

Version en ligne

OFFERTE !

pendant 1 an

+ QUIZ 

2^e édition

Microsoft Endpoint Configuration Manager

Exploitation et Administration

*Préface de Jason GITHENS,
Principal Program Manager Lead,
Microsoft Endpoint Manager
Microsoft Corp*

 Informatique technique



**Jean-Sébastien
DUCHÊNE**

**Guillaume
CALBANO**




Collection

epsilon

Préface

Avant-propos

1. Introduction	15
2. À qui ce livre s'adresse-t-il ?	16
3. Niveau de connaissances requis	17
4. Comment ce livre est-il structuré ?	17
5. Systèmes nécessaires	19
6. Remerciements	20

Chapitre 1

Aperçu et fondamentaux de ConfigMgr

1. Introduction	21
2. L'histoire de Configuration Manager	22
3. ConfigMgr as a Service	35
4. Version Current Branch ou à support étendu ?	38
5. Les fonctionnalités et nouveautés de Configuration Manager	39
5.1 Les fonctionnalités	39
5.2 Les nouveautés	43
5.2.1 De nouvelles bases avec ConfigMgr 1511, 1602, 1606, et 1610	43
5.2.2 La cogestion des machines avec ConfigMgr 1702, 1706, et 1710	46
5.2.3 Plus de temps réels avec ConfigMgr 1802, 1806, et 1810	49
5.2.4 La communauté à l'écoute avec ConfigMgr 1902, 1906, et 1910	54
5.2.5 Plus de mobilité avec ConfigMgr 2002, et 2006	58
6. La terminologie et les concepts	62
6.1 Quelle différence entre un client et un périphérique ?	62
6.2 La notion de site	63
6.3 La hiérarchie de sites	63

6.4	Les sites Configuration Manager	64
6.5	Les systèmes de site	66
6.6	SMS Provider	71
6.7	Les ressources	72
6.8	Les limites et groupes de limites	73
6.9	Les découvertes	74
6.10	Les collections	74
6.11	Les requêtes	75
7.	Les modes de gestion	76
7.1	La gestion traditionnelle et son client	76
7.2	La gestion moderne	80
7.3	La cogestion (Co-Management)	81
8.	L'administration orientée utilisateur	83
9.	Les interfaces	85
9.1	La console d'administration	85
9.1.1	Description des vues	86
9.1.2	Panneau principal	102
9.1.3	Vue détaillée des objets	103
9.1.4	Barre de navigation	103
9.1.5	Ruban	104
9.1.6	Organisation des objets	105
9.2	Le centre d'administration Microsoft Endpoint Manager	108
10.	Fonctionnalités d'accessibilité	112
10.1	Raccourcis-clavier	112
10.2	Accessibilité sous Microsoft Windows	112
11.	Le support des langues	113
12.	Les licences	113
13.	Les communications	116
13.1	Les communications site à site	117
13.2	Les communications intrasites	120
13.3	Les communications serveurs vers les ressources externes	120
13.4	Les communications client à serveurs	122
13.5	Les communications de la console	123
14.	La gestion du contenu	124
15.	L'optimisation du téléchargement du contenu	130

- 16. Les notions de déploiement et déploiement graduel 134
- 17. Installation d'un site primaire autonome 135
 - 17.1 Les prérequis 136
 - 17.2 Installation du site 141
 - 17.3 Configurations basiques du site 153
 - 17.3.1 Les découvertes 153
 - 17.3.2 Les limites et groupes de limites de site 159
 - 17.4 Déploiement du client ConfigMgr 164
 - 17.5 Configuration basique de la cogestion avec Microsoft Intune 173
 - 17.5.1 Création d'un abonnement Microsoft Intune 174
 - 17.5.2 Ajout du nom de domaine public au service 174
 - 17.6 Gestion de la mobilité via la Cloud Management Gateway (CMG) . 187
 - 17.6.1 Concepts 188
 - 17.6.2 Les prérequis 191
 - 17.6.3 Implémenter la Cloud Management Gateway 192
 - 17.7 Utilisation du Hub Communautaire 205
- 18. Conclusion 208

Chapitre 2
Inventaires

- 1. Introduction 209
- 2. Inventaire matériel 210
 - 2.1 Concepts et composants 210
 - 2.1.1 Terminologie 212
 - 2.1.2 Paramétrage de l'agent d'inventaire 213
 - 2.1.3 Fichiers utilisés par l'inventaire 214
 - 2.1.4 Dossiers de réception Inboxes 215
 - 2.2 Extensions de l'inventaire 215
 - 2.3 Exploitation de l'inventaire 221
 - 2.3.1 Console d'administration MECM 221
 - 2.3.2 Centre d'administration Microsoft Endpoint Manager 221
 - 2.3.3 Base de données SQL 223
 - 2.3.4 Resource Explorer 224
 - 2.3.5 Affichage des rapports d'inventaire 225
 - 2.4 Destruction des données d'inventaire 225

2.5	Rapports d'inventaire	226
2.6	Dépannage	227
2.6.1	Côté client	227
2.6.2	Côté serveur	228
3.	Inventaire logiciel et collecte de fichiers	229
3.1	Concepts et composants	229
3.1.1	Fichiers d'inventaire logiciel	232
3.1.2	Dossiers Inboxes	232
3.2	Exploitation de l'inventaire logiciel	233
3.3	Rapports d'inventaire logiciel	234
3.4	Dépannage	234
3.4.1	Côté client	234
3.4.2	Côté serveur	236
4.	Asset Intelligence	237
4.1	Prérequis	237
4.2	Catalogue	238
4.2.1	Catégories	238
4.2.2	Familles	238
4.2.3	Légendes	239
4.2.4	Configuration matérielle	239
4.3	Synchronisation du catalogue	240
4.3.1	Installation de l'Asset Intelligence Synchronization Point	240
4.3.2	Mise à jour du catalogue	242
4.4	Exploitation de l'inventaire étendu	242
4.5	Tableau de bord du cycle de vie (Product Lifecycle Dashboard)	244
4.6	Rapports Asset Intelligence	245
4.6.1	Rapports matériel	245
4.6.2	Rapports logiciels	246
4.6.3	Rapports de licences	246
4.6.4	Rapports sur le cycle de vie	247
4.7	Dépannage de l'inventaire et problèmes communs	247
5.	Contrôle logiciel	249
5.1	Concept et composants du contrôle de logiciel	249
5.2	Prérequis pour le contrôle logiciel	250
5.3	Exploitation du contrôle logiciel	251
5.4	Rapports du contrôle logiciel	254

5.5 Dépannage du contrôle logiciel 254
6. Conclusion 255

Chapitre 3
Requêtes, collections, rapports et CMPivot

1. Introduction 257
2. Requêtes 258
2.1 Concept et composants 258
2.2 Création de requêtes 259
2.3 Actions sur les requêtes 266
3. Collections 267
3.1 Concept et composants 267
3.2 Collection utilisateur 272
3.3 Collection système 286
3.4 Fenêtres de maintenance 302
3.5 Protection contre les déploiements à risque 305
3.6 Gestion de l'énergie 307
3.7 Bonnes pratiques 312
4. Rapports 315
4.1 Concept et composants 315
4.2 Reporting Service Point 316
4.2.1 Prérequis 316
4.2.2 Installation du rôle 317
4.3 Data Warehouse Service Point 320
4.3.1 Prérequis 322
4.3.2 Installation du rôle 323
4.3.3 Dépannage du Data Warehouse Service Point 326
4.4 Exploitation des rapports 327
4.4.1 Utilisation de la console 327
4.4.2 Utilisation de l'interface web 330
4.5 Souscription à des rapports 332
4.6 Personnalisation des rapports 336
4.6.1 Modification de rapports existants 337
4.6.2 Création de nouveaux rapports 338
4.7 Bonnes pratiques 339

4.8	Dépannage	340
5.	Power BI	341
6.	CMPIivot	352
6.1	Concept et composants	352
6.2	Exécution des requêtes	356
6.3	Dépannage de CMPIivot	361
7.	Conclusion	366

Chapitre 4

Outils de contrôle distant

1.	Introduction	367
2.	La prise en main à distance	368
3.	Le réveil sur le réseau	375
3.1	Présentation	375
3.2	Configuration de Wake On LAN	377
3.3	Wake-up proxy	379
3.4	Wake-up via les notifications clients	382
3.5	Utilisation des fonctions de réveil	382
3.6	Rapports	384
3.7	Dépanner Wake On LAN	384
4.	Les actions distantes des périphériques	384
4.1	Blocage du périphérique	385
4.2	Actions de diagnostic	385
4.3	Actions clientes	387
5.	Les actions des périphériques cogérés	388
6.	Conclusion	389

Chapitre 5
Distribution d'applications

- 1. Introduction 391
- 2. Vue d'ensemble de la télédistribution applicative 392
 - 2.1 Les concepts et objets 392
 - 2.2 Cibler les utilisateurs ou les systèmes ? 393
- 3. Planification de l'infrastructure de distribution 396
 - 3.1 Les prérequis 396
 - 3.2 Le catalogue d'applications en libre-service 397
 - 3.3 Le déploiement d'applications modernes Windows 397
- 4. Aperçu du modèle hérité : le package 398
 - 4.1 Les concepts 398
 - 4.2 La création d'un package 399
- 5. Présentation du modèle : Application 409
 - 5.1 Les concepts 409
 - 5.2 La création d'une application 413
 - 5.3 La création de types de déploiement 416
 - 5.3.1 Windows Installer 417
 - 5.3.2 Script Installer 418
 - 5.3.3 Redirection de l'utilisateur sur le magasin éditeur 427
 - 5.3.4 Packages d'application Windows 428
 - 5.3.5 Application Virtualization 428
 - 5.3.6 Mac OS 433
 - 5.3.7 Web Application 435
 - 5.3.8 Séquences de tâches 437
 - 5.4 Les applications achetées en volume 439
 - 5.5 La gestion des types de déploiement 446
 - 5.6 La gestion des applications 447
 - 5.6.1 L'historique des révisions 447
 - 5.6.2 Copier/importer/exporter une application 448
 - 5.6.3 Remplacer l'application 448
 - 5.6.4 Les groupes d'applications 450
 - 5.6.5 Retirer et supprimer une application 451
 - 5.6.6 Afficher les relations 452
 - 5.7 Les environnements virtuels App-V 452
 - 5.8 Les conditions et expressions globales 454

5.9	La gestion et le déploiement de Microsoft 365 Apps	460
5.9.1	Concepts (Office-as-a-Service)	461
5.9.2	Évaluer et suivre le déploiement	462
5.9.3	Déployer Microsoft 365 Apps et Office 2019	467
5.10	La gestion et le déploiement de Microsoft Edge	470
6.	Déploiement de vos applications	472
6.1	Maintenir le contenu sur les points de distribution	472
6.1.1	Distribution du contenu	473
6.1.2	Mise à jour du contenu	474
6.1.3	Retirer du contenu	474
6.2	Déployer les packages ou les applications	474
6.3	L'expérience utilisateur	479
6.4	Les demandes d'applications	482
6.5	Installer une application en temps réel	484
6.6	Suivre le déploiement	485
7.	Dépanner	486
8.	Conclusion	487

Chapitre 6

Sécurité des ressources

1.	Introduction	489
2.	La gestion des mises à jour logicielles	490
2.1	Concepts et composants	490
2.1.1	Les composants et terminologies	490
2.1.2	La gestion selon Microsoft	494
2.1.3	Le processus de mise à jour via ConfigMgr	498
2.1.4	Planifier sa stratégie de déploiement	500
2.1.5	Windows Update for Business	503
2.2	Préparation de l'infrastructure	507
2.2.1	Prérequis	507
2.2.2	Installation du rôle Software Update Point	511
2.2.3	Configuration de l'infrastructure de déploiement	518
2.3	Déploiement manuel des mises à jour	524
2.3.1	Mise en œuvre de votre stratégie de déploiement manuelle	524
2.3.2	Retirer une mise à jour de vos déploiements	532

- 2.4 Déploiement automatique des mises à jour 533
- 2.5 Déploiement de mises à jour tierces 539
 - 2.5.1 Utilisation de la fonctionnalité intégrée des mises à jour tierces 539
 - 2.5.2 Utilisation de System Center Updates Publisher 545
 - 2.5.3 Import d'un catalogue de mises à jour tiers 549
 - 2.5.4 Création de mises à jour 551
 - 2.5.5 Publication de mises à jour 554
- 2.6 Gérer les mises à jour du client Microsoft 365 Apps 556
 - 2.6.1 Configuration des prérequis 556
- 2.7 Gérer les mises à jour de Microsoft Edge 560
- 2.8 Gérer les mises à jour des drivers Surface 561
- 2.9 Orchestrer les mises à jour 563
- 2.10 Suivre le déploiement des mises à jour logicielles 568
- 2.11 Les opérations de maintenance sur les mises à jour 569
 - 2.11.1 Suppression des mises à jour expirées 569
 - 2.11.2 Nettoyage de WSUS 570
- 2.12 Dépanner le déploiement des mises à jour logicielles 571
- 3. La protection contre les logiciels malveillants avec Endpoint Protection . 572
 - 3.1 L'histoire de la protection antivirus de Microsoft 573
 - 3.2 Les nouveautés apportées par Endpoint Protection 574
 - 3.3 Préparation de l'infrastructure 575
 - 3.3.1 Installation du rôle Endpoint Protection Point 575
 - 3.3.2 Paramétrage de l'agent du client 578
 - 3.3.3 Présentation du client Endpoint Protection 580
 - 3.4 Planifier les stratégies Endpoint Protection 581
 - 3.4.1 Les stratégies antimalware 581
 - 3.4.2 Les stratégies Firewall 588
 - 3.5 Assurer la mise à jour d'Endpoint Protection 589
 - 3.6 Suivre l'évolution de la protection 590
 - 3.6.1 Les tableaux de bord 590
 - 3.6.2 Les notifications 593
 - 3.6.3 Les rapports 595
 - 3.7 Exécuter des actions sur les clients Endpoint Protection 595
 - 3.8 Dépanner la protection anti-logiciels malveillants 596

4.	La protection contre les attaques et menaces avec Microsoft Defender . . .	596
4.1	Concepts	597
4.2	Microsoft Defender for Endpoint	601
4.2.1	Prérequis	604
4.2.2	Création d'une stratégie Microsoft Defender for Endpoint . . .	605
4.2.3	Suivi et supervision de Microsoft Defender for Endpoint. . . .	607
4.3	Microsoft Defender Exploit Guard	608
4.3.1	Prérequis	610
4.3.2	Création d'une stratégie Microsoft Defender Exploit Guard .	610
4.4	Microsoft Defender Application Guard.	617
4.4.1	Prérequis	617
4.4.2	Création d'une stratégie Microsoft Defender Application Guard	618
4.5	Microsoft Defender Application Control	621
4.5.1	Prérequis	623
4.5.2	Création d'une stratégie Microsoft Defender Application Control.	624
4.6	Dépannage de la protection avec Microsoft Defender	625
5.	La gestion du chiffrement BitLocker.	626
5.1	Concepts	626
5.2	Considérations pour la migration de MBAM ou Active Directory . .	631
5.3	Prérequis	632
5.4	Déploiement des portails BitLocker.	637
5.5	Création d'une stratégie BitLocker	639
5.6	Suivi, supervision et dépannage de BitLocker.	645
6.	La connaissance de l'état de santé avec Device Health Attestation	648
6.1	Concepts	648
6.2	Prérequis	649
6.3	Affichage de l'état de santé.	652
7.	Conclusion	653

Chapitre 7
Déploiement de système d'exploitation

- 1. Introduction 655
- 2. Vue d'ensemble 655
 - 2.1 Qu'est-ce que l'OSD ? 655
 - 2.2 Déploiement ou provisionnement ? 657
 - 2.3 Les scénarios de déploiement 659
 - 2.4 Migrer ou mettre à niveau ? 660
 - 2.5 Les challenges d'un déploiement/provisionnement et d'une migration/mise à niveau 662
 - 2.6 Les concepts et méthodologies. 666
 - 2.7 Les outils proposés par Microsoft 669
 - 2.8 Pourquoi utiliser MDT ? 671
 - 2.9 Le déploiement sur des sites distants 672
- 3. Les prérequis pour les scénarios de déploiement 673
 - 3.1 Vue d'ensemble 673
 - 3.2 Démarrage sur le réseau 675
 - 3.3 Déploiement par multidiffusion (multicast) 679
 - 3.4 Peer Cache 682
 - 3.4.1 Prérequis 682
 - 3.4.2 Provisionner le contenu sur la machine source 683
 - 3.4.3 Configurer la machine source 685
 - 3.4.4 Configuration de la séquence de tâches de déploiement. 686
 - 3.5 Évaluation de la compatibilité avec Desktop Analytics 688
 - 3.6 Migration de l'état utilisateur 688
 - 3.7 Utilisation de MDT 691
- 4. Gérer les pilotes 692
 - 4.1 Concepts et méthodes de gestion 692
 - 4.2 Ajout des pilotes dans le catalogue 695
 - 4.3 Création d'un package de pilotes 699
- 5. Administrer les images 699
 - 5.1 Les images de démarrage 699
 - 5.2 Les images d'installation. 703
 - 5.3 Construire une image de référence 703
 - 5.3.1 Capture manuelle 704
 - 5.3.2 Séquence de tâches Build and capture 705

5.4	Assurer le cycle de vie du master	708
5.5	Générer des médias	711
6.	Création d'une séquence de tâches	713
6.1	Les modèles ConfigMgr	713
6.2	Les modèles MDT	737
7.	Préparer la migration des données	741
8.	Déployer, mettre à niveau et migrer un système d'exploitation.	742
8.1	Traitement des scénarios	742
8.2	Déployer la séquence de tâches	743
8.3	Cibler les machines	747
8.3.1	Méthode 1 : déploiement sur une machine référencée	748
8.3.2	Méthode 2 : import des informations d'une machine inconnue	749
8.3.3	Méthode 3 : utilisation de la fonctionnalité de déploiement sur des machines inconnues	750
8.4	Gérer les associations d'ordinateurs.	752
8.4.1	Aperçu.	752
8.4.2	Créer une association entre deux machines existantes	753
8.5	Redéployer une machine	754
8.6	Suivre le déploiement	755
8.7	Dépanner le déploiement	757
9.	Propulser vos déploiements.	762
10.	Enregistrement et provisionnement.	763
11.	Gérer le cycle de vie de Windows 10.	767
11.1	Windows-as-a-Service.	767
11.2	Les différents scénarios de mise à niveau	770
11.3	Évaluer et planifier avec Desktop Analytics	772
11.3.1	Concepts.	772
11.3.2	Prérequis	779
11.3.3	Création initiale du tenant Desktop Analytics	781
11.3.4	Interconnecter Desktop Analytics avec Microsoft Endpoint Configuration Manager.	783
11.3.5	Utilisation du service.	787

- 11.4 Mettre à niveau via les plans de maintenance 798
 - 11.4.1 Prérequis 799
 - 11.4.2 Création des plans de maintenance 800
 - 11.4.3 Dépanner 806
- 11.5 Suivi des versions/builds sur le parc informatique 807
- 12. Conclusion 810

Chapitre 8
Paramètres, maintenance et conformité

- 1. Introduction 811
- 2. Concepts et composants 813
- 3. Prérequis 817
- 4. Configuration Items : fonctionnement 819
 - 4.1 Windows Desktops and Servers : Settings et Compliance Rules ... 820
 - 4.2 Paramétrages pour les périphériques traditionnels Windows 10. ... 829
 - 4.3 Éléments de configuration pour les périphériques modernes 837
 - 4.4 Éléments de configuration
 pour les périphériques traditionnels Mac OS X 845
 - 4.5 User data and profiles et Configuration Items 848
 - 4.6 OneDrive for Business profiles 855
 - 4.7 Stratégie de mise à niveau de l'édition Windows 10 856
 - 4.8 Microsoft Edge Browser Profiles 858
 - 4.9 Gestion des éléments de configuration 859
- 5. Baselines 861
 - 5.1 Création et déploiement d'une baseline 861
 - 5.2 Import d'une baseline 865
 - 5.3 Baselines et GPO 867
- 6. Best Practices 870
 - 6.1 Meilleures pratiques Microsoft 870
 - 6.2 Baselines de sécurité 872
- 7. Remédiation 873
 - 7.1 Manuelle 874
 - 7.2 Automatique 875

8.	Accès aux ressources de l'entreprise	878
8.1	Les profils de connexion à distance	877
8.2	Les profils de certificats	880
8.2.1	Prérequis	881
8.2.2	Déploiement d'un certificat d'autorité de certification racine	881
8.2.3	Provisionnement de certificats personnels par import PFX	883
8.2.4	Provisionnement de certificats personnels via Simple Certificate Enrollment Protocol	885
8.3	Les profils VPN	901
8.4	Les profils Wi-Fi	903
8.5	Les profils Windows Hello for Business	906
9.	Suivi et dépannage de la conformité et des configurations	907
9.1	Suivi des indicateurs	907
9.1.1	La console d'administration	907
9.1.2	Les rapports	909
9.1.3	Côté périphériques	909
9.2	Dépannage	912
10.	Exécution de scripts	915
10.1	Concepts et prérequis	915
10.2	Création, approbation et déploiement d'un script	916
10.3	Suivi du déploiement	920
10.4	Dépannage de l'exécution des scripts	921
11.	Conclusion	922
	Conclusion	925
	Index	927



Chapitre 4

Outils de contrôle distant

1. Introduction

Le quotidien des administrateurs de postes de travail n'est pas sans contraintes, traduites par les difficultés d'administrer les machines à distance. Parfois, l'utilisateur fait appel aux opérateurs pour un problème ou une assistance. Le siècle précédent, l'opérateur aurait planifié un déplacement pour venir en aide à l'utilisateur. Aujourd'hui, les administrateurs souhaitent gérer de manière centralisée les ressources. Microsoft Endpoint Configuration Manager propose des outils de contrôle distants construits pour prendre la main sur la machine de l'utilisateur. On retrouve différents outils, dont certains (Remote Control et Remote Assistance) permettent d'obtenir la vision sur la session de l'utilisateur afin de dépanner un éventuel problème. D'autre part, l'administrateur doit opérer des changements sur les machines alors que l'utilisateur reste le principal maître de son outil. Il devient ainsi difficile d'installer des mises à jour logicielles, des applications ou des systèmes d'exploitation sans pour autant perturber et agacer l'utilisateur. Microsoft intègre le standard de réveil sur le réseau pour envoyer un ordre de démarrage lors de déploiements. Ceci peut permettre la planification des déploiements en dehors des heures de travail afin de limiter le trouble généré. Enfin, avec l'émergence des périphériques mobiles, les utilisateurs font appel aux administrateurs en cas de perte ou de vol du périphérique. ConfigMgr offre ainsi des actions à distance pour ces périphériques cogérés. Ce chapitre s'attachera à détailler chacune des possibilités et les différentes considérations nécessaires à l'implémentation.

2. La prise en main à distance

La prise en main à distance permet à un administrateur ou à un opérateur d'assister un utilisateur à distance. Ces outils peuvent participer à la résolution d'un problème matériel ou logiciel sans nécessiter le déplacement d'un technicien. L'opérateur peut prendre le contrôle de n'importe quelle machine de la hiérarchie lorsque celle-ci dispose du client ConfigMgr. Microsoft Endpoint Configuration Manager permet l'utilisation de trois outils de prise en main à distance : Remote Control, Remote Assistance et Remote Desktop.

■ Remarque

Les fonctionnalités présentées dans cette partie ne s'adressent qu'aux périphériques traditionnels Windows équipés d'un client ConfigMgr.

Activation et configuration des outils

Afin de configurer les outils, vous devez créer ou modifier une stratégie de paramétrage client pour activer les différents outils et les configurer.

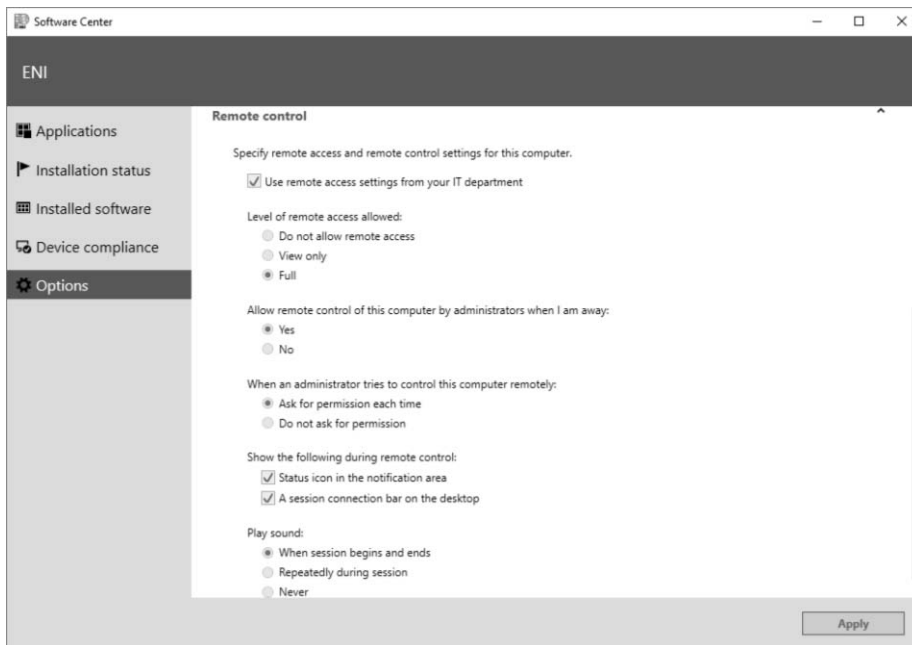
- ▶ Pour y accéder, ouvrez la console d'administration et naviguez dans **Administration - Overview - Client Settings**.
- ▶ Éditez une stratégie existante ou créez une nouvelle stratégie. Pour rappel, évitez de modifier la stratégie par défaut.
- ▶ Ajoutez ou éditez la section **Remote Tools** pour modifier les paramètres suivants :
 - **Remote Control** : un paramétrage permet la prise de contrôle d'une machine sur laquelle aucune session utilisateur n'a été ouverte. L'autorisation de l'utilisateur peut être demandée pour permettre la prise de contrôle. Vous pouvez y configurer les différents types de notifications visuelles (icône de notification) ou sonores. Vous pouvez choisir qui peut initier une connexion soit en autorisant les administrateurs locaux, soit en rajoutant les utilisateurs, soit en spécifiant des groupes autorisés. Ces derniers sont ensuite ajoutés au groupe local **ConfigMgr Remote Control Users**.
 - **Remote Assistance** : les paramètres permettent l'activation de l'ouverture d'une assistance à distance, sollicitée ou non, et le niveau d'accès.
 - **Remote Desktop** : vous pouvez gérer les paramétrages du bureau à distance en autorisant l'ouverture d'un bureau à distance et en configurant le niveau de sécurisation requis pour ouvrir la session.

Nom du paramètre	Description
Enable Remote Control on clients	Ce paramètre active les outils de contrôle distant sur les clients. Par défaut : désactivé.
Users can change policy or notification settings in Software Center	Cette option permet de laisser l'utilisateur changer les stratégies et paramètres de notification des outils de contrôle distant dans le Software Center. Par défaut : désactivé.
Allow Remote Control of an unattended computer	Cette option, sélectionnée, permet à l'administrateur d'utiliser le contrôle distant pour accéder à l'ordinateur verrouillé ou déconnecté. Par défaut : activé.
Prompt user for Remote Control permission	Affiche un message à l'utilisateur demandant son autorisation pour prendre le contrôle de la machine. Par défaut : activé.
Prompt user for permission to transfer content from shared clipboard	Affiche un message à l'utilisateur demandant son autorisation pour le partage du presse-papiers. Par défaut : désactivé.
Grant Remote Control permission to local Administrators group	Donne les droits de contrôle distant aux utilisateurs qui sont dans le groupe Administrateurs local. Par défaut : activé.
Access level allowed	Spécifie le niveau d'accès autorisé parmi : <ul style="list-style-type: none">- aucun accès ;- visionnage seulement ;- contrôle total (option par défaut).
Permitted viewers of Remote Control and Remote Assistance	Cette option permet à l'administrateur de spécifier des observateurs autorisés pour le contrôle distant et l'assistance à distance. Par défaut : aucun.
Show session notification icon on taskbar	Affiche une icône de notification dans la barre de tâches visant à informer qu'une session est active. Par défaut : activé.
Show session connection bar	Cette option affiche une barre de connexion hautement visible sur l'ordinateur client, qui indique qu'une session est active. Par défaut : activé.

Nom du paramètre	Description
Play a sound on client	Ce paramètre permet d'utiliser des sons qui indiquent quand une session de contrôle distant est active. Vous pouvez choisir parmi : – aucun son ; – à l'ouverture et fermeture de session (par défaut) ; – répétitivement durant la session.
Manage unsolicited Remote Assistance settings	Cette option permet à ConfigMgr de gérer les sessions d'assistance à distance non sollicitées. Les sessions non sollicitées sont des sessions qui sont initiées sans que l'utilisateur ait demandé une assistance. Par défaut : désactivé.
Manage solicited Remote Assistance settings	Cette option permet à ConfigMgr de gérer les sessions d'assistance à distance sollicitées. Les sessions sollicitées sont des sessions qui sont initiées lorsque l'utilisateur a demandé une assistance. Par défaut : désactivé.
Level of access for Remote Assistance	Donne le niveau d'accès pour l'assistance à distance parmi : – aucun accès (par défaut) ; – visionnage à distance seulement ; – contrôle total.
Manage Remote Desktop Settings	Cette option permet à ConfigMgr de gérer les paramètres bureau à distance (Remote Desktop). Note : les paramètres peuvent entrer en conflit avec ceux des stratégies de groupe si vous en utilisez au sein de l'entreprise. Par défaut : désactivé.
Allow permitted viewers to connect by using Remote Desktop Connection	Cette option permet aux observateurs autorisés de se connecter en utilisant une connexion Bureau à distance. Par défaut : désactivé.

Nom du paramètre	Description
Require network level authentication on computers that run Windows Vista operating system and later versions	Cette option requiert l'authentification au niveau du réseau (NLA) pour les connexions des services Bureau à distance sur les clients Windows Vista ou plus. L'ordinateur distant utilise un nombre limité de ressources avant l'authentification de l'utilisateur, au lieu de démarrer une connexion Bureau à distance complète, comme dans les versions précédentes. Cette option permet d'augmenter la sécurité de la machine. Par défaut : activé.

L'option permettant de laisser ou non l'utilisateur modifier les paramètres de prise de contrôle à distance via le menu **Options** du **Software Center** (centre logiciel) se matérialise par l'espace suivant :



Remote Control

Le contrôle à distance est l'outil intégré de ConfigMgr permettant aux opérateurs de prendre la main, avec ou sans approbation, sur la machine de l'utilisateur. L'accès à la machine n'est pas contraint par la jonction au domaine ; il est donc possible de prendre la main sur des ordinateurs en mode groupe de travail. Le contrôle à distance utilise le protocole construit pour le service Windows Live Mesh (TCP 2701) afin de permettre une optimisation du flux pour les réseaux lents. Il se décline sous la forme d'un service appelé *Configuration Manager Remote Control*.

Il offre les fonctions permettant d'envoyer un ordre [Ctrl][Alt][Suppr] ou de bloquer le clavier et la souris de l'utilisateur. L'outil intègre aussi un mécanisme de protection lors de la déconnexion réseau en verrouillant la machine que l'administrateur avait déverrouillée. On retrouve aussi la capacité de partager des fichiers entre l'ordinateur de l'opérateur et celui de l'utilisateur via un presse-papiers partagé.

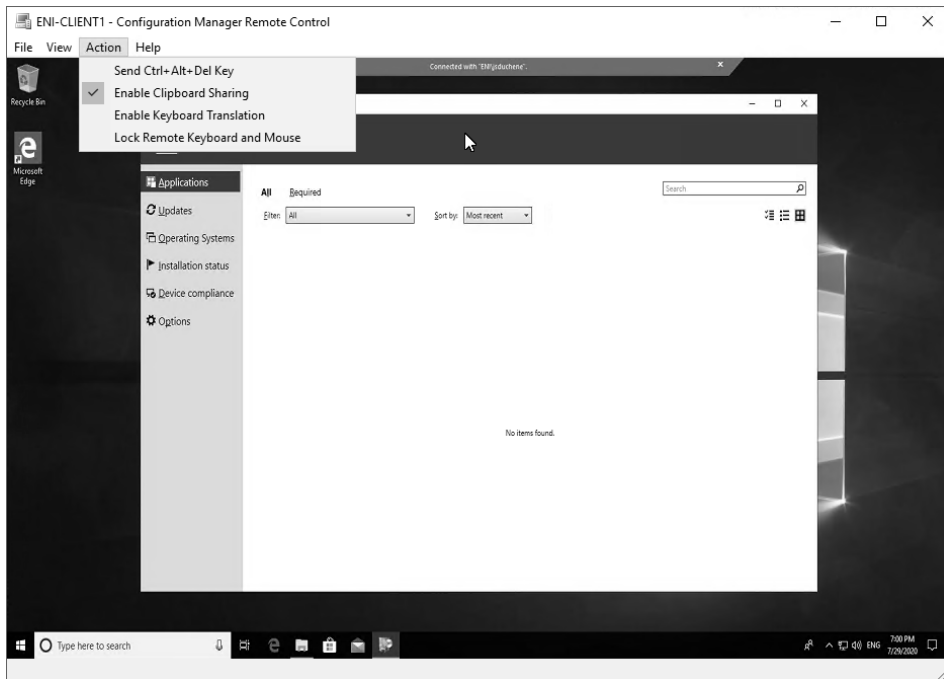
Il existe différents moyens d'utiliser cet outil de contrôle à distance. L'outil est exécutable à partir de la console d'administration. Pour cela, naviguez dans **Assets and Compliance - Overview - Devices** ou **Device Collections**. Sélectionnez la machine puis lancez la fonction **Start - Remote Control**. L'outil se lance en ouvrant la session sur la machine cible. Vous pouvez aussi utiliser l'outil indépendamment, via le menu **Démarrer**, en cliquant sur **Remote Control Viewer**. Vous devrez alors entrer le nom de la machine ou son adresse IP ainsi que le serveur de site utilisé pour envoyer les messages d'état.

■ Remarque

L'outil est aussi exécutable en ligne de commande : `CmRcViewer.exe <Machine> \\<serveur de site>`. Il est localisé dans <le répertoire d'installation ConfigMgr> `AdminConsole\Bin\x64`.

Seuls les opérateurs habilités peuvent prendre le contrôle d'une machine ; ils peuvent être déclarés via les stratégies ou définis comme administrateur local. En fonction des paramètres de l'outil appliqués sur le client dont vous prenez la main, l'utilisateur sera notifié et devra donner son autorisation. Celle-ci est accordée au travers d'une fenêtre affichant le nom du compte prenant le contrôle de la machine.

L'outil propose ensuite, via le menu **View**, la possibilité de passer en plein écran, de mettre à l'échelle la fenêtre ou de désactiver la barre d'état. Le menu **Action** donne accès aux fonctions de verrouillage du clavier et de la souris, d'envoi de la combinaison [Ctrl][Alt][Suppr] ou de partage du presse-papiers.



Remarque

L'outil de contrôle distant enregistre ses activités dans un fichier de journalisation `CMRcViewer.log` stocké dans le répertoire `%temp%` de la machine où il est exécuté.

ConfigMgr assure l'audit des opérateurs qui utilisent le contrôle à distance via les messages d'état. Vous pouvez suivre l'usage via les rapports ou les requêtes de message d'état suivants :

- All Computers remote controlled by a specific user.
- All remote control information.
- Remote Control Activity Initiated at a specific site.
- Remote Control Activity Initiated by a specific user.
- Remote Control Activity Initiated from a specific system.
- Remote Control Activity Targeted at a specific system.