichiers et de stockage (1 sur 12 installés)
- ☐ Services de stratégie et d'accès réseau

Description

L'accès à distance fournit une connectivité transparente via DirectAccess, les réseaux VPN et le proxy d'application Web. DirectAccess fournit une expérience de connectivité permanente et gérée en continu. Le service d'accès à distance (RAS) fournit des services VPN classiques, notamment une connectivité de site à site (filiale ou nuage). Le proxy d'application Web permet la publication de certaines applications HTTP et HTTPS spécifiques de votre réseau d'entreprise à destination d'appareils clients situés hors du réseau d'entreprise. Le routage fournit des fonctionnalités de routage classiques, notamment la traduction d'adresses réseau.

< Précédent

Suivant >

Installer

Annuler

Sélection d'un rôle

Si vous avez déjà un rôle installé, il sera déjà coché. L'avantage de cet assistant est que vous disposez d'une description sur la droite de l'écran et ce, pour chaque rôle !

Si vous sélectionnez un rôle, par exemple Serveur DNS, vous pouvez avoir une liste de fonctionnalités à choisir obligatoirement, comme c'est le cas avec le rôle "**Serveur DNS**" :

Ajouter les fonctionnalités requises pour Serveur DNS ?

Les outils suivants sont requis pour la gestion de cette fonctionnalité, mais ils ne doivent pas obligatoirement être installés sur le même serveur.

- ▲ Outils d'administration de serveur distant
 - ▲ Outils d'administration de rôles
 - [Outils] Outils du serveur DNS

☒ Inclure les outils de gestion (si applicable)

Ajouter des fonctionnalités

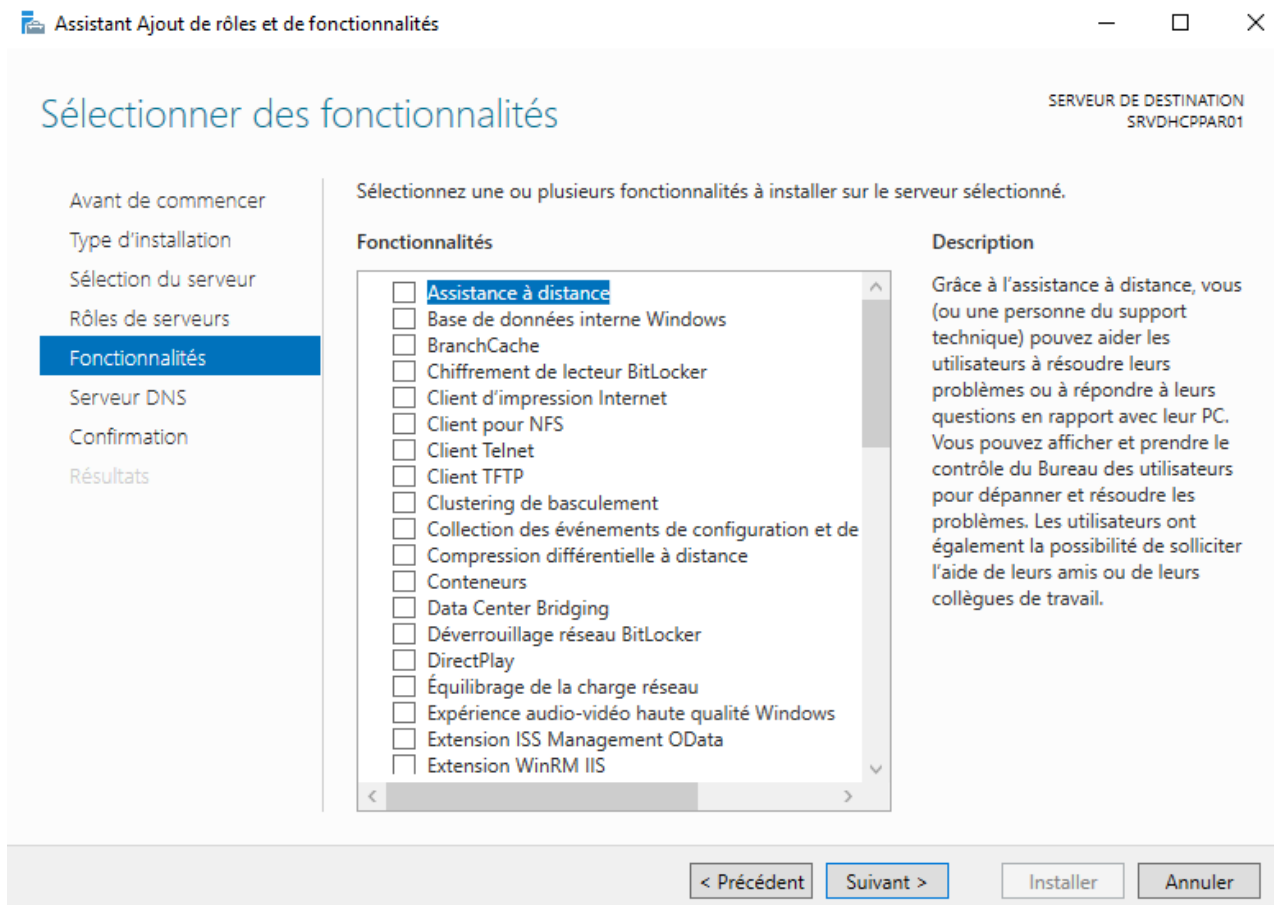
Annuler

Fonctionnalités obligatoires pour le rôle Serveur DNS

Cliquez sur “**Ajouter des fonctionnalités**” et vous reviendrez à l’écran de sélection des rôles.

Maintenant que vous avez choisi votre rôle, ici "DNS" (oui, je me répète), cliquez sur “**Suivant**”.

Vous vous retrouvez alors à nouveau sur l’écran de choix des fonctionnalités :



Liste des fonctionnalités d'un serveur Windows

Cette fois, ce ne sont pas uniquement les fonctionnalités obligatoires pour la bonne marche du rôle choisi précédemment, mais réellement toutes les fonctionnalités qu'il est possible d'ajouter à un serveur !

Par exemple, si, alors que vous installez le rôle DNS, vous vous rendez compte qu'avoir un client Telnet peut être intéressant, vous pouvez à ce moment cocher la case de cette fonctionnalité "Client Telnet". Rappelez-vous : **un rôle = une ou plusieurs fonctionnalités = un ou plusieurs services !**

Cliquez ensuite sur "**Suivant**", l'assistant vous offre à nouveau des informations sur le rôle sélectionné :

Serveur DNS

SERVEUR DE DESTINATION
SRVDHCPPAR01

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Serveur DNS

Confirmation

Résultats

Le système DNS (Domain Name System) fournit une méthode standard d'association de noms à des adresses Internet numériques. Cela permet aux utilisateurs de référencer les ordinateurs du réseau en utilisant des noms faciles à retenir au lieu de longues séries de chiffres. En outre, le système DNS intègre un espace de noms hiérarchique, ce qui permet que chaque nom d'hôte soit unique sur un réseau local ou étendu. Les services DNS Windows peuvent être intégrés aux services DHCP (Dynamic Host Configuration Protocol) sur Windows. Il n'est ainsi plus nécessaire d'ajouter des enregistrements DNS lorsque des ordinateurs sont ajoutés au réseau.

Éléments à noter :

- L'intégration du serveur DNS aux services de domaine Active Directory réplique les données DNS et d'autres données du service d'annuaire, ce qui facilite la gestion DNS.
- Les services de domaine Active Directory nécessitent l'installation d'un serveur DNS sur le réseau. Si vous installez un contrôleur de domaine, vous pouvez aussi installer le rôle serveur DNS avec l'Assistant Installation des services de domaine Active Directory, en sélectionnant le rôle Services de domaine Active Directory.

< Précédent

Suivant >

Installer

Annuler

Information sur le rôle DNS

Dès que vous avez lu et appris par cœur ces informations, cliquez à nouveau sur “**Suivant**” pour avoir un récapitulatif complet de ce que vous allez installer :

Confirmer les sélections d'installation

SERVEUR DE DESTINATION
SRVDHCPAR01

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Serveur DNS

Confirmation

Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

☐ Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Client Telnet

Outils d'administration de serveur distant

Outils d'administration de rôles

Outils du serveur DNS

Serveur DNS

[Exporter les paramètres de configuration](#)[Spécifier un autre chemin d'accès source](#)

< Précédent

Suivant >

Installer

Annuler

Liste des rôles et fonctionnalités qui seront installés

Il ne reste qu'à cliquer sur "**Installer**" pour lancer l'installation !

Voilà, vous devriez, avec ces éléments, maîtriser l'installation des rôles, fonctionnalités et services d'un serveur Windows !

Pour vous entraîner, n'hésitez pas à **installer également le rôle DHCP** à votre serveur.

Rendez-vous dans le prochain chapitre pour identifier comment surveiller votre serveur avant de vous lancer dans la configuration d'un rôle défini !

En résumé

- Les rôles sont les **fonctions premières** d'un serveur au sein d'un réseau.
- Les rôles peuvent avoir plus ou moins de **fonctionnalités** en fonction de leur complexité.
- La gestion des rôles et fonctionnalités se fait au travers de l'outil **Gestionnaire de serveur** qui se lance automatiquement au démarrage d'une session.
- Les **rôles** ont des **fonctionnalités obligatoires**.
- L'assistant d'ajout de rôle permet d'**ajouter des rôles, leurs fonctionnalités obligatoires éventuelles** mais aussi **toutes les fonctionnalités disponibles** sur Windows Server !

Rendez-vous dans le prochain chapitre pour identifier comment surveiller votre serveur avant de vous lancer dans la configuration d'un rôle bien défini !

Mettez en place la surveillance de votre serveur



Dans ce dernier chapitre de la partie 1, je vous propose de travailler sur un sujet souvent oublié ou effectué à la “va-vite” : la **surveillance**. Une bonne surveillance permet d’éviter de nombreux problèmes de disponibilité, d’inventaire, et de sécurité d’une façon plus générale !

Appréhendez la surveillance automatique de Windows Server

Microsoft a été jusqu’au bout du principe d’interface graphique, avec le gestionnaire de serveur, notamment. Vous n’avez pas à chercher plus loin pour avoir une surveillance de votre serveur ! Et voilà, le cours est terminé, merci... Non, allons jusqu’au bout du sujet.

Je vous propose d’analyser le contenu de cette surveillance automatisée, rendez-vous sur votre **tableau de bord** que vous maîtrisez bien, maintenant :

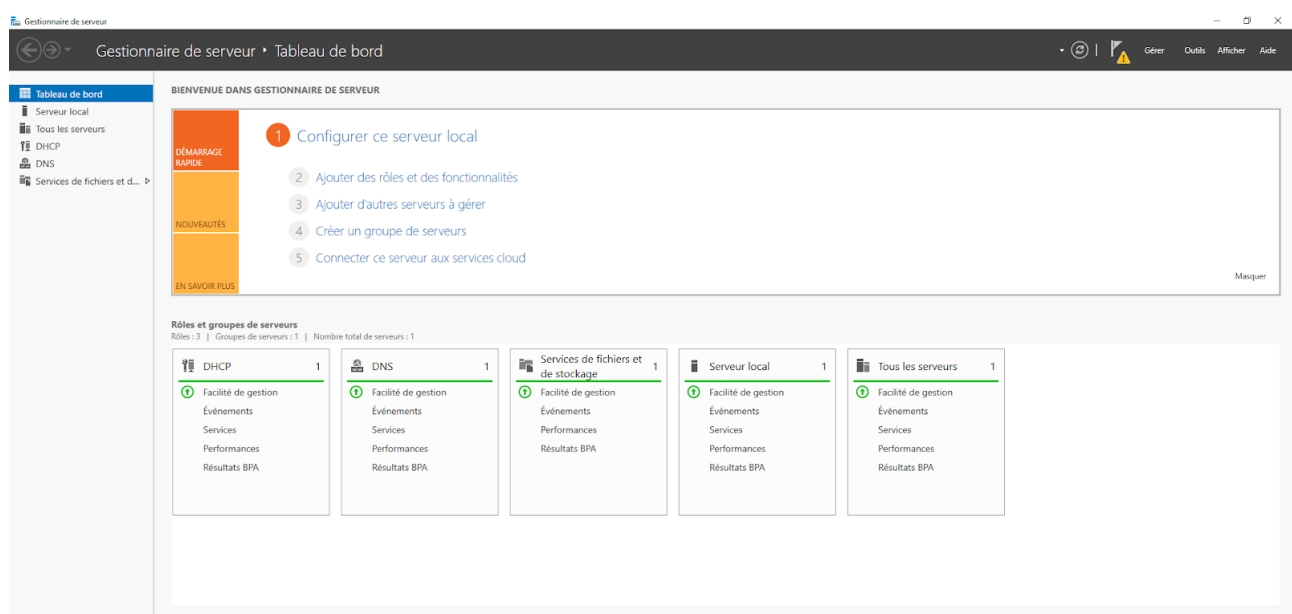
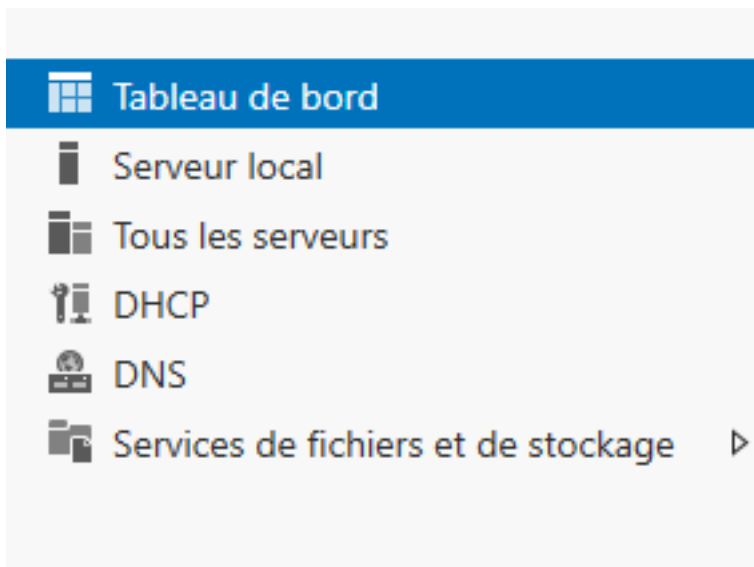


Tableau de bord d'un serveur Windows

Rappelez-vous, sur la gauche le menu d'accès rapide ; au milieu, le tableau de bord à proprement parler, avec une zone démarrage rapide et les éléments de surveillance, puis en haut à droite, le menu avec les notifications (matérialisées par un drapeau).

Tout d'abord, le **menu à gauche**. Il permet d'aller rapidement à un **serveur**, un **rôle** ou vos **groupes** de serveurs :



Menu du tableau de bord

Je vous propose de rester sur la partie **Serveur local** !

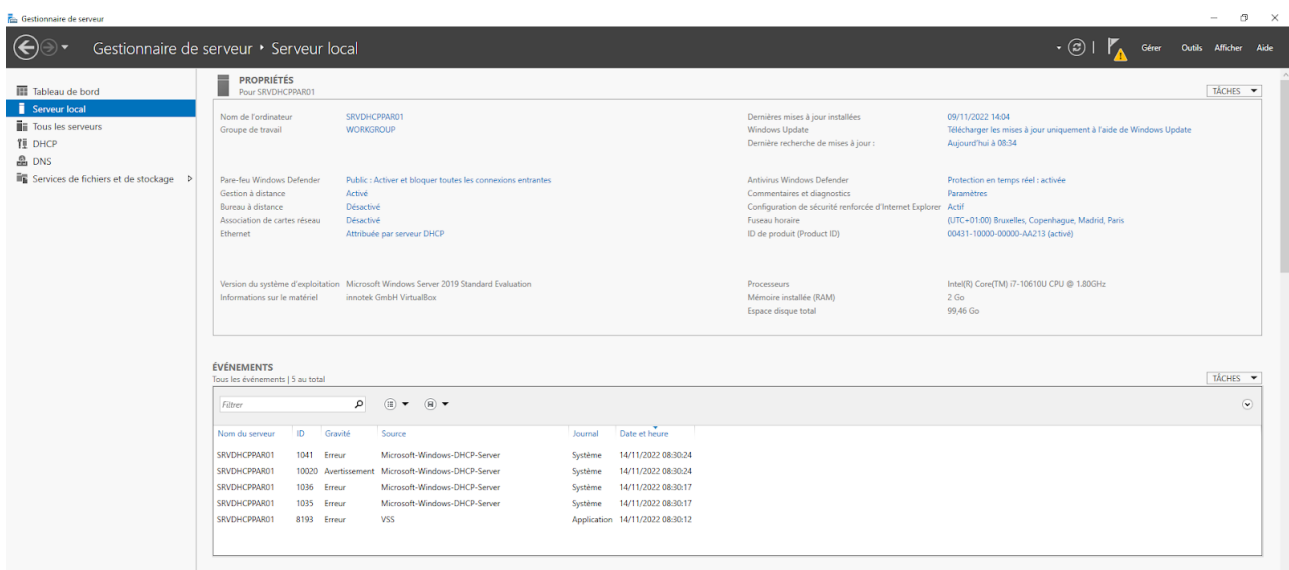


Tableau de bord du serveur local

Je ne reviens pas sur la première zone qui vous permet de retrouver les configurations de base de votre serveur (réseau, nom, état des mises à jour...). En-dessous, vous retrouvez les événements des différents journaux d'événements de votre serveur.

Microsoft a mis en place un système similaire à “journalctl” sous Linux. Tous les événements seront enregistrés dans ces différents journaux, et le tableau de bord vous les affichera tous ici. L’affichage est donc centralisé, et il est possible de n’afficher que des événements critiques (quel que soit le journal en question – pour rappel, il existe les journaux application, installation, système et sécurité, par défaut sous Windows).

Surveillez les événements de votre serveur

Par défaut, les événements **Critique**, **Erreur** et **Avertissement** sont affichés à partir des journaux :

ÉVÉNEMENTS

Tous les événements | 56 au total

Nom du serveur	ID	Gravité	Source	Journal
SRVDHCPPAR01	10020	Avertissement	Microsoft-Windows-DHCP-Server	Système
SRVDHCPPAR01	1036	Erreur	Microsoft-Windows-DHCP-Server	Système
SRVDHCPPAR01	1035	Erreur	Microsoft-Windows-DHCP-Server	Système
SRVDHCPPAR01	134	Avertissement	Microsoft-Windows-Time-Service	Système
SRVDHCPPAR01	134	Avertissement	Microsoft-Windows-Time-Service	Système
SRVDHCPPAR01	10016	Erreur	Microsoft-Windows-DistributedCOM	Système
SRVDHCPPAR01	10149	Avertissement	Microsoft-Windows-Remote Management	Système

SERVICES

Ces paramètres déterminent la façon dont le Gestionnaire de serveur collecte les données d'événements de serveurs dans le groupe de serveurs actuellement géré. Des modifications apportées aux valeurs par défaut et qui génèrent un nombre d'événements nettement supérieur dans la vignette des événements peuvent entraîner des réponses lentes du Gestionnaire de serveur.

Afficher les événements correspondant à ces niveaux de gravité

☒ Critique
 ☒ Erreur
 ☒ Avertissement
 ☐ Informatif

Obtenir les événements qui se sont produits dans le passé

24 heures

Obtenir les événements à partir des fichiers journaux d'événements suivants

Multiple

Affichage centralisé des événements des journaux par défaut
Sous cette partie Événements se trouve la partie Services :

SERVICES

Tous les services | 190 au total

Nom du serveur	Nom complet	Nom du service	Statut	Type de démarrage
SRVDHCPPAR01	Service d'infrastructure des tâches en arrière-plan	BrokerInfrastructure	En cours d'exécution	Automatique
SRVDHCPPAR01	Service Update Orchestrator pour Windows Update	UsoSvc	Arrêté	Manuel
SRVDHCPPAR01	Client DNS	Dnscache	En cours d'exécution	Automatique (déclenché)
SRVDHCPPAR01	Service de découverte automatique de Proxy Web pour les services HTTP Windows	WinHttpAutoProxySvc	En cours d'exécution	Manuel
SRVDHCPPAR01	Service de gestion radio	RmSvc	Arrêté	Manuel
SRVDHCPPAR01	Service Pulsation Microsoft Hyper-V	vmicheartbeat	Arrêté	Manuel (déclenché)
SRVDHCPPAR01	Service Broker de découverte en arrière-plan DevQuery	DevQueryBroker	Arrêté	Manuel (déclenché)

Tableau de bord de l'état des services du serveur local

Vous allez retrouver l'état de tous les services de votre serveur ! L'avantage, c'est que vous pourrez **relancer**, **arrêter** ou **démarrer** un service directement de cette zone en faisant un clic droit sur le nom du service.

Vérifiez votre conformité aux bonnes pratiques Microsoft

Ensuite se trouve le **Best Practice Analyzer** :

BEST PRACTICE ANALYZER

Avertissements ou erreurs | 0 sur 0 au total

Filtre appliqué. ✕ Effacer tout

Nom du serveur	Gravité	Titre	Catégorie
Correspondances introuvables.			

Best Practice Analyzer

Cet outil est très intéressant en termes de surveillance d'un serveur. Par exemple, j'ai installé le rôle DHCP sur mon serveur ; est-ce que ma configuration est validée par les guides et bonnes pratiques de Microsoft ? Je n'ai qu'à lancer le **"Best Practice Analyzer"** (BPA) pour le savoir via **"Tâches"**, **"Commencer l'analyse BPA"**, et voilà le résultat :

BEST PRACTICE ANALYZER
Avertissements ou erreurs | 3 sur 15 au total

TÂCHES ▼

Filtrer

Filtre appliqué. ✕ Effacer tout

Nom du serveur	Gravité	Titre	Catégorie
SRVDHCPPAR01	Avertissement	DHCP : les groupes de sécurité (Administrateurs DHCP et Utilisateurs DHCP) requis pour l'administration DHCP doivent être créés.	Sécurité
SRVDHCPPAR01	Erreur	DHCP : le serveur doit avoir au moins une étendue IPv4.	Configuration
SRVDHCPPAR01	Avertissement	DHCP : le serveur doit disposer d'autorisations Contrôle total pour les paramètres de Registre DHCP.	Prédéploiement

Résultat du BPA avec le rôle DHCP installé sur un serveur tout frais

En un clin d’œil (ou clic de souris), je sais que mon rôle DHCP n’est pas correctement configuré et qu’il **ne peut pas** fonctionner ! Charge à moi (et donc à vous) d’effectuer les modifications proposées.

Notez que bien souvent, si vous ne validez pas le BPA, le support de Microsoft ne pourra intervenir sur votre serveur. En effet, si vous ne suivez pas les guides et bonnes pratiques de Microsoft, ils ne peuvent pas vous aider dans la résolution d’un problème qui, pour eux, n’en est pas un.

Surveillez les performances de votre serveur

Sous le BPA se trouve la partie Performance :



Espace Performance du tableau de bord

Rarement utilisé, c’est pourtant un outil puissant pour diagnostiquer un problème de ressources sur son serveur. Pour l’activer, il suffit de cliquer sur “**Tâches**” puis sur “**Configurer des alertes de performance**” :

Définir les seuils d'alerte de performance

Une fois que vous avez modifié les seuils et cliqué sur Enregistrer, les données mises à jour s'affichent pour ce groupe ou rôle.

Utilisation du processeur (%)

Mémoire (Mo disponibles)

Définir la période d'affichage du graphique de performances

La zone de graphique de performances affiche les données de performance pendant le nombre de jours spécifié dans le paramètre Période d'affichage du graphique. Plus les valeurs sont basses, plus le graphique est bref.

Période d'affichage du graphique (en jo...

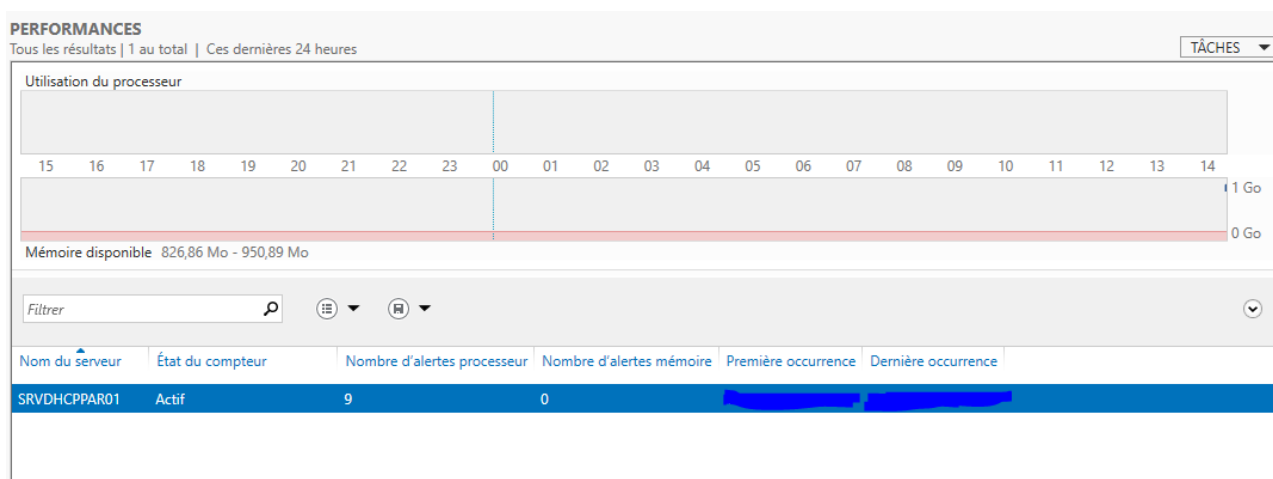
Enregistrer

Annuler

Seuils d'alerte de performance

Dans cet exemple, au-delà de 85 % d'occupation du processeur et à moins de 100 Mio de RAM disponible, vous aurez une alerte dans cette zone. Cela vous permettra d'investiguer plus en profondeur pour résoudre le souci.

Pour activer l'analyse en tant que telle, clic droit sur le nom du serveur puis **“Démarrer les compteurs de performances”** ! Il n'y a plus qu'à attendre des données et une potentielle alerte de performance :



Alerte de performance

Ainsi, vous savez comment identifier des problèmes de performance sur votre serveur. À vous d'investiguer pour en trouver la source et résoudre le problème !

Gardez le contrôle sur les rôles et fonctionnalités

Enfin, vous avez le récapitulatif des rôles et fonctionnalités installés sur votre serveur :

Nom du serveur	Nom	Type	Chemin d'accès
SRVDHCPPAR01	Serveur DHCP	Rôle	Serveur DHCP
SRVDHCPPAR01	Services de fichiers et de stockage	Rôle	Services de fichiers et de stockage
SRVDHCPPAR01	Partage de port TCP	Fonctionnalité	Fonctionnalités de .NET Framework 4.6\Services WCF\Partage de port TCP
SRVDHCPPAR01	Services WCF	Fonctionnalité	Fonctionnalités de .NET Framework 4.6\Services WCF
SRVDHCPPAR01	.NET Framework 4.6	Fonctionnalité	Fonctionnalités de .NET Framework 4.6\.NET Framework 4.6
SRVDHCPPAR01	Fonctionnalités de .NET Framework 4.6	Fonctionnalité	Fonctionnalités de .NET Framework 4.6
SRVDHCPPAR01	Windows PowerShell 5.1	Fonctionnalité	Windows PowerShell\Windows PowerShell 5.1

Surveillance des rôles et fonctionnalités de votre serveur

Ici, vous avez tout simplement un moyen simple et rapide d'identifier les rôles et fonctionnalités installés sur votre serveur ! Voilà, vous savez comment surveiller votre serveur grâce aux outils Microsoft !

En résumé

- Windows Server intègre de **nombreux outils de surveillance par défaut**.
- Vous avez la possibilité d'avoir un **tableau de bord** pour votre serveur local, mais également pour un groupe de serveurs.
- Le BPA (Best Practices Analyzer) vous permet de vérifier votre **conformité aux bonnes pratiques** de configuration Microsoft.

C'est la fin de cette première partie qui vous a permis de voir comment fonctionne le système Windows Server. Vous allez donc utiliser tout ceci afin d'installer et configurer différents services réseaux dans la prochaine partie.

En attendant, je vous propose de tester vos connaissances dans le quiz clôturant cette première partie.

Installez un serveur DHCP



Dans cette seconde partie, je vous propose de prendre en main différents rôles proposés par Microsoft, et de les installer sur votre serveur ! Vous allez commencer par le rôle Serveur DHCP qui permet, vous le savez déjà sûrement, d'automatiser la configuration de vos équipements au sein de votre réseau !

Rappelez-vous les fondamentaux de DHCP

Un petit rappel sur le fonctionnement de DHCP. **Dynamic Host Configuration Protocol** est, comme son nom l'indique, un protocole de configuration dynamique (automatique) des machines ! Ainsi vous supprimerez le risque de mauvaise manipulation lors de la configuration réseau de vos équipements, et apporterez donc une fiabilité dans votre réseau.

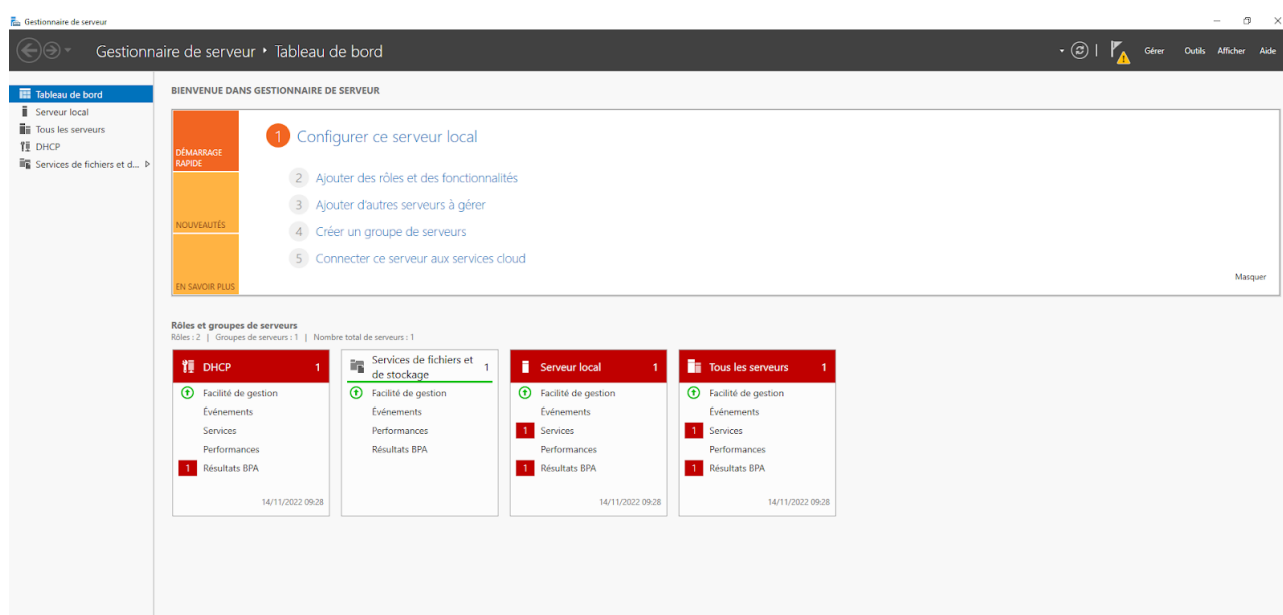
Microsoft implémente ici la **RFC2131** au sein du rôle **DHCP**.

Si l'on résume son fonctionnement, le serveur **DHCP** écoute sur le port **UDP 67**.

Si vous souhaitez en savoir plus, n'hésitez pas à lire [cette partie](#) du cours sur le fonctionnement des réseaux TCP/IP.

Installez le rôle Serveur DHCP

Pour ajouter ce rôle, vous savez quoi faire. Rendez-vous sur le gestionnaire de serveur, et dans la partie "**Ajouter un rôle ou une fonctionnalité**", cochez la case "**Serveur DHCP**" :



Rôle DHCP installé

Vous remarquerez que le tableau de bord vous alerte avec beaucoup de rouge et une notification. C'est normal, vous n'avez pas terminé la configuration de ce rôle.

Je vous propose de cliquer sur la notification puis sur "**Terminer la configuration**" ; vous devriez arriver sur cet écran :

Description

Description

Résumé

Les étapes suivantes seront effectuées pour configurer le serveur DHCP sur l'ordinateur cible :

Créez les groupes de sécurité suivants pour la délégation de l'administration du serveur DHCP.

- Administrateurs DHCP
- Utilisateurs DHCP

< Précédent

Suivant >

Valider

Annuler

Assistant de configuration du rôle Serveur DHCP

L'assistant vous indique les différentes étapes qui seront à mettre en œuvre pour configurer ce rôle. La première étape est **la création de groupes** pour la délégation d'administration. Cela vous permettra de créer un utilisateur qui n'aura d'autres droits que ceux d'administration de ce rôle !

Vous pouvez ensuite fermer cet assistant. Je vous propose maintenant d'utiliser la console de gestion du serveur DHCP qui va vous permettre d'administrer et surtout de configurer votre DHCP. Pour cela, rendez-vous sur la partie DHCP et avec un clic droit, sélectionnez le **Gestionnaire DHCP** :

← → ▾ Gestionnaire de serveur ▸ DHCP

- Tableau de bord
- Serveur local
- Tous les serveurs
- DHCP**
- Services de fichiers et d... ▸

SERVEURS
Tous les serveurs | 1 au total

🔍

Nom du serveur

Adresse IPv4

Facilité de gestion

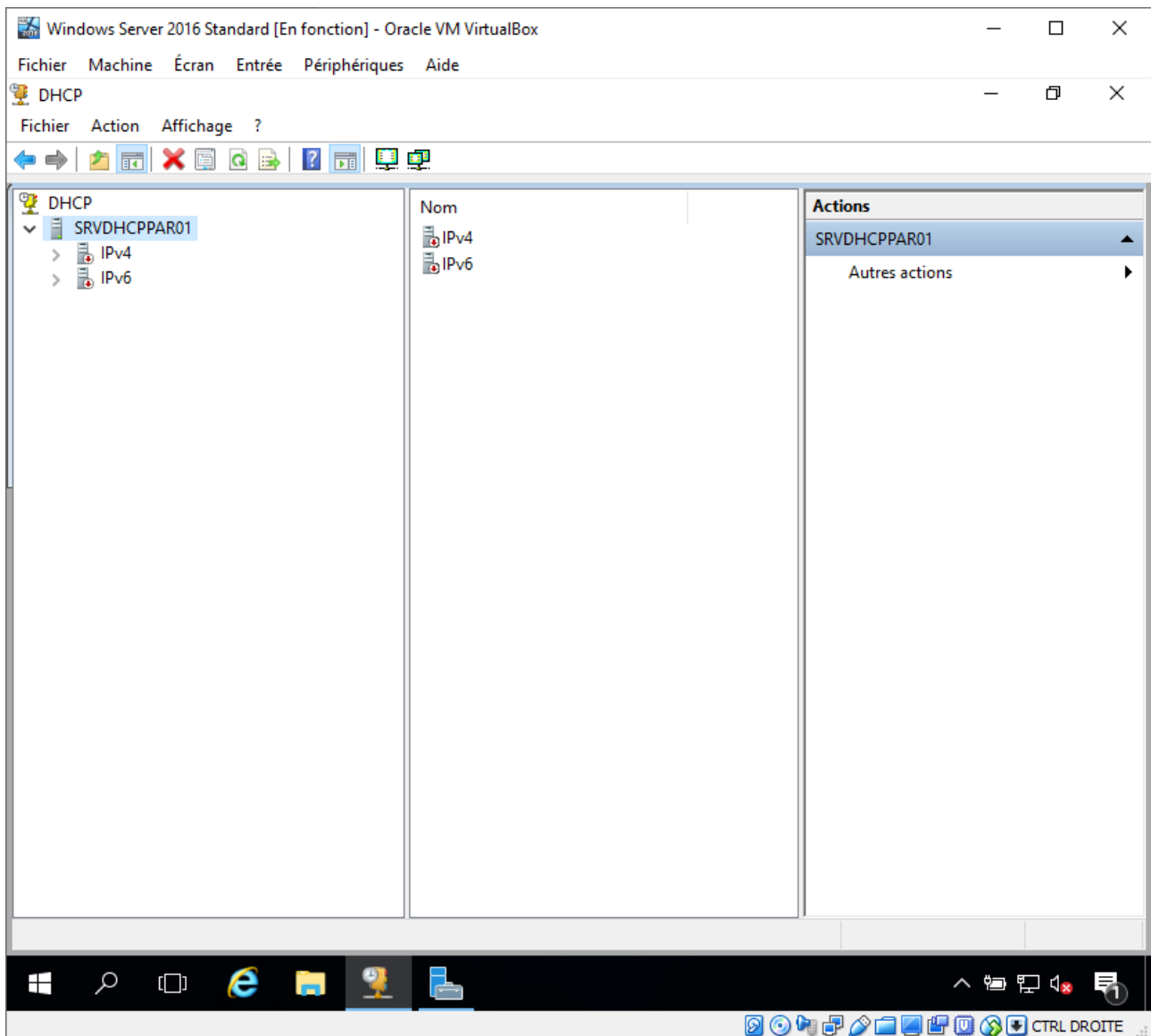
SRVDHCPPAR01	10.0.2.15	En ligne - Gestionnaire de performances non démarré
--------------	-----------	---

ÉVÉNEMENTS
Tous les événements | 16 au total

- Ajouter des rôles et fonctionnalités
- Arrêter le serveur local
- Gestion de l'ordinateur
- Connexion Bureau à distance
- Windows PowerShell
- Configurer l'association de cartes réseau
- Gestionnaire DHCP
- Gérer en tant que...
- Démarrer les compteurs de performances
- Actualiser
- Copier

Lancement du gestionnaire DHCP

Vous trouverez toutes les options pour configurer ce rôle :

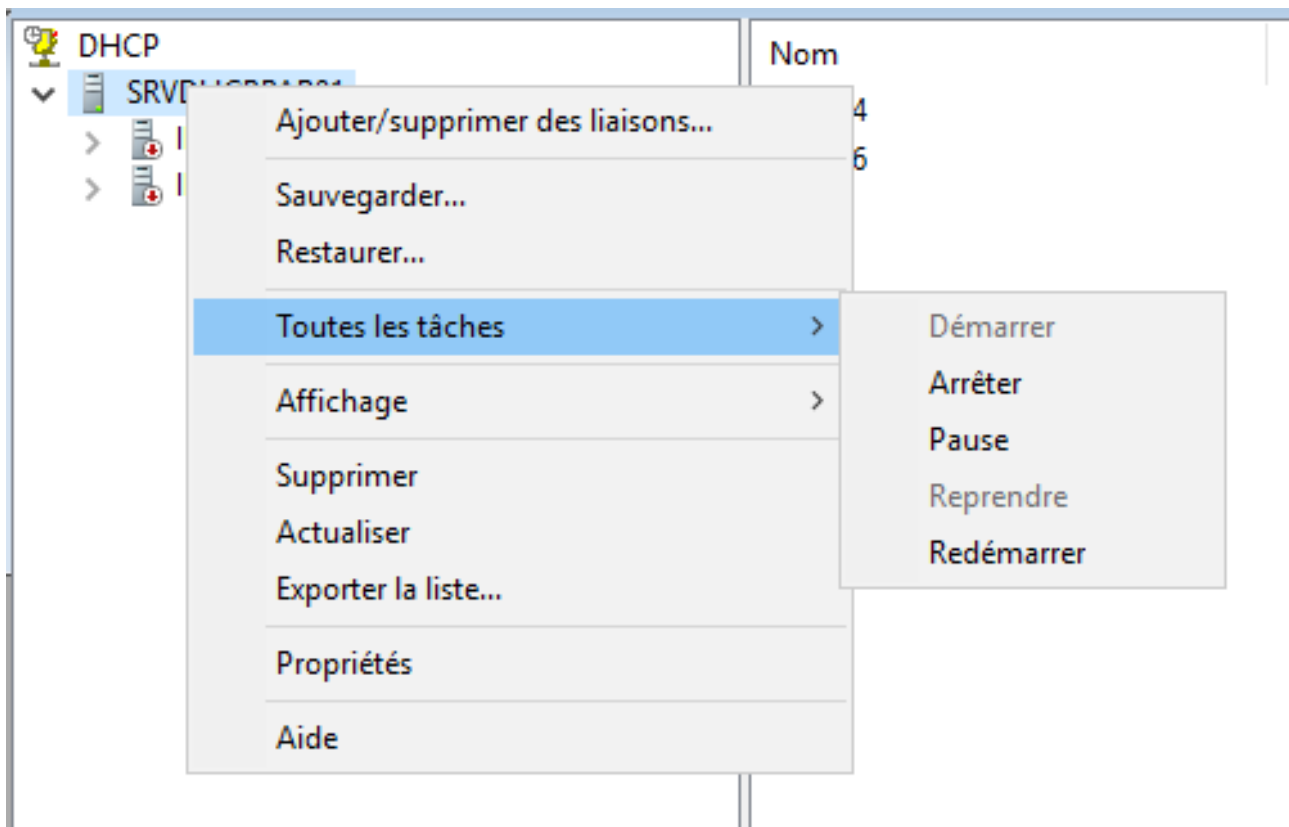


Gestionnaire DHCP

La fenêtre est découpée en trois : **à gauche** vos serveurs DHCP, **au milieu** les options de configuration et **à droite** les actions possibles en fonction du contexte. C'est notamment à cet emplacement que vous retrouverez, dans les actions, des raccourcis vers les menus qui s'afficheront, en faisant un clic droit.

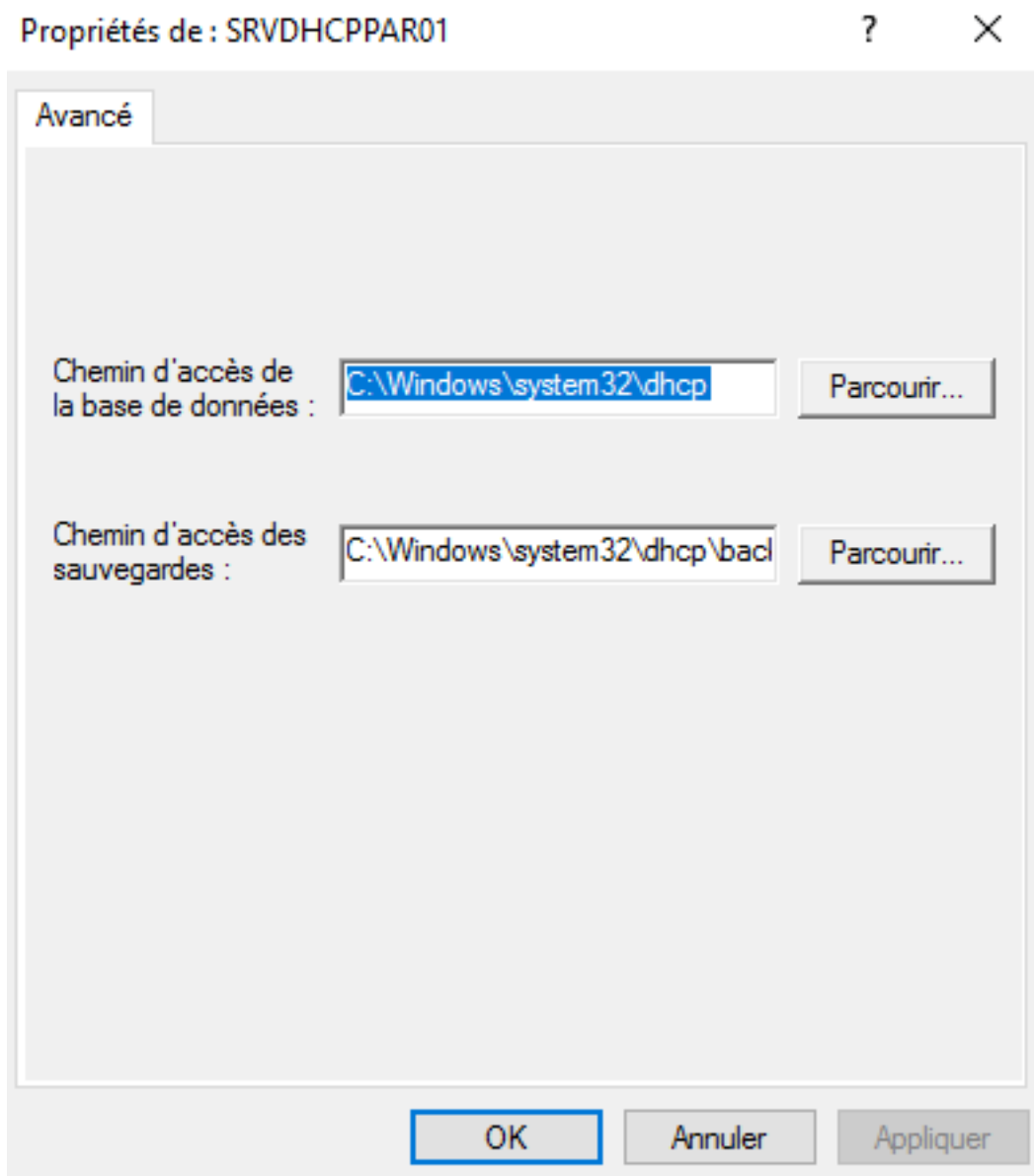
Gérez le service DHCP

Comme je vous l'ai dit, un rôle utilise des fonctionnalités qui se basent sur des services. La première chose que vous pouvez faire avec ce gestionnaire est de **stopper**, **démarrer** ou **redémarrer** le service associé au rôle DHCP. Vous devrez notamment redémarrer le service DHCP pour recharger la configuration. Rien de plus simple, un clic droit sur le nom du serveur hébergeant ce rôle, et dans "**Toutes les tâches**" vous pourrez effectuer toutes ces actions :



Action sur le service DHCP

Autre point, si vous lancez (toujours avec le clic droit sur le serveur) les propriétés, vous aurez connaissance de l'emplacement de la base de données utilisée par le service DHCP :



Emplacement de la base de données DHCP

Contrairement au monde Unix/Linux, Microsoft n'aime pas trop les fichiers plats au format texte. Il s'agit d'une base de données, soyez donc vigilant aux sauvegardes et restaurations en effectuant une copie de ce répertoire, ou en écrasant ce répertoire à l'aide du répertoire "backup" créé automatiquement.

Par défaut, le rôle DHCP peut fonctionner en IPv4 et IPv6. Dans ce cours, je ne traiterai que de l'IPv4, l'IPv6 étant encore à la traîne en termes de déploiement... Mais rassurez-vous, d'ici peu vous aurez sûrement à travailler en IPv6.

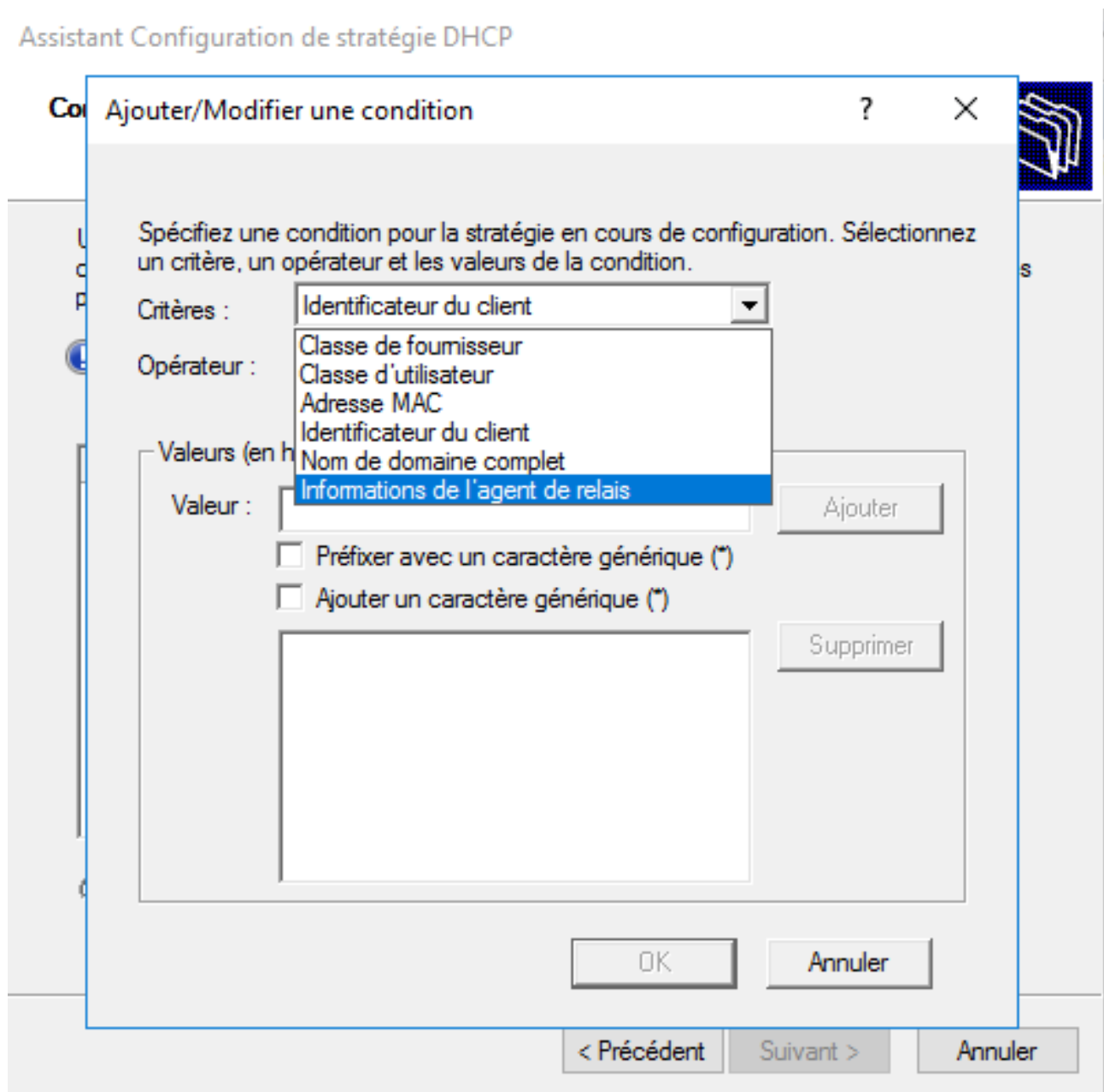
Vous avez donc les paramètres suivants disponibles :

- options de serveur ;
- stratégies ;
- filtres.

En sélectionnant IPv4 et avec un clic droit sur ce paramètre, vous pouvez créer des **étendues** d'adresses à distribuer avec votre serveur.

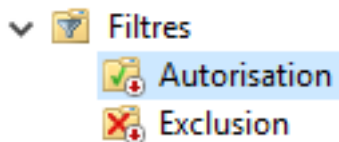
Une **étendue** est une plage d'adresses IP assignées aux ordinateurs demandant une adresse IP dynamique.

Ensuite vous pouvez définir des options propres à chaque étendue, mais également des options globales, ce sont les options de serveur qui s'appliqueront à toutes les étendues ! Les Stratégies vous permettront de définir des conditions de fourniture d'options ou d'adresses en fonction de critères particuliers. Par exemple, vous pourrez spécifier une passerelle par défaut différente à vos équipements Windows 2000... ou, plus plausible, fournir des options spécifiques de configuration aux équipements, avec des adresses MAC présentes dans une liste !



Mise en œuvre d'une stratégie DHCP

Enfin, vous pourrez mettre en place des exclusions ou des autorisations via les filtres :

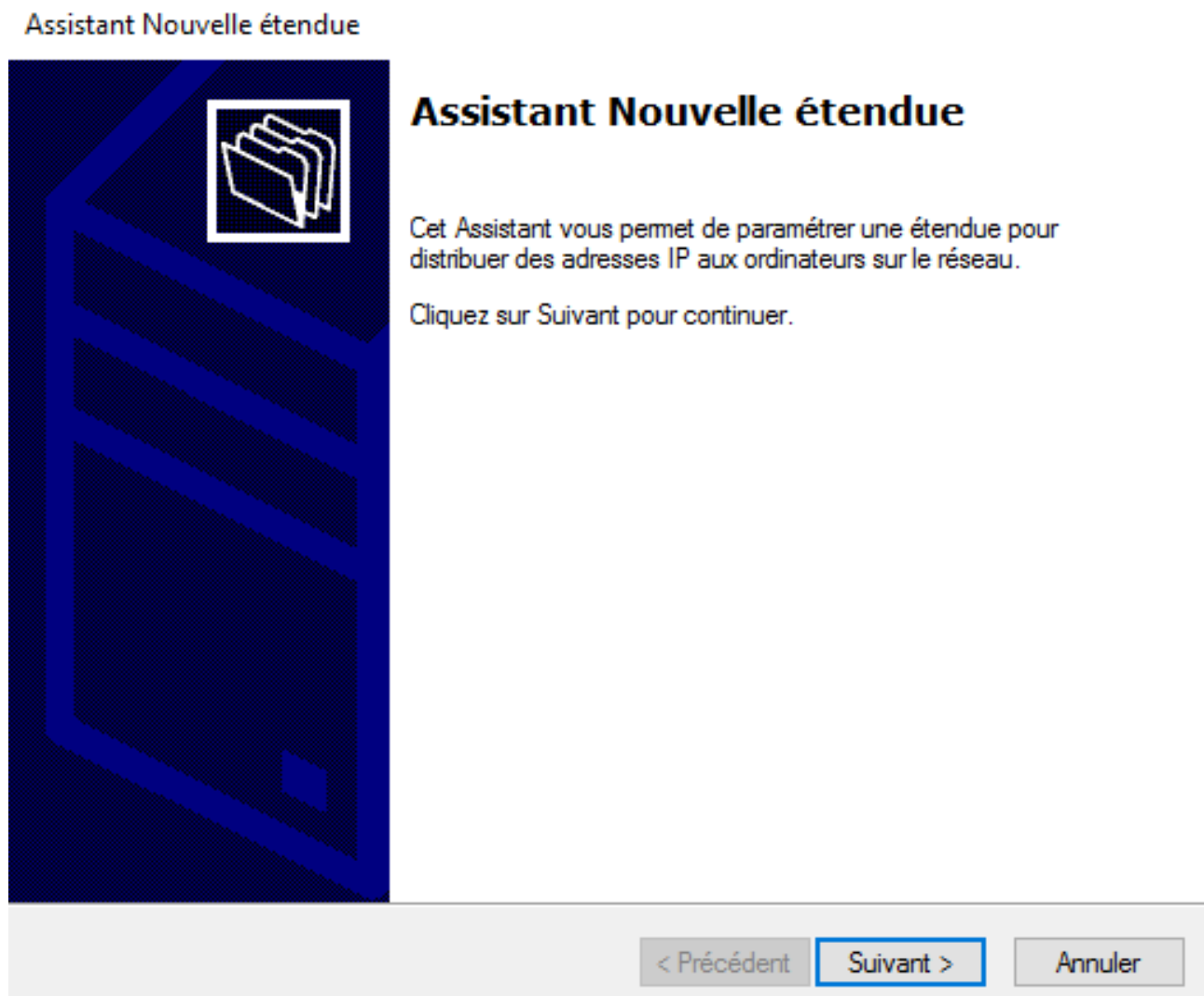


Filtres DHCP

Je vous conseille d'utiliser les deux : enregistrer les adresses MAC de tous vos appareils à cet endroit, et ne fournir une adresse IP que si l'adresse MAC se trouve dans la liste ! Vous pouvez ainsi coupler cela aux stratégies en spécifiant les identificateurs de client qui sont connus. Ainsi vous maîtriserez quels équipements accèdent à votre réseau.

Votre première étendue DHCP

Maintenant que vous connaissez parfaitement le fonctionnement du gestionnaire DHCP, je vous propose de créer votre première étendue. Pour cela, clic droit IPv4 sous le nom du serveur, puis **"Nouvelle étendue"** :



L'assistant Nouvelle étendue

Encore une fois, Microsoft vous permet de configurer cela au travers d'un assistant !

Cliquez sur Suivant et entrez un nom et une description pour votre étendue ! Après le nom et la description arrivent la plage d'adresses que vous allez fournir via le DHCP, ainsi que le masque de

sous-réseaux (je sais que vous maîtrisez ce sujet, vous avez suivi le cours [Apprenez le fonctionnement des réseaux TCP/IP](#)) !

Remplissez les différents champs comme bon vous semble, enfin plutôt selon vos besoins . En général, vous allez configurer **la plage d'adresses** (adresses de début et de fin), **la passerelle** et **le serveur DNS**. Vous pourriez également ajouter des options pour les téléphones IP (le serveur de téléphonie, par exemple).

Attention, pour plus de simplicité, choisissez dans un premier temps une étendue qui soit votre réseau IP. Dans notre cas, le serveur a été configuré avec l'adresse 10.0.2.15/8, on va donc demander au serveur DHCP de distribuer, par exemple, les adresses allant de 10.0.3.1 à 10.0.3.254.

Assistant Nouvelle étendue

Plage d'adresses IP

Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.



Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début : 10 . 0 . 3 . 1

Adresse IP de fin : 10 . 0 . 3 . 254

Paramètres de configuration qui se propagent au client DHCP.

Longueur : 8

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

< Précédent

Suivant >

Annuler

Plage d'adresses

L'écran suivant vous propose d'entrer des exclusions ou de retarder les réponses du serveur, pratique lorsque vous avez plusieurs serveurs DHCP sur un même sous-réseau :

Ajout d'exclusions et de retard

Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCP OFFER.



Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.

Adresse IP de début :

Adresse IP de fin :

Ajouter

Plage d'adresses exclue :

Supprimer

Retard du sous-réseau en
millisecondes :

< Précédent

Suivant >

Annuler

Configuration sans exclusion ni retard

Enfin, l'écran suivant vous propose de **définir** la durée du bail.

Souvent cette durée est laissée par défaut. Il vaut mieux y réfléchir à deux fois, car une attaque informatique connue porte justement sur la saturation des serveurs DHCP via la demande de nombreux baux... Si votre durée de bail est trop longue et que vous êtes victime de ce type d'attaque, vous pourrez paralyser la configuration automatique de votre réseau !

Durée du bail

La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.



La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours :	Heures :	Minutes :
8	0	0

< Précédent

Suivant >

Annuler

Durée du bail

Attention à ne pas tomber dans l'autre extrême : une durée trop courte ! Cela pourrait congestionner votre réseau en demandant à vos équipements de demander de renouveler leurs baux trop souvent.

Une fois la durée du bail configurée, vous avez la possibilité de vous arrêter là ou de poursuivre avec l'assistant pour configurer les options DHCP.

En poursuivant l'assistant, vous êtes guidé dans les options les plus utiles à paramétrer :

- routeur (passerelle par défaut) ;
- nom de domaine et serveurs DNS ;
- serveurs WINS.

Et enfin, vous avez la possibilité d'**activer** l'étendue :

Assistant Nouvelle étendue

Activer l'étendue

Les clients ne peuvent obtenir des baux d'adresses que si une étendue est activée.



Voulez-vous activer cette étendue maintenant ?

- ☒ Qui, je veux activer cette étendue maintenant
- ☐ Non, j'activerai cette étendue ultérieurement

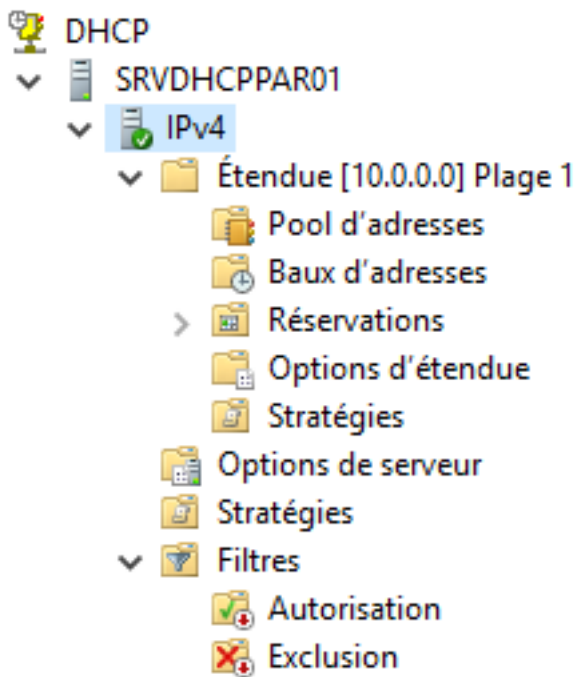
< Précédent

Suivant >

Annuler

Activation de votre étendue

Une fois l'étendue activée, votre rôle DHCP est opérationnel. Après avoir configuré et/ou activé une étendue, plus d'options apparaissent dans le gestionnaire sous IPv4, notamment les options liées aux pools d'adresses, baux d'adresses, réservations et les options d'étendue.



Étendue Plage 1

Cela vous permet de revenir sur des paramètres, de mettre en place des réservations d'adresses IP, d'observer les baux en cours de validité ou de mettre en œuvre une stratégie propre à cette étendue.

Paramétrez votre étendue en profondeur

Avant d'aller plus loin, je vous propose de faire **un clic droit** sur le nom de votre étendue. Vous aurez accès à des options supplémentaires qui peuvent être intéressantes :

Propriétés de : Étendue [10.0.0.0] Plage 1

Général DNS Avancé

Étendue

Nom de l'étendue : Plage 1

Adresse IP de début : 10 . 0 . 3 . 1

Adresse IP de fin : 10 . 0 . 3 . 254

Masque de sous-réseau : 255 . 0 . 0 . 0 Durée : 8

Durée de l'allocation pour les clients DHCP

☒ Limitée à :

Jours : 8 Heures : 0 Minutes : 0

☐ Illimitée

Description : Plage d'adresses distribuées par le serveur DHCP

OK Annuler Appliquer

Propriétés d'une étendue

Ce premier onglet n'est pas forcément très intéressant, car ce sont les paramètres de votre étendue que vous venez de configurer. Les deux autres onglets en revanche, eux, sont nouveaux :

- L'onglet **DNS** permet de **gérer la mise à jour des enregistrements DNS à chaque fourniture de configuration**. Cette option est très pratique pour obtenir une association IP<->nom qualifié de vos clients DHCP. Attention, il est possible que le serveur DHCP puisse écraser les enregistrements DNS existants, c'est pourquoi il peut être intéressant de mettre en place la protection des noms.

À noter l'option "**Toujours mettre à jour dynamiquement les enregistrements DNS**" qui n'est pas celle par défaut. Il peut toutefois être intéressant de créer un enregistrement DNS dès qu'une IP est fournie.

- L'onglet **Avancé** permet de choisir si seul le protocole DHCP sera utilisé, ou si le protocole BOOTP sera utilisé (ou les deux) ! Par défaut, seul DHCP est utilisé. BOOTP permet de fournir toutes les options de démarrage à un client. Dans certains cas, ce protocole peut être très pratique. Vous retrouvez ici le retard de réponse que le serveur peut inclure avant de fournir une réponse à un client demandant une configuration !

Autorisez les flux du serveur DHCP

Afin de fonctionner correctement, il vous reste une dernière étape à mettre en œuvre : **autoriser les flux au niveau du pare-feu Windows**. Pour cela, rendez-vous dans les outils d'administration (dans le menu Démarrer) et ouvrez le **"Pare-feu Windows avec fonctions avancées de sécurité"**. Créez une **"Règle de trafic entrant"** en spécifiant le protocole UDP sur les ports 67 et 68, puis autorisez ce flux et nommez la règle (par exemple Serveur DHCP). Vous avez mis en œuvre un serveur Windows avec un rôle de serveur DHCP. Félicitations !

Si vous souhaitez utiliser du multicast, il vous faudra également ouvrir le port UDP 2535.

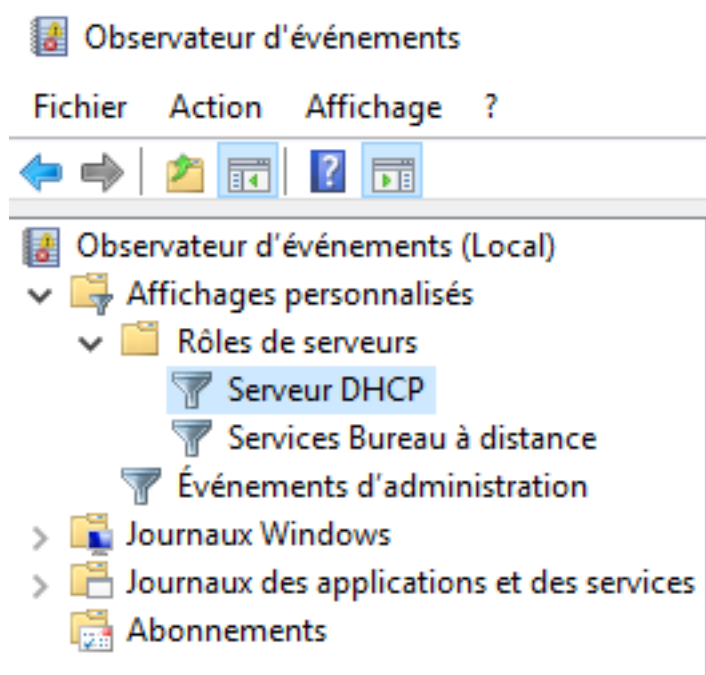
Diagnosticuez un problème sur votre DHCP

Ah, le diagnostic... Il peut arriver que votre serveur devienne capricieux et ne fournisse plus de configuration IP. Pour cela, la première chose à faire est d'aller voir au niveau des baux :

- Est-ce qu'il reste des baux disponibles ?
- Est-ce qu'il n'y a pas eu deux offres de configuration identiques distribuées ?
- Est-ce que mes flux sont vraiment ouverts et mon serveur joignable sur le réseau ?

Pour cela, il vous suffit de vous rendre dans la partie **Baux d'adresses** du gestionnaire DHCP.

Dans certains cas, le problème peut être plus profond ; à ce moment il vous faudra sortir votre observateur d'événements. Vous verrez qu'un **nouveau** journal sera disponible :

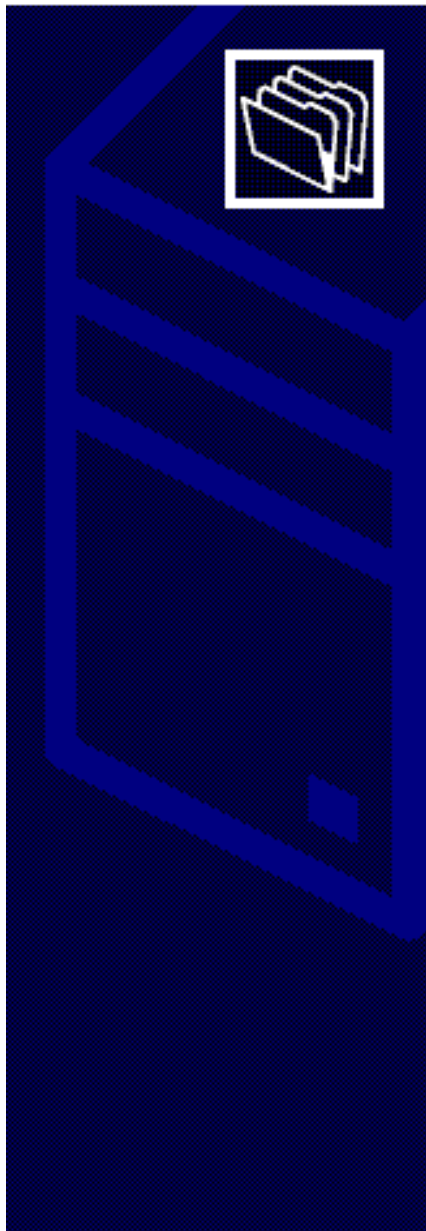


Nouveau journal Serveur DHCP

Redonnez votre serveur DHCP

Il est possible de mettre en place **deux serveurs DHCP** fournissant une étendue unique. **L'intérêt** : assurer la haute disponibilité du rôle. Pour cela, créez un nouveau serveur disposant du rôle **Serveur DHCP** sans aller plus loin (pas d'étendues), puis faites un clic droit sur le nom de votre serveur dans le gestionnaire DHCP sur IPv4, et choisissez **"Configurer un basculement"** :

Configurer un basculement



Introduction au basculement DHCP

Le basculement DHCP permet la haute disponibilité des services DHCP en synchronisant les informations des baux d'adresses IP entre deux serveurs DHCP. Le basculement DHCP fournit également un équilibrage de charge en matière de requêtes DHCP.

Cet Assistant vous guide tout au long de la configuration du basculement DHCP. Sélectionnez dans la liste suivante les étendues disponibles pouvant être configurées pour une haute disponibilité. Les étendues déjà configurées pour une haute disponibilité ne figurent pas dans la liste ci-dessous.

Étendues disponibles : ☒ Sélectionner tout

192.168.1.0

< Précédent

Suivant >

Annuler

Configurez un basculement

Ainsi, les bases de données seront synchronisées et les configurations fournies seront suivies non plus par un serveur, mais deux.

Les propriétés de votre serveur DHCP

Si vous cliquez sur IPv4 et affichez les propriétés, vous allez voir, comme pour votre étendue, qu'il est possible d'aller plus loin dans la configuration de votre rôle :

Propriétés de : IPv4



Général DNS Filtres Basculement Avancé

Serveur

☐ Mettre à jour les statistiques automatiquement toutes les :

Heures : Minutes :

☒ Activer l'enregistrement d'audit DHCP
Enregistre quotidiennement l'activité du serveur dans un fichier journal afin d'observer les performances du système et de résoudre les problèmes du service.

☐ Afficher le dossier de la table BOOTP
Affiche la table des serveurs qui peut contenir les entrées de configurations pour prendre en charge les clients BOOTP.

OK Annuler Appliquer

Propriétés IPv4

Vous avez la possibilité de mettre en place des statistiques de façon automatique, ce qui vous permettra d'observer à intervalles réguliers si votre serveur répond correctement, si les clients formulent des requêtes cohérentes, et l'occupation de votre étendue.

Pour voir les statistiques, dans le gestionnaire DHCP, faites un clic droit sur "IPv4", puis "Afficher les statistiques" :

Statistiques du serveur SRVDHCPPAR01			
Description	Détails		
Heure de début	14/11/2022 09:27:23		
Durée de fonctionnement	1 heures 8 minutes, 26 secondes		
Découvertes	0		
Offres	0		
Offres retardées	0		
Demandes	0		
Accusés de réception	0		
Accusés de réception négatifs	0		
Refus	0		
Libérations	0		
Nombre total d'étendues	1		
Étendues pour lesquelles un retard est configuré	0		
Nombre total d'adresses	254		
- Utilisées	0 (0%)		
- Disponibles	254 (100%)		
		Actualiser	Fermer

Statistiques d'un serveur DHCP

Voilà, vous savez presque tout sur le rôle DHCP ! Je vous laisse expérimenter toutes les possibilités offertes par Microsoft à ce sujet, car elles pourraient nécessiter un cours à part entière.

Allez plus loin

- La [RFC2131](#) sur DHCP (US).
- Les [nouveauautés du rôle](#).
- Le [guide d'installation](#) Microsoft (US).

En résumé

- Le rôle Serveur DHCP permet de **simplifier la configuration** de clients au sein d'un réseau.
- Tous les paramètres et options sont accessibles via **un assistant simplifiant** la prise en main et la mise en route.
- Microsoft permet d'**augmenter la sécurité** via la mise en redondance de deux serveurs disposant du rôle de Serveur DHCP.

Dans le prochain chapitre, vous découvrirez le service DNS, son fonctionnement et sa configuration.

Dans ce nouveau chapitre, je vous propose d'**installer le rôle de Serveur DNS** sur un serveur. Ce rôle est primordial pour de nombreux autres rôles (Active Directory, pour ne citer que le plus utilisé). Il permet d'**associer un nom qualifié à une adresse IP**. D'ailleurs, c'est sur ce protocole que se base le Web tel que nous le connaissons aujourd'hui.

Rappelez-vous les fondamentaux de DNS

DNS est l'abréviation de **Domain Name System**. Il s'agit d'un protocole qui permet d'associer un nom à une adresse IP.

Un client (souvent le navigateur web) envoie une demande pour connaître l'adresse IP du serveur web correspondant à l'adresse que vous avez entrée.

Par exemple, si vous allez sur **www.exemple.com**, votre navigateur doit demander quelle est l'adresse IP du serveur nommé **www** dans la zone DNS **exemple.com**.

Pour cela, il va envoyer une requête au serveur DNS configuré sur votre poste, et faire une demande de **type A** concernant **www.exemple.com**. Si votre serveur DNS **ne connaît pas** la réponse, il va alors se tourner vers un autre serveur DNS (souvent ce sera l'un des serveurs racines (Root Servers) gérant les enregistrements de la zone ".").

Dans cette zone particulière sont référencés les serveurs des zones **".com"**, **".fr"**, et d'une manière plus générale, **".extension du nom de domaine"**.

Alors votre serveur interrogera en retour le serveur de nom de la zone **".com"** à la recherche du serveur DNS de la zone **".com"**, et la mécanique recommencera à la recherche de la zone **exemple.com** qui renverra, à ce moment-là, l'enregistrement **A** correspondant au champ **www** de sa zone : vous devriez avoir l'IP 91.198.174.232.

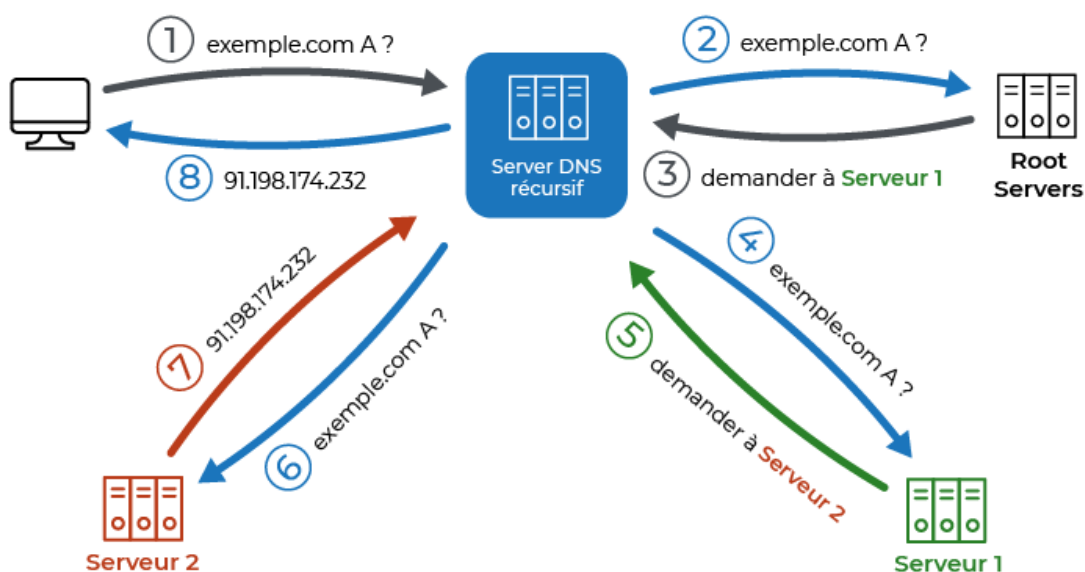


Schéma de fonctionnement du DNS

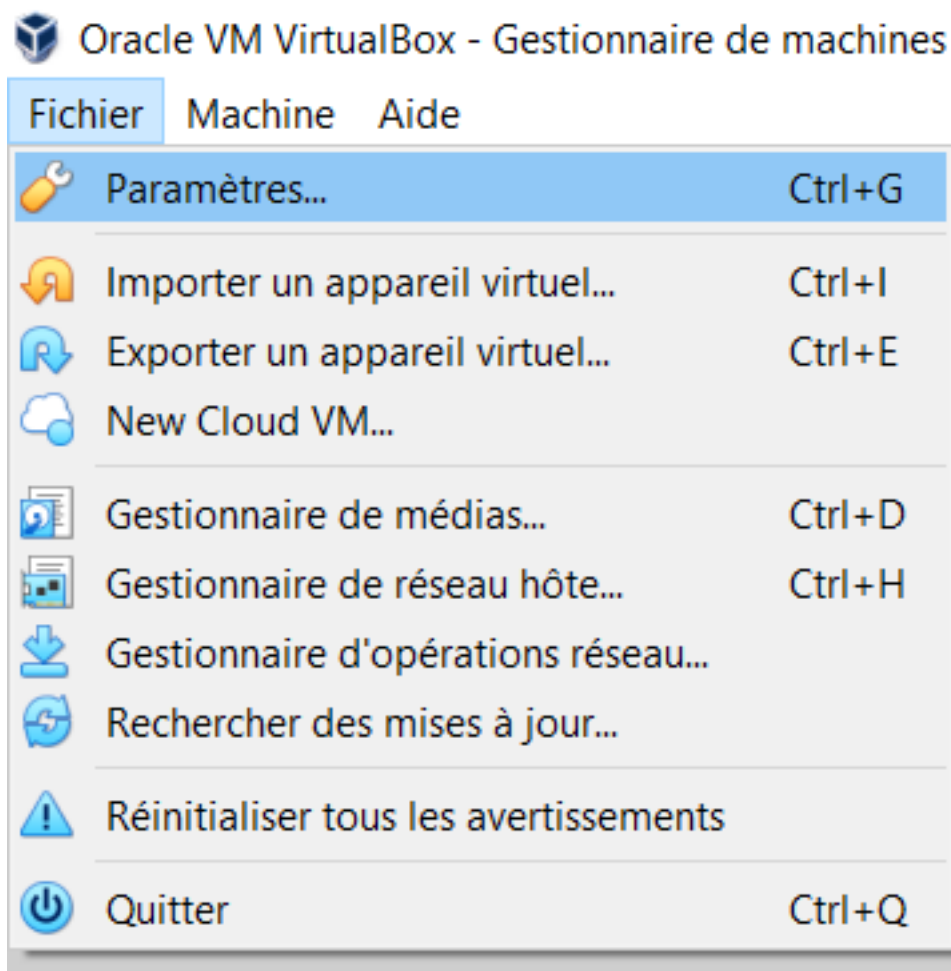
Avant de passer à la suite, si vous utilisez une machine virtuelle, vous allez devoir apporter quelques modifications à cette VM (Virtual Machine).

Comme vous le voyez sur le schéma précédent, votre serveur DNS doit pouvoir :

- Recevoir des requêtes provenant des machines sur votre réseau privé ;
- Envoyer des requêtes vers des serveurs DNS publics (qui se trouvent sur internet).

Il doit donc être connecté à la fois à votre **réseau privé** d'entreprise et au **réseau internet**, tout cela avec une carte réseau ayant **une adresse IP fixe**. En effet **l'adresse IP d'un serveur DNS** (tout comme celle d'un serveur DHCP), **doit toujours être statique** pour qu'il puisse être facilement retrouvé par les machines clients.

Pour pouvoir obtenir cette configuration sur VirtualBox (accès réseau privé + accès réseau internet + choix d'une adresse IP fixe), vous allez devoir modifier le mode de connexion dans Virtualbox. Pour cela, éteignez votre VM et allez dans les paramètres de VirtualBox :



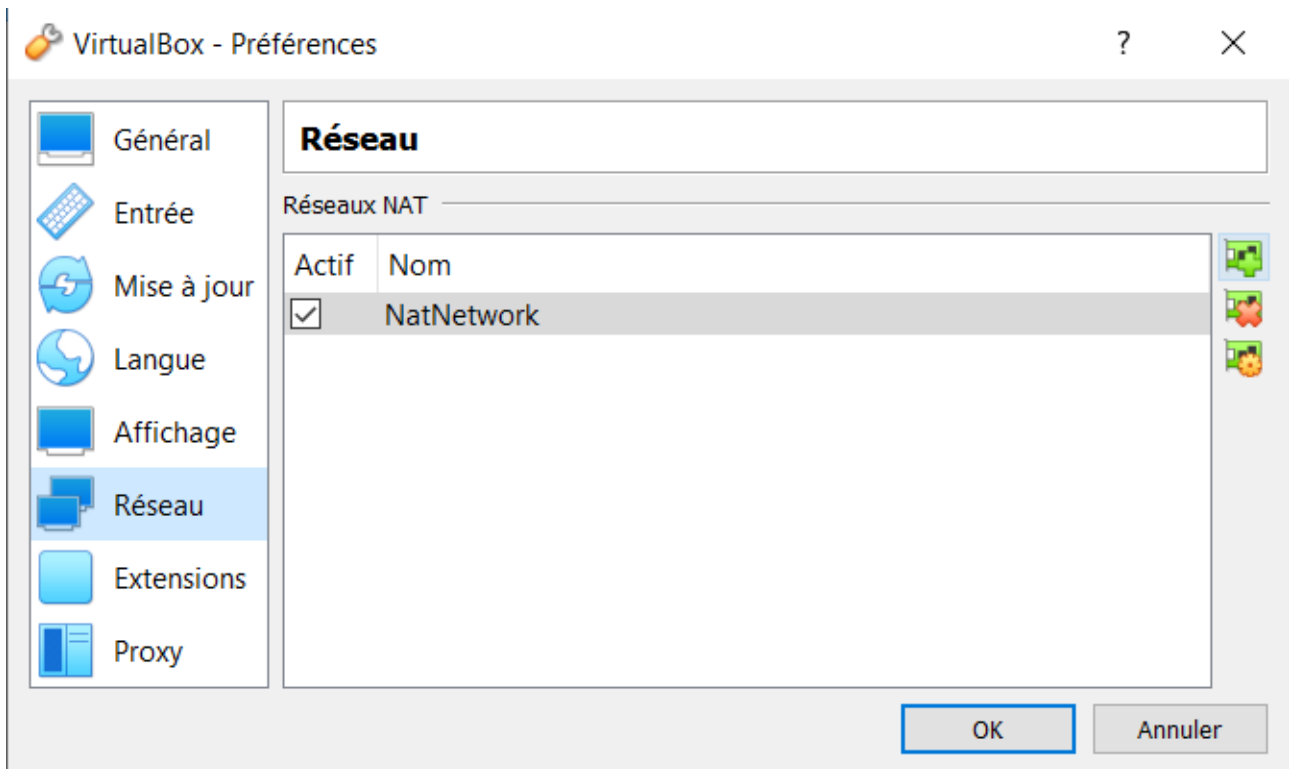
Accès aux paramètres de VirtualBox

La version 7 de VirtualBox a légèrement changé au niveau de l'interface graphique : pour accéder au menu de gestion du réseau, vous devrez suivre le chemin suivant :

Fichier -> Outils -> Network Manager.

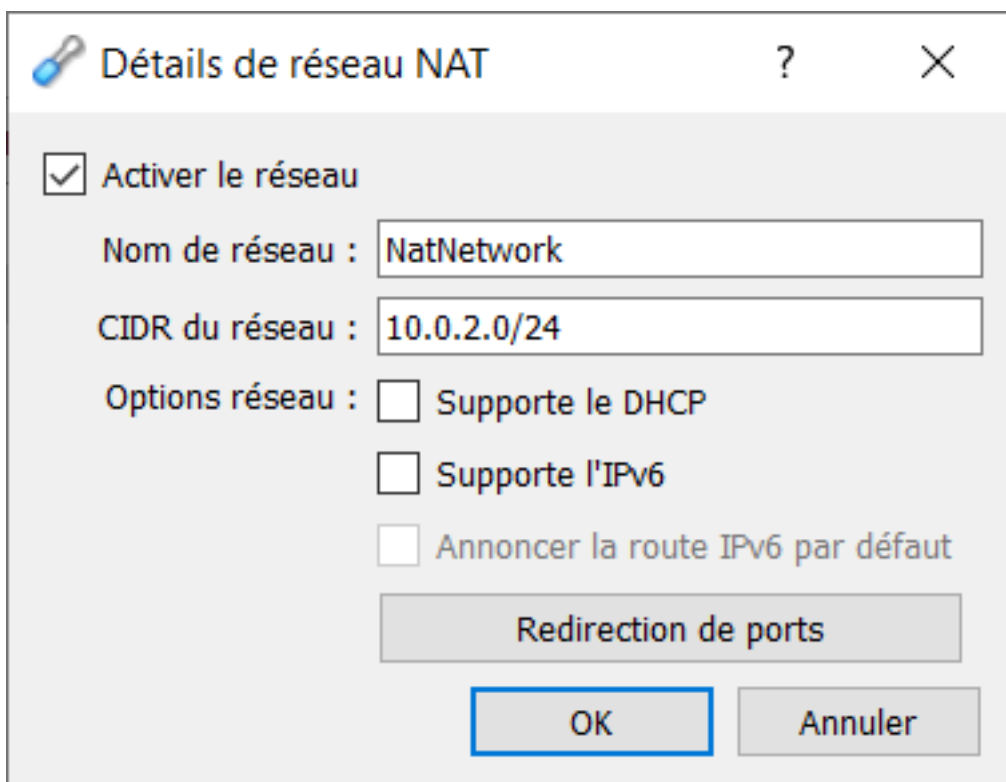
Cliquez ensuite sur l'onglet "Créer l'adaptateur virtuel", puis "Nat Networks".

Dans la fenêtre suivante, rendez-vous dans l'onglet "Réseau" et ajoutez un nouveau réseau NAT :



Préférences réseau

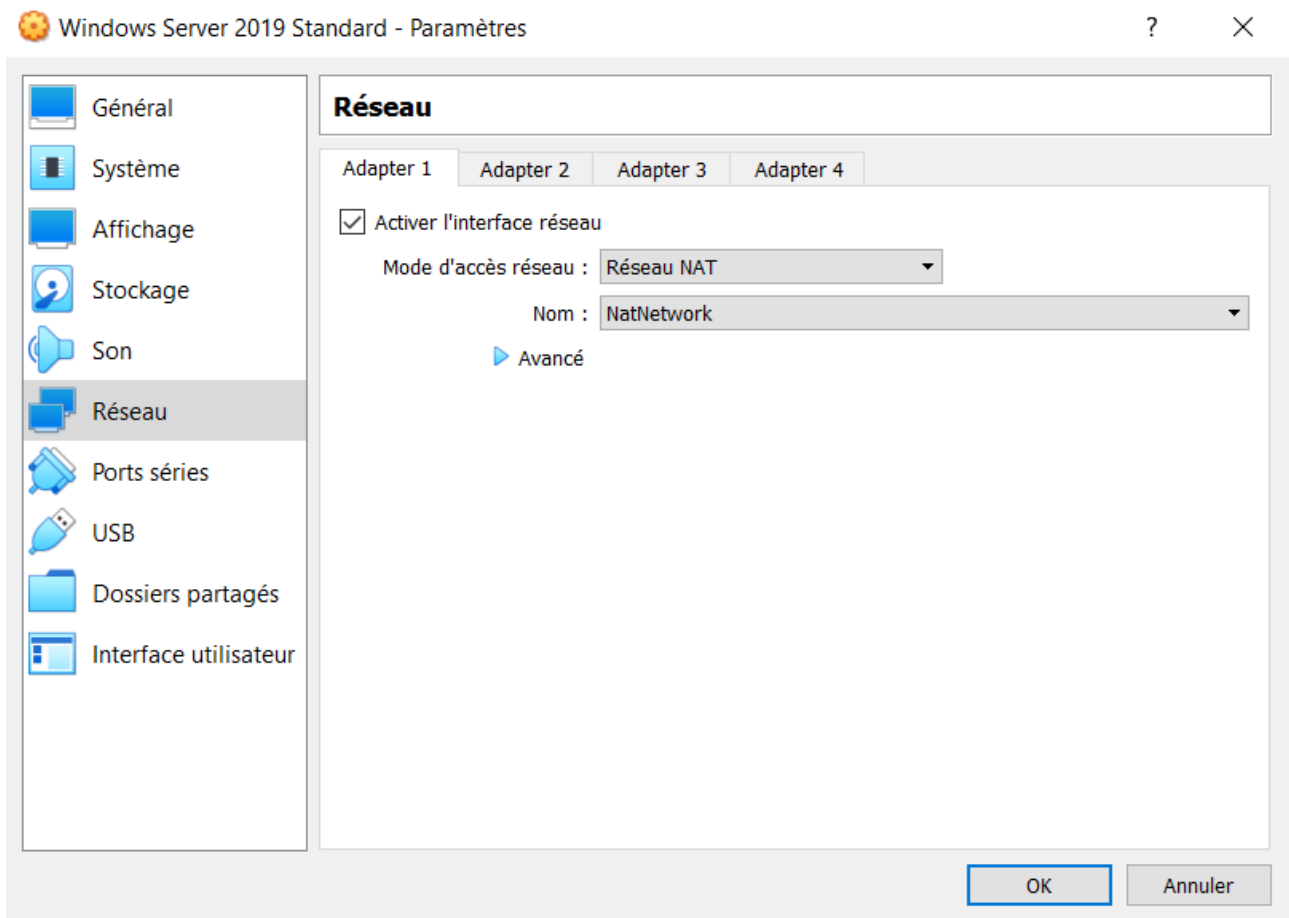
Dans les propriétés de ce réseau vous pouvez renseigner quel réseau IP vous souhaitez utiliser sur votre VM et surtout, vous pouvez décider de désactiver le DHCP sur ce réseau afin de pouvoir choisir manuellement l'adresse IP de vos VM. Décochez donc la case "Supporte le DHCP" :



Paramètres du réseau NAT

Vous pouvez valider les paramètres. Il ne vous reste plus qu'à associer la carte réseau de votre serveur Windows à ce nouveau réseau NAT nommé NATNetwork.

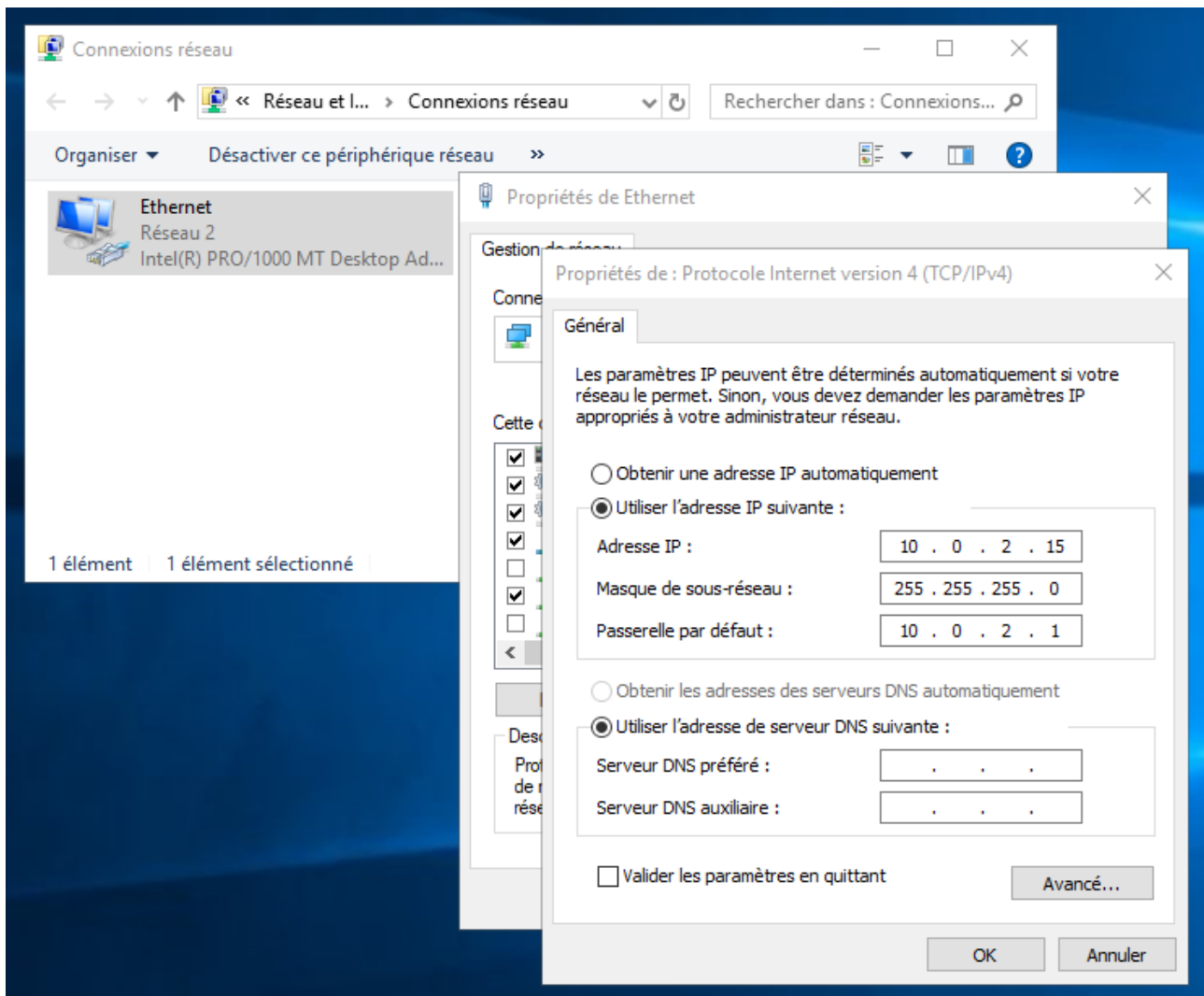
Pour cela rendez-vous dans la configuration matérielle de votre VM et sélectionnez ce nouveau mode réseau :



Configuration matérielle de la VM Serveur Windows

Une fois la configuration terminée, validez et démarrez votre serveur Windows. Vérifiez maintenant simplement que votre carte réseau soit bien configurée avec **une adresse IP statique qui soit dans le réseau que vous avez défini lors de la création du réseau NAT** Virtualbox.

Dans notre cas nous venons de créer un réseau NAT défini sur 10.0.2.0/24, nous pouvons donc choisir par exemple l'adresse IP 10.0.2.15. Renseignez également bien la passerelle qui sera toujours la première adresse du réseau, ici 10.0.2.1 :



Configuration IP de l'interface du serveur

Avec cette configuration vous devriez avoir accès à Internet depuis votre serveur, ce qui sera indispensable pour le fonctionnement du DNS.

Vous pouvez vérifier cela en faisant un ping vers l'adresse 8.8.8.8 par exemple :

```
Administrateur : Invite de commandes

(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>
C:\Users\Administrateur>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=36 ms TTL=112
Réponse de 8.8.8.8 : octets=32 temps=45 ms TTL=112
Réponse de 8.8.8.8 : octets=32 temps=39 ms TTL=112
Réponse de 8.8.8.8 : octets=32 temps=39 ms TTL=112

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 36ms, Maximum = 45ms, Moyenne = 39ms

C:\Users\Administrateur>
```

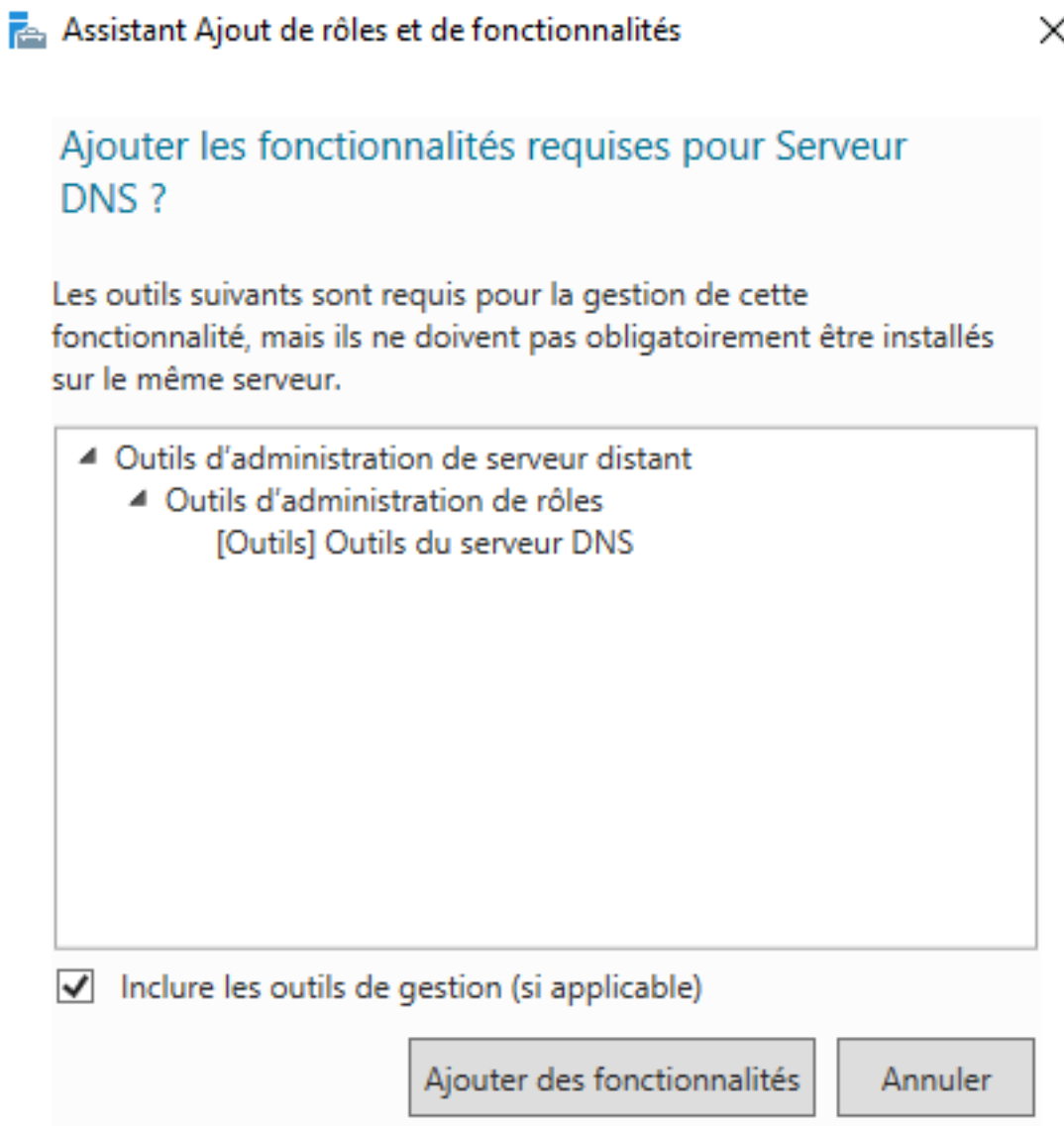
Ping fonctionnel vers Internet (adresse IP publique 8.8.8.8)

Installez le rôle Serveur DNS

Maintenant, je vous propose d'**installer le rôle DNS** sur un serveur Windows.

Pour ne pas mélanger les rôles, vous pouvez aussi décider d'installer le rôle DNS sur un autre serveur Microsoft si vous en avez un deuxième.

Pour cela, comme vous le savez, rendez-vous sur le **gestionnaire de serveur** et ajoutez un rôle. À la sélection du rôle, Microsoft vous propose comme pour le DHCP, des fonctionnalités obligatoires :



Fonctionnalités obligatoires du rôle Serveur DNS

Ensuite, vous avez des informations sur ce rôle, qui vous présentent le fonctionnement général (avec le lien au DHCP) et une configuration possible, préconisée par Microsoft, à savoir

l'intégration à l'Active Directory. Cela permet de bénéficier du **mécanisme de réplication de l'AD** pour simplifier la réplication des zones sur les serveurs AD (qui se doivent d'avoir le rôle Serveur DNS pour fonctionner) :

Serveur DNS

SERVEUR DE DESTINATION
SRVDHCPAR01

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Serveur DNS

Confirmation

Résultats

Le système DNS (Domain Name System) fournit une méthode standard d'association de noms à des adresses Internet numériques. Cela permet aux utilisateurs de référencer les ordinateurs du réseau en utilisant des noms faciles à retenir au lieu de longues séries de chiffres. En outre, le système DNS intègre un espace de noms hiérarchique, ce qui permet que chaque nom d'hôte soit unique sur un réseau local ou étendu. Les services DNS Windows peuvent être intégrés aux services DHCP (Dynamic Host Configuration Protocol) sur Windows. Il n'est ainsi plus nécessaire d'ajouter des enregistrements DNS lorsque des ordinateurs sont ajoutés au réseau.

Éléments à noter :

- L'intégration du serveur DNS aux services de domaine Active Directory réplique les données DNS et d'autres données du service d'annuaire, ce qui facilite la gestion DNS.
- Les services de domaine Active Directory nécessitent l'installation d'un serveur DNS sur le réseau. Si vous installez un contrôleur de domaine, vous pouvez aussi installer le rôle serveur DNS avec l'Assistant Installation des services de domaine Active Directory, en sélectionnant le rôle Services de domaine Active Directory.

< Précédent

Suivant >

Installer

Annuler

Informations sur le rôle Serveur DNS de l'assistant d'installation

Validez les informations finales et lancez l'installation en cliquant sur "**Installer**". Vous maîtrisez l'assistant maintenant, non ?

Cette fois il n'est pas nécessaire de redémarrer. Cette étape dépend des rôles, et vous serez averti par les notifications sur le tableau de bord si un redémarrage est nécessaire.

Gestionnaire de serveur

Gestionnaire de serveur • Tableau de bord

Tableau de bord

Serveur local
Tous les serveurs
DHCP
DNS
Services de fichiers et d...

BIENVENUE DANS GESTIONNAIRE DE SERVEUR

1 Configurer ce serveur local

2 Ajouter des rôles et des fonctionnalités

3 Ajouter d'autres serveurs à gérer

4 Créer un groupe de serveurs

5 Connecter ce serveur aux services cloud

Rôles et groupes de serveurs

Rôles : 3 | Groupes de serveurs : 1 | Nombre total de serveurs : 1

DHCP 1

DNS 1

Services de fichiers et de stockage 1

Serveur local 1

Tous les serveurs 1

Tableau de bord après installation du rôle Serveur DNS

Si vous allez sur le tableau de bord de votre serveur, vous pourrez noter à quel point le nommage est **primordial** ! J'ai volontairement laissé le nom que j'ai positionné sur le serveur lors de l'installation du rôle DHCP, voyez la confusion possible pour l'administrateur :

PROPRIÉTÉS			
Pour SRVDHCPPAR01			
Nom de l'ordinateur	SRVDHCPPAR01	Dernières mises à jour installées	09/11/2022 14:04
Groupe de travail	WORKGROUP	Windows Update	Télécharger les mises à jour uniquement à l'aide de Windows Update
		Dernière recherche de mises à jour :	Aujourd'hui à 08:34
Pare-feu Windows Defender	Public : Activer et bloquer toutes les connexions entrantes	Antivirus Windows Defender	Protection en temps réel : activée
Gestion à distance	Activé	Commentaires et diagnostics	Paramètres
Bureau à distance	Désactivé	Configuration de sécurité renforcée d'Internet Explorer	Actif
Association de cartes réseau	Désactivé	Fuseau horaire	(UTC+01:00) Bruxelles, Copenhague, Madrid, Paris
Ethernet	10.0.2.15	ID de produit (Product ID)	00431-10000-00000-AA213 (activé)
Version du système d'exploitation	Microsoft Windows Server 2019 Standard Evaluation	Processeurs	Intel(R) Core(TM) i7-10610U CPU @ 1.80GHz
Informations sur le matériel	innotek GmbH VirtualBox	Mémoire installée (RAM)	2 Go
		Espace disque total	99,46 Go

Rôle DNS installé sur SRVDHCPPAR01

Soyez vigilant : il n'est pas logique d'avoir un nom ne reflétant pas le rôle du serveur. Idéalement, il faudrait que le nom indique que le serveur est maintenant serveur DNS et DHCP. Attention toutefois, si votre serveur est accessible de l'extérieur de votre réseau, le fait de connaître, via son nom, son rôle, est une information critique. Entre les mains d'un pirate informatique, cela permet d'accélérer les recherches de vecteurs d'attaque. Il conviendra de correctement configurer le DNS pour éviter de faire fuiter de telles informations.

Maintenant que vous avez installé ce rôle, je vous propose de travailler sur sa gestion !

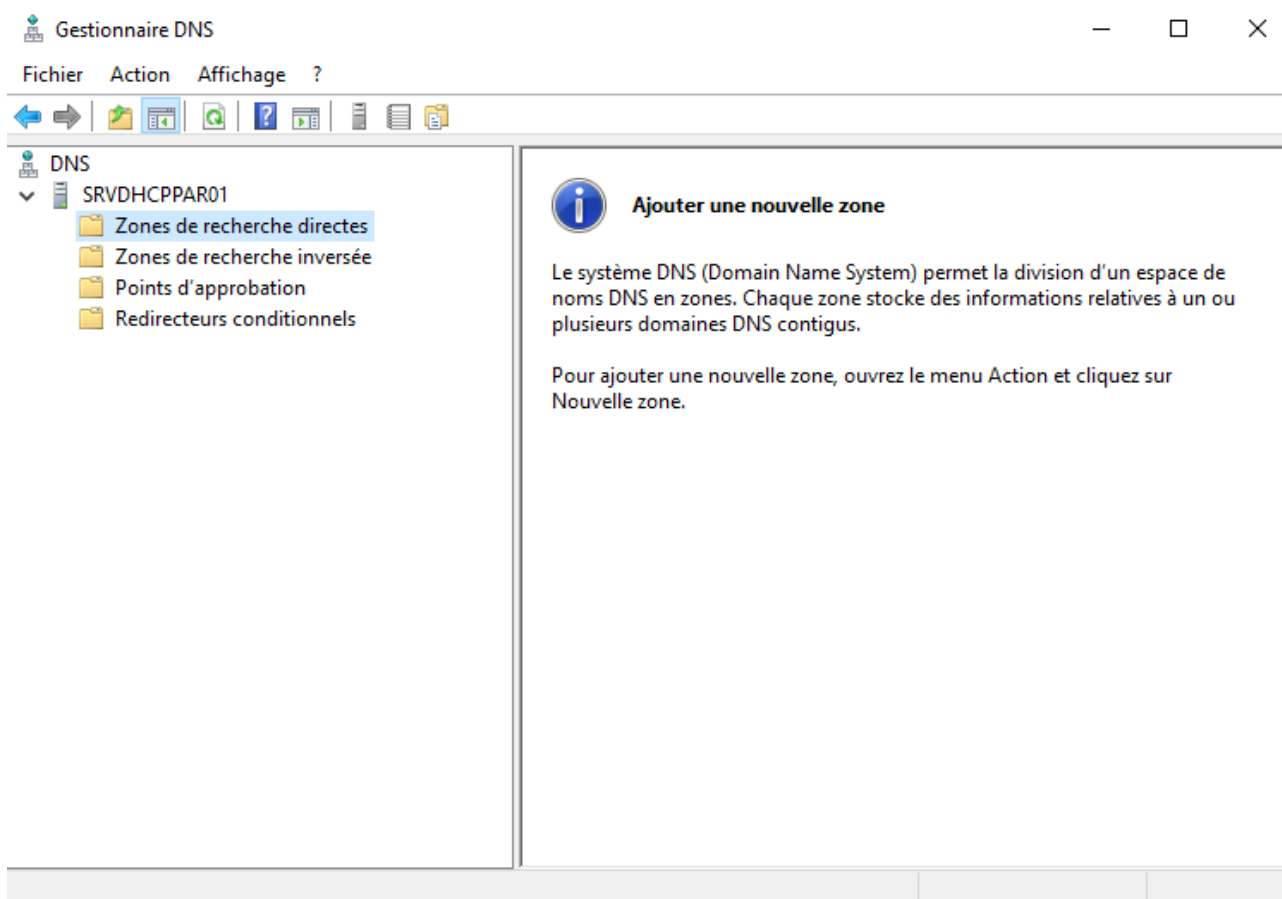
Gérez le service DNS

Tout comme le gestionnaire DHCP, il existe le gestionnaire DNS. Cette console dédiée à l'administration du rôle DNS permet de **créer les différentes zones** nécessaires au fonctionnement du DNS.

Pour y accéder, faites un clic droit sur votre serveur, puis "Gestionnaire DNS" :

The screenshot shows the Windows Server Management console. On the left, the 'Tableau de bord' sidebar has 'DNS' selected. The main pane is titled 'SERVEURS' and shows 'Tous les serveurs | 1 au total'. Below this is a table with columns: 'Nom du serveur', 'Adresse IPv4', 'Facilité de gestion', 'Dernière mise à jour', and 'Activation de Windows'. The table contains one entry: 'SRVDHCPPAR01', '10.0.2.15', 'Connecté', '14/11/2022 10:53:35', and '00431-10000-00000-AA213 (Activé)'. A right-click context menu is open over the server name, listing options like 'Ajouter des rôles et fonctionnalités', 'Arrêter le serveur local', 'Gestion de l'ordinateur', 'Connexion Bureau à distance', 'Windows PowerShell', 'Configurer l'association de cartes réseau', 'Gestionnaire DNS' (which is highlighted), 'Gérer en tant que...', 'Actualiser', and 'Copier'.

Accès au gestionnaire DNS



Gestionnaire DNS

La maîtrise des noms est un domaine souvent pris à la légère. Rappelez-vous que **100 % des requêtes vers Internet passent par le DNS**.

Avant de créer votre première zone directe, il faut savoir comment un serveur DNS fonctionne : à chaque requête d'un client, la réponse va être mise en cache localement. Ce cache permettra à votre serveur, après avoir récupéré l'adresse IP du serveur www.exemple.com, de répondre plus rapidement sans avoir à relancer une requête récursive aux serveurs "root", ainsi qu'au serveur de la zone "exemple.com". Ce cache doit être géré.

Pourquoi ce cache doit-il être géré ?

Eh bien, tout simplement pour éviter de garder en mémoire l'association www.exemple.com vers l'IP **91.198.174.232**.

Eh oui, si l'administrateur de ce serveur décide de changer d'adresse IP, il serait dommage de ne plus pouvoir accéder à www.exemple.com.

Attention donc à régler le cache à une valeur ni trop faible, ni trop forte.

Par défaut, cette valeur est d'une journée (24 h) pour les réponses positives (une adresse IP au moins existe pour un nom qualifié) et de 15 minutes pour les réponses négatives. Pour afficher ces informations, ouvrez PowerShell et tapez la commande `Get-DnsServerCache` :

```
Administrateur : Windows PowerShell

PS C:\Program Files> get-dnsservercache

MaxTTL : 1.00:00:00
MaxNegativeTTL : 00:15:00
MaxKBSize : 0
EnablePollutionProtection : True
LockingPercent : 100
StoreEmptyAuthenticationResponse : True
IgnorePolicies : False

PS C:\Program Files>
```

Configuration de cache du serveur DNS

Nous reviendrons dans la dernière partie de ce cours sur l'utilisation de PowerShell. Utilisez l'aide en ligne de Microsoft pour modifier ces valeurs.

Enfin, vous allez vous assurer que le rôle DNS est correctement configuré. Dans le gestionnaire DNS, avec un clic droit sur le nom du serveur, choisissez **“propriétés”** :

Propriétés de : SRVDHCPPAR01

?

×

Enregistrement de débogage Enregistrement des événements Analyse

Interfaces Redirecteurs Avancé Indications de racine

Sélectionnez les adresses IP qui serviront les requêtes DNS. Le serveur peut écouter les requêtes DNS sur toutes les adresses IP définies pour cet ordinateur, ou vous pouvez le limiter aux adresses IP sélectionnées.

Écouter sur :

☒ Toutes les adresses IP

☐ Uniquement les adresses IP suivantes :

Adresses IP :

☒ 10.0.2.15

OK Annuler Appliquer Aide

Propriétés du serveur DNS

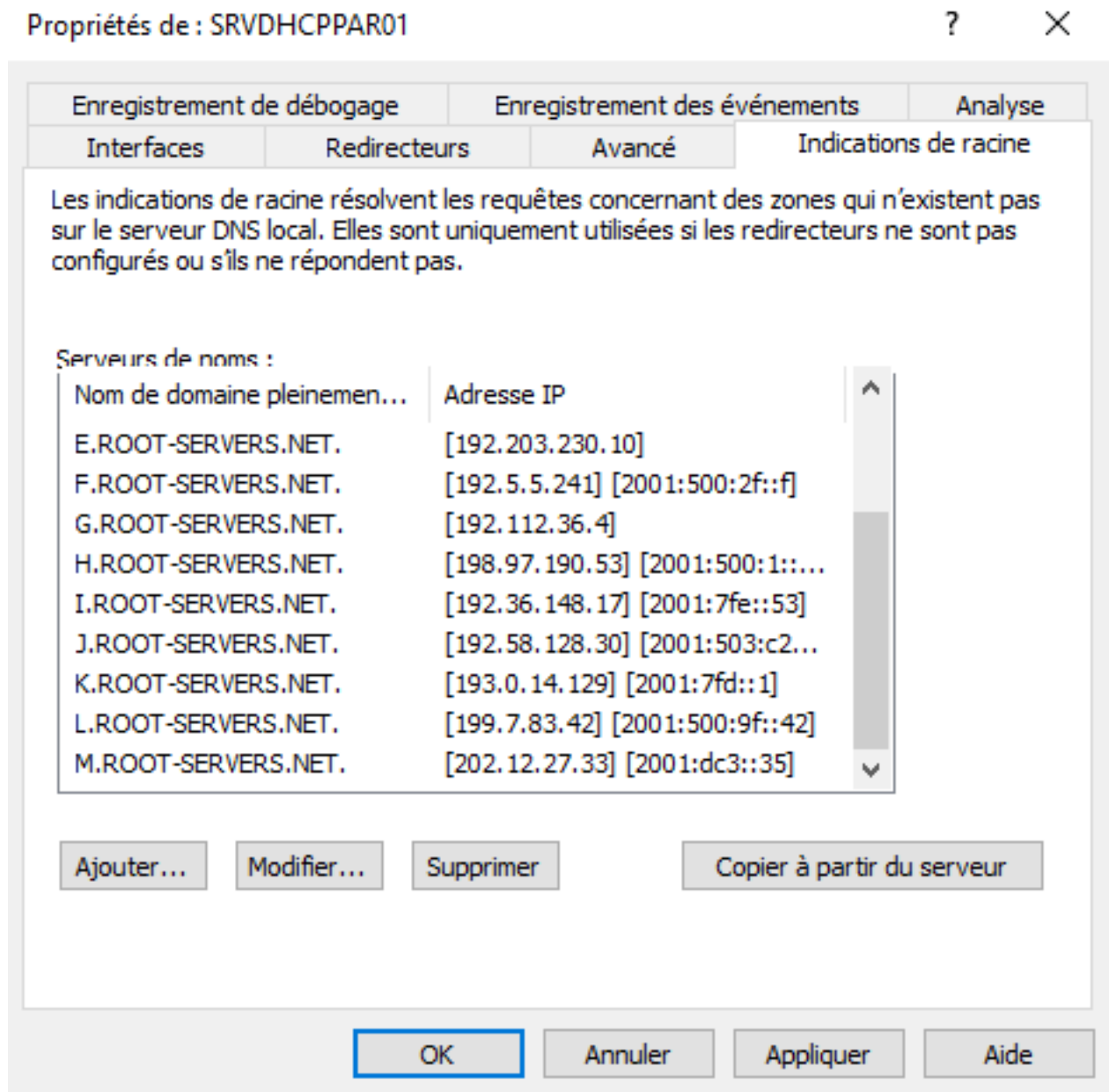
Le premier onglet permet de définir sur quelle interface votre serveur va recevoir et accepter les requêtes DNS. Dans notre cas, nous n'avons qu'une seule interface mais il est très courant que les serveurs d'entreprise aient plusieurs interfaces réseau.

Mais alors sur quelle interface doit écouter le service DNS ?

Tout dépend de votre réseau. Par défaut, il écoutera les requêtes DNS sur toutes les interfaces, et ce n'est pas du tout une bonne pratique. Si par exemple mon serveur avait 2 interfaces : une pour communiquer avec internet, et une autre pour communiquer avec le réseau privé de l'entreprise, il faudrait lui dire d'écouter les requêtes provenant uniquement du réseau privé. En effet, c'est de là que vont arriver les requêtes DNS, il n'y a donc aucune raison d'écouter également sur l'autre interface.

Dans notre cas, je vous propose de sélectionner uniquement l'**IP fixe** que vous avez configurée dans le premier chapitre.

Dirigez-vous sur l'onglet Indication de racine. Allez vérifier que votre serveur connaît les serveurs racines. Ce seront les serveurs qui seront contactés pour identifier une réponse à **www.exemple.com**, par exemple.



Serveurs racines connus de votre serveur DNS

Vous allez me dire, comment faire pour tester votre serveur DNS ? Il devrait être en mesure de répondre à n'importe quelle demande avec ces serveurs ?

Ouvrez, sur votre serveur, une invite de commande (un *Shell*). Tapez la commande **nslookup - 10.0.2.15** (où 10.0.2.15 est l'adresse IP de l'interface réseau de votre serveur). Vous entrez alors dans un client DNS interactif, en lien avec votre serveur ! Testez **www.exemple.com** :

```
nslookup - 10.0.2.15
```

```
Serveur par défaut : UnKnown
```

```
> www.exemple.com
```

Serveur : UnKnown

Réponse ne faisant pas autorité :

Nom : `www.exemple.com`

Addresses : `2606:2800:220:1:248:1893:25c8:1946`
`107.180.40.145`

Comme votre serveur n'est pas le gestionnaire de la zone **exemple.com**, il interroge récursivement les serveurs racines, puis le serveur DNS de la zone **exemple.com**. La réponse que votre serveur vous fournit ne fait pas autorité, car votre serveur la tient d'un autre serveur. 😊

Comment avoir des réponses faisant autorité ?

En disposant d'une zone DNS ; ça tombe bien, c'est ce que vous allez mettre en place !

Mettez en place votre première zone directe

Une **zone directe** permet d'associer un nom à une adresse IP, c'est bien plus simple pour nous, humains, de se rappeler d'un nom ; surtout qu'une adresse IP peut changer avec le temps, comme par exemple, lors d'un changement de fournisseur d'accès.

La première étape consiste à choisir un nom de domaine. Je vous propose de prendre une zone privée.

Prenez le cas suivant : suite à la configuration du DHCP, la direction de Gift S.A. vous demande de trouver un moyen de nommer les différents équipements et services sur le réseau. Le directeur en a marre de devoir taper l'adresse IP 10.0.2.10 pour accéder à l'intranet. Vous allez donc créer une zone directe pour le domaine "**gift.sa**" et y placer un enregistrement **A** faisant pointer **intranet.gift.sa** vers 10.0.2.10. Ainsi votre directeur pourra tranquillement taper **https://intranet.gift.sa** au lieu de l'adresse IP, mission réussie !

Pour cela, vous disposez (encore) d'un assistant. Cliquez sur Action en haut de votre écran puis sélectionnez "**Nouvelle zone...**".

Après l'écran de bienvenue, vous devriez avoir l'écran suivant :

Type de zone

Le serveur DNS prend en charge différents types de zones et de stockages.



Sélectionnez le type de zone que vous voulez créer :

☒ Zone principale

Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.

☐ Zone secondaire

Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.

☐ Zone de stub

Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.

☐ Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)

< Précédent

Suivant >

Annuler

Assistant de configuration d'un serveur DNS

Le premier choix est parfait, c'est ce que vous voulez faire. Validez ce choix par "**Suivant**", jusqu'à arriver sur la page du nom de la zone : il s'agit de "**gift.sa**", dans le cas présent. Puis la création du fichier de zone (et son emplacement sur votre serveur). Par défaut, le fichier s'appellera gift.sa.dns. Arrive ensuite la question des mises à jour dynamiques.

Cette option est à prendre avec des pincettes, car elle permet à un client de mettre à jour des enregistrements. Mal configurée, cette option permettrait à un utilisateur malveillant de changer vos enregistrements pour les envoyer vers l'adresse IP d'un serveur qu'il gère, et pourrait mener à une campagne de fuite d'informations... Attention donc !

Mise à niveau dynamique

Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.



Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.

Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

☐ N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)

Cette option n'est disponible que pour les zones intégrées à Active Directory.

☐ Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées

Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.



Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

☒ Ne pas autoriser les mises à jour dynamiques

Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent

Suivant >

Annuler

Gestion de la mise à jour dynamique des enregistrements DNS

Votre zone est créée, allez voir maintenant son contenu, en cliquant sur “**Terminer**” puis en dépliant “**Zones de recherche directes**” :

Gestionnaire DNS

Fichier Action Affichage ?

Nom	Type	Données
(identique au dossier parent)	Source de nom (SOA)	[1], srvdhcpar01., hostmaster.
(identique au dossier parent)	Serveur de noms (NS)	srvdhcpar01.

Arborescence :

- DNS
 - SRVDHCPPAR01
 - Zones de recherche directes
 - gift.sa
 - Zones de recherche inversée
 - Points d'approbation
 - Redirecteurs conditionnels

Zone de recherche directe “gift.sa”

Votre zone ne contient que **deux enregistrements** qui permettent d'identifier le serveur faisant autorité (SOA), et le serveur de noms (NS). Il serait intéressant de créer votre enregistrement intranet demandé par la direction. Pour cela, un clic droit dans la fenêtre de droite (ou sur le nom de la zone) et sélectionnez “**nouvel hôte A ou AAAA**”. Les enregistrements A sont pour les IPv4 et les AAAA pour les IPv6. Entrez **le nom de l'hôte** au sein de la zone (“intranet” donc) et **l'adresse IP** associée :

Nouvel hôte ✕

Nom (utilise le domaine parent si ce champ est vide) :

intranet

Nom de domaine pleinement qualifié (FQDN) :

intranet.gift.sa.

Adresse IP :

10.0.2.10

☐ Créer un pointeur d'enregistrement PTR associé

Ajouter un hôte Annuler

Créer un enregistrement A

Le serveur 10.0.2.10 n'existe pas mais partons du principe que c'est celui qui héberge le site web intranet.

Vous avez ici la possibilité de créer un **PTR**, vous verrez cela dans la section suivante, d'ici quelques minutes ; ne cochez pas cette case et validez via "**Ajouter un hôte**". Vous remarquerez le champ (non modifiable) du nom de domaine pleinement qualifié (*fully qualified domain name – FQDN*), il comporte un "point" à la fin qui représente la zone racine (root), suivi de l'extension "sa" puis du domaine "gift". Le nom qualifié de l'intranet est donc "*intranet.gift.sa.*"

Pour vérifier que votre enregistrement est correctement créé, relancez une invite de commande et tapez la commande `nslookup intranet.gift.sa 10.0.2.15` pour demander de quelle adresse IP dispose l'hôte "*intranet.gift.sa*" au serveur 10.0.2.15 :

```
>nslookup intranet.gift.sa 10.0.2.15
Server : UnKnown
Address: 10.0.2.15
```

```
Nom : intranet.gift.sa
Address : 10.0.2.10
```

Voilà, vous savez créer des enregistrements A sur une zone directe ! Vous allez pouvoir nommer tous vos équipements ou serveurs avec des noms et arrêter d'utiliser les adresses IP.

Découvrez les autres types d'enregistrements

Avant de passer à la zone inversée, je vous propose de voir quelques éléments supplémentaires. Le DNS permet de répondre à une requête d'un client, le type A permet de demander une adresse IP à partir d'un nom, mais de nombreux autres types sont disponibles, comme NS qui permet de connaître le serveur de noms. Sous Windows, vous pouvez effectuer des requêtes sur différents types avec l'option `set type=XXX`, où XXX est le type demandé.

Un autre type est le SOA (Start Of Authority), permettant de savoir quel serveur fait autorité sur une zone.

```
>nslookup - 10.0.2.15
Serveur par défaut : UnKnown
Address: 10.0.2.15
```

```
>set type=SOA
>gift.sa
Serveur : UnKnown
Address: 10.0.2.15
```

```
gift.sa
primary name server = srvdhcppar01
responsible mail addr = hostmaster
serial = 2
refresh = 900 (15 mins)
retry = 600 (10 mins)
expire = 86400 (1 day)
default TTL = 3600 (1 hour)
```

```
>set type=NS
>gift.sa
Serveur : UnKnown
Address: 10.0.2.15
```

```
gift.sa nameserver = srvdhcppar01
```

Un autre type est le **CNAME** qui permet d'associer un nom à un nom.

Cela peut être pratique pour donner un nom à un serveur en pointant sur le nom du service. Par exemple, cela peut être intéressant d'avoir un nom différent pour administrer l'intranet, mais il peut être long de taper "*intranet.gift.sa*" lorsque l'on administre ce service. Alors un **CNAME** "*int.gift.sa*" pointant sur *intranet.gift.sa* permet de résoudre ce problème :

```
>set type=CNAME
>int.gift.sa
Serveur : UnKnown
Address: 10.0.2.15
```

```
int.gift.sa canonical name = intranet
```

Il existe de nombreux types, les plus connus étant **NS**, **SOA**, **A**, **AAAA**, **CNAME**, **TXT**, **MX** (Mail eXchange pour les serveurs de messagerie). La méthode à mettre en œuvre est la même, quel que soit le type.

Mettez en œuvre votre première zone inversée

Maintenant que vous disposez d'une zone directe, ne serait-ce pas intéressant de créer une zone inversée ? C'est une association d'une **adresse IP à un nom**, en somme l'inverse de la zone directe. Cela permet de confirmer que le nom choisi dans une zone directe est bien associé à l'adresse IP, et donc d'interroger un DNS sur une adresse IP, si vous changez l'adresse du serveur DNS configuré sur votre serveur DNS, ici, dans la zone Serveur DNS préféré :

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

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 10 . 0 . 2 . 15

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

Passerelle par défaut : 10 . 0 . 2 . 2

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 10 . 0 . 2 . 15

Serveur DNS auxiliaire : . . .

☐ Valider les paramètres en quittant

Avancé...

OK Annuler

Configuration de votre serveur DNS comme serveur DNS de votre serveur
Toutes les requêtes de nom seront alors envoyées à votre serveur. Ouvrez alors une invite de commande et tapez `nslookup intranet.gift.sa` :

```
C:\Users\Administrateur>nslookup intranet.gift.sa
Serveur : UnKnown
```

Address: 10.0.2.15

Nom : intranet.gift.sa

Address: 10.0.2.10

```
C:\Users\Administrateur>nslookup 10.0.2.10
```

Serveur : UnKnown

Address: 10.0.2.15

*** UnKnown ne parvient pas à trouver 10.0.2.10 : Non-existent domain

Le nom **intranet.gift.sa** est bien résolu (par la zone directe) en 10.0.2.10, mais l'inverse ne se fait pas ! Il vous faut créer une zone inversée.

Pour cela, rendez-vous sur le Gestionnaire DNS et avec un clic droit sur la partie "zone inversée", sélectionnez "**Nouvelle zone**"; après l'écran d'accueil, vous devriez arriver sur l'écran suivant :

Assistant Nouvelle zone ✕

Type de zone 

Le serveur DNS prend en charge différents types de zones et de stockages.

Sélectionnez le type de zone que vous voulez créer :

- ☒ **Zone principale**
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.
- ☐ **Zone secondaire**
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.
- ☐ **Zone de stub**
Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.

☐ Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)

< Précédent Suivant > Annuler

Création d'une zone inversée

Là encore, vous disposez de différents types de zones en fonction du niveau de maîtrise que vous souhaitez. Nous n'aborderons ici que le type principal. L'écran suivant vous propose de choisir entre IPv4 et v6.

Idem, **ici restez sur IPv4**. Ensuite, vous n'avez plus qu'à entrer l'ID de votre réseau. Il s'agit des octets de l'adresse IP représentant votre réseau et enfin, le nom du fichier de zone vous sera proposé et à nouveau la mise à jour dynamique (idem, on refusera les mises à jour dynamiques) :

Assistant Nouvelle zone



Nom de la zone de recherche inversée

Une zone de recherche inversée traduit les adresses IP en noms DNS.



Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

☒ ID réseau :

10 . 0 . 2 .

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

☐ Nom de la zone de recherche inversée :

2.0.10.in-addr.arpa

< Précédent

Suivant >

Annuler

Id de réseau

Fin de l'Assistant Nouvelle zone



L'Assistant Nouvelle zone s'est terminé correctement. Vous avez spécifié les paramètres suivants :

Nom : 2.0.10.in-addr.arpa
 Type : Zone principale standard
 Type de recherche : Inversée
 Nom de fichier : 2.0.10.in-addr.arpa.dns

Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.

Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.

< Précédent

Terminer

Annuler

Finalisation de la création de la zone inversée

De la même façon que pour une zone directe, vous n'avez que deux enregistrements par défaut :

	Nom	Type	Données
DNS ▼ SRVDHCPPAR01 ▼ Zones de recherche directes gift.sa ▼ Zones de recherche inversée 2.0.10.in-addr.arpa Points d'approbation Redirecteurs conditionnels	(identique au dossier parent) (identique au dossier parent)	Source de nom (SOA) Serveur de noms (NS)	[1], srvdhcpar01., hostmaster. srvdhcpar01.

Zone inversée

Ajoutez un enregistrement de type **PTR** pour *intranet.gift.sa* (vous pouvez parcourir votre zone directe avec l'assistant de création d'enregistrement PTR pour être certain de pointer vers le bon nom !). **Entrez l'adresse IP** (enfin, juste le dernier octet), et vous obtenez votre premier enregistrement :



10.0.2.10

Pointeur (PTR)

intranet.gift.sa

Enregistrement PTR

Testez à nouveau la résolution inversée avec nslookup

```
C:\Users\Administrateur>nslookup 10.0.2.10
```

Serveur : UnKnown
Address: 10.0.2.15

Nom : intranet.gift.sa
Address: 10.0.2.10

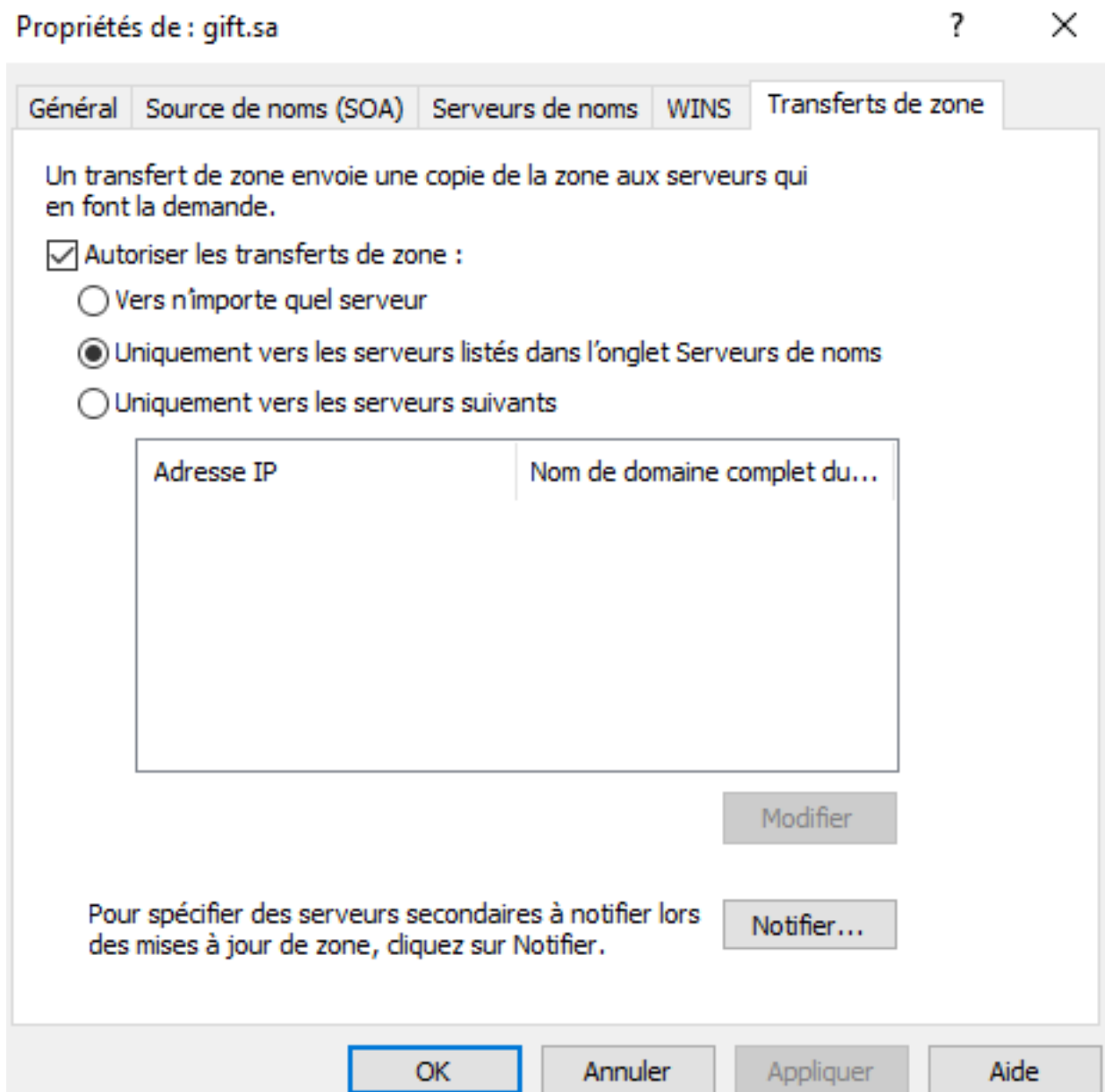
Voilà, vous avez maintenant un serveur DNS configuré pour simplifier la gestion du réseau de votre entreprise Gift S.A. Si vous souhaitez diagnostiquer le fonctionnement de votre serveur DNS, reprenez les méthodes et outils énoncés dans le chapitre précédent, ils restent valables pour tous les rôles et fonctionnalités !

Une dernière chose

Avant de vous laisser configurer d'autres rôles, il reste quelques configurations à mettre en œuvre. La première est **le transfert de zone**. Cette fonctionnalité est intéressante dans le cas où vous avez plusieurs serveurs pour une même zone (ce qui est une bonne chose), mais peut se montrer **dangereuse** si vous exposez votre serveur DNS publiquement.

Un transfert de zone contient tous les enregistrements d'une zone et permet donc de retrouver facilement toutes les adresses IP de vos équipements ; un attaquant pourrait s'en servir contre vous.

Pour cela, faites un clic droit sur le nom de votre zone, allez dans l'onglet "**Transfert de zone**" et refusez les transferts, ou listez les serveurs **de confiance** que vous allez **autoriser** à récupérer vos enregistrements ! Une bonne pratique consiste également à journaliser toutes les transactions DNS, mais cela vous le verrez en détail dans les cours concernant la surveillance d'un système :



Paramétrage des transferts de zone

Enfin, vous pouvez lancer le **BPA** de Microsoft sur ce rôle, pour vous assurer que votre configuration respecte les bonnes pratiques de Microsoft.

N'oubliez pas d'autoriser le port **UDP 53** sur votre pare-feu, sinon votre serveur DNS ne sera pas accessible sur le réseau ; rappelez-vous, vous avez activé le pare-feu pour bloquer tous les flux n'étant pas couverts par une règle de flux entrant !

Allez plus loin

- [RFC](#) régissant le fonctionnement du DNS.
- [Cours sur TCP/IP abordant le DNS](#).
- Liste des [différents types d'enregistrements DNS](#).
- Gestion du [cache DNS Microsoft](#).

En résumé

- Le rôle DNS de Windows Server permet de créer des **zones directes et inversées**.
- Le serveur DNS permet de **résoudre des noms en adresses IP et des adresses IP en noms**.
- Le **transfert de zone** doit être **restreint aux serveurs de confiance** uniquement.
- Un serveur DNS s'**interroge** à l'aide de la commande **nslookup** ou via les navigateurs web (entre autres).

Poursuivez votre apprentissage avec la mise en place d'un serveur de fichiers sous Windows Server, que nous allons voir dans le prochain chapitre !

Un des rôles les plus courants pour un serveur Windows est le serveur de fichiers. Grâce à ce rôle, vous allez pouvoir mettre à disposition en toute sécurité des fichiers sur votre réseau. Vous pourrez gérer **des droits d'accès** (lecture, écriture, modification...). Fournir ce type de rôle dans un réseau permet de **centraliser le point de stockage** des fichiers, facilitant ainsi la sauvegarde, la restauration, et permettant à plusieurs personnes de travailler ensemble sur un même fichier.

Rappelez-vous les fondamentaux du partage de fichiers

Pour qu'un fichier soit accessible sur votre réseau, un protocole de communication spécifique à l'échange de fichiers doit être utilisé. Sous Linux, il s'agit majoritairement du **NFS** (Network File System). Sous Windows, il est possible d'utiliser ce protocole, mais il n'est pas aussi bien intégré au système que l'est le protocole **SMB**, aussi appelé **CIFS**. **SMB** pour **Server Message Block** et **CIFS** pour **Common Internet File System**.

Ce protocole se caractérise par un client natif intégré à Microsoft Windows et un serveur que vous allez installer et configurer. Il se base sur **NTFS** pour la gestion des droits d'accès et les partages sont accessibles via un chemin universel (UNC – Universal Naming Convention) du type `\serveur\partage`.

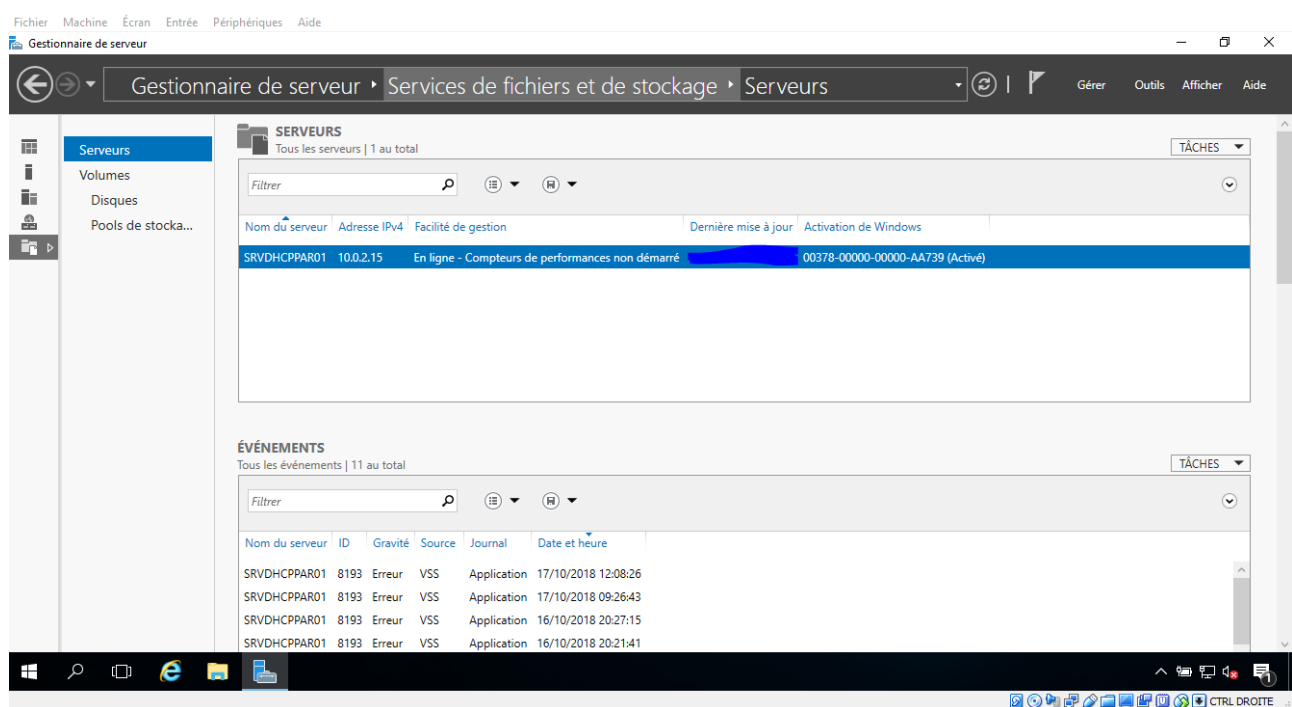
Si SMB peut vous faire penser à **SAMBA** (souvent rencontré sous Linux), c'est totalement normal, SAMBA est une implémentation open source du protocole propriétaire SMB de Microsoft. Vous pourrez donc partager vos fichiers via SMB et y avoir accès sur vos clients Linux.

Ceci étant dit, je vous propose d'entrer dans le vif du sujet !

Installez le rôle Serveur de fichiers

Attention une erreur s'est glissée dans la vidéo. Dans la liste des disques présents sur le serveur, les 2 nouveaux disques ajoutés sur le serveur devraient être de type USB. Or la vidéo montre que l'un d'eux est de type SATA.

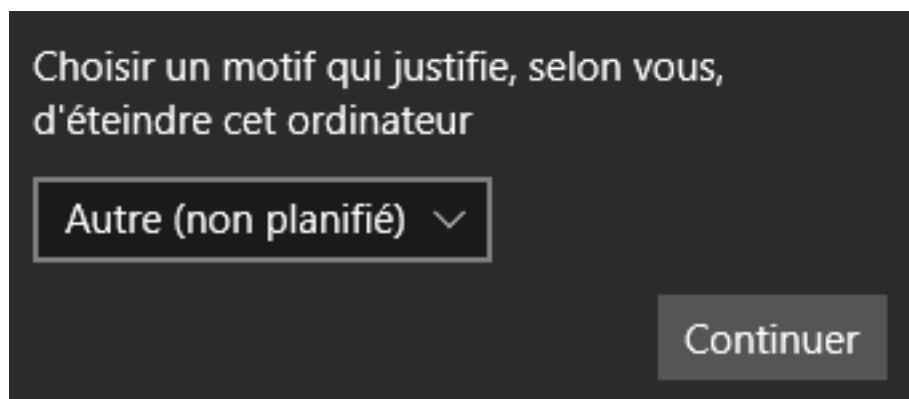
Sur votre **gestionnaire de serveurs**, vous avez sûrement observé la présence d'un rôle dont nous n'avions pas parlé, alors qu'il était déjà installé : le rôle Serveur de fichiers et de stockage :



Rôle Serveur de fichiers et de stockage installé par défaut

En effet, pour **stocker des fichiers**, il convient de **gérer le stockage**. Le mieux étant de mettre en œuvre un disque dédié à cet effet (ou plusieurs). Je vous propose donc de créer deux disques de 10 Gio sur votre machine virtuelle.

Pour cela, éteignez votre machine virtuelle et rendez-vous sur le menu de VirtualBox dans l'option "**Machine**", puis sélectionnez "**Paramètres**". Au passage, vous avez vu que Windows vous demande un motif pour l'arrêt de votre serveur :

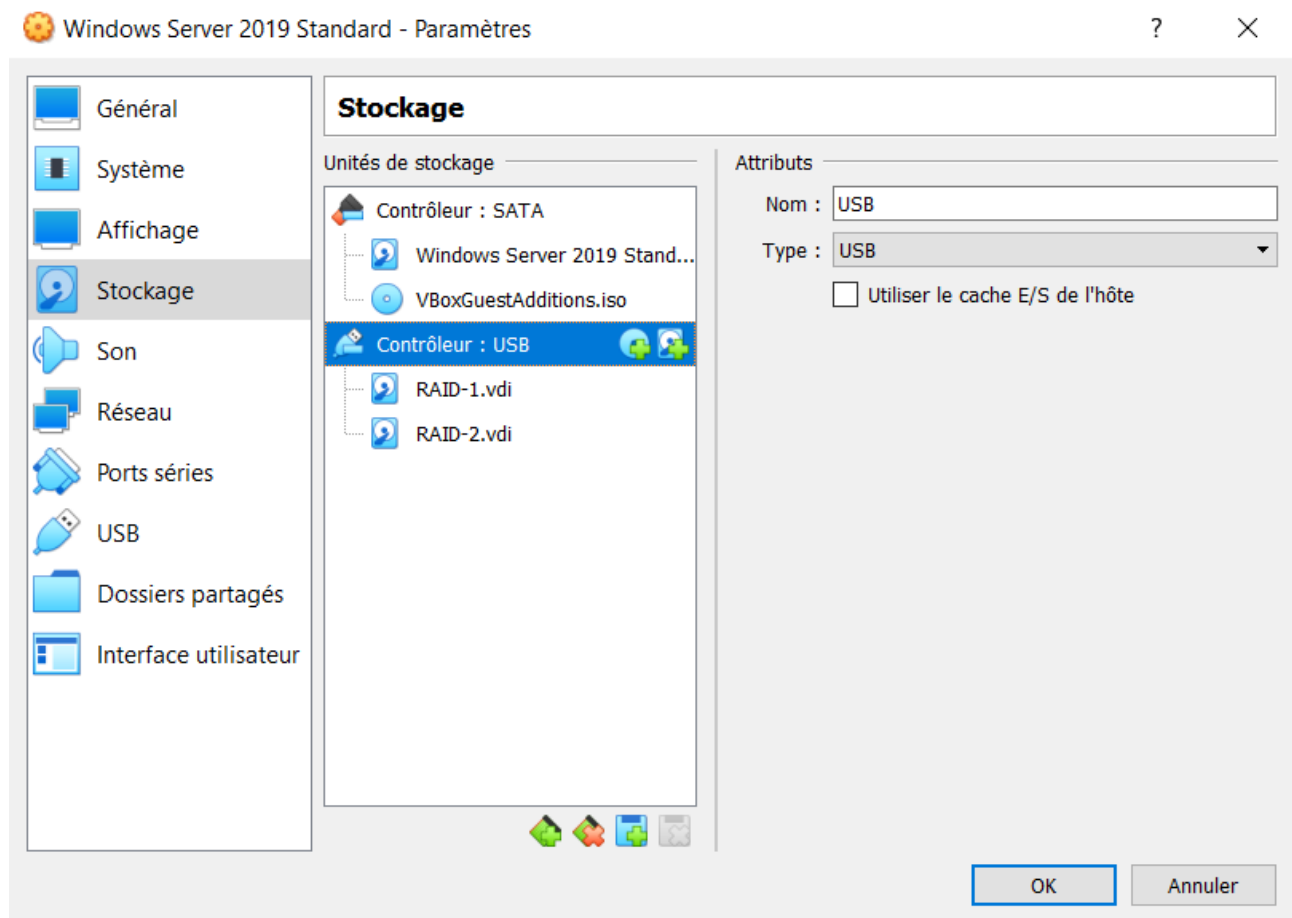


Motif d'arrêt et redémarrage d'un serveur

Cela permet d'identifier la raison de l'arrêt. En effet, si vous arrêtez votre serveur, ses rôles, fonctionnalités et services deviennent indisponibles. Il convient alors de s'assurer que cela est dû à une maintenance programmée ou à un événement non planifié. Cela permettra d'identifier clairement cet arrêt comme étant **programmé** et **légitime**, et donc de basculer ce temps d'indisponibilité dans les temps de maintenance.

Vous en saurez plus [dans le cours Supervision](#). Je vous propose donc de choisir le motif "**Système d'exploitation : reconfiguration (planifiée)**".

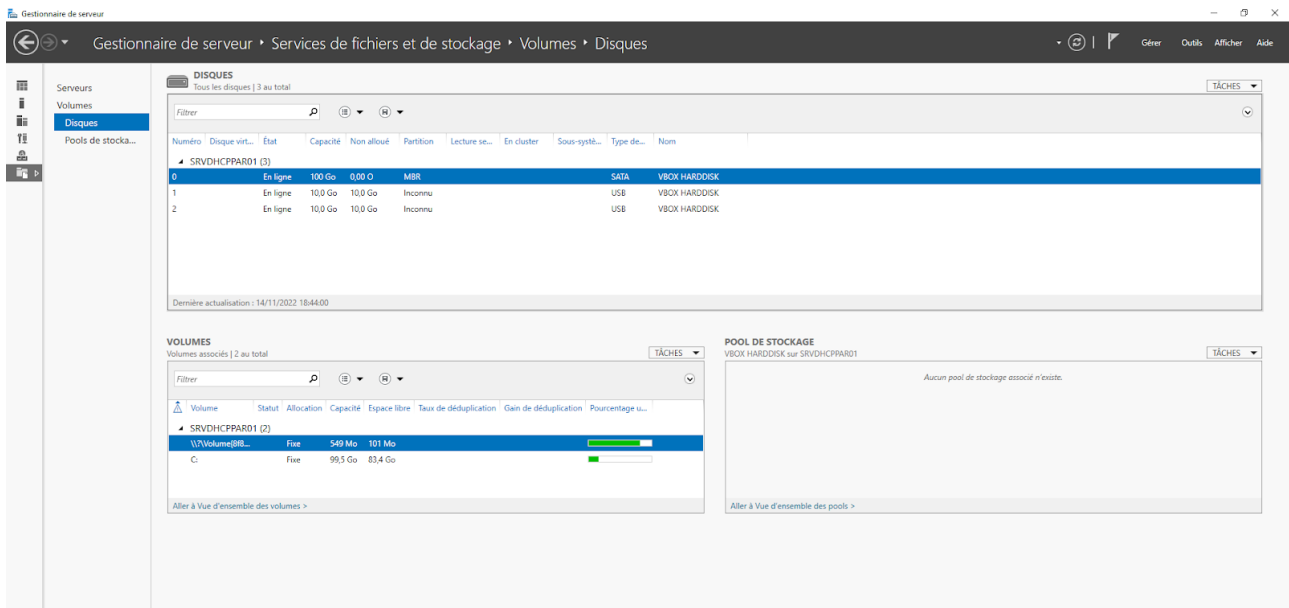
Rendez-vous dans la section “**Stockage**”, et sur un nouveau contrôleur USB ajoutez deux nouveaux disques :



Ajout de deux disques virtuels RAID_1.vdi et RAID_2.vdi à votre serveur

Un bug lié à Virtualbox empêche la création d'un pool de stockage avec 2 disques SATA. Si vous voulez pouvoir créer un pool de stockage vous devez absolument utiliser 2 nouveaux disques rattachés à un contrôleur USB, comme c'est le cas dans la capture d'écran ci-dessus.

Redémarrez ensuite votre serveur et rendez-vous à nouveau dans l'espace **Serveur de fichiers et de stockage** ; vous devriez voir les deux disques nouvellement installés dans la partie "Disques" :



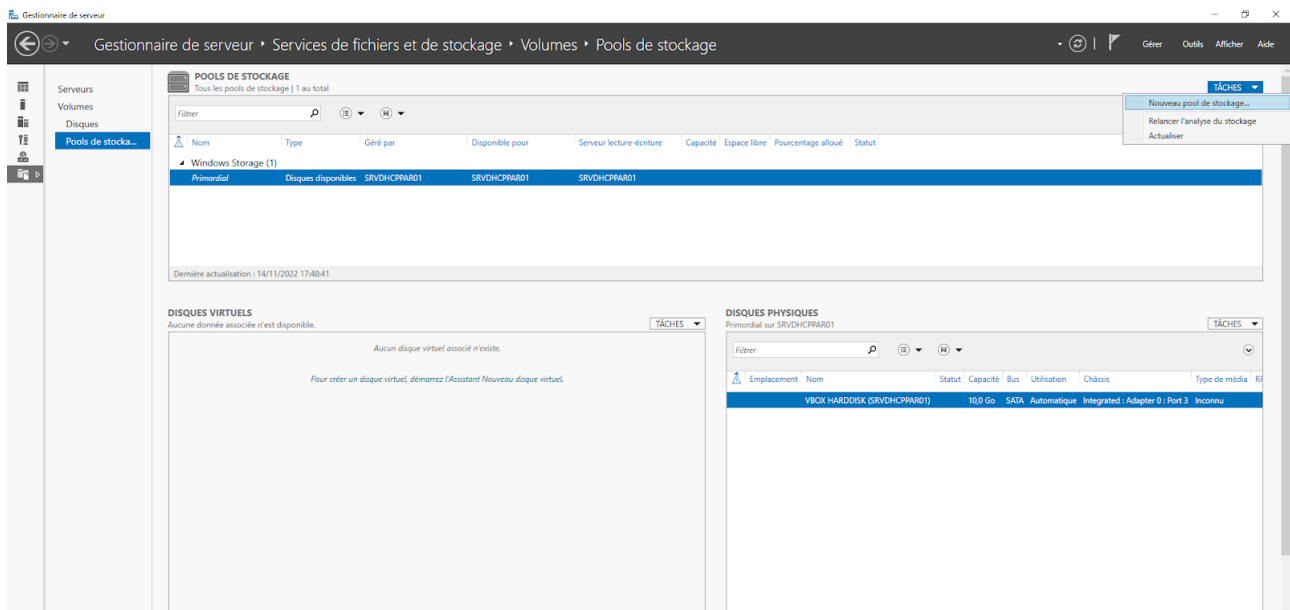
Deux nouveaux disques

La direction de Gift S.A. vous demande de mettre en place un partage réseau, afin de travailler à plusieurs sur le nouveau prototype d'un objet révolutionnaire. Il convient donc de sécuriser ces données. Pour cela, je vous propose de mettre en œuvre un **RAID** logiciel.

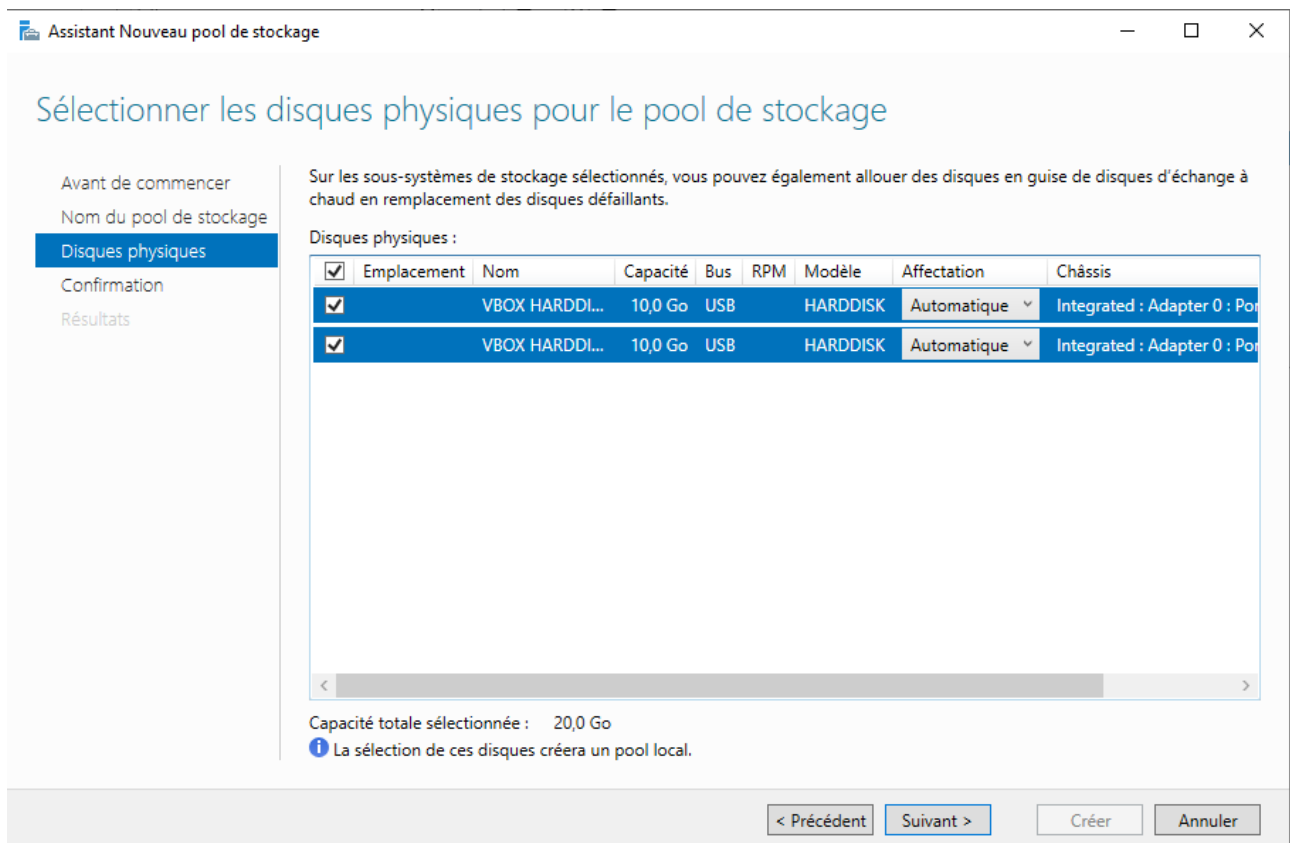
Je vous invite, si vous ne l'avez pas déjà fait, à suivre le cours [Montez un serveur de fichiers sous Linux](#), pour comprendre comment fonctionne le RAID sous Linux, dont la logique est presque la même que sous Windows Server :

- Vous devez dans un premier temps **initialiser vos disques physiques** en faisant un clic droit sur les disques dans la fenêtre actuelle ;
- Puis **créez un pool de stockage** dans la partie correspondante. Ce pool va permettre de regrouper les disques et de créer des disques virtuels qui pourront avoir des capacités de redondance (miroir) ou de parité (intégrité des données), afin d'augmenter la sécurité ;
- Puis **créez un disque virtuel**.

Hormis la première étape, toutes les étapes se font dans la partie "**Pool de stockage**" :



Création d'un pool de stockage et d'un disque virtuel.
Sélectionnez ensuite vos 2 disques de 10Go :



Création du pool de stockage avec les 2 disques durs

POOLS DE STOCKAGE								
Tous les pools de stockage 1 au total								
Filtrer								
Nom	Type	Géré par	Disponible pour	Serveur lecture-écriture	Capacité	Espace libre	Pourcentage alloué	Statut
Windows Storage (1)								
Pool1	Pool de stockage	SRVDHCPPAR01	SRVDHCPPAR01	SRVDHCPPAR01	19,0 Go	18,5 Go		

Dernière actualisation : 14/11/2022 18:44:54

Nouveau pool de stockage Pool1

Sélectionnez ensuite votre pool de stockage et créez un disque virtuel. Pour le cas de Gift S.A., je vous propose de partir sur un **miroir simple** qui utilisera les deux disques pour stocker les données (les fichiers seront écrits en simultané sur les deux disques, la perte d'un disque est transparente !).

Assistant Nouveau disque virtuel

Sélectionner la disposition de stockage

Avant de commencer
Nom du disque dur virtuel
Reconnaissance des boîti...
Disposition du stockage
Approvisionnement
Taille
Confirmation
Résultats

Disposition :
Simple
Mirror
Parity

Description :
Les données sont agrégées par bandes sur des disques physiques, créant ainsi deux ou trois copies de vos données. Ceci augmente la fiabilité mais réduit la capacité. Pour vous protéger en cas de défaillance d'un seul disque, utilisez au moins deux disques (trois si vous utilisez un cluster) ; pour vous protéger en cas de défaillances simultanées de deux disques, utilisez au moins cinq disques.

< Précédent
Suivant >
Créer
Annuler

Création d'un disque virtuel

Ensuite, vous devrez choisir le mode d'approvisionnement de l'espace. Pour cela, deux options existent, **fin** ("thin" en anglais) et **fixe**. Dans ce dernier cas, fixe, l'espace total du volume est proposé ; dans le cas de l'approvisionnement fin, vous fixez la taille.

L'avantage est qu'il est **possible de fournir un espace réduit** puis de pouvoir l'**augmenter** par la suite. Il est également possible d'**afficher plus d'espace** que réellement disponible physiquement.

Spécifier le type d'approvisionnement

Avant de commencer

Nom du disque dur virtuel

Reconnaissance des boîti...

Disposition du stockage

Approvisionnement

Taille

Confirmation

Résultats

Type de mise en service :

☒ Fin

Le volume utilise de l'espace nécessaire sur le pool de stockage, pouvant atteindre la capacité totale du volume.

☐ Fixe

Le volume utilise de l'espace du pool de stockage dont la taille est identique à celle du volume.

< Précédent

Suivant >

Créer

Annuler

Approvisionnement de l'espace disque

Finalisez la création de ce disque, et **créez le volume** qui accueillera vos données et se présentera avec une lettre de lecteur, ainsi qu'un système de fichiers (NTFS par défaut). La fenêtre de création de volume se lance normalement automatiquement après avoir créé le disque virtuel.

Assistant Nouveau volume

Sélectionner le serveur et le disque

Avant de commencer

Serveur et disque

Taille

Lettre de lecteur ou dossier

Paramètres du système d...

Confirmation

Résultats

Serveur :

Fournir à	Statut	Rôle du cluster	Destination
SRVDHCPPAR01	En ligne	Non-cluster	Local

Actualiser Relancer l'analyse

Disque :

Disque	Disque virtuel	Capacité	Espace libre	Sous-système
Disque 1		10,0 Go	10,0 Go	
Disque 2		10,0 Go	10,0 Go	
Disque 3	DisqueVirtuel	1,00 To	1 024 Go	Windows Storage

< Précédent Suivant > Créer Annuler

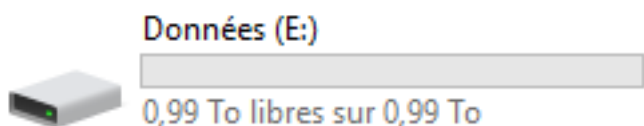
Création du volume associé au disque virtuel

Pour ma part, j'ai mis en œuvre **un disque virtuel** en miroir en approvisionnement fin de 1 To (oui, à partir de mes deux disques de 10Go).

DISQUES VIRTUELS							
PoolDeStockage sur SRVDHCPPAR01							
TÂCHES							
Filtrer							
Nom	Statut	Disposition	Approvisionnement	Capacité	Alloué	Volume	
DisqueVirtuel		Mirror	Fin	1,00 To	1,00 Go	E:	

DISQUES PHYSIQUES							
PoolDeStockage sur SRVDHCPPAR01							
TÂCHES							
Filtrer							
Emplacement	Nom	Statut	Capacité	Bus	Utilisé		
	VBOX HARDDISK (SRVDHCPPAR01)		10,0 Go	SATA	Automat		
	VBOX HARDDISK (SRVDHCPPAR01)		10,0 Go	SATA	Automat		

Nouveau disque de données de 1 To en miroir sur les deux disques physiques de 10 Gio.

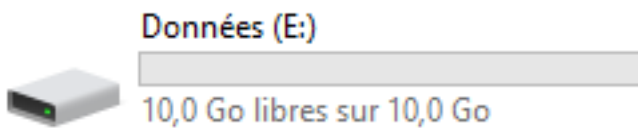


Volume associé au disque virtuel de 1 Tio

L'approvisionnement fin est pratique pour anticiper les besoins. Il autorise une certaine souplesse dans l'approvisionnement d'espace.

Sachez que vous aurez de toute façon une alerte dès que vous aurez atteint 70 % de l'espace physique réel. Il vous faudra à ce moment-là ajouter de nouveaux disques physiques afin de fournir le stockage nécessaire.

Je vous propose donc de rester raisonnable, avec 10 Gio de disque virtuel en miroir :

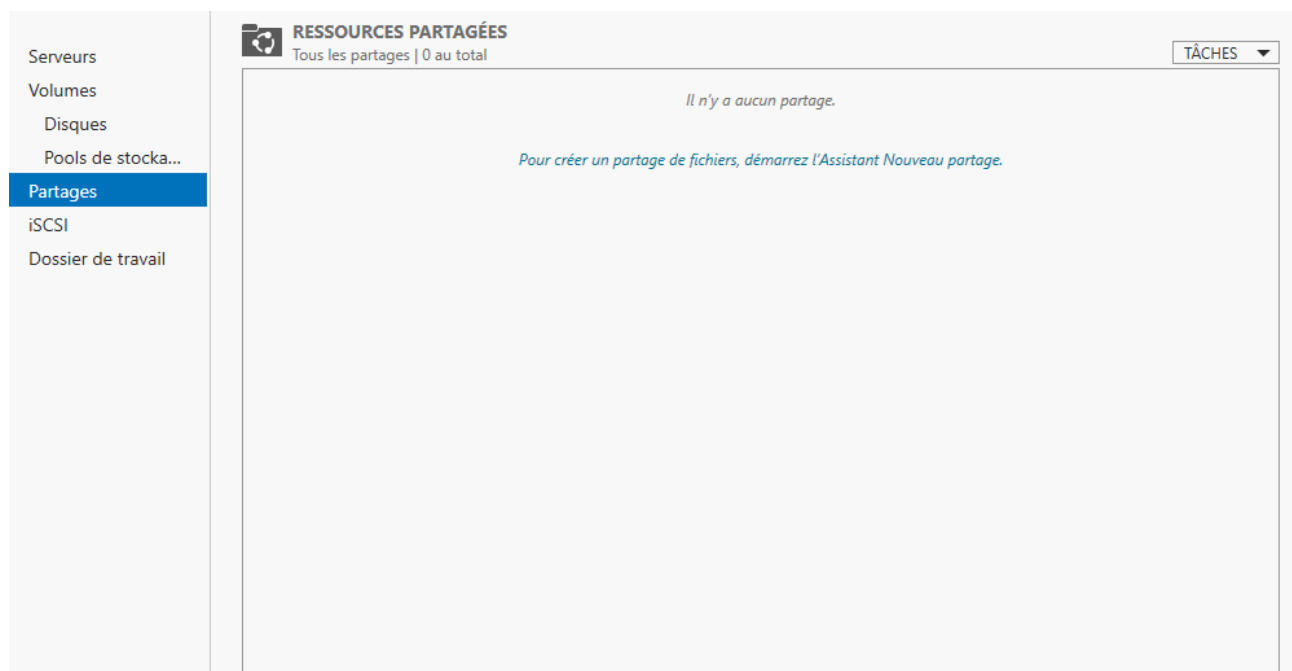


Volume de données avec 10 Gio en miroir sur les deux disques physiques

Je vous propose d'en rester là pour la gestion du stockage, le fonctionnement étant globalement le même que sous Linux.

Créez votre premier partage

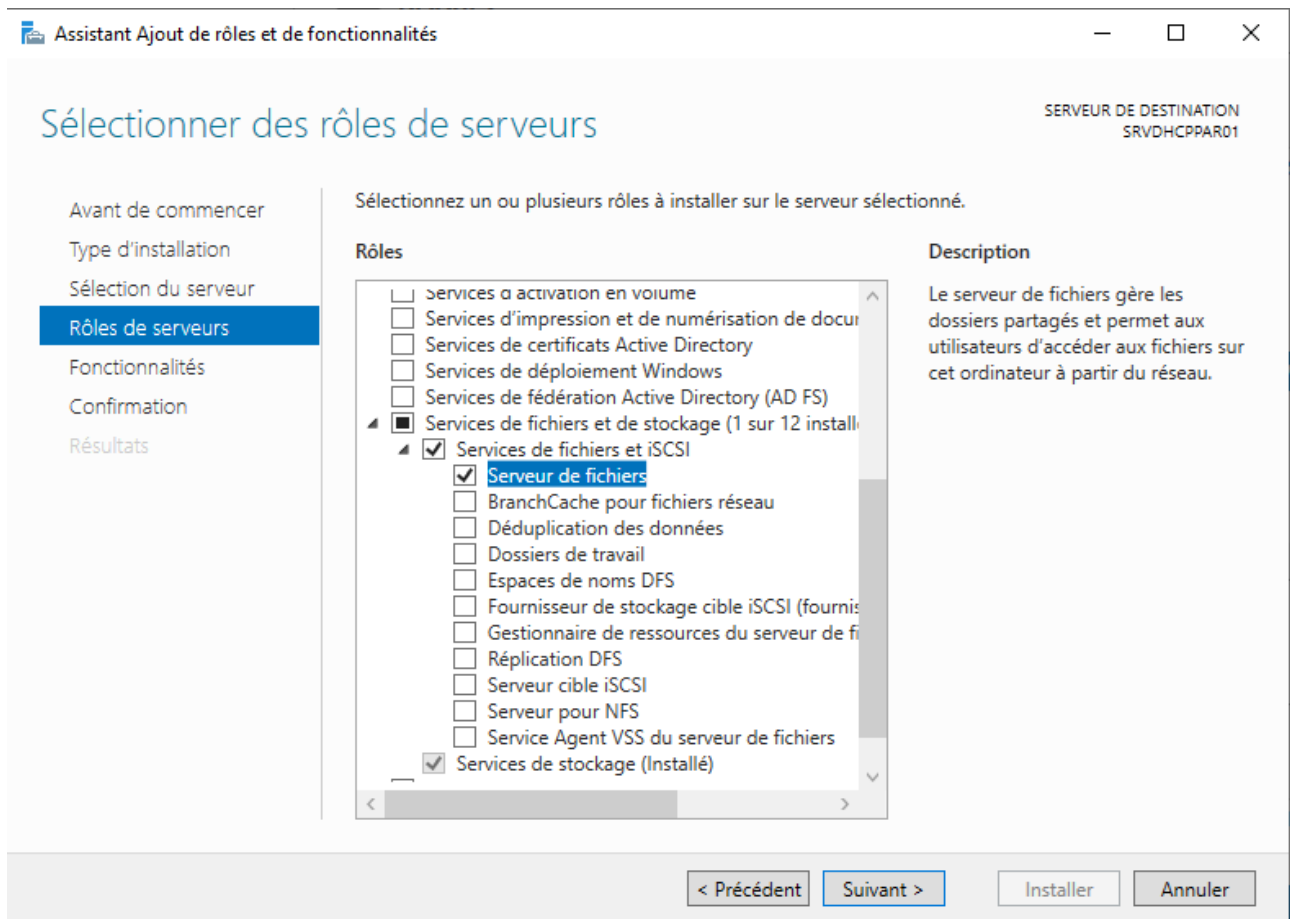
Maintenant que vous avez votre support pour vos données, il vous faut un dossier pour stocker les différents fichiers. Rendez-vous dans la partie “**Partages**”, puis dans l’encart “**Ressources partagées**” :



Ressources partagées

En cliquant sur le lien, vous aurez la possibilité de créer un nouveau partage.

Si vous ne voyez pas la partie "Partages" sur la gauche, c'est sans doute que le rôle Serveur de fichiers n'est pas installé. Pensez donc à le faire :



Sélection du rôle Serveur de fichiers

Lors de la création du partage, vous avez le choix entre 5 propositions via l'assistant de création de partages :

Sélectionner le profil de ce partage

Sélectionner un profil

Emplacement du partage
 Nom de partage
 Autres paramètres
 Autorisations
 Confirmation
 Résultats

Profil du partage de fichiers :

Partage SMB - Rapide
 Partage SMB - Avancé
 Partage SMB - Applications
 Partage NFS - Rapide
 Partage NFS - Avancé

Description :

Ce profil de base constitue le moyen le plus rapide de créer un partage de fichiers SMB, généralement utilisé pour partager des fichiers avec des ordinateurs Windows.

- Convient au partage général de fichiers.
- Les options avancées peuvent être configurées ultérieurement à l'aide de la boîte de dialogue Propriétés.

< Précédent

Suivant >

Créer

Annuler

Choix du mode de partage

- **SMB rapide** : le plus simple, vous fournissez un partage sur votre réseau via SMB ;
- **SMB avancé** : permet d'aller plus loin que le précédent en gérant des quotas et des droits avancés ;
- **SMB Applications** : utilisé pour Hyper-V et les bases de données ou autres serveurs ;
- **NFS rapide** : identique à SMB simple mais via NFS (avec donc une meilleure compatibilité avec Linux) ;
- **NFS avancé** : idem SMB avancé.

Je vous propose de rester sur SMB rapide. Sélectionnez votre nouveau volume de 1To, puis il vous est ensuite demandé le chemin d'accès et le nom du partage. De cette manière, le répertoire partagé sera accessible via le chemin UNC (Universal Naming Convention) suivant : \nom_serveur\nom_partage. Je vous propose d'appeler votre partage "**Sensible**".

Vous remarquerez alors que Windows créera ce répertoire dans un répertoire "**Shares**" qui accueillera tous les partages de ce volume. De même, l'accès via un chemin UNC est affiché \SRVDHCPPAR01\Sensible .

Je vous le redis, pour être sûr que vous vous en rappeliez dans votre pratique pro, le nommage du serveur est vraiment important.

Enfin, il vous sera proposé de configurer les paramètres de votre partage avec une option cochée par défaut : **Autoriser la mise en cache du partage**.

Il s'agit là d'une nouvelle fonctionnalité depuis Windows Server 2012, qui permet de synchroniser le partage sur un poste et de vous fournir un accès à vos données, même si le serveur n'est plus accessible.

L'activation de l'énumération basée sur l'accès permet de n'afficher dans l'explorer Windows que les partages auxquels l'utilisateur a accès. C'est une option intéressante qui permet de masquer un partage sensible aux utilisateurs ne disposant d'aucun droit sur les données en question ; je vous propose d'activer cette option.

Assistant Nouveau partage

Configurer les paramètres de partage

- Sélectionner un profil
- Emplacement du partage
- Nom de partage
- Autres paramètres**
- Autorisations
- Confirmation
- Résultats

☒ Activer l'énumération basée sur l'accès
L'énumération basée sur l'accès n'affiche que les fichiers et les dossiers dont un utilisateur possède les autorisations d'accès. S'il ne bénéficie pas d'autorisations en lecture (ou équivalentes) sur un dossier, Windows cache alors ce dernier de l'utilisateur.

☒ Autoriser la mise en cache du partage
La mise en cache met le contenu du partage à la disposition des utilisateurs hors connexion. Si la fonctionnalité BranchCache du service de rôle Fichiers réseau est installée, vous pouvez activer BranchCache sur le partage.

☐ Activer le cache de filiale (BranchCache) sur le partage de fichiers
BranchCache permet aux ordinateurs d'une succursale de mettre en cache les fichiers téléchargés à partir de ce partage, puis de les rendre disponibles en toute sécurité pour les autres ordinateurs de la succursale.

☒ Chiffrer l'accès aux données
Lorsqu'il est activé, l'accès distant aux fichiers de ce partage est chiffré. Cela a pour effet de sécuriser les données contre tout accès non autorisé lors de leur transfert vers ou depuis le partage. Si cette case à cocher est activée et grisée, cela signifie qu'un administrateur a activé le chiffrement pour l'ensemble du serveur.

< Précédent Suivant > Créer Annuler

Paramètres de partage

Enfin, la dernière et peut-être la plus importante, la possibilité de chiffrer l'accès aux données.

Il ne s'agit que du chiffrement de l'accès aux données et non du chiffrement des données elles-mêmes.

Ensuite, vous devez choisir des utilisateurs (ou mieux, des groupes) qui pourront disposer d'accès spécifiques en fonction de leurs besoins, par exemple pour le **"Principal"** utilisateur authentifié, les droits peuvent être **"Lecture seule"** :

Autorisations pour Sensible

Principal : Utilisateurs authentifiés [Sélectionnez un principal](#)

Type : Autoriser

S'applique à : Ce dossier, les sous-dossiers et les fichiers

Autorisations de base :

- ☐ Contrôle total
- ☐ Modification
- ☐ Lecture et exécution
- ☐ Affichage du contenu du dossier
- ☒ Lecture
- ☐ Écriture
- ☐ Autorisations spéciales

[Afficher les autorisations avancées](#)

☐ Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur

[Effacer tout](#)

[OK](#) [Annuler](#)

Autorisations pour Sensible

Une fois que vous avez terminé avec l'affectation des droits (qui est beaucoup plus simple, couplée à un Active Directory), vous pouvez **valider**. Vous avez alors un récapitulatif des paramètres choisis :

Assistant Nouveau partage

Confirmer les sélections

Sélectionner un profil

Emplacement du partage

Nom de partage

Autres paramètres

Autorisations

Confirmation

Résultats

Vérifiez que les paramètres suivants sont corrects, puis cliquez sur Créer.

EMPLACEMENT DU PARTAGE	
Serveur :	SRVDHCPPAR01
Rôle du cluster :	Non-cluster
Chemin d'accès local :	E:\Shares\Sensible
PROPRIÉTÉS DU PARTAGE	
Nom du partage :	Sensible
Protocole :	SMB
Énumération basée sur l'accès :	Activé
Mise en cache :	Activé
BranchCache :	Désactivé
Chiffrer les données :	Activé

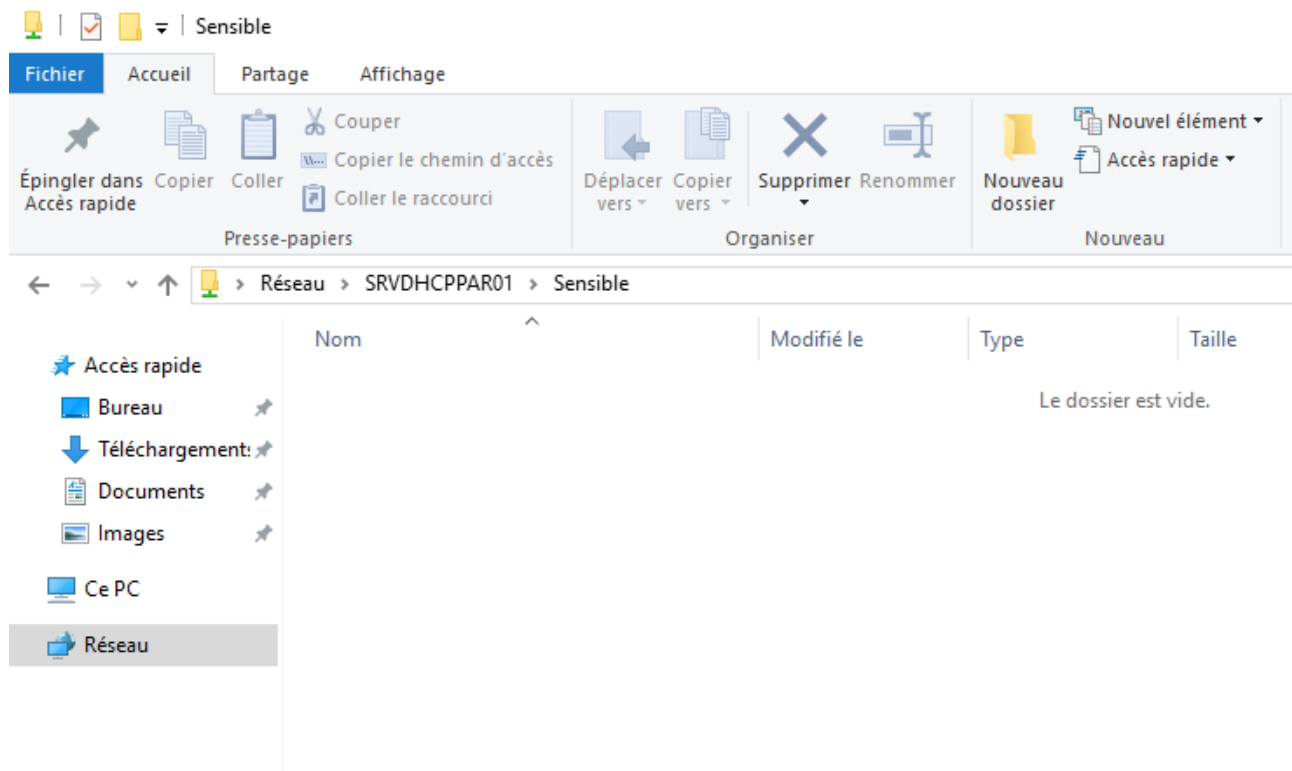
[< Précédent](#) [Suivant >](#) [Créer](#) [Annuler](#)

Paramètres du partage

Et voilà, votre partage est disponible via `\\SRVDHCPPAR01\Sensible` (à modifier avec le nom de votre serveur).

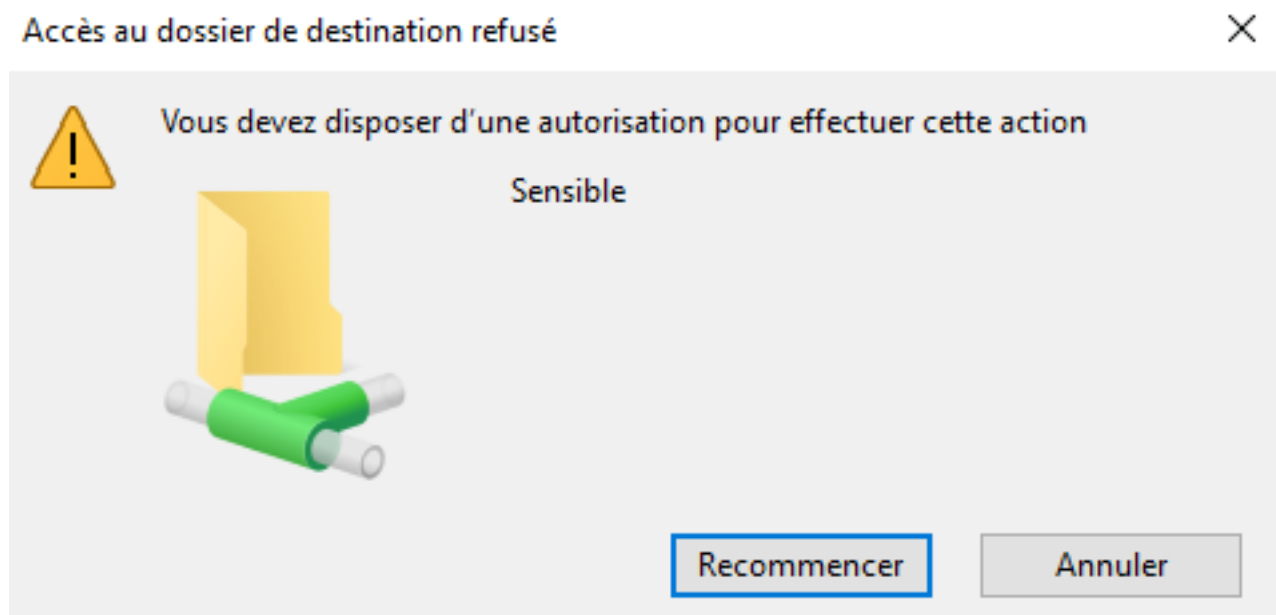
Accédez à votre partage

Pour cela, rien de plus simple sous Windows, un client SMB est intégré à l'explorer, il suffit d'entrer le chemin UNC du partage dans la barre d'adresse, et Windows vous en affiche le contenu :



Accès au partage Sensible

Par défaut, l'administrateur n'est pas obligatoirement libre de gérer les fichiers, il peut ne pas avoir accès aux données de **"Sensible"** s'il n'en a pas le besoin. Il pourra tout de même effectuer ses tâches d'administration sans pouvoir voir le contenu des données !



Accès refusé pour l'administrateur local sur le dossier "Sensible"

Il ne vous reste plus qu'à **autoriser les flux** sur votre pare-feu pour fournir l'accès à votre serveur de fichiers. Vous utilisez le protocole SMB, il faut donc ouvrir le port 445/TCP à destination de votre serveur sur votre réseau.

Allez plus loin

Je vous invite à regarder de près les possibilités de mise en cluster. Cela vous permettra d'avoir plusieurs serveurs pour héberger votre partage, ainsi vous augmenterez la disponibilité de vos données.

Vous trouverez également des informations utiles dans le cours [Installez et déployez Windows 10](#) sur les espaces de stockage, qui fonctionnent globalement de la même façon sous Windows 10.

En résumé

- Le **serveur de fichiers** est un **rôle par défaut** qui n'est pas complètement installé ; il faut terminer l'ajout de certaines fonctionnalités afin de pouvoir mettre en place un partage.
- Il existe **deux grands types de protocoles** disponibles, **SMB** et **NFS**, l'un propriétaire Microsoft, l'autre plutôt orienté vers le monde Unix, avec notamment une implémentation sous Linux et MacOS.
- Il est possible de **chiffrer l'accès aux données** via SMB.
- Windows Server met en œuvre **une virtualisation des disques** afin de faciliter la **sécurisation en miroir ou la parité**, pour garantir la fiabilité d'un partage.

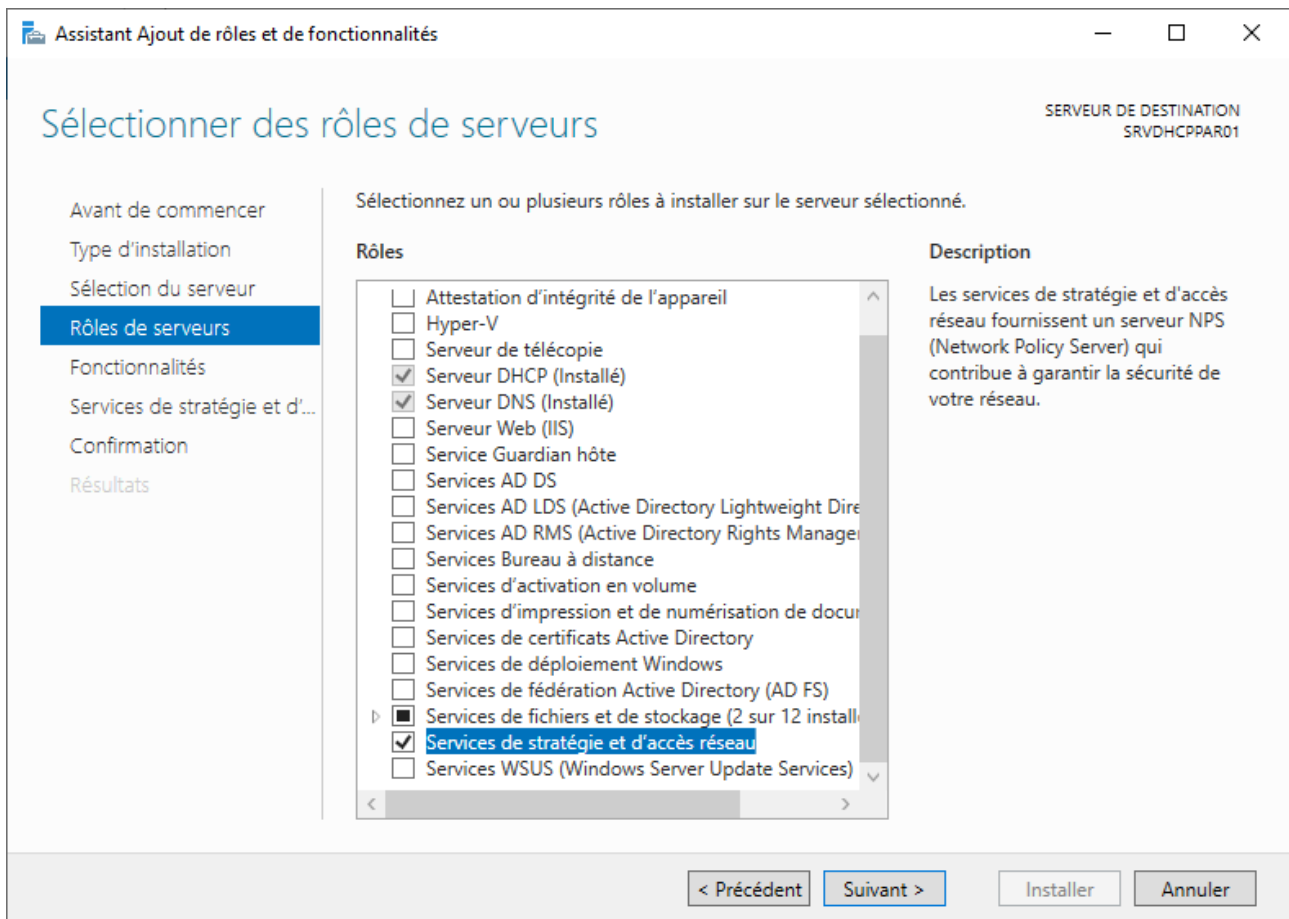
Dans le prochain et dernier chapitre de cette partie, vous découvrirez comment mettre en place le service d'accès réseau sur votre serveur et comprendrez son intérêt.

Dans ce dernier chapitre, je vous propose de **mettre en œuvre un rôle** trop souvent oublié : le **contrôle d'accès au réseau**. Microsoft propose ce rôle, afin de vous permettre de maîtriser quels équipements peuvent accéder à vos ressources en réseau.

Imaginez que votre direction vous demande de sécuriser l'accès au partage, mais avec un accès Wi-Fi (vulnérable de conception). Eh bien, grâce à ce rôle, vous allez pouvoir maîtriser votre Wi-Fi afin de le fournir de façon maîtrisée à votre direction !

Installez les services de stratégie et d'accès réseau

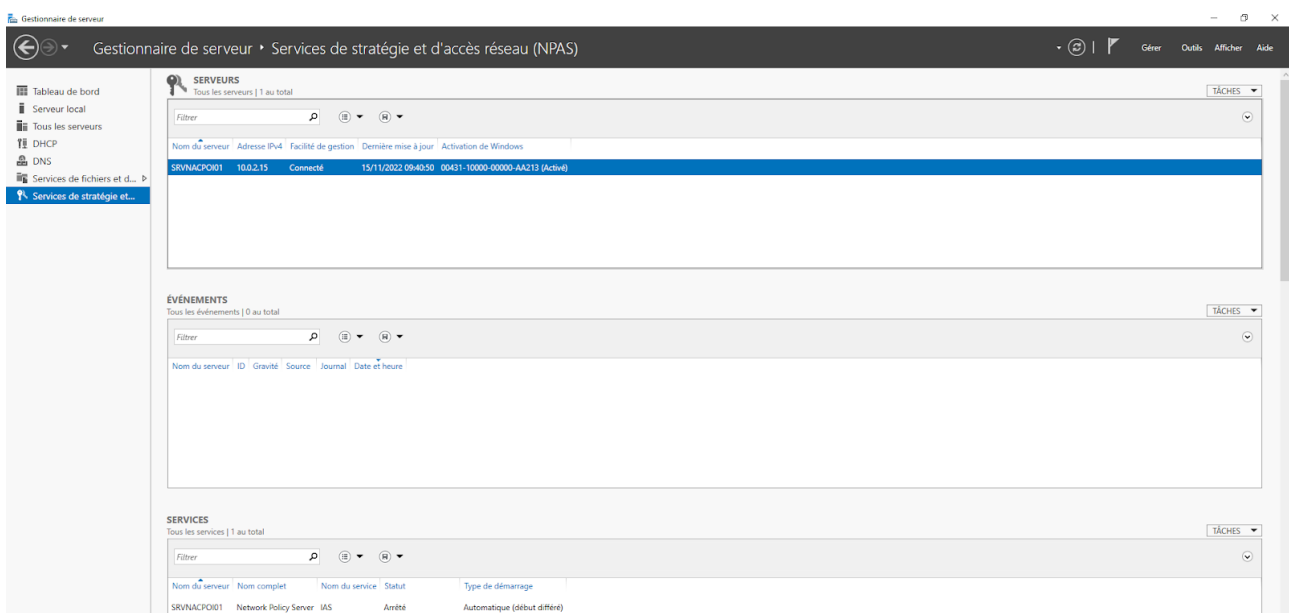
Le rôle de serveur d'accès au réseau s'installe via les **services de stratégie et d'accès au réseau**.



Ajout des services de stratégie et d'accès réseau

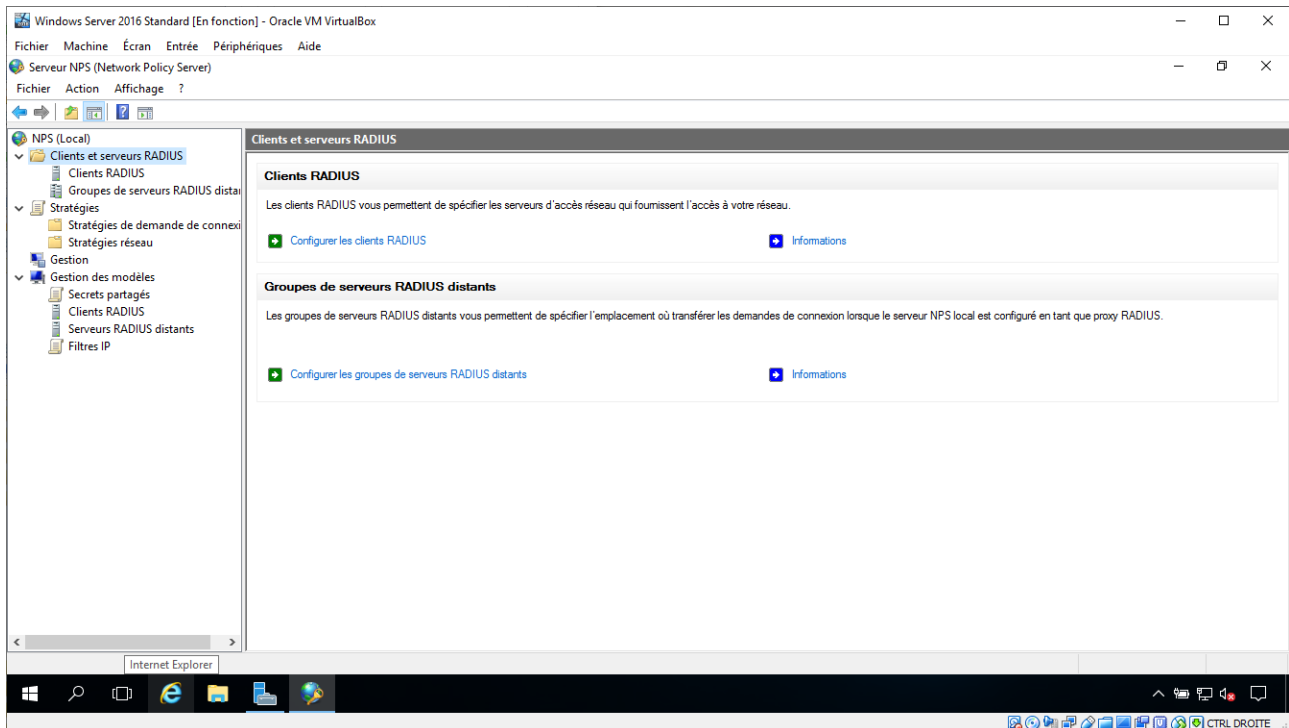
Dénommés **NPS** (*Network Policy Server*), ces services assurent le **contrôle d'accès** à votre réseau comme il vous est dit ; ce serveur agit comme un serveur **RADIUS** (*Remote Authentication Dial-in User Service*) qui est un protocole permettant justement de vérifier l'identité d'un client, ses droits, et de lui fournir un service (tel que l'accès à un réseau), s'il dispose de tels droits.

NPS peut aussi servir de proxy RADIUS, mais je vous propose de rester sur sa fonction première : le serveur RADIUS.



Services de stratégie et d'accès au réseau installé

Installez ce rôle (en toute logique, vous ne devriez pas avoir besoin de redémarrer votre serveur). Sélectionnez votre serveur. Ici j'ai nommé mon serveur SRVNACPOI01 : c'est un serveur SRV, pour le contrôle d'accès au réseau NAC (*Network Access Control*), et il est le premier (01) serveur situé à Poitiers (POI). Faites un clic droit sur la ligne correspondant à votre serveur et sélectionnez **"Serveur NPS"** :



Console de gestion du serveur NPS

Petite information supplémentaire sur les éditions de Windows Server concernant RADIUS. La version Standard de Windows Server permet de gérer **"seulement" 50 clients RADIUS**, alors que la version Datacenter ne restreint pas le nombre de clients ; cela permet de préciser vos critères de choix d'une édition de Windows Server, et donc de dimensionner votre réseau avec précision.

Avant de vous lancer dans l'implémentation de votre contrôle d'accès au réseau, il vous faut maîtriser la **terminologie** et le **fonctionnement** de **RADIUS** (commun à tous les protocoles d'accès).

Rappelez-vous les fondamentaux du contrôle d'accès

Avant tout, il faut identifier les clients. Il faudra donc avoir un client prenant en charge le protocole RADIUS ; l'avantage ici, c'est **l'utilisation des technologies Microsoft** : vous retrouverez des clients natifs pour chaque rôle de serveur.

C'est donc le cas ici, un poste Windows 10 Professionnel sera donc en mesure d'interroger un serveur RADIUS. À ceci près que le poste client ne sera pas le client RADIUS. En effet, il ne va pas directement demander au serveur d'accès s'il peut accéder au réseau. Pour cela, il devra s'appuyer sur un tiers qui, lui, consultera le serveur RADIUS.

Voici un **schéma de fonctionnement** du rôle d'accès au réseau de Microsoft.

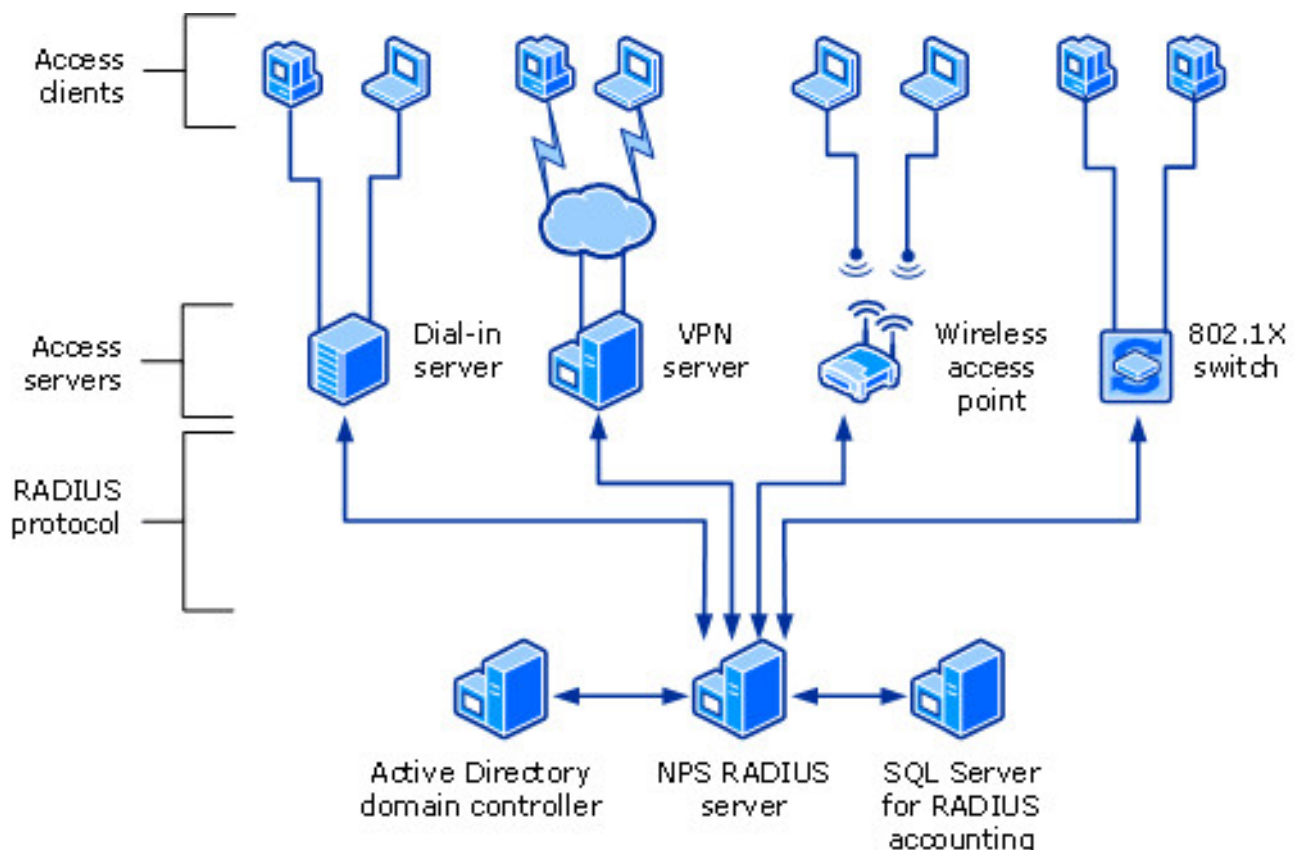


Illustration (issue du site de Microsoft) concernant le fonctionnement de RADIUS au travers du serveur NPS de Windows Server

Le poste client sera donc un **suppléant** (dans la terminologie RADIUS). Le client RADIUS est alors l'équipement qui fournira l'accès au réseau. Cela peut être un commutateur, un point d'accès Wi-Fi ou un serveur d'accès distant ou VPN.

Comme je ne souhaite pas que vous soyez obligé d'investir dans du matériel, je vous propose de comprendre le fonctionnement au travers, non pas de la mise en œuvre sous Windows, mais via **Packet Tracer**. Packet Tracer est un outil Cisco, gratuit, qui permet de comprendre rapidement le fonctionnement de RADIUS.

[Initiez-vous à Packet Tracer !](#)

Maquettez le contrôle d'accès au réseau

Lancez Packet Tracer et placez 4 équipements :

- Un serveur générique ;
- Un commutateur 2960 ;
- Un PC portable ;
- Un point d'accès Wi-Fi WRT300N.

Connectez votre serveur (FastEthernet0) au commutateur (n'importe quel port), puis le port "**Internet**" du point d'accès à ce même commutateur.

Il reste maintenant quelques étapes à mettre en œuvre :

- **Configurer la couche IP** sur l'AP (point d'accès Wi-Fi) et sur le serveur ;
- **Configurer la partie Serveur RADIUS** sur le serveur ;
- **Configurer le client RADIUS** sur le point d'accès ;
- **Mettre une carte Wi-Fi** sur le PC portable.

Commençons par le serveur, qui est le plus simple :

The screenshot shows the 'FastEthernet0' configuration window in Windows Server 2016 Std. The window has tabs for 'Physical', 'Config', 'Services', 'Desktop', and 'Custom Interface'. The 'Config' tab is active. On the left, there is a tree view with 'GLOBAL' (containing 'Settings' and 'Algorithm Settings') and 'INTERFACE' (containing 'FastEthernet0'). The main area shows the configuration for 'FastEthernet0'.

FastEthernet0 Configuration:

- Port Status:** ☒ On
- Bandwidth:** ☒ 100 Mbps ☐ 10 Mbps ☒ Auto
- Duplex:** ☐ Half Duplex ☒ Full Duplex ☒ Auto
- MAC Address:** 0001.970B.184D
- IP Configuration:**
 - ☐ DHCP
 - ☒ Static
 - IP Address:** 192.168.1.1
 - Subnet Mask:** 255.255.255.0
- IPv6 Configuration:**
 - ☐ DHCP
 - ☐ Auto Config
 - ☒ Static
 - IPv6 Address:** [Empty field]
 - Link Local Address:** FE80::201:97FF:FE0B:184D

Architecture RADIUS simulée

Puis par le point d'accès Wi-Fi en y insérant les configurations réseau ci-dessous :

Point d'accès Wifi

Physical Config GUI

GLOBAL

Settings

Algorithm Settings

INTERFACE

Internet

LAN

Wireless

Internet Settings

IP Configuration

☐ DHCP

☒ Static

☐ PPPoE

UserName

Password

Default Gateway

IP Address

Subnet Mask

DNS Server

192.168.1.2

255.255.255.0

Configuration IP du serveur

Maintenant que les configurations IP sont opérationnelles sur ces deux équipements, passez à la configuration du serveur et du client **RADIUS** :

La configuration du client RADIUS est très simple, il suffit de **spécifier l'adresse IP** du serveur RADIUS et de **définir un secret** (comme vous voulez sécuriser l'accès Wi-Fi, cela se passe dans la partie "Wireless") :

Point d'accès Wifi

Physical Config GUI

GLOBAL

Settings

Algorithm Settings

INTERFACE

Internet

LAN

Wireless

Wireless Settings

SSID: Default

Channel: 6

Authentication:

☐ Disabled ☐ WEP WEP Key:

☐ WPA-PSK ☐ WPA2-PSK PSK Pass Phrase:

☐ WPA ☒ WPA2

RADIUS Server Settings:

IP Address: 192.168.1.1

Shared Secret: secretRadius

Encryption Type: AES

Configuration du client RADIUS

Maintenant, passez à la configuration (très simplifiée dans ce simulateur) du serveur RADIUS, rendez-vous dans la partie **"Services"**, puis **AAA**.

Au passage, **AAA** signifie *Authentication, Authorization, Accounting/Auditing*. Ce protocole est la base du protocole RADIUS !

Entrez tout d'abord les informations sur le client RADIUS : un **nom**, son **IP** et le **secret** que vous avez entré sur le client. Puis définissez des utilisateurs dans la partie "User Setup" :

Server0

PhysicalConfigServicesDesktopProgrammingAttributes

SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP

AAA
Service ☐ On ☒ Off Radius Port 1645
Network Configuration
Client Name Wifi_AP Client IP 192.168.1.2
Secret secretRadius ServerType Radius

	Client Name	Client IP	Server Type	Key
1	Wifi_AP	192.168.1.2	Radius	secretRadius

Add
Save
Remove

User Setup
Username openclassrooms Password openclassrooms

	Username	Password
1	openclassrooms	openclassrooms

Add
Save
Remove

☐ Top

Configuration du serveur RADIUS

Passez ensuite à la configuration du supplican (à savoir le PC portable).

Retirez sa carte résea filaire et ajoutez-lui une carte Wi-Fi.

Attention, il faut éteindre le PC, retirer la carte réseau filaire et ajouter la carte réseau Wi-Fi, sans oublier de rallumer le PC !

Il ne vous reste qu'à configurer les identifiants définis précédemment :

Laptop0

Physical Config Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

Wireless0

Bluetooth

Wireless0

Port Status ☒ On

Bandwidth 300 Mbps

MAC Address 0060.5C28.1123

SSID Default

Authentication

☐ Disabled ☐ WEP WEP Key

☐ WPA-PSK ☐ WPA2-PSK PSK Pass Phrase

☐ WPA ☒ WPA2 User ID openclassrooms

☐ 802.1X Method: MD5 Password openclassrooms

User Name

Password

Encryption Type AES

IP Configuration

☒ DHCP

☐ Static

IPv4 Address

Subnet Mask

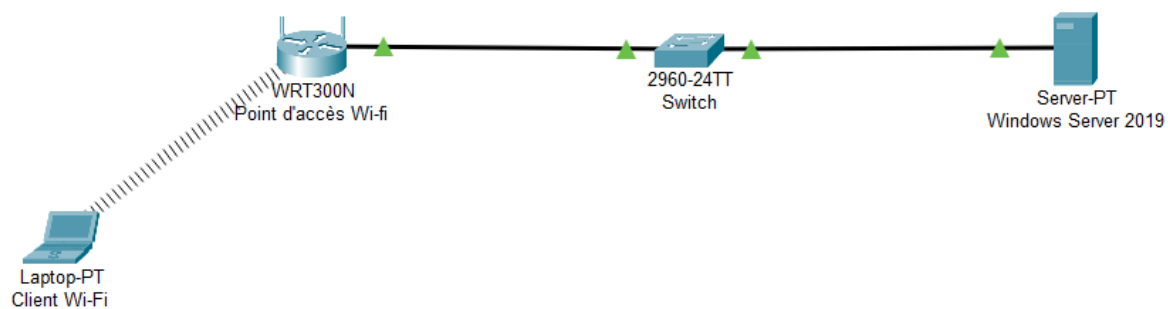
IPv6 Configuration

☐ Automatic

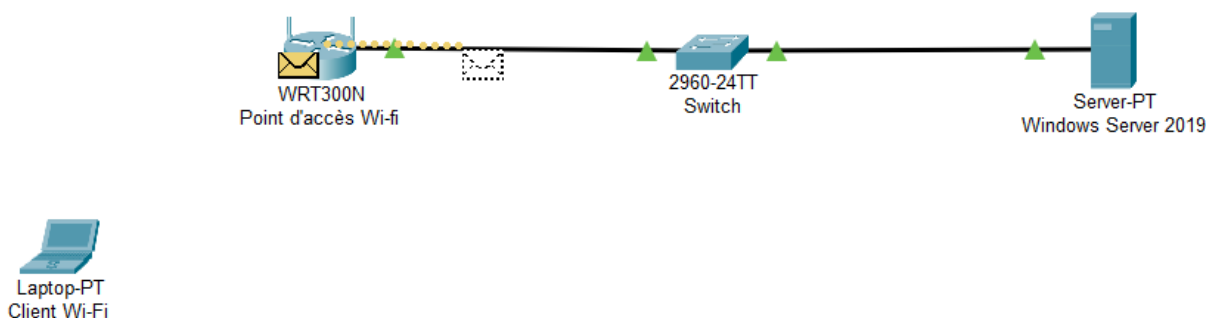
☐ Top

Configuration du PC portable

Fermez la fenêtre et attendez que **l'authentification** se mette en œuvre ; au bout de quelques secondes vous devriez avoir le résultat suivant :



Client Wi-Fi autorisé à se connecter au réseau grâce au protocole RADIUS
 Grâce à cette simulation rapide, vous avez compris comment fonctionne le protocole RADIUS.
 Vous pouvez alors passer **en mode Simulation** sous Packet Tracer, et redémarrer le serveur et le client Wi-Fi pour observer les “enveloppes” de données et les différents échanges liés au contrôle d’accès :

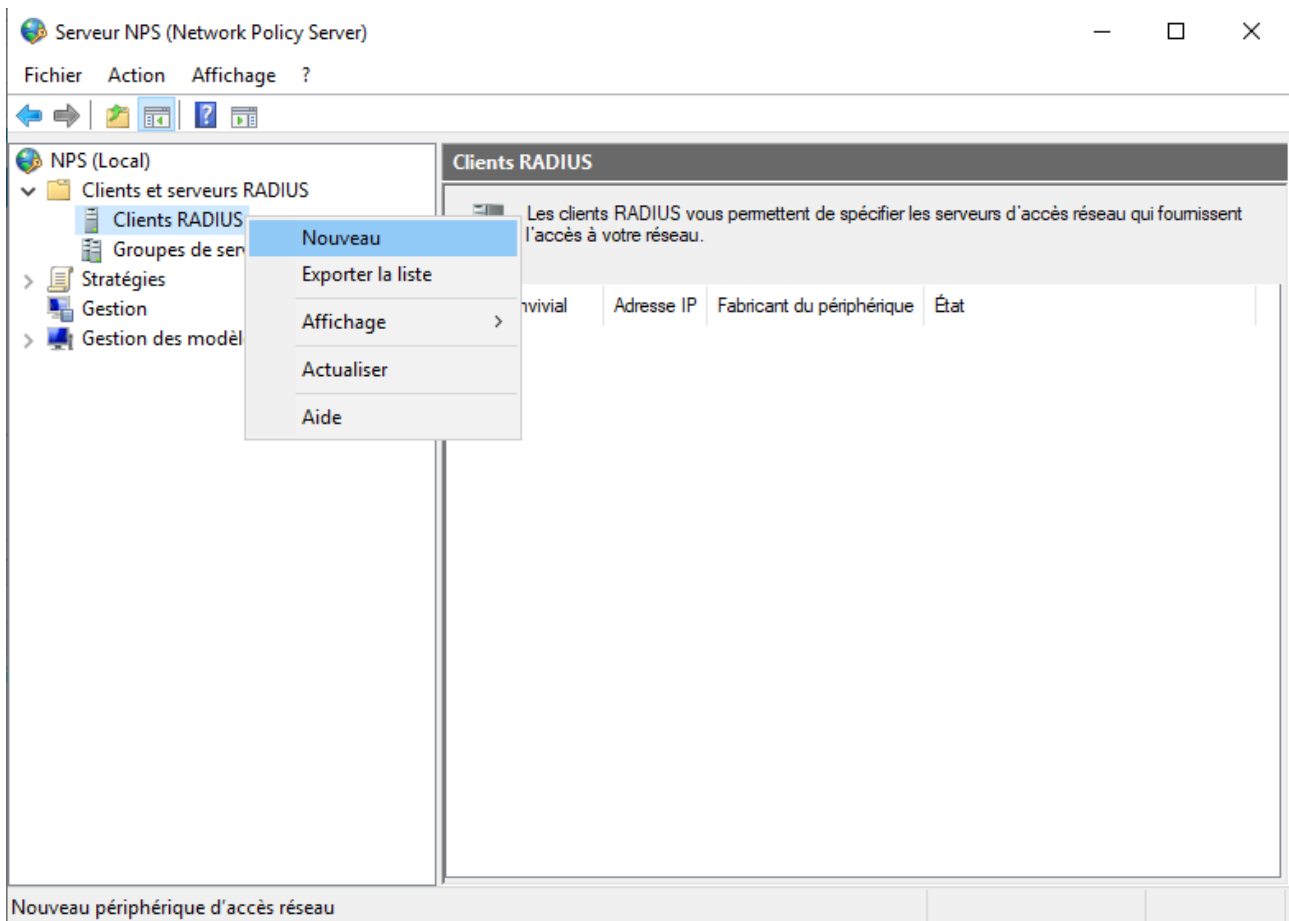


Échanges RADIUS précédant l’autorisation de l’accès au réseau pour le client Wi-Fi
 Maintenant que votre maquette fonctionne, **transposez** cela à votre Windows Server.

Si vous disposez de matériel compatible RADIUS, essayez de monter une maquette similaire. Les options étant propres à chaque matériel, je ne peux pas vous montrer où se trouvent les menus, mais comme vous le voyez, la partie Configuration d’un client RADIUS est extrêmement simple.

Transposez votre maquette sous Windows Server

La page de configuration d’un client RADIUS sous Windows est relativement la même que celle de Packet Tracer. Pour la trouver, rendez-vous sur le **Gestionnaire NPS** (Serveur NPS dans les outils d’administration), et ajoutez un client RADIUS en faisant un clic droit sur “**Clients RADIUS**” puis “**Nouveau**” :



Création d'un nouveau client RADIUS

La fenêtre suivante vous permet de configurer votre client :

Propriétés de Wifi_AP



Paramètres

Avancé

☒ Activer ce client RADIUS

☐ Sélectionner un modèle existant :

Nom et adresse

Nom convivial :

Adresse (IP ou DNS) :

Secret partagé

Sélectionnez un modèle de secrets partagés existant :

Aucun

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

☒ Manuel ☐ Générer

Secret partagé :

Confirmez le secret partagé :

OK

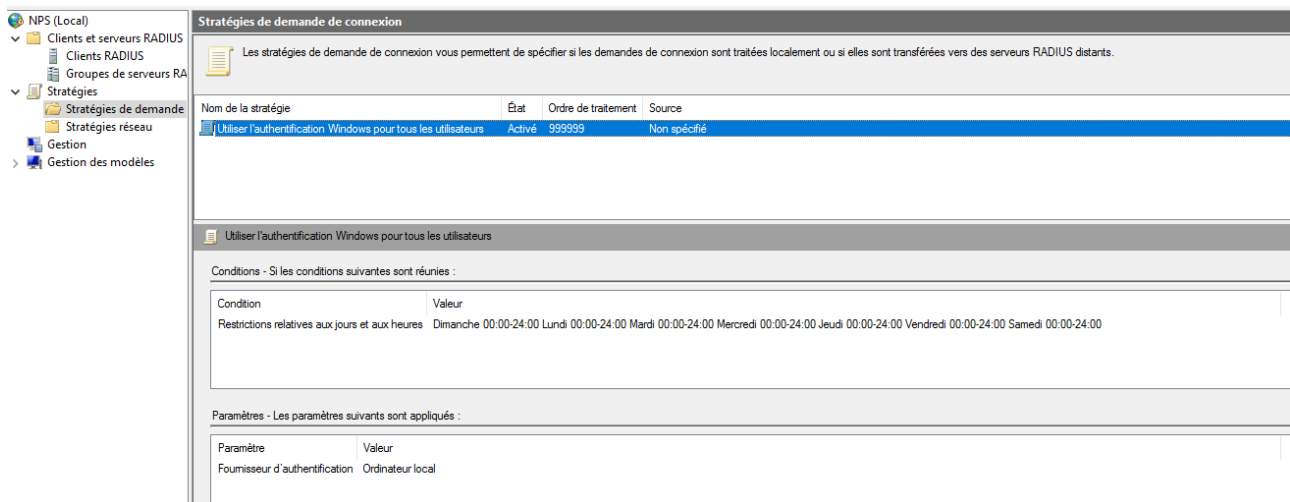
Annuler

Appliquer

Configuration d'un client RADIUS

Comme vous le voyez, rien de plus que dans Packet Tracer et sa simulation simpliste !

NPS permet, sous Windows Server, d'aller plus loin avec ce mécanisme, et notamment concernant les options sur la vérification de l'identité du client souhaitant accéder au réseau. Cela se trouve sous Windows, à l'emplacement "**Stratégies**" :

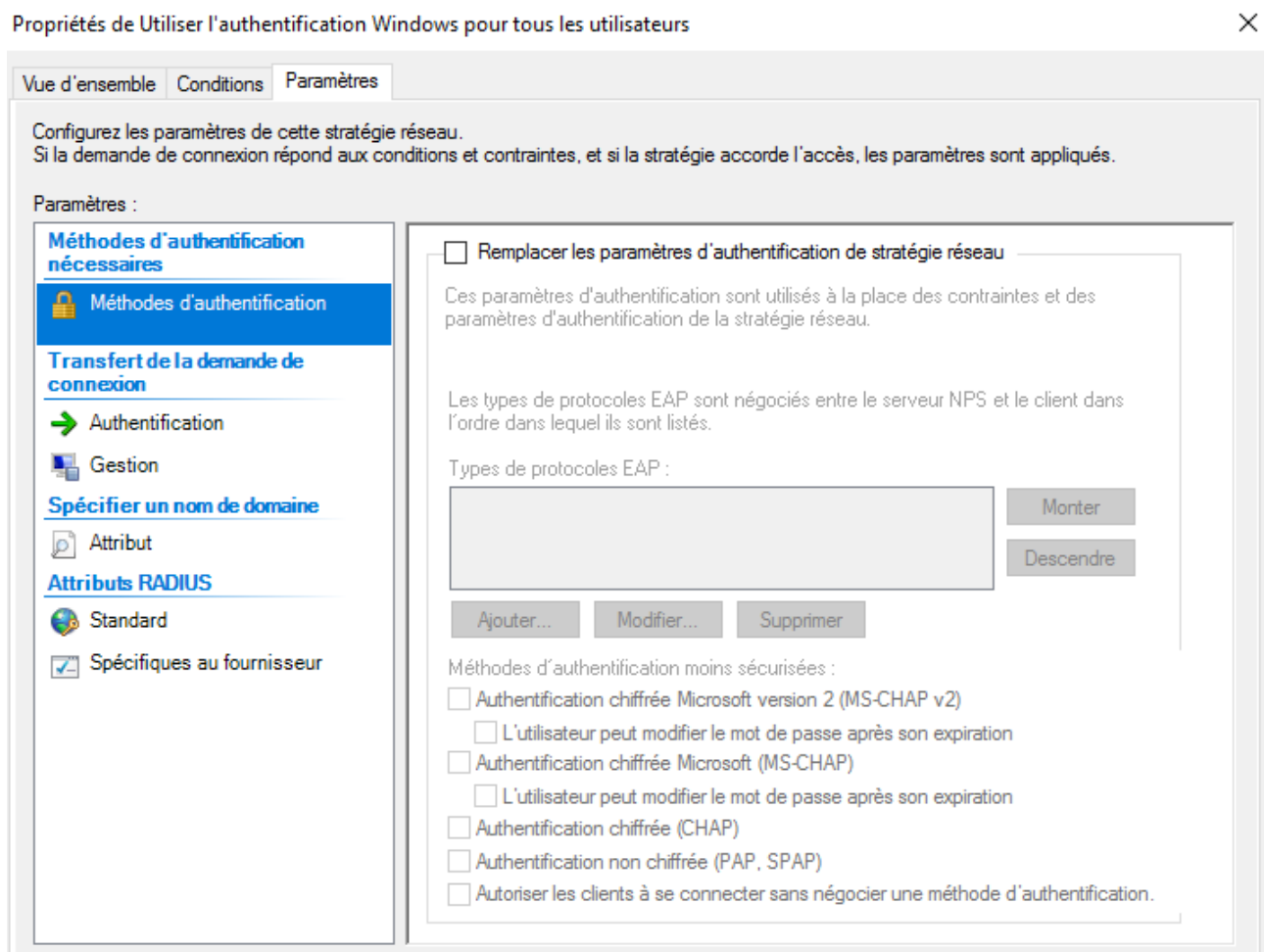


Stratégie de demande de connexion au réseau

Grâce à ces stratégies, il est possible de spécifier quels types de supplicants peuvent faire des demandes légitimes d'accès au réseau.

Une bonne pratique est d'utiliser les clients Windows étant inscrits au niveau de l'Active Directory ou mieux encore, de vérifier la présence d'un certificat sur le poste demandant l'accès au réseau.

Toutes ces possibilités se trouvent dans l'onglet **"Paramètres"** des propriétés de la stratégie :



Paramètres de la stratégie de demande d'accès au réseau

Ensuite, les stratégies réseau vous permettent de spécifier les accès effectifs à accorder aux demandeurs. Ici, j'ai autorisé les accès aux membres du groupe "**Utilisateurs**" du serveur NPS. Dans un cas réel, ce serait aux utilisateurs membres d'un groupe AD.

Voilà, vous savez tout (ou presque) sur le rôle d'accès au réseau. Libre à vous d'adapter cela en vous basant sur les ressources que je vous propose ci-après.

Allez plus loin

- [Guide Microsoft sur RADIUS.](#)
- [RFC décrivant le protocole RADIUS.](#)
- [Guide de l'ANSSI](#) sur la mise en place du contrôle d'accès au réseau.

En résumé

- Windows Server permet de **créer un Serveur RADIUS** à travers le rôle d'accès au réseau dit "**Serveur NPS**".
- **RADIUS** est un protocole faisant partie de la famille des **protocoles AAA** permettant l'authentification, l'autorisation et l'audit des accès.
- Avec le **Serveur NPS** de Windows, vous pouvez utiliser de **nombreuses options de vérification de l'identité** d'un équipement demandant un accès réseau, permettant d'authentifier avec précision les demandes d'accès.
- Les types d'**accès au réseau** peuvent **être conditionnés** à d'autres options spécifiées dans **des stratégies réseaux** permettant de limiter la bande passante, les horaires ou même les services accessibles.

Dans la prochaine partie, vous découvrirez tout ce qu'il faut savoir pour installer des services réseaux avancés tels que le service de déploiement, ou encore le service de mise à jour Windows.