

System Center Configuration Manager

Concepts, Architecture,
Déploiement et Support

*Préface de Jason GITHENS,
Principal Program Manager
System Center Configuration Manager
Microsoft Corp*

→ Informatique technique



Jean-Sébastien
DUCHÊNE

Guillaume
CALBANO



 **epsilon**
Collection

Préface

Avant-propos

- 1. Introduction 11
- 2. À qui ce livre s’adresse-t-il ? 12
- 3. Niveau de connaissances requis 13
- 4. Comment ce livre est-il structuré ? 13
- 5. Les systèmes nécessaires 14
- 6. Remerciements 15

Chapitre 1

Aperçu et fondamentaux de ConfigMgr

- 1. Introduction 17
- 2. Histoire de Configuration Manager 18
- 3. ConfigMgr as a Service 29
- 4. Version Current Branch ou à support étendu ? 32
- 5. Fonctionnalités et nouveautés de Configuration Manager 33
 - 5.1 Les fonctionnalités 33
 - 5.2 Les nouveautés 37
 - 5.2.1 System Center 2012 Configuration Manager 37
 - 5.2.2 Évolutions avec le Service Pack 1 40
 - 5.2.3 Évolutions avec ConfigMgr 2012 R2 42
 - 5.2.4 Évolutions avec ConfigMgr 2012 SP2/R2 SP1 46
 - 5.2.5 De nouvelles bases avec ConfigMgr 1511 49
 - 5.2.6 Les ajouts de ConfigMgr 1602 52
- 6. Terminologie et concepts 54
 - 6.1 Quelle différence entre un client et un périphérique ? 54
 - 6.2 La notion de site 55
 - 6.3 La hiérarchie de sites 56
 - 6.4 Les sites Configuration Manager 57
 - 6.5 Les systèmes de site 58
 - 6.6 SMS Provider 63

6.7	Les ressources	63
6.8	Les limites et groupes de limites	64
6.9	Les découvertes	65
6.10	Les collections	65
6.11	Les requêtes	66
7.	Les modes de gestion	66
7.1	La gestion traditionnelle et son client	66
7.2	La gestion moderne	71
8.	La console d'administration	71
8.1	Description des vues	73
8.2	Panneau principal	85
8.3	Vue détaillée des objets	86
8.4	Barre de navigation	87
8.5	Ruban	87
8.6	Organisation des objets	89
9.	Fonctionnalités d'accessibilité	91
9.1	Les raccourcis-clavier	91
9.2	Accessibilité sous Microsoft Windows	91
10.	Le support des langues	92
11.	Les communications	93
11.1	Les communications site à site	93
11.2	Les communications intrasites	96
11.3	Les communications serveurs vers les ressources externes	96
11.4	Les communications clients à serveurs	98
11.5	Les communications de la console	99
12.	La gestion du contenu	99
13.	La notion de déploiement	105
14.	Conclusion	105

Chapitre 2
Concevoir et déployer ConfigMgr

- 1. Introduction 107
- 2. Planification et conception d'une architecture 108
 - 2.1 Initialisation du projet 108
 - 2.2 Les licences 109
 - 2.3 Construction d'une hiérarchie ConfigMgr 112
 - 2.3.1 Rappels sur les sites 113
 - 2.3.2 Standalone ou CAS ? 113
 - 2.3.3 Les systèmes de site 116
 - 2.3.4 Gestion des limites et des groupes de limites 117
 - 2.4 Gestion de la capacité 117
 - 2.4.1 Les contraintes du produit 118
 - 2.4.2 Planifier la configuration matérielle 120
 - 2.4.3 Planifier la base de données de site 125
 - 2.5 L'administration orientée vers l'utilisateur 127
 - 2.6 Prendre en compte le réseau 129
 - 2.6.1 L'accès à la console d'administration 129
 - 2.6.2 La réplication intersites 130
 - 2.6.3 Les communications clientes 132
 - 2.6.4 Le contenu 134
 - 2.7 Gérer les scénarios spécifiques 143
 - 2.7.1 Gérer les clients en dehors de la forêt 143
 - 2.7.2 Planifier les périphériques en mobilité 145
 - 2.8 Les dépendances externes 149
 - 2.8.1 L'annuaire Active Directory 149
 - 2.8.2 Le déploiement de certificats 151
 - 2.8.3 Application Virtualization 151
- 3. Implémentation de ConfigMgr 152
 - 3.1 Active Directory 152
 - 3.2 Installation des sites 153
 - 3.2.1 Prérequis 154
 - 3.2.2 Installation du site d'administration central (CAS) 160
 - 3.2.3 Installation des sites primaires 164
 - 3.2.4 Installation des sites secondaires 168
 - 3.2.5 Installation de sites par script 171

3.3	Configuration d'un site	173
3.4	Installation de systèmes de site	179
3.4.1	Installation du Service Connection Point	180
3.4.2	Installation du Management Point	182
3.4.3	Installation du Fallback Status Point	184
3.4.4	Installation d'un Distribution Point	184
3.4.5	Installation d'un Distribution Point basé dans le cloud	187
3.4.6	Installation des rôles Enrollment Point et Enrollment Proxy Point	190
3.4.7	Installation de l'Asset Intelligence Synchronization Point . . .	191
3.4.8	Installation du Reporting Services Point	192
3.4.9	Installation des rôles Application Catalog Web Service Point et Application Catalog Website Point	194
3.4.10	Installation du Software Update Point	198
3.4.11	Installation du rôle Endpoint Protection Point	203
3.4.12	Installation du State Migration Point	205
3.4.13	Installation du Certificate Registration Point	207
3.5	Dépannage de l'installation	217
3.6	Installation de la console d'administration	224
4.	Conclusion	226

Chapitre 3

Planifier et gérer les clients traditionnels

1.	Introduction	227
2.	La découverte des ressources	228
3.	Planification des limites et des groupes de limites de site	238
4.	Planification du déploiement du client	242
4.1	Client Windows	242
4.1.1	Prérequis	242
4.1.2	Installation du client	247
4.2	Client pour serveurs UNIX/Linux	265
4.2.1	Prérequis	266
4.2.2	Installation du client	268

4.3	Client Mac	269
4.3.1	Prérequis	269
4.3.2	Installation du client	271
5.	Maintenance du client	276
5.1	Dépannage de l'installation du client	276
5.2	Surveillance de l'état de santé du client	278
5.3	Réaffectation du client	281
5.4	Dépannage du client	282
5.5	Lancement de notifications sur les clients	285
6.	Paramétrages des agents du client	288
6.1	Background Intelligent Transfer	289
6.2	Cloud Services	290
6.3	Client Policy	290
6.4	Compliance Settings	291
6.5	Computer Agent	291
6.6	Computer Restart	294
6.7	Endpoint Protection	294
6.8	Enrollment	296
6.9	Hardware Inventory	297
6.10	Metered Internet Connections	298
6.11	Power Management	298
6.12	Remote Tools	299
6.13	Software Deployment	301
6.14	Software Inventory	301
6.15	Software Metering	302
6.16	Software Updates	303
6.17	State Messaging	303
6.18	User and Device Affinity	304
6.19	Windows PE Peer Cache/Client Cache Settings	304
6.20	Quel est le jeu de paramètres résultant ?	305
7.	Mise à jour du client	306
8.	Désinstallation du client	309
9.	Conclusion	310

Chapitre 4**Planifier et gérer les périphériques modernes**

1. Introduction	311
2. Présentation des solutions	312
3. Le connecteur Exchange	314
3.1 Fonctionnement du connecteur	315
3.2 Prérequis	316
3.3 Configuration du connecteur	317
3.4 Aperçu des fonctionnalités	322
3.5 Dépannage	324
4. Gestion directe en mode On-Premises par enregistrement sur ConfigMgr	324
4.1 Fonctionnement	324
4.2 Prérequis	325
4.3 L'enregistrement	339
4.4 Aperçu des fonctionnalités	341
4.5 Dépannage	342
5. Gestion hybride via enregistrement dans Microsoft Intune	343
5.1 Fonctionnement	344
5.2 Prérequis	349
5.2.1 Création d'un abonnement Microsoft Intune	350
5.2.2 Ajout du nom de domaine public au service	351
5.2.3 Configuration des comptes utilisateurs	352
5.2.4 Mise en place d'Azure AD Connect	353
5.2.5 Gestion des mots de passe	357
5.2.6 Prérequis des périphériques	358
5.3 Paramétrage de ConfigMgr	359
5.3.1 Ajout de l'abonnement Microsoft Intune	359
5.3.2 Configuration des plateformes	364
5.3.3 Création de charte et conditions d'utilisation	375
5.4 Enregistrement des périphériques	377
5.4.1 iOS	377
5.4.2 Windows 10 Desktop	379
5.4.3 Windows 10 Mobile	384
5.4.4 Android	386
5.4.5 Mac OS X	388

- 5.5 Changement de propriétaire 390
- 5.6 Dépannage..... 391
- 6. Les rapports 392
- 7. Conclusion 393

Chapitre 5
Migration d'environnements

- 1. Introduction..... 395
- 2. Présentation de la migration..... 395
- 3. Planification de la migration..... 398
 - 3.1 Évaluation de la migration..... 398
 - 3.2 Validation des prérequis..... 399
 - 3.3 Planification des infrastructures 401
 - 3.4 Planification de la migration des objets 401
 - 3.4.1 Les collections 403
 - 3.4.2 Les objets 404
 - 3.4.3 Cas des objets non migrés..... 406
 - 3.5 Planification de la migration des clients 407
 - 3.6 Maintien de la continuité de service 408
 - 3.7 Mise à jour et réassignation des points de distribution 410
- 4. Configuration et migration..... 412
 - 4.1 Configuration de la hiérarchie source 412
 - 4.2 Les tâches de migration 414
 - 4.3 Réassigner des points de distribution 417
 - 4.4 Nettoyage des données de migration 420
- 5. Conversion des packages en applications 421
 - 5.1 Présentation de Package Conversion Manager..... 421
 - 5.2 Utilisation de Package Conversion Manager 422
- 6. Suivi et dépannage de la migration 425
 - 6.1 Suivi de la migration..... 425
 - 6.2 Les fichiers de journalisation 426
- 7. Conclusion 426

Chapitre 6

Sécurisation de ConfigMgr

1. Introduction	427
2. Planification de la sécurité	427
3. Role-Based Administration	429
3.1 Le SMS Provider	430
3.2 Les rôles de sécurité	431
3.3 Les étendues de sécurité	436
3.4 Le filtrage par collections	438
3.5 Les utilisateurs administratifs	438
3.6 Création d'une délégation plus granulaire	440
3.7 La délégation d'accès aux rapports	441
3.8 Auditer les permissions	443
3.9 Auditer les actions administratives	445
4. Sécurisation de l'infrastructure	449
4.1 Les recommandations générales	449
4.2 Active Directory	453
4.3 La base de données	454
4.4 Les serveurs web IIS	455
4.5 Les communications	457
4.5.1 Les communications site à site	457
4.5.2 Les communications intrasites	457
4.5.3 Les communications client/serveur	458
4.5.4 Les communications serveurs vers les ressources internes	466
4.5.5 Les communications serveurs vers les ressources Internet	466
4.5.6 Les communications de la console	467
4.6 Le contenu	468
4.7 Les comptes de service	469
4.8 Les groupes de sécurité	477
4.9 Les rôles de base de données	479
5. Les certificats	480
5.1 Aperçu des certificats	480
5.2 Déploiement des certificats web sur les systèmes de site	484
5.3 Création des certificats de supervision des rôles Management Point et State Migration Point	488
5.4 Déploiement des certificats clients Windows et UNIX	491

5.5 Déploiement des certificats pour les ordinateurs Mac 492
5.6 Gestion des certificats 493
6. Conclusion 494

Chapitre 7

Maintenance d'une infrastructure SCCM

1. Introduction 495
2. Planification de la continuité de service 495
2.1 Le serveur de site 496
2.2 La base de données 496
2.3 Le Management Point 497
2.4 Le Distribution Point 498
2.5 Le Software Update Point 499
2.6 Le State Migration Point 500
2.7 Le SMS Provider 500
2.8 Le Reporting Services Point 502
2.9 Les rôles du catalogue d'applications 503
2.10 Le Certificate Registration Point 503
2.11 Comment gérer les rôles n'ayant pas de mécanisme
de haute disponibilité ? 503
3. Planification de la reprise d'activité après un sinistre 504
3.1 Sauvegarde de l'infrastructure 504
3.1.1 Planification de la sauvegarde 504
3.1.2 Sauvegarde d'un CAS ou d'un site primaire 505
3.1.3 Comment gérer ce qui n'est pas sauvegardé par le produit ? . 510
3.1.4 Les mécanismes de restauration externes 512
3.2 La restauration 513
3.2.1 Que se passe-t-il durant la restauration ? 513
3.2.2 Restauration d'un CAS ou d'un site primaire 515
3.2.3 Cas des sites secondaires 523
4. Administration de l'infrastructure 524
4.1 Les exclusions antivirales 524
4.2 Fonctionnement et configuration de la télémétrie 526
4.3 Mise à jour de l'infrastructure 530
4.4 Mise à jour de la hiérarchie 531

4.4.1	Mise à jour de ConfigMgr 2012 vers Configuration Manager Current Branch	534
4.4.2	Déploiement d'une build	540
4.4.3	Mise à jour de la librairie PowerShell	552
4.5	Ajout de langues	553
4.6	Déplacement du serveur de site	555
4.7	Modification de la configuration SQL d'un site	556
4.8	PowerShell	557
4.9	La boîte à outils	558
4.10	Les tâches de maintenance	560
4.10.1	Les tâches de maintenance intégrées	560
4.10.2	Les opérations de maintenance	569
5.	Supervision de l'infrastructure	571
5.1	Le système d'alertes	571
5.2	Les messages d'état	574
5.3	Les fichiers de journalisation	586
5.4	Supervision avec System Center Operations Manager	587
6.	Dépannage de l'infrastructure	588
6.1	Les services	588
6.2	Les composants	591
6.3	Dépannage de la réplication SQL	599
6.4	Mise hors service de ConfigMgr	606
7.	Conclusion	608
	Conclusion	609
	Index	611



Chapitre 4

Planifier et gérer les périphériques modernes

1. Introduction

Avec la multiplication des périphériques et des usages, la gestion des périphériques mobiles et modernes est devenue une nécessité pour les entreprises. Le nombre de périphériques connectés à Internet continue de croître et la part d'utilisateurs possédant plus d'un périphérique ne cesse d'augmenter. En 2011, les utilisateurs avertis possèdent entre 5 et 7 périphériques connectés à Internet (ordinateurs, tablettes, smartphones, consoles de jeu, télévision connectée...). Ils sont ainsi de plus en plus demandeurs de nouvelles technologies en poussant l'usage de smartphones ou de tablettes en entreprise. On appelle cette tendance la consumérisation de l'IT. Nombre d'entreprises font le choix de fournir une gamme de téléphones pour couvrir les goûts des employés avec une approche *Choose Your Own Device*. D'autres prennent le pari du *Bring Your Own Device* (BYOD), laissant les usagers choisir leurs périphériques personnels, qu'ils utilisent à des fins professionnelles. Quelle que soit la direction, l'entreprise se doit de fournir un service permettant l'accès aux outils de travail sur ces nouveaux périphériques. En outre, le service informatique doit assurer la protection des données stockées sur des appareils parfois difficilement contrôlables. Les solutions de gestion des périphériques mobiles, ou Mobile Device Management, fleurissent et offrent des services divers et variés visant à couvrir les besoins des entreprises. Microsoft n'est pas un novice en la matière puisque l'entreprise proposait déjà System Center Mobile Device Manager 2008. Ce produit couvrait les périphériques mobiles équipés du système Windows Mobile 6.1. Microsoft décida d'intégrer la solution à son produit System Center Configuration Manager 2007. Après plusieurs années de retard, Microsoft propose avec System Center 2012 Configuration Manager des solutions à la gestion des périphériques mobiles.

System Center Configuration Manager Current Branch vient enrichir l'offre de gestion des périphériques modernes d'entreprise. On retrouve différents moyens de gérer ces périphériques : via un connecteur Exchange, via une infrastructure hybride couplée avec Microsoft Intune ou simplement en mode On-Premises. Tous ces mécanismes offrent des fonctionnalités différentes qui permettent de provisionner le périphérique, contrôler l'accès aux ressources de l'entreprise, prévenir les fuites de données, etc. Ce chapitre visera à détailler les solutions d'administration disponibles.

2. Présentation des solutions

La gestion des périphériques modernes diffère de celle des périphériques traditionnels. Elle a son propre cycle de vie avec quatre grandes étapes :

- L'**enregistrement** est la première phase, correspondant à la récupération du périphérique sans solution de gestion. L'utilisateur ou l'opérateur enregistre alors le périphérique dans une solution d'administration.
- Le **provisionnement** permet de rendre le périphérique opérationnel pour l'utilisateur en déployant les stratégies de sécurité, les applications, les profils VPN, Wi-Fi, et de certificats. Le but est de donner accès à tous les éléments et ressources nécessaires pour le travail de l'utilisateur.
- La **gestion et la protection** correspond aux étapes récurrentes d'administration. Le but est de surveiller la conformité du périphérique, prévenir les fuites de données et fournir des services comme l'accès en libre-service à des applications.
- Le **retrait** est la dernière phase qui peut intervenir lorsque le périphérique est volé (effacement complet) ou rendu (effacement sélectif).

System Center Configuration Manager propose différentes solutions qui supportent différents types de plateformes. On retrouve trois solutions :

- Le **connecteur Exchange Server** qui permet d'interconnecter l'infrastructure ConfigMgr à un Client Access Server Exchange pour récupérer les informations et gérer les périphériques via le protocole Exchange ActiveSync.
- Les **périphériques mobiles enregistrés par Microsoft Intune** et administrables directement à partir de Configuration Manager.
- Les **périphériques mobiles enregistrés par Configuration Manager** via la solution On-Premises introduite avec Configuration Manager Current Branch.

■ Remarque

ConfigMgr ne supporte pas l'utilisation de la gestion des périphériques modernes enregistrés via Microsoft Intune et en mode On-Premises par enregistrement via ConfigMgr. Les deux solutions nécessitant chacune un abonnement Microsoft Intune, vous devez utiliser l'une ou l'autre méthode. Il n'est pas possible de définir deux abonnements Microsoft Intune et deux autorités de gestion en même temps.
















Voici un récapitulatif des solutions et des plateformes qu'elles supportent :

Solutions	Périphériques mobiles supportés
Connecteur Exchange	– Tous les périphériques compatibles Exchange ActiveSync
Enregistré par Microsoft Intune	– Windows Phone 8 et 8.1 – Windows RT et Windows 8.1 RT – Windows 8.1 – Windows 10 Desktop et Mobile – iOS 7.1 et plus – Android 4.0 ou plus (y compris Samsung KNOX) – Mac OS X 10.9 ou plus
Enregistré par Configuration Manager On-Premises	– Windows 10 Pro et Entreprise – Windows 10 Mobile et Mobile Entreprise – Windows 10 Team (à partir de ConfigMgr 1602)

■ Remarque

La liste des périphériques supportés évolue. Pour obtenir les dernières informations, référez-vous à : <https://technet.microsoft.com/library/dn600287.aspx>

Les fonctionnalités proposées dépendent de la solution, voici un tableau récapitulatif :

Fonctionnalités\ Solutions	Connecteur Exchange	Enregistré par Microsoft Intune	Enregistré par Configuration Manager On-Premises
Sécurisation des communications par certificat			
Installation d'un client		 **	
Gestion par Internet			
Découverte			
Enregistrement			

Fonctionnalités\ Solutions	Connecteur Exchange	Enregistré par Microsoft Intune	Enregistré par Configuration Manager On-Premises
Inventaire matériel	✓ *	✓	✓
Inventaire logiciels	✗	✓ **	✓ **
Collection de fichiers	✗	✗	✗
Gestion des paramètres	✓ *	✓ **	✓ **
Déploiement d'applications	✗	✓	✓ *
Portail d'entreprise	✗	✓	✗
Accès conditionnel aux ressources de l'entreprise	✓ *	✓ **	✗
Effacement ou retrait à distance	✓	✓	✓

* *Fonctionnalités limitées*

** *Dépend de la plateforme*

Le reste du chapitre abordera la mise en œuvre des solutions comprenant le connecteur Exchange, la gestion par enregistrement sur ConfigMgr en mode On-Premises et par enregistrement sur Microsoft Intune.

3. Le connecteur Exchange

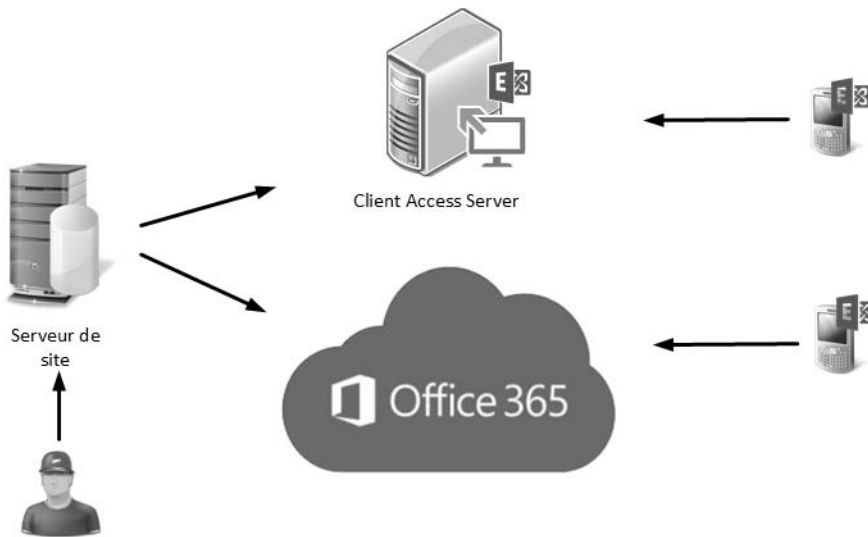
Le connecteur Exchange de Configuration Manager est un mécanisme mis en place par Microsoft pour ramener l'administration des périphériques mobiles, habituellement gérés par les administrateurs de messagerie, aux administrateurs des ressources.

■ Remarque

Outre la gestion des périphériques mobiles via ce biais, le connecteur Exchange est utilisé lorsque vous souhaitez faire de l'accès conditionnel à la messagerie, contrôlé via la gestion des périphériques mobiles enregistrés avec Microsoft Intune.

3.1 Fonctionnement du connecteur

Le connecteur permet à System Center Configuration Manager de se greffer à des serveurs CAS (*Client Access Server*) Exchange ou au service Office 365. Le but est de paramétrer des stratégies ou récupérer des informations relatives aux périphériques mobiles ayant configuré un compte de messagerie de l'organisation via une plateforme compatible avec le protocole Exchange ActiveSync.



L'administrateur ConfigMgr peut utiliser la console d'administration pour opérer les actions suivantes :

- Découvrir des périphériques.
- Consulter l'inventaire du terminal comprenant les propriétés suivantes :
 - Nom du périphérique.
 - Identifiant du périphérique.
 - Numéro IMEI.
 - Opérateur mobile.
 - Système d'exploitation.
 - Langue du système.
 - Numéro de téléphone.
 - Type de périphérique.
 - Modèle du périphérique.

- Nom de l'utilisateur.
- Nom.
- GUID.
- Et bien d'autres propriétés récupérées par ce biais.
- Appliquer des stratégies ActiveSync.
- Effacer à distance les données du périphérique.

3.2 Prérequis

La création du connecteur Exchange nécessite l'une des plateformes suivantes :

- Exchange Server 2010 SP1/SP2
- Exchange Server 2013
- Exchange Online (Office 365)

Si vous souhaitez utiliser un compte de service, celui-ci doit disposer des permissions suivantes :

- Clear-ActiveSyncDevice
- Get-ActiveSyncDevice
- Get-ActiveSyncDeviceAccessRule
- Get-ActiveSyncDeviceStatistics
- Get-ActiveSyncMailboxPolicy
- Get-ActiveSyncOrganizationSettings
- Get-ExchangeServer
- Get-Recipient
- Get-User
- Set-ADServerSettings
- Set-ActiveSyncDeviceAccessRule
- Set-ActiveSyncMailboxPolicy
- Set-CASMailbox
- New-ActiveSyncDeviceAccessRule
- New-ActiveSyncMailboxPolicy
- Remove-ActiveSyncDevice