Chapitre 1
Rôles et fonctionnalités

1. Organisation du livre

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

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

– **AD1**, **AD2**, **SV1** et **SRVCore** exécutant Windows Server 2016.

– Une machine cliente **CL10-01** sous Windows 10.

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

Certains scripts ou modèles d'administration au format ADM peuvent être téléchargés au niveau de la page de présentation du livre sur le site des Éditions ENI.

2. Les rôles

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

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

2.1 Accès à distance

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

Les services de rôle disponibles sont :

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

2.2 Hyper-V

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

2.3 DHCP (Dynamic Host Configuration Protocol)

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

2.4 DNS (Domain Name System)

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

2.5 IIS (Internet Information Services)

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

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

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

2.6 AD DS (Active Directory Domain Services)

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

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

2.7 AD FS (Active Directory Federation Services)

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

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

Plusieurs services de rôle le composent :

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

2.8 AD RMS (Active Directory Rights Management Services)

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

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

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

- **Active Directory Rights Management Server** : permet de protéger une ressource d'une utilisation non autorisée.
- **Prise en charge de la fédération des identités** : profite des relations fédérées entre deux organisations pour établir l'identité de l'utilisateur et lui fournir un accès à une ressource protégée.

2.9 AD CS (Active Directory Certificate Service)

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

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

- **Autorité de certification** : fournit une infrastructure à clé publique.
- **Inscription de l'autorité de certification via le web** : une interface web est installée afin de permettre à un utilisateur d'effectuer des demandes et renouvellements de certificats. Il est également possible de récupérer des listes de révocation de certificats ou d'effectuer une inscription à des certificats de cartes à puce.

– **Répondeur en ligne** : permet la gestion et la distribution des informations de statut de révocation.
– **Service d'inscription de périphérique réseau** : émet et gère les certificats des routeurs et des autres périphériques réseaux.
– **Service web Inscription de certificats** : ce service de rôle donne la possibilité aux utilisateurs et ordinateurs d'effectuer l'inscription et le renouvellement de certificats.
– **Service web Stratégie d'inscription de certificats** : donne aux utilisateurs et ordinateurs des informations sur la stratégie d'inscription de certificats.

2.10 Service de déploiement Windows (WDS)

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

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

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

2.11 Service de stratégie et d'accès réseau

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

Les services de rôle disponibles sont :

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

2.12 WSUS

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

Trois services de rôle sont disponibles :

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

2.13 Services de fichiers et iSCSI

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

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

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