



Ressourcesinformatiques

# Windows Server 2016

Architecture et Gestion  
des services de domaine  
Active Directory (AD DS)



Jean-François  
APREA



Les éléments à télécharger sont disponibles à l'adresse suivante :  
**<http://www.editions-eni.fr>**  
Saisissez la référence ENI de l'ouvrage **RI16WINAD** dans la zone de recherche  
et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

## Avant-propos

### Chapitre 1 Introduction aux services AD DS

1. Rôle du service d'annuaire dans l'entreprise. . . . .	19
2. Positionnement et innovations dans Windows Server . . . . .	21
2.1 Version majeure de Windows Server « Cloud OS » . . . . .	21
2.2 Évolutions en matière de sécurité . . . . .	23
2.3 Accès aux applications et mobilité . . . . .	23
2.4 Évolutions apportées par Windows Server 2008 R2, Windows Server 2012 R2 et Windows Server 2016 . . . . .	23
2.4.1 Innovations apportées à Active Directory . . . . .	25
2.4.2 AD DS : Audit . . . . .	25
2.4.3 AD DS : Gestion granulaire des stratégies de mot de passe . . .	26
2.4.4 AD DS : Contrôleurs de domaine en lecture seule . . . . .	26
2.4.5 AD DS : Redémarrage des services de domaine Active Directory . . . . .	27
2.4.6 AD DS : Aide à la récupération des données . . . . .	27
2.5 Intégration de l'innovation au sein de Windows Server . . . . .	27
3. Services fondamentaux et protocoles standards . . . . .	28

## Chapitre 2

### DNS : concepts, architecture et administration

1.	Introduction aux services de résolution de noms DNS . . . . .	31
1.1	Un peu d'histoire . . . . .	31
1.2	Que sont les services DNS ? . . . . .	33
1.3	Terminologie du système DNS . . . . .	35
1.3.1	L'espace de noms DNS (Domain Namespace) . . . . .	35
1.3.2	Hiérarchie DNS et espace de noms Internet . . . . .	40
1.4	Le DNS : base de données distribuée . . . . .	40
2.	Structure de l'espace DNS et hiérarchie des domaines . . . . .	43
2.1	Le domaine racine . . . . .	43
2.2	Les domaines de premier et deuxième niveau . . . . .	44
3.	Les enregistrements de ressources . . . . .	46
4.	Domaines, zones et serveurs DNS . . . . .	47
4.1	Domaines DNS et zones DNS . . . . .	48
4.2	Zones et fichiers de zones . . . . .	49
4.3	Noms de domaines DNS et noms de domaines Active Directory . . . . .	57
4.4	Types de zones et serveurs de noms DNS . . . . .	59
4.4.1	Serveurs de noms et zones primaires . . . . .	60
4.4.2	Serveurs de noms et zones secondaires . . . . .	63
4.4.3	Types de transferts de zones DNS . . . . .	67
4.4.4	Serveurs de cache et serveurs DNS . . . . .	70
5.	Mise en œuvre des zones standards : bonnes pratiques . . . . .	70
6.	Délégation des zones . . . . .	74
7.	Utilisation des redirecteurs . . . . .	77
7.1	Exposition du réseau privé sur Internet . . . . .	78
7.1.1	Le bon usage des redirecteurs pour optimiser les résolutions DNS . . . . .	79
7.1.2	Comportement des serveurs DNS avec ou sans l'usage d'un redirecteur . . . . .	79
7.1.3	Redirecteurs et types de requêtes DNS . . . . .	79
8.	Zones de stub . . . . .	80
8.1	Contenu d'une zone de stub . . . . .	80
8.2	Avantages des zones de stub . . . . .	81
8.3	Mise à jour des zones de stub . . . . .	82

8.3.1 Opérations sur les zones de stub . . . . .	82
9. Redirecteurs, zones de stub et délégation : bonnes pratiques . . . . .	84
10. Gestion des noms multihôtes . . . . .	85
11. Vieillessement et nettoyage des enregistrements DNS . . . . .	86
12. Options de démarrage du serveur DNS . . . . .	89
13. Récursivité des serveurs DNS et protection des serveurs . . . . .	93
13.1 Blocage des attaques de type Spoofing DNS . . . . .	93
13.2 Blocage des attaques de type Spoofing DNS sur les serveurs de type Internet . . . . .	93
14. Synthèse des rôles des serveurs DNS . . . . .	94
15. Commandes de gestion du service DNS . . . . .	96
15.1 La commande ipconfig . . . . .	96
15.1.1 Gestion du cache du client DNS et des enregistrements dynamiques . . . . .	96
15.1.2 Renouvellement de l'inscription du client DNS . . . . .	98
15.1.3 Nouvelles options de la commande ipconfig . . . . .	100
15.2 La commande NSLookup . . . . .	101
15.3 La commande DNSCmd . . . . .	103
15.4 La commande DNSLint . . . . .	106
15.5 La commande Netdiag . . . . .	107
16. Surveillance du service DNS . . . . .	107
16.1 Définition d'une base de référence . . . . .	108
16.2 Utilisation de la console Gestionnaire de serveur . . . . .	111
16.3 Utilisation des journaux d'événements . . . . .	113
16.4 Utilisation des journaux de débogage DNS . . . . .	115
17. Restauration des paramètres par défaut . . . . .	116
18. Interface NetBIOS et Configuration DNS du client Windows . . . . .	118
18.1 À propos de l'interface NetBIOS . . . . .	118
18.1.1 Interface NetBIOS et Configuration DNS du client Windows 10 Professionnel . . . . .	118
18.1.2 Types de noms à prendre en charge . . . . .	118
18.1.3 Positionnement de l'interface NetBIOS par rapport à TCP/IP . . . . .	119

# 4 **Windows Server 2016**

## Services de domaine Active Directory (AD DS)

18.2	Plate-forme Windows et interface NetBios . . . . .	121
18.2.1	Services NetBIOS et codes de services Microsoft. . . . .	121
18.2.2	Résolution de noms NetBIOS . . . . .	125
18.2.3	Ordre des résolutions NetBIOS. . . . .	125
18.2.4	Ordre de résolution d'un poste de travail de type H-node . . .	127
18.2.5	Interface et noms NetBIOS, résolutions WINS et domaines Active Directory . . . . .	130
18.3	Configuration d'un poste client Active Directory . . . . .	131
18.3.1	À propos des Clients Active Directory . . . . .	131
18.3.2	Postes de travail Windows et paramètres DNS nécessaires aux environnements de domaines Active Directory . . . . .	137
18.4	Demandes de résolutions DNS et NetBIOS : Processus de sélection de la méthode. . . . .	148
18.5	Test d'intégration dans Active Directory . . . . .	149
19.	Nouveautés des services DNS de Windows Server . . . . .	150
19.1	Services DNS de Windows Server 2008 R2 . . . . .	150
19.1.1	Introduction . . . . .	150
19.1.2	Chargement des zones en arrière-plan . . . . .	151
19.1.3	Support des adresses IPv6 . . . . .	152
19.1.4	Support DNS des contrôleurs de domaine en lecture seule . .	152
19.1.5	Support des zones de type GlobalNames . . . . .	153
19.1.6	Évolutions de la partie Client DNS. . . . .	156
19.1.7	Sélection des contrôleurs de domaine. . . . .	157
19.2	Nouveautés de Windows Server 2012 R2 . . . . .	159
19.3	Nouveautés de Windows Server 2016 . . . . .	160

### **Chapitre 3**

## **Intégration des zones DNS dans Active Directory**

1.	Introduction . . . . .	163
2.	Objets ordinateurs Active Directory et nommages. . . . .	164
3.	Avantages de l'intégration des zones DNS dans Active Directory . . . . .	167
3.1	Mise à jour en mode multimaître (ou maîtres multiples) . . . . .	167
3.2	Sécurité avancée des contrôles d'accès sur les zones et les enregistrements . . . . .	168
4.	Partitions d'annuaire par défaut . . . . .	173

5.	Intégration Active Directory et serveurs DNS Windows 2000 Server . . . . .	175
6.	Intégration Active Directory et serveurs DNS Windows Server 2016. . . . .	178
6.1	ForestDnsZones.NomForêtDns . . . . .	181
6.2	DomainDnsZones.NomdeDomaineDns . . . . .	181
6.3	Utilisation d'autres partitions de l'annuaire d'applications . . . . .	182
6.4	Création d'une partition dans l'annuaire d'applications Active Directory . . . . .	183
6.5	Réplication des partitions du répertoire d'applications et cas des catalogues globaux . . . . .	184
6.6	Stockage des zones, partitions d'applications et répliquions . . . . .	185
6.7	Zones DNS intégrées dans Active Directory et partitions d'annuaire AD LDS . . . . .	185
6.8	Conditions nécessaires pour réaliser un changement de stockage . . . . .	189
6.9	Indications de racines . . . . .	189
6.10	Stockage des zones dans Active Directory et enregistrements dynamiques des contrôleurs de domaines . . . . .	191
7.	Sécurisation des mises à jour dynamiques . . . . .	191
7.1	Configurer les mises à jour dynamiques sécurisées . . . . .	191
7.2	Mises à jour sécurisées et enregistrements DNS réalisés via DHCP . . . . .	195
7.3	Utilisation du groupe spécial DNSUpdateProxy pour réaliser les mises à jour dynamiques des zones DNS sécurisées . . . . .	198
7.4	Sécurisation des zones DNS et pouvoir du service serveur DHCP sur les contrôleurs de domaine Active Directory . . . . .	200
7.5	Commande Netsh et déclaration de l'authentification du serveur DHCP . . . . .	202
7.6	Conflits de gestion des autorisations sur les zones DNS . . . . .	202
8.	Intégration des serveurs DNS Windows avec l'existant . . . . .	203
8.1	À propos des RFC pris en charge par le service DNS de Windows Server 2003 et Windows Server 2008 R2 . . . . .	204
8.2	À propos des RFC 1034 et 1035 . . . . .	205
8.3	Consultation des RFC sur le Web . . . . .	205
8.4	Interopérabilité des services DNS de Windows Server . . . . .	206
8.5	Problème de compatibilité et recherche directe et inversée WINS . . . . .	206
8.6	Spécificité du service DNS de Windows Server et intégration dynamique via les serveurs DHCP . . . . .	207

# 6 **Windows Server 2016**

Services de domaine Active Directory (AD DS)

## **Chapitre 4**

### **Services de localisation AD DS et services DNS**

1. Introduction . . . . .	209
2. Service de Localisation DNS et sélection des contrôleurs de domaine . . . . .	210
3. Structure DNS et intégration dans l'annuaire Active Directory. . . . .	217
4. Enregistrements DNS Emplacement du service des contrôleurs de domaine . . . . .	220
4.1 Structure d'accueil de la zone DNS pour les enregistrements de ressources de type SRV . . . . .	220
4.1.1 À propos de l'enregistrement de ressources DNS de type SRV . . . . .	222
4.1.2 Enregistrements SRV inscrits par le service Ouverture de session réseau . . . . .	226
4.1.3 À propos de l'enregistrement DsaGuid._msdcs.NomdeForêt . . . . .	229
4.1.4 Enregistrements de ressources pour les clients non compatibles avec les enregistrements SRV . . . . .	230
4.2 Serveurs DNS non dynamiques et enregistrements dynamiques des contrôleurs de domaines . . . . .	230
4.3 À propos de la zone DNS du domaine racine de la forêt . . . . .	232
5. Contraintes et problèmes potentiels . . . . .	232
6. Contrôle rapide des enregistrements de ressources . . . . .	233
6.1 Tests des enregistrements DNS . . . . .	233
6.2 Réenregistrements des enregistrements de type SRV des contrôleurs de domaine . . . . .	235
6.3 Désenregistrement des enregistrements de type SRV des contrôleurs de domaine . . . . .	236
6.4 Nettoyage des caches du système de résolution DNS . . . . .	237

**Chapitre 5**  
**Composants de la structure logique**

- 1. Introduction aux composants de la structure logique ..... 239
- 2. Les domaines ..... 239
  - 2.1 Conteneur (container) au sein de la forêt ..... 242
  - 2.2 Niveaux fonctionnels des domaines ..... 244
  - 2.3 Gestion des stratégies au niveau des domaines ..... 248
  - 2.4 Délégation de l'administration des domaines  
et contrôle des paramètres spécifiques au domaine ..... 249
  - 2.5 Utilisation du domaine comme unité de réplication élémentaire ... 252
  - 2.6 Limites du domaine Active Directory et délégation contrainte .... 253
- 3. Contrôleurs de domaine et structure logique ..... 256
- 4. Les unités d'organisation (OU) ..... 260
- 5. Les arbres ..... 266
- 6. Les forêts ..... 277
  - 6.1 Critères, rôle et bon usage des forêts ..... 279
  - 6.2 Configuration de la forêt et domaine racine ..... 280
  - 6.3 Activation des nouvelles fonctionnalités de forêt  
de Windows Server ..... 282
  - 6.4 Unités de réplication et rôle des forêts ..... 289
  - 6.5 Maîtres d'opérations FSMO de forêts ..... 292
  - 6.6 La forêt et l'infrastructure physique Active Directory ..... 293
  - 6.7 Frontières de sécurité et rôle des forêts ..... 295
  - 6.8 Approbations au sein des forêts Active Directory ..... 297
    - 6.8.1 Bénéfices apportés par la transitivité des approbations .... 297
    - 6.8.2 Structure de la forêt et approbations ..... 298
    - 6.8.3 Approbations et objets TDO  
dans les forêts Active Directory ..... 299
    - 6.8.4 Types d'approbation supportés ..... 304
    - 6.8.5 Forêts Windows Server et approbations de forêts ..... 306
    - 6.8.6 Routage des suffixes de noms et approbations de forêts .... 308
    - 6.8.7 Utilisation de la commande Netdom pour créer  
et gérer les approbations ..... 312

# 8 \_\_\_\_\_ Windows Server 2016

## Services de domaine Active Directory (AD DS)

- 7. Réussir le processus de mise à niveau d'Active Directory vers les services de domaine Active Directory de Windows Server 2016 . . . . . 313
  - 7.1 Préparation de l'infrastructure Active Directory pour Windows Server 2016 . . . . . 314
  - 7.2 Mise en œuvre d'un nouveau contrôleur Windows Server 2016 . . . . . 317
  - 7.3 Réaffectation des rôles FSMO . . . . . 319
  - 7.4 Opérations de finalisation Post Migration . . . . . 320
    - 7.4.1 Modification des stratégies de sécurité des contrôleurs de domaine . . . . . 320
    - 7.4.2 Mise à jour des autorisations des objets GPO pour les anciens domaines migrés à partir de Windows 2003 . . . . . 322

### Chapitre 6

## Groupes, unités d'organisation et délégation

- 1. Usage des groupes en environnement Active Directory . . . . . 325
  - 1.1 Les différents types de groupes Windows . . . . . 325
    - 1.1.1 Les groupes de sécurité . . . . . 326
    - 1.1.2 Les groupes de distribution . . . . . 327
  - 1.2 Portée des groupes . . . . . 327
    - 1.2.1 Les groupes globaux . . . . . 328
    - 1.2.2 Les groupes locaux de domaine . . . . . 328
    - 1.2.3 Les groupes universels . . . . . 328
  - 1.3 Règles générales concernant les objets groupes . . . . . 329
    - 1.3.1 Bon usage des comptes de groupes . . . . . 329
    - 1.3.2 Bon usage des groupes universels . . . . . 330
- 2. Définition d'une structure d'unités d'organisation . . . . . 331
  - 2.1 Rôle des objets unités d'organisation . . . . . 331
  - 2.2 Utilisation des unités d'organisation et relation avec l'organisation de l'entreprise . . . . . 332
- 3. Délégation de l'autorité d'administration et utilisation des unités d'organisation . . . . . 334
  - 3.1 Structure basée sur la nature des objets gérés . . . . . 335
  - 3.2 Structure basée sur les tâches d'administration . . . . . 336

- 3.3 Facteurs à intégrer dans la définition d'une hiérarchie d'unités d'organisation . . . . . 336
  - 3.3.1 À propos des conteneurs par défaut . . . . . 337
  - 3.3.2 Critères d'emplacements, d'opérations et de types d'objets . . 340
- 4. Utilisation des unités d'organisation pour les stratégies de groupe . . . . . 344
- 5. Règles générales et bonnes pratiques . . . . . 345

**Chapitre 7**

**Principes fondamentaux des stratégies de groupe**

- 1. Technologie IntelliMirror . . . . . 347
  - 1.1 Introduction . . . . . 347
  - 1.2 Apports pour l'entreprise . . . . . 348
  - 1.3 Évolutions apportées aux GPO par les clients Windows 7 . . . . . 350
    - 1.3.1 Amélioration de la détection réseau (Network Location Awareness) . . . . . 351
    - 1.3.2 Multiples stratégies locales (LGPO) . . . . . 352
    - 1.3.3 Meilleure gestion des messages d'événements . . . . . 353
    - 1.3.4 Anciens ADM et nouveaux ADMX . . . . . 354
    - 1.3.5 Windows 10 prend en charge de nombreuses nouvelles catégories . . . . . 355
  - 1.4 Nouveautés apportées aux postes clients grâce aux évolutions des stratégies de groupe de Windows Server 2016 . . . . . 356
    - 1.4.1 Gestion centralisée des paramètres de gestion de l'alimentation . . . . . 356
    - 1.4.2 Possibilité de gérer les installations de périphériques USB non autorisées ainsi que la délégation de l'installation des pilotes d'impression à certains utilisateurs . . . . . 357
    - 1.4.3 Améliorations apportées aux paramètres de sécurité . . . . . 358
    - 1.4.4 Meilleure gestion des paramètres liés à Internet Explorer . . . 359
    - 1.4.5 Assignement des imprimantes en fonction du site Active Directory . . . . . 359
    - 1.4.6 Délégation de l'installation des pilotes d'impression via les GPO . . . . . 359
    - 1.4.7 Nouveaux objets GPO Starter . . . . . 360
    - 1.4.8 Paramètres du protocole NAP - Network Access Protection . 362

1.5	Préférences des stratégies de groupe de Windows Server 2016 . . . . .	364
1.5.1	Préférences ou stratégies de groupe ? . . . . .	364
1.5.2	Déploiement et prise en charge des Préférences de stratégies de groupe. . . . .	367
1.5.3	Familles de paramètres pris en charge par les Préférences de stratégies de groupe. . . . .	369
1.5.4	Opérations et Actions sur les Eléments des Préférences . . . . .	373
1.5.5	Arrêter le traitement des éléments de cette extension si une erreur survient . . . . .	374
1.5.6	Exécuter dans le contexte de sécurité de l'utilisateur connecté (option de stratégie utilisateur). . . . .	374
1.5.7	Supprimer l'élément lorsqu'il n'est plus appliqué. . . . .	374
1.5.8	Appliquer une fois et ne pas réappliquer . . . . .	374
1.5.9	Ciblage au niveau de l'élément de Préférences . . . . .	375
1.5.10	Utilisation des variables au sein de l'éditeur de cibles . . . . .	376
1.5.11	Suivi de l'exécution des Préférences des stratégies de groupe . . . . .	377
2.	Création et configuration d'objets stratégies de groupe . . . . .	379
2.1	Introduction . . . . .	379
2.2	Stratégies de groupe et relation avec les technologies . . . . .	379
2.3	Que contient une stratégie de groupe ? . . . . .	380
2.3.1	Modèles administratifs . . . . .	380
2.3.2	Règles de sécurité pour les ordinateurs et modèles de sécurité . . . . .	382
2.3.3	Gestion des applications . . . . .	388
2.3.4	Gestion de l'exécution des scripts . . . . .	392
2.3.5	Des services d'installation à distance RIS à WDS, MDT et SCCM . . . . .	393
2.3.6	Gestion des paramètres de configuration et de sécurité d'Internet Explorer . . . . .	394
2.3.7	Redirection des dossiers utilisateurs (dossiers spéciaux) . . . . .	397
2.3.8	Qu'est-ce qu'une stratégie de groupe ? . . . . .	401
2.3.9	Qu'est-ce qu'une stratégie locale ? . . . . .	402
2.4	Structure physique d'une stratégie de groupe . . . . .	404
2.4.1	Objet Conteneur de Stratégie de groupe . . . . .	404
2.4.2	Modèle de la stratégie de groupe. . . . .	406
2.4.3	Composants d'une stratégie de groupe. . . . .	407
2.4.4	Modèles de stratégie de groupe ADMX pour Windows 10. . . . .	409

2.4.5	Création du Central Store au sein du SYSVOL.....	416
2.4.6	À propos des dernières versions de modèles ADMX pour Windows 10 et Windows Server 2016.....	417
2.4.7	Recommandations sur l'administration des GPO en environnement Windows Windows 7 .....	418
2.5	Application des stratégies de groupe dans l'environnement Active Directory .....	419
2.5.1	Application à l'aide du modèle S,D,OU et ordre de traitement .....	419
2.5.2	Domaines Active Directory et domaines NT : L, S, D, OU et 4, L, S, D, OU .....	423
2.5.3	Liaisons des stratégies de groupe sur les objets Sites, Domaine, Unités d'organisation et mécanisme d'héritage ...	423
2.5.4	Liaisons et attribut gPLink .....	425
2.5.5	Sélection du contrôleur de domaine préféré.....	425
2.6	Création d'un objet stratégie de groupe avec la console GPMC ...	427
2.6.1	Création d'une stratégie de groupe non liée.....	428
2.6.2	Création d'une stratégie de groupe liée .....	428
2.6.3	Gestion des liens de stratégies de groupe.....	428
2.6.4	Suppression d'une stratégie de groupe .....	429
2.6.5	Désactivation d'une stratégie de groupe.....	430
2.6.6	Gestion des conflits de traitement des stratégies de groupe. .	430
2.6.7	Gestion du filtrage du déploiement des stratégies de groupe .	432
2.6.8	Points importants .....	434
2.6.9	Définition de filtres WMI .....	434
3.	Configuration des paramètres d'actualisation des stratégies de groupe ..	439
3.1	Rafraîchissement des stratégies de groupe .....	439
3.1.1	Rafraîchissement des stratégies en tâche de fond .....	439
3.1.2	Cycle de rafraîchissement .....	439
3.1.3	Rafraîchissement à la demande .....	440
3.2	Configuration de la fréquence de rafraîchissement des stratégies de groupe .....	440
3.3	Rafraîchissement à l'aide de Gpupdate.exe .....	442
3.4	Traitement des composants des stratégies de groupe sur les liaisons lentes .....	442
3.4.1	Traitement des paramètres de stratégie de groupe non modifiés.....	443

3.4.2	Activation de la détection de liens lents . . . . .	443
3.4.3	Forcer l'application des paramètres de stratégie même lorsqu'ils n'ont pas changé . . . . .	444
3.5	Interdiction du rafraîchissement pour les utilisateurs . . . . .	446
3.6	Traitement par boucle de rappel (Loopback) . . . . .	447
4.	Gestion des stratégies de groupe à l'aide de la GPMC . . . . .	449
4.1	Opération de sauvegarde et restauration des stratégies de groupe . .	449
4.2	Opération de copie de stratégies de groupe . . . . .	453
4.3	Opération d'importation des paramètres . . . . .	454
4.3.1	Pourquoi utiliser la fonctionnalité d'importation de la GPMC ? . . . . .	454
4.3.2	Utilisation d'une table de correspondances entre les objets de différents domaines ou forêts . . . . .	455
5.	Vérification et résolution des problèmes liés aux stratégies de groupe avec RsoP . . . . .	455
6.	Délégation du contrôle administratif sur les stratégies de groupe . . . . .	456
6.1	Accorder une délégation via le groupe Propriétaires créateurs de la stratégie de groupe . . . . .	457
6.2	Accorder une délégation à l'aide de la console de gestion GPMC . .	459
6.2.1	Accorder une délégation de liaison des stratégies de groupe . .	459
6.2.2	Accorder une délégation de modélisation des stratégies de groupe . . . . .	461
6.2.3	Accorder une délégation de création des filtres WMI . . . . .	461
7.	Recommandations pour la définition d'une stratégie de groupe pour l'entreprise . . . . .	462

## Chapitre 8

### Gestion des logiciels avec les stratégies de groupe

1.	Introduction à la gestion des logiciels . . . . .	465
1.1	IntelliMirror et la gestion des logiciels . . . . .	465
1.1.1	Change and Configuration Management = IntelliMirror plus WDS/MDT . . . . .	467
1.2	Le cycle de vie du logiciel . . . . .	467

- 2. Déploiement de logiciels ..... 472
  - 2.1 Les différentes étapes ..... 472
    - 2.1.1 Disposer d'un package MSI ..... 472
    - 2.1.2 Déployer le logiciel : distribution et Ciblage ..... 473
    - 2.1.3 Assurer la maintenance du logiciel ..... 477
    - 2.1.4 Supprimer le logiciel ..... 477
  - 2.2 Technologie Windows Installer et types de Packages ..... 477
    - 2.2.1 Logiciels au format Microsoft Windows Installer ..... 477
    - 2.2.2 Applications repackagées en format MSI ..... 480
    - 2.2.3 Fichiers .Zap ..... 481
    - 2.2.4 Remarques générales concernant les différents formats d'installation ..... 485
- 3. Configuration du déploiement des logiciels ..... 486
  - 3.1 Création d'un nouveau déploiement d'applications ..... 486
    - 3.1.1 Création ou modification d'une stratégie de groupe ..... 486
    - 3.1.2 Configuration des options de déploiement ..... 489
    - 3.1.3 Association des extensions de fichiers ..... 492
    - 3.1.4 Création des catégories des applications publiées ..... 493
- 4. Maintenance des logiciels déployés ..... 495
  - 4.1 Mise à niveau des applications ..... 495
  - 4.2 Déploiement des Service Packs et mises à jour ..... 498
  - 4.3 Suppression des logiciels ..... 499

**Chapitre 9**

**Configuration des rôles Active Directory**

- 1. Introduction ..... 503
  - 1.1 Services d'annuaire de Windows Server et services associés ..... 504
  - 1.2 Services de gestion des droits numériques AD RMS ..... 505
  - 1.3 Offrir un logon unifié SSO aux services Web via ADFS ..... 506
  - 1.4 Gestion des identités avec Active Directory, Azure AD et MIM 2016 ..... 507
  - 1.5 Services d'annuaire de Windows Server 2016 et services associés ... 508

2.	Fonctionnalités des services de domaine	
	AD DS de Windows Server 2016	509
2.1	Introduction	509
2.2	Rôle contrôleur de domaine et mode Server Core	510
2.2.1	À propos du mode Server Core	510
2.2.2	Limitations d'une installation en mode Server Core	512
2.2.3	Server Core et rôles Windows Server 2016	512
2.2.4	Installation de Windows Server 2016 en mode Server Core	513
2.2.5	Installation du rôle contrôleur de domaine AD DS en mode Server Core	516
2.2.6	Installation d'un contrôleur RODC en mode Server Core	517
2.3	Rôle de contrôleur de domaine en mode lecture seule	523
2.3.1	Sécurisation des mots de passe sur les contrôleurs RODC	524
2.3.2	Réplication des mots de passe sur les contrôleurs RODC	527
2.3.3	Préremplissage des mots de passe sur un contrôleur en lecture seule	531
2.3.4	Conditions requises pour déployer un contrôleur en mode lecture seule (RODC) et limitations	533
2.4	Pourquoi et comment évoluer vers le niveau fonctionnel de domaine Windows Server 2016 ?	535
2.5	Gestion des stratégies de mot de passe granulaires	538
2.6	Service d'audit Active Directory	544
2.7	Protection des objets Active Directory contre l'effacement	548
3.	Active Directory Certificate Services (AD CS)	550
3.1	Introduction aux infrastructures à clés publiques (PKI)	550
3.2	Les différents types de certificats	551
3.2.1	Introduction	551
3.2.2	Nature et contenu d'un certificat numérique	557
3.2.3	Certificats X.509 version 1	561
3.2.4	Certificats X.509 version 2	562
3.2.5	Certificats X.509 version 3	563
3.3	Les certificats et l'entreprise	574
3.3.1	Relation entre les certificats et les authentifications	574
3.3.2	Cadre d'utilisation des certificats	576
3.3.3	Utilisation des certificats numériques en entreprise	583
3.3.4	Certificats utilisateurs	585
3.3.5	Certificats pour les ordinateurs	586

- 3.3.6 Certificats pour les applications . . . . . 587
- 3.4 Stockage des certificats . . . . . 588
  - 3.4.1 Introduction . . . . . 588
  - 3.4.2 Stockage des certificats et interface CryptoAPI . . . . . 589
  - 3.4.3 Affichage des certificats : magasin logique  
et magasin physique . . . . . 592
  - 3.4.4 Archivage local des certificats expirés . . . . . 592
  - 3.4.5 Structure de rangement du magasin logique de certificats . . . . . 592
  - 3.4.6 Origine des certificats stockés dans les magasins . . . . . 595
  - 3.4.7 Protection et stockage des clés privées . . . . . 596
- 3.5 Console de gestion MMC des certificats . . . . . 598
- 3.6 Évolution des interfaces cryptographiques de Windows . . . . . 598
  - 3.6.1 Interface CNG (Cryptographic API Next Generation) . . . . . 598
- 4. Services de certificats de Windows Server 2016 . . . . . 600
  - 4.1 Introduction . . . . . 600
  - 4.2 Pourquoi utiliser une CA Microsoft Windows Server  
plutôt qu'une autre ? . . . . . 601
  - 4.3 Importance de l'architecture d'une infrastructure à clés publiques . . . . . 604
  - 4.4 Spécificités des autorités Windows Server . . . . . 605
    - 4.4.1 Composant MMC PKI d'entreprise . . . . . 606
    - 4.4.2 Enrôlement pour les périphériques réseau  
à l'aide du protocole MSCEP . . . . . 608
    - 4.4.3 Évolution des méthodes d'enrôlement web avec AD CS . . . . . 617
    - 4.4.4 OCSP et paramètres de validation du chemin d'accès . . . . . 621
  - 4.5 Nouveautés apportées par les autorités  
de certification Windows Server 2008 R2 . . . . . 633
    - 4.5.1 Amélioration des bases de données des autorités  
de certification devant gérer de grands volumes . . . . . 634
    - 4.5.2 Service web Inscription de certificats . . . . . 634
    - 4.5.3 Support de l'enrôlement des certificats entre les forêts . . . . . 635
- 5. Active Directory Federation Services (AD FS) . . . . . 636
  - 5.1 Concepts et fonctionnalités de base . . . . . 636
  - 5.2 Fonctionnalités apportées par Windows Server 2012 R2 . . . . . 639
  - 5.3 Nouveautés apportées par Windows Server 2016 . . . . . 640
  - 5.4 Installation du rôle AD FS . . . . . 641
  - 5.5 Références pour AD FS avec Windows Server . . . . . 645

# 16 \_\_\_\_\_ Windows Server 2016

## Services de domaine Active Directory (AD DS)

6.	Active Directory Lightweight Directory Services (AD LDS)	645
6.1	Concepts fondamentaux	645
6.2	AD LDS : Nouveautés apportées par Windows Server 2008 R2	646
6.3	Installation du rôle AD LDS	648
6.4	Références pour AD LDS avec Windows Server	663
6.5	Évolutions du rôle AD LDS	663
7.	Active Directory Rights Management Services (AD RMS)	664
7.1	Introduction	664
7.2	Concepts fondamentaux	665
7.3	Pourquoi utiliser les services AD RMS ?	666
7.4	AD RMS : nouveautés apportées par Windows Server 2016	666
7.5	Ajout du rôle AD RMS	669
7.6	Création du cluster AD RMS	673
7.7	Administration du cluster AD RMS	684
7.8	Ajout du client AD RMS	685
7.9	Validation du bon fonctionnement de la plate-forme RMS	686
7.10	Références pour AD RMS avec Windows Server 2016	696

## Chapitre 10

### Introduction à Azure Active Directory

1.	Gestion des identités et environnements hybrides	697
1.1	Azure : CAPEX vs OPEX	697
1.2	Évolution du modèle, des usages et de la gestion des identités	698
1.2.1	Gestion des identités	699
1.2.2	Azure AD, centré sur les identités et indispensable pour collaborer	700
1.3	Mobilité des utilisateurs et des périphériques avec EMS et Azure AD	700
1.3.1	Services offerts via Azure Active Directory Premium (AAD)	701
1.3.2	Services offerts via Microsoft Intune	701
1.3.3	Services offerts via Azure Rights Management (RMS)	702
1.3.4	Services offerts via Microsoft Advanced Threat Analytics (ATA)	702
1.4	Stratégie de gestion globale des identités	702
1.5	L'hybridation avec Azure est source de nouvelles solutions pour l'entreprise	703

1.6	Au centre du cloud Azure, Azure Active Directory . . . . .	704
2.	Azure Active Directory : pour quoi faire ? . . . . .	705
2.1	Gestion des identités, hybridation, SSO et applications SaaS . . . . .	705
2.2	Optimisé pour la suite Office 365 en environnement hybride . . . . .	707
2.3	Pour les développeurs, des API Azure AD faciles à utiliser . . . . .	708
3.	Versions d'Azure AD : gratuit, de base et Premium . . . . .	709
4.	Scénarios d'usage avec Azure Active Directory . . . . .	711
4.1	Introduction . . . . .	711
4.2	Authentification et expérience du logon de l'utilisateur . . . . .	712
4.3	Synchronisation des identités . . . . .	713
4.4	Fédération des identités . . . . .	715
	Index . . . . .	719

## Chapitre 3

# Intégration des zones DNS dans Active Directory

### 1. Introduction

Nous venons de voir que les zones DNS standards existent sous la forme de fichiers lesquels sont habituellement stockés dans `\System32\dns`. L'idée consiste maintenant à abandonner ce stockage pour utiliser celui proposé par les services d'annuaire Active Directory. Avant de rentrer dans les détails de cette intégration, il convient de faire remarquer que l'Active Directory et le DNS manipulent des noms qui semblent être identiques, mais qu'en fait ces noms appartiennent à des espaces bien différents.

Le tableau ci-dessous illustre le parallèle qui existe entre les éléments qui appartiennent au DNS et ceux qui appartiennent à l'Active Directory.

Éléments du DNS	Éléments et objets de l'annuaire Active Directory
Stockage de type fichier	Stockage de type base de données
Fichiers de zones dans <code>\System32\dns</code>	Objets containers de type <b>dnsZone</b>
Enregistrements de ressources (RR - Resource Record)	Objet de type <b>dnsNode</b>

Ainsi, on peut dire que l'espace DNS est composé de zones et d'enregistrements de ressources dans les zones, tandis que l'espace Active Directory, appelé « Forêt » dans sa totalité, est composé de domaines et d'objets au sein de ces domaines.

Les objets et attributs Active Directory utilisés dans le cadre du service DNS sont listés ci-dessous :

**DnsZone** : il s'agit d'un objet container créé au moment où une zone est créée dans l'Active Directory.

**DnsNode** : il s'agit d'un objet utilisé pour mapper un nom vers un enregistrement contenant plusieurs données.

**DnsRecord** : il s'agit d'un attribut de type multivaleurs associé à la classe d'objet dnsNode. Il est utilisé pour stocker les enregistrements de ressources dans l'objet dnsNode.

**DnsProperty** : il s'agit d'un attribut de type multivaleurs associé à la classe d'objet dnsNode. Il est utilisé pour stocker les informations de configuration de la zone.

Finalement, chaque zone intégrée à l'annuaire sera stockée dans un objet container de type dnsZone, lequel est identifié par le nom attribué à la zone au moment de sa création.

## 2. Objets ordinateurs Active Directory et nommages

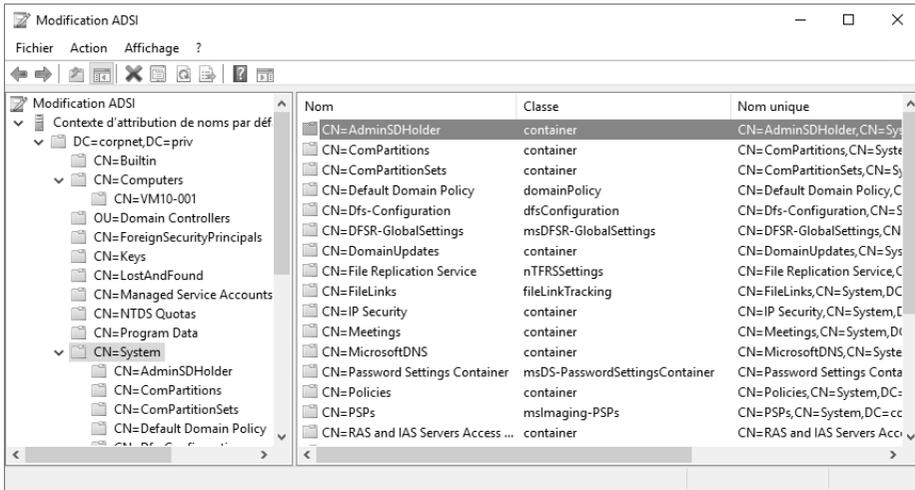
Chaque ordinateur membre d'un domaine Windows Active Directory existe sous la forme d'un objet de type Computer. La figure ci-après montre un ordinateur appartenant au domaine à l'aide de l'outil ADSI Edit.

### ■ Remarque

*Le composant logiciel enfichable ADSI Edit est intégré de base à Windows Server 2016. Vous pouvez y accéder en exécutant Adsiedit.msc ou aussi via le Gestionnaire de serveur. Notez que cet outil d'édition et de modification des objets contenus dans les partitions d'annuaire Active Directory existe depuis de nombreuses années et qu'il faisait partie des Outils de support livrés sur le CD-Rom de Windows Server 2003 et Windows 2000 Server.*

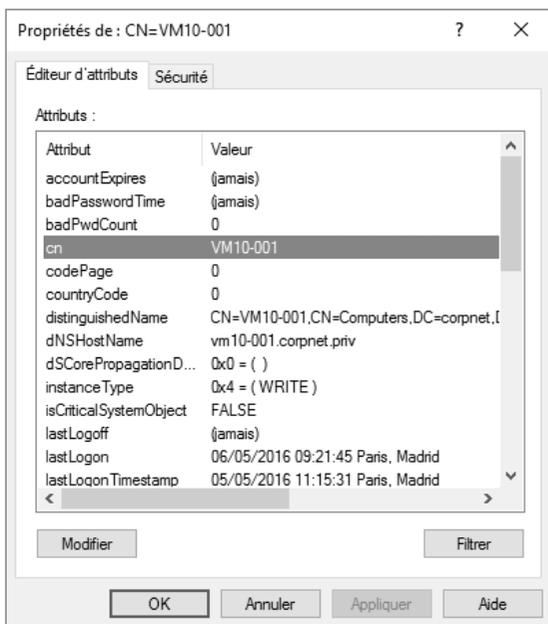
# Intégration des zones DNS dans Active Directory \_\_\_\_\_ 165

## Chapitre 3



*L'ordinateur VM10-001 dans le container Computers du domaine Corpnet.priv*

En tant qu'objet existant au sein de l'annuaire Active Directory, ses propriétés existent sous la forme d'attributs. Ainsi, ces attributs sont manipulés par l'annuaire lui-même, par les applications ou bien aussi par toute entité habilitée à le faire. La figure suivante montre la fenêtre permettant d'afficher ou de modifier les attributs d'un objet, toujours avec ADSI Edit.



*Propriétés de l'objet win7-001 et valeur de l'attribut dNSHostName*

Le tableau suivant présente les différents attributs d'un objet appartenant à la classe computer et étant en relation avec la problématique de nommage.

Attributs de l'objet	Désignation et valeur de l'attribut
<b>canonicalName</b>	Représente le nom canonique Active Directory de l'objet corpnet.priv/computers/vm10-001.
<b>cn</b>	Représente le nom commun LDAP de l'objet vm10-001.
<b>displayName</b>	Représente le nom d'affichage LDAP de l'objet vm10-001\$.
<b>distinguishedName</b>	Représente le nom distinct complet CN=vm10-001,CN=Computers,DC=corpnet,DC=priv.
<b>dNSHostName</b>	Représente le nom DNS sous la forme d'un FQDN vm10-001.corpnet.priv.
<b>name</b>	Représente le nom vm10-001.
<b>sAMAccountName</b>	Représente le nom SAM ( <i>Security Account Manager</i> ) de l'ordinateur vm10-001\$.

Attributs de l'objet	Désignation et valeur de l'attribut
<b>servicePrincipalName</b>	Représente les noms des identités (SPN, <i>Security Principal Names</i> ) HOST/vm10-001 HOST/vm10-001.corpnet.priv.

Comme expliqué précédemment, ce tableau montre qu'un ordinateur au sein du domaine Windows existe dans plusieurs espaces de nommage distincts. Les attributs les plus importants en termes de sécurité sont le **sAMAccountName** et le **servicePrincipalName**, lequel peut d'ailleurs être contrôlé à l'aide de la commande système **SetSPN.exe**.

Bien entendu, de nombreux autres attributs enrichiront l'annuaire d'informations dont l'usage sera plus perceptible.

Quelques exemples d'attributs sont présentés ci-après :

Attributs de l'objet <b>computer win10-001</b>	Désignation et valeur de l'attribut
<b>objectCategory</b>	CN=Computer,CN=Schema,CN=Configuration, DC=corpnet, DC=priv.
<b>operatingSystem</b>	Windows 10.

### 3. Avantages de l'intégration des zones DNS dans Active Directory

Les contrôleurs de domaine Windows Server permettent au service DNS de profiter des nombreuses avancées technologiques apportées par l'Active Directory. Ces avantages sont présentés ci-dessous.

#### 3.1 Mise à jour en mode multimaître (ou maîtres multiples)

Dans le modèle habituel de stockage des zones DNS, les mises à jour ne sont possibles que vers le serveur primaire pour la zone. De fait, un seul et unique serveur DNS servant de référence pour la zone est disponible en lecture et écriture. Il s'agit là d'une énorme limitation lorsque l'on souhaite profiter des mises à jour DNS en mode dynamique.

Un autre inconvénient majeur du modèle DNS traditionnel est que toute la disponibilité en écriture de la zone repose sur le seul et unique serveur principal. Si ce serveur n'est pas disponible, alors les requêtes de mise à jour formulées par des clients DNS ne sont pas traitées pour toute la zone. De plus, lorsque la zone arrive à expiration en fonction de la valeur fixée sur l'enregistrement de SOA, celle-ci passe au statut d'expirée et plus aucune demande de résolution DNS n'est traitée.

À l'inverse, lorsqu'une zone DNS est intégrée à l'Active Directory et que la zone est configurée pour supporter les mises à jour dynamiques, alors ces mises à jour peuvent aussi être prises en charge en mode multimaître. En fait, tout serveur DNS de type NS et contrôleur devient une source principale pour la zone. Par conséquent, la zone peut être mise à jour par les serveurs DNS fonctionnant sur tout contrôleur du domaine. Un tel concept permet d'offrir une disponibilité totale, pourvu que l'on dispose de plusieurs contrôleurs de domaine fonctionnant en tant que serveurs DNS. On notera que seuls les contrôleurs de domaine disponibles uniquement en lecture seule, appelés en anglais RODC pour *Read Only Domain Controllers*, font exception à la règle.

### 3.2 Sécurité avancée des contrôles d'accès sur les zones et les enregistrements

Chaque enregistrement de ressource DNS est un objet Active Directory de type dns-Node. À ce titre il existe et profite, comme tous les autres types d'objets de l'annuaire, des services de sécurité Active Directory. Dans notre cas, il s'agira des authentifications mutuelles utilisant le protocole Kerberos v5 et de l'usage des SPN. Le support des listes de contrôles d'accès vous permet de contrôler qui peut faire quoi sur chaque objet, c'est-à-dire sur chaque enregistrement DNS.

Bien entendu, tous ces objets disposent de permissions par défaut qui sécurisent l'environnement DNS, mais vous pourrez par exemple accéder aux fonctions des ACL (*Access Control List*) pour sécuriser de manière particulière un conteneur dnsZone dans l'arborescence Active Directory. La granularité d'administration est très fine puisque, en fonction des besoins de sécurité, vous aurez toujours la possibilité de gérer chaque zone et chaque enregistrement au sein d'une zone.

Le groupe intégré **Utilisateurs authentifiés** dispose d'une autorisation de type **Créer tous les objets enfants**. Cet ACL permet à tous les ordinateurs Windows supportant les authentifications Kerberos d'être authentifiés.

#### ■ Remarque

Le groupe de sécurité **Utilisateurs authentifiés** considère toutes les entités susceptibles d'être contrôlées qu'il s'agisse d'objets utilisateurs, de groupes ou d'objets de type ordinateurs membres du domaine Active Directory ou de tout domaine approuvé.