

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



eni

Armelin ASIMANE
Vahé TOULOUMIAN

À propos de ce livre

A. Avant-propos	16
1. À propos du livre	16
B. Conditions requises	17
1. Niveau/connaissances	17
2. Certifications précédentes	17
3. Matériel nécessaire pour les travaux pratiques	17
C. Le cursus de certification Microsoft	18
1. Détails du cursus MCSA	19
2. Détails du cursus MCSE	19

Chapitre 1**Présentation de Windows Server 2016**

A. Windows Server 2016	22
B. Nouvelle interface graphique	23
1. Menu Démarrer	24
2. Panneau de configuration et paramètres	26
a. Panneau de configuration	26
b. Nouvelle apparence des paramètres	26
3. Les programmes	28
4. Les raccourcis-clavier utiles	30
C. Déploiement de Windows Server 2016	31
1. Installation complète	32
2. Installation minimale (Server Core)	32
D. L'adressage IP	34
1. Adressage IP dynamique	34
2. Adressage IP statique	34
E. Les protocoles réseau	34
1. Modèle TCP/IP	34
2. Protocole IP	35
a. Adressage IPv4	35
b. Adressage IPv6	35
F. L'administration de Windows Server 2016	36
1. La console Gestion de l'ordinateur	36
2. La console Gestionnaire de serveur	38
3. Les outils d'administration	39

G. Travaux pratiques	39
1. Installer Windows Server 2016 en mode graphique	40
2. Installer Windows 2016 en mode Server Core.	48
3. Configurer l'interface réseau	52
4. Renommer un serveur avec sconfig.	57
5. Configurer l'adressage IP avec sconfig	59
H. Résumé du chapitre	62
I. Validation des acquis : questions/réponses	63

Chapitre 2

Les services de domaine Active Directory

A. Présentation d'Active Directory	68
1. Service d'annuaire	68
2. Gestion du service d'annuaire	69
a. Administrer Active Directory	70
b. Partitions Active Directory	74
3. Gestion des identités et des accès	75
4. Gestion des unités d'organisation	76
a. Ajouter une OU via l'interface graphique	77
b. Ajouter une OU via les commandes DOS.	81
c. Ajouter une OU avec PowerShell.	81
B. Forêts et domaines Active Directory	82
1. Forêts	82
2. Domaines	82
3. Arbres de domaines	83
C. Niveaux fonctionnels	83
1. Niveaux fonctionnels de forêt	83
2. Niveaux fonctionnels de domaine	84
3. Augmenter le niveau fonctionnel	85
D. Contrôleurs de domaine	86
1. Rôles FSMO	87
2. Catalogue global	90
3. Mise à niveau d'un contrôleur de domaine	93
4. Configuration du clonage d'un contrôleur de domaine	94
E. Mise en œuvre de la jointure de domaine hors ligne	95

F. Gestion des comptes d'utilisateurs	96
1. Administration des comptes d'utilisateurs	97
2. Création des comptes d'utilisateurs	97
a. Par lignes de commandes DOS	97
b. Par lignes de commandes PowerShell	98
3. Gestion des comptes inactifs et désactivés avec PowerShell	99
4. Délégation de la gestion des paramètres de mot de passe	99
G. Gestion des groupes de sécurité	101
1. Groupes globaux	102
2. Groupes de domaine locaux	102
3. Groupes universels	102
4. Gestion de l'appartenance à un groupe via les stratégies de groupe	103
5. Délégation de la création et de la gestion de groupes	104
H. Travaux pratiques	107
1. Installer le rôle AD DS via l'interface graphique	108
2. Installer le rôle AD DS sur une installation minimale	112
I. Résumé du chapitre	116
J. Validation des acquis : questions/réponses	116

Chapitre 3**Les stratégies de groupe**

A. Création et gestion d'objets de stratégies de groupe	120
1. Gestion des stratégies de groupe	120
2. Configuration d'un magasin central	122
3. Configuration des liens de GPO	123
4. Importation et exportation des GPO	124
5. Configuration des stratégies de groupe locales	126
6. Dépannage des stratégies de groupe	128
B. Configuration du traitement de la stratégie de groupe	129
1. Configuration de l'ordre et de la priorité du traitement	129
2. Configuration du blocage de l'héritage	130
3. Configuration du filtrage de sécurité	131
4. Mise à jour forcée de la stratégie de groupe	132
C. Configuration des paramètres d'une stratégie de groupe	133
1. Configuration de l'installation du logiciel	133
2. Configuration de la redirection des dossiers	134
3. Configuration de scripts	136

D. Configuration des préférences de la stratégie de groupe	137
1. Configuration des préférences d'imprimantes	137
2. Définition des mappages de lecteur réseau	138
3. Configuration des options d'alimentation	139
4. Configuration des paramètres de registre personnalisés	140
5. Configuration du déploiement des fichiers et des dossiers	140
6. Configuration du déploiement des raccourcis	142
7. Configuration du ciblage au niveau de l'élément	143
E. Travaux pratiques	144
1. Créer l'arborescence d'Unité d'organisation et les comptes AD	145
2. Créer une GPO d'installation de logiciel	145
3. Créer des préférences de stratégies de groupe	149
F. Résumé du chapitre	154
G. Validation des acquis : questions/réponses	154

Chapitre 4

Les services réseau avancés

A. Service DNS	158
1. Présentation du service DNS	159
2. Fonctionnement du service DNS	160
a. Outils en lignes de commandes DOS	161
b. Principe de résolution de noms DNS	162
3. Gestion du service DNS	163
a. Implémentation des événements détaillés	165
b. Enregistrements DNS	167
c. Nettoyage des enregistrements DNS	171
d. Redirecteurs du service DNS	174
e. Sauvegarde de la configuration DNS	176
4. Zones DNS	177
a. Zone principale	178
b. Zone secondaire	178
c. Zone de recherche inversée	179
d. Zone de stub	179
e. Zone GlobalNames	179
5. DNS et Active Directory	186
6. Sécurité du service DNS	187
a. Sécuriser le cache DNS	187
b. Configurer le pool de sockets DNS	188

c. Implémenter DNSSEC	190
7. Gestion du service DNS via Windows PowerShell.	192
B. Service DHCP	193
1. Présentation du service DHCP.	193
2. Gestion du serveur DHCP	193
3. Fonctionnement du service DHCP	195
a. Principe d'attribution d'une adresse IP en IPv4	196
b. Principe d'attribution d'une adresse IP en IPv6	197
4. Options de configuration du service DHCP.	198
5. Gestion du service DHCP via Windows PowerShell	203
6. Haute disponibilité du service DHCP	204
7. Sauvegarde et restauration du service DHCP	205
a. Sauvegarde automatique	205
b. Sauvegarde manuelle	206
c. Restauration	206
C. IPAM	207
1. Présentation du serveur IPAM	207
2. Installation et configuration de la gestion d'adresses IPAM.	210
3. Gestion de l'espace d'adressage IP	218
a. Plages d'adresses IP	219
b. Adresses IP	221
c. Blocs d'adresses IP	222
4. Surveillance et gestion d'IPAM	223
a. Serveurs DNS et DHCP.	223
b. Étendues DHCP.	224
c. Analyse des zones DNS.	224
d. Groupes de serveurs.	224
5. Catalogue des événements	225
D. Travaux pratiques	226
1. Installer et configurer le service DNS	227
2. Configurer le service DNS avec DNSSEC.	248
3. Installer et configurer le service DHCP.	260
4. Installer et configurer la haute disponibilité du service DHCP	274
E. Résumé du chapitre	283
F. Validation des acquis : questions/réponses	283

Chapitre 5**Les services de fichiers avancés**

A. Présentation des services de fichiers	288
1. Fonctionnement des services de fichiers	288
2. Gestion des services de fichiers	289
a. Administrer les services de fichiers	290
b. Rôles et services de stockage	295
B. Stockage réseau	297
1. Stockage SAN iSCSI	297
a. Fonctionnement du stockage iSCSI	298
b. Gestion du stockage iSCSI	300
2. Stockage SAN FCoE	301
3. Stockage NFS	301
4. Stockage DAS	301
5. Stockage NAS	301
C. Optimiser l'usage du stockage	302
1. Gestionnaire de ressources	302
a. Fonctionnement de FSRM	302
b. Gestion de FSRM	303
2. Gestion de quota	304
a. Création d'un quota	305
b. Création d'un modèle de quota	309
3. Gestion du filtrage de fichiers	311
a. Création d'un filtre de fichiers	312
b. Création d'un modèle de filtre	314
4. Gestion de la classification	317
a. Création d'une propriété de classification	318
b. Création d'une règle de classification	319
5. Gestion des rapports de stockage	322
D. Déduplication des données	323
1. Installer la déduplication des données	325
2. Activer la déduplication des données	326
3. Vérifier la déduplication	327
E. BranchCache	328
1. Présentation de BranchCache	328
a. Fonctionnement de BranchCache	328
b. Gestion de BranchCache	329

2. Mode de cache	332
a. Mode de cache hébergé	332
b. Mode de cache distribué.	333
3. Déploiement de BranchCache	334
F. Travaux pratiques	335
1. Créer une infrastructure iSCSI	336
2. Implémenter BranchCache	346
G. Résumé du chapitre	364
H. Validation des acquis : questions/réponses	364

Chapitre 6**Contrôle d'accès dynamique**

A. Contrôle d'accès dynamique.	368
1. Présentation du DAC.	368
2. Fonctionnement du DAC	368
a. Revendications.	370
b. Stratégie d'accès central	370
c. Règle d'accès central	371
3. Gestion du DAC	371
4. Implémentation du DAC.	373
B. Travaux pratiques	374
1. Configurer Kerberos	376
2. Créer les revendications	377
3. Configurer les propriétés.	380
4. Configurer la classification	382
5. Configurer une règle d'accès central.	388
6. Créer une stratégie d'accès central	391
7. Publier une stratégie d'accès	394
8. Tester l'accès aux ressources	397
C. Résumé du chapitre	398
D. Validation des acquis : questions/réponses	398

Chapitre 7	Déploiement distribué AD DS
A. Présentation du déploiement distribué AD DS	402
1. Gestion de forêts Active Directory	402
a. Gestion administrative	402
b. Partitions	403
2. Gestion de domaines Active Directory	403
a. Gestion administrative	403
b. Partitions	403
3. Déploiement distribué AD DS	403
a. Domaines ou forêts multiples	404
b. Mise à jour vers Windows Server 2016	405
c. Migration vers Windows Server 2016	406
d. Relations d'approbation	407
e. Routage des suffixes de noms	411
B. Travaux pratiques	414
1. Ajouter un domaine dans la forêt	414
2. Configurer une approbation AD DS	419
C. Résumé du chapitre	423
D. Validation des acquis : questions/réponses	424
Chapitre 8	Sites et services Active Directory
A. Présentation des sites Active Directory	428
1. Objectif des sites	428
a. Gestion des sites	429
b. Localisation des services	430
2. Les sites	430
3. Les sous-réseaux	430
4. Les serveurs de catalogue global	431
5. Les partitions Active Directory	432
6. Les liens de sites	432
a. Fonctionnement des liens de sites	433
b. Gestion des liens de sites	434
7. Les ponts de sites	436
B. Travaux pratiques	436
1. Renommer le site par défaut	437
2. Créer un site	438
3. Affecter des serveurs à un site	439

4. Créer des sous-réseaux.	440
5. Configurer le catalogue global	443
6. Configurer la mise en cache	443
C. Résumé du chapitre	445
D. Validation des acquis : questions/réponses	445

Chapitre 9**Répliquions Active Directory**

A. Présentation de la répliquions Active Directory	448
1. Répliquions Active Directory.	448
a. Planification des répliquions	449
b. Topologie de répliquions.	450
c. Objets de connexion	452
d. Répliquions vers des RODC	457
e. Répliquions des mots de passe (RODC)	458
f. Les conflits de répliquions	460
2. Répliquions SYSVOL	461
a. Présentation du répertoire SYSVOL	461
b. Répliquions du répertoire SYSVOL	463
3. Surveillance et dépannage	464
B. Travaux pratiques	465
1. Configurer la répliquions	466
2. Configurer la stratégie RODC	470
3. Surveiller la répliquions	477
C. Résumé du chapitre	480
D. Validation des acquis : questions/réponses	481

Chapitre 10**Services de certificats AD CS**

A. Infrastructures à clés publiques.	486
1. Présentation des PKI	486
2. Composants d'une PKI	488
3. Chiffrement.	489
B. Présentation d'AD CS.	489
1. Services de certificats AD CS	489
a. CA autonome.	490
b. CA d'entreprise	490
c. Gestion d'AD CS	490

2.	Hiérarchie de CA	492
a.	Infrastructure à deux couches	492
b.	Infrastructure à trois couches	493
c.	CA racine	495
d.	CA intermédiaire.	496
e.	CA émettrice	496
3.	Services de rôles AD CS	496
a.	Autorité de certification	496
b.	Demande de certificats via le web	497
c.	Répondeur en ligne	497
d.	Inscription de composants réseau	497
e.	Inscription des certificats.	497
f.	Stratégie des certificats	498
4.	Certificats	498
a.	Modèles de certificats	499
b.	Demande de certificat.	501
c.	Renouvellement de certificat.	501
d.	Configuration de l'archivage des clés	504
C.	Travaux pratiques	506
1.	Installer une CA autonome.	507
2.	Installer une CA d'entreprise	519
3.	Activer une CA émettrice	525
4.	Publier un certificat via des GPO	529
5.	Configurer l'interface Web	529
6.	Demander un certificat	538
D.	Résumé du chapitre	541
E.	Validation des acquis : questions/réponses	542

Chapitre 11

Services de gestion des droits

A.	Services de gestion des droits.	546
1.	Présentation d'AD RMS	546
a.	Fonctionnement d'AD RMS.	547
b.	Gestion d'AD RMS	548
c.	Composants d'AD RMS.	554
2.	Installation et configuration d'AD RMS.	554
a.	Schématiser l'infrastructure	554
b.	Prérequis d'installation.	555

3. Protection du contenu des fichiers	555
4. Sauvegarde d'AD RMS	557
B. Travaux pratiques	557
1. Préparer le déploiement AD RMS	558
2. Installer AD RMS	563
3. Post-installation AD RMS	565
4. Configurer la console AD RMS	570
5. Configurer les super utilisateurs	572
6. Configurer un modèle de stratégies	573
7. Créer une stratégie d'exclusion	578
8. Protéger du contenu	579
C. Résumé du chapitre	586
D. Validation des acquis : questions/réponses	586

Chapitre 12**Services de fédération AD FS**

A. Services de fédération	590
1. Présentation d'AD FS	591
a. Fonctionnement d'AD FS	591
b. Gestion d'AD FS	592
2. Revendications	593
3. Infrastructure AD FS	593
a. Infrastructure	594
b. Composants	595
4. Installation et configuration d'AD FS	596
B. Mise en œuvre du proxy d'application web	597
1. Installation et configuration du proxy d'application web	598
a. Installation	598
b. Configuration	599
2. Mise en œuvre de WAP en mode pass-through	600
3. Mise en œuvre de WAP en tant que Proxy AD FS	601
C. Travaux pratiques	601
1. Préparer le déploiement d'AD FS	602
2. Installer les serveurs AD FS	606
3. Configurer la signature de jetons	609
4. Configurer les revendications	609
5. Installer les proxy AD FS	610
D. Résumé du chapitre	611

E. Validation des acquis : questions/réponses	611
---	-----

Chapitre 13

La répartition de charge

A. Répartition de charge	614
1. Présentation de la répartition	614
a. Technologies existantes	615
b. Avantages et inconvénients	615
B. Répartition de charge réseau	617
1. Network Load Balancing	617
2. Différents modes de répartition	618
a. Prioritaire	618
b. Mode égal	619
c. Mode manuel	619
3. Modes de transmission	620
a. Unicast - Monodiffusion	620
b. Multicast - Multidiffusion	621
c. Multidiffusion IGMP	621
4. Affinité de répartition de charge	621
5. Convergence et haute disponibilité	622
C. Travaux pratiques	623
1. Installer et configurer le NLB	624
2. Gérer un cluster NLB	631
3. Gérer un cluster via PowerShell	640
4. Simuler la répartition de charge	642
D. Résumé du chapitre	645
E. Validation des acquis : questions/réponses	645

Chapitre 14

Cluster et haute disponibilité

A. Haute disponibilité	648
1. Présentation de la haute disponibilité	648
2. Solutions de haute disponibilité	649
B. Clusters de basculement	649
1. Présentation des clusters	649
2. Fonctionnement d'un cluster	649
a. Réseaux	650
b. Basculement	651

c. Volumes partagés	653
d. Console de gestion du cluster	654
e. Administration d'un cluster de basculement.	655
f. Quorum	658
g. Installation et configuration d'un cluster	659
h. Les rôles	661
i. Optimisation des CSV	662
C. Travaux pratiques	662
1. Installer IIS sur chaque nœud	664
2. Connecter les nœuds au disque iSCSI	664
3. Créer un cluster de serveurs	665
4. Créer un volume partagé de cluster	670
5. Configurer un rôle de serveur	670
6. Simuler une panne dans le cluster	672
D. Résumé du chapitre	672
E. Validation des acquis : questions/réponses	673

Chapitre 15

Cluster de basculement Hyper-V

A. Virtualisation avec Hyper-V	678
1. Présentation d'Hyper-V	678
a. Installation du rôle Hyper-V	680
b. Gestion d'Hyper-V	681
c. Gestion d'Hyper-V via SCVMM	682
B. Haute disponibilité avec Hyper-V	682
1. Réplication	682
2. Clusters de basculement	682
3. Migration des machines virtuelles	683
C. Travaux pratiques	684
1. Préparer le stockage Hyper-V	685
2. Installer le rôle Hyper-V	688
3. Importer des machines virtuelles	691
4. Configurer la réplication Hyper-V	691
5. Configurer la réplication d'une VM	693
6. Configurer le basculement de cluster	695
7. Migrer une machine virtuelle	696
8. Migrer le stockage d'une VM	697
9. Redimensionner un VHDX à chaud	697

D. Résumé du chapitre	699
E. Validation des acquis : questions/réponses	699

Chapitre 16**Sauvegarde et restauration**

A. Présentation de la récupération d'urgence	702
1. Récupération d'urgence	702
2. Présentation de la sauvegarde	704
3. Sauvegarde Windows Server.	705
a. Gestion de la sauvegarde Windows Server.	707
b. Planification de la sauvegarde Windows	708
c. Configuration de la sauvegarde Windows	710
d. Configuration de la restauration des données	710
e. Défragmentation hors ligne de la base de données Active Directory	712
f. Nettoyage de métadonnées de la base d'annuaire Active Directory	714
B. Récupération des données.	714
1. Clichés instantanés.	714
2. Corbeille Active Directory	717
C. Travaux pratiques	718
1. Installer un outil de sauvegarde	719
2. Configurer la sauvegarde Windows	719
3. Restaurer des données.	728
4. Microsoft Azure Backup.	730
D. Résumé du chapitre	742
E. Validation des acquis : questions/réponses	742

Tableau des objectifs	745
---------------------------------	-----

Index.	747
----------------	-----

Chapitre 11

A. Services de gestion des droits	546
B. Travaux pratiques	557
C. Résumé du chapitre	586
D. Validation des acquis : questions/réponses	586



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.

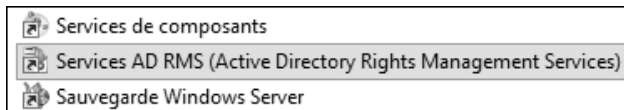
L'installation d'un serveur AD RMS crée un premier serveur dans un cluster racine. Ce cluster n'a rien à voir avec les technologies de clustering Microsoft ou de répartition de charge réseau. Un cluster racine AD RMS apporte simplement une solution de haute disponibilité pour les requêtes utilisateurs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

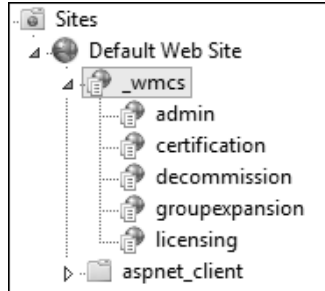
- **Stockage centralisé** : cela permet de stocker la clé de chiffrement dans la base de données du cluster AD RMS. Ainsi, chaque serveur qui rejoint le cluster peut récupérer automatiquement la clé de chiffrement sans intervention de l'administrateur.
- **Stockage manuel** : cela oblige à sélectionner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

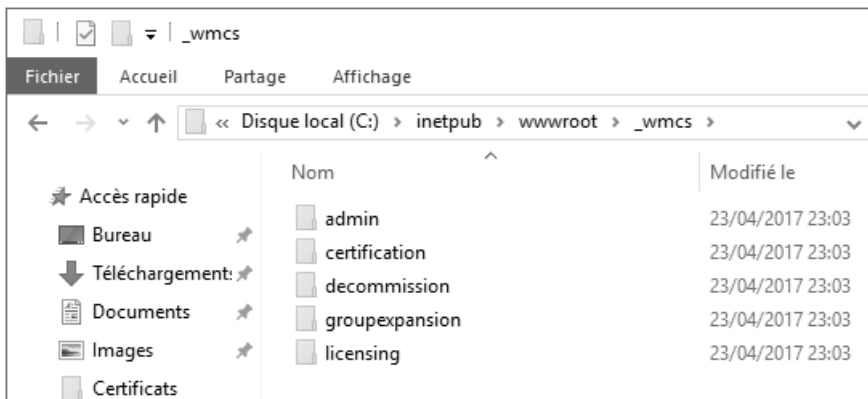


Le cluster AD RMS racine est quant à lui accessible via une URL qu'il est préférable d'associer à un alias DNS à déclarer au préalable dans le serveur de noms de votre organisation. Le cluster AD RMS racine utilise les répertoires virtuels suivants dans l'arborescence du site web par défaut :



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`

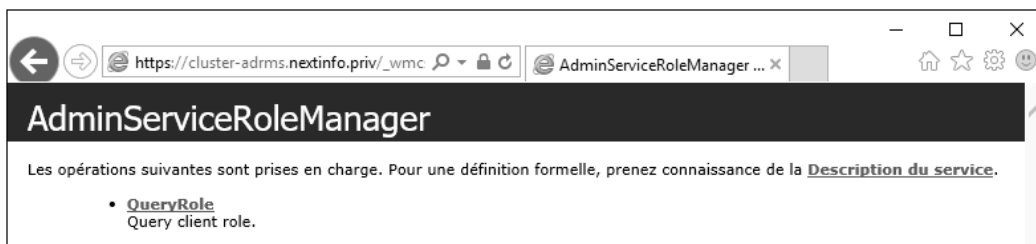


Afin de vérifier si le service web Gestionnaire de rôles AD RMS est fonctionnel, il suffit d'accéder à l'URL suivante :

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** :

Pools d'applications

Cette page permet de consulter et de gérer la liste des pools d'applications sur le serveur. Les pools d'application sont associés aux processus de travail, comportent une ou plusieurs applications et permettent d'isoler les différentes applications.

Nom	État	Version du ...	Mode pipeline ...	Identité	Applications
.NET v4.5	Démarré	v4.0	Intégré	ApplicationPoolIdentity	0
.NET v4.5 Classic	Démarré	v4.0	Classique	ApplicationPoolIdentity	0
_DRMSAppPool1	Démarré	v4.0	Classique	NEXTINFO\svc-adrms	6
DefaultAppPool	Démarré	v4.0	Intégré	ApplicationPoolIdentity	1

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 :

Propriétés de : cluster-adrms.nextinfo.priv (Local)

Paramètres du proxy Enregistrement Point de connexion de service

Général URL du cluster Serveurs AD RMS Certificat du serveur

Les URL suivantes sont utilisées par les clients AD RMS pour se connecter au cluster Gestionnaire de licences et de certification.

URL intranet

Gestionnaire de licences : [https:// cluster-adrms.nextinfo.priv/_wmcs/licensing](https://cluster-adrms.nextinfo.priv/_wmcs/licensing)

Certification : https://cluster-adrms.nextinfo.priv/_wmcs/certification

URL extranet

Points de connexion utilisés par les clients extranet pour les services fournis par les clusters.

Gestionnaire de licences : http://_wmcs/licensing

Certification : http://_wmcs/certification

OK Annuler Appliquer Aide

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

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