

SERVICE MANAGER : INTÉGRATION AVEC OPERATIONS MANAGER ET CONFIGURATION MANAGER

Ou comment connecter Service Manager avec votre infrastructure Active Directory et l'interfacer avec vos solutions de supervision et de gestion du cycle de vie des serveurs et postes de travail

>> Par Aurélien Bonnin et François Dufour

INTRODUCTION

System Center Service Manager 2010 (SCSM) est le dernier né de la suite Microsoft System Center (sans compter le récent rachat d'Opalis par Microsoft). La version RTM tant attendue a été officiellement annoncée fin Avril 2010 lors de l'événement Microsoft majeur autour des technologies System Center, le Microsoft Management Summit 2010 se tenant à Las Vegas.

SCSM vient ainsi compléter la suite Microsoft System Center en tant qu'outil de gestion des services informatiques intégrant les bonnes pratiques MOF et ITIL adaptées à vos besoins. SCSM permet la gestion des incidents et des problèmes, la gestion des changements, la gestion des risques et de la conformité...

>> SCSM VIENT AINSI COMPLÉTER LA SUITE MICROSOFT SYSTEM CENTER EN TANT QU'OUTIL DE GESTION DES SERVICES INFORMATIQUES INTÉGRANT LES BONNES PRATIQUES MOF ET ITIL ADAPTÉES À VOS BESOINS

Pour cela, SCSM s'intègre nativement avec Active Directory, Operations Manager ou encore Configuration Manager.

Cet article traite des différentes possibilités offertes par les trois principaux connecteurs proposés par défaut dans le produit :

- Active Directory,
- System Center Operations Manager,
- System Center Configuration Manager.

PRÉSENTATION DE L'ENVIRONNEMENT

System Center Service Manager 2010 supporte dans sa version RTM trois scénarii d'installation, les deux premiers étant uniquement destinés à des fins de maquettage/tests tandis que le 3ème représente la Best-Practice lorsqu'il s'agit d'implémenter SCSM dans votre environnement de production :

- 1er scénario : Installation de SCSM sur un ordinateur unique
 - Configuration minimale supportée

- Le Serveur de gestion SCSM est installé sur l'hôte physique Windows Server 2008
- Le Serveur Data Warehouse SCSM est installé lui dans une machine virtuelle Hyper-V hébergée sur le serveur de Gestion SCSM
- 2nd scénario : Installation de SCSM sur deux ordinateurs séparés
 - Séparation physique des rôles Serveur de gestion et Data Warehouse SCSM
 - Séparation des serveurs SQL et par la même occasion des bases de données Service Manager, et Data Warehouse
 - Performances supérieures au scénario 1
- 3ème scénario : Installation de SCSM sur quatre ordinateurs séparés
 - Performances adaptées à une utilisation de la solution en production
 - Séparation des rôles Serveur de gestion et Data Warehouse SCSM
 - Séparation des serveurs SQL et par la même occasion

des bases de données Service Manager, et Data Warehouse

- Séparation des rôles SCSM et des bases de données respectivement associées à ces rôles

Un environnement du type « 2nd Scénario » a été utilisé pour réaliser les opérations décrites dans la suite de cet article (Cf. figure 1).

INTÉGRATION AVEC ACTIVE DIRECTORY

Le premier connecteur à implémenter et de loin le plus simple, le connecteur AD. Ce connecteur va permettre de synchroniser les objets de votre domaine AD dans votre CMDB et plus précisément les comptes utilisateurs, les groupes, les imprimantes et les comptes machines.

Pour créer le connecteur AD, ouvrir la console SCSM en tant qu'administrateur, aller dans le panneau Administration, sélectionner Connectors, puis dans la liste de tâches à droite de l'écran sélectionner Create Connector puis

IT MEDIA - Service Abonnements - BP 40002 - 78104 Saint Germain en Laye cedex
Tél +33 1 39 04 25 00 - Fax +33 1 39 04 25 05 - E-mail : abonnement@itpro.fr

3 MAGAZINES D'INFORMATIQUE PROFESSIONNELLE AU SERVICE DE VOS COMPÉTENCES ET CELLES DE VOS ÉQUIPES



IT Pro Magazine

N° ISSN 1961 - 3814

1er mensuel dédié aux professionnels des environnements Windows Server, SQL Server, Visual studio et .NET

11 numéros par an : 95 € TTC

1ère publication technologique dédiée aux professionnels des environnements

Windows Server, SQL Server, Visual Studio et .NET, IT Pro Magazine est un support de formation, et d'information 100% technologique conçu pour accompagner vos compétences et répondre à vos préoccupations quotidiennes. Entourez-vous d'experts, bénéficiez de l'expérience des meilleurs experts Français et internationaux



EXCHANGE MAGAZINE

N° ISSN 1767 - 6436

L'expert des responsables de messageries d'entreprise

5 numéros par an : 95 € TTC

La publication de référence des responsables informatiques en charge de la gestion et l'optimisation des environnements de messageries

et des plateformes collaborative d'entreprise. Exchange Server Magazine est une publication à forte vocation technologique et stratégique présentant des dossiers exclusifs, signés des meilleurs experts, un véritable concentré d'expertise pour vous accompagner dans la mise en place, la gestion et l'optimisation des technologies associées à la messagerie et à la plateforme collaborative d'entreprise.



System iNEWS

N° ISSN 1955 - 0081

La référence absolue des environnements AS/400, iSeries et i5

11 numéros par an : 95 € TTC

Depuis plus de 15 ans, System iNEWS accompagne la communauté System i, support inégalé, compétence mondialement reconnue, System iNEWS est la 1ère source éditoriale d'information technologique dédiée à cette plate-forme. System

iNEWS est depuis 1993 « LA » source éditoriale incontournable de la communauté des professionnels des moyens systèmes IBM.

► iPro.fr

Le Club Abonnés sur iPro.fr !

Des services exclusifs, réservés aux abonnés des magazines !

Le Club Abonnés regroupe des services exclusivement réservés aux abonnés, c'est un service inclus dans votre abonnement et un complément indissociable des magazines. Les Clubs Abonnés sont disponibles dans une rubrique dédiée sur le site www.iPro.fr. Ils vous donnent accès à l'intégralité des archives des magazines, au format .PDF soit près de 1200 dossiers publiés depuis 2002 complétés de tous les scripts, codes et autres exécutable qui complètent chaque mois les dossiers publiés dans IT Pro Magazine, System iNEWS et Exchange Magazine.

>> www.iPro.fr <<

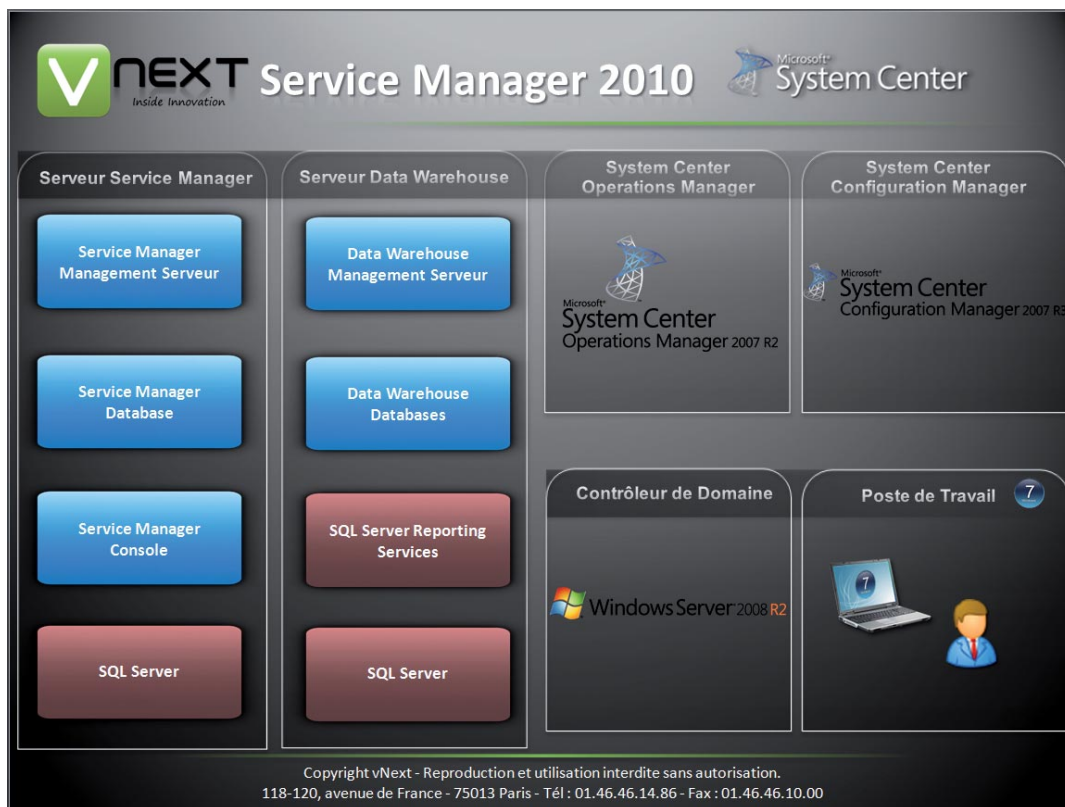


figure 1 – Description de l'environnement de test

Active Directory Connector (Cf. figure 2).

L'assistant vous proposera ensuite de nommer votre connecteur, de choisir le périmètre de synchronisation (l'ensemble du domaine ou juste une OU), de spécifier ensuite un compte d'action disposant des droits de lecture dans l'AD et finalement de choisir quels types d'objets importer. Une fois l'assistant terminé, il faut lancer une première synchronisation en cliquant sur Synchronise Now. Le temps de la synchronisation peut prendre plusieurs dizaines de minutes si votre cible comporte plusieurs milliers d'objets et cette opération pourra consommer jusqu'à 100% d'utilisation d'un des cœurs du CPU du Serveur de Gestion SCSM. Il est donc conseillé de lancer la synchronisation de l'AD durant les heures non-ouvrées et de disposer de CPU multi-cœurs afin de minimiser l'impact de la synchronisation.

Une fois la synchronisation de l'AD terminée, les objets sont visibles dans la console SCSM dans le panneau Configuration Items. On pourra par exemple retrouver nos comptes utilisateurs (Cf. figure 3)

Ces comptes pourront être ensuite exploités dans la console SCSM afin par exemple d'assigner un incident (Cf. figure 4)

INTÉGRATION AVEC SYSTEM CENTER OPERATIONS MANAGER

Nous allons voir ensemble comment exploiter les données recueillies par System Center Operations Manager (SCOM). Il existe en réalité non pas un mais deux connecteurs différents pour traiter les données SCOM. Le premier permet de synchroniser l'inventaire instancié dans la base SCOM au travers des différentes découvertes fournies dans les

**>> SYSTEM CENTER SERVICE MANAGER 2010
SUPPORTE DANS SA VERSION RTM TROIS SCÉNARIIS
D'INSTALLATION**

Management Packs et le second permet de transférer les alertes afin de générer automatiquement des incidents. Nous allons commencer par synchroniser l'inventaire SCOM.

Connecteur d'inventaire SCOM

La première étape consiste à importer un ensemble de Management Packs afin que SCSM dispose de la définition des classes d'objets découverts par SCOM. Pour cela, lancer

Powershell en tant qu'administrateur sur le Serveur de Gestion SCSCM et taper les commandes suivantes :

```
Get-ExecutionPolicy (noter le résultat)
Set-ExecutionPolicy Unrestricted
Set-Location \"Program Files\Microsoft System Center\Service Manager
2010\Operations Manager Management Packs"
.\installOMMPS.ps1
Set-ExecutionPolicy RemoteSigned (valeur notée lors de la première
commande)
Exit
```

Nous venons d'importer les Management Packs « par défaut » de SCOM. Si vous avez importé d'autres Management Packs dans votre environnement SCOM, il sera nécessaire de les importer également dans SCSCM afin d'étendre l'inventaire aux classes contenues dans ces derniers.

Nous allons ensuite créer le connecteur. Pour cela ouvrir la console SCSCM avec un compte administrateur, aller dans le panneau Administration, sélectionner Connectors puis dans la liste de tâches à droite de l'écran sélectionner Create Connector puis Operations Manager CI Connector. L'assistant de configuration du connecteur vous permet ensuite de définir le Root Management Server (RMS) SCOM auquel se connecter, de définir un compte d'action pour se connecter au RMS, de sélectionner les Management Pack à synchroniser et par conséquent les classes d'objets à synchroniser et finalement la fréquence de synchronisation (nul besoin d'une fréquence élevée, l'inventaire SCOM est peu variant).

Une fois le connecteur créé, une première synchronisation est initiée automatiquement. Les objets de base sont ensuite visibles dans le panneau Configuration Items (Cf. figure 5).

Nous allons maintenant ajouter les bases SQL détectées par SCOM dans notre CMDB. Pour cela, il faut :

- Importer le Management Pack SQL dans SCSCM
- Modifier notre connecteur afin de prendre en compte le Management Pack SQL
- Relancer une synchronisation

Une fois cette configuration faite, les nouveaux objets sont synchronisés dans la CMDB. Pour les afficher, nous devons créer une nouvelle vue dans ce dernier et afficher par exemple les objets de type SQL Database (Cf. figure 6).

Connecteur d'alerte SCOM

Nous allons maintenant tester le second type de connecteur SCOM, le connecteur d'alerte. De la même manière que pré-

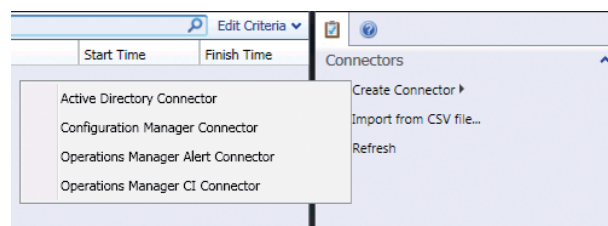


figure 2 – Sélection du connecteur

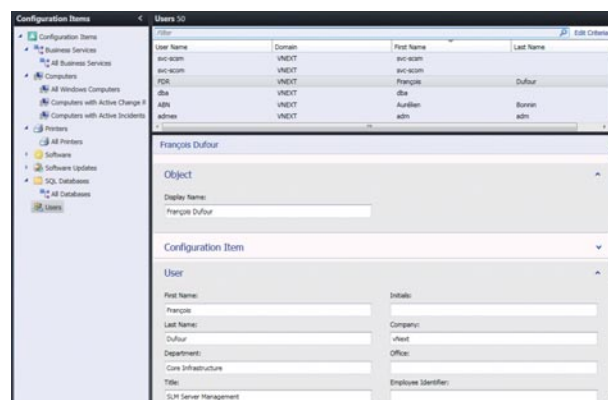


figure 3 – Comptes utilisateurs

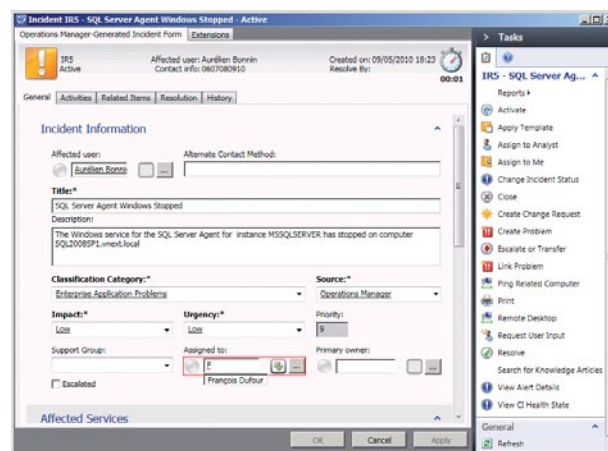


figure 4 – Assigner un Incident à un utilisateur

cedemment, créez un nouveau connecteur mais cette fois-ci sélectionnez Operations Manager Alert Connector. L'assistant nous permet de la même façon de choisir le RMS SCOM auquel se connecter et de sélectionner le compte d'action utilisé pour cette connexion. Nous avons également la possibilité de créer des règles afin de rediriger les alertes SCOM vers différents modèles d'incident SCSCM. Nous utiliserons le modèle d'incident par défaut pour les alertes SCOM. Finalement nous configurons notre connecteur afin que la synchronisation soit bidirectionnelle (Clôre l'alerte SCOM ferme l'incident SCSCM et vice-versa)

Une fois le connecteur créé dans la console SCSCM nous devons configurer SCOM. Pour cela, ouvrir la console SCOM

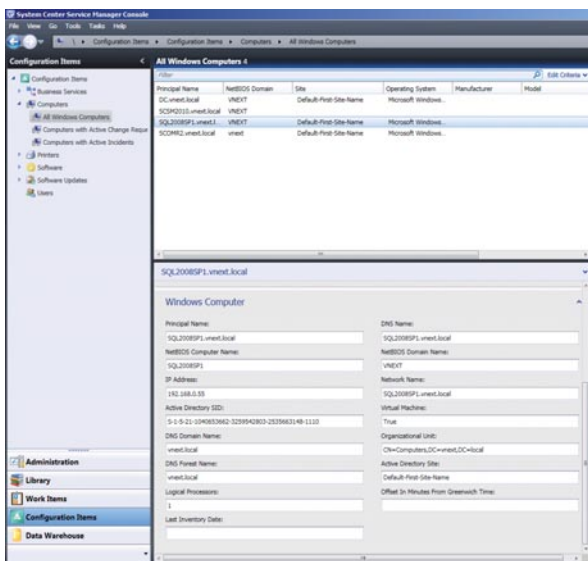


figure 5 – All Windows Computers

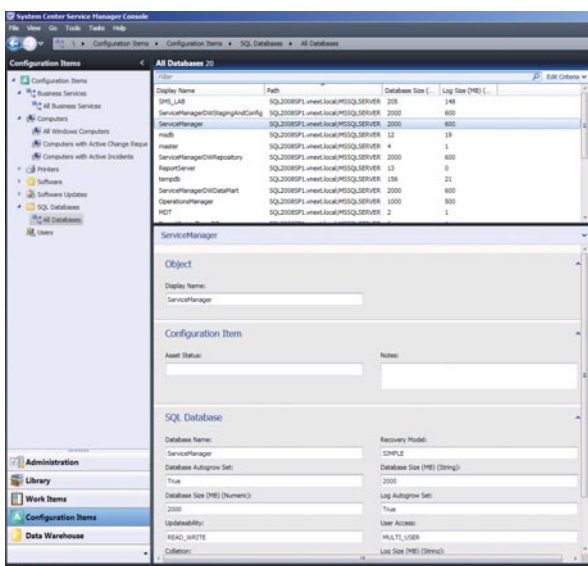


figure 6 – Nouvelle vue SQL Databases

avec un compte administrateur, aller dans le panneau Administration puis Product Connectors, Internal Connectors. Un nouveau connecteur doit être présent avec comme nom Alert Sync :<Nom du connecteur d'alerte SCSSM>. Faire un clic-droit et sélectionner Propriétés. Ici nous allons configurer un abonnement à l'identique des abonnements de notifications SCOM. Il est ainsi possible de filtrer les alertes transférées à SCSSM. Dans notre exemple, nous n'enverrons que les alertes critiques concernant SQL Server.

Afin de tester le connecteur d'alerte, nous allons arrêter l'agent SQL sur un des serveurs SQL supervisés par SCOM. Une alerte est ainsi générée dans la console SCOM (Cf. figure 7).

Et un incident est automatiquement créé dans SCSSM (Cf. figure 8).

Remarque : Le connecteur d'alerte est à utiliser une fois votre environnement SCOM parfaitement configuré. Dans le cas contraire, un trop plein d'alertes submergerait le Helpdesk d'incidents non pertinents.

INTÉGRATION AVEC SYSTEM CENTER CONFIGURATION MANAGER

Nous allons maintenant aborder l'import des données recueillies par System Center Configuration Manager (SCCM) dans la solution Service Manager. L'import des données d'inventaire logiciel et matériel ainsi que la liste des applications packagées, des mises à jour de sécurité, des ordinateurs et utilisateurs découverts ou bien encore la liste des lignes de standards (DCM) définis au sein de ConfigMgr sont synchronisés dans Service Manager par le biais d'un connecteur Configuration Manager.

L'ajout des données de « gestion de configuration » définies dans ConfigMgr au sein de Service Manager permet de mettre en place des méthodes automatiques de remédiation aux dérives de configuration détectées dans ConfigMgr, passant par la création automatique d'incidents dans Service Manager, l'exécution de la méthode de remédiation puis la mise à jour de l'incident Service Manager associé.

Connecteur d'inventaire SCCM

La première étape de cette intégration Service Manager/ Configuration Manager passe par la création d'un connecteur Configuration Manager.

Pour cela, sur le serveur de gestion SCSSM, ouvrir la console SCSSM avec un compte administrateur, aller dans le panneau Administration, sélectionner Connectors puis dans la liste de tâches à droite de l'écran sélectionner Create Connector puis Configuration Manager Connector.

L'assistant de configuration du connecteur Configura-

>> LA PREMIÈRE ÉTAPE CONSISTE À IMPORTER UN ENSEMBLE DE MANAGEMENT PACKS AFIN QUE SCSSM DISPOSE DE LA DÉFINITION DES CLASSES D'OBJETS DÉCOUVERTS PAR SCOM

tion Manager vous permet tout d'abord d'attribuer un nom au connecteur, de spécifier le Management Pack associé au type de connecteur choisi (« System Center Configuration Manager Connector Configuration »), de spécifier le nom du serveur hébergeant la base de données ConfigMgr ainsi que le nom de cette base et de préciser un compte utilisateur

disposant des droits administratifs sur cette même base de données (Cf. figure 9).

Remarque: Il est fortement conseillé de spécifier le serveur de site central de votre infrastructure ConfigMgr comme serveur cible du connecteur afin de disposer de l'ensemble des données d'inventaire de votre infrastructure.

L'assistant vous permet ensuite de sélectionner les regroupements à synchroniser avec Service Manager et de paramétrer la fréquence de synchronisation des données ConfigMgr. Les données ConfigMgr étant sujettes à des modifications fréquentes il est nécessaire de configurer une synchronisation journalière afin de disposer de données pertinentes et à jour dans la base de données Service Manager. Il sera ensuite nécessaire soit d'attendre la prochaine occurrence de synchronisation du connecteur soit d'initier manuellement cette première synchronisation afin d'importer les données ConfigMgr dans Service Manager.

Remarque: Si vous disposez d'un inventaire matériel ConfigMgr personnalisé par extensions d'inventaire et donc d'un fichier SMS_DEF.MOF personnalisé, il sera nécessaire

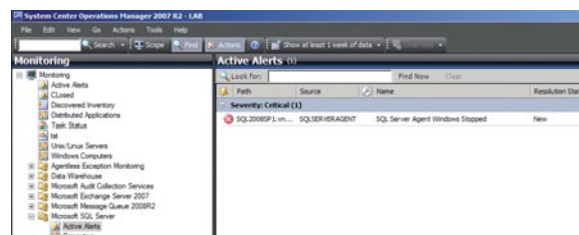


figure 7 – Alerte SCOM SQL

de créer un second connecteur Configuration Manager permettant de remonter les informations d'inventaire étendu dans Service Manager.

Une fois le processus de synchronisation achevé, on peut vérifier que les objets ConfigMgr ont bien été importés dans la CMDB Service Manager en tant que Configuration Items. Par exemple, les correctifs de sécurité synchronisés depuis le serveur ConfigMgr (Cf. figure 10).

Portail Libre-Service

La mise en place de l'intégration Service Manager/Conf-

DEMI HORIZ - 175x135

Client : AUTOPUB EXCHANGE

repassé : ITPRO MAG N°MAI

page 31

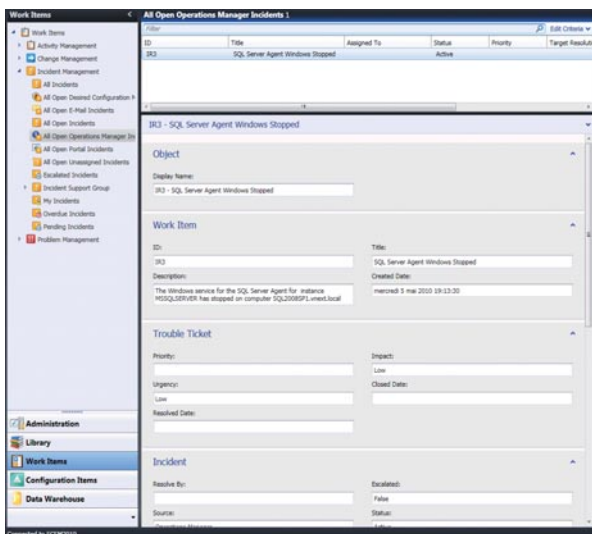


figure 8 – Incident SCSM SQL

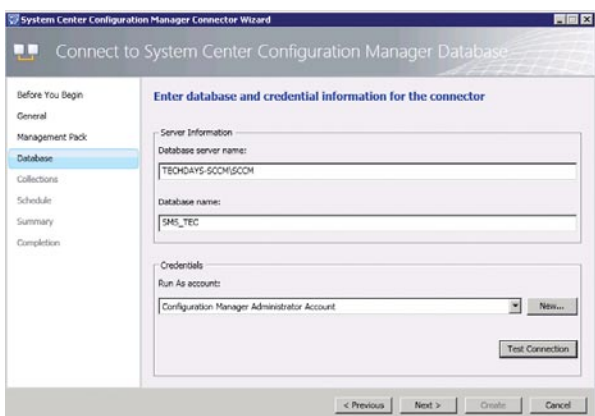


figure 9 – Configuration Connecteur Configuration Manager

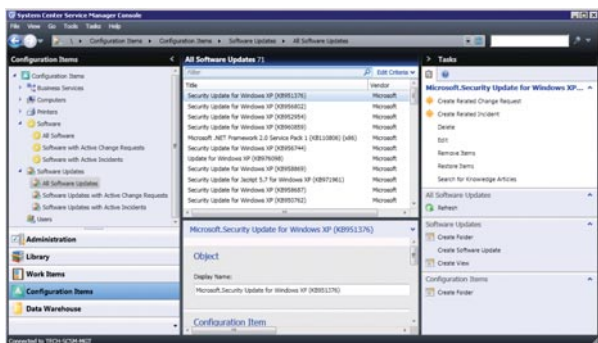


figure 10 – ConfigMgr Software Updates Packages

figuration Manager apporte également son lot de nouvelles fonctionnalités pour les utilisateurs finaux : la plus importante d'entre elles étant le portail libre-service permettant aux utilisateurs finaux d'effectuer des demandes de changements (modification du mot de passe utilisateur, ...), des demandes d'assistance ou bien encore de consulter les com-

munications de leur entreprise, l'état d'avancement de leurs demandes, etc. La fonctionnalité la plus attendue de ce portail libre-service est bien évidemment l'accès à la bibliothèque applicative de l'entreprise directement depuis cette interface Web, avec la possibilité de demander l'installation d'une application, installation pouvant être soumise ou non à une approbation de la direction de l'entreprise.

Une fois le portail Libre-Service déployé sur IIS ou SharePoint et configuré, une fois le paramétrage général du portail Libre-Service effectué, quelques prérequis doivent être satisfaits avant la mise en place de cette fonctionnalité. Il est ainsi nécessaire de :

- Accorder les droits nécessaires sur l'infrastructure Configuration Manager aux comptes de service Service Manager : ces comptes doivent disposer entre autres des droits de lecture du site SCCM, de gestion des collections ou encore des Configuration Items de DCM.
- Configurer un ou plusieurs modèles de demande de changement afin de définir pour chacune de ces demandes de changement si une approbation est nécessaire et si oui par qui celle-ci doit être effectuée.
- Créer un ou plusieurs Software Deployment Process dans Service Manager et leur associer un modèle de demande de changement
- Publier les applications Configuration Manager synchronisées dans le Portail Libre-Service

La dernière étape consiste à déployer l'Active-X nécessaire à tout utilisateur pour interagir avec le Portail Libre-Service. L'infrastructure Configuration Manager étant déjà présente, la méthode la plus simple pour déployer ce package MSI est bien entendu d'utiliser les fonctions de déploiement applicatif de ConfigMgr pour installer l'Active-X sur l'ensemble des postes de votre parc. Le package Portal Client.MSI se trouvant dans le répertoire \Setup des sources d'installation de Service Manager.

L'utilisateur final en se connectant depuis sa machine sur le Portail Libre-Service Service Manager <https://scsm-webportal/enduser> peut visionner les différentes communications de l'entreprise, mais surtout accéder à la bibliothèque applicative de son entreprise depuis la section Request Software, sélectionner le logiciel qui l'intéresse, obtenir des informations sur ce même logiciel concernant sa méthode d'approbation ou sa version, justifier de la nécessité de disposer de ce logiciel sur son ordinateur et soumettre sa demande de changement (Cf. figure 11).

En arrière-plan, SCSM reçoit une demande de changement, visible au niveau de la section Work Items\Change

Management\All Change Requests. Cette demande de changement est ensuite traduite en Activité visible dans la section Work Items\Activity Management\Review Activities\All Activities puis soumise au Workflow de validation entraînant la notification de l'approbateur puis une fois la demande approuvée, la création automatique d'un regroupement contenant l'ordinateur de l'utilisateur final et la publication du logiciel souhaité sur ce même regroupement (Cf. figure 12).

SCÉNARIO D'UTILISATION DE L'INTÉGRATION SERVICE MANAGER AVEC SYSTEM CENTER CONFIGURATION MANAGER ET SYSTEM CENTER OPERATIONS MANAGER

Vous l'aurez certainement compris au travers de ces quelques exemples d'utilisation de Service Manager, qu'une fois ce dernier configuré pour une complète intégration avec Configuration Manager et Operations Manager, de nombreux scénarii d'utilisation de la solution sont alors possibles.

On peut par exemple penser à un administrateur système se connectant sur un serveur de votre infrastructure et désinstallant/désactivant l'antivirus afin d'installer une nouvelle application sur ce serveur et oubliant tout simplement de le réinstaller/réactiver avant de se déconnecter du serveur et vaquer à d'autres occupations.

Operations Manager ayant été configuré pour surveiller le service antivirus remonterait alors une alerte sur l'état de santé de ce même service, générant automatiquement un incident dans Service Manager et dans le cas de la désinstallation de l'antivirus déclencherait alors le déploiement de l'antivirus au travers de Configuration Manager ou l'activation du service Antivirus au travers d'un script exécuté par Operations Manager.

RESSOURCES AUTOUR DE SERVICE MANAGER

- Technet Library: <http://technet.microsoft.com/en-us/library/ff461010.aspx>
- Offline Documentation: <http://technet.microsoft.com/en-us/library/ff521367.aspx>
- Blog de l'équipe Corp. Microsoft Service Manager :

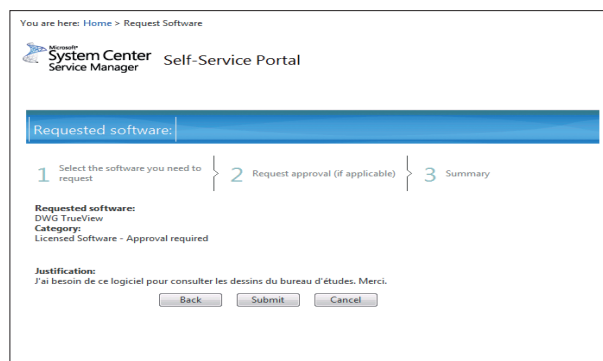


figure 11 – Soumettre une demande d'installation d'une application

<http://blogs.technet.com/servicemanager>

- Livres Blanc et Téléchargements : <http://www.microsoft.com/france/serveur/system-center/service-manager.aspx>
- Communauté Française System Center : <http://www.systemcenter.fr>

Aurélien BONNIN



Responsable de l'offre Desktop LifeCycle Management chez vNext
MVP Configuration Manager

Email: Aurelien.Bonnin@vNext.fr

Blog: <http://myitforum.com/cs2/blogs/abonnin>

François DUFOR

Responsable de l'offre Server Management chez vNext

Spécialiste Operations Manager

Email : Francois.Dufour@vNext.fr

Blog : <http://myitforum.com/cs2/blogs/fdufour>

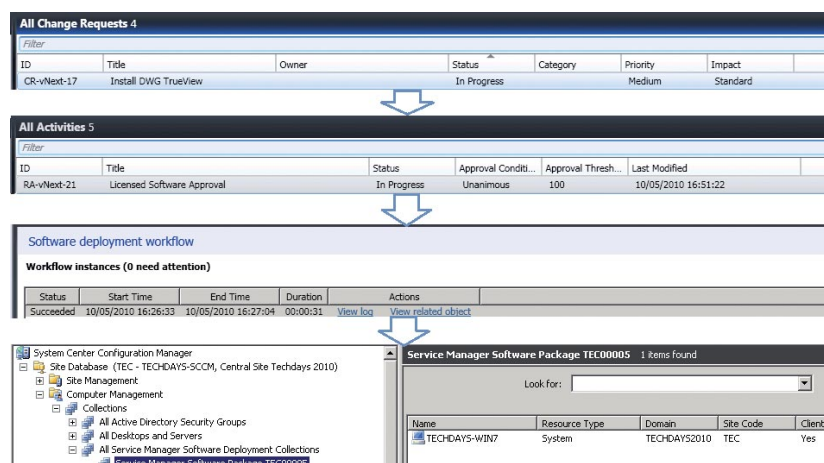


figure 12 – Workflow de demande de changement