

System Center 2012 R2 Configuration Manager (SCCM)

Concepts, Utilisation
et Administration

Préface de **Jean-Philippe DUPUICH**,
Chef Produit System Center - Microsoft France

Informatique technique



Microsoft
Most Valuable
Professional

Jean-Sébastien
DUCHÈNE

Guillaume
CALBANO




Collection

epsilon

Avant-propos

1. Introduction	19
2. À qui ce livre s'adresse-t-il ?	20
3. Niveau de connaissances requis	20
4. Comment ce livre est-il structuré ?	21
5. Les systèmes nécessaires	22
6. Remerciements	23

Chapitre 1

Aperçu et fondamentaux de ConfigMgr 2012

1. Introduction	25
2. L'histoire de Configuration Manager	26
3. Les fonctionnalités et nouveautés de Configuration Manager 2012	35
3.1 Les fonctionnalités	35
3.2 Les nouveautés	38
3.2.1 Évolutions avec le Service Pack 1	41
3.2.2 Évolutions avec ConfigMgr 2012 R2	43
4. La terminologie et les concepts	47
4.1 La notion de site	47
4.2 La hiérarchie de sites	47
4.3 Les sites Configuration Manager	48
4.4 Les systèmes de site	50
4.5 SMS Provider	54
4.6 Les ressources	54
4.7 Les limites et groupes de limites	55
4.8 Les découvertes	56
4.9 Les collections	56
4.10 Les requêtes	57
5. Le client	57
6. La console d'administration	62
6.1 Description des vues	63
6.2 Panneau principal	72
6.3 Vue détaillée des objets	72

6.4	Barre de navigation	73
6.5	Ruban	73
6.6	Organisation des objets	75
7.	Fonctionnalités d'accessibilité	77
7.1	Les raccourcis-clavier	77
7.2	Accessibilité sous Microsoft Windows	77
8.	Le support des langues	78
9.	Les communications	79
9.1	Les communications site à site	79
9.2	Les communications intrasites	81
9.3	Les communications serveurs vers les ressources externes	82
9.4	Les communications client à serveurs	83
9.5	Les communications de la console	84
10.	La gestion du contenu	84
11.	La notion de déploiement	89
12.	Conclusion	90

Chapitre 2

Concevoir et déployer ConfigMgr 2012

1.	Introduction	91
2.	Planifier et concevoir votre architecture	92
2.1	Initialisation du projet	92
2.2	Les licences	93
2.3	Construire sa hiérarchie	96
2.3.1	Rappel des sites	96
2.3.2	CAS ou pas CAS ?	97
2.3.3	Les systèmes de site	99
2.3.4	Gérer les limites et groupes de limites	100
2.4	Gestion de la capacité	101
2.4.1	Les contraintes du produit	101
2.4.2	Planifier la configuration matérielle	103
2.4.3	Planifier la base de données de site	108
2.5	L'administration tournée utilisateur	110

2.6	Prendre en compte le réseau	111
2.6.1	L'accès à la console d'administration	111
2.6.2	La réplication intersite	112
2.6.3	Les communications clientes	114
2.6.4	Le contenu	116
2.7	Gérer les scénarios spécifiques	124
2.7.1	Gérer les clients en dehors de la forêt	124
2.7.2	Planifier les clients Internet	127
2.8	Les dépendances externes	129
2.8.1	L'annuaire Active Directory	129
2.8.2	Le déploiement de certificats	131
3.	Implémentation de ConfigMgr 2012	132
3.1	Active Directory	132
3.2	Installation des sites	133
3.2.1	Les pré-requis	133
3.2.2	Installation du site d'administration central (CAS)	139
3.2.3	Installation des sites primaires	142
3.2.4	Installation des sites secondaires	146
3.2.5	Installation de sites par script	149
3.3	Configuration d'un site	150
3.4	Installation de systèmes de site	154
3.4.1	Installation du Management Point	156
3.4.2	Installation du Fallback Status Point	157
3.4.3	Installation d'un Distribution Point	158
3.4.4	Installation d'un Distribution Point basé dans le cloud	161
3.4.5	Installation des rôles Enrollment Point et Enrollment Proxy Point	164
3.5	Dépanner l'installation	165
3.6	Installation de la console d'administration	168
3.7	La mise hors service de ConfigMgr	171
4.	Conclusion	173

Chapitre 3**Planifier et gérer le client ConfigMgr**

1. Introduction	175
2. La découverte des ressources	176
3. Planifier les limites et groupes de limites de site	186
4. Planifier le déploiement du client	189
4.1 Client Windows	189
4.1.1 Les pré-requis	190
4.1.2 Installation du client	194
4.2 Client pour serveurs UNIX/Linux	211
4.2.1 Les pré-requis	211
4.2.2 Installation du client	213
4.3 Client Mac	214
4.3.1 Les pré-requis	215
4.3.2 Installation du client	216
5. Maintenir le client	221
5.1 Dépanner l'installation du client	221
5.2 Gérer l'état de santé du client	223
5.3 Réassigner le client	226
5.4 Dépanner le client	227
5.5 Lancer des notifications sur les clients	230
6. Mettre à jour le client	231
7. Désinstaller le client	233
8. Les paramètres des agents du client	234
8.1 Background Intelligent Transfer	235
8.2 Cloud Services	236
8.3 Client Policy	236
8.4 Compliance Settings	237
8.5 Computer Agent	237
8.6 Computer Restart	239
8.7 Endpoint Protection	240
8.8 Hardware Inventory	242
8.9 Metered Internet Connections	242
8.10 Mobile Devices ou Enrollment	243
8.11 Network Access Protection (NAP)	243

8.12 Power Management	244
8.13 Remote Tools	245
8.14 Software Deployment	247
8.15 Software Inventory	247
8.16 Software Metering	248
8.17 Software Updates	249
8.18 State Messaging	249
8.19 User and Device Affinity	250
8.20 Quel est le jeu de paramètres résultant ?	250
9. La gestion de l'énergie	251
10. Conclusion	256

Chapitre 4 Inventaires

1. Introduction	257
2. L'inventaire matériel	258
2.1 Concepts et composants	258
2.1.1 Terminologie	259
2.1.2 Paramétrage de l'agent d'inventaire	260
2.1.3 Les fichiers utilisés par l'inventaire	265
2.1.4 Dossiers de réception Inboxes	266
2.2 Extensions de l'inventaire	267
2.3 Exploiter l'inventaire	271
2.3.1 Console d'administration SCCM	271
2.3.2 Console SQL	271
2.3.3 Resource Explorer	272
2.3.4 Affichage des rapports d'inventaire	273
2.4 Destruction des données d'inventaire	273
2.5 Les rapports d'inventaire	274
2.6 Dépannage	275
2.6.1 Côté client	275
2.6.2 Côté serveur	277

3.	Inventaire logiciel et collecte de fichiers	277
3.1	Concepts et composants	277
3.1.1	Fichiers d'inventaire logiciel	280
3.1.2	Dossiers Inboxes	280
3.2	Exploiter l'inventaire logiciel	281
3.3	Les rapports d'inventaire logiciel	282
3.4	Dépannage	282
3.4.1	Côté client	282
3.4.2	Côté serveur	283
4.	Asset Intelligence	284
4.1	Pré-requis	285
4.2	Catalogue	285
4.2.1	Catégories	286
4.2.2	Familles	286
4.2.3	Légendes	286
4.2.4	Configuration matérielle	287
4.3	Synchronisation du catalogue	288
4.3.1	Installation de l'Asset Intelligence Synchronization Point	288
4.3.2	Mise à jour du catalogue	288
4.4	Exploitation de l'inventaire étendu	289
4.5	Les rapports Asset Intelligence	292
4.5.1	Rapports matériel	292
4.5.2	Rapports logiciels	293
4.5.3	Rapports de licences	293
4.6	Dépannage de l'inventaire et problèmes communs	294
5.	Contrôle logiciel	295
5.1	Concept et composants du contrôle de logiciel	296
5.2	Pré-requis pour le contrôle logiciel	296
5.3	Exploiter le contrôle logiciel	297
5.4	Les rapports du contrôle logiciel	300
5.5	Dépannage du contrôle logiciel	300
6.	Conclusion	301

Chapitre 5
Requêtes, collections et rapports

- 1. Introduction 303
- 2. Requêtes 304
 - 2.1 Concept et composants 304
 - 2.2 Création de requêtes 305
 - 2.3 Actions sur les requêtes 311
- 3. Collections 312
 - 3.1 Concept et composants 312
 - 3.2 Collection utilisateur 316
 - 3.3 Collection système 328
 - 3.4 Fenêtres de maintenance 343
 - 3.5 Bonnes pratiques 347
- 4. Rapports 350
 - 4.1 Concept et composants 350
 - 4.2 Reporting Service Point 351
 - 4.2.1 Pré-requis 351
 - 4.2.2 Installation du rôle 352
 - 4.3 Exploiter les rapports 355
 - 4.3.1 Utilisation de la console 355
 - 4.3.2 Utilisation de l'interface web 358
 - 4.4 Souscription à des rapports 360
 - 4.5 Personnalisation des rapports 364
 - 4.5.1 Modification de rapports existants 364
 - 4.5.2 Création de nouveaux rapports 365
 - 4.6 Bonnes pratiques 367
 - 4.7 Dépannage 368
- 5. Conclusion 369

Chapitre 6**La distribution d'applications**

1. Introduction	371
2. Vue d'ensemble de la télédistribution applicative	372
2.1 Les concepts et objets	372
2.2 Cibler les utilisateurs ou les systèmes ?	373
3. Planifier l'infrastructure de distribution	374
3.1 Les pré-requis	374
3.2 Le catalogue d'applications	375
3.3 Le déploiement d'applications modernes Windows	380
4. Aperçu du modèle hérité : le package	381
4.1 Les concepts	381
4.2 Création d'un package	382
5. Présentation du nouveau modèle : les applications	390
5.1 Les concepts	390
5.2 Créer une application	394
5.3 Créer des types de déploiement	397
5.3.1 Windows Installer	397
5.3.2 Script Installer	398
5.3.3 Redirection de l'utilisateur sur le magasin éditeur	405
5.3.4 Packages d'application Android, Windows, Windows Phone et iOS	407
5.3.5 Application Virtualization	408
5.3.6 Mac OS	410
5.3.7 Web Application	413
5.4 Gérer les types de déploiement	413
5.5 Gérer les applications	414
5.5.1 L'historique des révisions	414
5.5.2 Copier/importer/exporter une application	415
5.5.3 Remplacer l'application	416
5.5.4 Retirer et supprimer une application	417
5.5.5 Afficher les relations	417
5.6 Les environnements virtuels App-V	418
5.7 Les conditions et expressions globales	419

6.	Déployer vos applications	425
6.1	Maintenir le contenu sur les points de distribution	425
6.1.1	Distribution du contenu	425
6.1.2	Mise à jour du contenu	425
6.1.3	Retirer du contenu	426
6.2	Déployer les packages ou les applications	426
6.3	L'expérience utilisateur	428
6.4	Les demandes d'applications	433
6.5	Suivre le déploiement	433
7.	Dépanner	434
8.	Conclusion	435

Chapitre 7

La sécurité des ressources clientes

1.	Introduction	437
2.	La gestion des mises à jour logicielles	438
2.1	Concepts et composants	438
2.1.1	Les composants et terminologies	438
2.1.2	La gestion selon Microsoft	440
2.1.3	Le processus de mise à jour via ConfigMgr	445
2.1.4	Planifier sa stratégie de déploiement	447
2.2	Préparation de l'infrastructure	449
2.2.1	Pré-requis	449
2.2.2	Installation du rôle Software Update Point	454
2.2.3	Configuration de l'infrastructure de déploiement	458
2.3	Déployer manuellement les mises à jour	460
2.3.1	Mise en œuvre de votre stratégie de déploiement manuelle	460
2.3.2	Retirer une mise à jour de vos déploiements	467
2.4	Déployer automatiquement les mises à jour	468
2.5	Déploiement de mises à jour tierces	472
2.5.1	Installation et configuration de System Center Updates Publisher	472
2.5.2	Import d'un catalogue de mises à jour tiers	474
2.5.3	Création de mises à jour	475
2.5.4	Publication de mises à jour	478
2.6	Suivre le déploiement des mises à jour logicielles	479

2.7	Suppression des mises à jour expirées	480
2.8	Dépanner le déploiement des mises à jour logicielles	481
3.	La protection contre les logiciels malveillants avec Endpoint Protection	483
3.1	L'histoire de la protection antivirus de Microsoft.	483
3.2	Les nouveautés apportées par System Center 2012 Endpoint Protection.	484
3.3	Préparation de l'infrastructure	485
3.3.1	Installation du rôle Endpoint Protection Point	485
3.3.2	Paramétrage de l'agent du client	486
3.3.3	Présentation du client Endpoint Protection	489
3.4	Planifier les stratégies Endpoint Protection.	490
3.4.1	Les stratégies antimalware	490
3.4.2	Les stratégies Firewall	495
3.5	Assurer la mise à jour d'Endpoint Protection	496
3.6	Suivre l'évolution de la protection.	497
3.6.1	Les tableaux de bord	497
3.6.2	Les notifications.	499
3.6.3	Les rapports	501
3.7	Exécuter des actions sur les clients Endpoint Protection	501
3.8	Le client Endpoint Protection pour les systèmes alternatifs	502
3.8.1	Endpoint Protection pour Mac	503
3.8.2	Endpoint Protection pour serveurs UNIX/Linux.	506
3.9	Dépanner la protection anti-logiciels malveillants	514
4.	La sécurisation de l'accès au réseau avec Network Access Protection	515
4.1	Concepts	515
4.2	Les pré-requis.	517
4.3	Installation du System Health Validator Point.	518
4.4	Configuration du composant System Health Validator Point.	519
4.5	Configuration d'une stratégie NAP	520
4.6	Configuration des clients	522
4.6.1	Configuration des postes de travail	523
4.6.2	Configuration du client ConfigMgr	524
4.7	Configuration des mises à jour.	525
4.8	Suivre la protection et la remédiation des clients.	527
4.9	Dépanner NAP	527
5.	Conclusion	529

Chapitre 8**Le déploiement de système d'exploitation**

1. Introduction	531
2. Vue d'ensemble	531
2.1 Qu'est-ce que l'OSD ?	531
2.2 Présentation des scénarios	533
2.3 Les challenges d'un déploiement et d'une migration	534
2.4 Les concepts et méthodologies	536
2.5 Les outils de déploiement proposés par Microsoft	539
2.6 Pourquoi utiliser MDT ?	540
3. Les pré-requis	541
3.1 Vue d'ensemble	541
3.2 Démarrage sur le réseau	544
3.3 Le déploiement par multidiffusion (multicast)	548
3.4 Upgrade Assessment Tool (UAT)	551
3.5 Migration de l'état utilisateur	552
3.6 Utilisation de MDT	554
4. Gérer les pilotes	556
4.1 Concepts et méthodes de gestion	556
4.2 Ajout des pilotes dans le catalogue	558
4.3 Création d'un package de pilotes	561
5. Administrer les images	562
5.1 Les images de démarrage	562
5.2 Les images d'installation	565
5.3 Construire une image de référence	566
5.3.1 Capture manuelle	566
5.3.2 Séquence de tâches Build and capture	567
5.4 Assurer le cycle de vie du master	570
5.5 Générer des médias	571
5.6 Provisionnement de disques virtuels (VHD)	573
5.6.1 Pré-requis	574
5.6.2 Création du VHD	575
5.6.3 Maintien du VHD	577
5.6.4 Import dans la librairie System Center Virtual Machine Manager	577

6.	Création d'une séquence de tâches	578
6.1	Les modèles ConfigMgr	578
6.2	Les modèles MDT	591
7.	Préparer la migration des données	596
8.	Déployer et migrer un système d'exploitation.	597
8.1	Traitement des scénarios	597
8.2	Cibler les machines	598
8.2.1	Méthode 1 : déploiement sur une machine référencée	598
8.2.2	Méthode 2 : import des informations d'une machine inconnue	599
8.2.3	Méthode 3 : utilisation de la fonctionnalité de déploiement sur des machines inconnues	601
8.3	Gérer les associations d'ordinateurs.	602
8.3.1	Aperçu.	602
8.3.2	Créer une association entre deux machines existantes	603
8.4	Redéployer une machine	604
9.	Propulser vos déploiements.	605
10.	Suivre le déploiement	606
11.	Dépanner	608
12.	Conclusion	611

Chapitre 9

La gestion des périphériques mobiles

1.	Introduction	613
2.	Présentation des solutions.	614
3.	Le connecteur Exchange	616
3.1	Fonctionnement du connecteur.	616
3.2	Les pré-requis.	617
3.3	Configuration du connecteur.	618
3.4	Aperçu des fonctionnalités.	623
3.5	Dépannage.	625
4.	La gestion native par enregistrement sur ConfigMgr	625
4.1	Fonctionnement	625
4.2	Les pré-requis.	626

4.3	L'enregistrement	628
4.4	Aperçu des fonctionnalités	630
4.5	Dépannage	630
5.	La gestion via Windows Intune	631
5.1	Fonctionnement	631
5.2	Les pré-requis	636
5.2.1	Création d'un abonnement Windows Intune	636
5.2.2	Ajout du nom de domaine public au service	637
5.2.3	Configuration des comptes utilisateurs	638
5.2.4	Mise en place de DirSync	639
5.2.5	La gestion des mots de passe	643
5.2.6	Les pré-requis des périphériques	644
5.3	Paramétrage de ConfigMgr	647
5.3.1	Ajout de l'abonnement Windows Intune	647
5.3.2	Configuration du connecteur Windows Intune	650
5.4	L'enregistrement des périphériques	650
5.4.1	iOS	650
5.4.2	Windows Phone	652
5.4.3	Windows RT et Windows 8.1	653
5.4.4	Android	654
5.5	Les extensions Windows Intune	655
5.6	Dépanner	657
6.	Les rapports	658
7.	Conclusion	659

Chapitre 10

La gestion de la conformité

1.	Introduction	661
2.	Concept et composants	662
3.	Pré-requis	666
4.	Configuration Items : fonctionnement	667
4.1	Settings et Compliance Rules	667
4.2	User data and profiles et Configuration Items	676
4.3	Éléments de configuration pour les périphériques mobiles	682

4.4	Éléments de configuration pour les systèmes Mac OS X	686
5.	Baselines : fonctionnement	689
5.1	Baselines : création et déploiement	689
5.2	Baselines : import	693
5.3	Baselines et GPO	694
6.	L'accès aux ressources de l'entreprise	698
6.1	Les profils de connexion à distance	698
6.2	Les profils de certificats	701
6.2.1	Pré-requis	701
6.2.2	Déploiement d'un certificat d'autorité de certification racine	701
6.2.3	Provisionnement de certificats personnels via Simple Certificate Enrollment Protocol	703
6.3	Les profils VPN	717
6.4	Les profils Wi-Fi	720
6.5	Les profils email	722
7.	Best Practices	725
7.1	Les meilleures pratiques Microsoft	725
7.2	Security Compliance Manager 3	727
8.	Exploitation de la conformité	729
8.1	Côté serveur	730
8.2	Côté client	732
9.	Remédiation	735
9.1	Manuelle	735
9.2	Automatique	737
10.	Les rapports	741
11.	Dépannage	741
12.	Conclusion	743

Chapitre 11

Les outils de contrôle distant

1.	Introduction	745
2.	La prise en main à distance	746

3.	Le réveil sur le réseau	751
3.1	Présentation	751
3.2	Configuration de Wake On LAN	751
3.3	Wake-up Proxy	754
3.4	Utilisation des fonctions de réveil	757
3.5	Les rapports	757
3.6	Dépanner Wake On LAN	757
4.	La gestion hors bande	758
4.1	Les pré-requis Out-of-Band	759
4.2	Implémentation de la gestion hors bande	762
4.3	Provisionnement des machines	768
4.4	Utilisation des fonctionnalités	771
4.5	Les rapports	776
4.6	Dépanner la gestion hors bande	776
5.	Conclusion	777

Chapitre 12

La migration d'environnements

1.	Introduction	779
2.	Présentation de la migration	779
3.	Planification de la migration	782
3.1	Étudier la migration	782
3.2	Validation des pré-requis	783
3.3	Planifier les infrastructures	785
3.4	Planifier la migration des objets	786
3.4.1	Les collections	787
3.4.2	Les objets	789
3.4.3	Le cas des objets non migrés	791
3.5	Planifier la migration des clients	792
3.6	Assurer la continuité de service	793
3.7	Mise à jour et réassignation des points de distribution	794
4.	Configurer et migrer	796
4.1	Configuration de la hiérarchie source	796
4.2	Les tâches de migration	798
4.3	Mise à niveau des points de distribution	801

4.4	Terminer et nettoyer la migration	805
5.	Transformer les packages en applications	805
5.1	Présentation de Package Conversion Manager	805
5.2	Utilisation de Package Conversion Manager	806
6.	Suivre et dépanner la migration	809
6.1	Suivre la migration	809
6.2	Les fichiers de journalisation	810
7.	Conclusion	810

Chapitre 13

Sécurisation de ConfigMgr 2012

1.	Introduction	811
2.	Planifier la sécurité	811
3.	Role-Based Administration	813
3.1	Le SMS Provider	814
3.2	Les rôles de sécurité	815
3.3	Les étendues de sécurité	820
3.4	Le filtrage par collections	822
3.5	Les utilisateurs administratifs	822
3.6	Créer une délégation plus granulaire	824
3.7	La délégation d'accès aux rapports	825
3.8	Auditer les permissions	827
3.9	Auditer les actions administratives	829
4.	Sécuriser l'infrastructure	833
4.1	Les recommandations générales	833
4.2	Active Directory	837
4.3	La base de données	838
4.4	Les serveurs web IIS	839
4.5	Les communications	840
4.5.1	Les communications site à site	841
4.5.2	Les communications intrasites	841
4.5.3	Les communications client/serveur	842
4.5.4	Les communications serveurs vers les ressources externes	850
4.5.5	Les communications de la console	850

4.6	Le contenu	850
4.7	Les comptes de service	851
4.8	Les groupes de sécurité	861
4.9	Les rôles de base de données	862
5.	Les certificats	864
5.1	Aperçu des certificats	864
5.2	Déploiement des certificats web sur les systèmes de site	868
5.3	Créer les certificats de supervision des rôles Management Point et State Migration Point	872
5.4	Déployer les certificats clients Windows et UNIX	875
5.5	Déployer les certificats pour les ordinateurs Mac	876
5.6	Gérer les certificats	877
6.	Conclusion	878

Chapitre 14

Maintenir une infrastructure SCCM 2012

1.	Introduction	879
2.	Planifier la continuité de service	879
2.1	Le serveur de site	880
2.2	La base de données	880
2.3	Le Management Point	881
2.4	Le Distribution Point	882
2.5	Le Software Update Point	883
2.6	Le State Migration Point	883
2.7	Le SMS Provider	884
2.8	Le Reporting Services Point	885
2.9	Les rôles du catalogue d'applications	886
2.10	Le System Health Validator Point	886
2.11	Le Certificate Registration Point	887
2.12	Comment gérer les rôles n'ayant pas de mécanisme de haute disponibilité ?	887
3.	Planifier la reprise d'activité après un désastre	888
3.1	Sauvegarder son infrastructure	888
3.1.1	Planifier la sauvegarde	888
3.1.2	Sauvegarder un CAS ou un site primaire	889

3.1.3	Comment gérer ce qui n'est pas sauvegardé par le produit ?	893
3.1.4	Les mécanismes de restauration externes	895
3.2	La restauration	895
3.2.1	Que se passe-t-il durant la restauration ?	895
3.2.2	Restauration d'un CAS ou d'un site primaire	898
3.2.3	Gérer le cas des sites secondaires	905
4.	Administrer l'infrastructure	906
4.1	Les exclusions antivirales	906
4.2	Mettre à jour	908
4.2.1	Déploiement d'un Cumulative Update	909
4.2.2	Déploiement d'un Service Pack	914
4.2.3	Déploiement de la Release 2	920
4.3	Ajouter des langues	922
4.4	Déplacer le serveur de site	923
4.5	Modifier la configuration SQL d'un site	925
4.6	PowerShell	926
4.7	La boîte à outils	927
4.8	Les tâches de maintenance	929
4.8.1	Les tâches de maintenance intégrées	929
4.8.2	Les opérations de maintenance	938
5.	Superviser l'infrastructure	940
5.1	Le système d'alertes	940
5.2	Les messages d'état	943
5.3	Les fichiers de journalisation	953
5.4	Superviser avec System Center Operations Manager	955
6.	Dépannage de l'infrastructure	955
6.1	Les services	956
6.2	Les composants	958
6.3	Dépanner la réplication SQL	967
7.	Conclusion	972
	Conclusion	973
	Index	975



Chapitre 3

Planifier et gérer le client ConfigMgr

1. Introduction

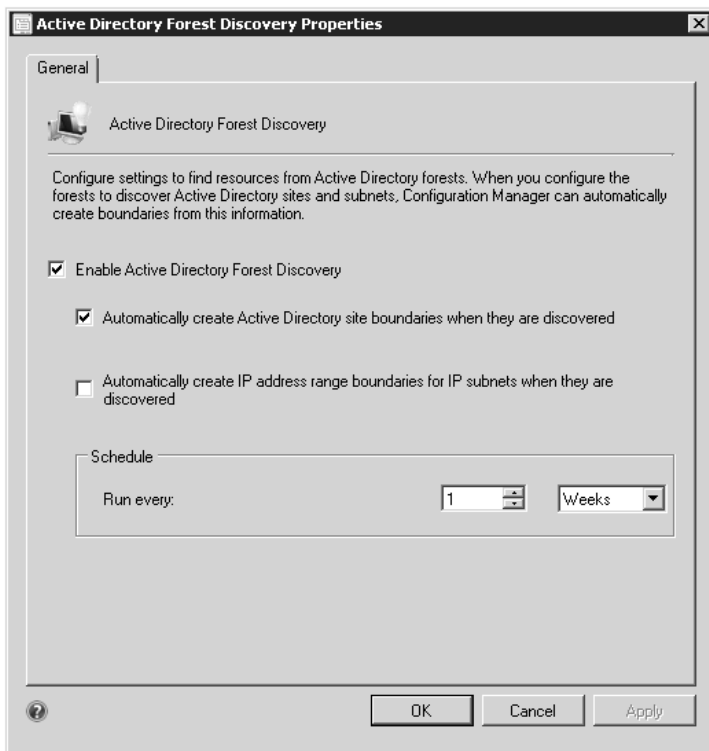
Nous avons vu précédemment comment planifier et déployer une infrastructure ConfigMgr. System Center 2012 Configuration Manager repose sur un mode client/serveur. Ce chapitre abordera les notions nécessaires à la planification, au déploiement et au maintien des clients SCCM. Nous verrons d'abord comment découvrir les ressources et quelle stratégie adopter. Nous aborderons la notion de limites de site nécessaires à l'administration et au contrôle des clients. Nous détaillerons le processus de déploiement du client et les étapes opérées par celui-ci pour devenir opérationnel. La partie suivante traitera de la planification des différents clients Windows, UNIX et Mac en détaillant les pré-requis et les méthodes d'installation proposées. Une fois le client déployé, vous pourrez retrouver une section dédiée au dépannage afin d'y retrouver les fichiers de journalisation, rapports et outils à votre disposition pour cette tâche. Nous détaillerons plus particulièrement la nouvelle fonctionnalité de gestion de l'état de santé du client permettant de donner une vision précise et globale des clients ConfigMgr. Nous listerons les différentes méthodes à votre disposition pour mettre à jour le client lors de la sortie de mises à jour cumulatives. Chaque agent du client dispose d'un ensemble de paramètres, nous détaillerons comment créer des stratégies et quels paramètres sont disponibles. Enfin, nous verrons comment assurer une gestion de l'énergie des ressources clientes afin de réduire et suivre la consommation électrique du parc.

2. La découverte des ressources

Le processus de découverte de ressources permet de provisionner la base de données System Center 2012 Configuration Manager avec les enregistrements de ressources ordinateur ou utilisateur administrables par le produit. Le processus de découverte inclut la création d'un enregistrement de données de découverte (DDR) pour chaque ressource. Cet enregistrement contient des informations comme le nom NetBIOS, les adresses IP, les sous-réseaux, la version de système d'exploitation, le domaine, le dernier utilisateur à s'être connecté. Il est utilisé par le processus Discovery Data Manager sur le serveur de site pour identifier la ressource puis la stocker dans la base de données. Cette opération n'a que pour but d'enregistrer la ressource pour qu'elle apparaisse dans la vue **Assets and Compliance**. Lorsqu'un enregistrement de données de découverte est créé au niveau d'un site secondaire, celui-ci est transféré au site primaire parent pour être traité. Les données de découverte sont rendues disponibles grâce au processus de réplication intersites au travers de l'ensemble de la hiérarchie.

System Center 2012 Configuration Manager offre différents processus de découverte. Ceux-ci ont pour but de répondre à tous les besoins. Pour les découvrir, ouvrez la console d'administration et naviguez dans **Administration - Overview - Hierarchy Configuration - Discovery Methods**.

La méthode Active Directory Forest Discovery ne découvre pas de ressources à proprement parler. Cette méthode a été implémentée pour faciliter les tâches d'administration nécessaires à la mise en œuvre et au maintien du produit. Elle permet la découverte des informations importantes comme les domaines, sites et sous-réseaux Active Directory. Vous pouvez choisir de créer des limites de site sur la base des sites Active Directory et/ou des sous-réseaux IP découverts. Cette opération est un gain de temps car il ne vous restera plus qu'à grouper ces limites pour définir les étendues d'administration. La découverte est désactivée par défaut et programmée pour s'exécuter une fois par semaine. Il vous est possible de configurer la méthode de découverte de forêts Active Directory au niveau des sites primaires et/ou du site d'administration centrale.

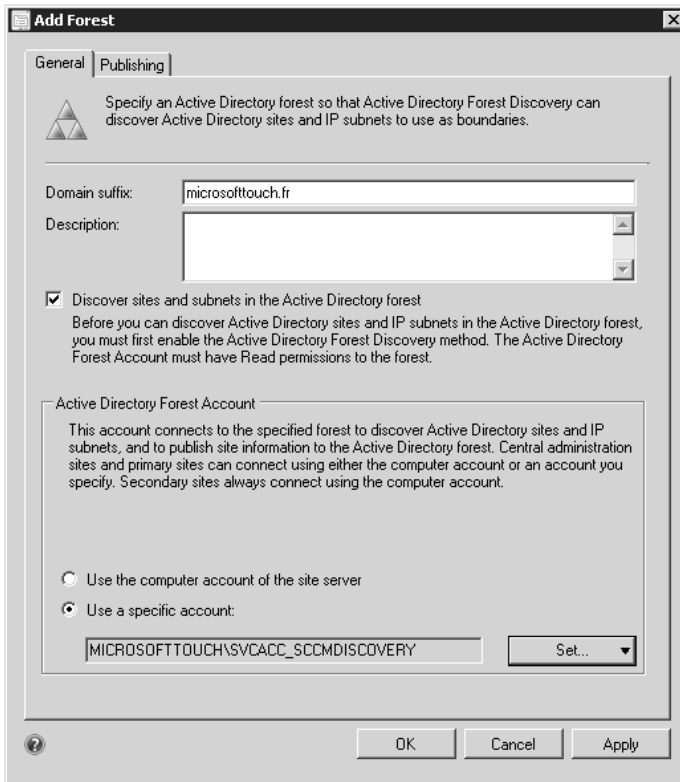


Remarque

Dans le cadre d'une hiérarchie, il est recommandé de n'activer la découverte de forêt que sur un seul site (par exemple sur le CAS) lorsque vous l'utilisez pour créer les limites.

Par défaut, le serveur de site découvre la forêt dans lequel il est installé. Vous pouvez retrouver les informations dans la partie **Administration - Overview - Hierarchy Configuration - Active Directory Forests**.

Si vous souhaitez gérer des clients dans des forêts distantes ne disposant pas par exemple de relation d'approbation bidirectionnelle, vous pouvez ajouter d'autres forêts en sélectionnant **Add Forest**. Vous devez y renseigner le suffixe du domaine, le compte utilisé pour découvrir les informations (par défaut le compte machine du serveur de site). Vous pouvez choisir de découvrir les sites et les sous-réseaux de cette forêt. En fonction du paramétrage spécifié dans la découverte de forêt, les limites de site pourront être créées automatiquement.



Remarque

Pour rappel, le niveau fonctionnel de forêt Windows Server 2012 R2 n'est pas supporté par ConfigMgr 2012 R2.

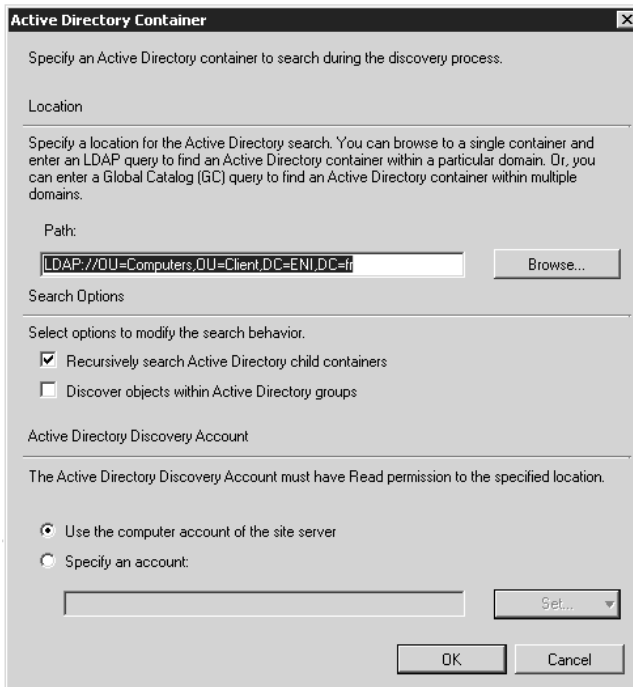
L'onglet **Publishing** permet de sélectionner les sites ConfigMgr que vous souhaitez publier dans la forêt que vous ajoutez. Pour cela, vous devez avoir procédé à l'extension de schéma Active Directory, à la création du conteneur System Management et le compte spécifié doit avoir le contrôle total dans la forêt ajoutée. Par défaut, le serveur de site publie les informations dans son domaine ou à la racine de la forêt si le serveur de site n'en fait pas partie. Vous pouvez ainsi préciser quel domaine ou quel contrôleur de domaine doit être utilisé pour opérer ce processus de publication.

Les trois méthodes de découverte Active Directory suivantes permettent de découvrir des ressources diverses par le biais d'un processus exécuté par le serveur de site. Le processus tente de contacter le contrôleur de domaine le plus proche de lui.

Il vous est cependant possible de spécifier quel contrôleur de domaine doit servir à cette opération. Pensez tout de même à spécifier un contrôleur de domaine disposant d'une connexion réseau rapide. En outre, le compte machine du serveur de site doit disposer des accès en lecture.

La méthode Active Directory System Discovery permet la découverte des ordinateurs dans votre annuaire Active Directory. Afin de créer l'enregistrement DDR (moins d'un kilo-octet), la méthode doit pouvoir être en mesure de résoudre le nom de domaine pleinement qualifié (FQDN) de la machine.

- ▣ Cette méthode n'est pas activée par défaut et doit l'être en cochant la case **Enable Active Directory System Discovery**.
- ▣ Vous devez ensuite définir les conteneurs que vous souhaitez découvrir avec un chemin au format LDAP. Vous pouvez spécifier des conteneurs dans des domaines différents. Dans ce cas de figure, vous pouvez spécifier un compte utilisateur disposant des droits de lecture pour aller lire les informations.
- ▣ Les options **Recursively search Active Directory child containers** et **Discover objects within Active Directory groups** permettent de faire de la découverte d'objets dans les sous-conteneurs et dans les groupes Active Directory.



L'onglet **Polling Schedule** permet de configurer l'intervalle d'exécution de cette découverte. Par défaut, la découverte complète est effectuée tous les 7 jours à 00h00. Le processus inclut aussi une découverte incrémentale exécutée toutes les 5 minutes pour trouver les nouvelles ressources ou celles ayant été modifiées depuis le dernier cycle de découverte.

■ Remarque

Les méthodes de découverte Active Directory sont très consommatrices en ressource processeur à la fois pour le serveur de site mais aussi pour le contrôleur de domaine cible. Elles peuvent aussi légèrement impacter le réseau. C'est pour cette raison qu'il n'est pas conseillé de configurer une programmation agressive pour la découverte complète. Microsoft recommande aussi de configurer les conteneurs de recherche au plus près et de ne pas cibler la racine du domaine.

La découverte récupère un certain nombre d'attributs des objets découverts dans Active Directory. Par défaut, les attributs objectGUID, name, SAMAccountName, objectSID, primaryGroupID, dNSHostName, userAccountControl, lastLogonTimestamp, distinguishedName sont découverts. L'onglet **Active Directory Attributes** permet d'étendre la découverte à d'autres attributs que vous pouvez utiliser pour stocker certaines valeurs. Ceci peut vous permettre, par exemple, de mettre en place une stratégie de déploiement spécifique à votre organisation.

L'onglet **Options** permet de configurer des stratégies d'exclusion d'ordinateurs. Les annuaires Active Directory ne sont pas toujours à jour et les entreprises ne disposent pas nécessairement de procédure de nettoyage des enregistrements. La découverte peut ainsi remonter un nombre important d'ordinateurs n'existant plus au sein de l'entreprise. L'option **Only discover computers that have logged on to a domain in a given period of time** permet d'exclure les machines qui ne se sont pas connectées au domaine durant une période définie (90 jours par défaut) en utilisant l'attribut **lastlogonTimestamp**. Cet attribut n'est arrivé qu'avec le niveau fonctionnel de domaine Windows Server 2003. La seconde option **Only discover computers that have updated their computer account password in a given period of time** permet d'exclure les machines qui n'ont pas changé de mot de passe durant une période spécifique (90 jours par défaut) en utilisant l'attribut **PwdLastSet**.

■ Remarque

Si vous cochez les deux options, les machines qui ne répondent pas à au moins un des deux critères sont automatiquement exclues.

La méthode Active Directory User Discovery permet la découverte des utilisateurs dans votre annuaire Active Directory. Cette méthode est indispensable si vous souhaitez déployer des applications en ciblant les utilisateurs. Elle n'est pas activée par défaut et doit l'être en cochant la case **Enable Active Directory User Discovery**.