

Les éléments à télécharger sont disponibles à l'adresse suivante :

<http://www.editions-eni.fr>

Saisissez la référence ENI de l'ouvrage **EI22STR** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Préface

Chapitre 1

Introduction

1. Avant-propos	15
2. Introduction	16
3. À propos du livre.	16
3.1 L'aspect technique	17
3.2 L'organisation des informations	18
3.3 Le public concerné	19
4. L'évolution des versions de Windows	20
5. Les systèmes d'exploitation Microsoft	21
5.1 Windows 10	21
5.2 Windows 11	22
5.3 Windows Server et Windows Client	23
5.3.1 Les nouveautés de Server 2022.	24
5.3.2 Windows Server 2025.	28
5.3.3 Les nouveautés	28
5.3.4 Les suppressions ou fonctionnalités qui n'évolueront plus	33
5.3.5 Windows 11	35
5.4 Le point sécurité	39

2 ————— **Les stratégies de groupe** pour sécuriser votre infrastructure Microsoft

Chapitre 2

Stratégie locale et de domaine

1. Introduction	41
1.1 Qu'est-ce qu'une stratégie de groupe ou GPO ?	42
1.2 Les paramètres de stratégie de groupe.	42
1.3 Structure des paramètres de stratégie de groupe	43
1.4 Fichiers registry.pol	45
1.5 Le cache des stratégies de groupe.	46
2. Les stratégies locales dans un Workgroup.	47
2.1 Stratégie de groupe locale multiple	49
2.1.1 La stratégie de groupe locale	50
2.1.2 Stratégie de groupe administrateurs et non-administrateurs.	51
2.1.3 Stratégie de groupe local par utilisateur	56
2.1.4 Stratégie de sécurité locale	59
2.1.5 Kit de ressources de conformité de la sécurité	62
2.2 Mode de traitement des trois objets de stratégie de groupe locale	65
3. Présentation d'Active Directory.	65
3.1 Les différents états d'un serveur Windows	66
3.2 Active Directory : objets physiques et logiques	67
3.3 Maîtres d'opérations de domaine.	69
3.4 Active Directory, une étape primordiale.	70
3.5 Une structure bien ordonnée.	71
4. Structure d'une stratégie de groupe.	72
4.1 Introduction	72
4.1.1 Fichiers ADM et ADMX	73
4.1.2 Fichiers ADMX et ADML	74
4.2 Structure des fichiers ADMX.	77
4.2.1 Schéma du fichier	78
4.2.2 Définitions des catégories	80

4.3	Structure des fichiers ADML	81
4.3.1	Schéma du fichier	82
4.3.2	Définitions des catégories	84
4.4	Création d'un fichier ADMX personnalisé	84
4.5	Remarques.	85
5.	Le magasin central	86
5.1	Création du magasin central	86
5.2	Remplir le magasin central.	88
5.3	Sources externes de modèles d'administration	88
5.3.1	Téléchargement de fichiers ADMX de source extérieure	89
5.3.2	Modèles d'administration pour Microsoft Office 2016 . .	89
5.3.3	ADMX Migrator.	90
6.	Les filtres WMI	91
6.1	Syntaxe des filtres WMI.	92
6.1.1	Syntaxe WMI de base.	93
6.1.2	Exemples de requête WMI	94
6.1.3	Création d'un filtre WMI	95
6.1.4	Lier un filtre WMI	98
6.2	Exporter et importer les filtres WMI.	99
6.2.1	Exporter un filtre WMI	100
6.2.2	Importer un filtre WMI	101
7.	Liens et téléchargements	103
8.	Conclusion et commentaires	103

4 _____ **Les stratégies de groupe** pour sécuriser votre infrastructure Microsoft

Chapitre 3

GPO, AD et processus d'application

1. Introduction	105
2. La clé est Active Directory	106
2.1 Les contrôleurs de domaine	107
2.1.1 Promotion du premier contrôleur de domaine	108
2.1.2 Ajout d'un contrôleur de domaine supplémentaire	108
2.2 Modèle de structure des unités d'organisation	110
3. Création et cycle de vie d'une stratégie de groupe	114
3.1 Localisation des GPO	114
3.2 Permissions et droits d'accès sur les GPO	116
3.2.1 Création de GPO	116
3.2.2 Consulter et modifier les autorisations	117
3.2.3 Le conteneur Politiques dans Active Directory	117
3.2.4 Le conteneur GPC	119
3.2.5 Le conteneur GPT	120
3.3 Synchronisation des éléments GPC et GPT	121
4. Application des stratégies sur les postes de travail	126
4.1 Niveaux d'application dans Active Directory	127
4.2 Ordre d'application	128
4.3 Héritage des stratégies de groupe	128
4.4 Bloquer l'héritage	130
4.5 Priorité des stratégies de groupe	132
5. Les GPO dans un environnement multitorêt	133
6. Processus d'application des stratégies	134
6.1 Comprendre comment s'appliquent les GPO	134
6.2 Principes généraux d'application des GPO	135
6.2.1 Processus d'application	136
6.2.2 Processus d'application initial pour les versions Windows 2000 à 2022	137
6.2.3 Processus d'application pour les postes clients Windows	138

6.2.4	Le Fast Boot	139
6.3	Appliquer les GPO manuellement	141
6.3.1	Commandes de Windows XP et des versions suivantes	141
6.3.2	Commande depuis un serveur	142
7.	Application par connexion distante et liens lents	143
7.1	Détection de liens lents dans Windows	144
7.1.1	Windows 2000 et XP	144
7.1.2	Windows 7 et versions ultérieures.	144
7.2	Paramètres appliqués par liens lents	145
8.	Conclusion	147

Chapitre 4

Les outils de gestion des GPO

1.	Introduction	149
2.	Administrer et gérer les GPO	150
3.	Gérer les GPO avec la console de gestion des stratégies de groupe GPMC 3.0	151
3.1	Implémenter la console GPMC 3.0	151
3.1.1	Installation de la fonctionnalité Gestion des stratégies de groupe	151
3.2	Fonctionnalités de la console GPMC 3.0.	155
3.2.1	Création et édition de stratégies de groupe	155
3.2.2	Lier des objets stratégies de groupe	162
3.2.3	Utiliser l'option Appliqué.	165
3.2.4	Gérer la précedence des stratégies	167
3.2.5	Gérer les héritages des stratégies	169
3.2.6	Forcer les stratégies dans la console GPMC	171
3.2.7	Rechercher des stratégies	172
3.3	Configuration des paramètres de stratégies	174
3.3.1	Configuration du nœud ordinateur.	177
3.3.2	Configuration du nœud utilisateur.	179

6 **Les stratégies de groupe**

pour sécuriser votre infrastructure Microsoft

3.3.3	Génération de rapports	180
3.4	Sécurité et délégation	182
3.5	Sauvegarde et restauration des stratégies	185
3.5.1	Sauvegarder une stratégie	186
3.5.2	Restaurer une stratégie	189
3.5.3	Importer des paramètres	192
3.6	Les GPO Starter	197
3.6.1	Créer le dossier Starter GPO	198
3.6.2	Créer un objet GPO Starter	200
3.6.3	Démarrer une stratégie à partir d'une GPO Starter	202
3.6.4	Échanger les GPO Starter	204
3.7	Rechercher des paramètres avec les filtres	204
3.7.1	Introduction	204
3.7.2	Utiliser les filtres	204
3.8	Utilisation des outils de commentaires	209
3.9	Les nouvelles fonctionnalités dans la console GPMC 3.0	211
3.9.1	La réplication Active Directory	212
3.9.2	Forcer l'actualisation des stratégies de groupe	217
4.	Gestion des stratégies de groupe avec PowerShell	220
4.1	Prérequis	221
4.2	Principales commandes PowerShell	221
4.3	Commandes du module GroupPolicy pour la gestion des GPO	225
4.3.1	Création d'une stratégie de groupe	225
4.3.2	Lier une stratégie de groupe	234
4.3.3	Sauvegarde des stratégies de groupe	236
4.3.4	Restauration d'une stratégie de groupe	241
4.4	PowerShell pour nous dépanner et analyser	243
4.4.1	L'héritage des stratégies de groupe	243
4.4.2	Création d'un rapport HTML de jeu résultant RSoP	246
4.5	Résumé	249

5. Gestion avancée avec AGPM 4.0	249
5.1 Quelques termes employés avec AGPM	250
5.2 Les différents rôles	251
5.3 Cycle de vie d'une GPO avec AGPM	253
5.4 Édition d'une stratégie de groupe hors ligne	254
5.5 Intégration complète dans GPMC	254
5.5.1 Prérequis pour le composant serveur	255
5.5.2 Prérequis pour le composant client	255
5.5.3 Modifications apportées à la console GPMC 3.0	256
5.6 Historique et différences de configuration d'une GPO	261
5.7 Conclusion	263
6. Comparaison de stratégie de groupe	264
6.1 Policy Analyser	264
6.1.1 Récupération de l'outil	264
6.1.2 Comparaison de deux stratégies de groupes	266
6.2 PowerShell	271

Chapitre 5

Les préférences de stratégie de groupe

1. Introduction	277
2. Les préférences de stratégie de groupe	278
2.1 Caractéristiques des préférences	278
2.2 Configurer une nouvelle préférence	279
2.3 Fonctionnalités des préférences de stratégie de groupe	280
3. Explorer les préférences	282
3.1 Liste des paramètres de préférences	283
3.1.1 Configuration ordinateur - Paramètres Windows	284
3.1.2 Configuration utilisateur - Paramètres Windows	285
3.2 Création d'un objet de préférence	286
3.2.1 Configuration d'un objet de préférence	286
3.2.2 Déterminer l'action que la préférence doit effectuer	289

8 **Les stratégies de groupe** pour sécuriser votre infrastructure Microsoft

4. Configuration des objets de préférences	289
4.1 Configuration des préférences du conteneur Paramètres Windows	290
4.1.1 Paramètres de préférences communs aux deux nœuds .	290
4.1.2 Paramètres de préférences des utilisateurs	299
4.2 Configuration des préférences du conteneur Paramètres du Panneau de configuration	301
4.2.1 Paramètres de préférences communs aux ordinateurs et aux utilisateurs	301
4.2.2 Paramètres de préférences des utilisateurs	320
4.3 Options des objets de préférences existants	326
5. Architecture et fonctionnement des préférences de stratégie	327
5.1 Administrer les préférences	327
5.2 Appliquer les préférences	328
5.3 Gérer les composants de préférences sur les postes d'administration	328
5.3.1 Administrer les préférences de stratégie depuis un poste Windows 7 ou supérieur	329
5.3.2 Administrer les préférences de stratégie depuis un serveur Windows Server	329
6. Conclusion et commentaires	330

Chapitre 6 **Stratégies de groupe et sécurité**

1. Introduction	333
2. Création du domaine et stratégies par défaut	334
2.1 La stratégie Default Domain Policy.	335
2.1.1 Les paramètres de stratégies du domaine	335
2.1.2 Modifier la Default Domain Policy ou en créer une nouvelle.	336
2.2 Stratégie Default Domain Controllers Policy	337

2.3 Réparer les stratégies par défaut	337
3. Configurer la Default Domain Policy	338
3.1 Configuration de la stratégie de mot de passe	342
3.2 Configuration de la stratégie de verrouillage du compte	342
3.3 Configuration de la stratégie Kerberos	343
4. Sécurité et mots de passe	344
4.1 Préparer l'implémentation de FGPP	347
4.2 Créer un PSO avec ADSI Edit	348
4.2.1 Assigner un PSO	356
4.2.2 PSO et Active Directory	359
4.2.3 Utiliser Specops	363
4.3 Création du PSO avec le Centre d'administration Active Directory	364
4.4 Conclusion et commentaires	367
5. Élever le niveau de sécurité avec les outils d'audit	368
5.1 Utiliser les stratégies de groupe pour auditer	368
5.1.1 Les différents paramètres d'audit	368
5.1.2 Auditer les stratégies de groupe avec une stratégie de groupe	371
5.1.3 Auditer les modifications d'objets	371
5.1.4 Directory Service Changes	376
5.1.5 Activer Directory Service Changes	377
5.1.6 Auditer un objet spécifique	377
5.1.7 Auditer les accès aux fichiers réseau	381
5.1.8 Configuration avancée de la stratégie d'audit	381
5.2 Conclusion et commentaires	383
6. Sécurité applicative	384
6.1 Stratégie de restriction logicielle	385
6.1.1 Créer une stratégie avec une règle supplémentaire	391
6.1.2 Comment et quand appliquer les GPO de restriction ?	393
6.1.3 Dépanner les stratégies de restriction	394
6.1.4 Vérifier manuellement le registre	394

10 _____ Les stratégies de groupe

pour sécuriser votre infrastructure Microsoft

6.1.5	Créer un journal d'événements	395
6.2	Applocker	395
6.2.1	Côté sécurité	396
6.2.2	Que pouvons-nous faire avec Applocker ?	396
6.2.3	Les scénarios d'AppLocker	397
6.2.4	Quand Utiliser AppLocker ?	397
6.2.5	Création d'une stratégie AppLocker	398
6.3	Windows Defender Application Control (WDAC)	398
6.3.1	Quel environnement pour WDAC ?	399
6.3.2	WDAC et Smart App Control	399
6.3.3	Les stratégies présentes	400
6.4	Comparaison des trois solutions	403
7.	Comment les attaquants agissent	405
7.1	Les méthodes courantes	405
7.2	Les contre-mesures ou atténuations	406
8.	Conclusion et commentaires	407

Chapitre 7

Implémentation de la sécurité au sein d'un SI

1.	Notions fondamentales	409
1.1	L'identité et le SID	409
1.1.1	Les autorités communes	411
1.1.2	SID de l'autorité NT	412
1.1.3	SID de l'autorité NT - pour le composant BUILTIN	412
1.1.4	SID de l'autorité NT - pour Active Directory	413
1.1.5	Object GUID et SID	414
1.2	L'identité et le jeton d'accès	415
1.3	Taille de jeton	416
1.4	Les Privileged Acces Workstation (PAW)	416
1.5	Les bastions d'administration	418
1.6	Le Tiering	420
1.7	Tiering : les silos d'authentification	423

1.8	Tiering : les stratégies de restriction de login	425
1.9	Tiering : la solution idéale	426
1.10	Sécuriser les machines du domaine avec des objets GPO. . . .	426
1.11	Point sécurité	427
2.	Comment durcir nos environnements ?	427
2.1	Analyser la configuration de sécurité avec PingCastle.	428
2.2	Analyser la configuration de sécurité avec Purple Knight . . .	434
2.3	Sécuriser avec Microsoft Security Compliance Toolkit (SCT)	441
2.4	Sécuriser avec HardeningKitty	447
2.5	Sécuriser avec HardenAD.	453
2.5.1	Ce que contient cet outil	453
2.5.2	Séquence de tâches	454
2.5.3	Le Tiering selon Harden	457
2.5.4	Quels comptes utiliser ?	459
2.5.5	Le modèle de délégation	460
2.5.6	Redirections des comptes Utilisateurs et Ordinateurs. .	464
2.5.7	Les stratégies de restriction de login pour les Tiers	465
2.5.8	La gestion des groupes Administrateurs Local	473
2.5.9	Stratégies de groupes de durcissement	475
2.5.10	Filtres WMI.	475
2.6	Créer un nouvel Active Directory : Hello-My-Dir	477
2.6.1	Comment récupérer le projet.	477
2.6.2	Configuration de l'outil	479
2.6.3	Promotion du contrôleur de domaine	480
2.6.4	Durcir Active Directory	481
2.6.5	Le résultat	482
2.6.6	Audit avec PingCastle.	484

12 _____ Les stratégies de groupe

pour sécuriser votre infrastructure Microsoft

Chapitre 8

Dépanner les stratégies de groupe

1. Introduction	485
2. Méthodologie	486
2.1 Éléments de recherche	487
2.1.1 Les exigences liées à l'infrastructure	487
2.1.2 Les environnements mixtes	487
2.1.3 Les autorisations	488
2.1.4 Le domaine Active Directory	488
2.1.5 La connectivité réseau	488
2.1.6 Les stratégies appliquées par liens lents	489
2.1.7 Les serveurs DNS	489
2.1.8 Le partage SYSVOL	489
2.1.9 La réplication Active Directory NTFRS ou DFSR	490
2.1.10 Les stratégies par défaut	491
2.1.11 Dans la console GPMC	492
2.2 Organiser les permissions	494
3. Les outils de diagnostic	495
3.1 GPOTool	495
3.1.1 Utilisation de GPOTool	495
3.1.2 Isoler les erreurs de réplication	497
3.2 Un jeu de stratégie résultant RSoP	498
3.2.1 Résultats de stratégie de groupe	499
3.2.2 Modélisation de stratégie de groupe	506
3.2.3 GPResult	513
3.3 Gpupdate	516
3.4 Replmon	516
3.5 Les journaux d'événements	517
3.6 L'Observateur d'événements	517
3.6.1 Le mode classique	517
3.6.2 Le mode avancé	521

3.6.3 L'Observateur d'événements sur les contrôleurs de domaine	524
4. Conclusion et commentaires	528

Chapitre 9 **Étude de cas**

1. Introduction	529
2. Cas pratiques	530
2.1 Stratégies de la Configuration ordinateur	531
2.1.1 Cas 1 - Configurer le Pare-feu Windows grâce aux stratégies de groupe	531
2.1.2 Cas 2 - Mettre en place une stratégie de clé publique ..	539
2.1.3 Cas 3 - Déployer les applications avec les stratégies de groupe	562
2.1.4 Cas 4 - Gérer et définir les membres des groupes locaux	570
2.2 Stratégies de la Configuration utilisateur	575
2.2.1 Cas 5 - Configurer le bureau idéal pour vos utilisateurs	575
2.2.2 Cas 6 - Restreindre l'accès au Panneau de configuration	578
2.3 Stratégies de préférences	581
2.3.1 Cas 7 - Connecter les lecteurs réseau grâce aux préférences	581
2.3.2 Cas 8 - Faciliter l'accès à l'intranet de la société	583
2.3.3 Cas 9 - Gestion des mots de passe des comptes Administrateurs locaux	584
2.3.4 Cas 10 - Permettre à votre entreprise de faire des économies d'énergie	598
2.4 Implémentation de la sécurité	598
2.4.1 Le contexte	598
2.4.2 Schéma d'infrastructure	600
2.4.3 Rapport PingCastle	601

14 _____ **Les stratégies de groupe**

pour sécuriser votre infrastructure Microsoft

2.4.4 L'administration en Tier.....	603
2.4.5 Le Tier zéro.....	603
2.4.6 Le Tier 1 et 2.....	604
2.4.7 Le Tier Legacy.....	605
2.4.8 Ce qu'il reste à faire.....	605
3. Conclusion et commentaires.....	605

Conclusion

1. Conclusion.....	609
2. Liens Internet.....	611

Index.....	613
------------	-----

Les éléments à télécharger sont disponibles à l'adresse suivante :

<http://www.editions-eni.fr>

Saisissez la référence ENI de l'ouvrage **EI22WINA** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Introduction

1. Avant-propos	19
2. À qui s'adresse cet ouvrage ?	20
3. Reproduction des labs	20
4. Nouveautés de Windows Server 2022	21
4.1 Éditions de Windows Server 2022	21
4.2 Gestion du matériel	22
4.3 Sécurité	22
4.4 Autres nouveautés	22
5. Types d'installation	23
6. Déployer un serveur Core	23
6.1 Présentation du lab	24
6.2 Déploiement du serveur Core	24
6.3 Installation des RSAT dans Windows 10	32

Chapitre 1

Active Directory

1. Types de domaines Active Directory	41
1.1 Le lab pour la mise en œuvre des domaines	42
1.2 Domaine racine de la forêt	43
1.3 Domaine racine d'un arbre	43
1.4 Sous-domaine	44
1.5 Relation d'approbation	44
1.5.1 Transitivité et direction	45
1.5.2 Autres types de relation d'approbation	46
1.6 Niveaux de privilèges	47

2 _____ Windows Server 2022

Administration avancée

2.	Mise en œuvre d'une forêt multidomaine	48
2.1	Création du domaine racine	49
2.1.1	Considérations sur le matériel des contrôleurs de domaine . . .	49
2.1.2	Installation d'ADDS (Active Directory Domain Services)	50
2.1.3	Promotion du serveur en contrôleur de domaine	52
2.1.4	Installation et configuration d'ADDS avec PowerShell	57
2.1.5	Bug des redirecteurs DNS	58
2.2	Création des sous-domaines	59
2.2.1	Promotion du contrôleur d'un sous-domaine	59
2.2.2	Création des sous-domaines avec PowerShell	62
2.3	Création du domaine d'arborescence	63
2.4	Création de la relation d'approbation de raccourci	66
3.	Relation d'approbation de forêt et approbation externe	69
3.1	Configuration des DNS	70
3.2	Relation d'approbation de forêt	70
3.2.1	Schéma de principe du lab	71
3.2.2	Mise en œuvre du routeur BLR	71
3.2.3	Mise en œuvre du domaine externe	75
3.2.4	Création des redirecteurs conditionnels	76
3.2.5	Création de la relation d'approbation de forêt	78
3.2.6	Création d'approbation externe avec authentification sélective	87
4.	Rôles FSMO	94
4.1	Introduction aux rôles FSMO	94
4.2	Descriptions des rôles FSMO	95
4.3	Déplacer des rôles FSMO	99
4.3.1	Installation d'un contrôleur de domaine secondaire	99
4.3.2	Transfert des rôles FSMO	103
4.3.3	Saisir les rôles FSMO	105
5.	Base de données Active Directory	108
5.1	Partitions de la base de données	108
5.2	Défragmenter la base de données Active Directory	111
5.3	Déplacer la base de données Active Directory	115
5.3.1	Déplacement de la base de données et des logs	115
5.3.2	Sauvegarde de la base de données	117

6.	Schéma Active Directory	120
6.1	Prérequis à la modification du schéma	121
6.2	Modification du schéma.	123
6.2.1	Modification d'un attribut	123
6.2.2	Gestion du cache	129
7.	Dossier sysvol	130
7.1	Vérification de la réplication	131
7.2	Ajout de stratégies de groupe.	132
8.	Sites Active Directory	134
8.1	Concepts de base.	134
8.1.1	Réplication intrasite	136
8.1.2	Réplication intersites.	137
8.1.3	Exemple de topologie de réplication.	138
8.2	Le lab pour la mise en œuvre des sites Active Directory	139
8.3	Mise en œuvre de sites Active Directory.	140
8.4	Gestion en lignes de commande	148
9.	Contrôleur de domaine en lecture seule.	150
9.1	Déploiement d'un RODC.	151
9.1.1	Lab de déploiement d'un RODC.	151
9.1.2	Mise en œuvre d'un RODC.	151
9.2	Décommissions d'un contrôleur de domaine	162
10.	Gestion avec PowerShell	164
10.1	Peupler Active Directory	164
10.2	Import en masse d'utilisateurs.	166
10.3	Gestion des utilisateurs avec PowerShell	168

Chapitre 2

Le service DHCP

1.	Le lab	171
1.1	Configuration du serveur Core	172
1.2	Configuration du client1	173
2.	Installation du service DHCP	174
2.1	Installation en PowerShell	174
2.2	Gestion et héritage des options DHCP	177

4 _____ Windows Server 2022

Administration avancée

3.	Agent relais DHCP.	182
3.1	Création de l'étendue	182
3.2	Mise en place de l'agent relais.	184
4.	Mise à jour dynamique du DNS	188
5.	Autres types d'étendues.	195
5.1	Étendues de multicast.	195
5.2	Étendues globales	197
5.3	Étendues fractionnées.	200
6.	Stratégies DHCP	206
6.1	Stratégie avec les classes d'utilisateurs.	206
6.2	Stratégie avec l'adresse MAC	214
6.3	Autres exemples de stratégies	219
6.4	Gestion et application des stratégies DHCP	222
7.	Filtrage d'adresses MAC	223
8.	DHCP IPv6.	227
8.1	Bases du protocole IPv6	227
8.1.1	Types d'adresses IPv6.	228
8.1.2	Notation des adresses IPv6	229
8.2	Mécanismes du DHCP IPv6	229
8.3	Le lab DHCP IPv6	230
8.4	Adressage IPv6.	230
8.4.1	Adressage de DC-ecole.	230
8.4.2	Adressage de core1	232
8.4.3	Configuration du routeur	234
8.4.4	Configuration de l'étendue DHCP IPv6	236
9.	Clustering DHCP.	240

Chapitre 3 Le service DNS

1. Principes de base	247
1.1 Indications de racines	247
1.1.1 Visualiser les indications de racines	248
1.1.2 Modifier les indications de racines	249
1.2 Gestion du cache	250
2. Le lab	252
2.1 Configuration du NAT	253
2.1.1 Configuration des cartes réseau	253
2.1.2 Installation du routage NAT	255
2.2 Ajout de la route statique	257
3. Redirecteurs	259
3.1 Redirecteurs globaux	259
3.2 Redirecteurs conditionnels	261
4. Processus de résolution du serveur DNS	263
5. Enregistrements DNS	264
6. Gestion des zones et des enregistrements	265
6.1 Gestion des machines à plusieurs cartes réseau	266
6.2 Gestion des zones DNS Active Directory	268
6.2.1 Recréer un enregistrement	268
6.2.2 Recréer la zone DNS Active Directory	268
6.2.3 Configuration du nettoyage des zones	270
7. Création de zones DNS dans Windows Server	274
7.1 Zones principales	274
7.1.1 Création de zones principales directes	274
7.1.2 Création de zones principales inversées	278
7.1.3 Création de zone principale hors Active Directory	284
7.2 Zones secondaires	286
7.2.1 Création d'une zone secondaire directe	286
7.2.2 Création d'une zone inversée secondaire	292
7.3 Zones de stub	296

6 **Windows Server 2022**

Administration avancée

7.4	Création des zones avec PowerShell	303
7.4.1	Création de zones principales	303
7.4.2	Création de zones secondaires	303
7.4.3	Création de zones de stub	304
8.	Stratégies DNS	304
8.1	Présentation des stratégies DNS	304
8.2	Concepts de base	305
8.2.1	Conditions et actions	305
8.2.2	Étendues de zone DNS	305
8.3	Création d'une stratégie de répartition de charge	305
8.4	Création d'une stratégie de gestion des réseaux IP	308
9.	DNSSEC	310
9.1	Concepts généraux	310
9.2	Mise en place de DNSSEC	311
9.2.1	Signature de la zone DNS	311
9.2.2	Vérification de la signature	318
9.2.3	Paramétrage de la stratégie de groupe	318
10.	Délégation DNS et sous-domaine	322
11.	Réglages supplémentaires du service DNS	329
11.1	Round robin	329
11.2	Limitation du taux de réponse	331
11.2.1	Paramètres de la limitation du taux de réponse	331
11.2.2	Configuration de la limitation du taux de réponse	332
11.3	Plage de ports aléatoires	333
11.4	Désactiver la récursivité	333
12.	Surveillance du service DNS	334
12.1	Propriétés du serveur	334
12.1.1	Onglet Monitoring	335
12.1.2	Onglet Event Logging	336
12.1.3	Onglet Debug Logging	337
12.2	Observateur d'évènements	340

Chapitre 4 Le stockage

1. Systèmes de fichiers dans Windows Server 2022	349
1.1 Introduction	349
1.2 Comparer NTFS et ReFS	350
1.3 Nouvelles fonctionnalités apportées par ReFS	351
1.3.1 Résilience des données.	351
1.3.2 Amélioration des performances	352
2. Le lab	353
3. Pools de stockage et espaces de stockage	354
3.1 Concepts de base.	354
3.2 Spécifications	355
3.2.1 Connectiques.	355
3.2.2 Boîtiers JBOD.	355
3.2.3 Types de résilience.	356
3.3 Création d'un pool et d'un espace de stockage	356
3.4 Pool et espace de stockage avec PowerShell	369
3.5 Agrandir un pool de stockage.	372
4. Partages avancés	374
4.1 Gestion du protocole SMB.	374
4.1.1 Monitoring du SMB 1	374
4.1.2 Activation et désactivation du protocole SMB	375
4.1.3 Gestion de SMB 1 par stratégie de groupe	376
4.2 Création de partages SMB avancés	377
4.3 Création de partages NFS avancés.	385
4.4 Mise en évidence de l'énumération basée sur l'accès	392
4.5 Gestion des partages en PowerShell	397
5. File Server Resource Manager (FSRM).	399
5.1 Paramétrage de base du serveur de fichiers.	399
5.1.1 Paramétrage du serveur d'e-mail.	401
5.1.2 Limites de notifications.	402
5.2 Création de quotas personnalisés	402
5.2.1 Création d'un modèle de quota.	402
5.2.2 Création et application de quotas.	406
5.3 Filtrage des types de fichiers	407

8 _____ Windows Server 2022

Administration avancée

6.	Déduplication des données	413
6.1	Concepts de base	413
6.2	Mise en œuvre de la déduplication	416
6.3	Déduplication avec PowerShell	421
6.4	Surveillance de la déduplication	425
6.4.1	Journaux d'évènements	425
6.4.2	Tâches planifiées	425
6.4.3	Surveillance avec PowerShell	427
7.	Réplica de stockage	428
7.1	Présentation des réplicas de stockage	428
7.2	Prérequis et limitations	430
7.3	Mise en œuvre d'un réplica de stockage	431
8.	Distributed File System (DFS)	436
8.1	Introduction à DFS	436
8.2	Principes de fonctionnement	437
8.2.1	Principes de base	437
8.2.2	Gestion des espaces de noms	438
8.2.3	Gestion de la réplication	439
8.3	Installation et configuration de DFS	440
8.3.1	Création de l'espace de noms	441
8.3.2	Mise en place de la réplication	449
8.3.3	Tester la réplication	464
8.4	Redondance du serveur d'espace de noms	466
8.5	Paramétrages supplémentaires	469
8.5.1	Gestion des références et des sites Active Directory	469
8.5.2	Retirer un serveur d'espace de noms de la référence	469
8.5.3	Changer la place d'un serveur dans la référence	470
8.5.4	Gestion des sites Active Directory	470
8.5.5	Énumération basée sur l'accès	471
9.	Stockage iSCSI	472
9.1	Introduction à l'iSCSI	472
9.2	Création de cibles iSCSI	473
9.2.1	Installation du rôle	473
9.2.2	Création de la cible iSCSI	475
9.2.3	Connexion de l'initiateur	485
9.2.4	Mise en place de l'authentification CHAP	491

Chapitre 5 Hyper-V

1. Introduction à la virtualisation dans Hyper-V	495
1.1 Introduction	495
1.2 Systèmes invités compatibles	497
1.3 Configuration requise	498
1.4 Limites supérieures	499
1.4.1 Pour les hôtes de virtualisation	499
1.4.2 Pour les machines virtuelles	499
2. Lab Hyper-V	500
3. Installation du rôle Hyper-V	502
3.1 Installation avec PowerShell	502
3.2 Installation en mode graphique	503
3.3 Gestion depuis la machine client	507
3.4 Création d'une première machine virtuelle	508
4. Paramétrage des serveurs Hyper-V	517
4.1 Groupe administrateurs Hyper-V	517
4.2 Activation de la virtualisation imbriquée	518
4.3 Mode session étendue	519
4.4 Changer les emplacements par défaut	521
5. Configuration d'une machine virtuelle	523
5.1 Paramétrage de la mémoire	523
5.1.1 Mémoire de démarrage	524
5.1.2 Mémoire dynamique	524
5.1.3 Poids de la mémoire	524
5.1.4 Visualisation de la mémoire	525
5.1.5 Architecture NUMA	525
5.2 Fichiers de pagination	526
5.3 Démarrage sécurisé	527
5.4 Service d'intégration	529
5.5 Attribution d'appareils en mode discret	530
5.5.1 Introduction	530
5.5.2 Préparation du matériel	531
5.5.3 Configuration de la machine virtuelle	532
5.5.4 Reconfigurer le périphérique dans l'hôte	532

5.6	Démarrage et arrêt automatiques	532
5.6.1	Démarrage automatique	532
5.6.2	Arrêt automatique	533
6.	Gestion des machines virtuelles	534
6.1	Export et import de machines virtuelles	534
6.1.1	Export de la machine virtuelle.	535
6.1.2	Import de la machine virtuelle	536
6.1.3	Création de machines virtuelles avec PowerShell	541
6.2	PowerShell direct et PSsession	541
6.2.1	Présentation	541
6.2.2	Exécution de scripts.	543
6.2.3	Sessions persistantes	544
6.3	Points de contrôle	546
6.3.1	Principes de base.	546
6.3.2	Types de points de contrôle	546
6.3.3	Utilisation des points de contrôle.	547
6.3.4	Points de contrôle automatiques	547
6.3.5	Gestion en PowerShell des points de contrôle	548
6.4	Gestion de la version des machines virtuelles	549
6.5	Groupes de machines virtuelles	550
6.6	Groupes de CPU	552
7.	Gestion des disques de machines virtuelles	556
7.1	Ajout et configuration de disques virtuels	556
7.1.1	Ajout d'un nouveau disque	556
7.1.2	Modification d'un disque.	559
7.1.3	Qualité de service de stockage.	562
7.2	Pass-through disk	563
7.3	Disques de différenciation	565
7.3.1	Présentation des disques de différenciation	565
7.3.2	Mise en œuvre des disques de différenciation	567
7.4	Gestion des disques avec PowerShell.	571
8.	Gestion du réseau dans Hyper-V	572
8.1	Switchs virtuels.	572
8.1.1	Généralités	572
8.1.2	Liaison d'un switch externe à la carte réseau physique.	573
8.1.3	Création d'un switch externe	575

8.1.4	Raccordement des machines virtuelles.	578
8.1.5	Switch interne et NAT	579
8.2	Configuration des cartes réseau	581
8.2.1	Adresse MAC	581
8.2.2	Accélération matérielle	582
8.2.3	Fonctionnalités avancées.	583
8.3	Groupement de cartes réseau.	583
8.3.1	Grouper les cartes physiques.	583
8.3.2	Utilisation de l'équipe dans un switch Hyper-V	587
8.4	Migration à chaud de machines virtuelles	589
8.4.1	Configuration d'Hyper-V	590
8.4.2	Délégation contrainte Kerberos	591
8.4.3	Considérations supplémentaires.	595
8.4.4	Migration du stockage et de la machine	596
8.4.5	Migrer la machine et le stockage simultanément	596
8.4.6	Migration de la machine seule	600
9.	Hyper-V réplica	609
9.1	Configuration des serveurs pour Hyper-V réplica	610
9.2	Mise en place d'Hyper-V réplica	612
9.3	Utilisation d'Hyper-V réplica.	617
9.3.1	Basculement planifié	618
9.3.2	Basculement en cas de désastre.	619
10.	Conteneurs et Docker	620

Chapitre 6

Le clustering avec Windows Server

1.	Introduction au clustering	625
1.1	Généralités.	625
1.2	Considérations sur le réseau.	626
1.3	Quorum.	626
1.4	Accès au stockage	627
2.	Mise en place du lab	628

3.	Cluster de basculement	629
3.1	Configuration du stockage	629
3.1.1	Pré-configuration des initiateurs iSCSI	629
3.1.2	Configuration du serveur de stockage	630
3.1.3	Configuration finale des initiateurs	635
3.2	Préparation du cluster	637
3.2.1	Installation de la fonctionnalité	637
3.2.2	Test de la configuration	638
3.3	Création du cluster	643
3.4	Configuration du cluster	646
3.4.1	Configuration réseau	646
3.4.2	Ajout de rôles de cluster	652
3.4.3	Gestion du propriétaire du rôle	659
4.	Serveur de fichiers SOFS	664
4.1	Introduction au SOFS	664
4.2	Préparation du lab	665
4.3	Création du cluster SOFS	666
4.3.1	Installation du rôle	666
4.3.2	Vérifications	668
4.3.3	Ajout du CSV	670
4.3.4	Création de partages	672
4.3.5	Réglage du cache des partages	676
5.	Cluster Hyper-V	677
5.1	Installation du cluster Hyper-V	677
5.1.1	Préparation du cluster	677
5.1.2	Créer une première VM	678
5.2	Import de machines virtuelles	682
5.3	Fonctionnalités de clustering	688
5.3.1	Répartition de charge	688
5.3.2	Réseaux protégés	690
5.3.3	Surveillance des machines virtuelles	691
6.	Espaces de stockage direct	691
6.1	Introduction	691
6.1.1	Concepts de base	691
6.1.2	Notions sur l'hyperconvergence	692
6.2	Adaptation du lab	693

6.3	Préparation des machines.	694
6.4	Installation du cluster	695
6.5	Création des espaces de stockage directs.	698
7.	Répartition de charge réseau.	702
7.1	Introduction	702
7.2	Préparation du lab.	703
7.3	Mise en œuvre de l'équilibrage de charge	703
7.3.1	Installation des rôles et fonctionnalités.	703
7.3.2	Création et paramétrage du cluster	704
7.3.3	Ajouter un hôte au cluster	712
7.3.4	Vérification du fonctionnement du cluster	715
8.	Clusters étendus	716
8.1	Présentation et concepts de base	716
8.2	Prérequis	718
8.3	Azure Stack HCI.	718

Chapitre 7 Windows Server et Azure

1.	Introduction.	719
1.1	Cas d'usage	719
1.2	Moyens de connexion.	720
1.3	Entra ID.	720
1.4	Outils de gestion.	721
1.4.1	Windows Admin Center	721
1.4.2	Azure Arc	722
1.5	Comptes Azure et Microsoft 365	722
2.	Le lab	723
3.	Synchronisation d'annuaire	723
3.1	Concepts de base.	723
3.2	Domaines Microsoft 365 et Active Directory.	724
3.3	Préparation de l'Active Directory	728
3.3.1	Corbeille Active Directory.	728
3.3.2	Nettoyage de l'annuaire Active Directory	730
3.3.3	Utilitaire IDfix.	730

14 _____ Windows Server 2022

Administration avancée

3.4	Mise en œuvre de la synchronisation	730
3.4.1	Synchronisation initiale	732
3.4.2	Configuration de la synchronisation	738
3.4.3	Réécriture du mot de passe	742
3.4.4	Synchronisation PTA	744
4.	Serveurs avec Azure Arc	746
4.1	Concepts de base	746
4.2	Fonctionnement de l'agent	747
4.2.1	Prérequis Windows Server	747
4.2.2	Prérequis Azure	747
4.2.3	Fonctionnement	748
4.2.4	Mise à jour de l'agent	748
4.2.5	Connectivité réseau	748
4.3	Installation de l'agent Azure Arc	749
4.3.1	Préparation de l'installation	749
4.3.2	Installation de l'agent	752
4.4	Ajout de Windows Admin Center	754
4.4.1	Paramétrage des droits	755
4.4.2	Installation	756
4.5	Ajouter plusieurs serveurs	759
4.5.1	Création du principal de sécurité	760
4.5.2	Création du script de déploiement	762
4.5.3	Finalisation du script de déploiement	765
4.5.4	Noms réservés	766
4.5.5	Déploiement du script	767
5.	Supervision de l'infrastructure	767
5.1	Azure Monitor	767
5.1.1	Installer l'extension Azure Monitor	767
5.1.2	Mettre en route les insights	770
5.1.3	Création de tableaux de bord	772
5.2	Création d'alertes avec Azure Monitor	774
5.2.1	Préparation de la collecte des données	774
5.2.2	Création de l'alerte	778
5.3	Application de stratégies Azure	786

6.	Windows Admin Center	790
6.1	Installation de WAC	790
6.2	Ajout de machines	796
6.3	Première connexion à une machine	799
6.4	Ajouter des extensions	801
6.5	Lier un compte Azure	804
7.	Contrôleurs de domaines dans Azure	810
7.1	Concepts de base	810
7.2	Considérations pratiques	811
7.2.1	Adresses IP statiques dans Azure	811
7.2.2	Rôles FSMO et catalogue global	811
7.2.3	Emplacement de la base de données Active Directory	811
7.2.4	Éteindre la machine virtuelle	811
7.3	Création d'un contrôleur de domaine dans Azure	812
7.4	Microsoft Entra ID ADDS	823
7.4.1	Concepts de base	823
7.4.2	Considérations sur les domaines	824
7.4.3	Considération réseau	825
7.4.4	Versions d'Entra ID ADDS	826
7.4.5	Limitations d'Entra ID ADDS	826
8.	Azure File Sync	826
8.1	Introduction	826
8.1.1	Gestion des conflits	827
8.1.2	Synchronisation initiale	827
8.1.3	Hiérarchisation cloud	827
8.1.4	Cas d'usage	828
8.2	Création du stockage cloud	828
8.3	Mise en place d'Azure File Sync	832
8.3.1	Création du service de synchronisation	832
8.3.2	Création du groupe de synchronisation	833
8.3.3	Installation de l'agent Azure File Sync	834
8.3.4	Paramétrage de la synchronisation	840
9.	Il faut tout effacer	846

Chapitre 8

La sécurité de Windows Server

1. Sauvegarde Windows Server	851
1.1 Planification et première sauvegarde	851
1.2 Restauration	861
1.3 Gestion des sauvegardes	867
2. BitLocker.	870
2.1 Concepts de base.	870
2.1.1 Puce TPM	870
2.1.2 Fonctionnalités de BitLocker.	872
2.1.3 Protecteurs BitLocker.	873
2.2 Installation de BitLocker.	873
2.3 Cryptage d'un disque de données	875
2.3.1 Installation sur le contrôleur de domaine.	875
2.3.2 Paramétrage des stratégies de groupe	876
2.3.3 Sauvegarde dans Active Directory et activation	877
2.4 Crypter le disque système	878
2.4.1 Configuration des stratégies	878
2.4.2 Chiffrement du disque système	880
3. Microsoft Defender	884
3.1 Paramétrage de base	885
3.2 Gestion de Microsoft Defender	891
3.3 Gestion par stratégies de groupe	893
4. Bases de référence de sécurité	896
4.1 PolicyAnalyser.	897
4.2 Import des stratégies.	902
4.3 Documentation.	908
5. Active Directory Certificat Services (ADCS).	911
5.1 Notions de base du cryptage	911
5.1.1 Cryptage symétrique	912
5.1.2 Cryptage asymétrique	912
5.1.3 Fonctionnement des clés	913
5.1.4 Hashing.	913
5.1.5 Signature digitale	914
5.1.6 Enveloppe digitale	914

5.2	Certificats	915
5.2.1	Chaîne de confiance	916
5.2.2	Autorité racine ADCS	917
5.3	Installation d'ADCS	918
5.3.1	Installation	918
5.3.2	Post-installation	920
5.3.3	Vérifications	926
5.4	Inscription par le Web	930
5.5	Infrastructure de clé publique (PKI)	935
5.5.1	Architecture deux tiers	935
5.5.2	Architecture 3 tiers	936
5.6	Sécurisation du serveur web IIS	936
5.6.1	Création d'un modèle de certificat	936
5.6.2	Création d'un certificat à partir d'un modèle	941
5.6.3	HTTPS dans le serveur web IIS	945
5.7	Sauvegarde d'ADCS	948
5.7.1	Sauvegarde de la base de données et de la clé	948
5.7.2	Sauvegarde des paramètres de l'autorité	951
6.	DNS over HTTPS	952
6.1	Mise en œuvre	953
6.2	Configuration avec les stratégies de groupe	956
	Index	959