

Gérer les postes de travail hors réseaux établissement avec Microsoft SCCM

Yves Daniou

DSI du rectorat de Grenoble
7 place Bir-Hakeim
38000 Grenoble

Julien Mercier

DSI du rectorat de Grenoble
7 place Bir-Hakeim
38000 Grenoble

Résumé

La DSI du rectorat de l'académie de Grenoble gère un parc de près de 2000 postes de travail Windows, environ un tiers de ces machines étant des portables utilisés principalement hors de nos réseaux internes. Avec la rénovation du service de Gestion de Parc (GDP) entamée en 2016, il est apparu nécessaire de se doter d'une solution unique et centralisée permettant de gérer le cycle de vie complet des postes de travail. Un des besoins forts était que le produit puisse réaliser les inventaires matériels et logiciels, le déploiement d'applications et la gestion des mises à jour du système quel que soit le réseau depuis lequel le poste est connecté. Il nous a donc fallu évaluer une solution qui permette nativement une connexion la plus sécurisée possible aux serveurs internes, tout en restant transparente pour l'utilisateur final et facilement administrable par nos équipes.

Microsoft System Center Configuration Manager (SCCM) a finalement été choisi puis intégré en 2018, étant le seul produit permettant une gestion quasi-complète des postes connectés sur Internet, à condition qu'ils possèdent chacun un certificat client x509 pour se connecter de manière sécurisée à l'infrastructure académique SCCM depuis l'extérieur.

Notre présentation s'attachera à décrire ces besoins ainsi que les raisons qui nous ont poussé à choisir SCCM, avant de présenter l'architecture sécurisée mise en place ainsi que les modalités de certification x509 automatique de l'ensemble du parc de postes de travail grâce à l'IGC de Microsoft, Active Directory Certificates Services (ADCS). Enfin, nous présenterons notre retour d'expérience sur les différents services SCCM fonctionnels hors réseau interne.

Mots-clefs

SCCM, postes de travail, gestion de parc informatique, inventaire, déploiement logiciel, PKI, IGC

1 Introduction

En 2018, la DSI du rectorat de l'académie de Grenoble m'a demandé d'étudier l'intégration d'un seul logiciel permettant de remplacer tous ceux déjà utilisés au rectorat pour la gestion du cycle de vie d'un poste de travail. J'ai donc consacré cinq mois à évaluer, maquetter et installer une solution permettant de gérer un poste de travail depuis l'inventaire, en passant par le déploiement du système d'exploitation et des logiciels, jusqu'à la gestion de ses mises à jour et ce quelque soit le réseau depuis lequel il serait connecté. J'ai travaillé sur la phase finale d'installation en collaboration avec Julien Mercier, de l'équipe de Gestion De Parc (GDP) du rectorat, qui est le responsable du groupe d'administrateurs chargé de l'exploitation du logiciel.

2 Le projet : contexte et besoins

2.1 Contexte et existant

La DSI du rectorat gère un parc de près de 2000 postes de travail répartis sur 43 sites géographiques distincts, installés en très grande majorité sous système d'exploitation Microsoft Windows. Sur ces 2000 postes, environ 600 sont des portables utilisés uniquement en mode nomade par des cadres ou conseillers et inspecteurs pédagogiques, médecins, donc très rarement connectés sur les réseaux internes de l'établissement.

Historiquement, ce parc était géré par six services informatiques distincts, avec autant d'outils et de procédures différents. En 2012, ces services ont fusionné en une DSI unique académique avec pilotage central. Le service de gestion de parc issu de cette réorganisation, composé d'une quinzaine d'informaticiens répartis sur 5 sites géographiques, a la charge de gérer l'ensemble du parc résultant. Le besoin d'harmonisation des infrastructures, outils et procédures qui a suivi a amené les équipes du service à faire des choix structurants : migration de l'ensemble des postes et des comptes utilisateurs vers un référentiel unique *Active Directory* (AD), mise en place d'*OCS Inventory* et GLPI (*Gestion Libre de Parc informatique*) ainsi que de MDT (*Microsoft Deployment Tool*) au niveau de l'ensemble des services académiques gérés par l'équipe.

2.2 Besoins

Il est apparu ensuite dans un second temps la nécessité de rationaliser cette suite d'outils cloisonnés pour se diriger vers un outil unique et centralisé, permettant de gérer le cycle de vie complet des postes de travail de la première installation du système exploitation jusqu'à la réforme de la machine. Une des contraintes fortes pesant sur le choix de l'outil était que les fonctions d'inventaire, de déploiement de logiciels et de gestion des mises à jour puissent également s'effectuer sur les postes nomades ne se connectant pas aux réseaux de l'établissement (un peu moins d'un tiers du parc total). La seconde était un budget relativement limité, qui n'aurait pas autorisé l'achat d'un progiciel coûteux.

2.3 Évaluation et choix de la solution

Ces besoins impératifs réduisaient nettement les choix d'outils possibles et induisaient de fortes exigences de sécurité. Profitant de l'opportunité d'un accord-cadre national avec l'éditeur Microsoft, le progiciel commercial *System Center Configuration Manager* (SCCM) a été évalué en priorité pour sa capacité à supporter la gestion hors réseaux locaux des postes de travail portables.

Les fonctionnalités suivantes ont été maquettées :

- inventaires matériel et logiciel ;
- déploiement du système d'exploitation et des pilotes (non accessible depuis l'extérieur du réseau interne) ;
- déploiement logiciel et catalogue d'applications ;
- gestion des mises à jour du système d'exploitation et des logiciels.

Il en a résulté que, mis à part le déploiement de systèmes d'exploitation, les autres fonctionnalités pouvaient effectivement être exposées sur Internet, moyennant l'obligation que chaque PC possède un certificat x509 de type TLS client pour s'authentifier auprès de l'infrastructure SCCM. Le produit correspondant par ailleurs aux besoins du service de gestion de parc, il a été décidé de l'intégrer en 2018 dans l'infrastructure académique, en prenant en compte en parallèle la problématique de certification des postes.

3 Mise en place de l'architecture sécurisée

Le « *challenge* » quand on parle de sécurité est parfois de concilier ces impératifs sécuritaires tout en ne faisant pas peser de contraintes démesurées sur les utilisateurs ou les administrateurs. De prime abord, il nous semblait difficilement concevable pour répondre au besoin exprimé par l'équipe de Gestion De Parc d'exposer directement sur Internet un serveur SCCM. Obstacle peut-être « culturel », et que l'on a surmonté, d'une part en évaluant le produit sur une période assez longue (un mois) et, d'autre part en cherchant une solution transparente pour tout le monde permettant de sécuriser plus fortement cette partie de l'architecture dédiée aux clients hors réseaux internes.

3.1 Pré-requis : accès à l'Active Directory pour les serveurs SCCM

Un premier problème de sécurité s'est posé avec l'adhérence de la solution à l'annuaire Active Directory. Avant de pouvoir faire des déploiements de logiciels ciblant des utilisateurs, pas seulement des machines, il fallait que le serveur SCCM de DMZ ait un accès à un des contrôleurs du domaine, tous situés dans nos zones internes. Nous avons décidé, plutôt que d'ouvrir un accès direct entre le serveur SCCM de DMZ et un contrôleur, de configurer en DMZ un contrôleur de domaine en lecture seule (*Read-Only Domain Controller*, RODC). Cette solution permet d'empêcher (ou de limiter) la répllication des mots de passe de l'annuaire AD présents sur les contrôleurs de domaine internes vers le RODC, tout en y répliquant tous les autres attributs. Cela nous est apparu une solution intéressante pour limiter les risques en cas de compromission du serveur AD situé en DMZ, les authentifications des utilisateurs étant transmises via le RODC à un contrôleur interne possédant les mots de passe. De plus, on évite ainsi un accès direct trop large du serveur SCCM de DMZ à des serveurs internes. Une autre solution plus complexe, documentée par Microsoft, aurait pu consister à monter une nouvelle forêt en DMZ avec des approbations avec notre forêt principale : elle a été jugée trop lourde dans notre contexte.

Au final, nous avons identifié et autorisé ces flux réseau minimaux depuis le RODC vers le domaine (DC) :

Protocole	Service	Port	Remarque
LDAP	TCP + UDP	389	
Kerberos	TCP + UDP	88	
RPC	TCP + UDP	135	Nécessite un « <i>helper RPC</i> » sur le pare-feu
Microsoft DS	TCP + UDP	445	
NTP	UDP	123	Uniquement vers le contrôleur « Émulateur PDC »
Global Catalog	TCP	3268	

Depuis le domaine vers le RODC, nous avons ouvert uniquement un flux *Remote Procedure Call* (RPC), notre pare-feu se chargeant, grâce à un module nommé « *helper RPC* », d'ouvrir dynamiquement les bonnes plages de ports, à partir de la requête contenue dans les paquets RPC émis à destination du port 135.

3.2 Mise en place d'une Infrastructure de Gestion de Certificats académique

Ensuite, afin d'adresser la problématique de la certification massive des 600 clients portables du parc, le responsable du service de gestion du parc a pointé la lourdeur de l'opération dans le cas éventuel de l'utilisation des services de Terena ou bien de la Plateforme Nationale de Confiance Numérique de l'Éducation nationale (PNCN), dont nous avons consulté les responsables. En effet, aussi bien avec Terena qu'avec la PNCN, toutes les opérations de ce processus de certification sont difficilement automatisables simplement et de bout en bout (génération de la paire de clés, soumission de la requête puis intégration du certificat dans la machine, sans compter la gestion du renouvellement, la durée d'exploitation des PC étant généralement supérieure à la durée de validité d'un certificat x509). L'ensemble des utilisateurs et des ordinateurs du périmètre étant géré dans un domaine Active Directory unique, il a donc été choisi de déployer, après maquettage, la fonctionnalité d'Infrastructure de Gestion de Certificats (IGC ou PKI) *Active Directory Certificates Services* (ADCS).

Au vu du succès des premiers résultats, le Responsable de la Sécurité des Systèmes d'Information (RSSI) de l'académie a souhaité que l'ensemble du parc de postes fixes et portables soit certifié, permettant un haut niveau de sécurité y compris en interne. Dans l'optique que ce prérequis à SCCM ne soit pas exclusivement dédié à ce logiciel, nous avons voulu construire une IGC académique suivant au plus près les bonnes pratiques de l'éditeur. Après de nombreux échanges avec mon collègue en charge de la sécurité du réseau Racine¹, et également RSSI adjoint de l'académie, nous avons proposé une architecture à quatre tiers.

1. Réseau Privé Virtuel (RPV) national qui interconnecte à l'intérieur d'une académie tous les sites administratifs puis à l'échelle nationale interconnecte toutes les académies et les centres d'hébergement entre eux.

Ce service ADCS, complètement intégré à la gestion du domaine AD, a été déployé sous forme d'architecture trois tiers (autorité racine hors-ligne, autorité de délivrance jointe au domaine AD, serveur de publication des listes de révocation) plus un tiers externe supplémentaire, un mandataire inverse *web* :

1. une autorité de certification racine autonome, non jointe au domaine Active Directory, dont l'unique rôle est de signer le certificat de l'autorité émettrice. Selon les bonnes pratiques, ce serveur virtuel est configuré sans carte réseau et éteint après l'opération de signature du certificat de l'AC émettrice. Il doit être rallumé une fois par an, un peu avant l'expiration de la liste de révocation du certificat qu'il a délivré, en l'occurrence celui de l'autorité intermédiaire du point 3 chargée elle de délivrer les certificats aux clients finaux. L'opération de publication consiste à récupérer la CRL sur le serveur afin de la publier manuellement sur le serveur *web* du point 3 ci-après ;
2. une autorité de certification intermédiaire dite d'entreprise, jointe au domaine, chargée de l'émission des certificats finaux à partir du modèle configuré. Étant membre du domaine AD et allumée en permanence, cette AC peut publier automatiquement sa liste de révocation sur le serveur web dédié ;
3. un serveur Microsoft de publication web des certificats des autorités racine et intermédiaire (AIA), ainsi que de leurs listes de révocation (CRL). Nous avons privilégié uniquement ce mode de publication, au détriment des méthodes LDAP et Server Message Block (SMB), pour éviter toute référence à des serveurs internes dans les certificats délivrés ;
4. un dernier tiers sous la forme d'un serveur web Linux avec le rôle de mandataire inverse, implanté dans une « zone démilitarisée » (DMZ) en IP publique, contrairement aux trois serveurs précédents hébergés dans une zone réseau interne. Ce serveur est uniquement chargé de servir aux clients les requêtes de CRL et d'AIA. Les URL des fichiers sont ajoutées dans les extensions des deux autorités de certification, afin de permettre à un client, quel que soit son emplacement réseau, d'accéder aux fichiers sans devoir accéder au réseau interne.

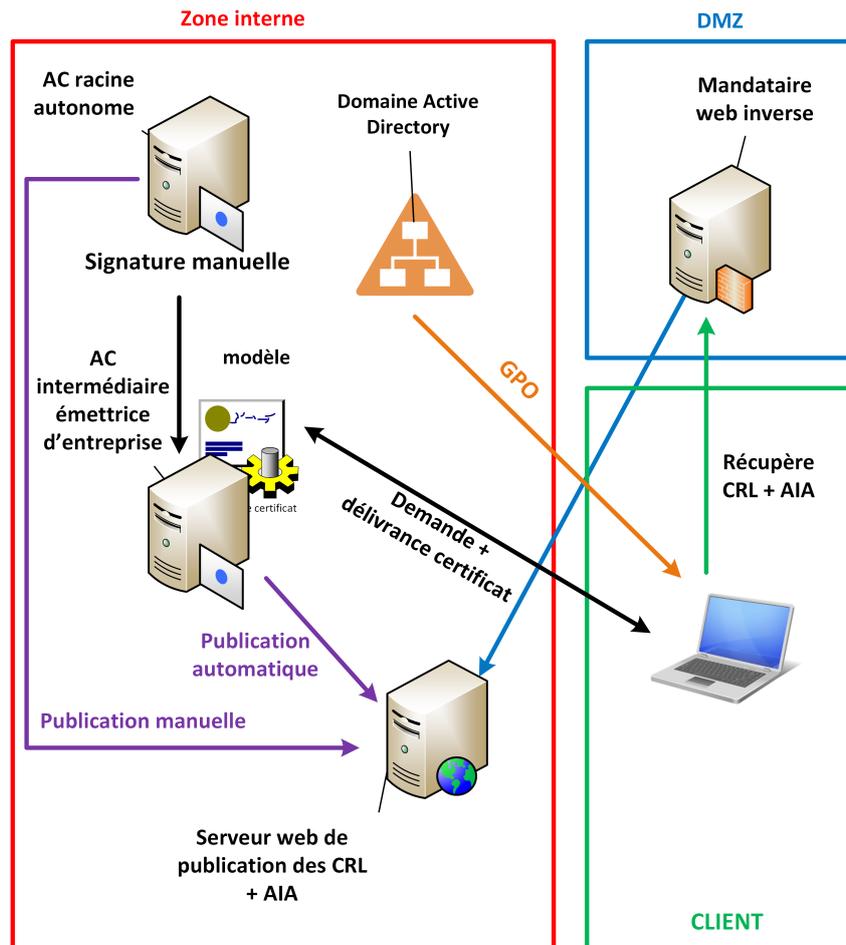


Figure 1 - Architecture de l'IGC académique

À cette architecture technique, nous avons proposé d'ajouter en parallèle une organisation des tâches entre les intervenants :

- l'Ingénieur Sécurité Racine (ISR). Il est au final le responsable de la politique de certification et donc de la chaîne de confiance numérique. À ce titre, il procède à l'administration système de l'autorité de certification racine. Il doit aussi publier périodiquement manuellement la liste de révocation de l'autorité racine, cette dernière opération étant obligatoire, sous peine d'interrompre toute la chaîne de confiance de l'IGC ;
- l'équipe systèmes et réseaux. Elle est en charge de l'administration système de l'autorité intermédiaire émettrice, ainsi que des serveurs de publication web ;
- l'équipe Gestion De Parc. Elle a un rôle de gestionnaire des certificats sur l'autorité intermédiaire émettrice. Sa tâche la plus importante est de révoquer les certificats des ordinateurs volés ou mis au rebut ainsi que de ceux renommés, puisque le nom du sujet du certificat correspondrait au nom de l'ordinateur.

Au final, cette IGC académique a permis l'automatisation quasi-totale du processus de certification des postes, seule la révocation du certificat en cas de vol ou de réforme de la machine restant une opération manuelle à la charge de l'équipe de gestion du parc.

3.3 Mise en place de l'architecture SCCM de production

Faire un choix d'architecture équilibrée pour SCCM n'a pas été des plus simples, nombre de conseils plus ou moins contradictoires existant dans la bibliographie et sur les sites web des consultants spécialisés certifiés par l'éditeur. Pour la répartition des serveurs internes centraux, nous avons installé deux serveurs afin de répartir un minimum la charge de travail et d'isoler, sur le plan de la sécurité, les fonctions :

- un serveur de site primaire avec sa base SQL server, regroupant les rôles autour de la manipulation des données ;
- un second système de site, regroupant tous les rôles exposés au travers du serveur web IIS.

La difficulté de cette phase de définition de l'architecture a été de déterminer la place du serveur SCCM dédié aux postes connectés sur Internet, ainsi que sa dépendance à l'Active Directory. Concernant ce serveur, nous avons d'après les documentations trois choix :

- soit l'installer dans une DMZ et l'exposer directement sur Internet. Cette solution, que nous jugions risquée, revenait à exposer un serveur IIS directement sur Internet, avec le risque en cas de faille de sécurité que le serveur SCCM soit compromis, puis éventuellement par rebond ultérieur les serveurs de la même zone réseau ;
- soit l'installer dans une DMZ et l'exposer sur Internet indirectement, uniquement à travers un équipement mis en coupure, en l'occurrence pour notre contexte nos équipements matériels de répartition de charge (F5 BIG-IP), à qui l'on pourrait déléguer le filtrage des certificats X.509 clients, ceci afin de n'aiguiller sur le serveur SCCM que des requêtes supposées légitimes, provenant de postes clients de l'académie ;
- soit enfin tout simplement ne pas installer ce serveur SCCM, mais se reposer sur les boîtiers F5 BIG-IP qui adresseraient directement nos serveurs SCCM internes, sur le même principe que la solution numéro deux. Cette solution n'avait, comme la première, pas notre préférence car elle allait à l'encontre de nos principes de cloisonnement des différentes zones réseau, internes et DMZ.

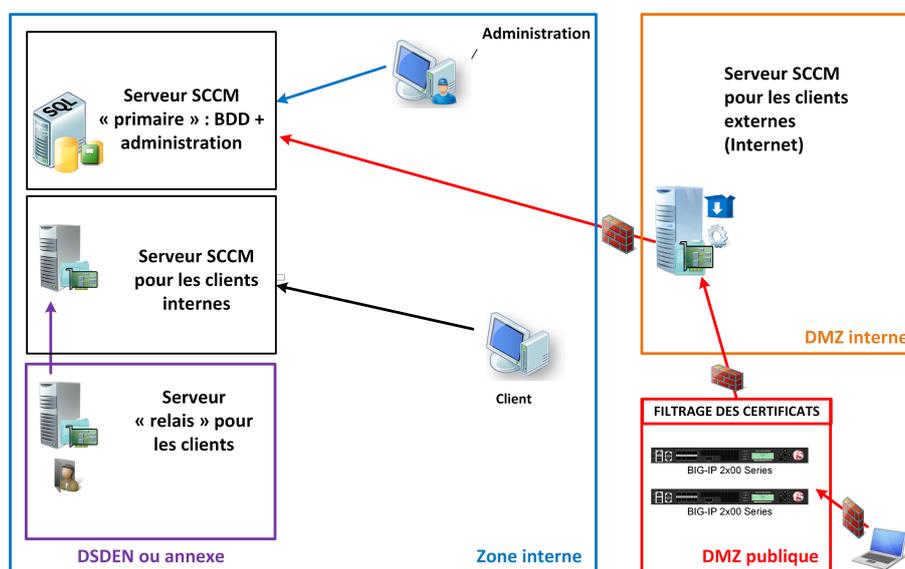


Figure 2 - Architecture cible de l'infrastructure SCCM

Au final, c'est la deuxième solution qui a été validée et que nous avons donc mis en œuvre.

3.4 Filtrage des certificats TLS

Le but de cette brique supplémentaire est de limiter l'exposition du serveur SCCM et, par filtrage au niveau des propriétés du certificat, de n'autoriser que les certificats TLS clients délivrés par notre IGC interne n'étant ni expirés ni surtout révoqués. C'est possible avec SCCM, les informations permettant au serveur d'identifier le poste de travail résidant au niveau applicatif et n'étant pas le nom du poste, DNS ou Windows, figurant dans le nom complet du certificat ou bien dans le champ SAN (*Subject Alternative Name*). Initialement, nous pensions pouvoir assurer ce filtrage et le « pontage » TLS sur les boîtiers de répartition de charge F5-BigIP que nous possédions, installés en frontal des DMZ applicatives. Malheureusement, Microsoft conseille et détaille cette configuration pour sa propre passerelle de sécurité nommée « *Forefront Threat Management Gateway* », mais aucune documentation n'existe pas pour notre matériel F5 Big-IP, pourtant très répandu.

Il s'avère que c'est tout à fait possible avec des F5 mais nous n'y sommes pas arrivés dans les délais impartis. Temporairement, nous avons donc mis en place un mandataire inverse Apache 2.4 en coupure, serveur qui assure la terminaison TLS ainsi qu'un filtrage des certificats, avant de re-chiffrer le flux en direction du serveur SCCM de DMZ. Nous utilisons pour ce filtrage 3 directives de configuration :

- SSLVerifyClient : pour activer la vérification des certificats x509 clients ;
- SSLCARevocationCheck : pour vérifier à partir de la *Certificate Revocation List* (CRL) si le certificat client n'a pas été déclaré révoqué (ce qui est le cas pour les ordinateurs perdus, volés ou tout simplement mis au rebus) ;
- SSL Require pour opérer au niveau de la localisation racine (/) un filtrage par expression régulière sur les propriétés du certificat, ceci afin de nous assurer que le champ « nom complet de l'émetteur » du certificat présenté par le client correspond bien à l'autorité de notre IGC et que son champ « nom alternatif du sujet (DNS) » au domaine DNS de nos postes de travail.

4 Les services SCCM accessibles depuis l'extérieur : exploitation et retour d'expérience

Nous sommes actuellement en phase de pré-production sur l'académie, avant que nous ne soyons complètement prêts pour la bascule vers la nouvelle solution SCCM. Certaines des fonctionnalités ne sont pas disponibles lorsque l'agent se trouve sur Internet : le Wake On Lan, l'exécution de séquences de tâches pour installer un système d'exploitation, le contrôle de l'ordinateur à distance... Nous utilisons les trois fonctionnalités principales disponibles hors réseau local : inventaires, déploiements et mises à jour du système.

4.1 Pré-requis : un agent SCCM déployé et fonctionnel

Le pré-requis est l'installation d'un agent sur tous les postes de travail à gérer. Nous avons choisi de le pousser automatiquement depuis le serveur central SCCM vers les postes. Pour que cette installation fonctionne, le serveur chargé de pousser le client doit d'abord pouvoir résoudre correctement le nom DNS du poste client qui doit être membre du domaine AD et enfin plusieurs paramètres doivent avoir été appliqués au préalable par un objet de stratégie de groupe (GPO) :

- un compte de service, renseigné également côté serveur SCCM, doit être administrateur local du poste afin de pouvoir installer l'agent ;
- des règles de pare-feu avancées pour le trafic entrant doivent être appliquées ;
- l'ordinateur doit être configuré pour obtenir depuis l'autorité de certification interne le certificat X509 nécessaire à la connexion sécurisée.

Pour l'établissement de la communication chiffrée, l'ordinateur doit également avoir récupéré dans l'AD - mécanisme natif dans un domaine Microsoft - les certificats des autorités de certification racine et intermédiaire de l'académie. L'agent SCCM détermine ensuite automatiquement qu'il est en mode « PKI » et qu'il se trouve sur l'Intranet ou sur Internet.

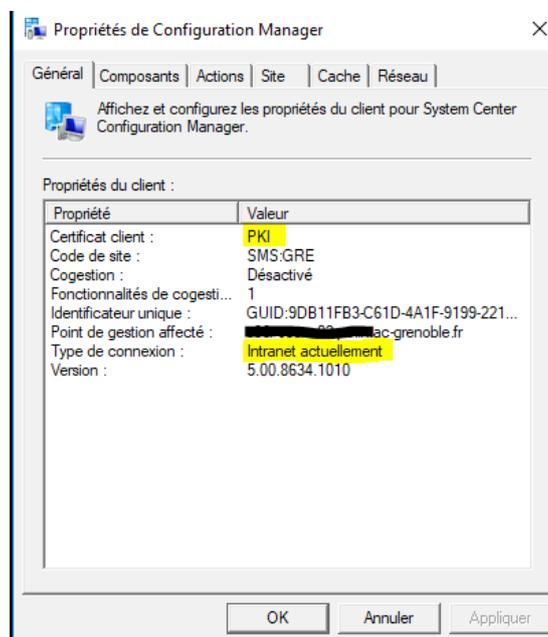


Figure 3 - Propriétés d'un agent SCCM

Tant qu'il est capable de joindre un contrôleur de domaine ou un « point de gestion » SCCM sur son réseau local, il utilise les paramètres de connexion Intranet. Dans le cas contraire, il utilise les serveurs de rôle SCCM paramétrés pour une connexion Internet. Dans les deux cas, l'agent ira récupérer ses paramètres, définis de manière centralisée par l'administrateur, auprès de son point de gestion.

4.2 Inventaires matériel et logiciel

Avant tout, il faut cerner les définitions particulières des inventaires au sens de Microsoft SCCM. Un « inventaire matériel » comprend l'inventaire des composants matériels de la machine ainsi que celui de ces composants logiciels, mises à jour du système comprises. La notion « d'inventaire logiciel » (non utilisé dans notre structure) est là pour récupérer si besoin à la demande des administrateurs des informations sur les postes, tels l'inventaire d'un type de fichiers dans l'arborescence d'un volume ou bien le contenu d'un fichier.

Ces services sont parfaitement fonctionnels hors du réseau local et les remontées d'inventaire se font vers le rôle de « point de gestion », par défaut sur le port TCP/443. Comme les autres données envoyées par les clients à leur point de gestion, on peut demander qu'elles soient signées. Leur fréquence d'envoi est personnalisable, tout comme leur contenu, depuis la console centrale : Un décalage temporel aléatoire permet d'étaler les remontées durant un intervalle configurable, même si en pratique ça n'est utile que pour des parcs de postes de travail vraiment importants : les inventaires envoyés sont des deltas du premier inventaire de la machine et un service du serveur SCCM les intègre ensuite au fur et à mesure de leur réception dans la base de données.

Spécifiez des paramètres d'inventaire matériel pour des ordinateurs client.

Paramètres de périphérique

Activer l'inventaire matériel sur les clients Oui ▾

Calendrier de l'inventaire matériel A lieu tous les 1 jours à compter du 26/04/2018 11:00 Calendrier...

Délai aléatoire maximal (minutes) 120 ▾

Classes d'inventaire matériel Déf. classes...

Figure 4 - Paramétrage centralisé de l'inventaire matériel

Pour qui maîtrise WMI (Windows Management Instrumentation), l'inventaire matériel peut même être enrichi de classes d'inventaire personnalisées. Par défaut, on retrouve cependant toutes les informations habituellement nécessaires ainsi qu'une historique des changements ayant eu lieu sur la machine entre chaque inventaire (ajout ou suppression de matériel, logiciel...). Malheureusement, et c'est une grosse limite du progiciel à notre sens, elles ne peuvent être enrichies des informations administratives (localisation, service...) et financières (coût, date d'achat, garantie...) tel qu'on peut le faire avec GLPI par exemple.

4.3 Déploiements logiciels et centre logiciel

SCCM permet de déployer sur les machines des scripts et des logiciels, ainsi que leurs mises à jour. Le contenu à déployer peut l'être sous forme de « packages » (ancienne méthode) ou « d'applications » (méthode « moderne »). L'objet application comprend en effet d'avantages de paramètres pour contrôler finement l'installation, la désinstallation et la planification du déploiement d'un logiciel sur plusieurs types de périphériques et systèmes d'exploitation différents. C'est donc cet objet que l'on utilise en priorité pour déployer un logiciel chez nous. Tout objet « application » comprend aussi un ou plusieurs types de déploiement dans lequel on va déterminer si l'application est obligatoire ou disponible et pour quel type de configuration matérielle. Au final, l'application est rendue disponible sous forme de paquets répliqués sur des « points de distribution » SCCM situés au plus près des clients, qui iront y récupérer les déploiements dont ils sont la cible, une fois que leur point de gestion leur en aura donné l'ordre.

Si une application est marquée obligatoire, elle est déployée « classiquement » de manière planifiée et l'interaction avec l'utilisateur est limitée ; dans le second cas, l'application apparaît dans le centre logiciel, un composant de l'agent SCCM, qui liste l'ensemble des applications rendues disponibles et installables par l'utilisateur.²

2. Un autre outil côté client existe : le catalogue logiciel. Il n'a pas été pas installé dans notre cas, étant ancien et peu pratique.

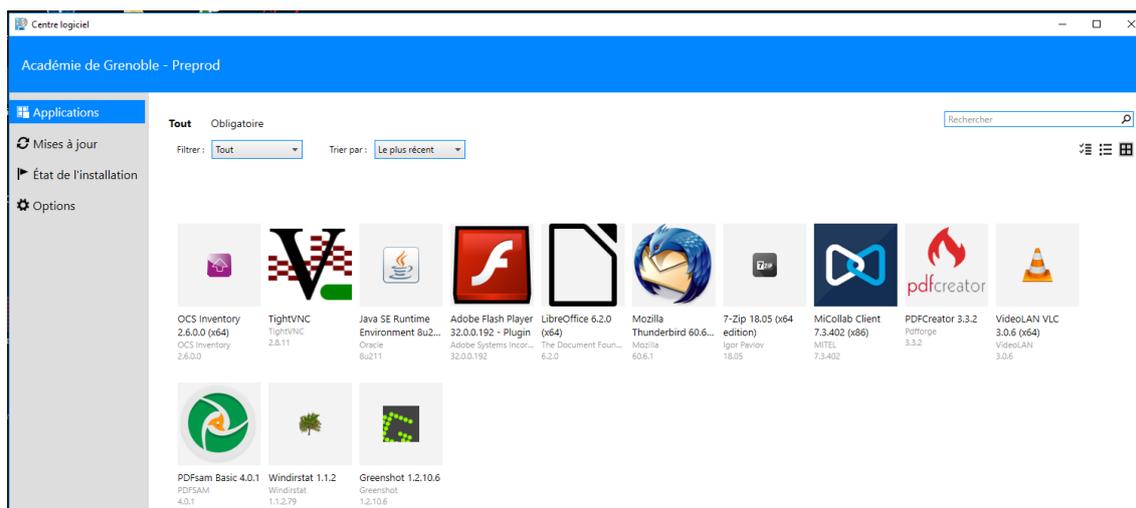


Figure 5 - Centre logiciel SCCM

Un des gros intérêts du produit est d'offrir ce catalogue applicatif disponible en permanence aux populations nomades, quelque soit le réseau de connexion. Bien qu'il soit possible de proposer également une mise à niveau de système d'exploitation par ce biais, nous avons préféré rejeter cette solution qui pourrait donner des résultats hasardeux.

La première des limitations constatées, c'est qu'il n'est pas possible de rendre une application disponible optionnellement dans le centre logiciel en ciblant une collection d'utilisateurs. En effet, seule une collection d'ordinateurs peut être la cible d'une mise à disposition facultative dans le centre logiciel. La seconde limitation est que le flux de travail permettant de gérer des approbations d'installations par la DSI, par exemple pour des applications onéreuses, n'est plus disponible dans le centre logiciel alors qu'il l'était dans l'ancien composant appelé « catalogue logiciel ».

4.4 Mises à jour du système d'exploitation

La mécanique de mise à jour des postes hors LAN passe par l'exposition d'un serveur *Windows Server Update Services* (WSUS) en DMZ et l'ajout du rôle de « point de mise à jour logicielle » sur le serveur SCCM de DMZ. Pour les administrateurs déjà familiers de WSUS, on retrouve une partie de la logique : sélection des produits dont on souhaite synchroniser les mises à jour et pour le type de mise à jour (critique, fonctionnalité...). La mécanique permet ensuite de créer à partir de l'ensemble des mises à jour synchronisés des groupes de mises à jour que l'on va télécharger dans les paquets à distribuer puis déployer sur des collections d'ordinateurs cibles, le tout étant organisable de manière personnalisable par l'administrateur.

Nous avons choisi dans ce cadre une stratégie assez basique pour la pré-production : un administrateur sélectionne tous les mois via un filtre simple toutes les mises à jour du mois (les « *Patch Tuesday* ») qu'il regroupe par type de système et par mois et que l'on synchronise ensuite dans un paquet logiciel regroupant toute l'année en cours. Ce paquet est ensuite déployé sur les collections d'ordinateurs cibles, après avoir été synchronisé au plus près des postes. Des rapports pré-définis permettent enfin de suivre la progression des déploiements sur le parc. Coté client, quand on active la fonctionnalité de mise à jour logicielle, l'agent SCCM se contente d'ajouter une stratégie de sécurité locale spécifiant l'emplacement du serveur de mise à jour. Une fois que le calcul des mises à jour manquantes par rapport à celles assignées est effectué, le paquet de mises à jour est installé par l'agent SCCM.

Nous rencontrons pour le moment une difficulté en cours d'analyse pour les postes connectés sur Internet. À terme, quand elle sera résolue, l'idée serait d'ajouter une étape intermédiaire dans la validation des mises à jour en les testant tout d'abord sur un parc réduit de postes de travail avant de les généraliser à l'ensemble du parc.

5 Conclusion

De notre point de vue, Microsoft SCCM permet de gérer de manière très intégrée un parc de postes de travail nomades Windows. D'autres systèmes seraient gérables (tablettes, ordiphones...) mais nous n'avons pas testé ces fonctionnalités, qui restent plutôt dévolues chez nous à un gestionnaire de flotte mobile. Durant ces phases d'installation et de pré-production, nous avons pu cependant nous rendre compte d'un gros manque dans le progiciel, à savoir l'absence de fonctionnalité de gestion administrative du parc. Nous l'avons contourné en utilisant un greffon qui permet d'importer les inventaires SCCM dans GLPI afin d'enrichir ces derniers.

À l'usage, il faut aussi préciser que le produit est relativement complexe : il nous semble que consacrer un Équivalent Temps Plein à son administration n'est pas de trop pour préparer les paquets applicatifs, les mises à jour des systèmes d'exploitation et les séquences de tâches d'installation...