

Introduction

1. Introduction	17
2. Les différentes éditions de Windows Server 2016	17
3. Les grands axes de Windows Server 2016	19
3.1 Un meilleur contrôle de l'information	19
3.2 Une meilleure protection du système d'information tournée vers la mobilité et le cloud	20
3.3 Une plate-forme évolutive	22

Domaine Active Directory

1. Introduction	25
2. Présentation du service d'annuaire Microsoft : Active Directory Domain Services	25
2.1 Définition d'un domaine Active Directory	26
2.2 Fonctionnalités de l'Active Directory sous Windows Server 2016	29
2.2.1 Installation d'un annuaire Active Directory	29
2.2.2 Configuration système du futur contrôleur de domaine	29
2.2.3 Installation du rôle AD DS	31
2.2.4 Présentation de l'audit lié au service d'annuaire	45

2.2.5 Contrôleur de domaine en lecture seule	53
2.2.6 Stratégies de mot de passe et de verrouillage de compte granulaire	61
2.2.7 Active Directory en tant que service Windows	65
2.2.8 Clonage d'un contrôleur de domaine Active Directory virtualisé	68
2.2.9 Capture instantanée de l'Active Directory	71
2.2.10 Les comptes de service administrés	75
2.2.11 La corbeille Active Directory	84
2.2.12 Autres spécificités depuis Windows Server 2008 R2	92
3. Les stratégies de groupe	94
3.1 Détection des liens lents	94
3.2 Mise en cache des stratégies de groupe	95
3.3 Le format ADMX	97
3.4 Journaux d'événements	98
3.5 Paramètres de stratégies de groupe à connaître	99
3.6 La console Gestion de stratégie de groupe	101
3.7 Les objets GPO Starter	108
4. Azure AD	109
5. Les autres composants associés à un service d'annuaire	121
5.1 Active Directory Federation Services (AD FS)	121

5.2 Le Workplace Join	124
5.3 Active Directory Rights Management Services (AD RMS)	126
5.4 Active Directory Certificate Services (AD CS)	127
6. Conclusion	130
Architecture distribuée d'accès aux ressources	
1. Introduction	131
2. Description de DFS	131
3. Installation	133
3.1 Le module d'espace de noms	134
3.2 Le module de réplication	134
3.3 La console d'administration	134
3.4 Le cas des contrôleurs de domaine	134
3.5 La procédure d'installation graphique	135
4. Configuration du service DFS	143
4.1 Les différents types de racines distribuées	143
4.1.1 Les racines autonomes	143
4.1.2 Les racines de noms de domaine	143

4.2 La création des liaisons DFS et des cibles DFS	148
4.3 La réplication	154
4.3.1 Les filtres de réplication	155
4.3.2 La mise en place graphique de la réplication	155
4.3.3 La topologie de réplication	164
5. Configuration avancée	164
5.1 Les méthodes de classement	164
5.1.1 La configuration au niveau des racines DFS	164
5.1.2 La configuration au niveau des liaisons DFS	166
5.1.3 La configuration au niveau des cibles DFS	166
5.2 La délégation d'administration	167
6. L'administration de DFS avec PowerShell	168
6.1 L'administration des espaces de noms avec PowerShell	168
6.1.1 Gestion des racines	168
6.1.2 Gestion des cibles (dossiers) et des accès	170
6.2 L'administration de la réplication avec PowerShell	170
6.2.1 Exemple de création de l'infrastructure nécessaire pour un groupe de réplication de deux serveurs	171
6.2.2 Le clonage de base DFSR	172

7. L'utilisation de DFS et les bons usages	174
8. Interaction avec d'autres composants	175
8.1 La détection du site par DirectAccess	175
8.2 Le support de la déduplication par DFS	175
8.3 DFS dispose d'un fournisseur WMI complet (espaces de noms et réplication)	176
9. BranchCache	178
9.1 L'installation de BranchCache	178
9.2 La configuration des partages	186
9.3 La configuration des clients	187
10. Les dossiers de travail	194
10.1 Présentation	194
10.2 Les prérequis	195
10.3 L'installation sur le serveur	196
10.4 La configuration sur le poste client	206
11. Conclusion	210

Haute disponibilité

1. Introduction	213
2. Les choix d'architecture	214
2.1 Les différentes architectures	214
2.2 La haute disponibilité, nirvana de votre infrastructure ?	216
3. La répartition de charge (cluster NLB)	218
3.1 Prérequis pour NLB	218
3.2 Créer une ferme NLB	219
3.3 Configurer la ferme	222
3.4 Exemple : ferme web IIS	225
3.5 Mise à niveau d'une ferme NLB	226
4. Le cluster à basculement	227
4.1 Validation de votre cluster	232
4.2 Mise en œuvre du cluster	233
4.2.1 Configurer le réseau pour le cluster	234
4.2.2 Configurer le stockage pour le cluster	235
4.2.3 Configurer le quorum pour le cluster	236
4.2.4 L'installation du cluster	237
4.2.5 Mise en place d'un cluster de fichiers	245
4.2.6 Cas particuliers	

4.3 Migration d'un cluster d'une version antérieure à Windows Server 2016 vers Windows Server 2016	250
4.4 Configuration d'un cluster à basculement en multisite	251
4.5 Mise à jour adaptée aux clusters à basculement	254
5. Conclusion	255
5. Conclusion	261
Mise en place des services réseau d'entreprise	
1. Introduction	263
2. Le choix de l'infrastructure réseau	263
2.1 Le choix de l'architecture réseau	264
2.1.1 La zone DNS	264
2.1.2 La classe réseau	265
2.2 L'installation d'un serveur DHCP	265
2.2.1 Définition	265
2.2.2 L'installation	265
2.2.3 La configuration	266
2.2.4 Les réservations	280
2.2.5 L'enregistrement DNS basé sur les stratégies DHCP	282
2.2.6 La configuration de la bascule d'étendue DHCP	

288

3. La mise en place des systèmes de résolution de noms

295

3.1 La résolution DNS

295

3.1.1 Définition

295

3.1.2 L'installation

295

3.1.3 Les différents types de zones

296

3.1.4 Les différents types de réplication

297

3.1.5 Les zones de recherche inversée

298

3.1.6 La zone GlobalNames dite GNZ

298

3.1.7 Les tests et vérifications

299

3.1.8 Les différents types d'enregistrement

300

3.1.9 Les bons usages

301

3.1.10 DNSSEC

301

3.1.11 L'administration de DNS avec PowerShell

317

3.1.12 Les améliorations apportées par Windows Server 2012 R2 et Windows Server 2016

320

3.2 La résolution WINS

320

3.2.1 Définition

321

3.2.2 L'installation

321

3.2.3 La configuration

321

3.2.4 La réplication entre serveurs WINS

321

3.2.5 Quand et pourquoi utiliser WINS ?

321

	322
4. La mise en place de la quarantaine réseau	322
5. La mise en place d'une autorité de certification	322
5.1 L'installation de base	323
5.2 Les éléments configurables	338
5.3 Les requêtes par modèles de certificats	344
5.4 Les requêtes personnalisées	357
5.5 Un peu d'administration	371
6. Conclusion	381

Les évolutions du réseau

1. La console IPAM	383
1.1 Les avantages de cette solution	384
1.2 L'architecture IPAM	384
1.3 L'installation	385
1.4 La configuration initiale	388
1.5 Les groupes utilisés par IPAM	399
1.6 Les tâches d'administration courantes	400
1.7 Les limites à prendre en compte	

1.8 La migration d'IPAM vers IPAM 2016	400
1.9 Les rôles d'IPAM 2012 R2	401
1.9.1 La liste des rôles intégrés	404
1.9.2 La création d'un rôle personnalisé	404
1.9.3 La création d'une étendue d'accès	405
1.9.4 La définition des stratégies d'accès	406
	407
2. Le protocole IPv6	409
2.1 Tableau d'équivalence IPv4 et IPv6	410
2.2 Les commandes principales	411
2.3 La configuration de DHCPv6	412
2.3.1 Configuration du client DHCPv6 sur le serveur DHCP	413
2.3.2 Configuration du service DHCPv6	414
2.4 La configuration DNSv6 de la zone de recherche inversée	419
2.5 TEREDO	424
2.6 ISATAP	424
	424
3. L'association de cartes réseau en équipe (teaming)	425
4. Présentation de SMBv3	429
4.1 Les caractéristiques de SMBv3	429
4.2 Pratique : mise en place du mode multicanal	429

4.2.1 Les prérequis	431
4.2.2 Les commandes PowerShell	431
4.3 Remarques	431
4.4 Les modifications de SMB depuis Windows Server 2012 R2	435
5. La passerelle WSG (Windows Server Gateway)	436
5.1 L'installation	436
5.1.1 Sur le serveur Hyper-V	437
5.1.2 Configuration de la passerelle WSG	438
5.1.3 La configuration du routeur interne	438
5.2 Schéma d'un exemple d'utilisation	439
5.3 En conclusion	440
6. L'expérience Windows Server Essentials	440
6.1 L'installation	441
6.2 La configuration initiale	445
6.3 L'administration	448
6.4 La configuration du client sur le poste utilisateur	451
6.5 L'utilisation	457
6.6 Conclusion	458
7. Conclusion	

	459
Services Bureau à distance	
1. Introduction	461
2. Mise en œuvre des services Bureau à distance	465
2.1 Administration à distance	467
2.2 Installation des services Bureau à distance	471
2.2.1 Prérequis	472
2.2.2 Installation en mode Démarrage rapide	473
2.2.3 Installation en mode Déploiement standard	479
2.2.4 Installation en mode MultiPoint	482
2.2.5 Installation en PowerShell	482
2.3 Présentation du Gestionnaire des services Bureau à distance	484
3. Configuration	489
3.1 Propriétés du déploiement	489
3.2 Configuration d'une collection de sessions	490
3.2.1 Installation d'un logiciel sur un serveur de sessions	499
3.2.2 Maintenance d'un serveur de sessions	499
3.2.3 Amélioration de l'expérience utilisateur sur un serveur de sessions	500

3.3 Configuration d'une collection de bureaux virtuels	503
3.4 Déployer des applications avec RemoteApp	509
4. Configuration avancée	514
4.1 Configuration de l'accès web des services Bureau à distance	514
4.2 Configuration de la passerelle des services Bureau à distance	519
4.3 Configuration du Gestionnaire de licences des services Bureau à distance	530
4.4 RemoteFX	535
4.4.1 RemoteFX pour un hôte de virtualisation des services Bureau à distance	536
4.4.2 RemoteFX pour un hôte de session Bureau à distance	538
4.4.3 RemoteFX utilisé pour la redirection USB	539
5. Conclusion	540
Accès distant	
1. Introduction	541
2. Principe de l'accès distant	541
2.1 Accès par téléphone	542
2.1.1 Généralités sur les connexions Dial-up	542
2.1.2 Avantages et inconvénients des connexions Dial-up	542

2.2 Accès via Internet	543
2.2.1 Généralités sur les VPN	543
2.2.2 Les différents types de VPN proposés sous Windows Server 2016	545
2.2.3 Avantages et inconvénients du VPN	546
2.2.4 DirectAccess, le "VPN killer"	547
2.2.5 Rôle Proxy d'application web	548
2.2.6 Fonctionnalités d'accès distant de Windows Server 2016	549
3. Mettre en place un accès sécurisé à travers Internet	551
3.1 Mise en place d'une liaison VPN	551
3.1.1 Installation du rôle Accès à distance	552
3.1.2 Configuration des fonctionnalités VPN	554
3.2 Gestion de la sécurité des accès	562
3.3 Gestion de l'authentification RADIUS	569
3.4 Implémentation de DirectAccess derrière un pare-feu	572
3.5 Supervision des connexions	577
4. Conclusion	579

Application Internet

1. Mettre en place un serveur intranet/Internet	581
--	------------

1.1 Présentation d'IIS 10	581
1.1.1 Présentation générale	581
1.1.2 Architecture héritée	582
1.1.3 Administration	582
1.1.4 Fonctionnalités d'IIS 10 dans Windows Server 2016	584
1.2 Installation du rôle Serveur Web (IIS) en mode Windows Server minimal (Core)	585
1.2.1 Installation par défaut	585
1.2.2 Installation complète	586
1.3 Installation du rôle Serveur Web (IIS) en mode graphique	586
2. Créer un site web	590
2.1 Création et configuration d'un site	590
2.2 Utilisation des en-têtes d'hôte	595
2.3 Mise en place d'une DMZ	597
2.4 Implémentation du CPU Throttling	598
3. Monter un site FTP avec isolation des utilisateurs	601
3.1 Installation du rôle Serveur FTP	601
3.2 Configuration de l'isolation des utilisateurs	602
3.3 Configuration de la restriction des tentatives de connexion	608
4. Conclusion	

	609
Réduire la surface d'attaque	
1. Introduction	611
2. Principes du serveur Core	611
2.1 Restrictions liées à une installation minimale	611
2.2 Installation minimale	612
3. Configurer localement un serveur Core	614
3.1 Sconfig	614
3.2 Paramètres régionaux	615
3.3 Résolution de l'écran	616
3.4 Économiseur d'écran	617
3.5 Gestion des pilotes	618
3.6 Activation de Windows	618
3.7 Gestion du rapport d'erreurs	620
3.8 Configurer le fichier de pagination	621
3.9 Gérer les journaux d'événements	621
4. Gestion à distance	622

4.1 Activation du Bureau à distance	622
4.2 Activation de WinRM	623
5. Sécuriser le serveur Core	625
5.1 Gestion du pare-feu	625
5.2 Gestion automatique des mises à jour	626
5.3 Sauvegarder le serveur	626
6. Mise en place d'un serveur Core et des applications associées	627
6.1 Installation des rôles et des fonctionnalités	627
6.1.1 Les rôles réseau	627
6.1.2 Le rôle serveur de fichiers	629
6.1.3 Le rôle serveur d'impression	631
6.2 Service d'annuaire (AD)	631
6.3 Exécuter des applications 32 bits	632
6.4 Utilisation des fonctionnalités à la demande	632
6.5 Fonctionnalités PowerShell	633
7. Nano Server	634
7.1 Principe	634
7.2 Installation	635
8. Conclusion	

	639
Consolider vos serveurs	
1. Introduction	641
2. Pourquoi consolider ?	641
2.1 Virtuel versus Physique	641
2.1.1 Optimisation des coûts	642
2.1.2 Les limites de la virtualisation	643
2.2 De nouvelles problématiques	645
2.2.1 Environnement mutualisé	645
2.2.2 Sauvegarde	646
2.3 Préparer le déploiement	648
2.3.1 Prérequis	648
2.3.2 Méthodologie	650
2.3.3 Déterminer les serveurs et les applications propices à la virtualisation	651
2.3.4 Respect des meilleures pratiques	653
3. Déployer Hyper-V	655
3.1 Installation	655
3.1.1 Installation du rôle Hyper-V	655

3.1.2 Configuration du rôle	655
3.1.3 Configuration des réseaux virtuels	657
3.1.4 Configuration du stockage	658
3.2 Versions et générations de machines virtuelles	660
3.2.1 Les versions et formats de machines virtuelles	660
3.2.2 Les générations de machines virtuelles	661
3.3 Création et configuration d'une machine virtuelle	665
3.3.1 Dynamic Memory	667
3.3.2 Resource Metering	668
3.3.3 Redimensionnement de disques durs virtuels à chaud	670
3.3.4 Gestion de la QoS sur le stockage d'une machine virtuelle	671
3.3.5 Activation automatique de machines virtuelles	673
3.3.6 Exportation de machines virtuelles à chaud	674
3.3.7 Amélioration de VM Connect (RDP over VMBus)	674
3.3.8 PowerShell Direct (PowerShell over VMBus)	680
3.3.9 Identification des cartes réseau virtuelles	680
3.3.10 Protection de machines virtuelles (shielded VM)	683
3.3.11 Affectation de périphériques (Discret Device Assignment)	686
3.3.12 Points de contrôle de production	687
3.4 Conteneurs Hyper-V (Hyper-V containers)	688
3.5 Gestion de la haute disponibilité avec Hyper-V	690

3.5.1 Live Migration	690
3.5.2 Réplicas Hyper-V	692
3.5.3 Partage de disques virtuels (Shared VHDX)	696
3.6 System Center Virtual Machine Manager (SCVMM)	702
3.7 Mises à jour Windows	709
4. Conclusion	711
Déploiement des serveurs et postes de travail	
1. Introduction	713
2. Préparer son déploiement en choisissant bien sa stratégie	713
2.1 Définir le périmètre	714
2.2 Gestion des licences	715
2.3 Choix de l'édition et du type d'installation	716
3. Créer et déployer des images de système d'exploitation	716
3.1 Microsoft Deployment Toolkit	717
3.2 Lite Touch	724
3.3 WDS	730
4. Pour aller plus loin...	

	734
4.1 Microsoft Application Compatibility Toolkit	734
4.2 Environnement à la demande	735
4.3 ImageX	735
4.4 DISM (Deployment Image Servicing and Management)	737
4.5 Zero Touch avec SCCM	737
4.6 Joindre le domaine sans réseau	737
4.7 En cas de problème	738
5. Conclusion	739
Sécuriser votre architecture	
1. Introduction	741
2. Les principaux risques de sécurité au sein d'un domaine Active Directory	742
2.1 Déroulement d'une attaque type	742
2.2 Risques liés à l'identité des comptes au sein d'un annuaire Active Directory	744
3. Conception d'une architecture sécurisée	746
3.1 Approche par tiers de confiance	746
3.2 Sécurisation des contrôleurs de domaine	751

3.2.1 Sécurité physique	751
3.2.2 Sécurité au démarrage	752
4. Protection des comptes privilégiés et bonnes pratiques	753
4.1 Principe de moindre privilège et JEA	753
4.2 Les différents types de compte	754
4.2.1 Compte utilisateurs VS compte administrateur	754
4.2.2 Comptes à privilèges	757
4.3 Les technologies permettant de protéger les comptes et les accès	759
4.3.1 Protected Users ou Utilisateurs protégés	759
4.3.2 Silos de stratégies d'authentification	761
4.3.3 Credential Guard	762
4.3.4 Sécuriser l'accès RDP	763
4.3.5 Le contrôle d'accès utilisateur	767
4.3.6 Gérer vos groupes à l'aide des groupes restreints	772
5. Autres protections natives de Windows Server 2016	774
5.1 AppLocker ou le contrôle de l'application	774
5.1.1 Configuration d'AppLocker	775
5.1.2 Exemple de règles AppLocker visant à protéger ses ordinateurs clients des menaces les plus communes	782
5.2 Le chiffrement des données via BitLocker	784

5.2.1	Activation de la puce TPM sur les ordinateurs	787
5.2.2	Activation de BitLocker sur les ordinateurs	787
5.2.3	Déploiement de BitLocker sur les ordinateurs de l'Active Directory	788
5.2.4	Visualiser les clés de récupération BitLocker	789
5.3	Les outils de sécurité indispensables	793
5.3.1	SCM (Security Compliance Manager)	793
5.3.2	EMET (Enhanced Mitigation Experience Toolkit)	794
5.3.3	CFG (Control Flow Guard)	795
5.3.4	Reliability Workbook	795
5.4	Le contrôle d'accès dynamique	796
5.4.1	Principe du contrôle d'accès dynamique	796
5.4.2	Terminologie	797
5.4.3	Méthodes de mise en œuvre et prérequis	798
5.4.4	Étude d'un exemple et analyse des besoins	798
5.4.5	Pour aller plus loin	812
6.	Délégation d'administration au sein de l'Active Directory	814
6.1	Approche de la délégation d'administration	814
6.2	Délégation de comptes utilisateur	815
7.	Sécurisation du réseau	822
7.1	Le Pare-feu Windows	

7.2 La sécurisation des transactions réseau via IPsec	822
	832
8. Conclusion	836
Cycle de vie de votre infrastructure	
1. Introduction	837
2. Gestion des sauvegardes	837
2.1 Windows Server Backup	838
2.1.1 Installation de Windows Server Backup	839
2.1.2 Création d'une sauvegarde complète planifiée	840
2.1.3 Création de la sauvegarde planifiée de dossiers	844
2.1.4 Outils associés à WSB et sauvegardes uniques	846
2.1.5 Les clichés instantanés	847
2.2 Restauration de données	851
2.2.1 Restauration de fichiers et/ou de dossiers	851
2.2.2 Restauration de l'état du système	853
2.3 Stockage	855
2.3.1 Grappe RAID	855
2.3.2 Espaces de stockage	856

2.4 Resilient File System (ReFS)	858
2.5 Déduplication des données	860
3. Gestion des mises à jour	866
3.1 Présentation de WSUS	866
3.2 Installation de WSUS	867
3.3 Utilisation de WSUS	871
4. Conclusion	877
Se préparer pour le futur	
1. Après Windows Server 2016	879
Index	881