Editions ENI

Windows Server 2016

Installation, gestion du stockage et des traitements

Examen 70-740

dans la collection Certification

Extrait

Prérequis

☒Posséder des compétences sur l'administration système

☒Posséder des notions sur la migration de serveur

Objectifs

☒Effectuer la création d'une image Nano Server

☒Vue d'ensemble du mode Core

☒Présentation des scénarios de migration

A. Présentation de Nano Server

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

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

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

Nano Server est une fonctionnalité apparue avec Windows Server 2016. Assez semblable au mode Core, il ne permet pas pour sa part de connexion locale. Il faut noter également une modification au niveau du support applicatif. En effet, Nano Server ne supporte que des applications, agents… 64 bits. La gestion des mises à jour s'en trouve également facilitée. En effet, le nombre de correctifs nécessaires est largement réduit.

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

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

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

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

B. Mise en place de Nano Server

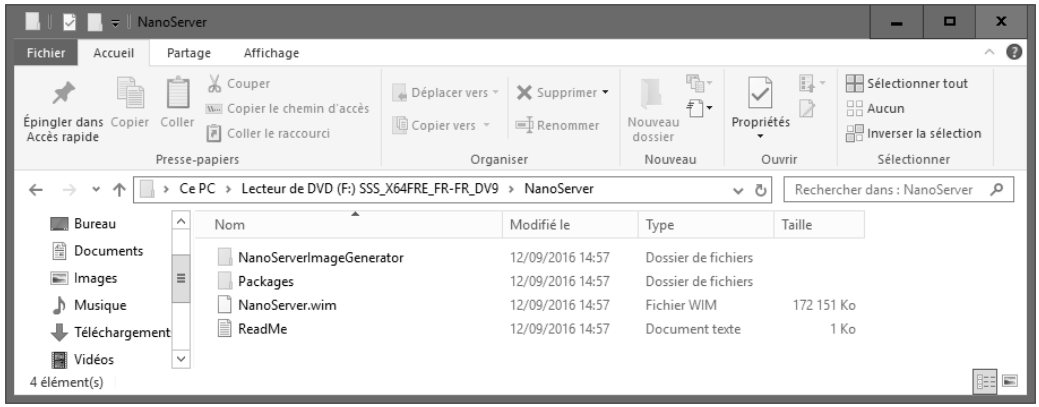
Nous l'avons vu dans le point précédent, l'utilisation de Nano Server nécessite la création d'une image. L'ensemble des fichiers nécessaires à la création sont présents dans le dossier Nano Server du DVD Windows Server 2016.

Par la suite, la création peut être effectuée par l'intermédiaire de trois moyens :

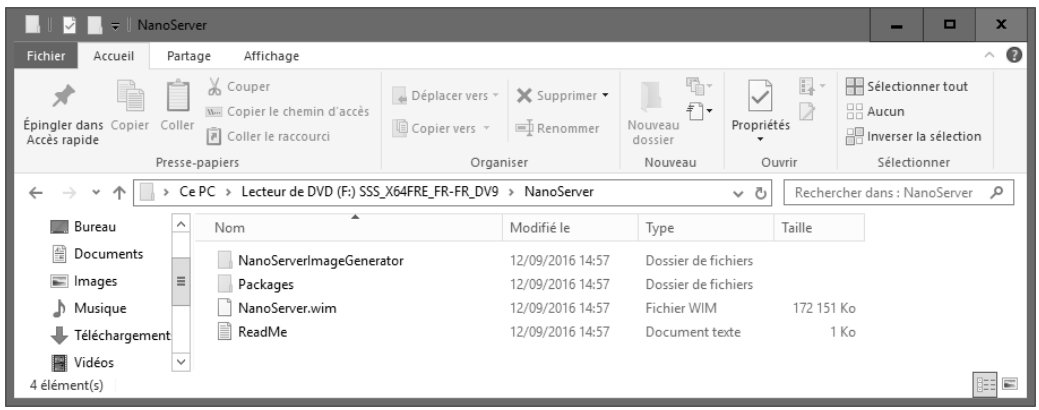
- Utilisation d'une image VHD avec un serveur Hyper-V
- Utilisation d'une image VHD avec un poste physique (boot sur VHD)
- Déploiement par l'intermédiaire d'une image WIM

1. Installation de la fonctionnalité

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

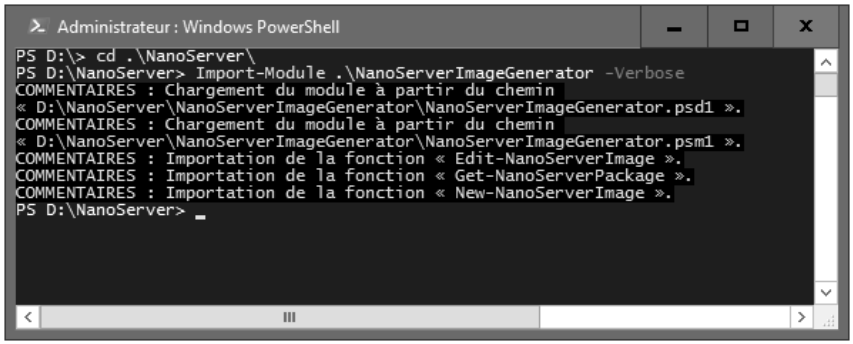


L'ensemble des fichiers présents dans le dossier NanoServer doit être copié dans une partition locale (poste de travail Windows 10, serveur…).



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

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



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

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

Définition des différents arguments :

`-Edition` : édition de l'image Nano Server (Standard ou Datacenter).

`-DeploymentType` : définit le type de déploiement souhaité (WIM, image VHD pour du boot sur VHD ou image VHD pour un hôte Hyper-V).

`-MediaPath` : chemin de l'image ISO de Windows Server 2016.

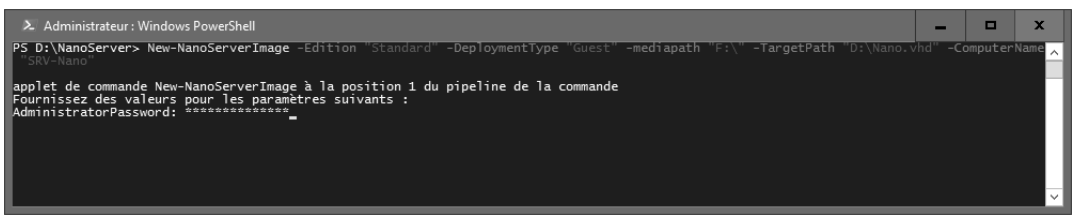
`-BasePath` : commutateur optionnel, il est utilisé lors de la création d'un fichier Wim. Les sources nécessaires à la création d'une image WIM sont copiées dans ce répertoire. La cmdlet **`New-NanoServerWim`** peut être utilisée sans spécifier le commutateur **`-MediaPath`**.

`-TargetPath` : permet d'indiquer le chemin du répertoire de destination ainsi que le nom de l'image. Cette dernière est de plus composée de son extension.

`-ComputerName` : nom de l'ordinateur Nano Server.

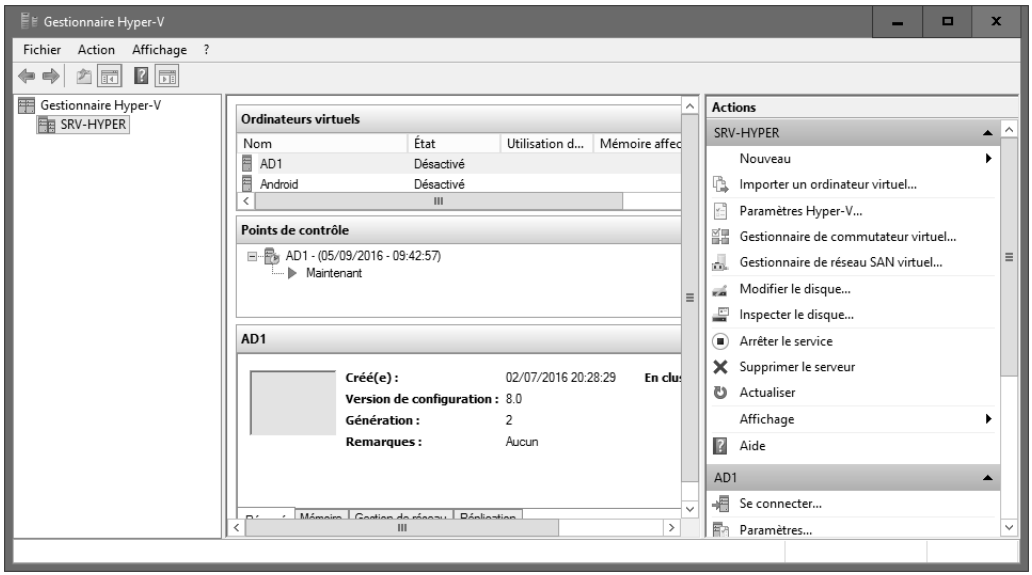
`-Packages` : utilisé pour l'installation de rôles ou fonctionnalités. Il est évidemment possible de combiner plusieurs packages (séparés par une virgule).

`-Other` : utilisé par certains packages (pilotes…). Il est nécessaire d'utiliser **`-OEMDrivers`** pour une utilisation sur un serveur physique… Le commutateur sera complété par le chemin où sont présents les pilotes.

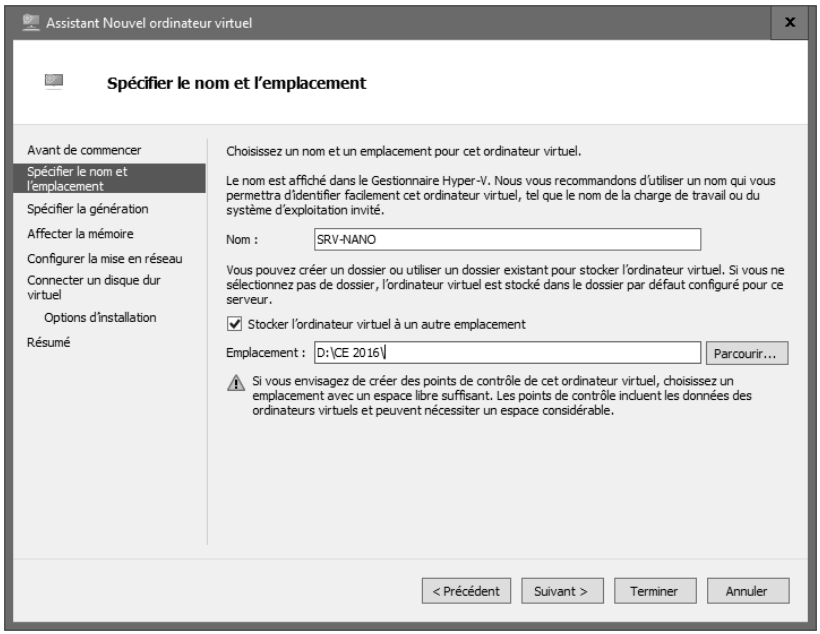


L'image est maintenant créée et présente dans le répertoire défini dans la commande. La machine virtuelle doit maintenant être créée dans Hyper-V.

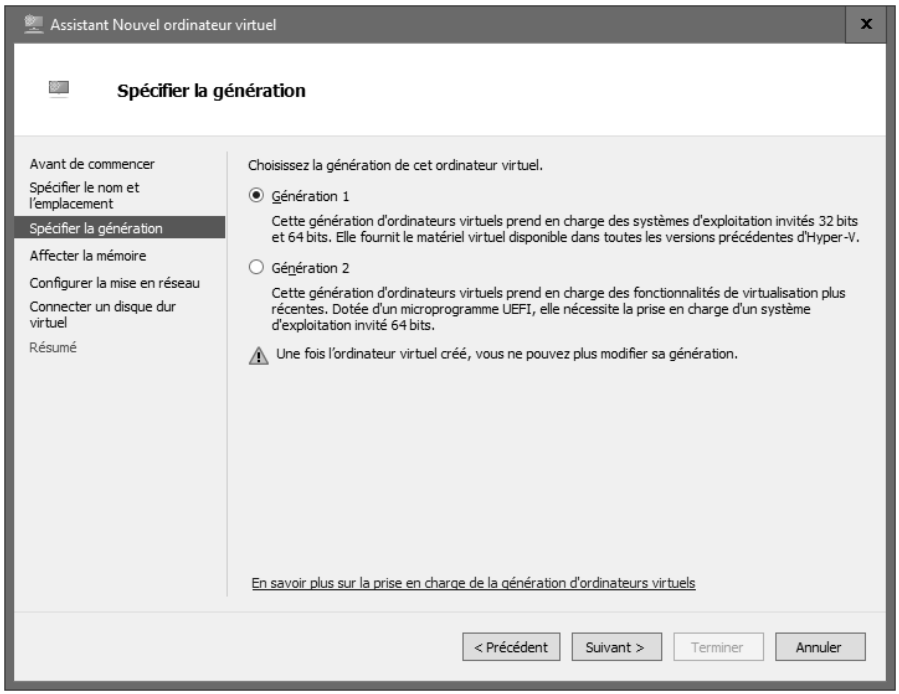
Depuis la console Gestionnaire Hyper-V, il est nécessaire de cliquer sur **Nouveau** puis **Ordinateur virtuel**.



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



Le choix de la génération est important car la modification de la génération est impossible après avoir créé la machine. Si le fichier VHD précédemment créé est de type VHD, il est nécessaire de créer une VM de génération 1. Dans le cas de l'utilisation d'un fichier de type VHDX, une VM de génération 2 peut être utilisée.



Editions ENI

Windows Server 2016

Infrastructure réseau

Examen 70-741

dans la collection Certification

Extrait

Prérequis

☒Avoir des notions sur l'adressage IP.

☒Connaître les différents paramètres qui composent une configuration IP.

☒Connaître la différence entre un adressage statique et dynamique.

Objectifs

☒Définition du rôle DHCP.

☒Présentation des fonctionnalités offertes par le service.

☒Gestion de la base de données.

☒Mise en place de la maintenance du serveur DHCP.

☒Mise en place d'un DHCP relais.

A. Introduction

Le serveur DHCP (*Dynamic Host Configuration Protocol*) est un rôle assez important dans une architecture réseau. Son rôle est la distribution de configuration IP, permettant aux équipements connectés au réseau de dialoguer entre eux.

B. Rôle du service DHCP

DHCP est un protocole qui permet d'assurer la configuration automatique des interfaces réseau. Cette configuration comprend une adresse IP, un masque de sous-réseau mais également une passerelle et des serveurs DNS. D'autres paramètres supplémentaires peuvent être distribués (serveur WINS…).

La taille des réseaux actuels oblige de plus en plus à éliminer l'adressage statique saisi par un administrateur sur chaque machine par un adressage dynamique effectué par le biais du serveur DHCP. Ce dernier offre l'avantage d'offrir une configuration complète à chaque machine qui en fait la demande mais plus particulièrement, il est impossible de trouver deux configurations identiques (deux adresses IP identiques distribuées). Le conflit IP est donc évité, l'administration s'en trouve également facilité.

Le serveur est capable d'effectuer une distribution de configuration IPv4 ou IPv6.

1. Fonctionnement de l'allocation d'une adresse IP

Si l'interface réseau est configurée pour obtenir un bail DHCP, elle va tenter d'obtenir un bail par l'intermédiaire d'un serveur DHCP. Cette action s'opèrera par l'échange de plusieurs trames entre le client et le serveur.

La machine envoie à l'aide d'une diffusion (envoi d'un *broadcast*), un datagramme (**DHCP Discover**) sur le port 67.

Tout serveur qui reçoit ce datagramme diffuse une offre DHCP au client (**DHCP Offer**), ce dernier peut évidemment recevoir plusieurs offres. Le port utilisé pour l'offre est le 68.

Le client retient la première offre qu'il reçoit et diffuse sur le réseau un datagramme (**DHCP Request**). Ce dernier va comporter l'adresse IP du serveur et celle qui vient d'être proposée au client, le but étant la demande de l'assignation de l'adresse pour le serveur qui a été retenu mais également d'informer les autres serveurs DHCP qu'ils n'ont pas été retenus.

Le serveur envoie un datagramme d'accusé de réception (**DHCP ACK**, *Acknowledgement*) qui assigne au client l'adresse IP et son masque de sous-réseau ainsi que la durée du bail et éventuellement d'autres paramètres.

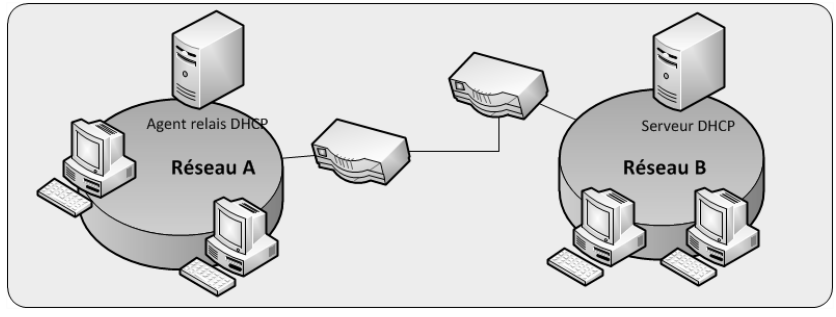
La liste des options que le serveur DHCP peut accepter est définie dans la RFC 2134.

Un bail DHCP (configuration attribuée à un poste) a une durée de validité, cette variable de temps est définie par l'administrateur. À 50 % de la durée du bail, le client commence à demander le renouvellement du bail qui lui a été octroyé. Cette demande est faite uniquement au serveur qui a attribué le bail. Si ce dernier n'a pas été renouvelé, la prochaine demande s'effectuera à 87,5 % de la durée du bail. Au terme de ce dernier, si le client n'a pas pu obtenir de renouvellement ou une nouvelle allocation, alors l'adresse est désactivée et il perd la faculté d'utiliser le réseau TCP/IP.

2. Utilisation d'un relais DHCP

Du fait de l'utilisation de trames de type *broadcast*, les trames n'ont pas la possibilité de passer les routeurs. Ceci implique donc d'avoir un serveur pour chaque sous-réseau IP. Ce besoin de plusieurs serveurs peut représenter un coût excessif pour l'entreprise. Pour remédier à ce problème, il convient de mettre en place un relais DHCP. Ce dernier permet de transférer les demandes de bail à un serveur présent sur un autre réseau.

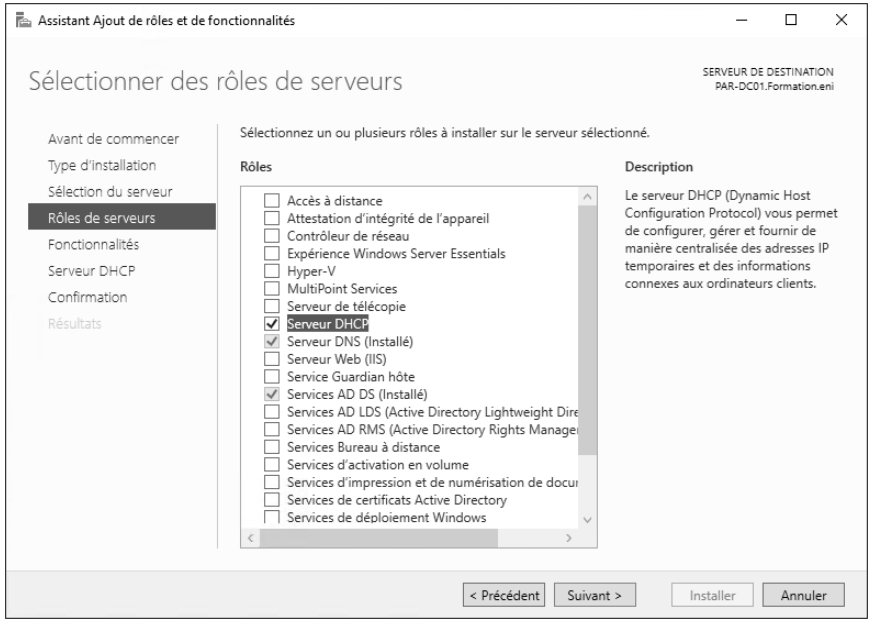
Le relais DHCP est installé sur le réseau A, il a en charge de récupérer les demandes de DHCP faites sur le sous-réseau IP. Il transfère par la suite les différentes requêtes qu'il a reçues au serveur DHCP présent sur le réseau B.



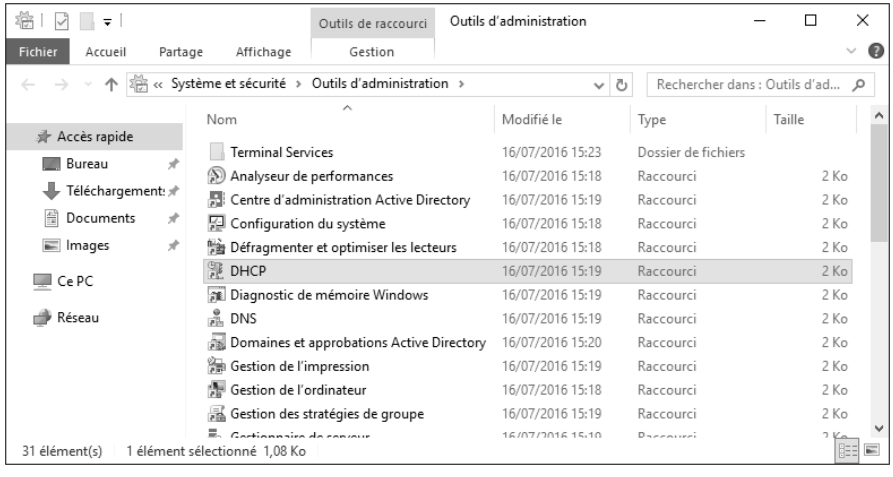
Il convient néanmoins de s'assurer du débit de la ligne et des temps de réponse.

C. Installation et configuration du rôle DHCP

Comme pour les autres services qui peuvent être ajoutés au serveur, DHCP est un rôle. Son installation s'effectue à l'aide de la console Gestionnaire de serveur en cochant simplement le rôle dans la fenêtre de sélection du rôle.



Après avoir procédé à l'installation, la console est présente dans les Outils d'administration.



Le rôle est maintenant installé, mais il n'est pas configuré.

1. Ajout d'une nouvelle étendue

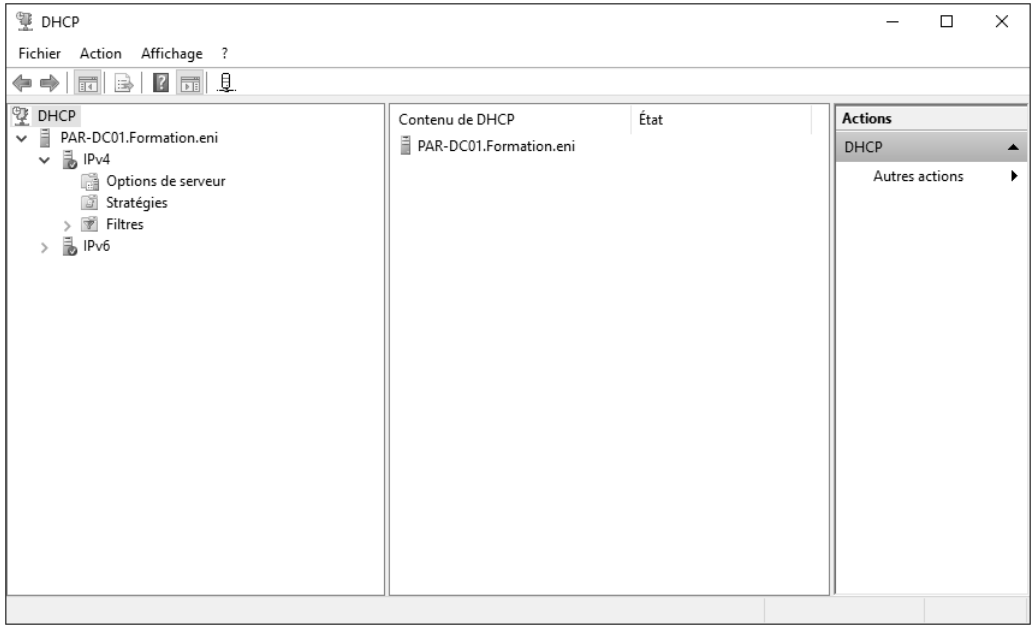
Une étendue DHCP est constituée d'un pool d'adresses IP (172.16.0.10 à 172.16.0.200), lorsqu'un client effectue une demande, le serveur DHCP lui attribue une des adresses du pool.

La plage d'adresses IP disponibles pour l'étendue est nécessairement contiguë. Pour éviter la distribution de certaines adresses, il est possible de faire des exclusions d'une adresse ou d'une plage. Ces dernières peuvent être assignées à un poste de façon manuelle sans risquer un conflit d'IP, puisque le serveur ne distribuera pas ces adresses.

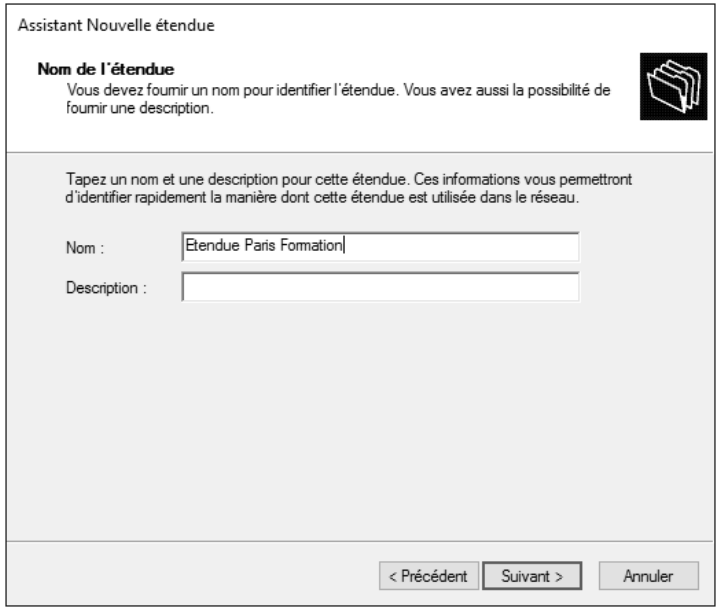
Utilisation de la règle 80/20 pour les étendues

Il est possible d'avoir deux serveurs DHCP actifs sur le réseau en découpant le pool d'adresses en deux. La règle du 80/20 permet dans un premier temps d'équilibrer l'utilisation des serveurs DHCP mais surtout de pouvoir avoir deux serveurs sans risque de conflit IP. Le serveur 1 distribue 80 % du pool d'adresses, alors que le serveur 2 est configuré pour distribuer les adresses restantes (20 %).

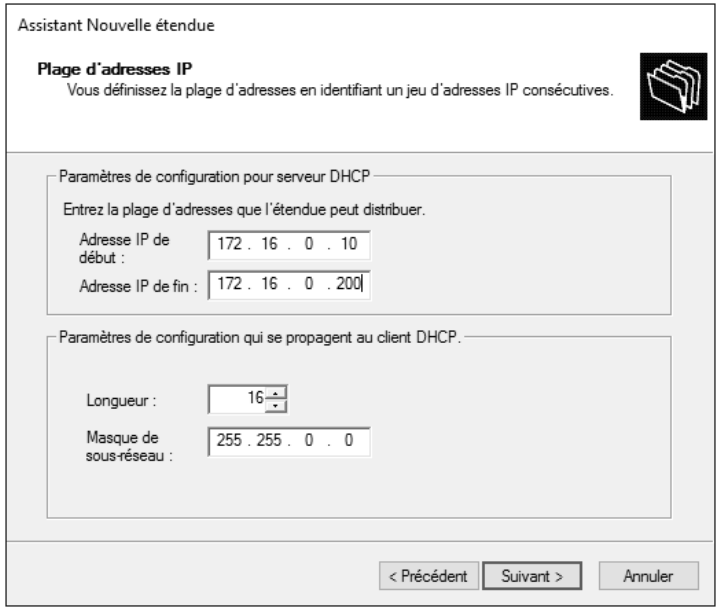
En développant **PAR-DC01.Formation.eni** puis **IPv4**, on peut s'apercevoir qu'il n'existe pas d'étendue. Cette dernière doit être créée afin que le serveur puisse distribuer des baux d'adresses.



Ainsi, en effectuant un clic droit sur IPv4, il est possible de créer une nouvelle étendue. Cette dernière porte un nom qu'il est nécessaire de saisir dans l'assistant de création.

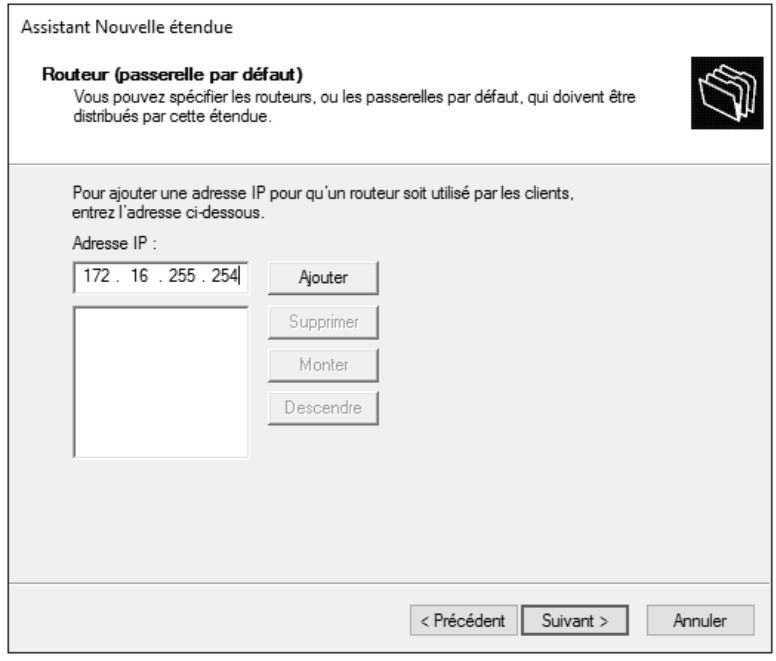


Par la suite, la plage d'adresses disponibles doit être définie (de 172.16.0.10 à 172.16.0.200).



Il est possible d'avoir dans cette plage certaines adresses qu'il est nécessaire d'exclure, ces dernières étant attribuées à des imprimantes. La liste d'exclusion est ainsi configurée, elle contient une adresse ou une plage d'adresses qui ne peut être configurée dans la plage adressable.

Un bail contient également une durée, par défaut cette valeur est configurée à 8 jours, il est évidemment possible d'augmenter ou diminuer ce nombre de jours. Par la suite, il est possible de saisir l'adresse de la ou des passerelles qui doivent être utilisées. De même le ou les serveurs DNS sont également à configurer. Ces options (DNS, passerelle par défaut…) sont par la suite distribuées au client qui effectue la demande d'un bail, il est donc préférable de s'assurer des informations saisies.



Dans un domaine Active Directory, il est nécessaire de procéder à l'autorisation du serveur DHCP. Les serveurs DHCP Microsoft non autorisés voient leur service arrêté par Active Directory.

2. Configuration des options dans le DHCP

Les options permettent de distribuer des options supplémentaires dans le bail, telles que le nom de domaine DNS et l'adresse du serveur DNS. Trois types d'options existent :

- **Les options de serveur** : elles s'appliquent à toutes les étendues du serveur ainsi qu'aux réservations. **Si la même option est configurée dans les options d'étendue, c'est cette dernière qui l'emporte, l'option serveur est donc ignorée**.

Editions ENI

Windows Server 2016

Gestion des identités

Examen 70-742

dans la collection Certification

Extrait

Chapitre 11

Prérequis

☒Avoir des notions de base sur l'administration de Windows Server 2016.

☒Avoir des notions de base sur la gestion des sécurités NTFS.

☒Savoir gérer une infrastructure AD CS.

Objectifs

☒Comprendre la gestion des droits AD RMS.

☒Connaître les différents composants d'une infrastructure AD RMS.

☒Savoir installer une infrastructure AD RMS.

☒Savoir configurer une infrastructure AD RMS.

☒Savoir déployer une infrastructure AD RMS.

☒Savoir protéger l'intégrité des données.

A. Services de gestion des droits

Depuis Windows Server 2008, les services de gestion des droits se présentent sous la forme d'un rôle de serveur nommé AD RMS (*Active Directory Rights Management Services*). AD RMS permet d'étendre les droits de sécurité NTFS afin d'apporter une sécurité supplémentaire visant à protéger l'intégrité des données. En comparaison, les services de gestion des droits sous Windows Server remplissent les mêmes fonctions que la gestion des droits numériques pour le contenu audio ou vidéo (DRM, *Digital Rights Management*).

1. Présentation d'AD RMS

AD RMS est un rôle de serveur qui permet de protéger l'intégrité des données générées par votre entreprise. Cela permet notamment de préserver la propriété intellectuelle ainsi que le contenu des données hébergées ou échangées avec d'autres partenaires. La protection d'un serveur de fichiers via les traditionnelles sécurités NTFS peut s'avérer limitée dans un processus de gestion des droits numériques. AD RMS permet d'étendre la sécurité NTFS afin de protéger, par exemple, le contenu des fichiers Office. Lorsqu'un utilisateur accède à un partage réseau pour ouvrir un document Word, le système vérifie les ACL afin de s'assurer que l'utilisateur est bien habilité à lire ou modifier le contenu. Or, une fois le document ouvert, la sécurité NTFS ne peut empêcher le contenu d'être préservé. Ainsi, l'utilisateur ayant ouvert le fichier peut également imprimer les données affichées, voire les copier afin de les modifier ultérieurement. AD RMS permet de répondre à ce besoin de sécurité en implémentant une couche supplémentaire au travers d'une nouvelle technologie qui peut se baser sur les composants AD DS (Services de domaine Active Directory), AD CS (Services de certificats) et AD FS (Services de fédération). Grâce à l'implémentation du rôle de serveur AD RMS, vous pouvez protéger le contenu de vos données à l'intérieur de votre réseau d'entreprise comme à l'extérieur. Ce rôle de serveur est en quelque sorte une évolution du service de gestion des droits Microsoft (RM : *Rights Management*), disponible avec le système d'exploitation Windows Server 2003 sous la forme d'un service Windows nommé RMS (*Rights Management Services*).

a. Fonctionnement d'AD RMS

Pour protéger les données sensibles de votre entreprise, une infrastructure de gestion des droits Active Directory repose sur un ensemble de serveurs AD RMS qui gèrent l'ensemble des règles de protection des données ainsi que l'échange des certificats et licences d'accès au service. La configuration de l'infrastructure ainsi que les journaux d'activités sont stockés dans une base de données. Les utilisateurs accèdent au contenu protégé et chiffré à l'aide d'un client AD RMS qui s'authentifie automatiquement auprès d'un annuaire Active Directory afin de s'assurer que l'utilisateur est habilité à profiter du contenu protégé. L'utilisateur obtient ensuite un certificat lui permettant de déchiffrer les données protégées. Les services de gestion des droits reposent également sur les services web IIS. L'ensemble des utilisateurs ou groupe devant accéder aux services de gestion des droits Active Directory doit posséder une adresse e-mail configurée dans leur profil Active Directory.

AD RMS est notamment compatible avec les applications suivantes :

- Pack Office 2007 / 2010 / 2013 et ultérieurs
- Microsoft SharePoint 2003 / 2007 / 2013 et ultérieurs
- Microsoft Exchange Server 2007 / 2010 / 2013 et ultérieurs
- XPS Viewer
- Internet Explorer (nécessite l'installation d'un module complémentaire)
- Adobe Acrobat Reader

L'installation d'une telle infrastructure nécessite également la formation des utilisateurs car c'est à eux de définir les éléments à sécuriser en indiquant si le document généré peut être lu, écrit, copié, imprimé, etc. Ces données sont stockées directement dans le document afin que ce dernier puisse être échangé en dehors de l'infrastructure du réseau d'entreprise. Seuls les utilisateurs authentifiés ou disposant d'un certificat valide peuvent accéder aux données protégées. Quand un utilisateur sécurise un document à l'aide des services de gestion des droits, l'infrastructure AD RMS génère une licence d'utilisation stockée au sein du document. Si l'utilisateur fait partie de votre organisation, ou d'une entité approuvée via les services de fédération, le client AD RMS installé sur la machine cliente demande automatiquement une licence d'utilisation à l'infrastructure AD RMS.

Pour faciliter la gestion des droits lorsqu'un utilisateur génère du contenu, un administrateur de l'infrastructure AD RMS peut également déployer des modèles de stratégies de droits. En fonction de l'utilisation du contenu, un utilisateur pourra ainsi appliquer le modèle de stratégie directement sans avoir à se soucier des éléments à configurer pour protéger efficacement son contenu.

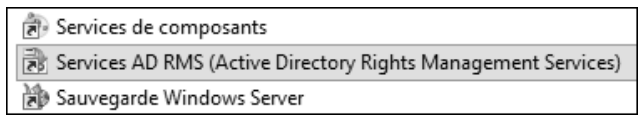
L'installation d'un serveur AD RMS crée un premier serveur dans un cluster racine. Ce cluster n'a rien à voir avec les technologies de clustering Microsoft ou de répartition de charge réseau. Un cluster racine AD RMS apporte simplement une solution de haute disponibilité pour les requêtes utilisateurs en utilisant une technologie propre aux services de gestion des droits Active Directory. Si l'infrastructure AD RMS est censée fonctionner avec un seul serveur de gestion des droits, il est possible d'utiliser une base de données interne nommée WID (*Windows Internal Database*), qui est intégrée au système d'exploitation. Cette instance de base de données n'autorise la création que d'un seul serveur dans le cluster AD RMS racine. Une infrastructure AD RMS supporte au minimum l'utilisation d'une base de données Microsoft SQL Server 2008.

L'installation du premier serveur du cluster racine AD RMS nécessite la création d'une clé de chiffrement. Cette clé doit être affectée à tous les serveurs qui rejoignent le cluster afin qu'ils puissent à leur tour chiffrer des certificats ou des licences à transmettre aux utilisateurs. Il existe deux méthodes de stockage de cette clé de chiffrement :

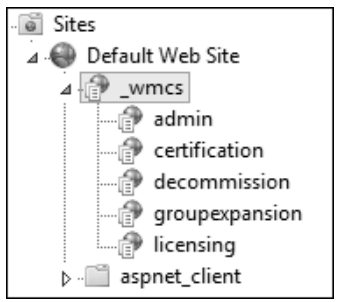
- **Stockage centralisé** : cela permet de stocker la clé de chiffrement dans la base de données du cluster AD RMS. Ainsi, chaque serveur qui rejoint le cluster peut récupérer automatiquement la clé de chiffrement sans intervention de l'administrateur.
- **Stockage manuel** : cela oblige à sélectionner un fournisseur de service cryptographique pour chiffrer la clé, qui doit être par la suite stockée manuellement par vos soins. Chaque serveur demandant à joindre le cluster doit récupérer cette clé de chiffrement avant d'intégrer le cluster racine AD RMS.

b. Gestion d'AD RMS

La gestion du rôle de serveur AD RMS se fait au travers d'un composant logiciel enfichable situé à l'emplacement suivant : **%SYSTEMROOT%\system32\AdRmsAdmin.msc**

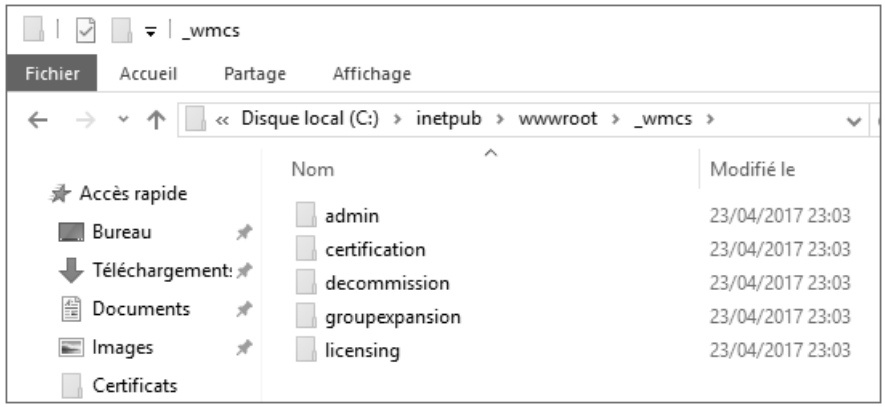


Le cluster AD RMS racine est quant à lui accessible via une URL qu'il est préférable d'associer à un alias DNS à déclarer au préalable dans le serveur de noms de votre organisation. Le cluster AD RMS racine utilise les répertoires virtuels suivants dans l'arborescence du site web par défaut :



Ces répertoires virtuels hébergent les services web utiles à la gestion du cluster AD RMS. La console de gestion est configurée pour pointer vers l'URL du cluster AD RMS en utilisant les protocoles HTTP ou HTTPS selon la configuration du gestionnaire des services Internet (IIS). En environnement de production, il est préférable de sécuriser l'accès au cluster AD RMS en implémentant l'authentification SSL, offrant ainsi une protection par certificat.

Les répertoires virtuels dédiés à la gestion des services de gestion de droits sont stockés localement dans le répertoire suivant : **C:\inetpub\wwwroot_wmcs**

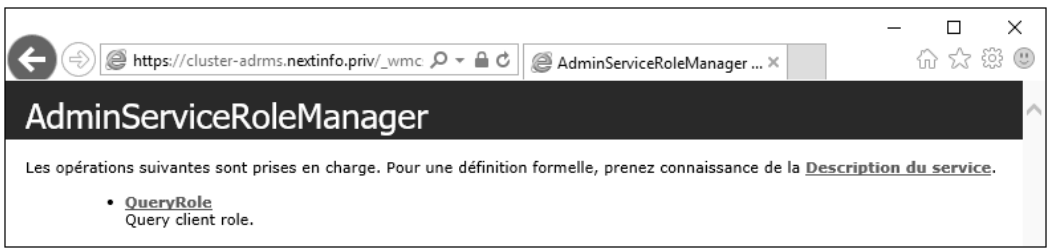


Afin de vérifier si le service web Gestionnaire de rôles AD RMS est fonctionnel, il suffit d'accéder à l'URL suivante :

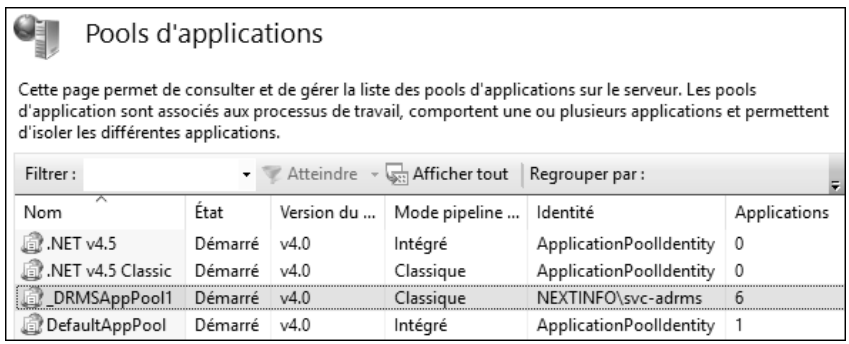
http://<Alias DNS du cluster>/_wmcs/admin/RoleMgr.asmx

ou

https://<Alias DNS du cluster>/_wmcs/admin/RoleMgr.asmx



Les services web AD RMS sont gérés au travers d'un pool d'applications nommé **_DRMSAppPool1**. Ce pool d'application utilise le compte de service renseigné durant l'installation du rôle de serveur AD RMS en se basant sur le **Framework .NET 4.0.30319** :



Le gestionnaire de licences AD RMS est accessible via l'URL suivante :

https://cluster-adrms.<domaine DNS>/_wmcs/licensing

Il est cependant possible de modifier à tout moment l'URL du gestionnaire de licences via les propriétés du cluster AD RMS, en cliquant sur l'onglet **URL du cluster**. Dans ce même onglet, il est possible de configurer des URL Extranet, afin de rendre AD RMS disponible à l'extérieur du réseau de l'entreprise :

Le gestionnaire de certificat AD RMS est accessible via l'URL suivante :

https://cluster-adrms.<domaine DNS>/_wmcs/certification/certification.asmx