System Center 2012 R2 Configuration Manager (SCCM)

Concepts, Utilisation et Administration

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

informatique technique

Jean-Sébastien DUCHÊNE

Guillaume CALBANO

Collection EPSILON

eni Editions

Table des matières

Avant-propos

Chapitre 1
Aperçu et fondamentaux de ConfigMgr 2012

Chapitre 2
Concevoir et déployer ConfigMgr 2012

Chapitre 3
Planifier et gérer le client ConfigMgr

Chapitre 4
Inventaires

Chapitre 5
Requêtes, collections et rapports

Chapitre 6
La distribution d'applications

Chapitre 7
La sécurité des ressources clientes

Chapitre 8
Le déploiement de système d'exploitation

Chapitre 9
La gestion des périphériques mobiles

Chapitre 10
La gestion de la conformité

Chapitre 11
Les outils de contrôle distant

Chapitre 12
La migration d'environnements

Chapitre 13
Sécurisation de ConfigMgr 2012

Chapitre 14
Maintenir une infrastructure SCCM 2012

Chapitre 3
Planifier et gérer le client ConfigMgr

1. Introduction

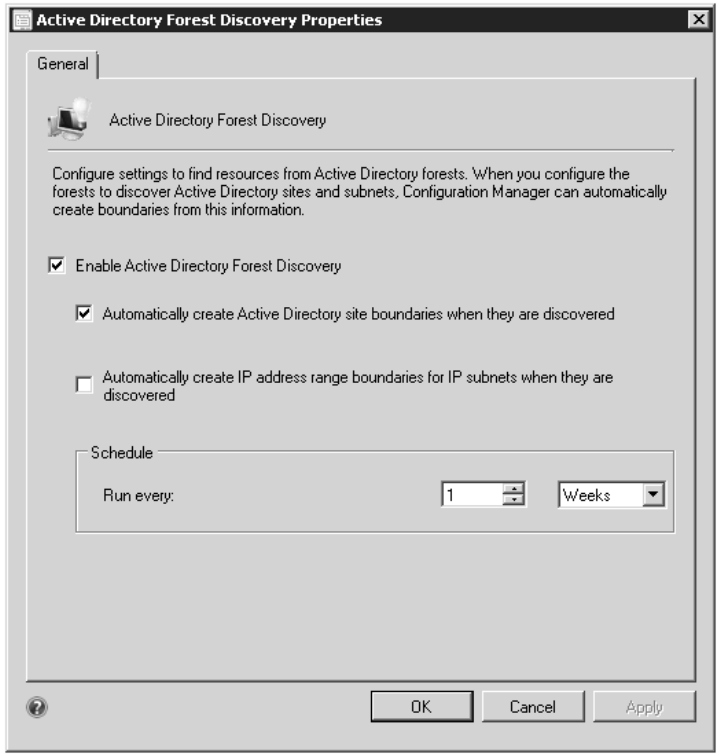
Nous avons vu précédemment comment planifier et déployer une infrastructure ConfigMgr. System Center 2012 Configuration Manager repose sur un mode client/serveur. Ce chapitre abordera les notions nécessaires à la planification, au déploiement et au maintien des clients SCCM. Nous verrons d'abord comment 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 paramétrages, nous détaillerons comment créer des stratégies et quels paramétrages 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.

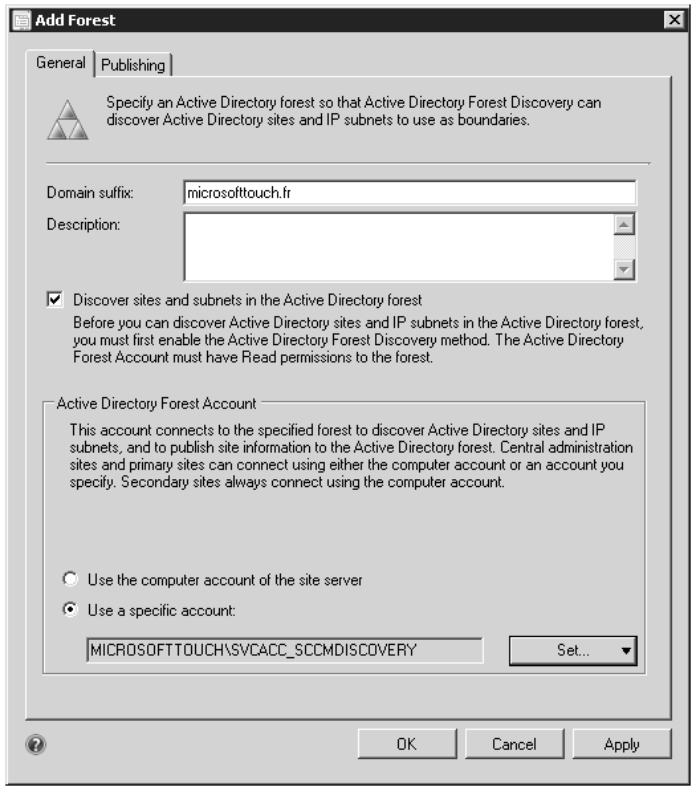


Remarque

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.

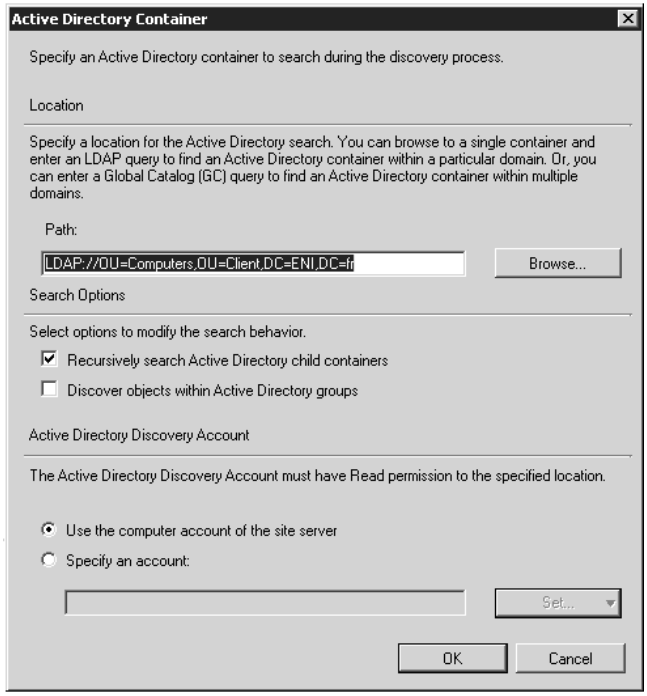
L'onglet **Publishing** permet de sélectionner les sites ConfigMgr que vous souhaitez publier dans la forêt que vous ajoutez. Pour cela, vous devez avoir procédé à l'extension de schéma Active Directory, à la création du conteneur System Management et le compte spécifié doit avoir le contrôle total dans 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**.