Clonage d'un contrôleur de domaine virtualisé

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

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

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

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

Le contexte de sécurité du serveur source est utilisé par le contrôleur de domaine cloné afin de communiquer avec le serveur ayant le rôle **Emulateur PDC**. Ce dernier doit exécuter nécessairement **Windows Server 2012 R2**.

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

1. Les différents composants du clonage

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

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

Les vérifications préalables effectuées sont les suivantes :

- Le contrôleur de domaine qui est en train d'être préparé est autorisé pour le clonage (utilisation du groupe Contrôleur de domaine clonable).
- Le serveur ayant le rôle d'**émulateur PDC** doit exécuter **Windows Server 2012 R2**.
- Les programmes ou services listés par l'exécution de la commande **Get-ADDCCloningExcludedApplicationList** sont inclus dans le fichier **CustomDCCloneAllowList.xml**.

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

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

CustomDCCloneAllowList.xml : ce fichier permet de créer des exceptions pour des applications non compatibles avec le clonage. Cette opération est obligatoire sans quoi les opérations suivantes sont impossibles. Exécutez **Get-ADDCCloningExcludedApplicationList** afin de trouver les différents services et programmes non présents dans le

fichier **DefaultDCCloneAllowList.xml**. Le commutateur **GenerateXml** doit être utilisé afin de permettre la génération du fichier XML.

2. Pré-requis au clonage

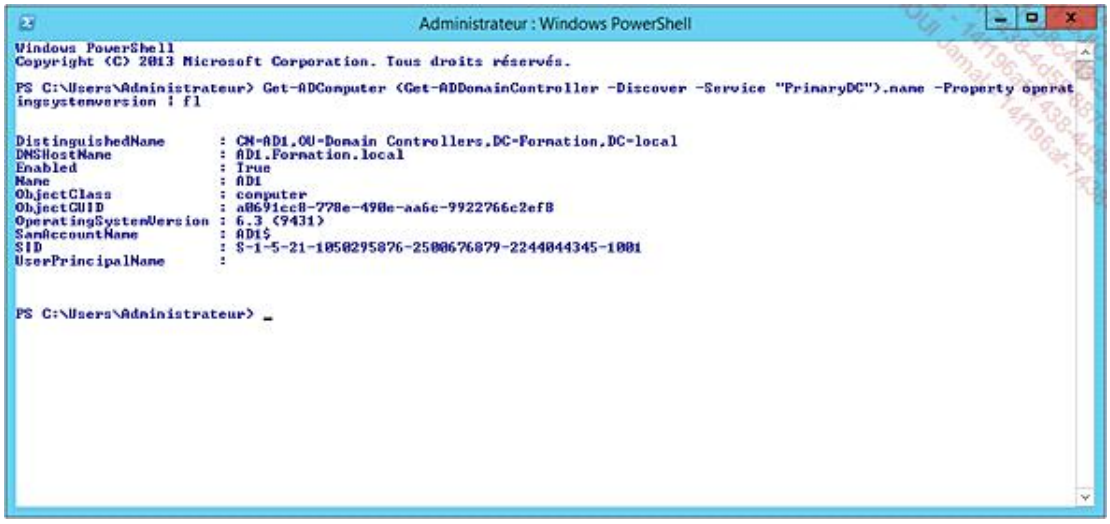
- Le compte utilisé doit être membre du groupe **Administrateurs du domaine** et la console PowerShell doit, elle, être exécutée avec l'élévation de privilège.

Effectuez un clic droit sur **PowerShell** et sélectionnez **Exécuter comme administrateur**.

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

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

Le script peut être téléchargé sur la page Informations générales.



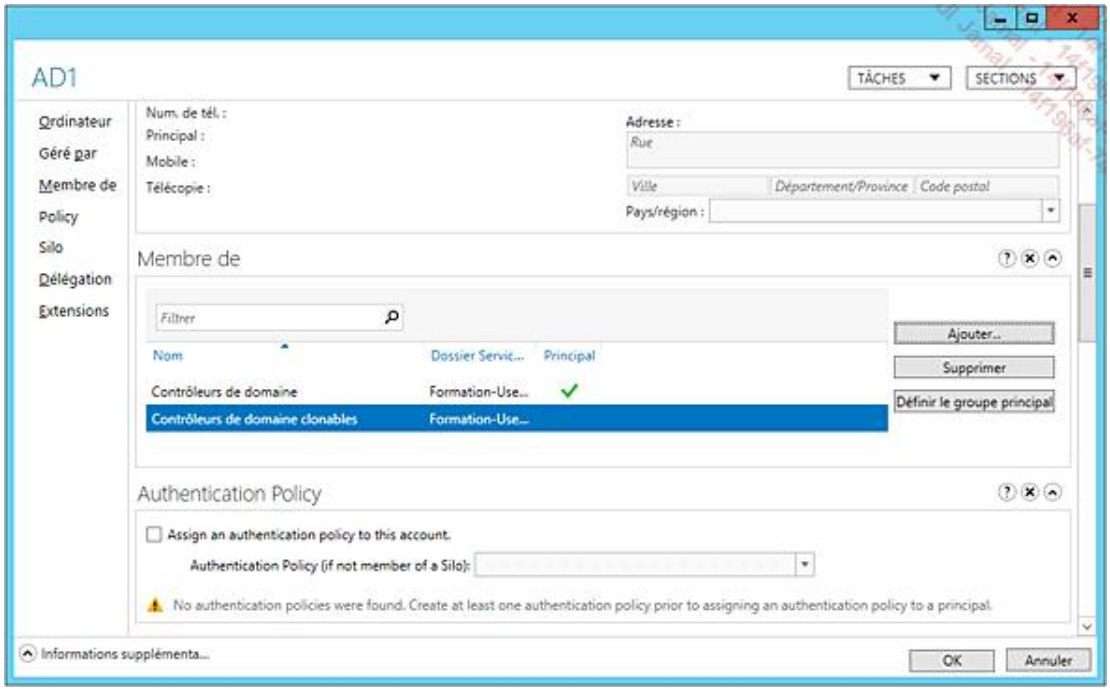
- Il est recommandé de s'assurer de l'état de santé du contrôleur de domaine afin de dupliquer un serveur sain. Pour cela, utilisez la commande **dcdiag**. Visitez ce site pour avoir plus d'informations sur cette commande : http://blogs.technet.com/b/askds/archive/2011/03/22/what-does-dcdiag-actually-do.aspx
- Si le contrôleur de domaine source est également serveur DNS, le clone a également le rôle de serveur DNS. Les zones DNS **doivent être intégrées à Active Directory**.
- Lors du clonage, l'adresse configurée dans le client DNS du serveur n'est pas dupliquée vers la destination ; elle est spécifiée dans le fichier **DCCloneConfig.xml**. Si ce dernier ne contient pas l'information, le client DNS pointera sur lui-même en tant que serveur préféré par défaut. Si besoin, il est nécessaire de mettre à jour les délégations DNS pour le contrôleur domaine cloné.
- Les serveurs ayant les rôles suivants ne peuvent pas être clonés :
  - DHCP (Dynamic Host Configuration Protocol)

- Active Directory Certificate Services (AD CS)
- Active Directory Lightweight Directory Services (AD LDS)

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

3. Mise en place de la solution de clonage

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



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

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

La commande PowerShell ci-dessous peut également être utilisée.

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

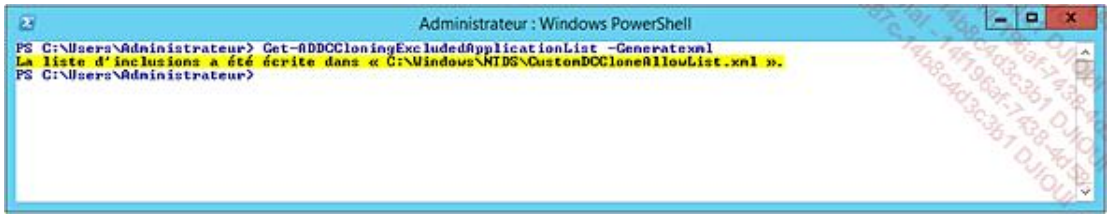
Le script peut être téléchargé sur la page Informations générales.

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

La commande doit être exécutée avant le lancement de la commande PowerShell **New-ADDCCloneConfigFile**. Si ce

dernier détecte des applications exclues, le fichier **DCCloneConfig.xml** n'est pas créé.

- Saisissez dans la console PowerShell : **Get-ADDCCloningExcludedApplicationList -Generate XML**



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

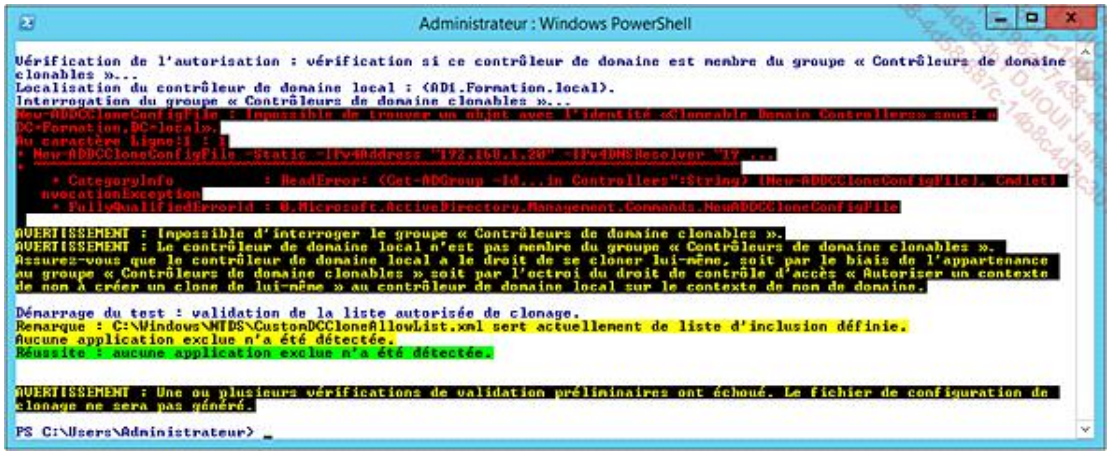
Le script peut être téléchargé sur la page Informations générales.

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

- Saisissez dans la console PowerShell la commande :

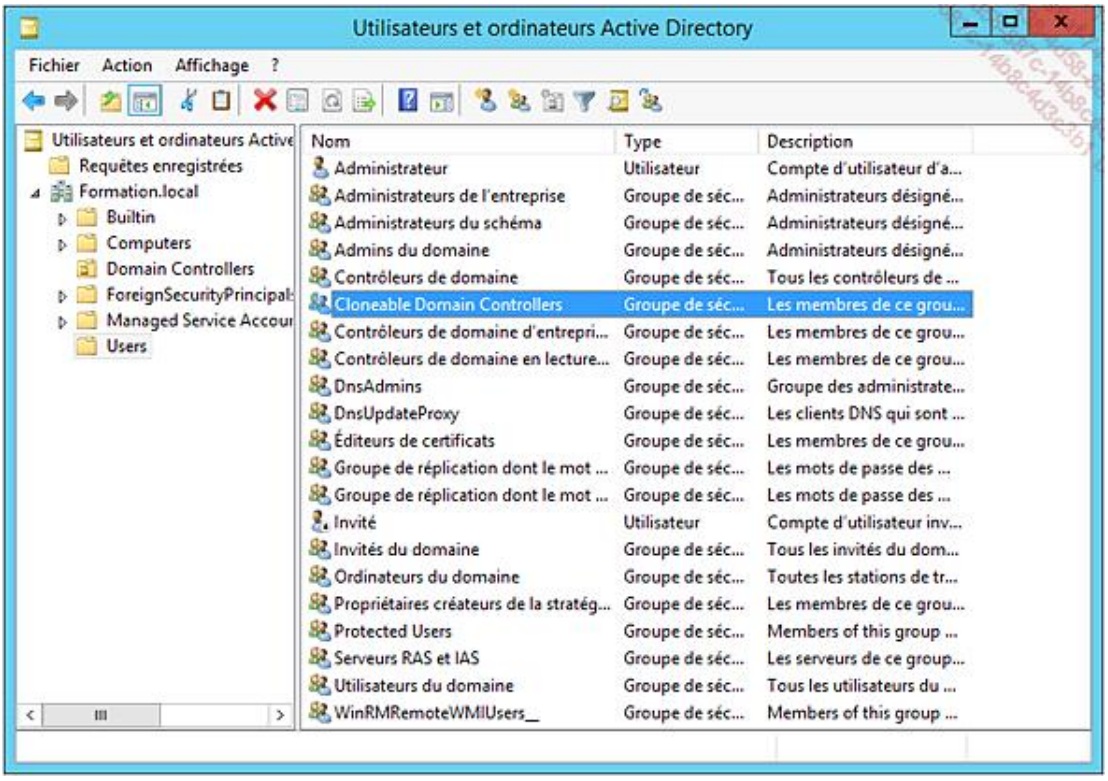
New-ADDCCloneConfigFile -Static -IPv4Address "192.168.1.20" -IPv4DNSResolver "192.168.1.10" -IPv4SubnetMask "255.255.255.0" -CloneComputerName "AD3" -IPv4DefaultGateway "192.168.1.254" -SiteName "Marseille"

Si une erreur apparaît indiquant l'impossibilité de trouver le groupe Cloneable Domain Controller, créez un groupe portant ce nom dans le dossier système Users puis ajoutez AD1 en tant que membre ou renommez le groupe contrôleurs de domaine clonables.

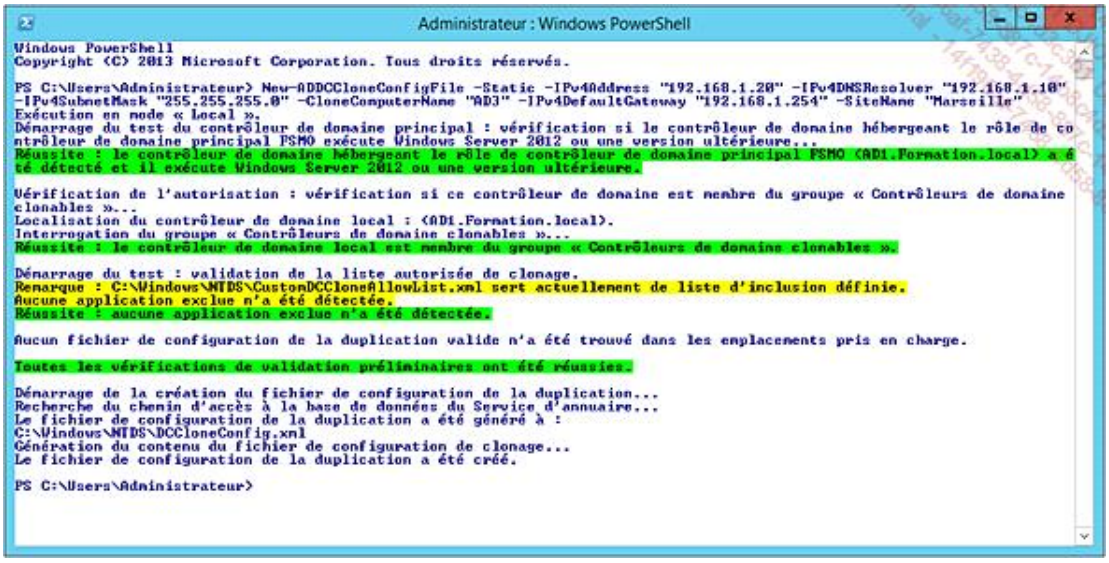


Une erreur apparaît car le groupe **Contrôleurs de domaine clonables** n'a pas été renommé en tant que **Cloneable Domain Controllers**.

- Renommez le groupe **Contrôleurs de domaine clonables** présent dans le conteneur Users en **Cloneable Domain Controllers**.



Relancez la commande PowerShell, l'instruction fonctionne désormais.



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

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

Si le contrôleur de domaine n'est pas mis en tant que serveur DNS préféré, le clonage échoue.

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

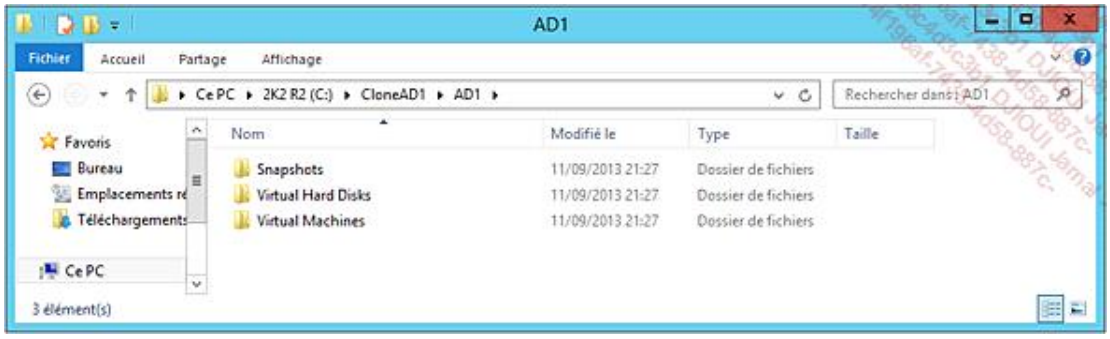
4. Exportation et importation du contrôleur de domaine source

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

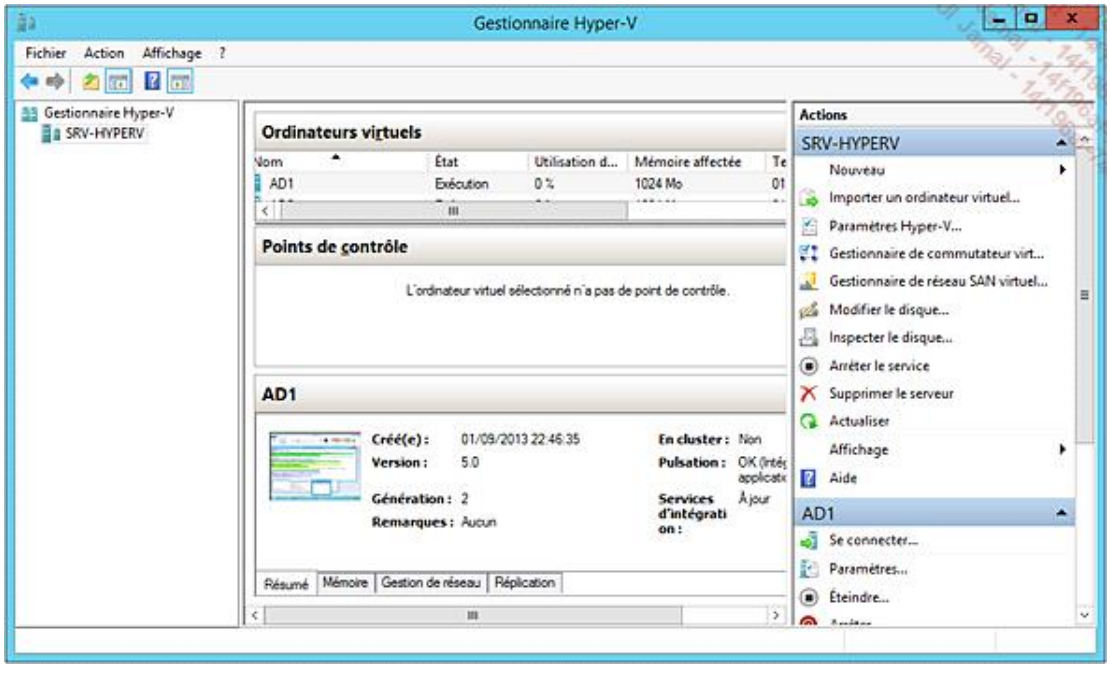
Il est nécessaire d'être au minimum membre du groupe Administrateur local.

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

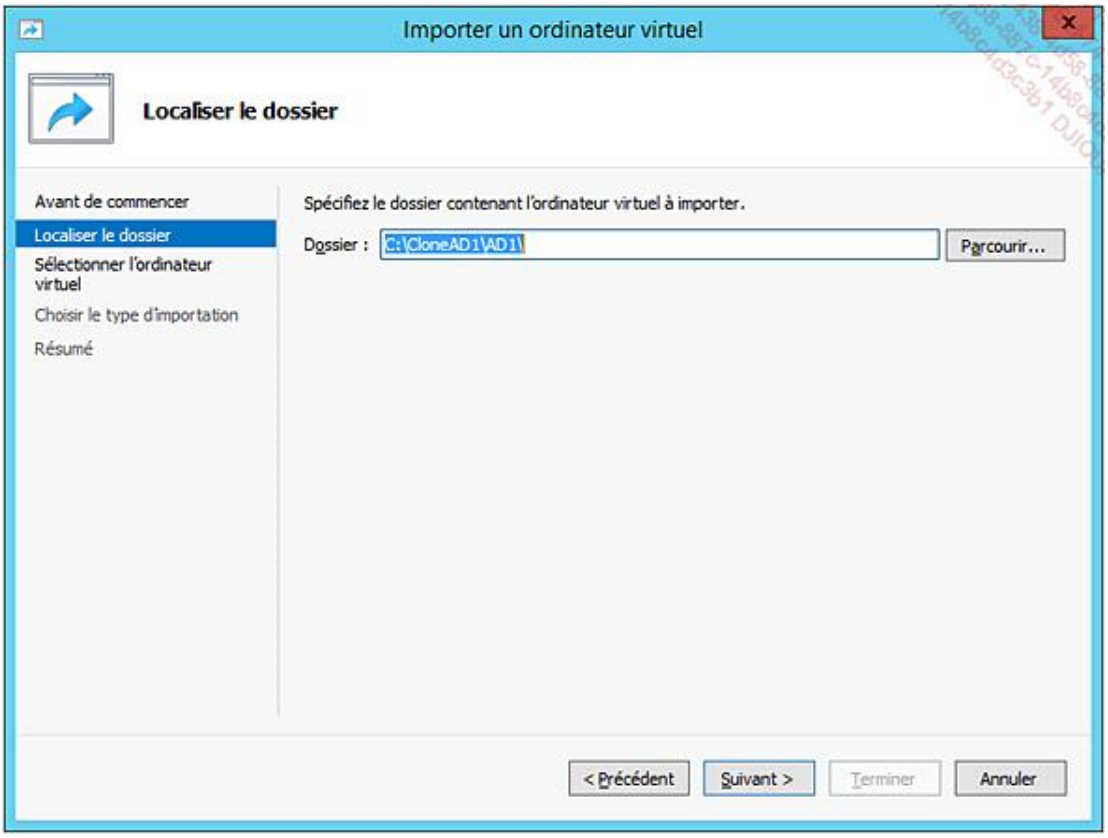
- Arrêtez le serveur **AD1** afin de pouvoir l'exporter.
- Il est désormais possible avec Windows Server 2012 R2, d'effectuer une exportation de la VM sans avoir à l'éteindre, néanmoins dans le cas d'un clonage, un arrêt est nécessaire.
- Exportez **AD1** dans le dossier **c:\CloneAD1** en effectuant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



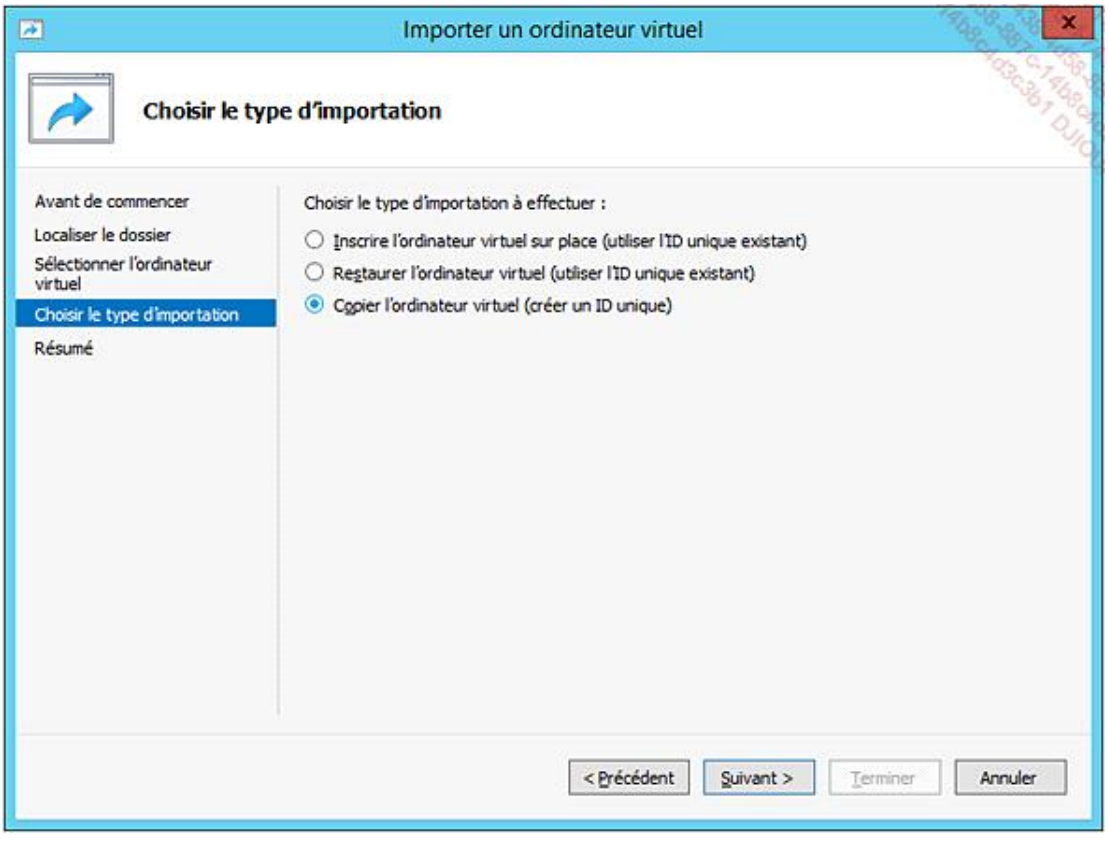
- Dans le bandeau **Actions** de la console **Gestionnaire Hyper-V**, cliquez sur **Importer un ordinateur virtuel**.



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

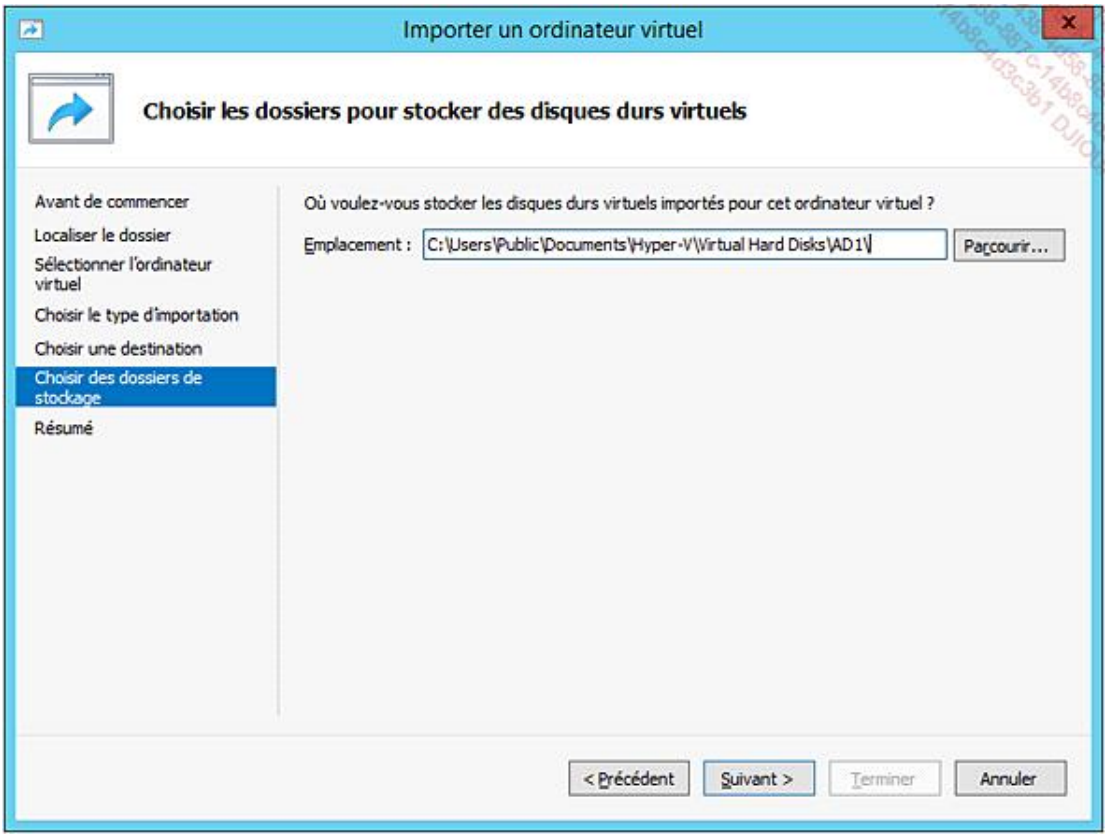


- Dans la fenêtre **Sélectionner l'ordinateur virtuel**, cliquez sur **Suivant**.
- Dans le choix du type d'importation, sélectionnez **Copier l'ordinateur virtuel (créer un ID unique)** puis cliquez sur **Suivant**.



- Cliquez sur **Suivant**.

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



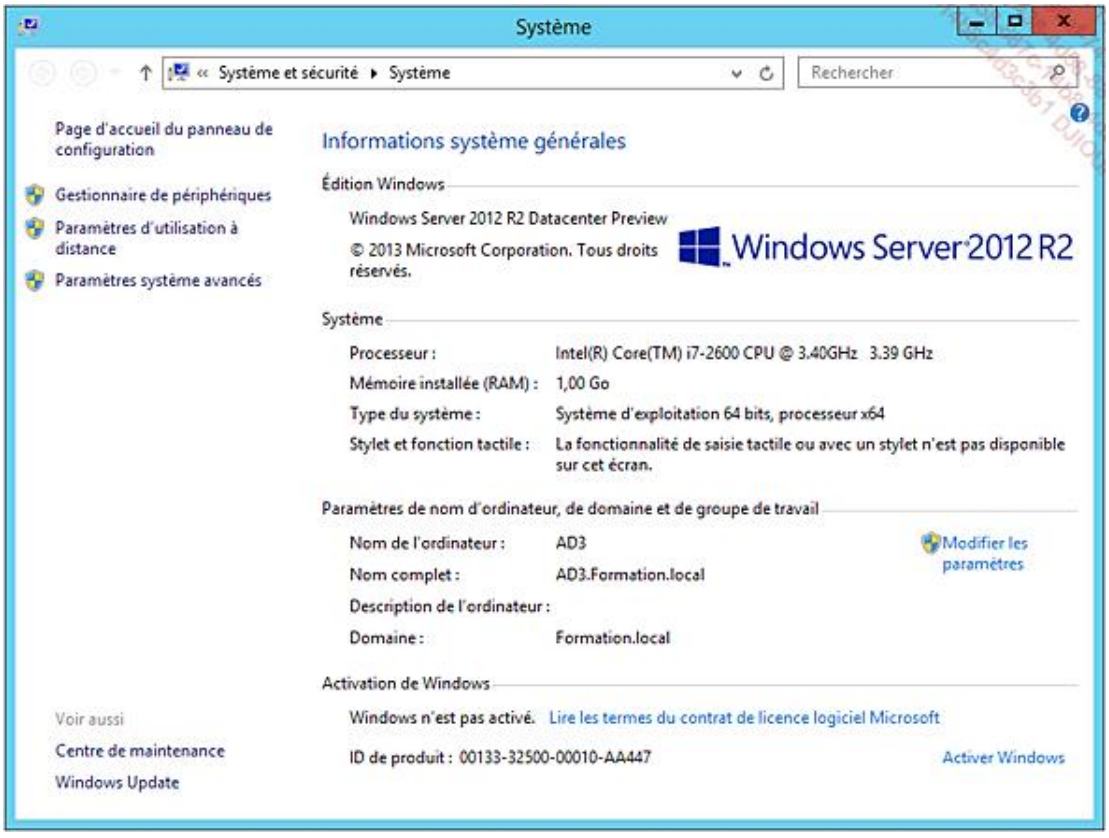
- Lancez l'importation en cliquant sur **Terminer**.
- Renommez la machine virtuelle nouvellement importée et donnez-lui le nom d'AD3.

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

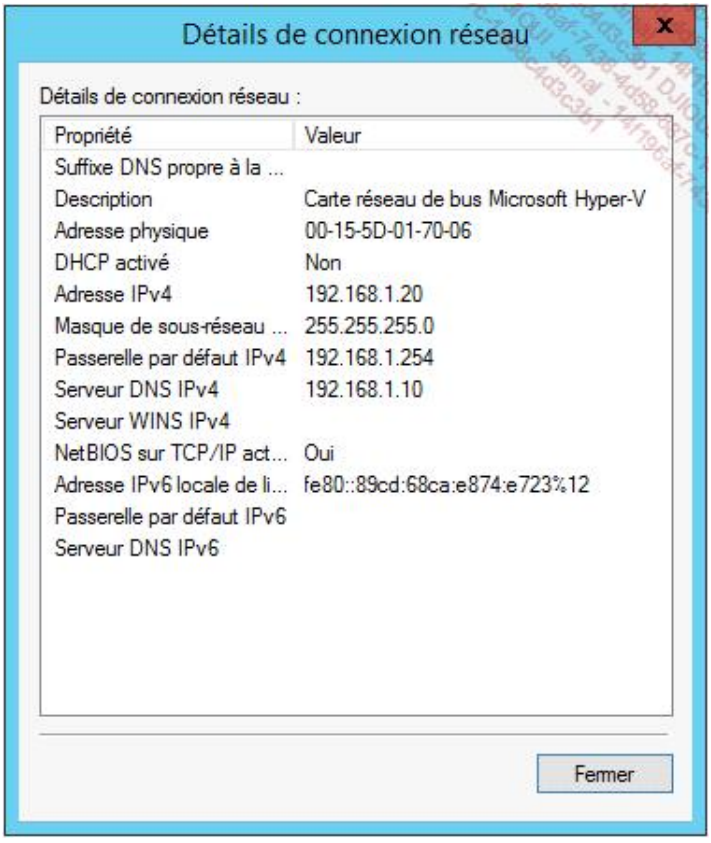
- Démarrez en premier la machine source.

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

Le nom du poste a bien été configuré.



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



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

Les rôles DNS et AD DS ont bien été installés.