Version expérimentale
En cours de validation

RÉSUMÉ THÉORIQUE – FILIÈRE SYSTEMES ET RESEAUX

M202 – Administrer un environnement Windows

105 heures

SOMMAIRE

MODALITÉS PÉDAGOGIQUES

1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques.

2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life.

3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life

4

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life.

5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage

Chapitre 1

Environnement de travail sous Windows Server

Dans ce module, vous allez :

- Préparer l'environnement de travail sous Windows Server
- Créer les machines virtuelles

5 heures

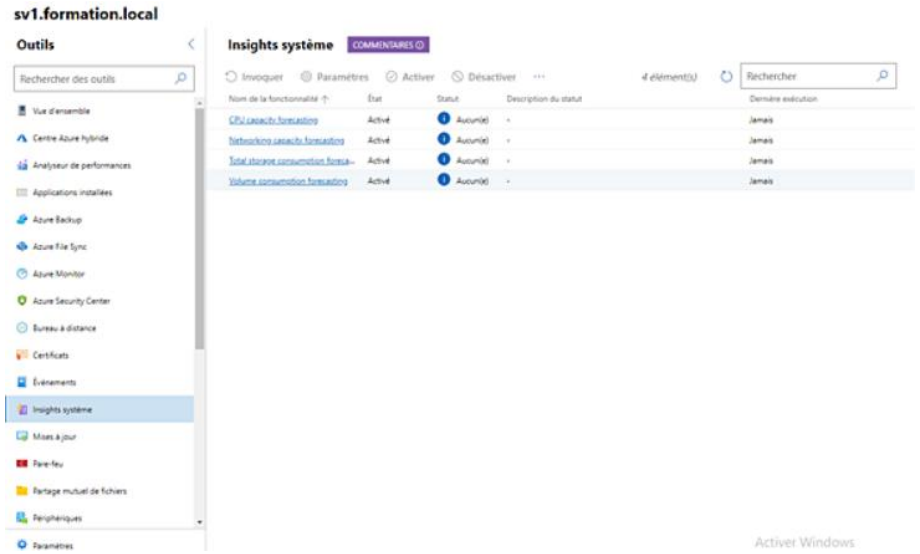
Préparer l'environnement de travail sous Windows Server 2019

1. Définition du système exploitation server
2. Présentation de Windows Server 2019
3. **Configuration requise pour l’installation**
4. **Installation du système hôte (complète /minimale)**

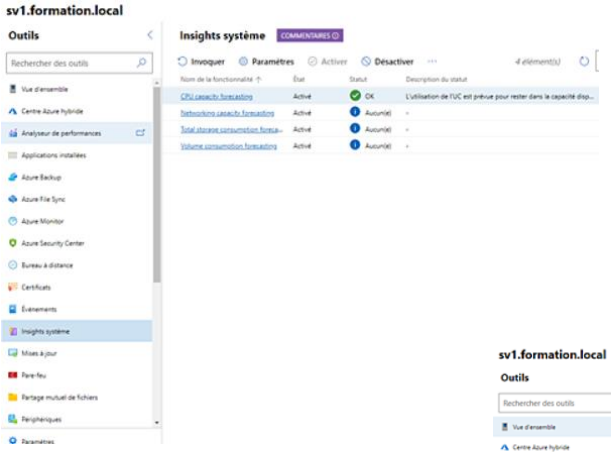
PARTIE 1

Présentation des capacités

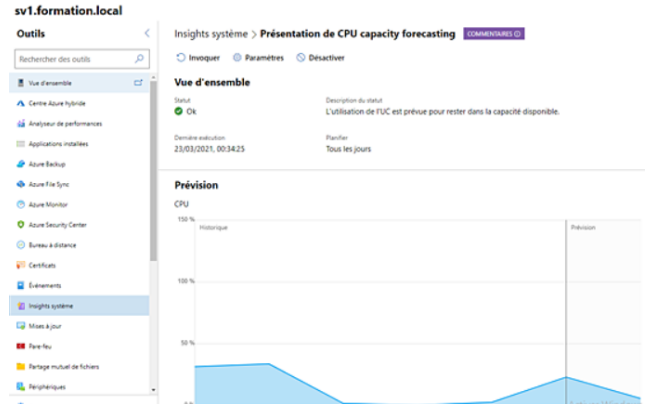
- En sélectionnant le nœud **Insights système**, les quatre capacités sont accessibles.



- Il est ainsi possible d'invoquer cette capacité en cliquant sur le lien puis sur le bouton **Invoquer**.



- La capacité est en cours…



Définition 1 : Le bac à sable

Le bac à sable

- Le bac à sable est un environnement virtuel ou physique de test qui permet de travailler sans perturber les machines ou serveurs en production.
- La virtualisation permet de diminuer le nombre de machines physiques nécessaires. Ainsi un seul serveur est nécessaire pour faire fonctionner plusieurs machines virtuelles. Il sera néanmoins nécessaire d'avoir les ressources suffisantes (mémoire, espace disque suffisants...).

PARTIE 1

Configuration nécessaire :

- Un serveur ou machine robuste est nécessaire pour faire tourner les machines virtuelles. Le serveur utilisé est équipé d'un Pentium Core i7 3,40 GHz et de 16 Go de RAM. Le rôle Hyper-V a été installé sur un système d'exploitation Windows Server 2019. Il est possible d'utiliser un autre système d'exploitation ou un autre système de virtualisation.
- Si votre configuration est inférieure à celle-ci, il suffira de démarrer seulement les machines virtuelles nécessaires. Il est utile de conserver un minimum de 1 Go à 2 Go pour la machine hôte

PARTIE 1

Configuration nécessaire :

Avant de procéder à l'installation de Windows Server 2019 sur le poste physique, il est nécessaire de s'assurer de respecter les prérequis du système d'exploitation.

- **Processeur** : 1,4 GHz minimum et architecture 64 bits.
- **Mémoire RAM** : 2 Go de mémoire RAM est le strict minimum. Afin de pouvoir virtualiser des machines virtuelles, 8 Go sont recommandés.
- **Espace disque** : une installation de base avec aucun rôle nécessite un espace disque de 15 Go. Il faut prévoir un espace plus ou moins conséquent en fonction du rôle du serveur.

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

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

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

Attention, il n'est plus possible de basculer le serveur d'une installation complète vers une installation minimale et inversement.

Créer les machines virtuelles

Ce que vous allez apprendre dans ce chapitre :

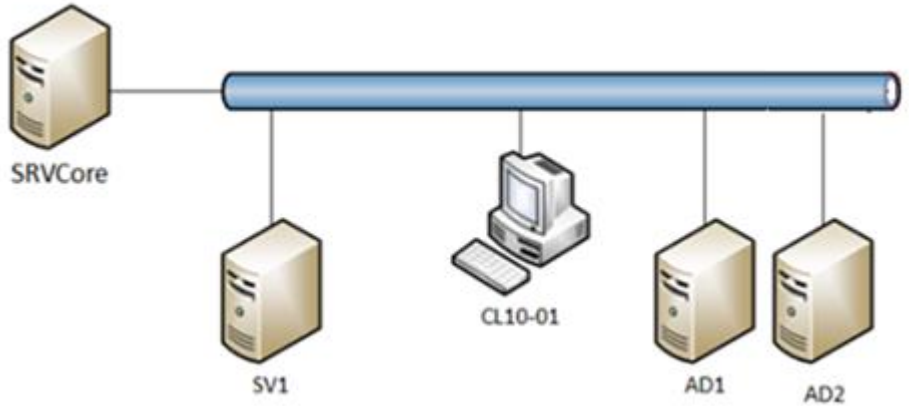
1. Schéma de la maquette
2. Machine virtuelle AD1
3. Machine virtuelle AD2
4. Machine virtuelle SV1
5. Machine virtuelle SRVCore
6. Machine virtuelle CL10-01
7. Les points de contrôle

Créer les machines virtuelles

Création des machines virtuelles

Schéma de la maquette

- Cinq machines virtuelles vont être créées, les systèmes d'exploitation utilisés sont Windows Server 2019 ou Windows 10. De plus certains ateliers (migration d'un serveur de fichier, migration du DHCP…) nécessitent une machine virtuelle exécutant Windows Server 2012 R2.
- La maquette contient quatre serveurs et un poste de travail virtuel :
- **AD1**, contrôleur de domaine du domaine formation.local.
- **AD2**, contrôleur de domaine du domaine formation.local.
- **SV1**, serveur membre du domaine formation.local.
- **SRVCore**, serveur en version core (installation minimale), non membre du domaine).
- **CL10-01**, poste client sous Windows 10 membre du domaine formation.local.



PARTIE 1

PARTIE 1

Rôles installés et configuration des serveurs et postes :

	Rôles installés	Configuration IP
AD1	Active Directory, DNS et DHCP	Adresse IP : 192.168.1.90 Masque de sous-réseau : 255.255.255.0 Passerelle par défaut : 192.168.1.254 Serveur DNS primaire : 192.168.1.90 Serveur DNS auxiliaire : 192.168.1.91
AD2	Active Directory et DNS	Adresse IP : 192.168.1.91 Masque de sous-réseau : 255.255.255.0 Passerelle par défaut : 192.168.1.254 Serveur DNS primaire : 192.168.1.91 Serveur DNS auxiliaire : 192.168.1.90
SV1	Aucun rôle	Adresse IP : 192.168.1.92 Masque de sous-réseau : 255.255.255.0 Passerelle par défaut : 192.168.1.254 Serveur DNS primaire : 192.168.1.90
SRVCore	Aucun rôle	Adresse IP : 192.168.1.93 Masque de sous-réseau : 255.255.255.0 Passerelle par défaut : 192.168.1.254 Serveur DNS primaire : 192.168.1.90
CL10-01	Aucun rôle	Adresse IP : 192.168.1.94 Masque de sous-réseau : 255.255.255.0 Passerelle par défaut : 192.168.1.254 Serveur DNS primaire : 192.168.1.90

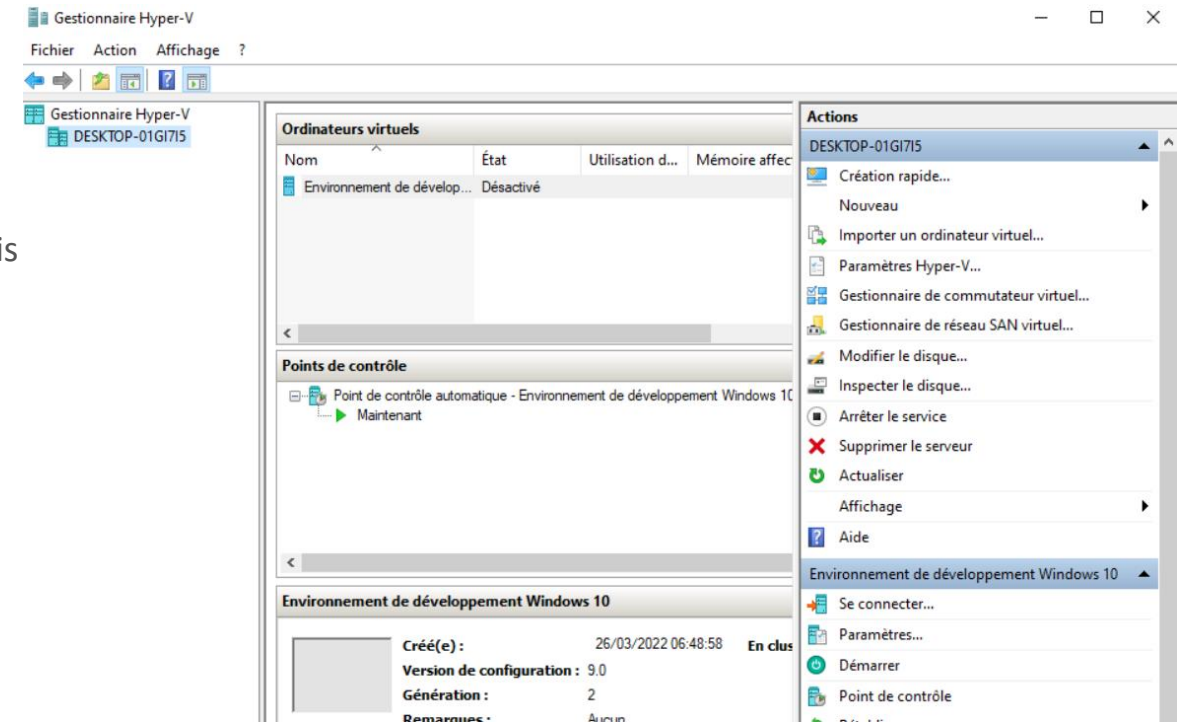
NB: L'installation et la configuration des rôles sont détaillées dans les chapitres suivants.

Machine virtuelle AD1

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

.

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

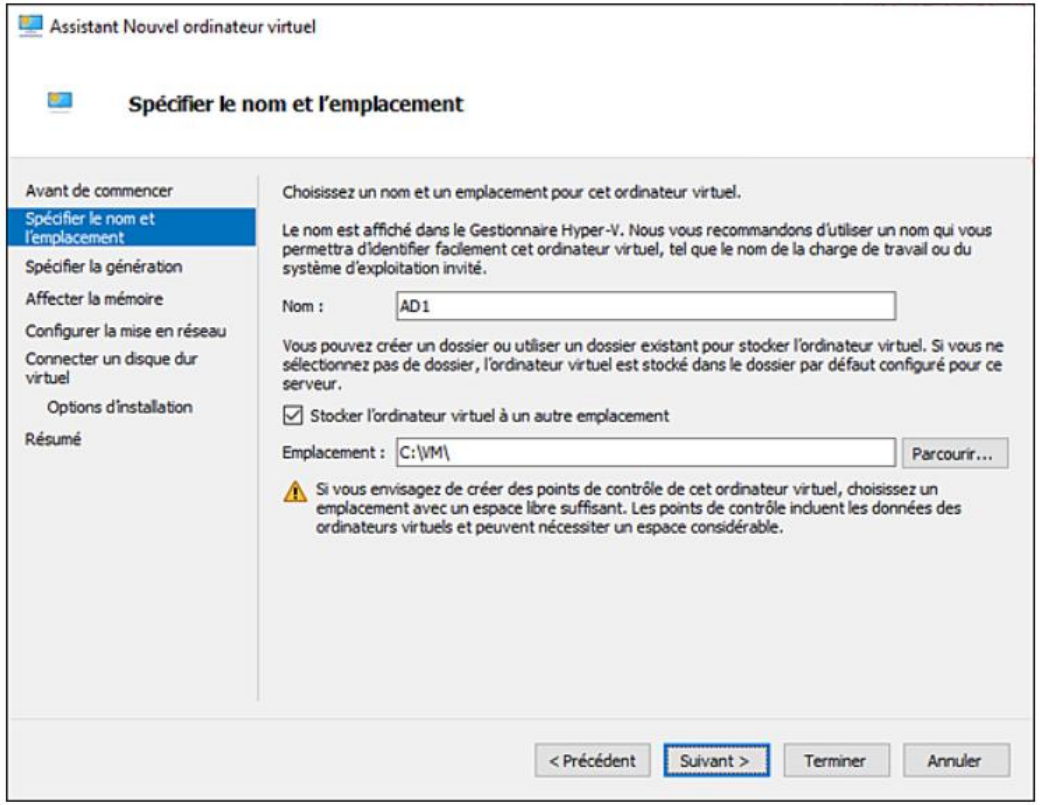


PARTIE 1

Machine virtuelle AD1

.

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

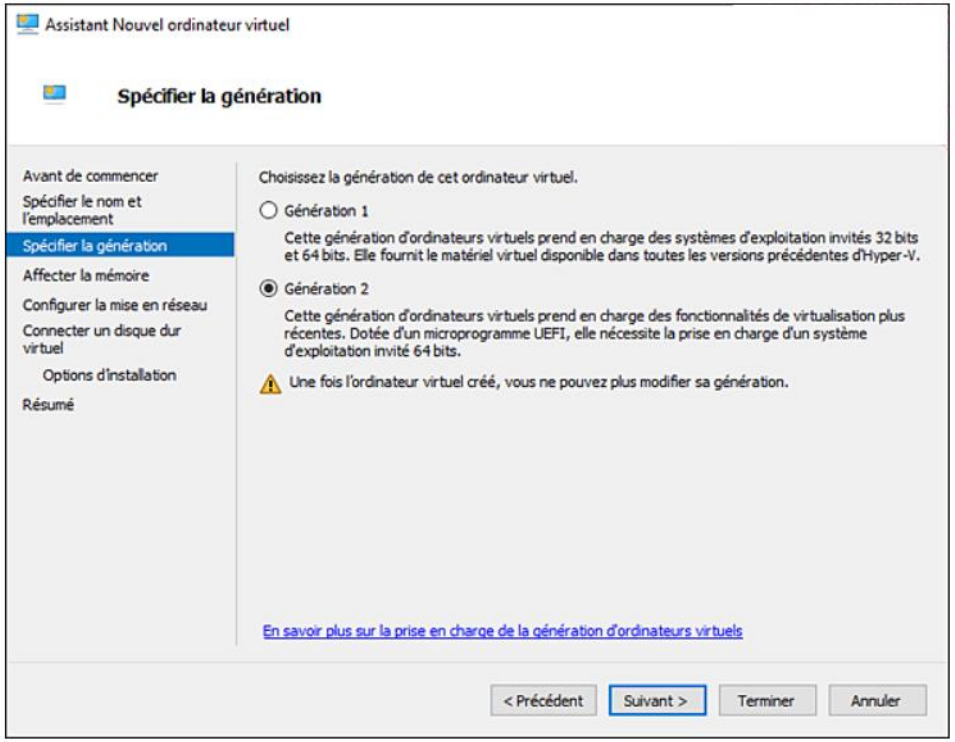


PARTIE 1

Machine virtuelle AD1

.

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

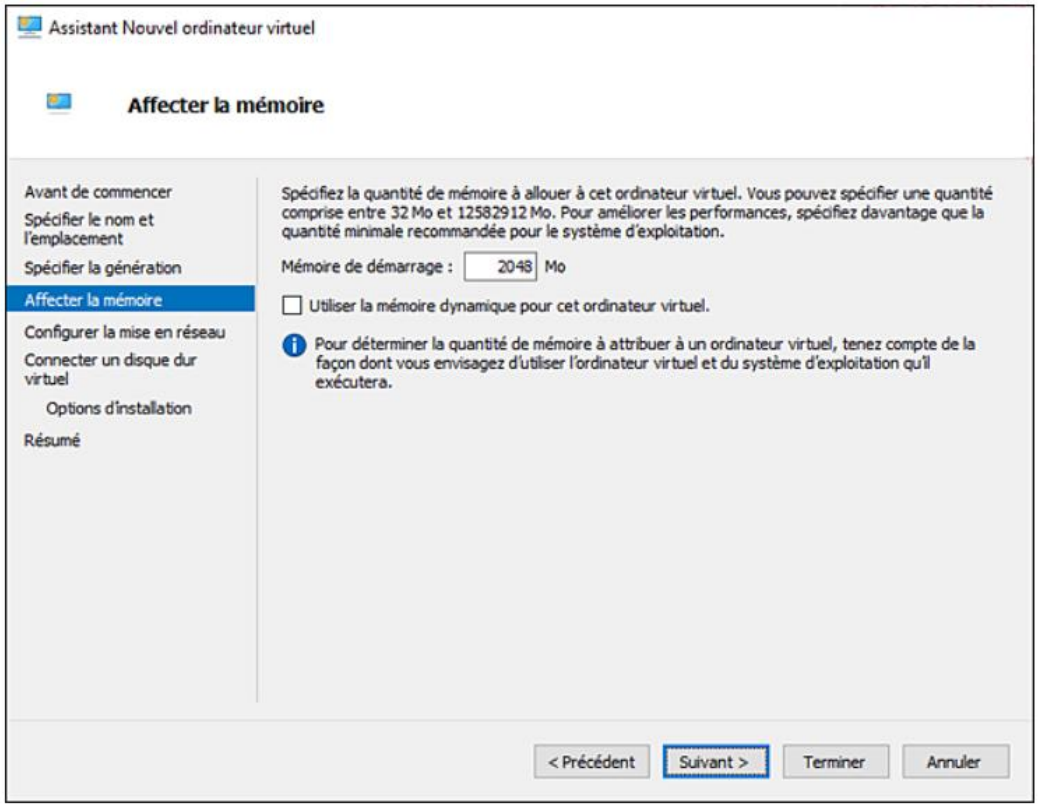


PARTIE 1

Machine virtuelle AD1

.

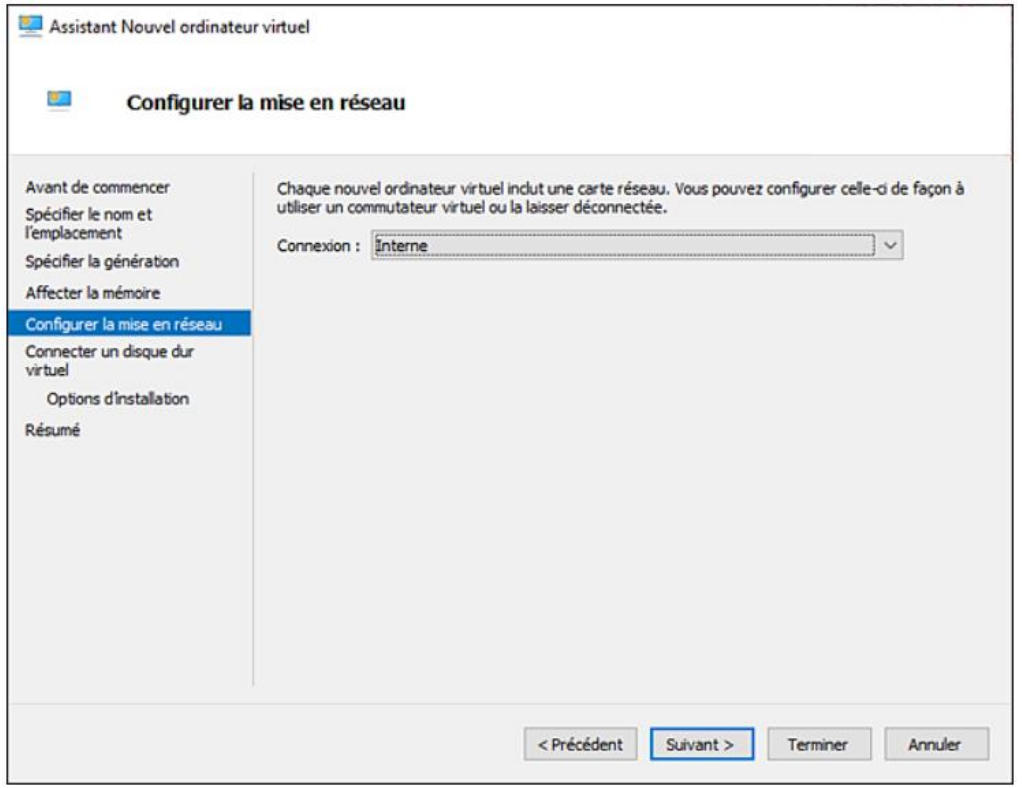
- Saisissez **2048** dans le champ **Mémoire de démarrage**, ou plus si souhaité.



PARTIE 1

Machine virtuelle AD1

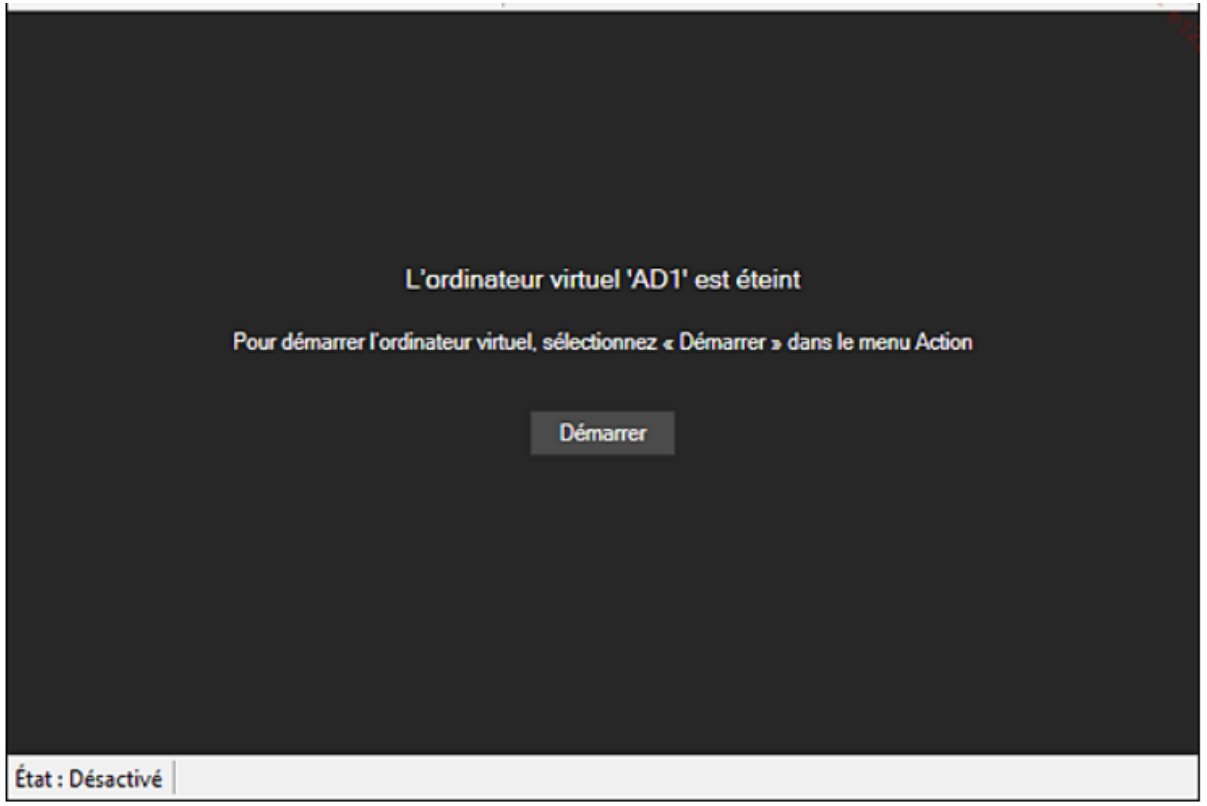
- Dans la fenêtre **Configurer la mise en réseau**, sélectionnez la carte réseau souhaitée (interne ou carte réseau physique) puis cliquez sur **Suivant**
- Saisissez **60** dans le champ **Taille** du disque et validez à l'aide du bouton **Suivant**.
- Connectez à la machine virtuelle l'ISO ou le DVD de Windows Server 2019 et cliquez sur **Suivant**.
- Dans la fenêtre du résumé, cliquez sur **Terminer**.
- La nouvelle machine apparaît dans la fenêtre centrale de la console.
- Le disque dur de la machine est créé mais vierge. Il est nécessaire de le partitionner et d'installer un système d'exploitation.



PARTIE 1

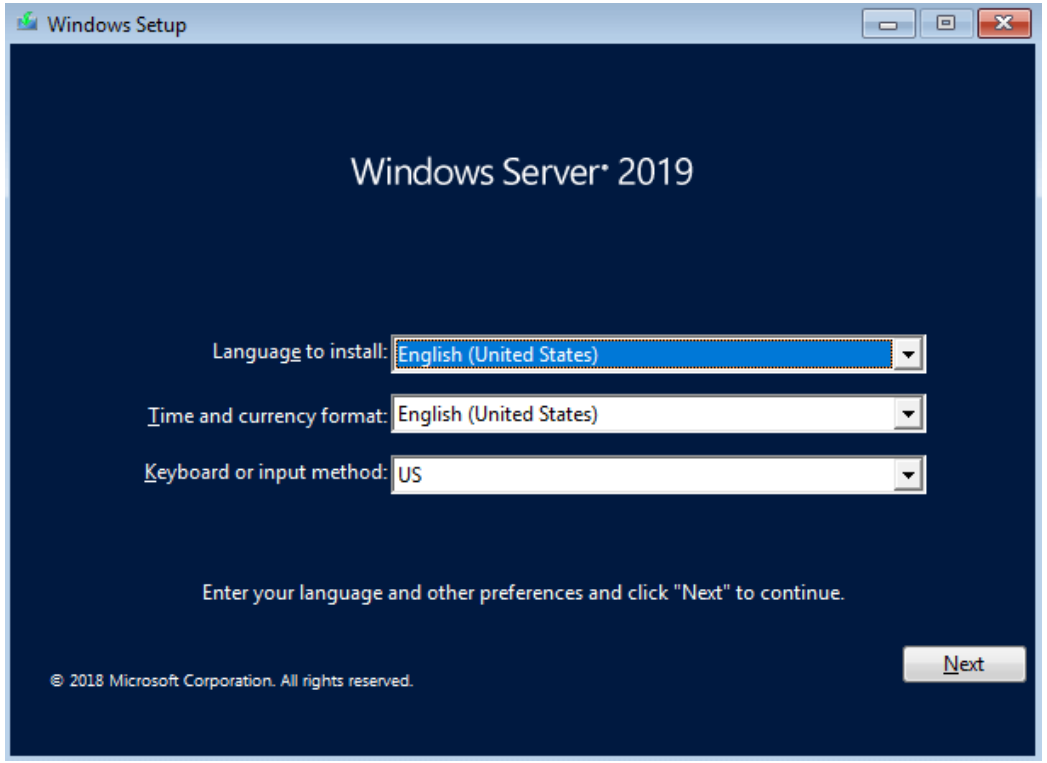
Installation du système d'exploitation

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



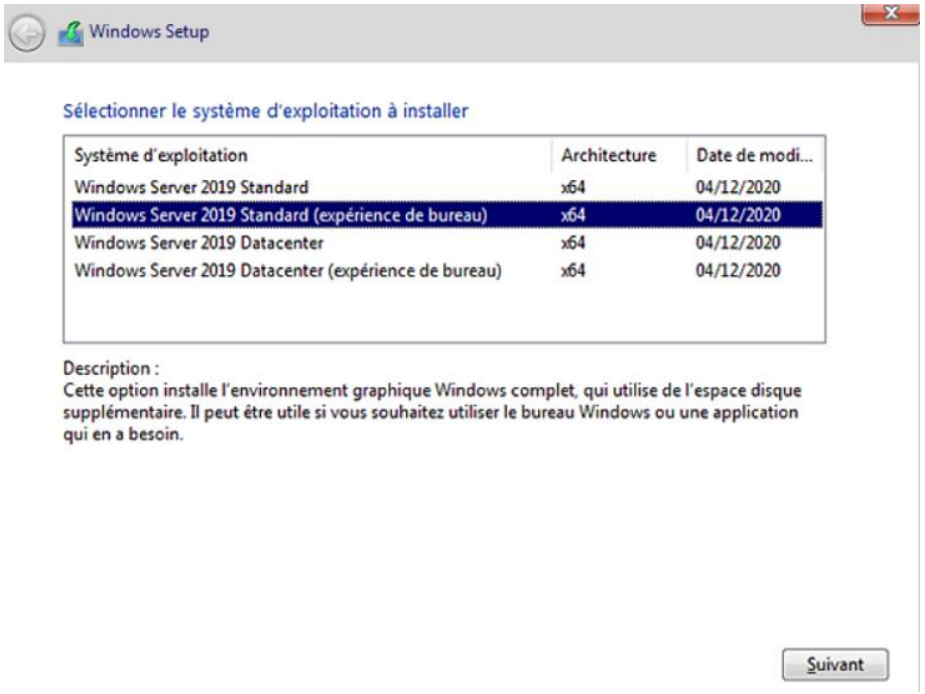
Installation du système d'exploitation

- La machine démarre et l'installation de Windows Server 2019 débute.
- Dans la fenêtre du choix des langues (la langue française est sélectionnée par défaut), cliquez sur **Suivant**.



Installation du système d'exploitation

- Cliquez sur **Installer maintenant** pour lancer l'installation.
- Cliquez sur **Windows Server 2019 Standard (expérience de bureau)** puis cliquez sur **Suivant**.

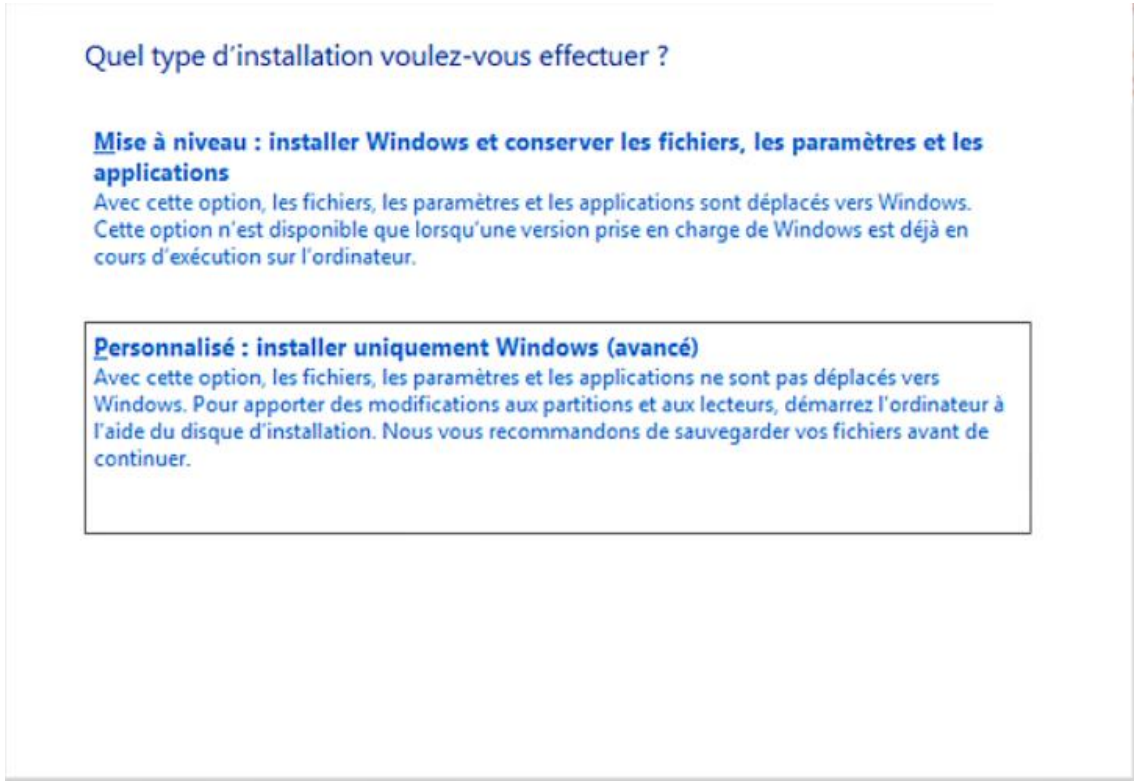


- **Acceptez la licence puis cliquez sur Suivant.**

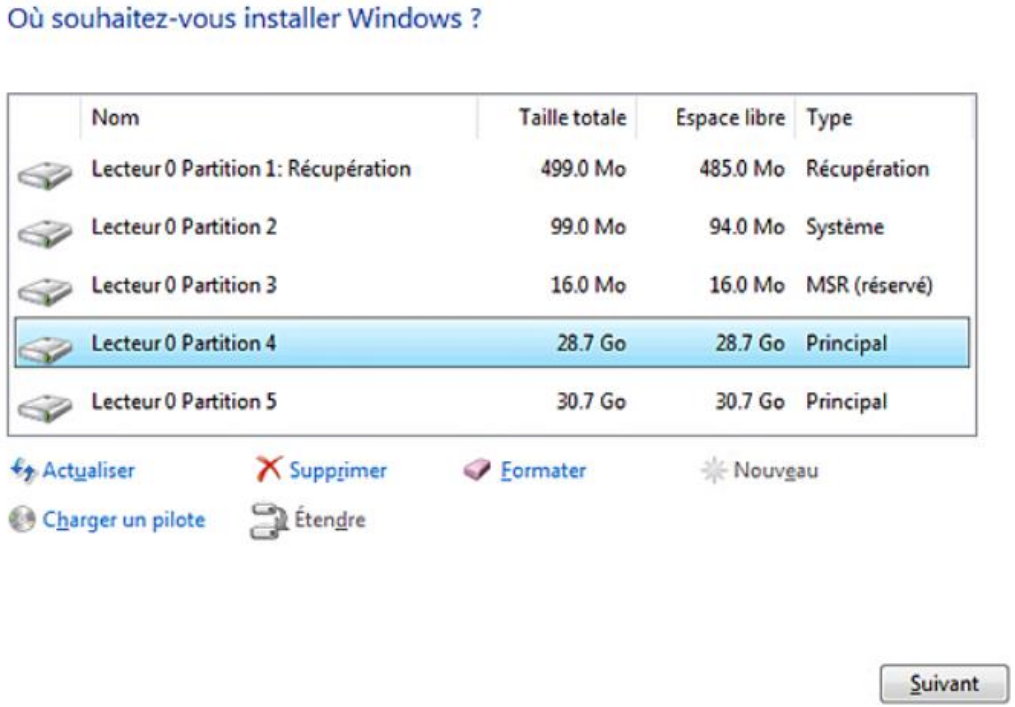
PARTIE 1

Installation du système d'exploitation

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



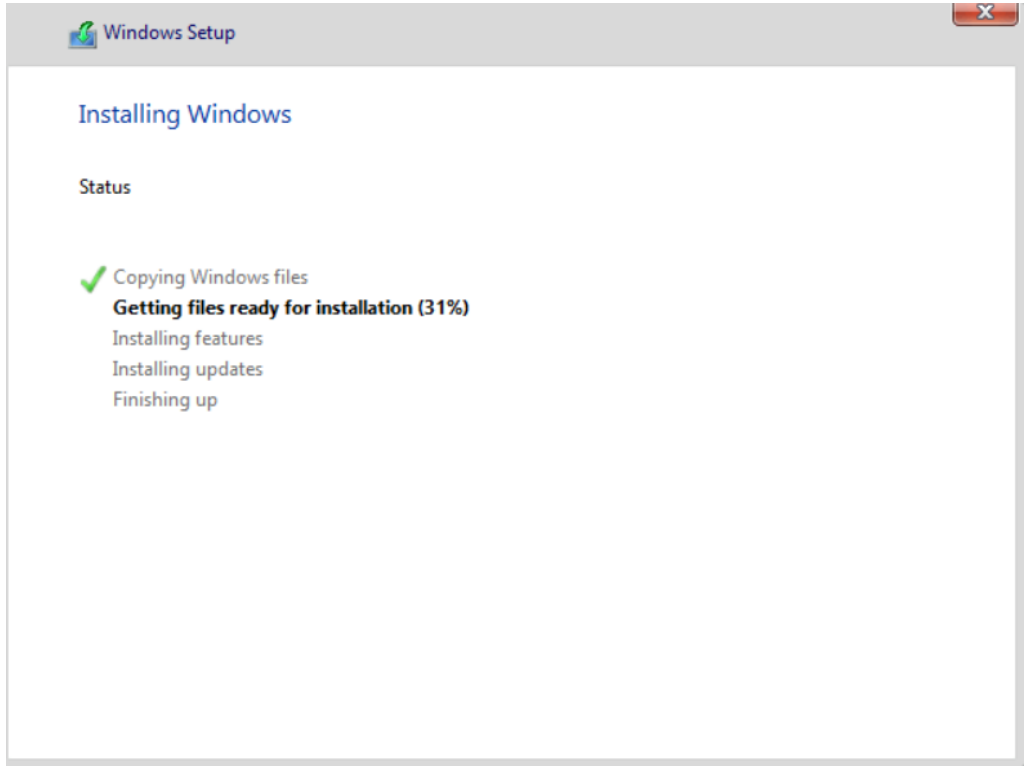
- À l'aide de l'option **Nouveau**, créez deux partitions de 30 Go.



PARTIE 1

Installation du système d'exploitation

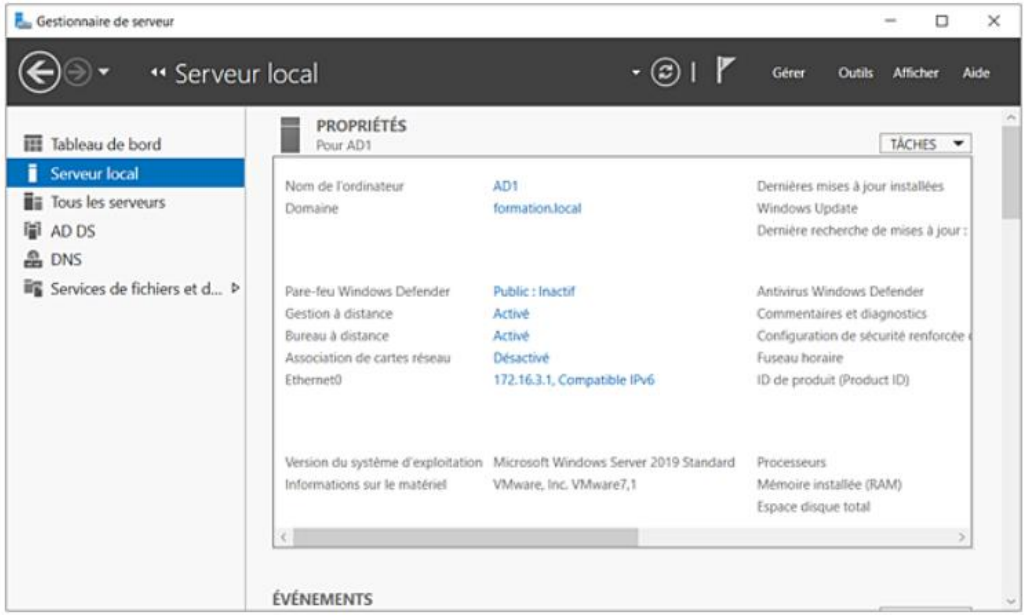
- Cliquez sur la première partition puis sur **Suivant**.
- L'installation est en cours…
- Saisissez le mot de passe **Pa$$w0rd** puis confirmez-le.
- L'installation est maintenant terminée. L'étape suivante est la modification du nom du serveur ainsi que la configuration IP de la machine.



Configuration post-installation

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

- Ouvrez une session en tant qu'**administrateur** en saisissant le mot de passe configuré à la section précédente.
- Dans la console **Gestionnaire de serveur**, cliquez sur **Serveur local**.
- Cliquez sur le **Nom de l'ordinateur** afin d'ouvrir les propriétés système.
- Dans la fenêtre **Propriétés système**, cliquez sur **Modifier** puis saisissez le nom du serveur (**AD1**).
- Cliquez deux fois sur **OK** puis sur **Fermer**.
- Redémarrez la machine virtuelle afin de rendre effectives les modifications.

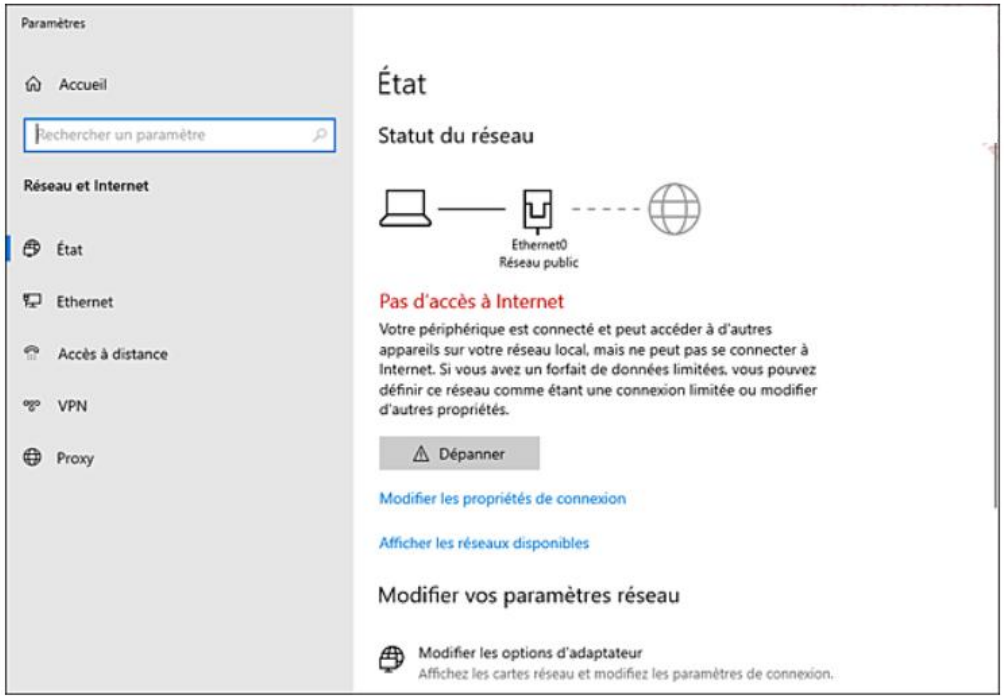


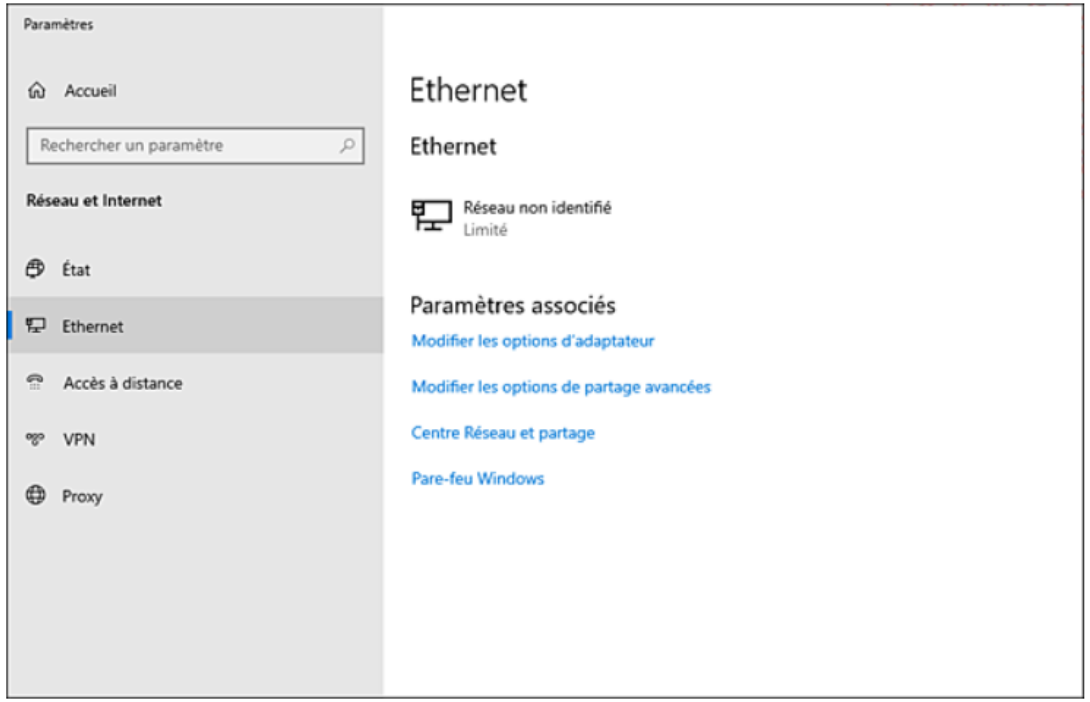
PARTIE 1

PARTIE 1

Configuration post-installation

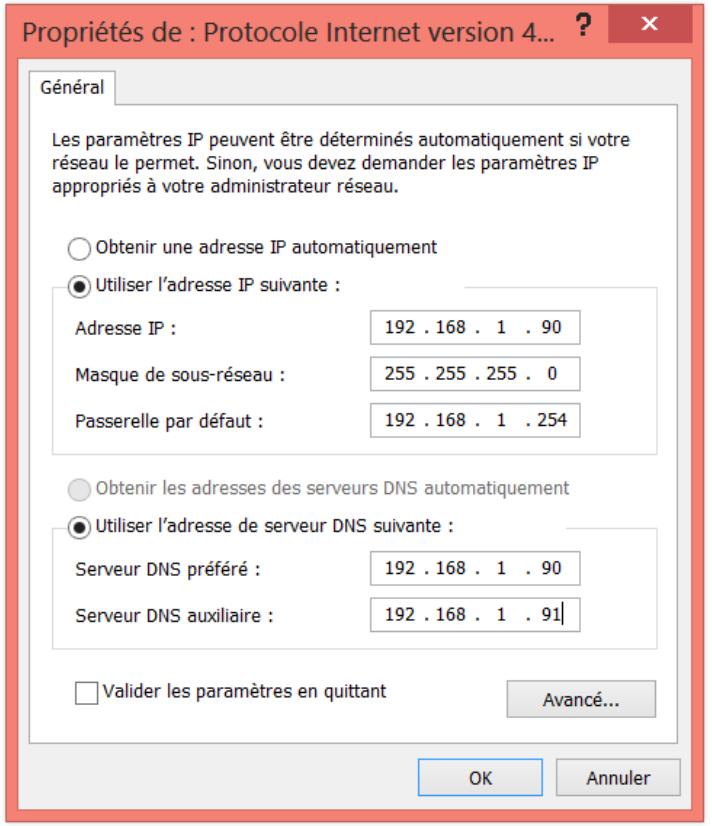
- Il est désormais nécessaire de configurer l'adressage IP de la carte réseau.
- Effectuez un clic droit sur le **Centre Réseau et partage** présent dans la zone de notification (icône à gauche de l'heure) puis cliquez sur **Ouvrir le paramètre réseau et internet**.
- Cliquez sur **Ethernet** dans le menu de gauche.
- Une nouvelle fenêtre se lance, cliquez sur Modifier les options d'adaptateur.





Configuration post-installation

- Double cliquez sur la carte réseau, puis sur **Propriétés**.
- Dans la fenêtre des propriétés, double cliquez sur **Protocole Internet Version 4 (TCP/IPv4)**.
- Configurez l'interface réseau comme ci-dessous
- Les manipulations à reproduire étant les mêmes, seuls les paramètres seront détaillés pour les machines virtuelles suivantes.
- Les modifications à effectuer sont le nom du poste et sa configuration IP.



PARTIE 1

Configuration post-installation

Machine virtuelle AD2

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

  Adresse IP : 172.16.3.2

  Masque de sous-réseau : 255.255.20.0

  Serveur DNS préféré : 172.16.3.2

  Serveur DNS auxiliaire : 172.16.3.1

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

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

Configuration post-installation

Machine virtuelle SV1

- Ce serveur est membre du domaine. Différents rôles seront installés par la suite.La quantité de mémoire allouée est de **2048 Mo** et le disque virtuel de **60 Go** est divisé en deux partitions.

  Nom du poste : SV1

  Adresse IP : 172.16.3.3

  Masque de sous-réseau : 255.255.20.0

  Serveur DNS préféré : 172.16.3.1

  Serveur DNS auxiliaire : 172.16.3.2

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

Configuration post-installation

Machine virtuelle SRVCore

- Ce serveur est installé en mode sans interface utilisateur (mode core). Toutes les configurations seront apportées dans les chapitres suivants.
- La quantité de mémoire allouée est de **1024 Mo** et le disque virtuel de **30 Go** est partitionné avec une seule partition.

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

Machine virtuelle CL10-01

- Poste client sous **Windows 10 1809**, cette machine est membre du domaine. La configuration IP se fera par l'intermédiaire d'un **serveur DHCP**.
- La quantité de mémoire allouée est de **2048 Mo** et le disque virtuel de **30 Go** est partitionné avec une seule partition.

Nom du poste : CL10-01

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

Chapitre 2

Hyper-V

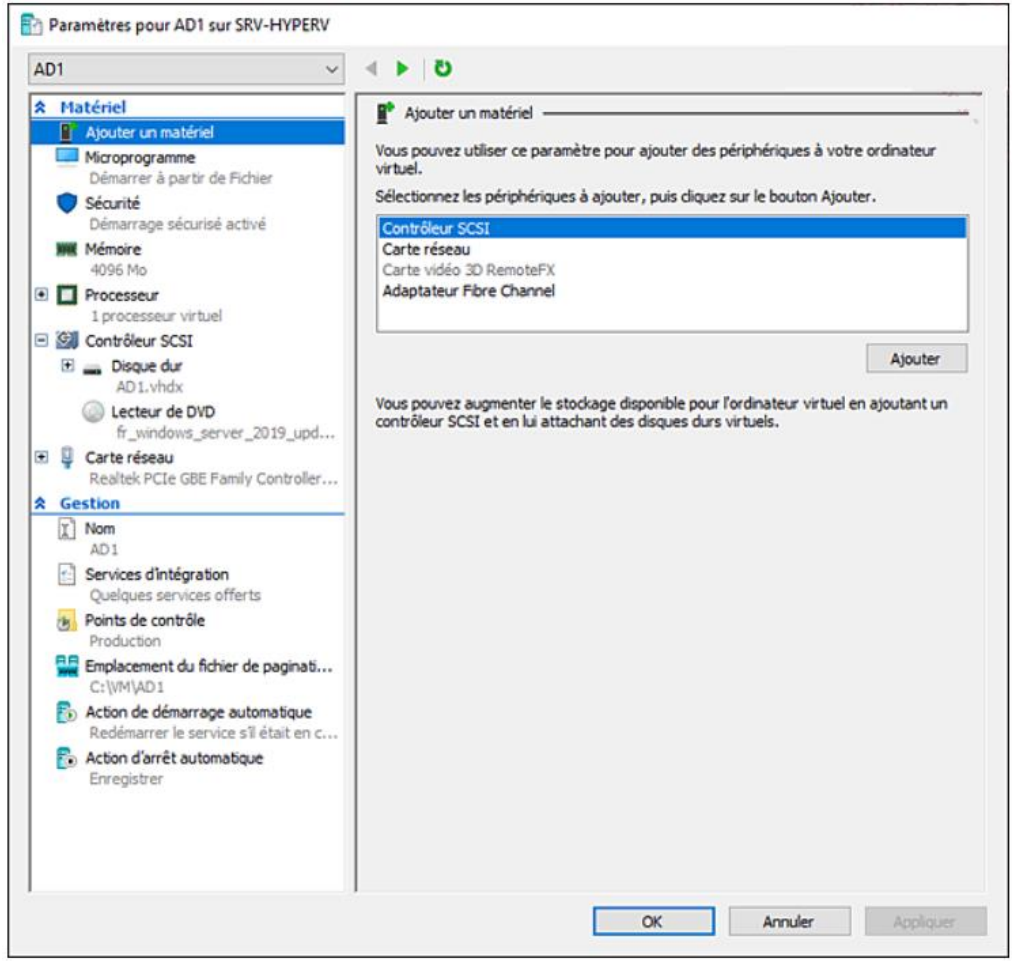
1. Implémentation d'Hyper-V
2. Le disque dur des machines virtuelles
3. Gestion des réseaux virtuels
4. Gestion des machines virtuelles

- **Hyper-V** est le système de virtualisation de Microsoft, il est présent dans les systèmes d'exploitation depuis Windows Server 2008, et Windows 8 sur les systèmes d'exploitation client.
- Cet hyperviseur offre l'avantage d'offrir un accès immédiat au matériel de la machine hôte, et donc de meilleurs temps de réponse. L'installation s'effectue par l'intermédiaire de la console **Gestionnaire de serveur** ou en PowerShell.

Par défaut, une machine virtuelle utilise les équipements suivants :

- BIOS : le BIOS d'un ordinateur physique est simulé, plusieurs facteurs peuvent être configurés :
  - L'ordre de boot pour la machine virtuelle (réseau, disque dur, DVD…).
  - Le démarrage sécurisé qui permet d'empêcher le code non autorisé de s'exécuter au démarrage de la machine virtuelle.
- Mémoire RAM : une quantité de mémoire vive est allouée à la machine virtuelle. Un maximum de 1 To de mémoire peut être alloué pour des machines virtuelles de génération 1. Pour les génération 2, une limite de 12 To maximum peut être allouée. Depuis Windows Server 2008 R2 SP1, il est possible de mettre en place la mémoire dynamique (traitée plus loin dans ce chapitre).
- Processeur : comme pour la mémoire, il est possible d'allouer un ou plusieurs processeurs (en fonction du nombre de processeurs et du nombre de cœurs de la machine physique). Un maximum de 64 processeurs peut être appliqué à une machine virtuelle pour une génération 1. Concernant la génération 2, un maximum de 240 processeurs virtuels est possible.
- Contrôleur SCSI : ajoute un contrôleur SCSI à la machine virtuelle. Il est ainsi possible d'ajouter des disques durs ou des lecteurs de DVD. En choisissant la création d'une machine virtuelle de génération 2, il est impossible d'ajouter un contrôleur IDE.
- Carte réseau : depuis Windows Server 2012 R2, la carte réseau de la machine virtuelle peut désormais effectuer un boot PXE (démarrage sur le réseau et chargement d'une image) sans être de type hérité.

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



PARTIE 1

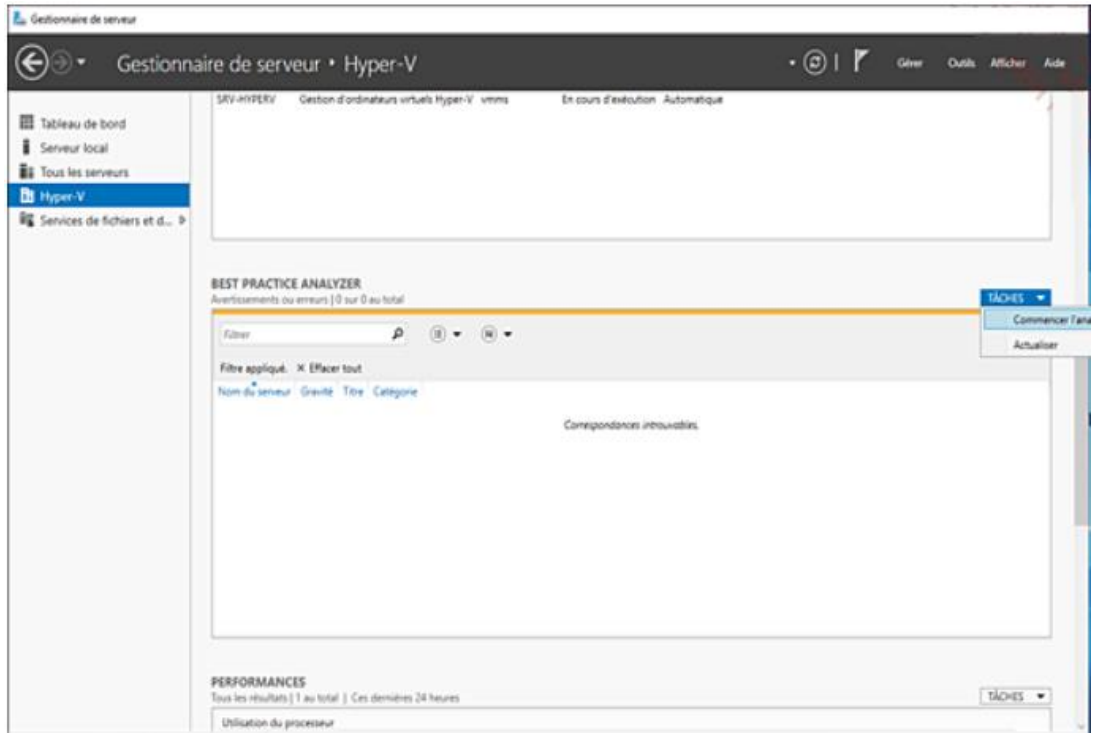
- Les services d'intégration permettent une amélioration des performances de la machine virtuelle. Ils offrent des fonctionnalités intéressantes telles que la copie de fichiers invités ou l'utilisation de pilotes de périphériques synthétiques. Il est possible de procéder à l'activation/désactivation des différentes fonctionnalités offertes par les services d'intégration directement depuis l'hôte Hyper-V. Il est intéressant de noter que l'ensemble des fonctionnalités sont activées par défaut à l'exception de la fonctionnalité **Interface de services d'invité Hyper-V**.
- L'ensemble des composants nécessaire aux services d'intégration est présent dans les systèmes d'exploitation. Aucune opération ne doit être effectuée post installation. Seuls les systèmes d'exploitation Windows Server 2008 R2 SP1, Windows Server 2008 SP2 et Windows 7 SP1 nécessitent l'installation de toutes les mises à jour critiques pour pouvoir utiliser les services d'intégration correctement. Les systèmes d'exploitation Windows XP et Windows Server 2003 ne sont pas pris en charge avec un serveur Hyper-V sous Windows Server 2019.
- Concernant les machines Linux, les composants nécessaires ont été ajoutés à certains noyaux pour certaines éditions. Pour les noyaux plus anciens, Microsoft met à disposition les pilotes LIS installables.
- Afin d'obtenir des performances adéquates avec la machine virtuelle, il est important de vérifier le support de la distribution Linux avec Hyper-V sous Windows Server 2019 depuis le site de Microsoft.

01 - Implémentation d'Hyper-V

Présentation du Best Practice Analyser

Le BPA ou Best Practice Analyser est un outil intéressant. Il permet d'avoir des recommandations suite à l'installation du rôle. Il est donc très facile de vérifier si on respecte les bonnes pratiques recommandées par Microsoft. En cas de non-respect, la règle de recommandation s'affiche avec un détail permettant la mise en conformité.

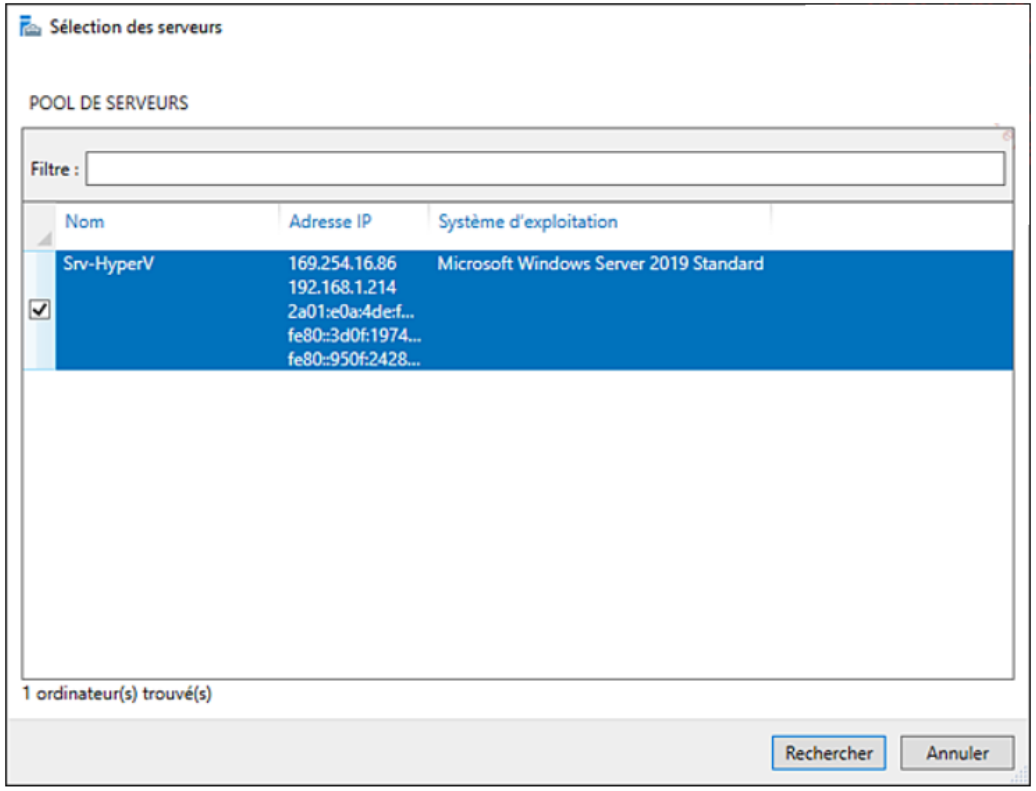
- Depuis la console Gestionnaire de serveur du serveur Hyper-V, cliquez sur **Hyper-V**. Dans la section BEST PRACTICE ANALYSER, cliquez sur **TÂCHES** puis sur **Commencer l'analyse BPA**.



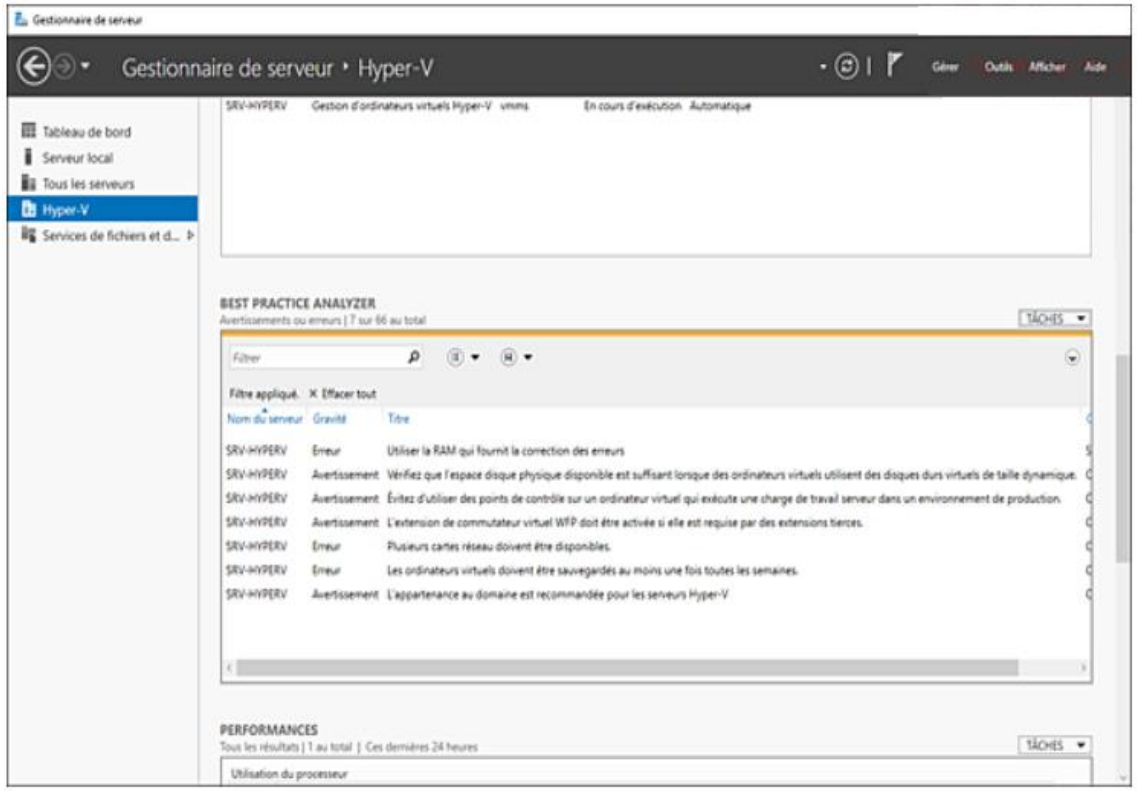
PARTIE 1

PARTIE 1

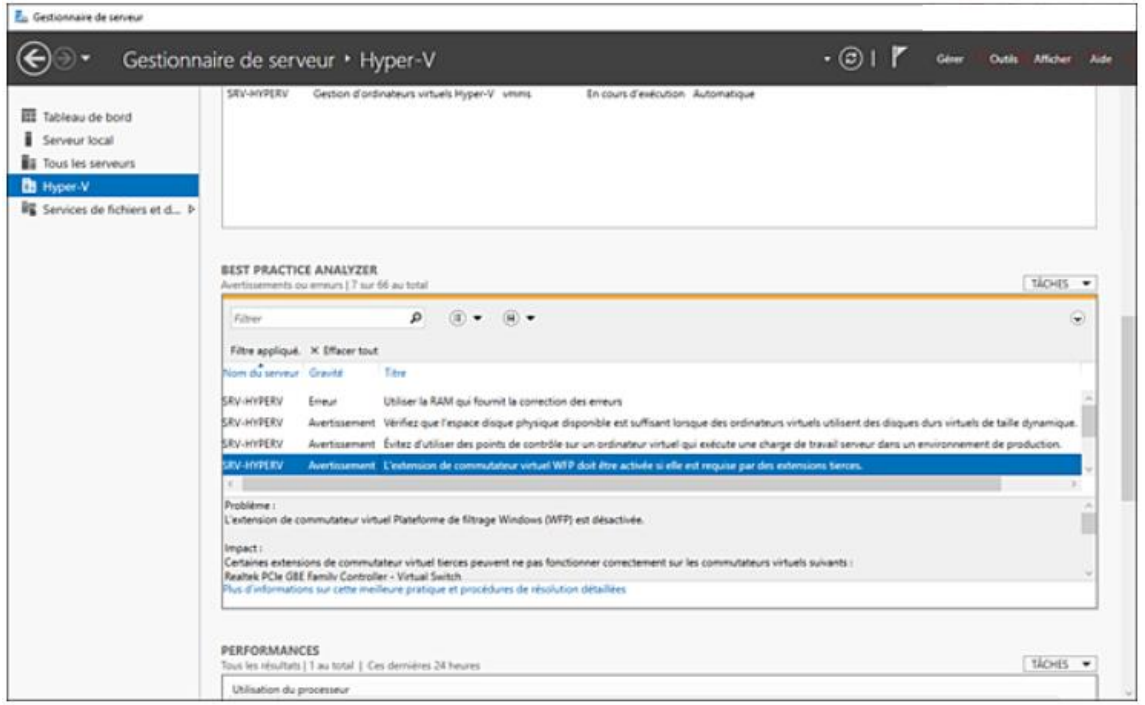
- Une fenêtre de sélection des serveurs apparaît. Sélectionnez le serveur souhaité puis cliquez sur **Rechercher**.



- La vérification est en cours. À l'issue de cette vérification, plusieurs éléments sont présents. Le niveau de **gravité** apparaît ainsi que le titre.



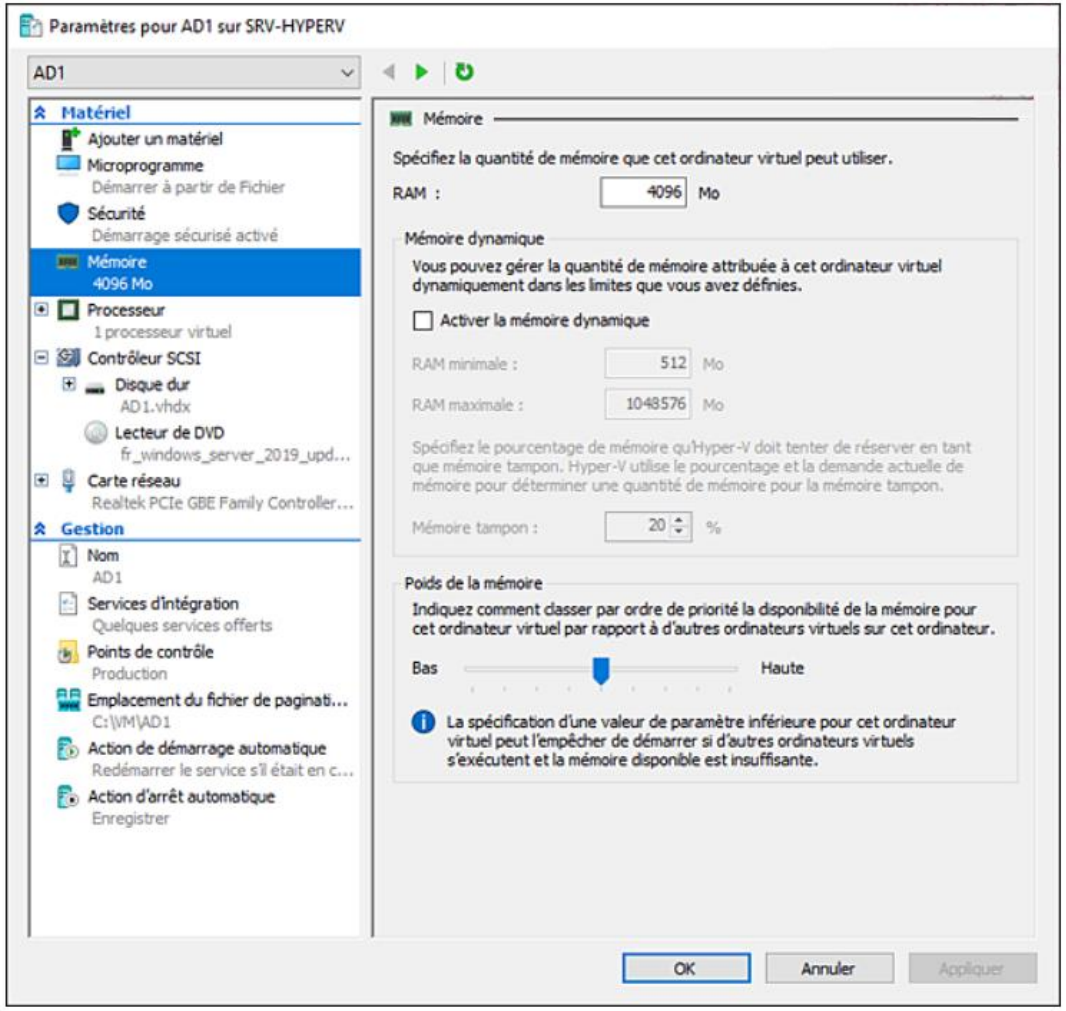
- Lors de la sélection d'un élément, il est possible de connaître l'impact que l'opération à effectuer peut avoir (interruption de service, etc.). Un lien est également présent permettant d'obtenir plus d'informations sur cette bonne pratique.
- Après avoir résolu le problème, relancez l'analyse BPA depuis le menu **TÂCHES**. L'élément doit disparaître.



PARTIE 1

PARTIE 1

- À la sortie de Windows Server 2008, le système de virtualisation Hyper-V permettait d'assigner une quantité de mémoire statique uniquement. Ainsi, le nombre de machines virtuelles s'en trouve réduit. Si un serveur se voit attribuer 4 Go de RAM, la quantité réservée est identique même s'il n'y a aucune activité sur la machine virtuelle.
- La mémoire dynamique permet d'allouer une quantité minimum de mémoire. Néanmoins si la machine virtuelle a besoin de plus de mémoire, elle est autorisée à demander une quantité supplémentaire. Cela ne peut excéder la quantité maximale accordée. Cette fonctionnalité a été introduite dans les systèmes d'exploitation serveurs depuis Windows Server 2008 R2 SP1.
- Il n'est pas recommandé d'utiliser cette fonctionnalité avec certains rôles et logiciels (Exchange par exemple).
- Introduite avec Windows Server 2012, la mémoire tampon est une solution pour l'allocation de la mémoire minimum liée au démarrage de la machine virtuelle. De ce fait le manque de mémoire lors du démarrage d'une VM est comblé par l'utilisation de cette mémoire tampon (*Memory Buffer*). Celle-ci va permettre d'effectuer une allocation de mémoire de manière très rapide



Le disque dur des machines virtuelles

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

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

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

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

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

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

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

- Certaines opérations peuvent être effectuées sur un fichier VHD. Il est par exemple possible de le compacter afin de réduire la taille utilisée ou de le convertir (format VHD en VHDX). Lors de la conversion du disque virtuel, le contenu est alors copié vers le nouveau fichier (par exemple lors de la conversion d'un fichier de type taille fixe en fichier de type taille dynamique). Une fois les données copiées et le nouveau disque mis en place, l'ancien fichier est supprimé.
- D'autres opérations comme la réduction d'un fichier dynamique sont réalisables. Cette option permet de réduire la taille d'un disque si ce dernier n'utilise pas tout l'espace qui lui est affecté. Pour les disques de type taille fixe, il est nécessaire en amont de convertir le fichier VHD en fichier de type dynamique.
- Ces actions peuvent être réalisées à l'aide de l'**Assistant Modification de disque dur virtuel**, option **Modifier le disque...** dans le bandeau **Actions**.
- Il est également possible d'utiliser les cmdlets PowerShell **resize-partition** et **resize-vhd** pour effectuer le compactage d'un disque dur virtuel dynamique

- Un disque de différenciation permet de réduire la taille de stockage nécessaire. En effet, cela consiste à créer un disque parent commun à plusieurs machines et un disque qui contient les modifications (apportées au disque parent), le disque qui contient les modifications étant propre à chaque machine.
- La taille nécessaire au stockage des machines virtuelles s'en trouve donc réduite. Attention, la modification d'un disque parent cause l'échec des liens du disque de différenciation. Il est donc nécessaire par la suite de reconnecter les disques de différenciation en utilisant l'option **Inspecter disque…** dans le bandeau **Actions**.
- Il est possible de créer ce type de disque en utilisant la cmdlet PowerShell **New-VHD**.
- La commande ci-dessous permet la création d'un disque nommé **Differentiel.vhd**, ce dernier utilise un disque parent nommé **Parent.vhd**.

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

Le disque dur des machines virtuelles

Les checkpoints dans Hyper-V

- Un checkpoint correspond à une "photo" de la machine virtuelle au moment où il est effectué. Ce dernier est contenu dans un fichier portant l'extension **avhd** ou **avhx** en fonction du type de fichier de disque dur choisi. Pour effectuer la création, il est nécessaire de sélectionner la machine puis de cliquer sur l'option Checkpoint dans le bandeau Actions.
- Chaque machine peut posséder jusqu'à 50 checkpoints. Si ce dernier est créé lorsque la machine est démarrée, le contenu de la mémoire vive est également intégré dans le fichier. Lors de la restauration d'un checkpoint, il est possible que la machine virtuelle ne puisse plus se connecter au domaine. En effet son application peut avoir pour conséquence de rompre le canal sécurisé entre le contrôleur de domaine et la machine cliente. Il est possible de le réinitialiser en effectuant une nouvelle jonction au domaine ou en utilisant certaines commandes DOS.
- **Attention** cette fonctionnalité ne remplace en aucun cas la sauvegarde, car les fichiers avhd ou avhdx sont stockés sur le même volume que la machine virtuelle. En cas de casse du disque, tous les fichiers sont perdus et il est impossible de les restaurer.

PARTIE 1

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

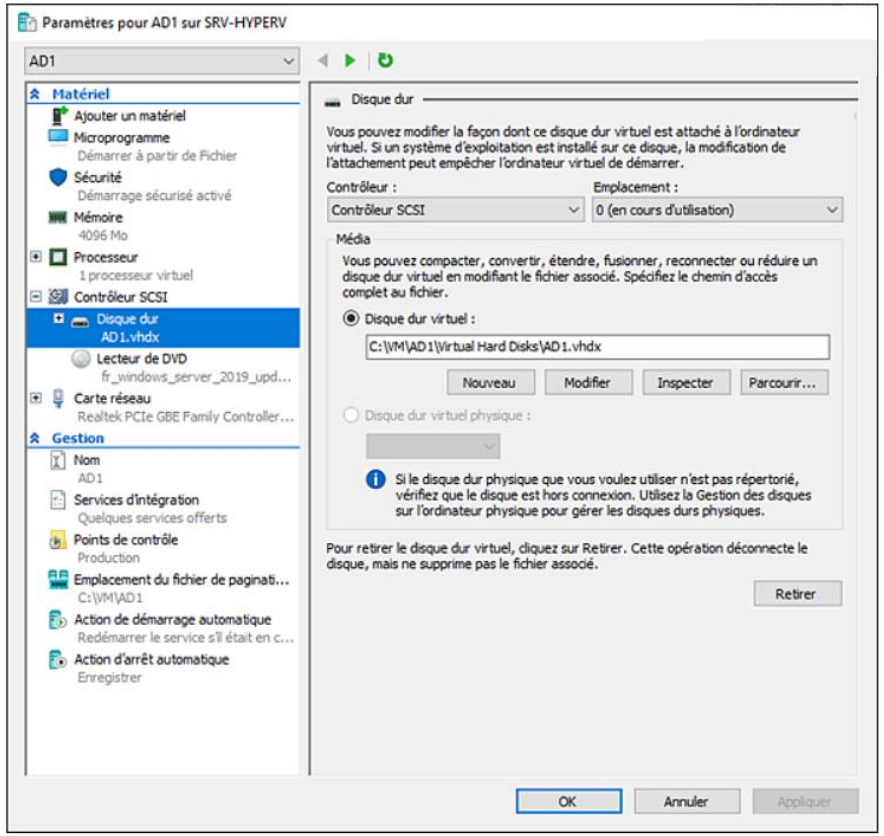
Néanmoins, il est nécessaire de respecter certains prérequis pour la mise en place d'un Guest cluster utilisant des disques virtuels partagés :

- Un cluster à basculement Hyper-V à 2 nœuds.
- Les serveurs exécutent obligatoirement Windows Server 2012 R2 ou version supérieure.
- Les serveurs sont membres du même domaine.
- Le VHDX partagé doit être positionné sur un volume partagée CSV (*Cluster Shared Volume* - Stockage en mode block) ou un SOFS avec SMB 3 (stockage en mode fichier).

Le disque dur des machines virtuelles

Redimensionner la taille d'un VHD à chaud

- La fonctionnalité de redimensionnement d'un fichier VHD a été améliorée afin de pouvoir maintenant être effectuée lorsque la machine virtuelle est en fonctionnement.
- Les administrateurs ont maintenant la possibilité d'effectuer cette opération sans éteindre le serveur et donc sans couper l'accès à une fonctionnalité (Exchange, serveur de fichiers…). Néanmoins la fonctionnalité n'est opérationnelle que pour des fichiers VHDX connectés à un contrôleur SCSI. La taille peut être augmentée ou réduite.
- Pour effectuer cette opération, il est nécessaire de procéder aux actions suivantes :
  - Effectuez un clic droit sur une machine virtuelle puis sélectionnez l'option **Paramètres**.
  - Sélectionnez le disque **.vhdx** de la machine puis cliquez sur **Modifier**.

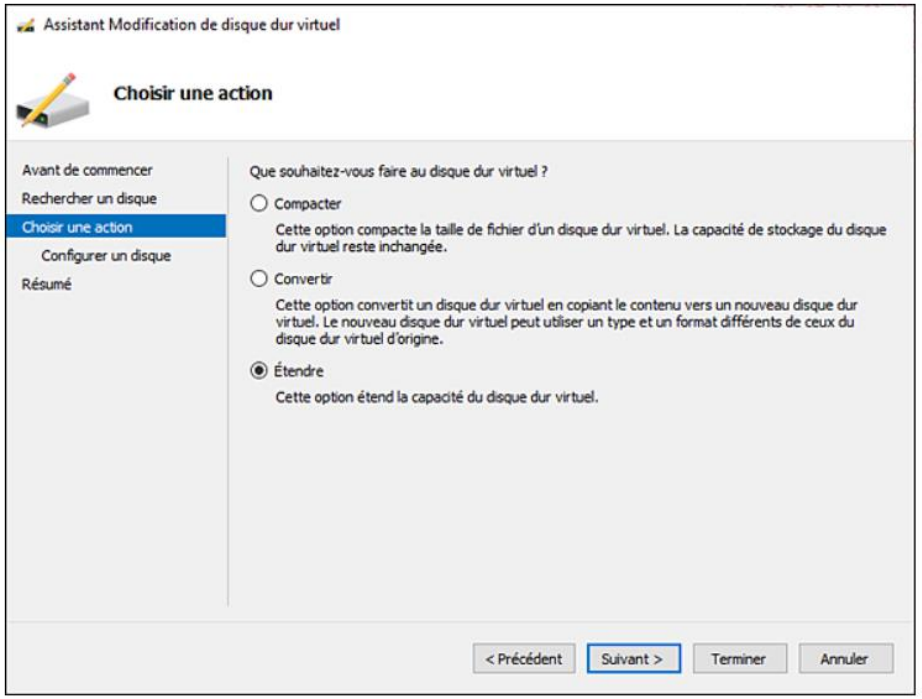


PARTIE 1

Le disque dur des machines virtuelles

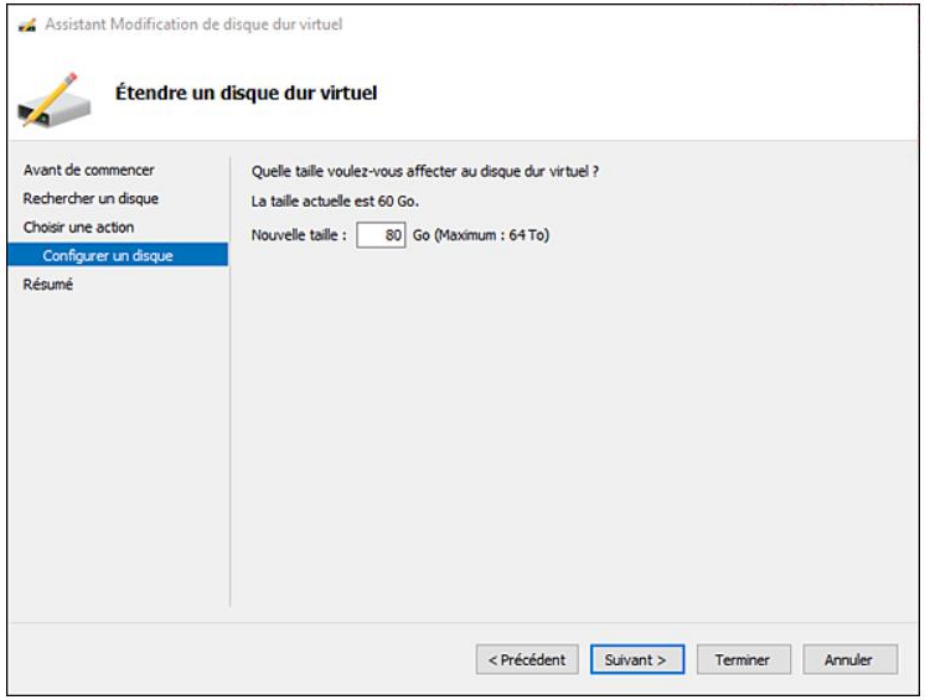
Redimensionner la taille d'un VHD à chaud

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



- Indiquez une taille supérieure à celle actuelle puis cliquez sur **Suivant**.
- Enfin, cliquez sur **Terminer** pour valider l'action.

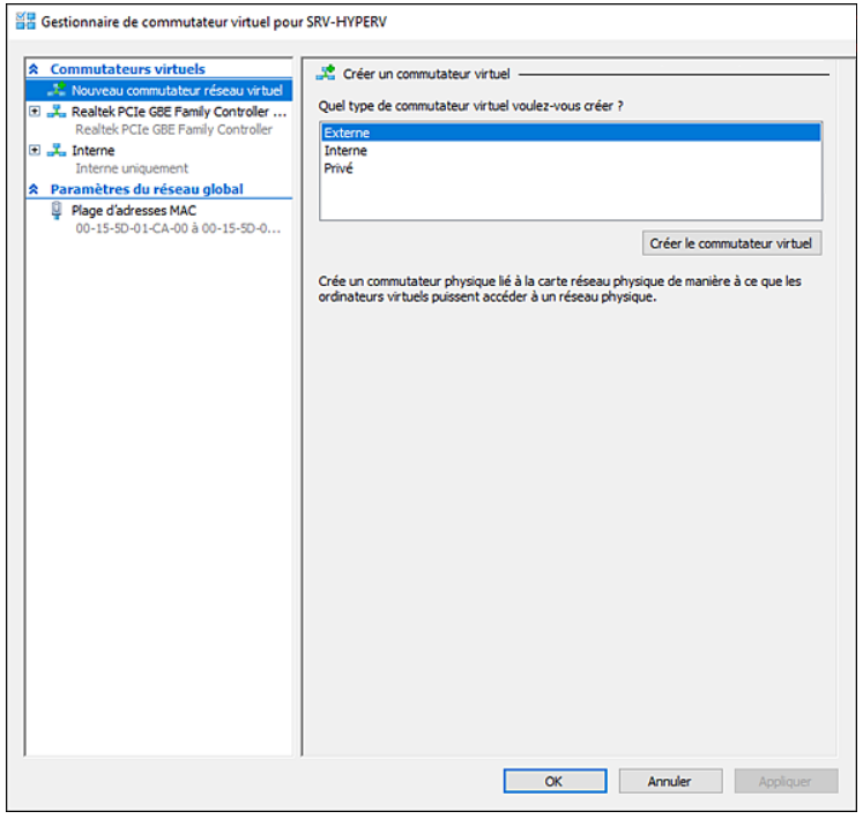
La taille du disque dur virtuel a été étendue alors que la machine était en cours d'exécution.



PARTIE 1

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

- Le principe d'un commutateur virtuel est le même que celui d'un commutateur (switch) physique que l'on peut trouver sur n'importe quel réseau informatique. Connu sous le terme de réseau virtuel avec Windows Server 2008, on parle maintenant de commutateur virtuel. Il est possible de gérer ces derniers en utilisant l'option **Gestionnaire de commutateur virtuel** dans le bandeau **Actions**.
- Trois types de switch peuvent être créés :
  - **Externe** : avec ce type de commutateur virtuel, il est possible d'utiliser la carte réseau de la machine hôte dans la machine virtuelle. Ainsi, cette dernière obtient une connexion sur le réseau physique lui permettant d'accéder à un équipement ou un serveur du réseau de production.
  - **Interne** : permet la création d'un réseau entre la machine physique et les machines virtuelles. Il permet la communication entre les machines virtuelles ainsi qu'avec l'hôte physique qui les héberge. Il n'est pas lié à carte réseau physique, il est donc impossible pour les machines virtuelles d'accéder au réseau local.
  - **Privé** : la communication peut se faire uniquement entre les machines virtuelles, la machine hôte ne peut pas contacter une des VM.

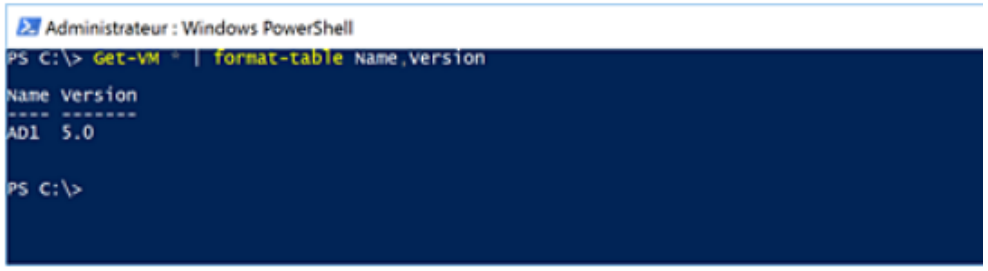


PARTIE 1

Mise à niveau de la version d'une VM

- Les versions Hyper-V sous Windows Server 2012/2012 R2 et Windows Server 2016/2019 utilisent une version des fichiers de configuration de la machine virtuelle différente. Ainsi certaines fonctionnalités offertes par le nouvel hyperviseur peuvent ne pas fonctionner sur la machine importée.
- Les machines virtuelles possédant une version 5 sont compatibles avec des Hyper-V fonctionnant sous Windows Server 2012 R2 et versions supérieures. Ceux possédant une version 8 peuvent pour leur part fonctionner uniquement sur un hyperviseur Windows Server 2016 minimum.
- Les cmdlets PowerShell permettent de connaître la version des machines hébergées. La commande ci-dessous affiche la version de chaque machine virtuelle.

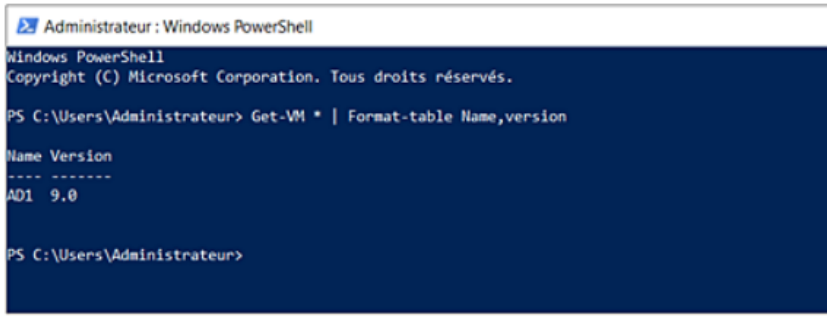
Get-VM * | format-table Name,Version



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

Update-Vm Version vmname

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



- Il est intéressant de noter qu'il est impossible de passer d'une version9 à une version 5

PARTIE 1

Dans les anciennes versions d'Hyper-V, il était impossible de procéder à l'ajout de mémoire à chaud. En effet, cette opération ne pouvait être effectuée qu'après avoir éteint la machine. Dès lors, le service offert (Exchange, serveur de fichiers...) était inaccessible. Windows Server 2016 et 2019 offrent la possibilité de modifier la quantité de mémoire allouée à la machine virtuelle, et ce même si cette dernière est allumée. Il est néanmoins nécessaire d'avoir un hyperviseur sous Windows Server 2016 ou 2019.

Néanmoins, seules les machines virtuelles de génération 2 sont concernées (Windows ou Linux). Dans le cas ci-dessous, la machine virtuelle est de génération 2.

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

Deux nouvelles extensions sont donc utilisées :

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

Dans les anciennes versions d'Hyper-V, il était impossible de procéder à l'ajout de mémoire à chaud. En effet, cette opération ne pouvait être effectuée qu'après avoir éteint la machine. Dès lors, le service offert (Exchange, serveur de fichiers...) était inaccessible. Windows Server 2016 et 2019 offrent la possibilité de modifier la quantité de mémoire allouée à la machine virtuelle, et ce même si cette dernière est allumée. Il est néanmoins nécessaire d'avoir un hyperviseur sous Windows Server 2016 ou 2019.

Néanmoins, seules les machines virtuelles de génération 2 sont concernées (Windows ou Linux). Dans le cas ci-dessous, la machine virtuelle est de génération 2.

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

Deux nouvelles extensions sont donc utilisées :

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

Support des OS Linux

- Hyper-V permet depuis quelques années la virtualisation de systèmes d'exploitation Linux. Les périphériques émulés ou spécifiques sont supportés par Hyper-V pour les machines virtuelles Linux et FreeBSD. Les périphériques émulés offrent l'avantage de ne pas nécessiter de logiciels supplémentaires, néanmoins ils offrent des performances moindres par rapport à une machine virtuelle utilisant des périphériques spécifiques à hyper-V. Il est fortement conseillé d'utiliser ce dernier cas ; les pilotes nécessaires à l'exécution de périphériques spécifiques à Hyper-V sont contenus dans les Linux Integrations Services (LIS) ou FreeBSD Integration Services (BIS). Les services d'intégration Linux sont maintenant intégrés au noyau Linux excepté si vous utilisez une ancienne version de celui-ci (pas de réseau sur la VM dans ce dernier cas). Microsoft met à disposition les différents pilotes nécessaires à la virtualisation d'un OS Linux. Attention toutefois, toutes les distributions Linux ne sont pas prises en compte. Il en est de même concernant les versions de FreeBSD.
- Les distributions Linux supportées sont les suivantes :
  - CentOS, Red Hat Enterprise, Debian, Oracle, Suse, Ubuntu, FreeBSD
- Il est possible depuis Windows Server 2016 de bénéficier du Secure Boot pour les VM sous Linux. Cela nécessite néanmoins d'avoir une machine virtuelle de génération 2. Cette fonctionnalité nécessite d'exécuter la commande PowerShell suivante sur la machine hôte :

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

La fonctionnalité HGS

- **La fonctionnalité HGS** (*Host Guardian Service*) consiste à protéger des machines virtuelles hébergées sur un hôte Hyper-V. Avec cette fonctionnalité, les VM possèdent une protection optimale. Seul le propriétaire de la VM a la possibilité de s'y connecter au travers d'outils de gestion à distance qu'il a activés. Windows Server 2019 apporte des améliorations au niveau de la fonctionnalité HGS.
- Le SGH de secours permet l'utilisation d'une machine virtuelle protégée avec une connectivité intermittente au serveur possédant le rôle Service Guardian hôte. Avec ce mode, il est possible d'ajouter plusieurs URL dans le cas où le primaire HGS ne répond pas. Pour cette option, il est nécessaire d'utiliser deux serveurs Windows Server 2019 ou Windows Server 2016. Les deux serveurs doivent posséder la clé matérielle nécessaire pour effectuer le démarrage de la VM protégée.
- Windows Server 2019 offre en outre le mode Offline. Ce dernier permet le démarrage d'une machine virtuelle même si le service HGS est indisponible. Pour cela, il est nécessaire de s'assurer que la configuration de sécurité de l'hôte Hyper-V n'a pas subi de changement. Une mise en cache spéciale du protecteur de clé est effectuée sur l'hôte Hyper-V. Ce protecteur de clé est crypté avec la configuration de sécurité de l'hôte. Ainsi, même si le service HGS est indisponible, l'hôte Hyper-V peut utiliser le protecteur de clé mis en cache pour démarrer la machine virtuelle. Lors de la modification d'un paramètre de sécurité (désactivation du Secure Boot par exemple), le protecteur de clé mis en cache devient invalide, le service HGS doit dans ce cas être contacté pour démarrer la machine virtuelle.

Snapshot et PowerShell direct

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

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

- Certains prérequis sont néanmoins nécessaires pour pouvoir utiliser la fonctionnalité PowerShell direct. La machine hôte hébergeant le rôle Hyper-V doit exécuter Windows Server 2016/2019 ou Windows 10. La machine virtuelle (machine invitée) doit également exécuter Windows Server 2016/2019 ou Windows 10. Il n'est donc pas possible d'utiliser PowerShell direct sur des systèmes antérieurs à Windows Server 2016/Windows 10.
- **Notez** également que la machine virtuelle doit être en cours d'exécution localement sur l'hôte Hyper-V. Elle doit évidemment être allumée et posséder au moins un profil utilisateur configuré. La fonctionnalité PowerShell direct nécessite au minimum d'avoir un compte possédant le droit administrateur Hyper-V.

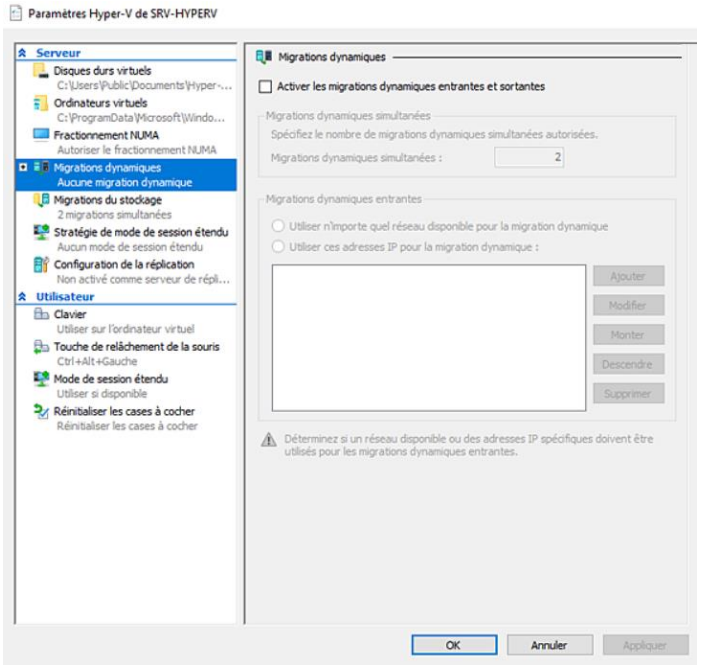
Réplica et live migration

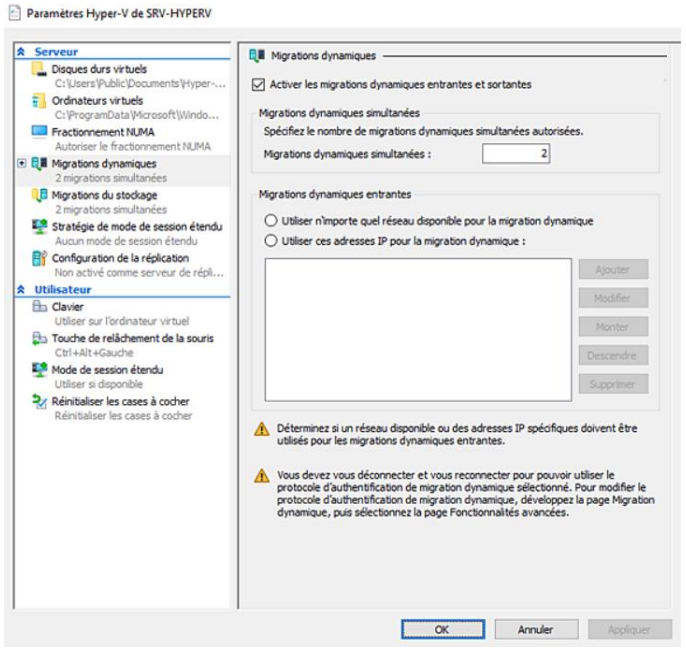
- Le déplacement de machine virtuelle d'un hôte Hyper-V vers un autre hôte Hyper-V est possible depuis plusieurs versions. La fonctionnalité Live Migration est utilisée pour effectuer ce déplacement. Pour pouvoir effectuer cette opération, l'utilisateur doit être membre du groupe Administrateur Hyper-V sur le serveur source et destination. De plus le serveur doit exécuter Windows Server 2012 R2 ou version ultérieure. La fonctionnalité Live Migration doit pour sa part être activée et configurée sur les deux serveurs. Pour pouvoir activer la fonctionnalité, le serveur doit être membre du domaine AD.

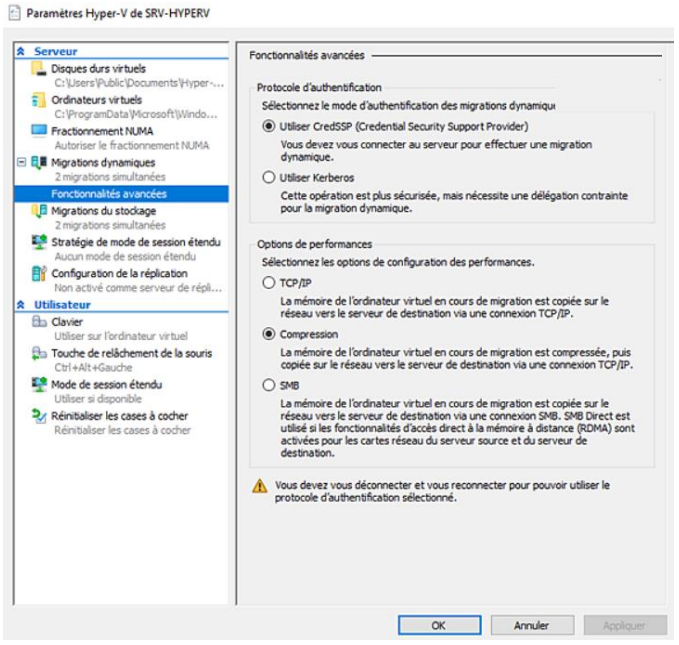
PARTIE 1

Configuration de Live Migration

- Depuis la console **Gestionnaire Hyper-V**, effectuez un clic droit sur le serveur puis cliquez sur **Paramètres Hyper-V** dans le menu contextuel. Dans la fenêtre des paramètres, cliquez sur **Migrations dynamiques**.
- Il est possible dans cette fenêtre de configurer le nombre de migrations dynamiques simultanées ainsi que le réseau à utiliser.
- L'onglet **Fonctionnalités avancées** permet de définir le type d'authentification souhaitée (CredSSP ou Kerberos) ainsi que les options de performances.





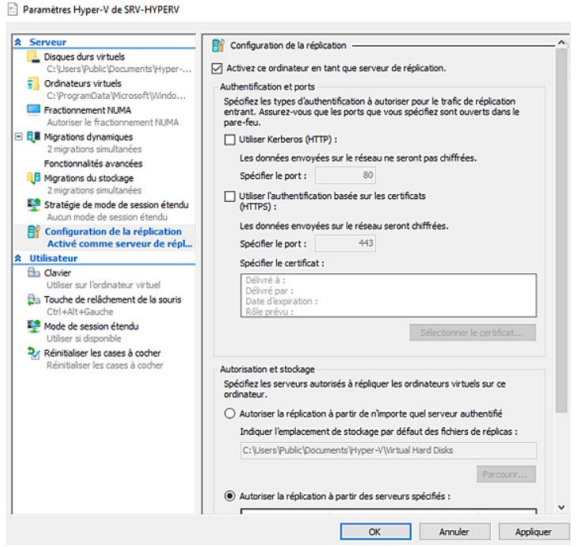


Configuration de Live Migration

- Par la suite, le déplacement peut être opéré à l'aide de la console Hyper-V, en sélectionnant la machine virtuelle puis en choisissant **Déplacer** dans le menu **Actions**. Il est également possible de procéder à la migration d'une machine virtuelle par l'intermédiaire de la commande Powershell :

```
Move-VM LMTest TestServer02 -IncludeStorage -DestinationStoragePath D:\LMTest
```

- Afin d'assurer une haute disponibilité, il est également possible de procéder à la mise en place d'un réplica. Ce dernier consiste à copier la machine virtuelle sur un autre serveur
- **Notez** que les deux serveurs peuvent faire partie du même réseau ou être séparés géographiquement. Il est dans ce cas important de valider que la ligne WAN utilisée est en capacité de supporter l'opération. La réplication peut être effectuée au travers du protocole HTTP ou HTTPS. (distant, …). Celui-ci ne sera utilisé qu'en cas de panne du serveur principal.



PARTIE 1

QUIZ PARTIE 1

https://docs.google.com/forms/d/1IsIBS7uK-OruFFplm4Pglfwh_IWEiCRiBQ8u_o2waYU/prefill

PARTIE 1

Chapitre 2

Console gestionnaire de serveur

Dans ce module, vous allez :

- Le gestionnaire de serveur
- **Serveur en mode installation minimale**
- **Installation de rôles avec une installation en mode core**
- Suppression du groupe de serveurs
- **Les conteneurs**
- Windows admin center

5 heures

Serveur en mode installation minimale

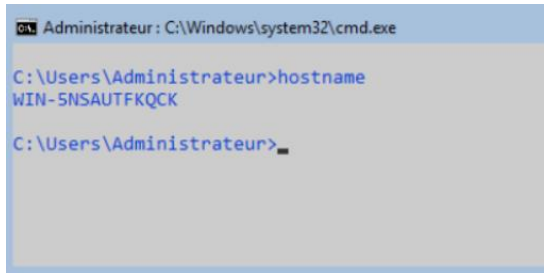
1. mode installation minimale

mode installation minimale

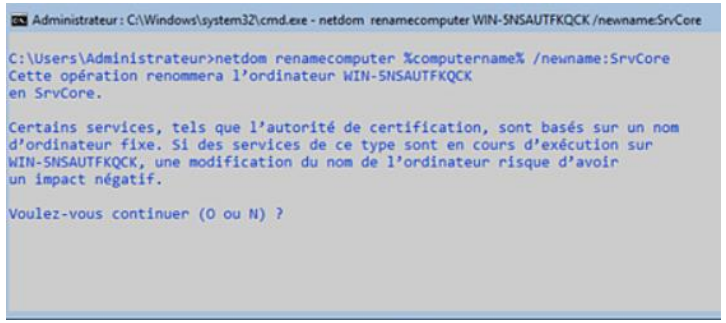
Lorsqu'un serveur est installé en mode **Installation minimale**, le programme **explorer.exe** n'est pas installé. Seule l'invite de commandes est présente.

- Démarrez la machine virtuelle **SRVCore** puis ouvrez une session en tant qu'**administrateur**.
- Saisissez dans l'invite de commandes DOS la commande hostname.

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



- Tapez dans l'invite de commandes DOS netdom renamecomputer %computername% /NewName:SrvCore puis appuyez sur **[Entrée].**
- Saisissez O puis appuyez sur la touche **[Entrée].**
- Redémarrez le serveur à l'aide de la commande shutdown -r -t 0.



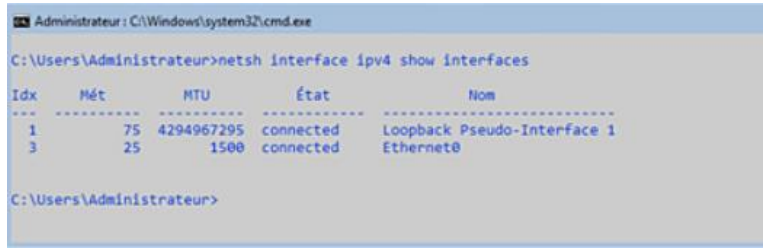
Le commutateur **-r** permet d'effectuer un redémarrage du serveur, **-t 0** indique un redémarrage immédiat.

PARTIE 1

mode installation minimale

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

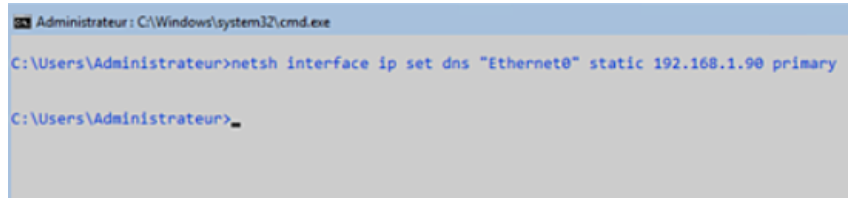
- Saisissez la commande `netsh interface ipv4 show interfaces` puis appuyez sur la touche **[Entrée].**



- Le nom de la carte réseau est **Ethernet0**.
  Configurez la carte réseau à l'aide de la commande : `netsh interface ipv4 set address name="NomCarte" source=static address=192.168.1.93 mask=255.255.255.0 gateway=192.168.1.254`
- Puis validez à l'aide de la touche **[Entrée].**

Remplacez **NomCarte** par le véritable nom de la carte réseau, **Ethernet0** dans notre cas.

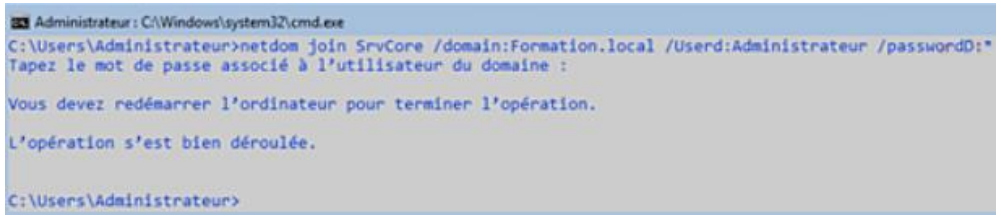
- La carte a été configurée mais l'adresse du serveur DNS n'a pas été renseignée.
  Utilisez la commande `netsh interface ip set dns "NomCarte" static 192.168.1.90 primary` puis validez à l'aide de la touche **[Entrée].**



PARTIE 1

mode installation minimale

- Vérifiez la configuration de la carte à l'aide de la commande ipconfig /all.
  - Il est maintenant possible de joindre le serveur au domaine.
  - Saisissez la commande : netdom join SRVCore /domain:Formation.local /UserD:Administrateur /passwordD:*
  - Puis appuyez sur la touche **[Entrée].**



- La dernière étape est donc le redémarrage afin de prendre en compte la jonction au domaine.
  - Saisissez la commande shutdown -r -t 0.
  - Désactivez le firewall en saisissant la commande netsh firewall set opmode disable.

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

PARTIE 1

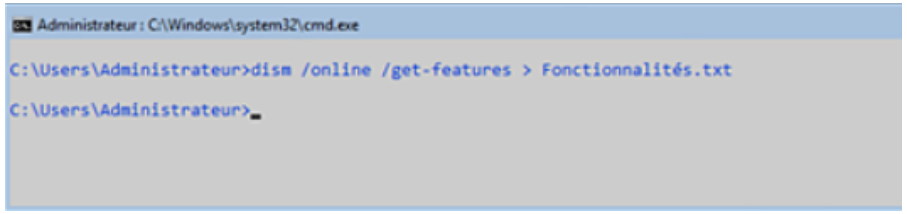
Installation de rôles avec une installation en mode Core

1. **Afficher la liste des rôles et fonctionnalités**
2. **Ajouter un rôle ou une fonctionnalité**
3. **Supprimer un rôle ou une fonctionnalité**

Afficher la liste des rôles et fonctionnalités

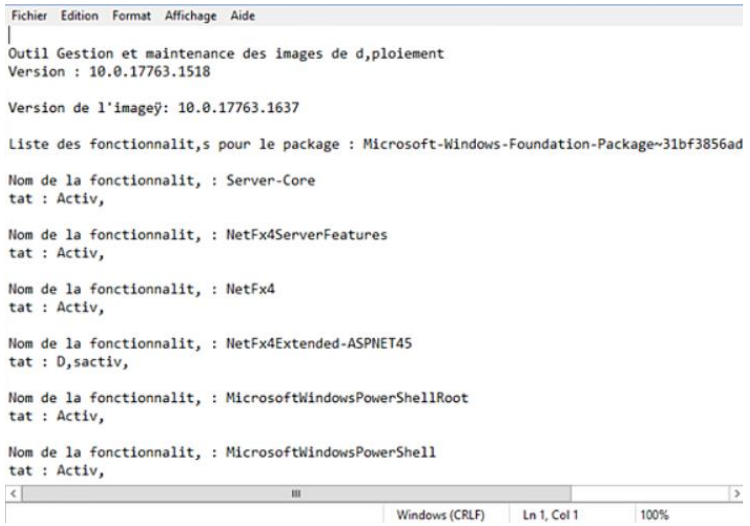
Le serveur ne possède pas d'interface graphique, l'installation doit donc s'effectuer en ligne de commande. Nous allons utiliser la commande dism pour lister, activer ou supprimer une fonctionnalité du système d'exploitation.

- Saisissez dans l'invite de commandes dism /online /get-features > Fonctionnalités.txt puis appuyez sur la touche **[Entrée].**
- Les fonctionnalités disponibles dans le système d'exploitation en cours d'exécution (commutateur /online) sont répertoriées (/get-features). Le résultat est écrit dans le fichier Fonctionnalités.txt.



- Saisissez Notepad **Fonctionnalités.txt** afin d'ouvrir le fichier contenant le résultat.
- Le fichier donne le nom de la fonctionnalité et son état

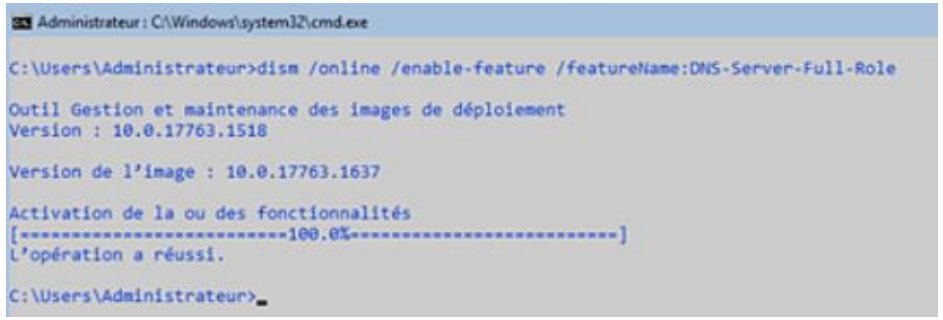
fonctionnalité et état



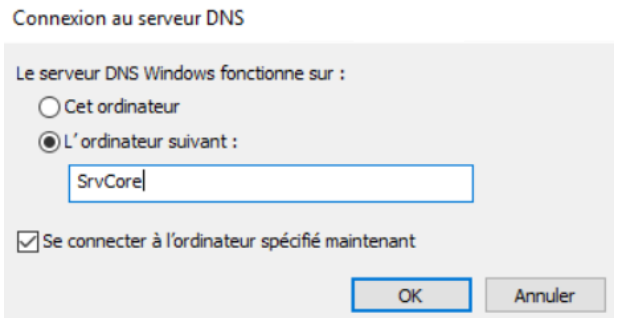
PARTIE 1

Ajouter un rôle ou une fonctionnalité

- L'ajout d'une fonctionnalité s'effectue également avec la commande dism. La première étape est de récupérer le nom de la fonctionnalité qu'il est nécessaire d'installer.
- Le nom du rôle pour serveur DNS est : **DNS-Server-Full-Role**.
- Dans l'invite de commandes, saisissez dism /online /enable-feature /featureName:DNS-Server-Full-Role puis appuyez sur la touche **[Entrée].**



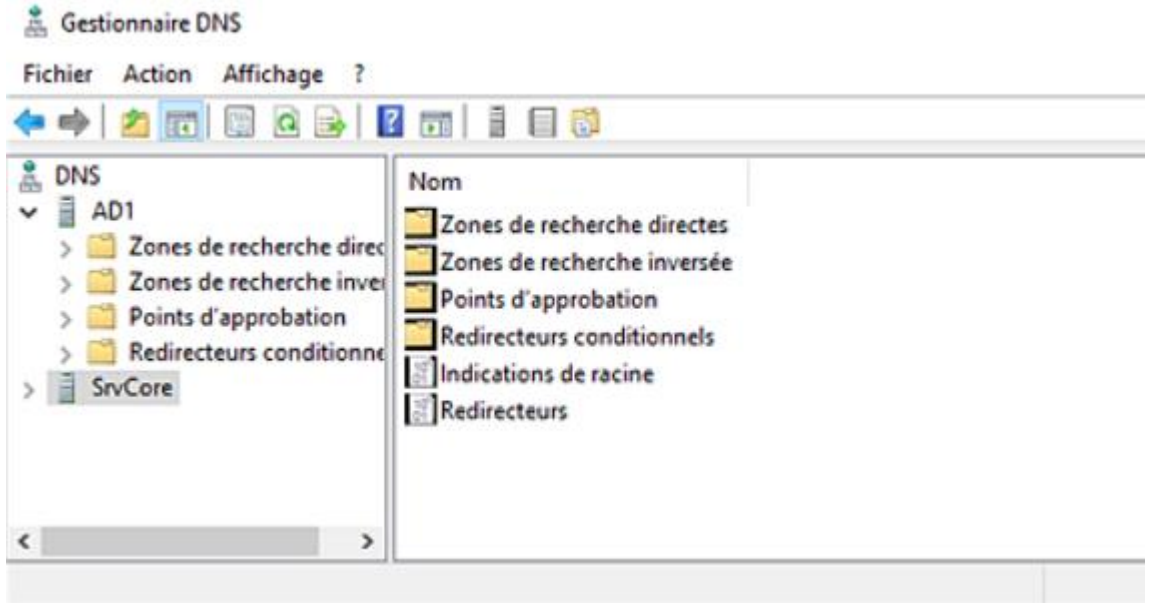
- Lancez la console DNS sur **AD1**.
- Effectuez un clic droit sur **DNS** puis sélectionnez **Établir une connexion au serveur DNS…** dans le menu contextuel.
- Sélectionnez le bouton radio **L'ordinateur suivant :** puis dans le champ saisissez **SrvCore**.
- Cliquez sur **OK**.



PARTIE 1

Ajouter un rôle ou une fonctionnalité

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



- La gestion du serveur DNS installé sur **SrvCore** peut être réalisée à distance.

PARTIE 1

Supprimer un rôle ou une fonctionnalité

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

Sur SrvCore, saisissez la commande dism /online /disable-feature /featureName:DNS-Server-Full-Role puis appuyez sur la touche **[Entrée].**

- Le rôle est maintenant supprimé du serveur.
- Saisissez **Y** puis appuyez sur la touche **[Entrée]** pour redémarrer le serveur.

PARTIE 1

Les conteneurs

1. Présentation
2. **Mise en place**

Présentation

- Conteneur est une fonctionnalité présente depuis Windows Server 2016. Avec cette fonctionnalité, le système d'exploitation est virtualisé.
- Lors de l'exécution d'une application présente dans un conteneur, cette dernière pense s'exécuter sur son propre système. Elle est réellement présente sur le même serveur que les autres applications.
- Les conteneurs sont donc différents de la virtualisation de machine. Dans ce dernier cas, il n'est pas possible d'isoler une application. Si la machine virtuelle héberge trois applications, elles utilisent toutes le même système d'exploitation.
- Avec les conteneurs, l'exécution d'une application s'effectue maintenant sans impacter le système d'exploitation.

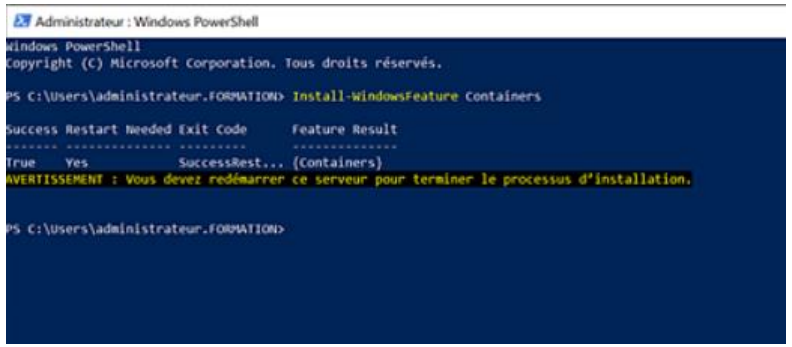
Présentation

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

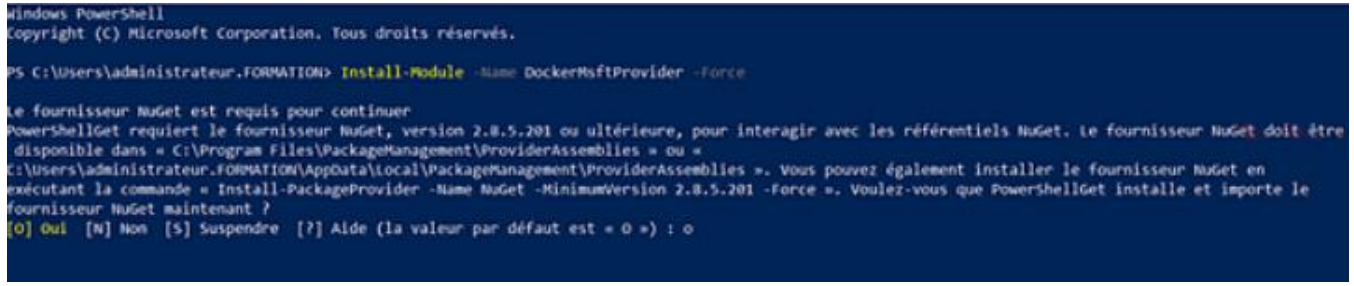
NB : L'administration s'effectue par l'intermédiaire du client Docker ou tout simplement en PowerShell. Le déploiement des applications dans le cloud va s'en trouver facilité.

Mise en place

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



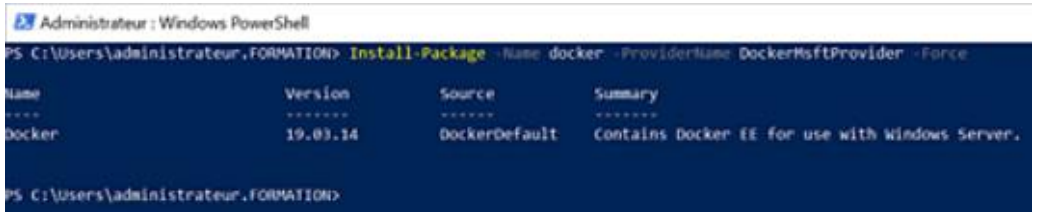
- Redémarrez le serveur à l'aide de la commande shutdown -r -t 0.
- Le module PowerShell nommé **DockerMsftProvider** peut maintenant être installé. Exécutez la commande Install-Module -Name DockerMsftProvider -Force. Saisissez **O** puis appuyez sur la touche **[Entrée].**



PARTIE 1

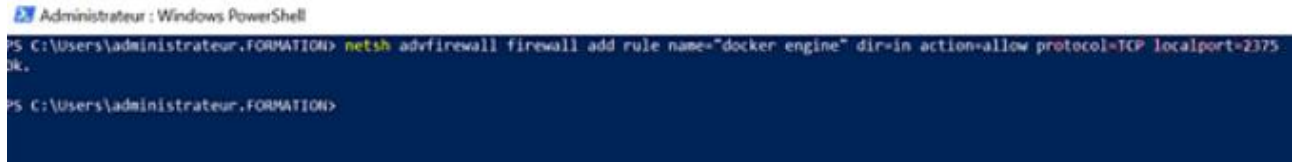
Mise en place

- Il est nécessaire de procéder à l'installation du package. Pour cela, exécutez la commande suivante : Install-Package -Name docker -ProviderName DockerMsftProvider -Force.



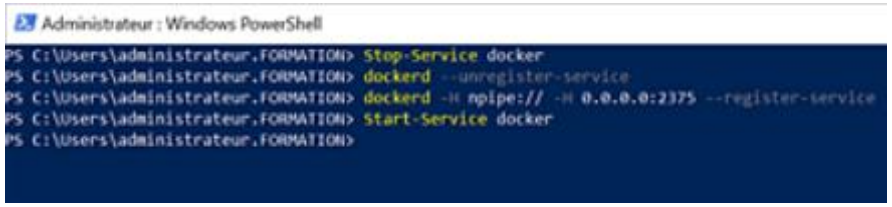
- Une configuration du pare-feu est nécessaire. Utilisez la commande Netsh pour procéder à la configuration.

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



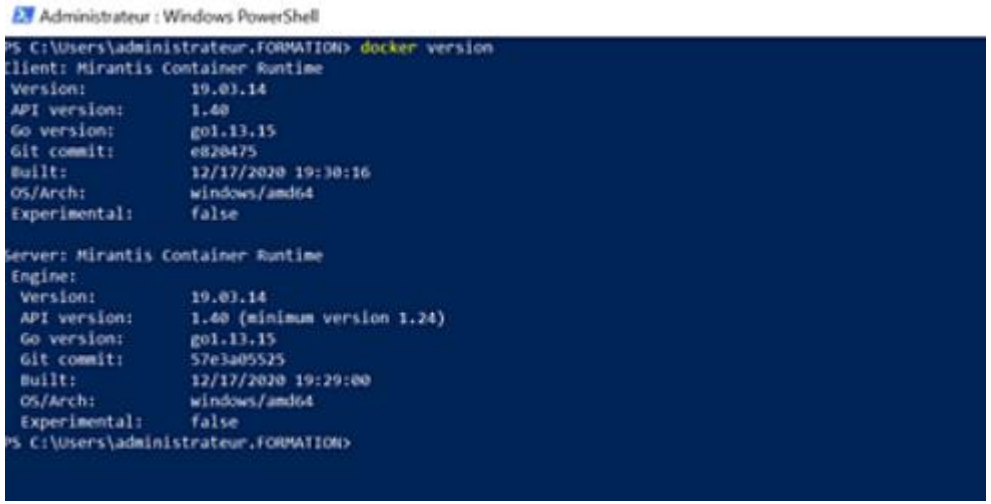
- La configuration du service Docker (démon) peut maintenant être effectuée. Cette opération s'effectue à l'aide des commandes ci-dessous. Il est nécessaire de stopper le service puis de configurer le démon pour une écoute sur Pipe et TCP. Enfin, le service est par la suite redémarré.

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



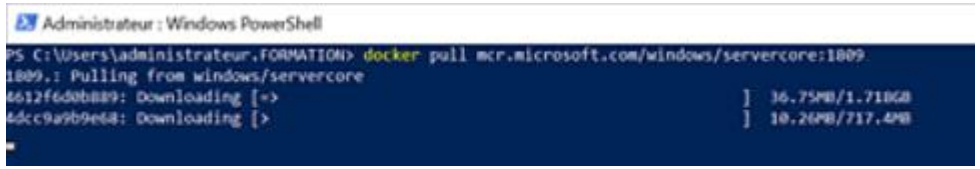
Mise en place

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

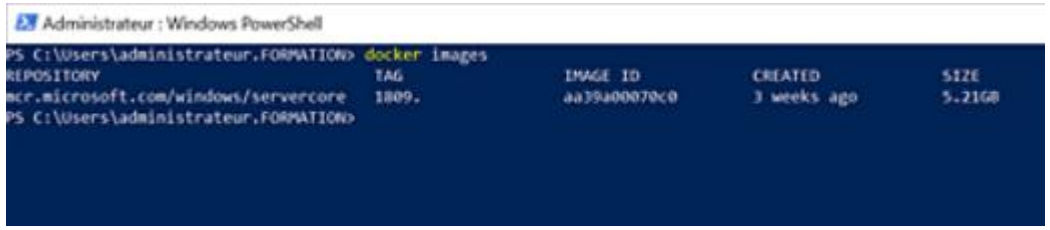


- L'image de base peut désormais être récupérée à l'aide de la commande

docker pull mcr.microsoft.com/windows/servercore:1809.



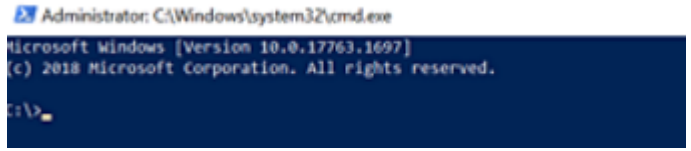
- Les images peuvent être visualisées à l'aide de la commande docker images.



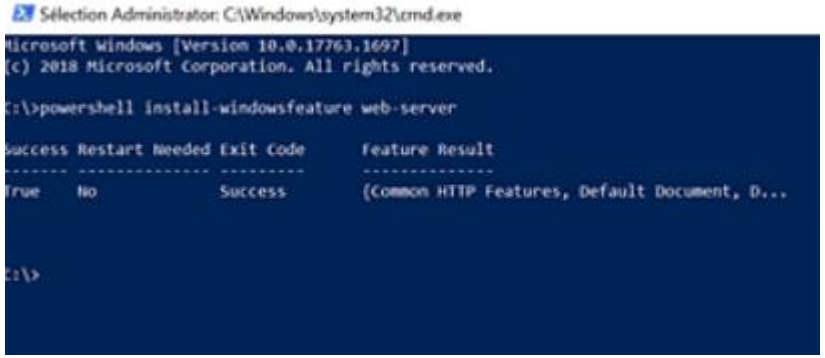
PARTIE 1

Mise en place

- Le conteneur peut maintenant être créé. Exécutez la commande : docker run --name website -it mcr.microsoft.com/windows/servercore:1809 cmd.
- Une console s'affiche.



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

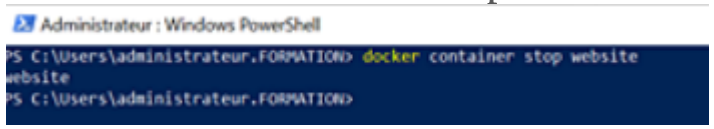


- IIS est maintenant installé ; l'image peut être créée depuis ce conteneur. Ceci permettra de créer des conteneurs avec IIS préinstallé.
- Saisissez la commande Exit pour revenir à la console DOS.
- Vérifiez que le conteneur est toujours démarré en saisissant la commande docker container ls. Si aucun conteneur n'est présent, exécutez la commande docker container start website.

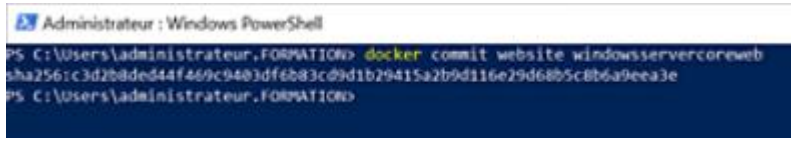
PARTIE 1

Mise en place

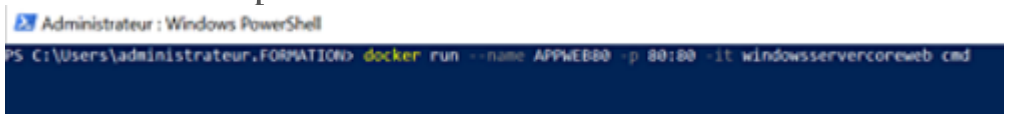
- Exécutez la commande docker container stop website, ceci permet de procéder à l'arrêt du conteneur.



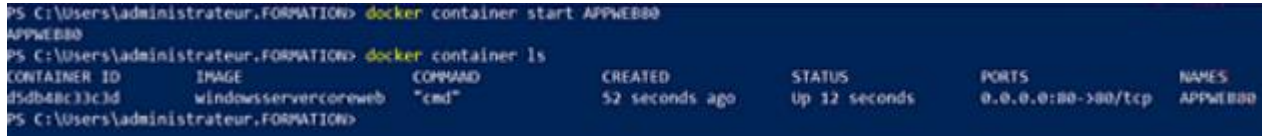
- Exécutez docker commit website windowsservercoreweb pour effectuer la création de l'image.



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



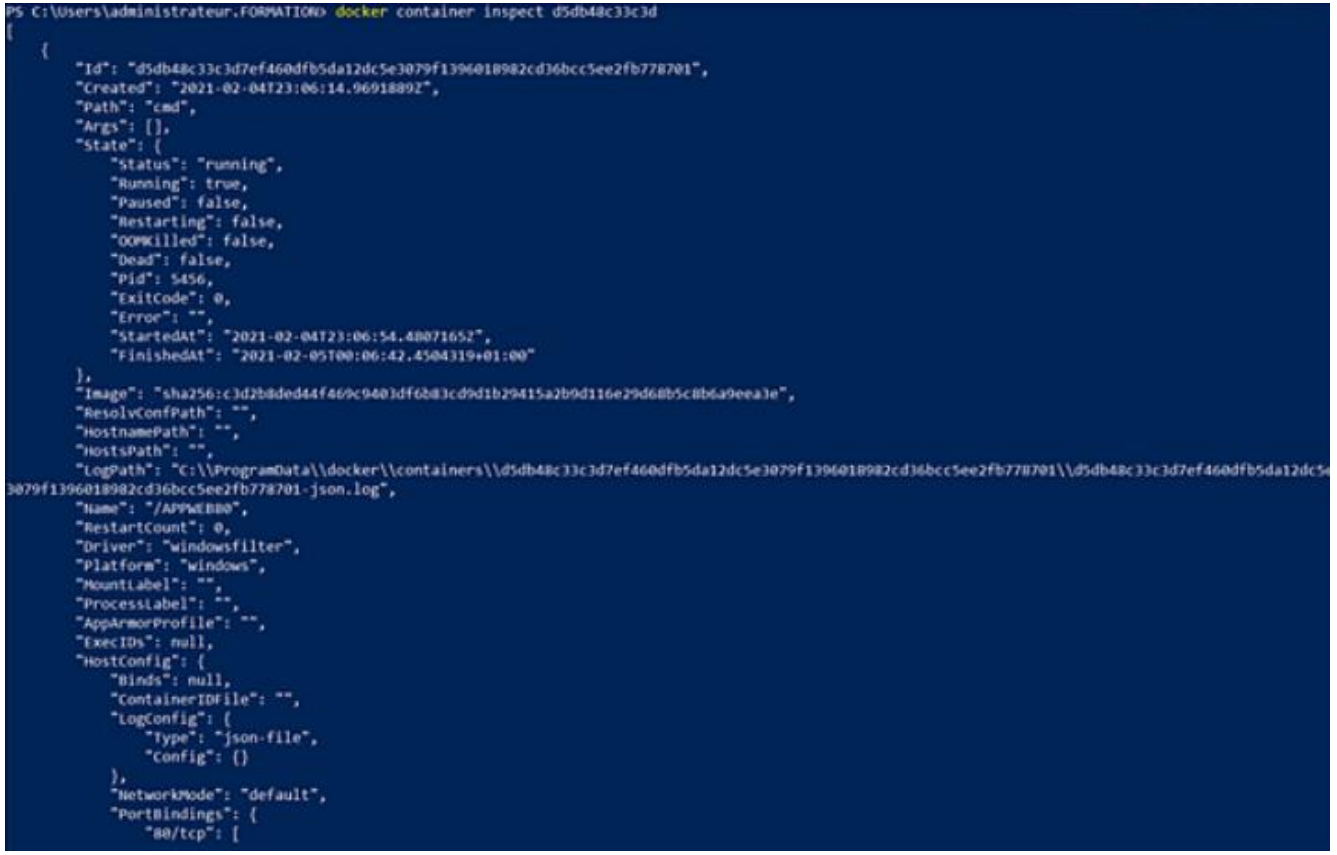
- Le nouveau conteneur est maintenant en place et peut être utilisé.
- Exécutez la commande Exit puis docker container start APPWEB80. Récupérez l'ID du conteneur à l'aide de la commande docker container ls.



PARTIE 1

Mise en place

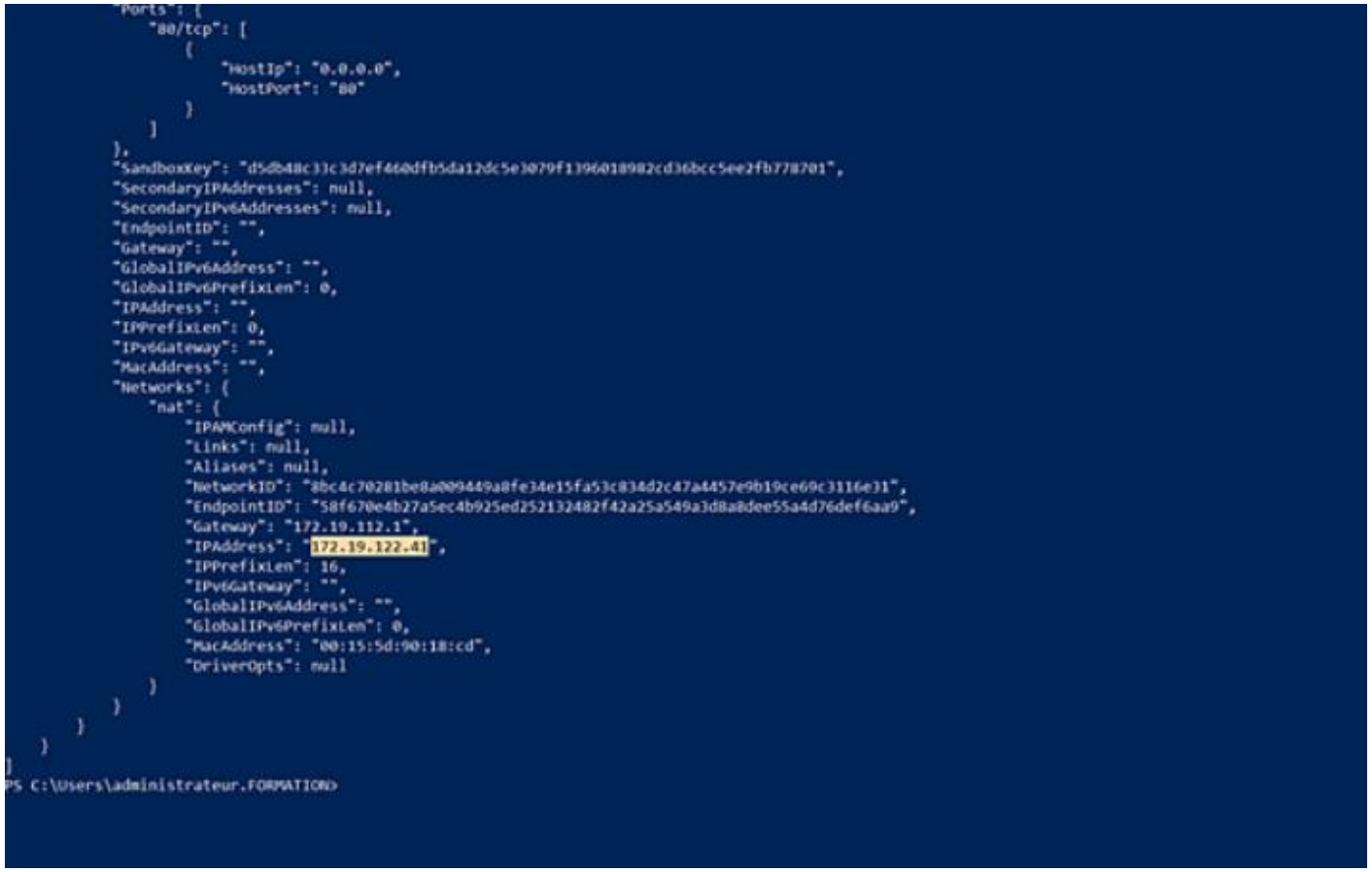
- Une fois récupéré l'ID du conteneur utilisant l'image Windowsservercoreweb, exécutez la commande docker container inspect IDContainer.



PARTIE 1

Mise en place

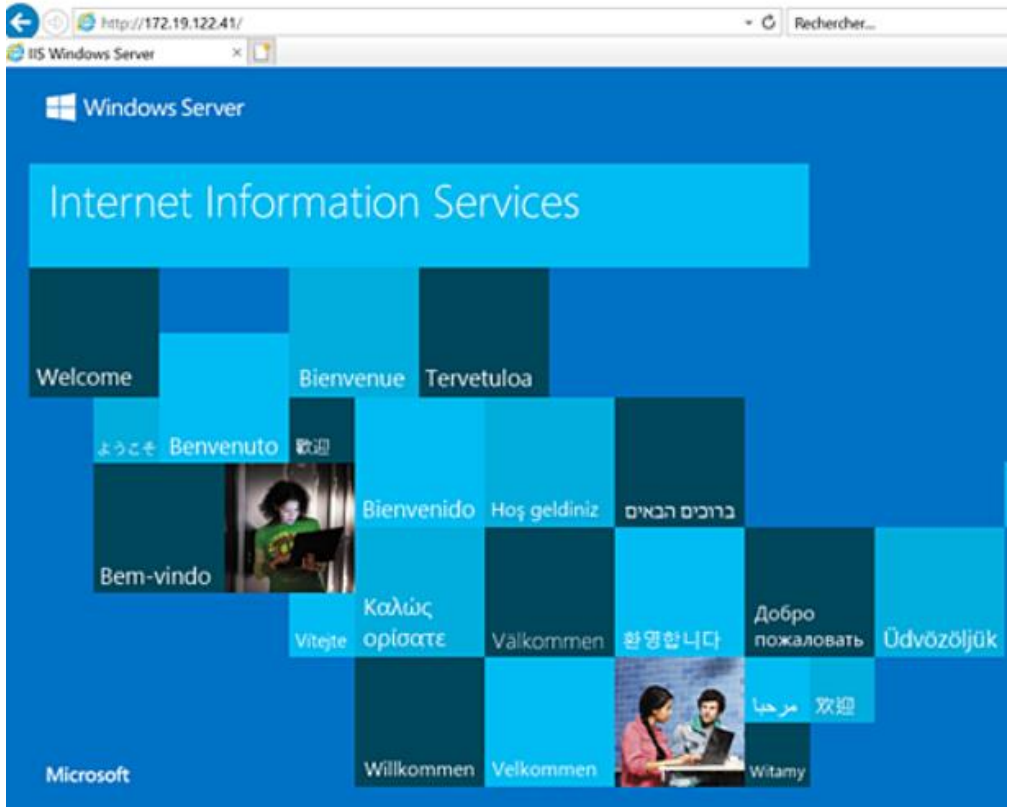
La catégorie Networks contient l'adresse IP du conteneur.



PARTIE 1

Mise en place

En utilisant l'adresse IP, l'accès au serveur web peut être effectué.



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

PARTIE 1

Chapitre 3

Service de domaine Active Directory

Dans ce module, vous allez :

1. Comprendre les services de l'Active Directory
2. Mise en place d'un contrôleur de domaine
3. Redémarrage de l'AD
4. Mise à niveau d’un contrôleur de domaine D'une ancienne version
5. Cloner un contrôleur de domaine virtualisé
6. **Manipuler Azure Active Directory**

15 heures

Manipuler Azure Active Directory

Ce que vous allez apprendre dans ce chapitre :

1. Fonctionnalités offertes par Azure AD
2. **Synchronisation d'un annuaire local**
3. **Authentification forte dans Azure**
4. Le portail web Self-Service
5. Mise en place de Hybrid AD Join

Azure Active Directory

- Cette section du chapitre traitant d'Active Directory présente la partie Azure Active Directory. il est nécessaire de créer un compte démo sur le portail d'Azure puis d'activer la version d'évaluation d'Azure AD Premium.
- La plateforme Azure offre de nombreuses fonctionnalités dont la possibilité d'utiliser un annuaire Active Directory. Il permet ainsi la gestion des identités pour toutes les activités dans le cloud (accès aux applications SAAS…).
- Généralement synchronisé avec un annuaire *on-premises* (présent dans le réseau local de l'entreprise), il offre également la possibilité de procéder à la création de comptes utilisateurs et groupes depuis l'interface web.
- Documentation des différentes versions :

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

- Azure AD est utilisé par des services en ligne tels que Office 365 ou Intune pour l'autorisation d'accès au service. La fonctionnalité d'authentification forte vient compléter la gestion des identités. Il est en effet possible d'activer pour certains utilisateurs l'obligation d'utiliser une authentification à deux facteurs (authentification forte).
- En plus de leur couple login/mot de passe, une partie ou l'ensemble des utilisateurs devront utiliser un deuxième mécanisme d'authentification. Ce dernier peut être une application installée sur un smartphone qui fournit un code. Celui-ci possède une durée de vie très courte. Il est également possible de recevoir un SMS contenant un code à saisir. La troisième solution va consister à valider son identité par la réception d'un appel téléphonique et la pression d'une touche du téléphone. Microsoft recommande pour des raisons de sécurité l'utilisation de l'application Microsoft Authentificator en lieu et place des solutions Telecoms (SMS, appel).
- L'édition Premium offre un portail web permettant la mise en place de délégation. Il est ainsi possible de permettre aux utilisateurs d'effectuer le changement de mot de passe ou la création de groupes d'utilisateurs.
- Avec Windows 10, une entreprise peut intégrer les postes directement dans l'annuaire Azure AD, et ce, même si la machine est déjà jointe à un domaine Active Directory (Hybrid AD Join).
- Les étapes permettant d'intégrer des postes Windows 10 à Azure AD sont détaillées plus loin dans ce chapitre. Le sujet jonction Azure AD Join (pas de jonction à un annuaire Active Directory) est également traité sur le blog de l'auteur : http://www.nibonnet.fr/?p=1169.
- Le portail Azure AD est accessible depuis l'URL https://aad.portal.azure.com.

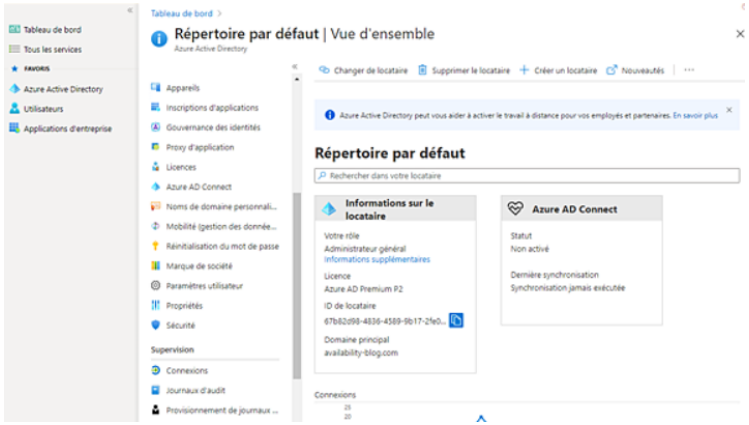
Manipuler Azure Active Directory

Synchronisation d'un annuaire local

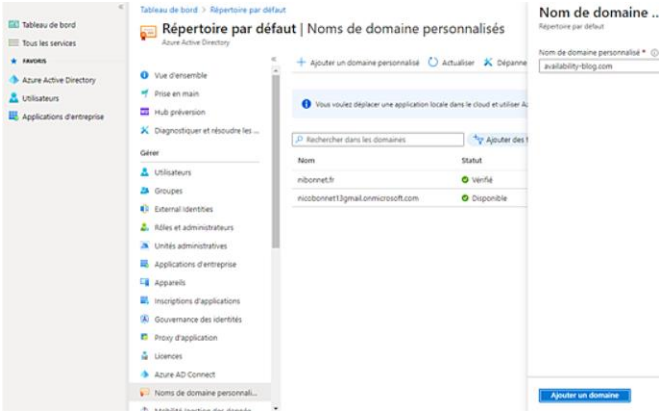
PARTIE 1

- Il est intéressant de synchroniser un annuaire AD avec Azure Active Directory. Ceci permet d'assurer l'authentification unique dans le réseau local ou depuis un équipement mobile (ordinateur portable, smartphone). Ainsi l'utilisateur utilisera son login/mot de passe pour accéder aux ressources présentes dans Azure ou en interne.
- Avant de pouvoir synchroniser l'annuaire Active Directory, il est nécessaire d'ajouter le nom de domaine à utiliser.
- Depuis le portail Azure Active Directory (https://aad.portal.azure.com), accédez à la fonctionnalité Azure Active Directory en cliquant dessus sur le bandeau de gauche.

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

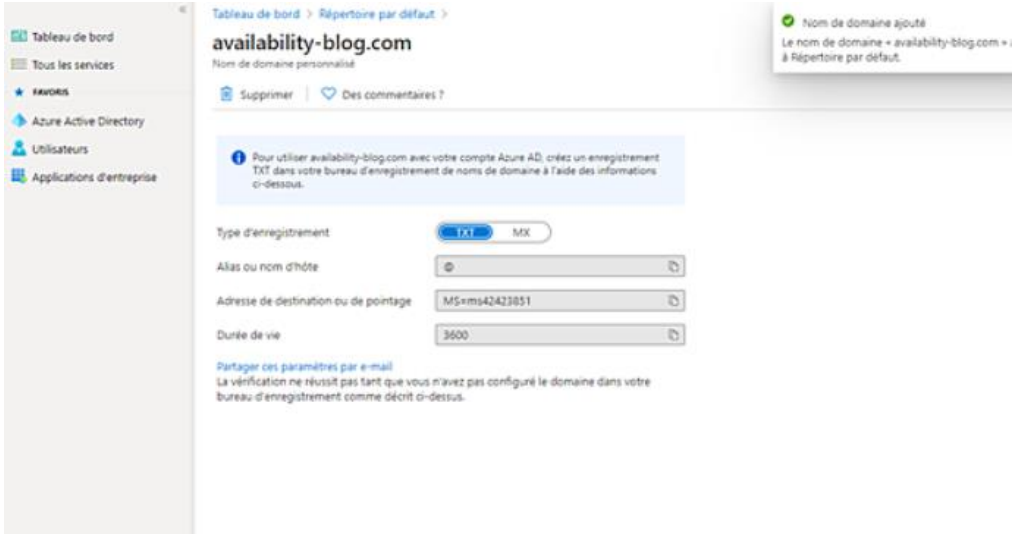


- Cliquez sur **Ajouter un domaine personnalisé** puis ajoutez le nom de domaine. Cliquez ensuite sur le bouton **Ajouter un domaine**.

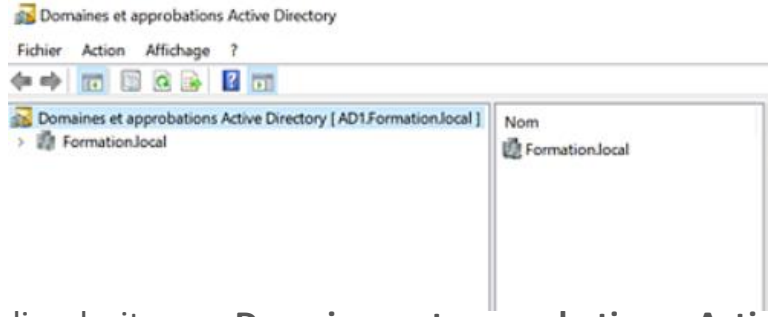


- Il est nécessaire de procéder à l'ajout d'un enregistrement dans le DNS de la zone afin d'effectuer à la vérification du nom de domaine. Suite à l'ajout, la valeur de l'enregistrement TXT est donnée, l'opération d'ajout s'effectuera dans le DNS de votre register.

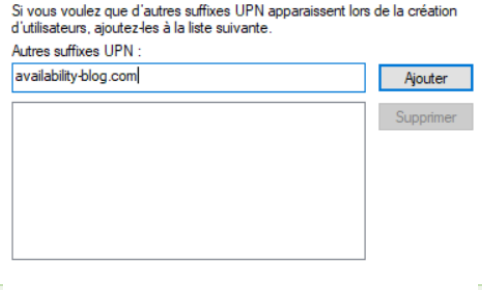
Après avoir ajouté l'enregistrement, cliquez sur le bouton **Vérifier**.



- L'UPN (*User Principal Name*) des comptes utilisateurs à synchroniser peut maintenant être modifié. Il est nécessaire dans un premier temps de procéder à l'ajout du nom de domaine précédemment ajouté à Azure.
- Depuis le contrôleur de domaine, accédez à la console **Domaines et approbations Active Directory**.



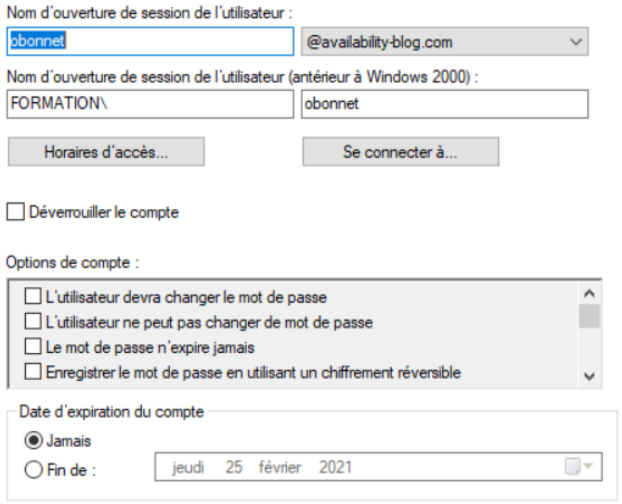
- Effectuez un clic droit sur **Domaines et approbations Active Directory** puis cliquez sur **Propriétés**. Ajoutez le nom de domaine puis cliquez sur **Ajouter**. Validez la modification à l'aide du bouton **OK**.



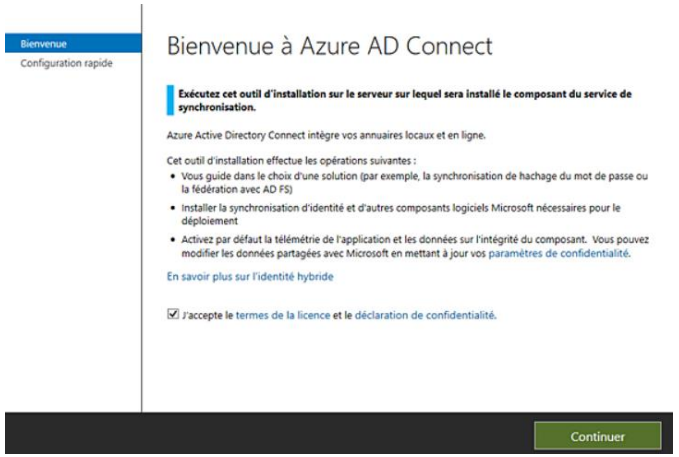
PARTIE 1

PARTIE 1

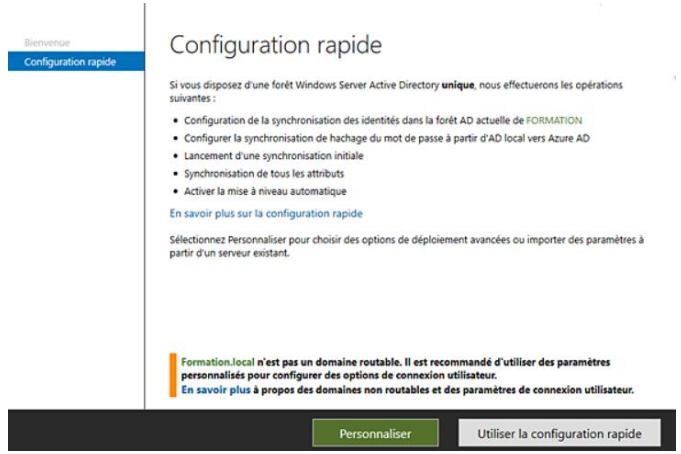
- L'UPN peut maintenant être attribué aux utilisateurs qui doivent être synchronisés. La synchronisation va être opérée par unité d'organisation. Cette dernière permet de limiter la synchronisation AD / Azure AD.



- La synchronisation peut maintenant être effectuée. Cette opération se réalise à l'aide de l'outil Azure AD Connect présent à l'adresse ci-dessous : https://www.microsoft.com/en-us/download/details.aspx?id=47594
- Une fois installé sur un serveur membre, un assistant se lance. Acceptez la licence puis cliquez sur **Continuer**.

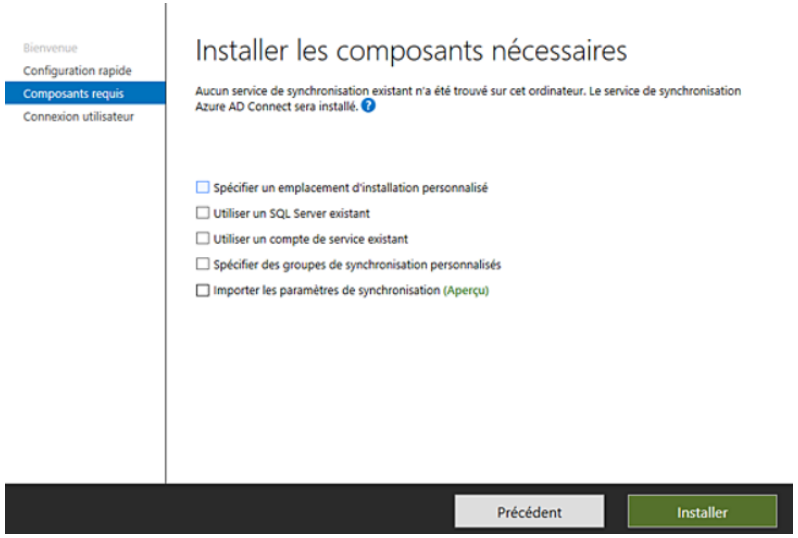


- Le bouton **Personnaliser** va permettre de personnaliser l'installation, il est donc intéressant d'utiliser ce type d'installation.

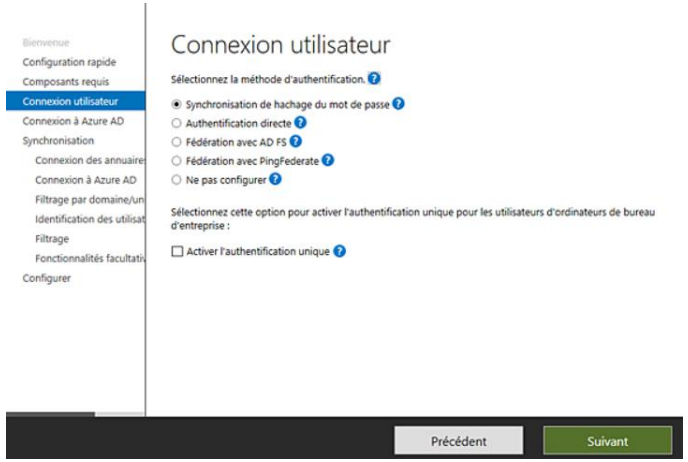


PARTIE 1

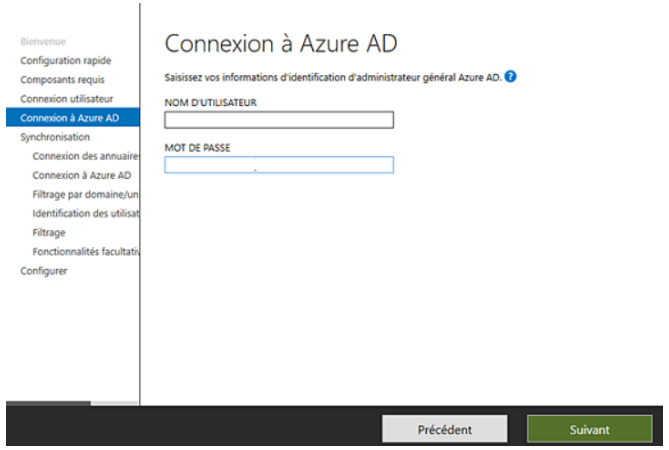
- La fenêtre suivante permet l'utilisation d'une base de données SQL particulière ainsi que d'autres options d'installation. Le bouton **Installer** permet de procéder à l'installation des différents composants.



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

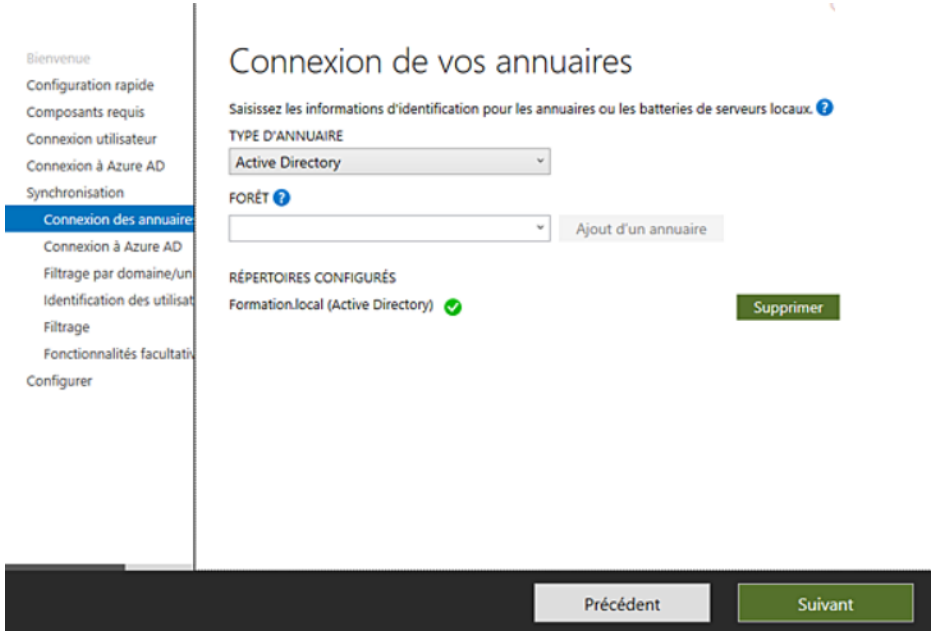


- Il est nécessaire de saisir les identifiants d'un compte possédant des droits d'administrateur au niveau de l'annuaire Azure AD.

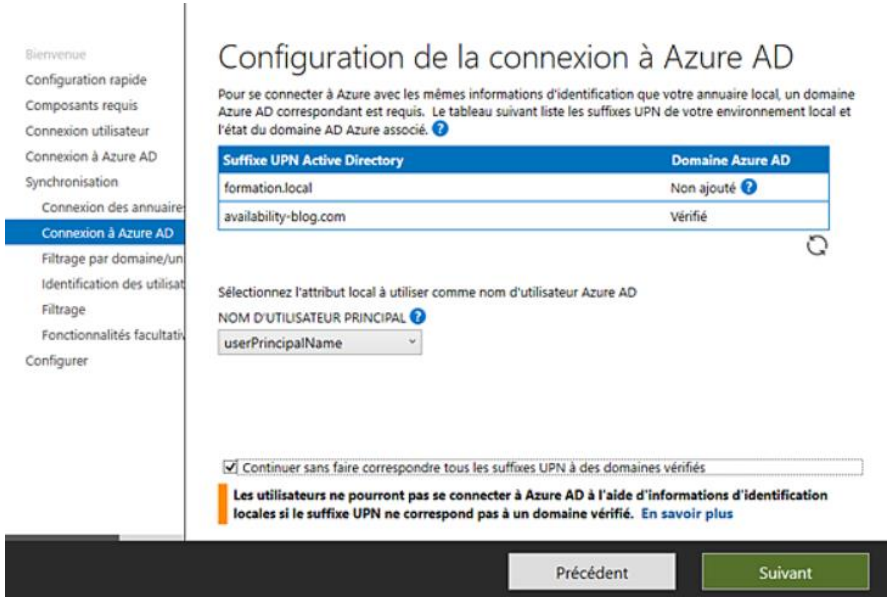


PARTIE 1

- AAprès la validation des identifiants Azure AD, il est nécessaire de cliquer sur **Ajout d'un annuaire** puis, dans la fenêtre qui s'affiche, de saisir les identifiants de l'annuaire local (sous la forme domaine\compte). Il est nécessaire d'utiliser un compte utilisateur ne possédant pas de droit d'administration (admins du domaine…). L'utilisation d'un compte Administrateur n'est plus autorisé. Une configuration supplémentaire devra être effectuée au niveau de l'ACL du domaine.

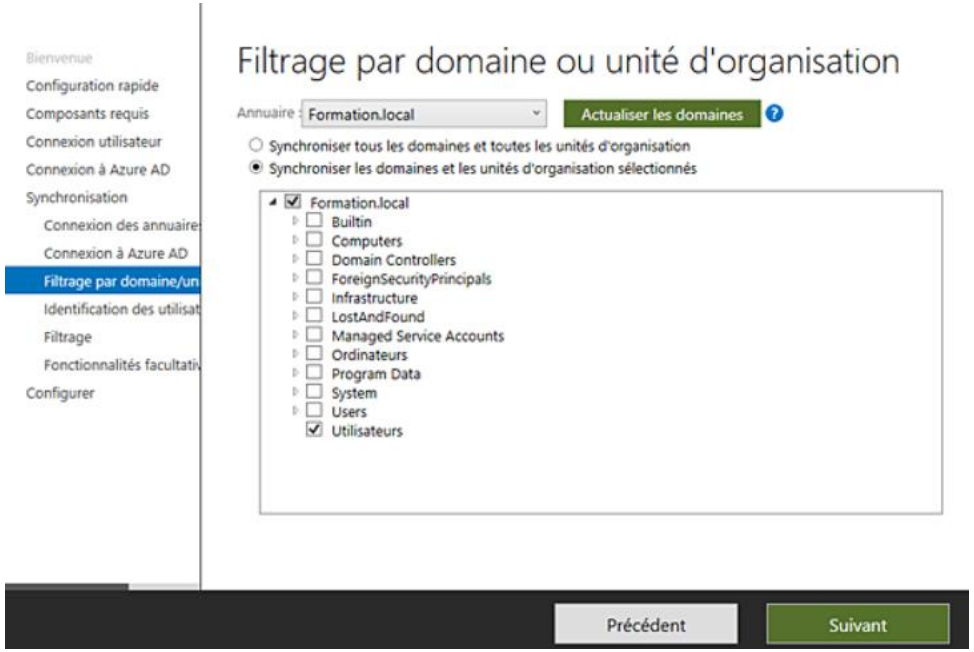


L'attribut local à utiliser est l'UPN (*User Principal Name*). Cochez **Continuer sans faire correspondre tous les sufffixes UPN à des domaines vérifiés** puis cliquez sur **Suivant**. En effet l'UPN Formation.local propre à l'annuaire Active Directory n'est pas présent dans Azure AD.



PARTIE 1

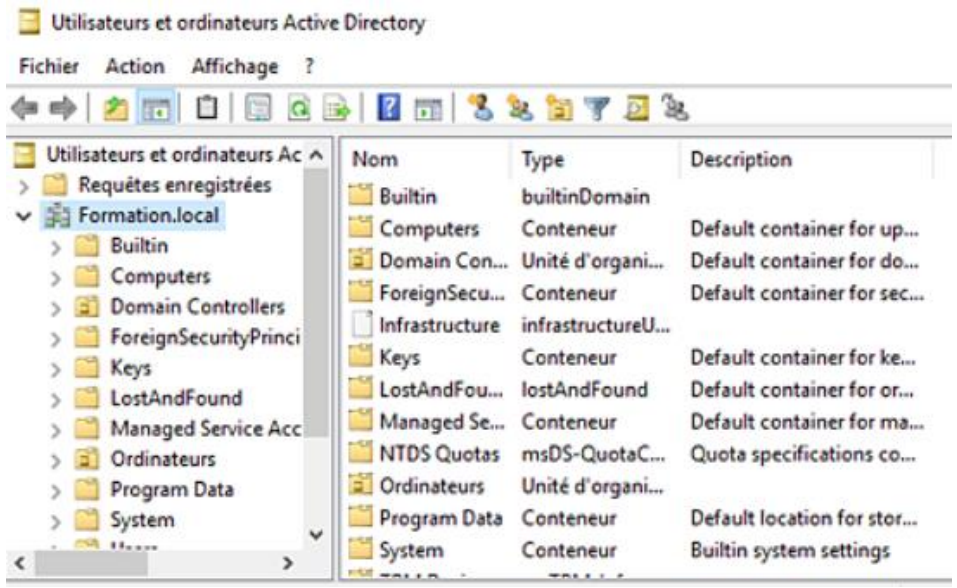
Cliquez sur **Synchroniser les domaines et les unités d'organisations sélectionnés** puis sélectionnez uniquement les unités d'organisations qui doivent être sélectionnées.



Les fenêtres suivantes peuvent être validées sans apporter de modifications. La synchronisation est maintenant fonctionnelle et s'opère toutes les 30 minutes.

Suite à la configuration, le compte utilisateur doit se voir octroyer des autorisations au niveau de la racine du domaine. Ces autorisations permettent d'effectuer la synchronisation des mots de passe.

- Depuis la console **Utilisateurs et ordinateurs Active Directory**, cliquez sur **Affichage** puis sur **Fonctionnalités avancées**.



- Effectuez un clic droit sur la racine du domaine (Formation.local ici) puis accédez aux propriétés. Cliquez sur **Sécurité** puis **Ajouter**.
- Ajoutez le compte utilisateur utilisé puis autoriser les droits **Réplication de toutes les modifications de l'annuaire** et **Réplication des changements de répertoire**.

Cliquez sur **OK**. Lors de la prochaine synchronisation, le hash des mots de passe sera répliqué. Il est également possible de forcer cette synchronisation à l'aide de la commande

```
Start-AdSyncSyncCycle -policytype delta.
```

Cette Cmdlet PowerShell doit être exécutée sur le serveur Azure Ad Connect.

PARTIE 1

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

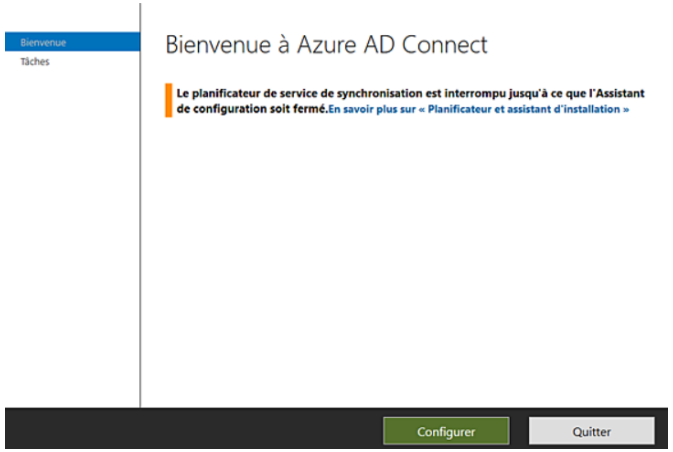
Cette fonctionnalité offre l'avantage de ne plus avoir à saisir de mot de passe pour un utilisateur déjà authentifié par les contrôleurs de domaine interne de l'entreprise.

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

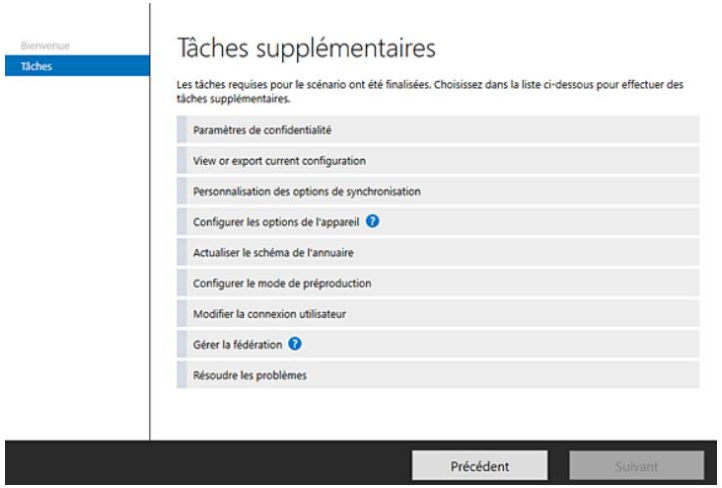
La fonctionnalité s'active par l'intermédiaire de Azure AD Connect et ne nécessite pas de logiciel ou utilitaire supplémentaire.

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

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

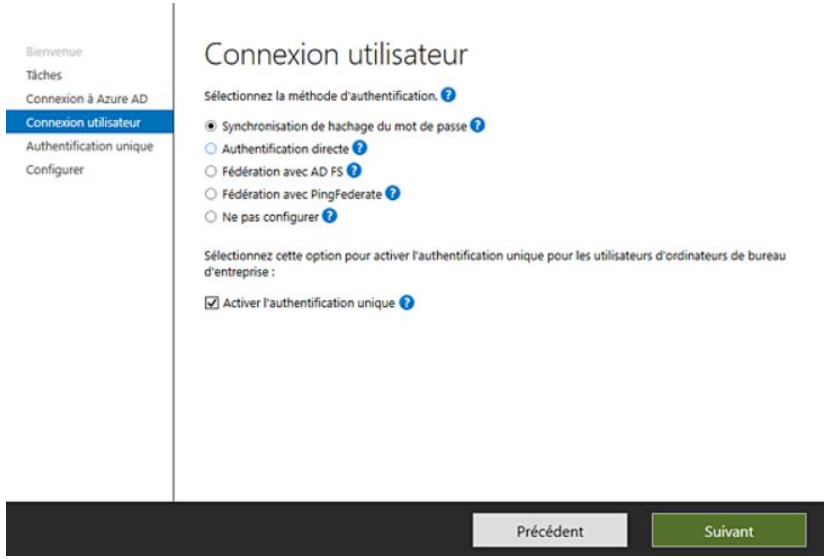


Cliquez sur **Modifier la connexion utilisateur** puis cliquez sur **Suivant**.

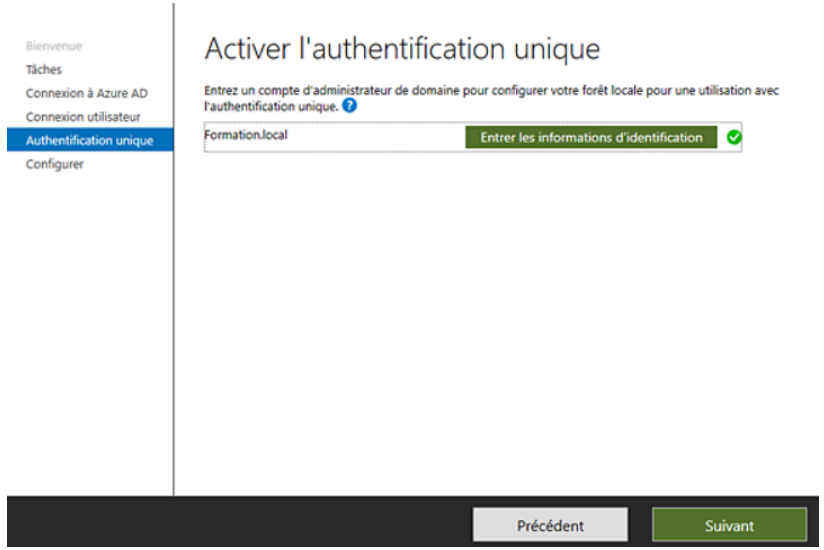


PARTIE 1

- Après avoir saisi les identifiants pour se connecter à Azure Active Directory, cochez la case **Activer l'authentification unique** puis cliquez sur **Suivant**.

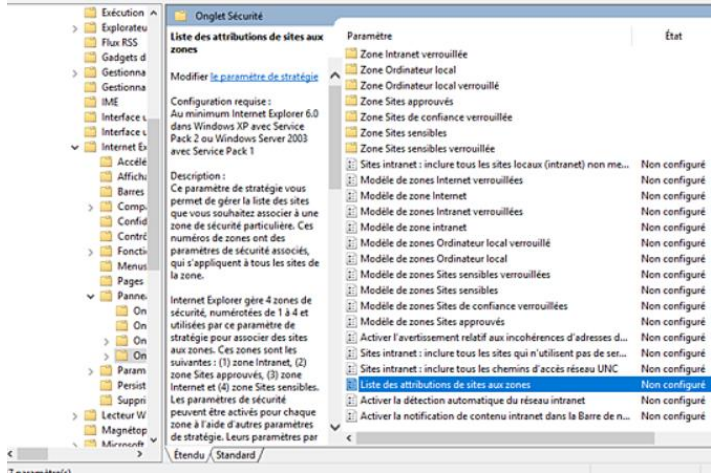


- Il est maintenant nécessaire de saisir les identifiants de connexion. Pour cela, cliquez sur le bouton **Entrer les informations d'identification**. Saisissez les identifiants d'un compte administrateur du domaine.



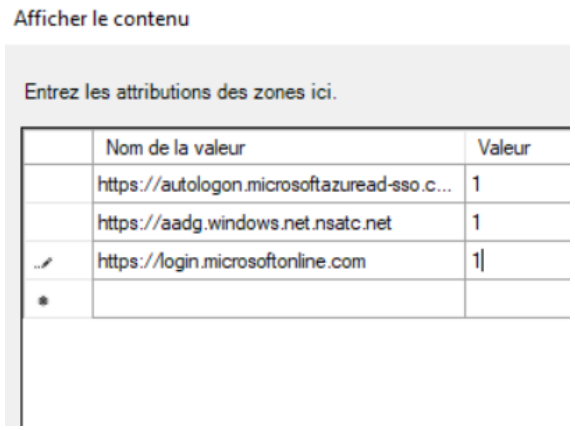
- La synchronisation peut maintenant être lancée. Dans la fenêtre **Configurer**, cliquez sur le bouton **Configurer**.

- Pour que le SSO fonctionne, il est nécessaire que le poste de travail soit membre du domaine AD. De plus, une stratégie de groupe doit être créée afin de configurer les différents navigateurs.
- Dans le cas de Firefox, il est nécessaire de télécharger les fichiers ADMX afin de configurer le paramètre SPNEGO présent dans Configuration utilisateur - stratégies - Modèles d'administration - Mozilla - Firefox - Authentication. Après avoir activé le paramètre pour Firefox, saisissez https://autologon.microsoftazuread-sso.com dans le champ **valeur**.
- La stratégie créée pour l'ensemble des navigateurs doit être liée à une unité d'organisation contenant les utilisateurs concernés par le SSO. Dans l'exemple ci-dessous, nous configurons la stratégie pour Internet Explorer. Microsoft Edge et Google Chrome hériteront ainsi des paramètres.
- Saisissez le nom de la stratégie de groupe puis cliquez sur **OK**.
- Éditez la stratégie de groupe puis accédez au paramètre **Liste des attributions de sites aux zones** présent dans **Configuration utilisateur** - **Modèles d'administration** - **Composants Windows** - **Internet Explorer** - **Panneau de configuration Internet** - onglet **Sécurité**.



- Ajoutez les URL suivantes et la valeur 1.
- https://autologon.microsoftazuread-sso.com/
- https://aadg.windows.net.nsatc.net
- https://login.microsoftonline.com

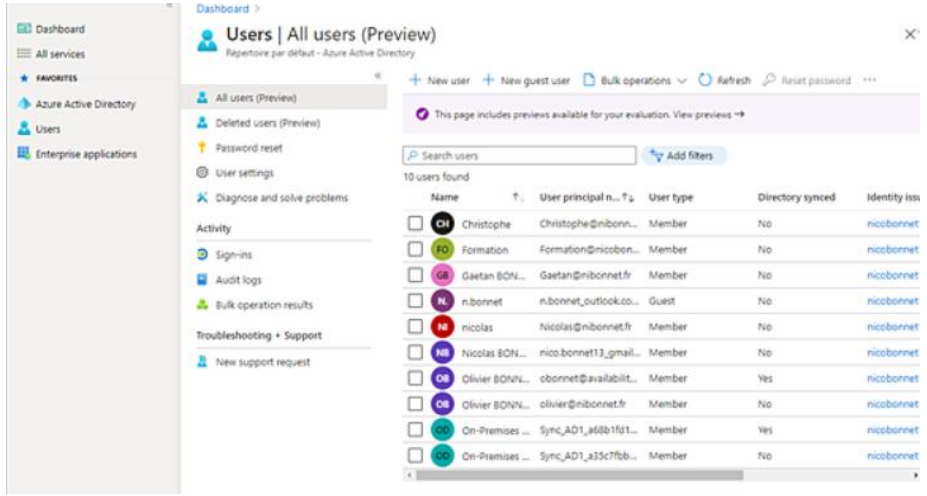
PARTIE 1



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

PARTIE 1

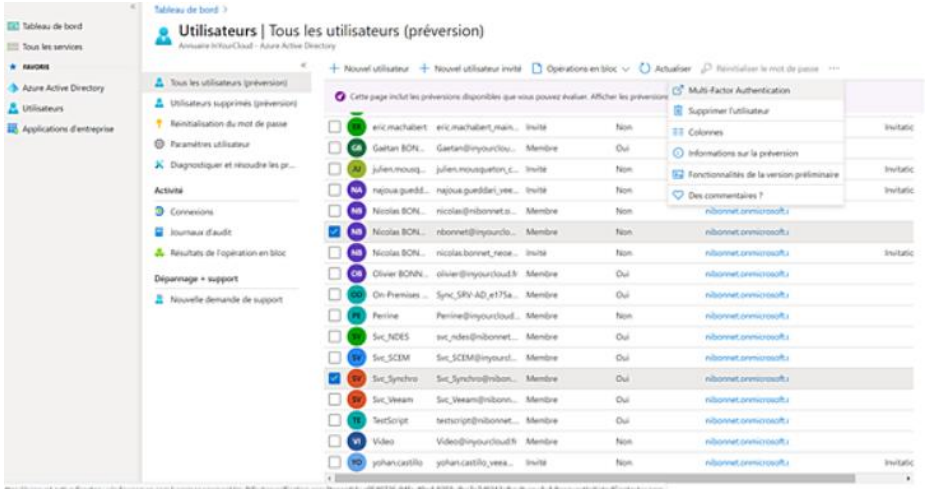
- Comme dans un annuaire Active Directory, Azure AD peut contenir des utilisateurs.



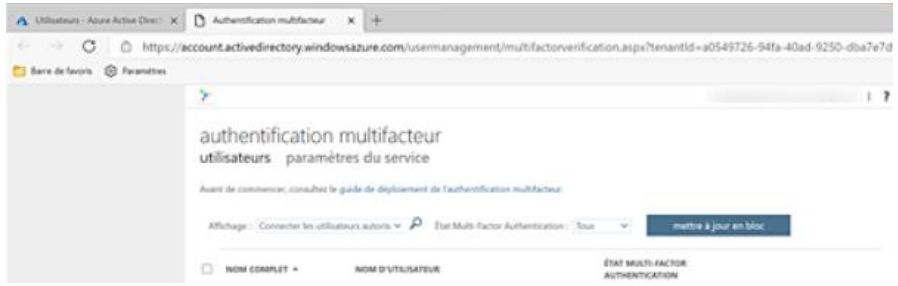
- En sélectionnant un utilisateur, il est possible d'accéder à ses attributs. Son nom, son prénom et son nom d'utilisateur s'affichent.
- Depuis cette même fenêtre, il est possible de configurer le rôle de l'utilisateur (délégation d'autorisation). En production, il est préférable d'utiliser un groupe d'utilisateurs, ceci afin de simplifier l'administration.
- L'onglet **Profil** permet, lui, de visualiser les informations propres à l'utilisateur (service, numéro de téléphone…).
- Depuis Windows 10, il est possible de joindre un poste de travail à un annuaire Azure AD. Ce dernier peut être joint à Active Directory et Azure Active Directory (Hybrid AD Join) ou uniquement à Azure AD (Azure AD Join).
- L'onglet **Appareils** permet de visualiser les équipements de l'utilisateur.

PARTIE 1

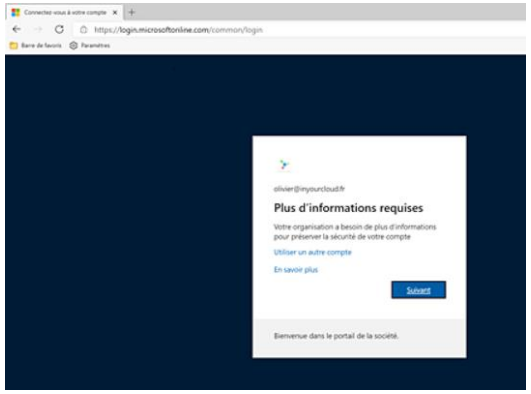
- Certaines applications peuvent contenir des informations confidentielles (CRM…), d'autres sont "la vitrine" de l'entreprise (Twitter…). Il est donc important d'activer l'authentification forte en fonction du degré de confidentialité des données contenues par l'utilisateur.
- L'activation de l'authentification forte s'effectue depuis l'interface web https://aad.portal.azure.com. Sélectionnez Active Directory puis cliquez sur **Tous les utilisateurs**. Dans le bandeau supérieur, cliquez sur **...** puis sur **Multi-Factor Authentication**.



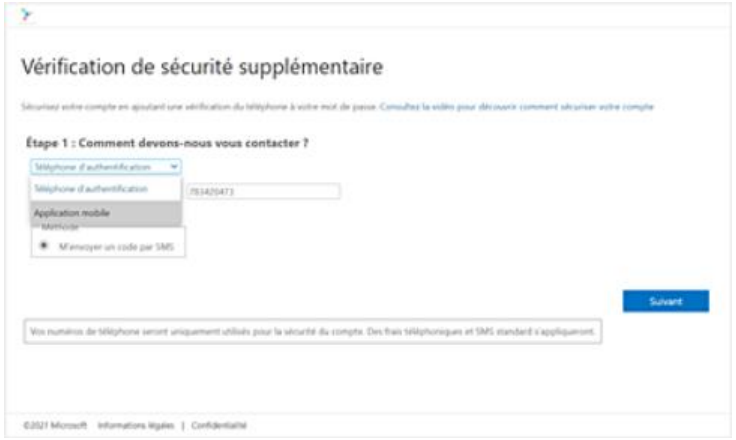
- Sélectionnez les utilisateurs souhaités puis cliquez sur **Activer**.



- Une fenêtre s'affiche. Il est nécessaire de cliquer sur **Activer multi-factor authentication** pour procéder à l'activation du MFA.
- Lors de la prochaine connexion de l'utilisateur (au portail applicatif, par exemple : http://myapps.microsoft.com/), ce dernier devra sélectionner le type d'authentification souhaité.

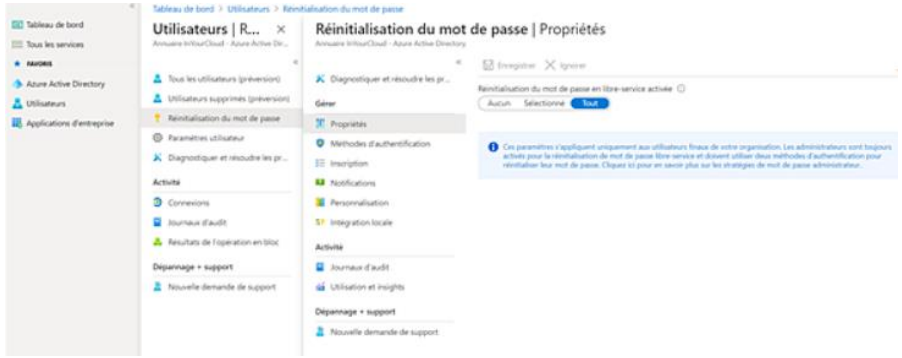


- Plusieurs possibilités d'authentification sont offertes à l'utilisateur. Pour des raisons de sécurité, il est fortement recommandé d'utiliser l'application mobile et non la partie télécom (appel ou SMS).



- Après avoir configué l'application, l'authentification forte est activée.

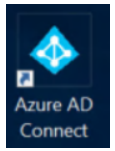
- Ce portail web offre la possibilité aux utilisateurs Azure AD de réinitialiser leur mot de passe sans intervention de l'équipe IT.
- Cette fonctionnalité nécessite une licence Azure AD Premium pour les comptes synchronisés avec un annuaire Active Directory. Pour les comptes cloud, une licence Azure AD free est suffisante. Avant de pouvoir accéder au portail web, il est nécessaire de procéder à la configuration de la politique de réinitialisation du mot de passe utilisateur. Cette opération consiste à activer le paramètre présent dans l'onglet **Réinitialisation du mot de passe**. Il est possible d'autoriser la fonctionnalité pour tout le monde ou pour un groupe d'utilisateurs.



- L'administrateur a la possibilité de définir le nombre de méthodes d'identification nécessaires pour procéder à la réinitialisation. Les méthodes disponibles doivent également être sélectionnées.
- La configuration de la fonctionnalité réinitialisation est terminée, les autres menus permettent de configurer les notifications et d'effectuer certaines personnalisations.

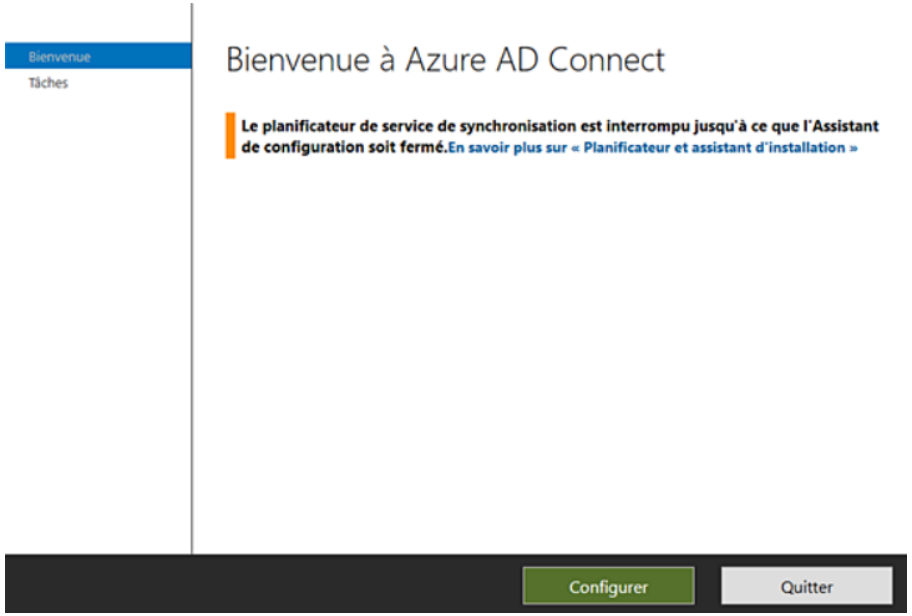
Modification de Azure AD Connect

- La réinitialisation du mot de passe nécessite une reconfiguration de l'outil Azure AD Connect. L'icône d'accès à la configuration de l'outil est présente sur le bureau du serveur Azure AD Connect.

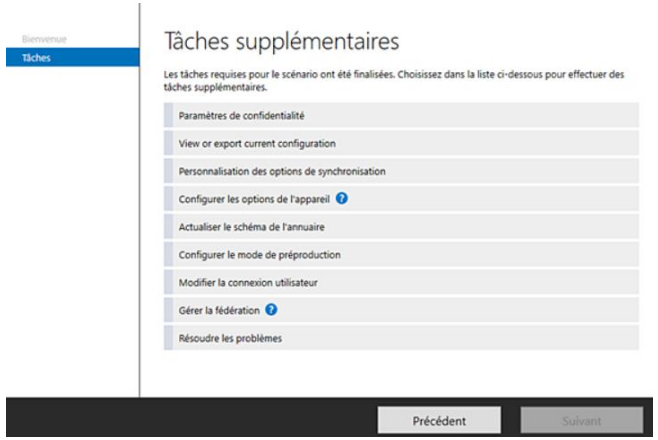


PARTIE 1

- L'assistant de configuration apparaît, il est nécessaire de cliquer sur **Configurer**.



- Un grand nombre d'opérations sont possibles, l'activation de la fonctionnalité réinitialisation du mot de passe est présente dans **Personnalisation des options de synchronisation** puis cliquez sur **Suivant**.



- Après avoir saisi le mot de passe du compte administrateur, il est possible de cocher **Réécriture du mot de passe**.