

Préface

Avant-propos

**Chapitre 1**  
**Introduction au Cloud computing**

- 1. Introduction ..... 13
- 2. Comparatif des grands acteurs du Cloud public ..... 19
  - 2.1 Positionnement ..... 20
  - 2.2 Modèle économique ..... 21
  - 2.3 Infrastructure as a Service ..... 22
  - 2.4 Platform as a Service ..... 23
  - 2.5 Software as a Service ..... 24
- 3. Modèles d'exploitation ..... 25
  - 3.1 On-Premise ..... 25
  - 3.2 Cloud public ..... 26
  - 3.3 Cloud privé ..... 26
  - 3.4 Cloud hybride ..... 27
- 4. Acteurs majeurs ..... 30
- 5. Points essentiels à retenir ..... 30

**Chapitre 2**  
**Le Cloud public Microsoft**

- 1. Introduction ..... 33
- 2. Implantation géographique ..... 40
- 3. Centre de données ..... 43
- 4. Sécurité de l'infrastructure Azure ..... 44
  - 4.1 Centre de gestion de la confidentialité ..... 45
  - 4.2 Localisation des données ..... 48

# 2 **Microsoft Azure**

Gérez votre Système d'Information dans le Cloud

4.3	Accès des données par Microsoft	48
4.4	Sécurité des données	49
4.5	Incident de sécurité	49
5.	Accès à Azure via un poste de travail	50
6.	Accès à Azure depuis l'entreprise	51
7.	Serveur de rebond	53
8.	Azure Bastion	53
9.	Normes et certifications	54
10.	Service Level Agreement	55
11.	Support technique	59
11.1	Microsoft Learn	63
11.2	État des services Azure	65
12.	Abonnement	66
12.1	Types d'abonnements Azure	68
12.1.1	Paiement à l'utilisation ou Pay-As-You-Go	68
12.1.2	Cloud Solution Provider	69
12.1.3	Contrats Entreprise ou EA	71
12.1.4	Licence Open	75
12.1.5	Azure Hybrid Benefit	76
12.1.6	Évaluation gratuite	78
12.2	Gestion de la facturation	81
12.2.1	Azure Cost Management	81
12.2.2	Facture	83
12.2.3	Power BI	86
12.3	Estimation du coût d'utilisation des ressources	90
12.3.1	Calculatrice Azure	91
12.4	Compte Microsoft ou professionnel/scolaire	96
12.5	Les rôles BuiltIn (ou Rôles intégrés)	105
12.5.1	Propriétaire	106
12.5.2	Contributeur	106
12.5.3	Lecteur	106

13. Modèles de déploiement . . . . . 109  
14. Points essentiels à retenir . . . . . 112

**Chapitre 3**  
**Interfaces d'exploitation**

1. Interfaces graphiques . . . . . 113  
  1.1 Portail Azure . . . . . 113  
    1.1.1 Menu . . . . . 114  
    1.1.2 Accueil Azure . . . . . 116  
    1.1.3 Tableau de bord . . . . . 116  
    1.1.4 Éléments de base du portail . . . . . 119  
    1.1.5 Notifications . . . . . 127  
  1.2 Catégories . . . . . 128  
    1.2.1 Délégation de droits . . . . . 132  
    1.2.2 Étiquette . . . . . 133  
    1.2.3 Modèle de déploiement . . . . . 136  
  1.3 Journal d'activité . . . . . 139  
2. Azure Marketplace . . . . . 143  
  2.1 Installation d'un système d'exploitation . . . . . 146  
  2.2 Publication d'une application . . . . . 147  
  2.3 Prix . . . . . 148  
3. Azure Cloud Shell . . . . . 149  
4. Azure PowerShell . . . . . 151  
  4.1 Windows PowerShell ISE . . . . . 156  
  4.2 Aide sur les applets PowerShell . . . . . 160  
5. Azure CLI (ou Bash) . . . . . 161  
  5.1 Installation sur un poste Windows . . . . . 163  
  5.2 Installation sur un poste Linux . . . . . 164  
  5.3 Affichage des abonnements . . . . . 168  
  5.4 Définition de l'abonnement actif . . . . . 168

# 4 **Microsoft Azure**

Gérez votre Système d'Information dans le Cloud

5.5	Commandes de création. . . . .	168
5.5.1	Création d'un groupe de ressources . . . . .	168
5.5.2	Création d'un compte de stockage. . . . .	169
5.5.3	Création d'un réseau virtuel . . . . .	169
5.5.4	Création d'un sous-réseau. . . . .	169
5.5.5	Création d'une adresse IP publique . . . . .	169
5.5.6	Création d'une adresse IP privée. . . . .	169
5.5.7	Création d'une machine virtuelle. . . . .	170
5.6	Commandes d'affichage . . . . .	170
5.6.1	Visualisation de l'état des machines virtuelles . . . . .	170
5.6.2	Visualisation des objets d'Azure Active Directory . . . . .	170
5.6.3	Affichage des régions . . . . .	170
5.7	Commandes de modification. . . . .	171
5.7.1	Ajout d'un nouveau disque. . . . .	171
5.7.2	Définition d'une étiquette . . . . .	171
5.8	Commandes de gestion . . . . .	172
5.8.1	Arrêt d'une machine virtuelle. . . . .	172
5.8.2	Démarrage d'une machine virtuelle . . . . .	172
5.9	Commandes de suppression . . . . .	173
5.9.1	Suppression d'une machine virtuelle . . . . .	173
5.9.2	Suppression d'un groupe de ressources . . . . .	173
6.	Points essentiels à retenir . . . . .	173

## **Chapitre 4** **Concepts de base**

1.	Introduction . . . . .	175
2.	Convention de nommage. . . . .	175
3.	Groupe de ressources . . . . .	177
3.1	Verrou . . . . .	178
3.2	Déplacement de ressources . . . . .	179
3.3	Suppression d'une ressource ou d'un groupe de ressources . . . . .	182

- 4. Machine virtuelle ..... 183
- 5. Disque managé ..... 187
  - 5.1 Taille du disque et performance ..... 188
  - 5.2 Sécurité ..... 190
- 6. Compte de stockage ..... 191
  - 6.1 Blob ..... 195
  - 6.2 Conteneur ..... 196
  - 6.3 Table ..... 202
  - 6.4 File d'attente ..... 204
  - 6.5 Partage de fichiers (Azure Files) ..... 204
  - 6.6 Storage Service Encryption (SSE) ..... 208
  - 6.7 Suppression réversible des blobs ..... 210
  - 6.8 Clés d'accès ..... 212
    - 6.8.1 Signature d'accès partagé (SAP) ..... 214
    - 6.8.2 Stratégies d'accès au niveau du conteneur ..... 216
    - 6.8.3 Signature d'accès partagé (SAP) au niveau du blob. . . . . 217
  - 6.9 Authentification Azure Active Directory ..... 218
  - 6.10 Stockage froid ..... 219
  - 6.11 Archivage. .... 223
  - 6.12 Gestion du cycle de vie. .... 225
  - 6.13 Azure Premium Storage ..... 226
  - 6.14 Réplication ..... 229
    - 6.14.1 Stockage redondant local ou LRS. .... 230
    - 6.14.2 Stockage redondant dans une zone ou ZRS ..... 231
    - 6.14.3 Stockage géoredondant ou GRS. .... 231
    - 6.14.4 Stockage géoredondant avec accès en lecture  
ou RA-GRS ..... 231
    - 6.14.5 Stockage géoredondant interzone ou GZRS ..... 232
    - 6.14.6 Stockage géoredondant interzone  
avec accès en lecture ou RA-GZRS ..... 232
    - 6.14.7 Comparatif des niveaux de réplication ..... 232
  - 6.15 Coût. .... 234

# 6 **Microsoft Azure**

Gérez votre Système d'Information dans le Cloud

6.16	Importation et exportation de données	235
6.16.1	Outil Azure Import/Export	236
6.16.2	Data Box	237
6.17	Microsoft Azure Storage Explorer	238
7.	Réseau virtuel ou VNet	241
7.1	Sous-réseau	243
7.2	Peering	244
7.3	VNet-to-VNet	247
7.4	Routage	249
7.4.1	Itinéraires système	249
7.4.2	UDR	249
7.4.3	BGP	251
7.5	Liaison privée	252
7.6	DNS	257
7.7	Adresses IP	259
7.8	Équilibreur de charge	263
7.8.1	Groupe à haute disponibilité	268
7.8.2	Zone de disponibilité	270
7.8.3	Groupes de placement de proximité	271
7.9	Azure Application Gateway	272
7.10	Groupe de sécurité réseau ou NSG	276
7.11	Connectivité	281
7.11.1	VPN site à site	282
7.11.2	VPN point à site	290
7.11.3	ExpressRoute	296
8.	Key Vault	303
8.1	Suppression réversible	307
8.2	Protection contre le vidage	308
9.	Points essentiels à retenir	309

**Chapitre 5**  
**Machine virtuelle**

- 1. Introduction ..... 313
- 2. Générations 1 et 2..... 313
  - 2.1 Nested mode ..... 314
- 3. Tailles ..... 318
- 4. Coûts ..... 321
- 5. État Arrêté ou Arrêté (libéré) ..... 322
- 6. Azure Disk Encryption..... 325
- 7. Extensions..... 327
- 8. Linux ..... 329
  - 8.1 Création d'une machine virtuelle Linux ..... 330
  - 8.2 Accès SSH ..... 333
- 9. Transfert d'une machine virtuelle On-Premise vers Azure ..... 336
  - 9.1 Importation d'une machine virtuelle Windows dans Azure .. 336
    - 9.1.1 Installation du rôle Hyper-V ..... 337
    - 9.1.2 Création d'un ordinateur virtuel Windows 10 ..... 339
    - 9.1.3 Préparation à la duplication ..... 342
    - 9.1.4 Conversion d'un disque virtuel ..... 343
    - 9.1.5 Transfert du fichier VHD vers Azure ..... 343
    - 9.1.6 Création de la machine virtuelle dans Azure ..... 346
  - 9.2 Importation d'une machine virtuelle Linux dans Azure ..... 348
- 10. Dépannage d'une connexion à distance ..... 348
  - 10.1 Itinéraire ..... 348
  - 10.2 Méthodes de dépannage..... 350
  - 10.3 Connexion SSH ..... 355
  - 10.4 Demande de support ..... 357
- 11. Applet de gestion des machines virtuelles ..... 358
  - 11.1 Get-AzVM..... 359
  - 11.2 Stop-AzVM..... 360

# 8 **Microsoft Azure**

Gérez votre Système d'Information dans le Cloud

11.3 Restart-AzVM . . . . .	360
11.4 Remove-AzVM . . . . .	360
12. Points essentiels à retenir . . . . .	361

## **Chapitre 6** **Sauvegarde et PRA**

1. Sauvegarde . . . . .	363
1.1 Fonctionnalités de la solution . . . . .	364
1.1.1 Compression . . . . .	364
1.1.2 Déduplication . . . . .	364
1.1.3 Sécurité . . . . .	365
1.1.4 Rétention . . . . .	365
1.2 Tarifs . . . . .	365
1.3 Coffre Recovery Services . . . . .	367
1.4 Réplication . . . . .	368
1.5 Suppression réversible . . . . .	370
1.6 Azure Backup . . . . .	372
1.7 Agent Azure Backup . . . . .	375
1.8 Azure Backup Server . . . . .	384
2. Plan de Reprise d'Activité . . . . .	385
2.1 PRA interrégions . . . . .	388
2.2 Test de basculement . . . . .	391
3. Points essentiels à retenir . . . . .	394

## **Chapitre 7** **APP Service et conteneurisation**

1. Introduction . . . . .	397
2. Plan App Service . . . . .	398

- 3. Création d'un App Service . . . . . 399
  - 3.1 Nom de domaine personnalisé. . . . . 403
  - 3.2 Mise à jour sécurisée à l'aide de FTPS . . . . . 404
  - 3.3 Authentification . . . . . 407
  - 3.4 Sauvegardes. . . . . 411
  - 3.5 Emplacements de déploiement . . . . . 413
  - 3.6 Application Insights . . . . . 415
  - 3.7 Azure App Service Support . . . . . 418
  - 3.8 Alertes . . . . . 422
  - 3.9 Tarifs . . . . . 426
  - 3.10 Mise à niveau d'un plan App Service. . . . . 427
- 4. Conteneurisation . . . . . 428
  - 4.1 DevOps . . . . . 429
  - 4.2 Registre de conteneurs ACR . . . . . 430
  - 4.3 Azure Container Instances . . . . . 432
  - 4.4 Azure Container Apps . . . . . 434
  - 4.5 Azure Kubernetes Service. . . . . 437
    - 4.5.1 Architecture d'un cluster AKS . . . . . 438
- 5. Points essentiels à retenir. . . . . 447

**Chapitre 8**

**Base de données**

- 1. Introduction . . . . . 451
- 2. Azure SQL Database. . . . . 452
  - 2.1 Règle de pare-feu. . . . . 455
  - 2.2 Test de connectivité . . . . . 458
  - 2.3 Base de données unique et base de données élastique . . . . . 462
  - 2.4 Réplication . . . . . 462
  - 2.5 Coût d'exploitation. . . . . 465
- 3. Base de données MySQL . . . . . 466

4. Création d'une base de données (IaaS) . . . . .	469
4.1 Configuration de SQL Server pour l'authentification en mode mixte . . . . .	471
4.2 Création de connexions d'authentification SQL Server . . . . .	472
4.3 Connexion au moteur de base de données à partir d'un autre ordinateur . . . . .	474
5. Points essentiels à retenir . . . . .	476

## Chapitre 9 Azure Active Directory

1. Introduction . . . . .	477
2. Utilisateur . . . . .	481
3. Azure RBAC . . . . .	483
4. Groupe . . . . .	485
5. Tenant . . . . .	487
6. Identités managées . . . . .	491
7. Éditions . . . . .	494
8. SLA . . . . .	495
9. Azure AD Connect . . . . .	495
10. Azure MFA . . . . .	507
11. Points essentiels à retenir . . . . .	516

## Chapitre 10 Supervision

1. Supervision . . . . .	519
1.1 Métriques . . . . .	520
1.2 Journaux d'activité . . . . .	521
1.3 Traces distribuées . . . . .	523
1.4 Modifications . . . . .	524

- 2. Azure Monitor ..... 524
  - 2.1 Les alertes Azure ..... 525
  - 2.2 Log Analytics ..... 530
  - 2.3 Network Watcher ..... 532
- 3. Points essentiels à retenir ..... 534

**Chapitre 11**  
**Cas concrets**

- 1. Introduction ..... 537
- 2. Une infrastructure hautement disponible ..... 539
  - 2.1 Création du PRA interrégions ..... 540
- 3. La DSI dans Azure ..... 542
  - 3.1 Hub and Spoke ..... 542
- 4. Une sauvegarde très... délicate ..... 543

Index ..... 547

Les éléments à télécharger sont disponibles à l'adresse suivante :  
**<http://www.editions-eni.fr>**  
Saisissez la référence ENI de l'ouvrage **EP2AZAD** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

## Préface

## Avant-propos

## Chapitre 1 Introduction

1. Présentation du livre . . . . .	13
2. Le cloud . . . . .	13
2.1 Les différents modèles du cloud . . . . .	15
2.1.1 IaaS . . . . .	15
2.1.2 PaaS . . . . .	16
2.1.3 SaaS . . . . .	17
2.2 Les modèles de déploiement du cloud . . . . .	17
2.2.1 Le cloud public . . . . .	17
2.2.2 Le cloud privé . . . . .	18
2.2.3 Le cloud hybride . . . . .	18
2.3 Les enjeux du cloud . . . . .	19
2.4 Les acteurs sur le marché . . . . .	19
3. Microsoft Azure . . . . .	22
3.1 Ce que propose Microsoft Azure . . . . .	22
3.2 Microsoft Azure et les scénarios hybrides . . . . .	23
3.3 La gestion des identités hybrides . . . . .	23
4. Tendances et priorités en 2023 . . . . .	26
4.1 Protection des identités . . . . .	28
4.2 Modernisation de la sécurité des identités . . . . .	28
4.3 Zero Trust . . . . .	29
4.4 Simplification et gouvernance . . . . .	30
4.5 Utilisateurs mobiles . . . . .	30

# 2 ————— Azure Active Directory

Gestion des identités hybrides (concepts et mise en œuvre)

## Chapitre 2

### Fournisseur d'identité Azure Active Directory

1.	Microsoft Entra	31
1.1	Introduction	31
1.2	Azure Active Directory	33
1.3	Permissions Management	33
1.4	Verified ID	34
2.	Enterprise Mobility and Security	35
2.1	Azure Active Directory	35
2.2	Azure Information Protection	36
2.3	Microsoft Defender for Cloud Apps	38
2.4	Microsoft Intune	39
2.5	Microsoft Advanced Threat Analytics	39
2.6	Microsoft Defender for Identity	41
2.7	EMS et les licences	41
3.	Azure Active Directory	42
3.1	Présentation d'Azure Active Directory	42
3.2	Éditions d'Azure Active Directory	44
3.3	Limites d'Azure Active Directory	46
4.	Microsoft et l'identité	47
4.1	Différences entre AD DS et Azure Active Directory	47
4.2	Les identités Microsoft dans le cloud	48
4.2.1	Azure Active Directory	48
4.2.2	AD DS sur une machine virtuelle Azure	48
4.2.3	Azure Active Directory Domain Services	49
5.	L'identité hybride	53
5.1	Scénarios d'usage	53
5.1.1	Microsoft 365	54
5.1.2	EMS	54
5.1.3	Application SaaS	54
5.2	Identité hybride et authentification	55
5.2.1	La synchronisation de hash de mot de passe	55
5.2.2	L'authentification unique transparente avec la synchronisation de mot de passe	57
5.2.3	Le Pass-Through : authentification directe	58
5.2.4	La fédération avec Active Directory Federation Services	60

- 5.2.5 PingFederate . . . . . 61
- 5.3 Quel moyen d'authentification ? . . . . . 62
- 5.4 Architecture Azure Active Directory . . . . . 65
- 6. Débuter avec Azure Active Directory . . . . . 68
  - 6.1 Préparation du bac à sable . . . . . 68
    - 6.1.1 Environnement Azure . . . . . 68
    - 6.1.2 Machines virtuelles - serveurs . . . . . 79
    - 6.1.3 Configuration réseau . . . . . 86
    - 6.1.4 Création du domaine Active Directory . . . . . 90
    - 6.1.5 Création de la structure utilisateurs . . . . . 103
  - 6.2 Création d'un annuaire Azure Active Directory . . . . . 106
    - 6.2.1 Création d'un tenant Office 365 . . . . . 106
    - 6.2.2 Souscription d'un abonnement EMS E5 . . . . . 113
  - 6.3 Configuration . . . . . 116
    - 6.3.1 Découverte de l'interface Azure Active Directory  
Admin Center . . . . . 117
    - 6.3.2 Création d'un compte d'administrateur global . . . . . 143
    - 6.3.3 Ajout d'un domaine public personnalisé . . . . . 147
    - 6.3.4 Personnalisation . . . . . 149
  - 6.4 Azure Active Directory et PowerShell . . . . . 151

**Chapitre 3**  
**Gestion des utilisateurs et des groupes**

- 1. Les utilisateurs dans Azure Active Directory . . . . . 157
  - 1.1 Création des utilisateurs . . . . . 157
    - 1.1.1 Création des utilisateurs en interface graphique . . . . . 158
    - 1.1.2 Création des utilisateurs en PowerShell . . . . . 161
  - 1.2 Gestion des utilisateurs . . . . . 163
    - 1.2.1 Réinitialiser un mot de passe . . . . . 163
    - 1.2.2 Supprimer un utilisateur . . . . . 165
    - 1.2.3 Restaurer un utilisateur . . . . . 166
    - 1.2.4 Donner un rôle à des utilisateurs . . . . . 167
    - 1.2.5 Propriétés des utilisateurs Azure Active Directory . . . . . 177
    - 1.2.6 Comprendre le sign-in des utilisateurs . . . . . 183

# 4 Azure Active Directory

Gestion des identités hybrides (concepts et mise en œuvre)

2. Les groupes dans Azure Active Directory . . . . .	184
2.1 Types de groupes . . . . .	184
2.1.1 Groupes de sécurité . . . . .	184
2.1.2 Groupes Microsoft 365 . . . . .	184
2.2 Type d'appartenance . . . . .	185
2.2.1 Affecté . . . . .	185
2.2.2 Utilisateur dynamique . . . . .	186
2.2.3 Appareil dynamique . . . . .	199
2.2.4 Appartenance à un groupe dynamique . . . . .	201
2.3 Création des groupes affectés . . . . .	206
2.3.1 Création des groupes en interface graphique . . . . .	206
2.3.2 Création des groupes en PowerShell . . . . .	207
2.4 Gestion des groupes . . . . .	208
2.4.1 Vue d'ensemble . . . . .	219
2.4.2 Propriétés des groupes . . . . .	220
2.4.3 Ajout et suppression de membres . . . . .	221
2.4.4 Propriétaire de groupe . . . . .	222
2.4.5 Appartenance aux groupes . . . . .	224
2.4.6 Applications . . . . .	226
2.4.7 Licences . . . . .	227
2.4.8 Attribution de rôles Azure . . . . .	227
3. La gestion des licences . . . . .	227
3.1 Présentation des licences . . . . .	228
3.2 Affectation des licences . . . . .	228
3.2.1 Affectation de licence à un utilisateur en interface graphique . . . . .	229
3.2.2 Affectation de licence à un utilisateur en PowerShell . . . . .	233
3.2.3 Affectation de licence à un groupe en interface graphique . . . . .	241
3.2.4 Affectation de droit d'accès à un groupe Azure Active Directory . . . . .	242

## Chapitre 4

### Gestion des appareils

1. Introduction . . . . .	247
1.1 Le Modern Management . . . . .	248
1.2 L'identité d'appareil dans Azure Active Directory . . . . .	250

- 1.3 Paramètres dans Azure Active Directory ..... 251
- 2. Inscription d'appareils - Azure AD Registration ..... 254
  - 2.1 Comment inscrire un poste Windows 10  
dans Azure Active Directory ? ..... 255
  - 2.2 Propriétés de l'appareil inscrit ..... 259
- 3. Jonction d'appareils - Azure AD Join ..... 261
  - 3.1 Comment joindre un poste Windows 10  
dans Azure Active Directory ? ..... 262
  - 3.2 Propriétés de l'appareil joint ..... 266
  - 3.3 Gestion des appareils joints à Azure Active Directory ..... 267
  - 3.4 Audit et logs ..... 268
- 4. Appareils hybrides dans Azure Active Directory ..... 270
  - 4.1 Concept ..... 270
  - 4.2 Fonctionnement ..... 271
- 5. Les jetons PRT ..... 272

**Chapitre 5**  
**Gestion des applications**

- 1. Introduction ..... 275
- 2. Les applications intégrées à Azure Active Directory ..... 275
  - 2.1 Introduction ..... 276
  - 2.2 Les avantages ..... 279
  - 2.3 Les types d'applications ..... 279
- 3. Intégration d'applications dans Azure Active Directory ..... 280
  - 3.1 Démarches ..... 280
  - 3.2 Intégrer une application SaaS ..... 283
    - 3.2.1 Authentification SSO ..... 286
    - 3.2.2 Création et ajout des utilisateurs Azure Active Directory ... 292
    - 3.2.3 Ajout de l'utilisateur au niveau de l'application ..... 293
  - 3.3 Gestion d'une application intégrée ..... 296
  - 3.4 Signature de jeton SAML ..... 304
  - 3.5 Consultation des rôles claims dans un jeton SAML ..... 307
  - 3.6 Fonctionnement du SAML avec Azure Active Directory ..... 311

# 6 --- Azure Active Directory

Gestion des identités hybrides (concepts et mise en œuvre)

4.	Enregistrement d'applications . . . . .	312
4.1	Introduction . . . . .	312
4.2	Inscrire une application dans Azure Active Directory . . . . .	321
4.2.1	Introduction . . . . .	321
4.2.2	Cas d'une inscription d'application pour développeurs . . . . .	321
5.	Azure Application Proxy . . . . .	341
5.1	Présentation . . . . .	342
5.2	Fonctionnement d'Azure Application Proxy . . . . .	343
5.3	Exemples . . . . .	344
5.4	Publication d'applications IIS . . . . .	344
5.4.1	Téléchargement et installation du connecteur proxy . . . . .	345
5.4.2	Intégration de l'application locale dans Azure Active Directory . . . . .	351
5.4.3	Ajout d'un utilisateur au niveau de l'application . . . . .	354
5.4.4	Test d'accès à l'application depuis l'extérieur . . . . .	354
5.4.5	Test depuis le portail Myapps . . . . .	355
5.5	Mode d'authentification . . . . .	356

## Chapitre 6

### Gestion des identités hybrides

1.	Introduction . . . . .	359
2.	Extension d'un Active Directory local vers Azure Active Directory . . . . .	360
2.1	Pourquoi étendre ses utilisateurs vers Azure Active Directory ? . . . . .	361
2.2	Les attributs Active Directory stockés dans Azure Active Directory . . . . .	362
2.3	Avant d'étendre son Active Directory . . . . .	363
2.4	L'outil IdFix . . . . .	368
3.	Azure Active Directory Connect . . . . .	370
3.1	Présentation d'AAD Connect . . . . .	370
3.2	Architecture . . . . .	370
3.3	Topologies avec AAD Connect . . . . .	371
4.	Avant d'installer AAD Connect . . . . .	373
4.1	Prérequis Azure Active Directory . . . . .	373
4.2	Prérequis AD DS . . . . .	373
4.3	Prérequis serveur AAD Connect . . . . .	373

4.4	Prérequis du serveur SQL	375
4.5	Prérequis des comptes d'administration et comptes de services	375
4.6	Prérequis réseau	375
5.	Installation d'AAD Connect	379
5.1	Installation personnalisée	381
5.2	Configuration Express Settings	395
5.3	Validation et configuration supplémentaire	395
5.4	Activation de la synchronisation avec le Hash Sync	403
5.5	Vérification de l'état de la synchronisation	406
6.	Active Directory Federation Services	408
6.1	Installation d'AD FS	409
6.1.1	Prérequis	411
6.1.2	Installation AD FS interne	415
6.2	Installation du Web Application Proxy	425
7.	AAD Connect et les options d'authentification	433
7.1	Synchronisation de hachage de mot de passe	433
7.1.1	Configuration	434
7.1.2	Validation	436
7.2	Le Pass-through	437
7.2.1	Prérequis	437
7.2.2	Configuration	438
7.2.3	Validation	440
7.3	La fédération avec AD FS	441
7.3.1	Configuration	442
7.3.2	Vérification	444
7.4	Fonctionnalité de déploiement intermédiaire	445
8.	Gestion d'AAD Connect	449
8.1	Personnalisation de la synchronisation	449
8.1.1	Filtrage des unités d'organisation	449
8.1.2	Fonctionnalités en options	452
8.1.3	Applications Azure AD	453
8.1.4	Attributs Azure AD	453
8.2	Gestion des appareils hybrides	454
8.2.1	Prérequis	455
8.2.2	Configuration Azure AD hybride	455
8.2.3	Configuration du Device writeback	459

# 8 **Azure Active Directory**

Gestion des identités hybrides (concepts et mise en œuvre)

8.2.4	Opérations au niveau des appareils . . . . .	463
8.3	Le mode Staging . . . . .	468
8.3.1	Introduction . . . . .	468
8.3.2	Configuration . . . . .	469
8.4	Export et import d'une configuration AAD Connect . . . . .	470
9.	AAD Connect Health . . . . .	471
9.1	AAD Connect Health pour AADS . . . . .	471
9.2	AAD Connect Health AD FS . . . . .	478
9.3	AAD Connect Health Sync . . . . .	481
10.	Azure AD Connect Cloud Sync . . . . .	485
10.1	Introduction . . . . .	485
10.2	Installation . . . . .	491
10.3	Configuration du SSO . . . . .	511
10.4	Migration d'AAD Connect vers Azure AD Connect Cloud Sync . . . . .	515
11.	Résumé . . . . .	523

## **Chapitre 7**

### **Gestion de la synchronisation**

1.	AAD Connect . . . . .	525
1.1	Présentation des outils . . . . .	525
1.1.1	Import du module PowerShell . . . . .	526
1.1.2	Architecture de synchronisation . . . . .	530
1.2	Synchronisation des utilisateurs . . . . .	533
1.3	Le filtrage . . . . .	535
1.3.1	Éditeur de règles de synchronisation . . . . .	539
1.3.2	Création de règle de synchronisation positive . . . . .	542
1.4	Connecteur space . . . . .	555
1.4.1	Connecteur space Active Directory . . . . .	556
1.4.2	Connecteur space Azure Active Directory . . . . .	562
1.5	Métaverse . . . . .	563
1.5.1	Metaverse Designer . . . . .	563
1.5.2	Metaverse Search . . . . .	565
1.5.3	Propriétés des objets . . . . .	568

2.	Opérations et configurations	573
2.1	AAD Connect Scheduler	573
2.2	Changement de mots de passe du compte de service AD Sync	579
2.3	Prévention des suppressions accidentelles	581
2.4	Statistiques	582
3.	Problématique	583
3.1	Cas réel d'entreprise	584
3.2	Explication	584
3.3	Démonstration	585

## Chapitre 8

### Azure Active Directory, sécurité et collaboration

1.	Introduction	591
2.	Zero Trust	592
3.	Accès conditionnel	596
3.1	Introduction	596
3.2	Types de configuration d'accès conditionnel	599
3.2.1	Affectations	599
3.2.2	Applications ou actions cloud	600
3.2.3	Conditions	604
3.2.4	Contrôles d'accès	606
3.3	État de la stratégie d'accès conditionnel	609
3.4	Création d'une stratégie d'accès conditionnel	610
3.5	Emplacements nommés	624
3.6	Modèles de stratégie d'accès conditionnel	626
3.7	Importer des stratégies d'accès conditionnel	632
3.8	Accès conditionnel avec points forts d'authentification	634
3.9	Conditions d'utilisation	648
3.10	Conception et matrice de stratégies d'accès conditionnels	654
3.11	Bonnes pratiques	658
3.12	Zero Trust avec accès conditionnel	665
3.13	Logs Azure Active Directory et accès conditionnel	666
3.14	Accès conditionnel en mode Rapport uniquement	669
3.15	Accès conditionnel et PowerShell	671

# 10 \_\_\_\_\_ Azure Active Directory

Gestion des identités hybrides (concepts et mise en œuvre)

4.	Azure Active Directory Identity Protection.....	673
4.1	Introduction .....	673
4.2	Détection des risques .....	674
4.3	Configuration d'Azure Identity Protection .....	685
4.4	Simulation .....	703
5.	Azure MFA.....	704
5.1	Présentation d'Azure MFA .....	709
5.2	Licences .....	712
5.3	Tour d'horizon .....	716
5.3.1	Méthodes d'authentification.....	717
5.3.2	Authentification multifacteur.....	729
5.4	Gestion du MFA via les accès conditionnels .....	739
5.5	Gestion des méthodes d'authentification pour les utilisateurs .....	744
5.6	MFA et stratégies d'accès conditionnel .....	749
5.7	Authenticator Lite.....	754
5.7.1	Introduction.....	754
5.7.2	Prérequis .....	754
5.7.3	Activation.....	755
5.8	Bonnes pratiques.....	757
5.9	MFA et utilisateur final .....	758
5.9.1	Enregistrement MFA .....	758
5.9.2	Portail My Account .....	764
6.	Gestion des mots de passe et des comptes.....	771
6.1	Azure Active Directory Password Protection .....	771
6.1.1	Configuration du Password Smart Lockout.....	772
6.1.2	Configuration du Password Smart Lockout on-premise.....	775
6.2	PasswordLess avec FIDO2 .....	786
6.2.1	Introduction.....	787
6.2.2	Présentation de FIDO2 .....	788
6.2.3	PasswordLess et méthodes d'authentification.....	788
6.2.4	Activation du PasswordLess sur Azure Active Directory .....	792
6.2.5	Démarche pour l'utilisateur final .....	796
6.3	Comptes brise-glace .....	806
6.3.1	Introduction.....	806
6.3.2	Bonnes pratiques .....	807
6.3.3	Création de comptes brise-glace .....	808
6.3.4	Surveillance des comptes brise-glace.....	809

6.4	Réinitialisation de mots de passe en libre-service . . . . .	811
6.4.1	Prérequis . . . . .	813
6.4.2	Activation du SSPR . . . . .	814
6.4.3	Paramètres . . . . .	817
7.	Collaboration . . . . .	826
7.1	Azure B2B . . . . .	826
7.2	Cross-tenant . . . . .	828
7.3	Prérequis et informations . . . . .	830
7.4	Vue d'ensemble . . . . .	831
7.5	Configuration par défaut . . . . .	835
7.6	Cas d'usage . . . . .	841
7.7	Utilisateurs invités . . . . .	867
7.7.1	Invitation par e-mail . . . . .	867
7.7.2	Synchronisation entre clients . . . . .	872
7.8	Conclusion . . . . .	890
8.	PIM (Privileged Identity Management) . . . . .	890
8.1	Introduction . . . . .	891
8.2	Mise en place . . . . .	894
8.3	Configuration . . . . .	896
8.4	Activation de rôles via PIM . . . . .	906
8.5	Activation de PIM sur les groupes Azure AD . . . . .	910
8.6	Rapports . . . . .	917
8.7	Révision des accès . . . . .	918
9.	Microsoft Entra . . . . .	925
9.1	Interface Microsoft Entra . . . . .	927
9.2	Identity Governance . . . . .	929
9.3	Identités de charge de travail . . . . .	940
9.3.1	Types d'identités de charge de travail . . . . .	941
9.3.2	Bonnes pratiques de sécurité . . . . .	944
10.	Azure Active Directory Secure Score . . . . .	945
10.1	Présentation . . . . .	945
10.2	Fonctionnement . . . . .	945

# 12 \_\_\_\_\_ Azure Active Directory

Gestion des identités hybrides (concepts et mise en œuvre)

## Conclusion

1. Introduction . . . . .	949
2. L'identité hybride . . . . .	950
3. La gestion des appareils . . . . .	951
4. Le Modern Management . . . . .	952
5. La sécurité . . . . .	953
6. Ce que nous avons abordé . . . . .	953
6.1 La conception d'une architecture hybride . . . . .	954
6.2 L'extension vers Azure Active Directory . . . . .	954
6.2.1 AAD Connect . . . . .	954
6.2.2 Méthodes d'authentification . . . . .	955
6.3 La gestion de l'hybridation . . . . .	955
6.3.1 Utilisateurs . . . . .	955
6.3.2 Ordinateurs . . . . .	955
6.4 Azure Active Directory, la sécurité et la collaboration . . . . .	956
6.4.1 L'accès conditionnel . . . . .	956
6.4.2 Azure B2B . . . . .	956
6.4.3 Azure Active Directory Application Proxy . . . . .	957
6.4.4 Azure Active Directory Password Protection . . . . .	957
6.4.5 Azure Active Directory MFA . . . . .	957
6.4.6 Azure Active Directory Identity Protection . . . . .	957
6.4.7 Privileged Identity Management . . . . .	957
6.4.8 Stratégie Zero Trust 2.0 Azure AD . . . . .	958
6.4.9 Paramètres de sécurité par défaut . . . . .	958
6.4.10 Le fonctionnement de l'authentification Azure AD . . . . .	958
Index . . . . .	959