Collection Certifications

Préparation à la certification **MCSA**

Windows Server 2016

Gestion des identités

EXAMEN N°70-742

77 travaux pratiques
155 questions réponses

OFFERT :
UN EXAMEN BLANC en ligne
avec réponses commentées et détaillées

Armelin ASIMANE
Vahé TOULOUMIAN

eni

À propos de ce livre

Chapitre 1 Présentation de Windows Server 2016

Chapitre 5 Les services de fichiers avancés

Chapitre 7 **Déploiement distribué AD DS**

Chapitre 8 **Sites et services Active Directory**

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.

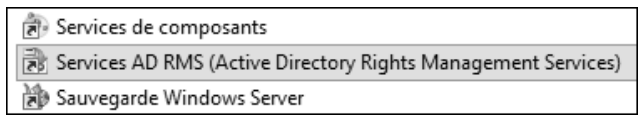
L'installation d'un serveur AD RMS crée un premier serveur dans un cluster racine. Ce cluster n'a rien à voir avec les technologies de clustering Microsoft ou de répartition de charge réseau. Un cluster racine AD RMS apporte simplement une solution de haute disponibilité pour les requêtes utilisateurs 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 :

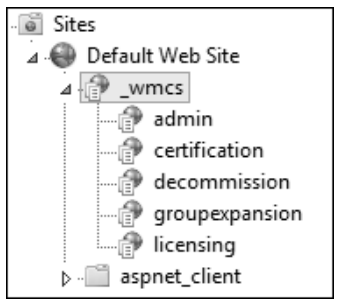
- **Stockage centralisé** : cela permet de stocker la clé de chiffrement dans la base de données du cluster AD RMS. Ainsi, chaque serveur qui rejoint le cluster peut récupérer automatiquement la clé de chiffrement sans intervention de l'administrateur.
- **Stockage manuel** : cela oblige à sélectionner 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**

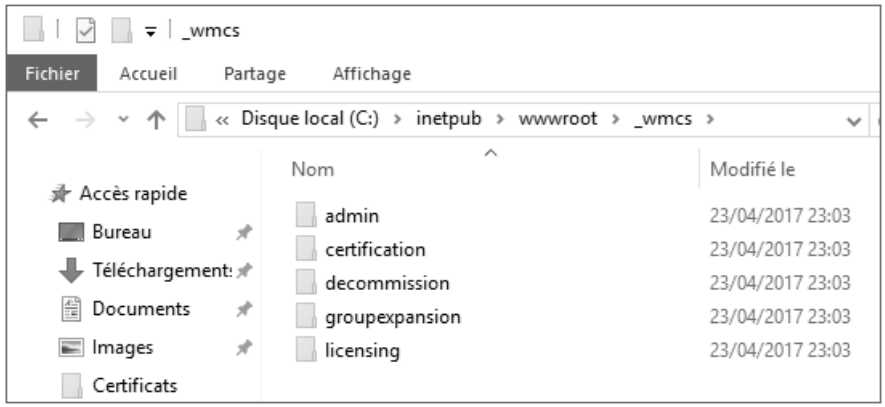


Le cluster AD RMS racine est quant à lui accessible via une URL qu'il est préférable d'associer à un alias DNS à déclarer au préalable dans le serveur de noms de votre organisation. Le cluster AD RMS racine utilise les répertoires virtuels suivants dans l'arborescence du site web par défaut :



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**

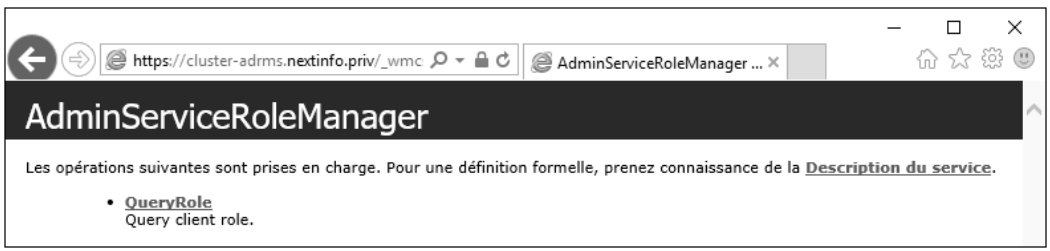


Afin de vérifier si le service web Gestionnaire de rôles AD RMS est fonctionnel, il suffit d'accéder à l'URL suivante :

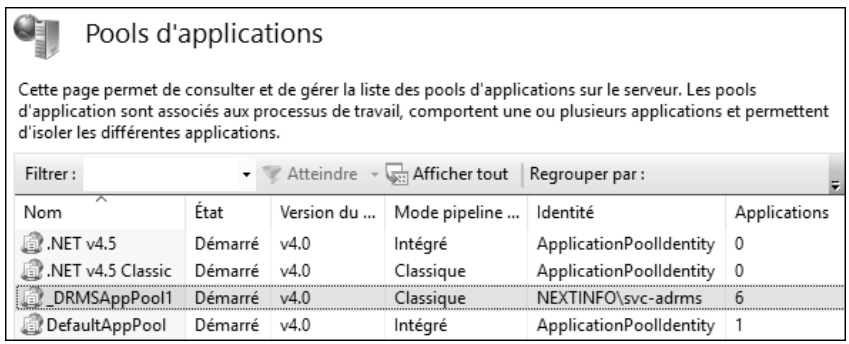
http://<Alias DNS du cluster>/_wmcs/admin/RoleMgr.asmx

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