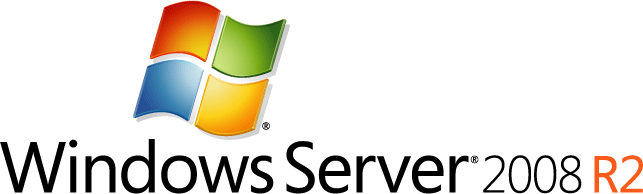
****

****  
  
**Guide de référence technique de Volume Activation**

**Windows 7 et Windows Server 2008 R2**

Microsoft Corporation

Date de publication : Juillet 2009

Résumé

Le présent guide de référence s’adresse aux analystes programmeurs dont les organisations envisagent de déployer les versions Volume Activation des systèmes d’exploitation Windows® 7 et Windows Server® 2008 R2. Il vient compléter le *Guide de planification de Volume Activation*, le *Guide de déploiement de Volume Activation*, ainsi que le *Guide des opérations de Volume Activation*.

Le présent document et tout autre document auquel il est fait référence sont fournis à titre informatif uniquement. Microsoft exclut toute garantie, expresse ou tacite, en ce qui concerne ce document. Les informations contenues, y compris les URL et références à des sites Internet, sont sujettes à modification sans préavis. L’utilisateur assume entièrement le risque lié à l’utilisation et aux résultats de l’utilisation de ce document. Sauf indication contraire, les sociétés, organisations, produits, noms de domaine, adresses électroniques, logos, personnes, lieux et événements donnés en exemple dans le présent document sont entièrement fictifs. Toute ressemblance avec une société, une organisation, un produit, un nom de domaine, une adresse électronique, un logo, une personne, un lieu ou un événement réel serait fortuite et involontaire. L’utilisateur est tenu d’observer la réglementation relative aux droits d’auteur applicables dans son pays. Sans préjudice aux droits d’auteur, aucune partie de ce document ne peut être reproduite, stockée ou introduite dans un système de restitution, ou transmise à quelque fin ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre) sans l’autorisation expresse et écrite de Microsoft Corporation.

Microsoft peut détenir des brevets, avoir déposé des demandes d’enregistrement de brevets ou être titulaire de marques, de droits d’auteur ou d’autres droits de propriété intellectuelle portant sur tout ou partie des éléments faisant l’objet du présent document. Sauf stipulation expresse contraire d’un contrat de licence écrit de Microsoft, la fourniture du présent document n’a pas pour effet de vous concéder une licence sur ces brevets, marques, droits d’auteur ou autres droits de propriété intellectuelle.

© 2009 Microsoft Corporation.

Microsoft, Active Directory, Hyper-V, Windows, Windows Server et Windows Vista sont des marques du groupe de sociétés Microsoft.

Les noms des sociétés et produits existants mentionnés peuvent être des marques de leur détenteur respectif.

**Table des matières**

[Introduction 1](#_Toc237163575)

[Expérience utilisateur 3](#_Toc237163576)

[Options Slmgr.vbs 6](#_Toc237163577)

[Paramètres de registre 15](#_Toc237163578)

[Paramètres des objets de stratégie de groupe 19](#_Toc237163579)

[Temporisation d’activation KMS 21](#_Toc237163580)

[Ordre de recherche de la découverte KMS 23](#_Toc237163581)

[Scénarios d’activation 24](#_Toc237163582)

[Scénarios KMS 24](#_Toc237163583)

[Implémentation KMS par défaut pour un réseau de site unique 24](#_Toc237163584)

[Implémentation KMS dans un réseau global complexe 25](#_Toc237163585)

[Scénarios MAK 29](#_Toc237163586)

[Activation indépendante MAK 30](#_Toc237163587)

[Activation MAK par proxy 34](#_Toc237163588)

[Prise en charge du VAMT pour l’activation KMS 41](#_Toc237163589)

[Conversion de clients KMS en activation MAK 42](#_Toc237163590)

[Clés d’hôte KMS de produits 45](#_Toc237163591)

[Valeurs de stratégie d’activation 47](#_Toc237163592)

[Clés d’installation de client KMS 48](#_Toc237163593)

[Codes d’erreur d’activation 50](#_Toc237163594)

[Journal des événements Windows 59](#_Toc237163595)

[Méthodes et propriétés WMI 64](#_Toc237163596)

[Glossaire 75](#_Toc237163597)

[Liens de ressources 77](#_Toc237163598)

# Introduction

Le présent guide fournit des informations de référence techniques pour le [Guide de planification de Volume Activation](http://go.microsoft.com/fwlink/?LinkId=155926), le [Guide de déploiement de Volume Activation](http://go.microsoft.com/fwlink/?LinkId=150083%20(éventuellement%20en%20anglais)), et le [Guide des opérations de Volume Activation](http://go.microsoft.com/fwlink/?LinkId=150084). Pour une présentation de Microsoft® Volume Activation et de ses composants, voir le [Guide de planification de Volume Activation](http://go.microsoft.com/fwlink/?LinkId=155926). Ce guide référence contient ce qui suit :

* Expérience utilisateur
* Options Slmgr.vbs
* Paramètres de registre
* Paramètres des objets de stratégie de groupe
* Temporisation d’activation du service Gestionnaire de clés (KMS)
* Ordre de recherche de la découverte KMS
* Scénarios d’activation
* Clés d’hôte KMS de produits
* Valeurs de stratégie d’activation
* Clés d’installation de client KMS
* Codes d’erreur d’activation
* Journal des événements Windows®
* Méthodes et propriétés WMI (Windows Management Instrumentation)
* Glossaire
* Ressources

**Remarque**Pour la prise en charge d’autres logiciels utilisant Volume Activation, reportez-vous aux documents spécifiquement rédigés pour ces applications.

Le présent guide utilise les conventions suivantes :

* Les lignes de commande et options de lignes de commande apparaissent en gras.
* Les espaces réservés dans les options de lignes de commande sont encadrés par des crochets angulaires (<>).
* Les options des lignes de commande optionnelles sont encadrées par des crochets droits ([]).
* Les noms des sous-clés de registre et des valeurs apparaissent en gras.

# Expérience utilisateur

Windows® 7 et Windows Server® 2008 R2 affichent des notifications et des boîtes de dialogue adaptées aux problèmes d’activation spécifiques. Le Tableau 1 décrit dans quelle mesure ces notifications et boîtes de dialogue correspondent à chaque problème.

**Remarque**   Les principales éditions de Windows Server 2008 ne sont pas dotées du système de notifications.

Tableau 1. Bulles et boîtes de dialogue pour l’état de notification

| **Problème** | **Bulle de notification** | **Boîte de dialogue correspondante** |
| --- | --- | --- |
| Une copie récemment installée de Windows n’a pas été activée à la fin de la période de grâce d’activation. |  | C:\Users\Jerry\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\04T7PPNO\AlternateURL.JPG |
| Une copie précédemment activée de Windows détecte des modifications du système BIOS et du matériel informatique requérant la réactivation de Windows. En outre, un client KMS activé ne se réactive pas lui-même dans un délai de 180 jours. |  | 37-HW OOT.jpg |
| Windows a été activé via le KMS et n’a pas renouvelé son activation dans le délai de 180 jours plus une période de grâce de 30 jours. |  | 37-KMS OOT.jpg |
| La validation en ligne échoue ou une tentative d’activation est détectée qui permet à des copies non-autorisées de Windows de contourner l’activation de produit. |  | 37-NG.jpg |
| Windows détecte qu’un composant de licence Windows a été modifié. |  | 37 - No Key.jpg |
| Windows détecte que ses fichiers de licence ont été modifiés. |  | 37 - Reinstall.jpg |

# Options Slmgr.vbs

Dans la mesure où WMI change dans Windows 7 et Windows Server 2008 R2, le script Slmgr.vbs n’est pas destiné à fonctionner sur des plateformes. L’utilisation de Slmgr.vbs pour gérer un système Windows 7 ou Windows Server 2008 R2 à partir du système d’exploitation Windows Vista® n’est pas prise en charge. Toute tentative de gestion d’un système de niveau inférieur à partir de Windows 7 ou de Windows Server 2008 R2 générera une erreur d’incompatibilité de version spécifique. Par exemple, l’exécution de **cscript slmgr.vbs <nom\_ordinateur\_vista> /dlv** générera le message suivant :

Microsoft (R) Windows Script Host Version 5.8  
Copyright (C) Microsoft Corporation. Tous droits réservés.

L’ordinateur distant ne prend pas en charge cette version de SLMgr.vbs

Pour gérer des clients distants, utilisez l’outil VAMT (Volume Activation Management Tool) version 1.2 ou ultérieure, ou créez des scripts WMI personnalisés qui tiennent compte des différences entre les plateformes. Pour plus d’informations sur les méthodes et propriétés WMI de Volume Activation, reportez-vous à la section, «  », ultérieurement dans le présent guide de référence.

Ce qui suit décrit la syntaxe du script Slmgr.vbs, et le Tableau 2 détaille chaque option de ligne de commande :

slmgr.vbs [NomOrdinateur [MotDePasse Utilisateur]] [<Option>]

**Remarque**Pour la prise en charge d’autres logiciels utilisant Volume Activation, reportez-vous aux documents spécifiquement rédigés pour ces applications.

Tableau 2. Options des lignes de commande Slmgr.vbs

| **Option** | **Description** |
| --- | --- |
| **[NomOrdinateur]** | Nom d’un ordinateur distant (le nom par défaut est celui de l’ordinateur local) |
| **[Utilisateur]** | Compte disposant du privilège requis sur l’ordinateur distant |
| **[MotDePasse]** | Mot de passe du compte disposant des privilèges requis sur l’ordinateur distant |
| **Options globales** | |
| **/ipk product\_key** | Tente d’installer une clé de produit 5×5. La clé de produit fournie par le paramètre est confirmée valide et applicable au système d’exploitation installé. Si tel n’est pas le cas, une erreur est renvoyée.  Si la clé est valide et applicable, elle est installée. Si une clé est déjà installée, elle est remplacée de manière silencieuse.  Pour éviter toute instabilité dans le service de licences, le système ou le service de protection logicielle doit être redémarré.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges, ou la valeur de registre **Opérations d’utilisateur standard** doit être paramétrée de sorte à autoriser des utilisateurs ne disposant pas des privilèges requis à accéder au service de protection logicielle. |
| **/ato [ID d’activation]** | Pour les versions commerciales et les systèmes en volume pour lesquels une clé hôte KMS ou une clé d’activation multiple (MAK) est installée, **/ato** invite Windows à tenter une activation en ligne.  Quant aux systèmes pour lesquels une clé de licence en volume générique (GVLK) est installée, cette option invite à une tentative à l’activation KMS. Les systèmes ayant été configurés pour suspendre les tentatives d’activation KMS automatiques (**/stao**) tentent toujours une activation KMS lorsque l’option **/ato** est exécutée.  Le paramètre **[ID d’activation]** étend la prise en charge de l’option **/ato** pour identifier une édition Windows installée sur l’ordinateur. Le fait de spécifier le paramètre **[ID d’activation]** permet d’isoler les effets de l’option pour l’édition associée à cet ID d’activation. Exécutez **Slmgr.vbs /dlv** pour obtenir tous les ID d’activation de la version installée de Windows. Si vous avez besoin de prendre en charge d’autres applications, reportez-vous aux guides fournis pour ces applications pour plus d’informations.  L’activation KMS ne requiert pas de privilèges plus élevés. Toutefois, une activation en ligne requiert une élévation de privilèges, ou la valeur de registre **Opérations d’utilisateur standard** doit être paramétrée de sorte à autoriser des utilisateurs ne disposant pas des privilèges requis à accéder au service de protection logicielle. |
| **/dli [ID d’activation | Tous]** | Affiche les informations de licence.  Par défaut, **/dli** affiche les informations de licence de l’édition Windows active installée. Le fait de spécifier le paramètre **[ID d’activation]** permet d’afficher les informations de licence de l’édition spécifiée associée à cet ID d’activation. Le fait de spécifier **[Tous]** comme paramètre affichera toutes les informations de licence des produits installés applicables.  Cette opération ne requiert pas de privilèges plus élevés. |
| **/dlv [ID d’activation | Tous]** | Affiche les informations de licence détaillées.  Par défaut, **/dlv** affiche les informations de licence du système d’exploitation installé. Le fait de spécifier le paramètre **[ID d’activation]** permet d’afficher les informations de licence de l’édition spécifiée associée à cet ID d’activation. Le fait de spécifier le paramètre **[Tous]** affiche toutes les informations de licence des produits installés applicables.  Cette opération ne requiert pas de privilèges plus élevés. |
| **/xpr [ID d’activation]** | Affiche la date d’expiration d’activation du produit. Par défaut, cela concerne l’édition Windows actuelle et est principalement utile aux clients KMS dans la mesure où l’activation des éditions commerciales et MAK est perpétuelle.  Le fait de spécifier le paramètre **[ID d’activation]** permet d’afficher la date d’expiration d’activation de l’édition spécifiée associée à cet ID d’activation.  Cette opération ne requiert pas de privilèges plus élevés. |
| **Options avancées** | |
| **/cpky** | Certaines opérations de maintenance requièrent que la clé de produit soit disponible dans le registre lors des opérations OOBE (Out-of-Box Experience). L’option **/cpky** supprime la clé de produit du registre pour éviter que cette clé soit volée par un code malveillant.  Pour les installations commerciales qui déploient des clés, les meilleures pratiques recommandent l’exécution de cette option. Cette option n’est pas requise pour les clés hôtes KMS et MAK dans la mesure où elle correspond au comportement par défaut de ces clés. Cette option n’est nécessaire que pour d’autres types de clés dont le comportement par défaut ne consiste pas à effacer la clé du registre.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **/ilc <fichier\_de\_licence>** | Cette option installe le fichier de licence spécifié par le paramètre requis. Ces licences peuvent être installées en tant que mesure de dépannage pour prendre en charge l’activation basée sur les jetons, ou dans le cadre d’une installation manuelle d’une application intégrée.  Les licences ne sont pas validées durant ce processus : La validation de licence est en dehors du champ d’application de Slmgr. En revanche, la validation est gérée par le service de protection logicielle à l’exécution.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges, ou la valeur de registre **Opérations d’utilisateur standard** doit être paramétrée de sorte à autoriser des utilisateurs ne disposant pas des privilèges requis à accéder au service de protection logicielle. |
| **/rilc** | Cette option réinstalle toutes les licences stockées dans %SystemRoot%\system32\oem and %SystemRoot%\System32\spp\jetons. Ce sont des copies « valides connues » stockées lors de l’installation.  Toutes les licences correspondantes dans le magasin de données de confiance sont remplacées. Toutes les licences supplémentaires (comme par exemple les licences d’émission (IL) d’une autorité de confiance (TA), les licences d’applications) demeurent intactes.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges, ou la valeur de registre **Opérations d’utilisateur standard** doit être paramétrée de sorte à autoriser des utilisateurs ne disposant pas des privilèges requis à accéder au service de protection logicielle. |
| **/rearm** | Cette option réinitialise les compteurs d’activation. Le processus **/rearm** est également appelé par **sysprep /generalize**.  Cette opération n’aura aucun effet si la sous-clé de registre HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\SkipRearm est égale à **1**. Se reporter à la section «  », ultérieurement dans le présent guide, pour obtenir plus d’informations sur cette sous-clé de registre.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges, ou la valeur de registre **Opérations d’utilisateur standard** doit être paramétrée de sorte à autoriser des utilisateurs ne disposant pas des privilèges requis à accéder au service de protection logicielle. |
| **/upk [ID d’activation]** | Cette option désinstalle la clé de produit de l’édition Windows actuelle. Après un redémarrage, le système sera dans un état Sans licence à moins qu’une une nouvelle clé de produit soit installée.  En outre, il est possible d’utiliser le paramètre **[ID d’activation]** pour spécifier un autre produit installé.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **Licences en volume : Options client KMS** | |
| **/skms Nom[:Port] | : port [ID d’activation] [ID d’activation]** | Cette option spécifie le nom ainsi que le port de l’ordinateur hôte KMS à contacter. Le paramétrage de cette valeur désactive l’auto-détection de l’hôte KMS.  Si l’hôte KMS utilise l’IP version 6 (IPv6) uniquement, l’adresse doit être spécifiée au format [nom d’hôte]:port. Les adresses IPv6 contiennent des deux-points (:), qui seront séparées par le script Slmgr.vbs.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **/ckms [ID d’activation]** | Cette option supprime le nom d’hôte KMS spécifié, l’adresse et les informations de port du registre et restaure le comportement de découverte KMS automatique.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **/skhc** | Cette option active la mise en cache de l’hôte KMS (par défaut), bloquant ainsi l’utilisation de la **priorité** et de la **pondération** du système de noms de domaine (DNS) après la découverte initiale d’un hôte KMS utilisé. Si le système ne peut plus contacter l’hôte KMS utilisé, la découverte sera retentée.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **/ckhc** | Cette option désactive la mise en cache de l’hôte KMS. Ce paramètre demande au client d’utiliser la découverte automatique DNS chaque fois qu’il tente une activation KMS (recommandé lorsque la **priorité** et la **pondération** sont utilisées).  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **Configuration de l’hôte KMS** | |
| **/sai <intervalle>** | Cette option définit l’intervalle en minutes des clients non activés pour tenter une connexion KMS. L’intervalle d’activation doit être compris entre 15 minutes et 30 jours, bien que la valeur par défaut (soit 2 heures) soit recommandée.  Le client KMS prend initialement cet intervalle dans le registre, mais il passe au paramètre du KMS après avoir reçu la première réponse du KMS.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **/sri <intervalle>** | Cette option définit l’intervalle de renouvellement en minutes des clients activés pour tenter une connexion KMS. L’intervalle de renouvellement doit être compris entre 15 minutes et 30 jours. Cette option est définie initialement à la fois côtés client et serveur KMS. La valeur par défaut est 10 080 minutes (soit 7 jours).  Le client KMS prend initialement cet intervalle dans le registre, mais il passe au paramètre du KMS après avoir reçu la première réponse du KMS.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **/sprt <port>** | Cette option définit le port sur lequel l’hôte KMS écoute les demandes d’activation de clients. Le port TCP par défaut est 1688.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **/sdns** | Activer la publication d’un hôte KMS dans le DNS (par défaut).  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **/cdns** | Désactiver la publication d’un hôte KMS dans le DNS.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **/spri** | Définir la priorité KMS sur Normal (par défaut).  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **/cpri** | Définir la priorité du service de gestion de clé sur Basse.  Utiliser cette option pour réduire la contention depuis le service de gestion de clé dans un environnement co-hébergé. Il est à noter que cette opération peut provoquer une insuffisance au niveau du service de gestion de clé, en fonction des autres applications ou rôles de serveur actifs. À utiliser avec précaution.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **Configuration d’activation basée sur les jetons** | |
| **/lil** | Répertorier les licences d’émission de l’activation basée sur les jetons. |
| **/ril <ILID> <ILvID>** | Supprimer la licence d’émission de l’activation basée sur les jetons.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **/stao** | Définir l’indicateur d’**activation uniquement basée sur les jetons**, désactivant l’activation KMS automatique.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **/ctao** | Effacer l’indicateur d’**activation uniquement basée sur les jetons** (par défaut), activant l’activation KMS automatique.  Cette opération doit être exécutée à partir d’une invite de commandes avec élévation de privilèges. |
| **/ltc** | Répertorier les certificats d’activation basée sur les jetons valides qui peuvent activer les logiciels installés. |
| **/fta <Empreinte de certificat> [PIN]** | Forcer l’activation basée sur les jetons à l’aide du certificat identifié. Le code confidentiel (PIN) optionnel est fourni pour déverrouiller la clé privée sans invite de PIN lorsque des certificats protégés par le matériel (comme par exemple des cartes à puce) sont utilisés. |

# Paramètres de registre

Le tableau 3 décrit les paramètres de registre que Volume Activation prend en charge.

Tableau 3. Paramètres de registre

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sous-clé de registre : HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** | | | | | |
| **Valeur** | **Type** | | **Description** | | **Étendue** |
| **Activation\AlternateURL** | **REG\_SZ** | | Contient en option une URL fournie par l’administrateur. Si cette clé est renseignée, certaines boîtes de dialogue d’activation incluront un nouveau lien - **En savoir plus sur l’activation en ligne** - qui s’ouvre dans le navigateur par défaut. | | Tout |
| **DisableDnsPublishing** | **REG\_DWORD** | | Attribuer une valeur autre que zéro pour bloquer la publication automatique vers le DNS par l’hôte KMS. | | KMS |
| **DnsDomainPublishList** | **REG\_MULTI\_SZ** | | **Format :** nom\_de\_domaine, <priorité>, <pondération>  Contient en option une liste de domaines complets que le service Gestionnaire de clés utilise pour publier automatiquement son enregistrement de service DNS (SRV). Le domaine racine du KMS est toujours utilisé ; il n’est donc pas nécessaire de l’inclure ici. Cela dépend de la valeur du paramètre **DisableDnsPublishing**.  Les paramètres de **priorité** et de **pondération** sont optionnels. S’ils ne sont pas fournis, ils sont définis sur **0** dans l’enregistrement SRV. | | KMS |
| **EnableKmsLowPriority** | **REG\_DWORD** | | Attribuer une valeur autre que zéro pour réduire la contention depuis le service Gestionnaire de clés dans un environnement co-hébergé. Noter que sur un système occupé, cela peut empêcher l’hôte KMS de maintenir un nombre suffisant. | | KMS |
| **KeyManagementServiceListeningPort** | **REG\_SZ** | | Définir cette valeur sur l’hôte KMS pour forcer le service Gestionnaire de clés à écouter le port TCP spécifié. L’hôte utilise le port TCP 1688 si cette valeur n’est pas spécifiée. | | KMS |
| **KeyManagementServiceName** | **REG\_SZ** | | Définir cette valeur pour forcer le client KMS à utiliser un hôte KMS spécifique. Aucune valeur par défaut.  Si un IdApp ou un IdRéf est spécifié, cette valeur est créée dans une sous-clé sous laquelle la valeur est stockée :  ..\SoftwareProtectionPlatform\APPID\_GUID\KeyManagementServiceName | | Client KMS |
| **KeyManagementServicePort** | **REG\_SZ** | | Définir cette valeur pour forcer le client KMS à utiliser un port TCP spécifique quand il communique avec un service Gestionnaire de clés. Le client utilise le port 1688 si cette valeur n’est pas spécifiée.  Si un IdApp ou un IdRéf est spécifié, cette valeur est créée dans une sous-clé sous laquelle la valeur est stockée :  ..\SoftwareProtectionPlatform\APPID\_GUID\KeyManagementServicePort | | Client KMS |
| **KeyManagementServiceVersion** | **REG\_SZ** | | Définir cette valeur pour la découverte automatique Microsoft Operations Manager (MOM) 2005 du KMS. Supprimer cette valeur si le service Gestionnaire de clés n’est plus exécuté sur l’ordinateur. | | KMS |
| **UserOperations** | **REG\_DWORD** | | Cette valeur n’existe pas par défaut, et la valeur par défaut est **0**, requérant une élévation de privilèges. Créer cette valeur et la définir sur **1** pour permettre aux utilisateurs standard d’installer des clés de produit, et d’activer et de réarmer des ordinateurs sans requérir d’élévation de privilèges.  Ce paramètre peut également être configuré par des objets de stratégie de groupe, qui sont stockés sous la sous-clé de registre **\stratégies**. | | Tout (pas uniquement le service Gestionnaire de clés) |
| **VLActivationInterval** | **REG\_DWORD** | | Cette valeur est définie initialement à la fois côtés client et serveur KMS. La valeur par défaut est 120 minutes (soit 2 heures). Le client KMS prend initialement cet intervalle dans le registre, mais il passe au paramètre du KMS après avoir reçu la première réponse du KMS. La valeur minimale est 15 minutes, et la valeur maximale 43 200 minutes (soit 30 jours). | | Serveur et client KMS |
| **VLRenewalInterval** | **REG\_DWORD** | | Cette valeur est définie initialement à la fois côtés client et serveur KMS. La valeur par défaut est 10 080 minutes (soit 7 jours). Le client KMS prend initialement cet intervalle dans le registre, mais il passe au paramètre du KMS après avoir reçu la première réponse du KMS. Le paramètre côté client ne sera donc jamais utilisé. La valeur minimale est 15 minutes, et la valeur maximale 43 200 minutes (soit 30 jours). | | Serveur et client KMS |
| **Sous-clé de registre : HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation** | | | | | |
| **Valeur** | **Type** | **Description** | | **Étendue** | |
| **Manual** | **REG\_DWORD** | **0** = Permettre une activation en ligne automatique (par défaut)  **1** = Désactiver l’auto-activation | | Hôte KMS et MAK mais pas client KMS | |
| **NotificationDisabled** | **REG\_DWORD** | **0** = Affichage d’avis et bulles relatifs à l’activation (par défaut)  **1** = Tous les avis relatifs à l’activation seront masqués si Windows ne se trouve pas dans un état de Notification ou Sans licence. Non recommandé. | | Tout (pas uniquement le service Gestionnaire de clés) | |

# Paramètres des objets de stratégie de groupe

Le tableau 4 décrit les paramètres de stratégie de groupe que les organisations peuvent utiliser pour éviter que le système d’exploitation change l’affichage du bureau en noir dans l’état de Notification.

Tableau 4. Paramètres des objets de stratégie de groupe

| **Nom de la stratégie** | **Description** |
| --- | --- |
| **Configuration utilisateur -> Modèles d’administration -> Panneau de configuration -> Personnalisation -> Empêcher de modifier l’arrière-plan du Bureau** | Empêche les utilisateurs d’ajouter ou de modifier l’image d’arrière-plan du Bureau.  Par défaut, les utilisateurs peuvent utiliser la page **Arrière-plan du Bureau** du Panneau de configuration Personnalisation ou Affichage pour ajouter une image d’arrière-plan (papier peint) à leur Bureau.  Si vous activez ce paramètre, aucun des paramètres d’arrière-plan du Bureau ne pourra être modifié par l’utilisateur.  Pour spécifier le papier peint pour un groupe, utilisez le paramètre **Papier peint** du Bureau.  **Remarque**   vous devez également activer le paramètre **Papier peint** du Bureau pour empêcher les utilisateurs de modifier le papier peint choisi pour le Bureau. Reportez-vous à l’article du site Microsoft Aide et Support, « Vous pouvez modifier le paramètre Papier peint du Bureau après que l’administrateur a sélectionné l’option ‘Empêcher de modifier le papier-peint’ dans la stratégie de groupe », à l’adresse <http://support.microsoft.com/kb/Q327998> pour plus d’informations.  Consultez également le paramètre **N’autoriser que les papiers peints au format bitmap**. |
| **Configuration utilisateur -> Modèles d’administration -> Bureau -> Bureau -> Papier peint du Bureau** | Spécifie l’image d’arrière-plan (le « papier peint ») affichée sur le Bureau des utilisateurs.  Ce paramètre vous permet de spécifier le papier peint du Bureau des utilisateurs et empêche ces derniers de modifier l’image ou sa présentation. Le papier peint spécifié peut être enregistré dans un fichier de type bitmap (\*.bmp) ou JPEG (\*.jpg).  Pour utiliser ce paramètre, entrez le chemin d’accès complet et le nom du fichier contenant le papier peint. Vous pouvez taper un chemin d’accès local, tel que C:\Windows\web\wallpaper\accueil.jpg, ou un chemin d’accès UNC, tel que \\Serveur\Partage\Logo.jpg. Si le fichier spécifié n’est pas disponible lorsque l’utilisateur ouvre sa session, aucun papier peint n’est affiché. Les utilisateurs ne peuvent pas spécifier un autre papier peint. Vous pouvez également utiliser ce paramètre afin de spécifier si l’image du papier peint doit être centrée, en mosaïque ou étirée. Les utilisateurs ne peuvent pas modifier cette spécification.  Si vous désactivez ce paramètre ou ne le configurez pas, aucun papier peint n’est affiché. Les utilisateurs peuvent toutefois sélectionner le papier peint de leur choix.  Consultez également le paramètre **N’autoriser que les papiers peints au format bmp** au même endroit et le paramètre **Empêcher le changement de papier peint** dans Configuration utilisateur\Modèles d’administration\Panneau de configuration.  **Remarque**   ce paramètre ne s’applique pas aux sessions de serveur Bureau à distance. |
| **Configuration utilisateur -> Modèles d’administration -> Panneau de configuration -> Personnalisation -> Empêcher de modifier les icônes du Bureau** | Empêche l’utilisateur de modifier les icônes du Bureau.  Par défaut, les utilisateurs peuvent utiliser la boîte de dialogue **Paramètres des icônes du Bureau** dans le Panneau de configuration Personnalisation ou Affichage pour afficher, supprimer ou modifier les icônes du Bureau.  Si vous activez ce paramètre, aucune des icônes du Bureau ne pourra être modifiée par l’utilisateur.  Pour les systèmes antérieurs à Windows Vista, ce paramètre masque également l’onglet **Bureau** dans le Panneau de configuration Affichage. |

# Temporisation d’activation KMS

La temporisation d’activation KMS est contrôlée par deux paramètres : le compteur d’activation et le compteur de renouvellement :

* L’intervalle d’activation KMS détermine la fréquence à laquelle le client KMS tente une activation avant qu’il soit activé et lors de la période de grâce et des notifications. Cette valeur est définie sur le client en exécutant **slmgr.vbs /sai *intervalle***. L’intervalle est indiqué en minutes, et la valeur par défaut est 120 minutes. Reportez-vous aux sections «  » et «  » pour plus d’informations. Une fois qu’un système contacte un hôte KMS, le paramètre de l’hôte KMS prévaudra sur le paramètre du client local.
* L’Intervalle de renouvellement KMS détermine la fréquence à laquelle le client KMS tente une réactivation avec le service Gestionnaire de clés, une fois qu’il a été activé. Cette valeur peut être définie en exécutant **slmgr /sri *intervalle***. L’intervalle est défini en minutes. La valeur par défaut est 10 080 minutes (soit 7 jours). Cette valeur peut être définie sur le client mais sera remplacée par la valeur que l’hôte KMS fournit.

Concrètement, le client KMS tente de contacter un hôte KMS au démarrage, et fait une nouvelle tentative à chaque intervalle d’activation (en minutes) en cas d’échec. Par défaut, cet intervalle est de deux heures. Lorsque l’activation KMS réussit, le client reçoit et stocke l’intervalle de renouvellement de l’hôte KMS, et Windows est activé pendant 180 jours. Le renouvellement de l’activation fonctionne sous forme de fenêtre défilante, à l’instar d’un bail DHCP (Dynamic Host Configuration Protocol). Le client est activé pendant 180 jours mais retente une réactivation à chaque intervalle de renouvellement (en minutes), par défaut, 7 jours. Si la réactivation réussit, la période de 180 jours est réinitialisée. Si elle échoue, le système détectera les changements de réseau ou d’autres événements éligibles pour déclencher une autre tentative. Après 15 minutes, le système arrête de surveiller les événements éligibles mais effectue une nouvelle tentative à chaque intervalle de renouvellement (en minutes).

Si une période de 180 jours s’écoule sans qu’une réactivation réussisse, le client passe en période de grâce hors tolérance. Si aucune activation n’est effectuée dans un délai de 30 jours après le passage en période de grâce hors tolérance, il passe en mode Notification.

# Ordre de recherche de la découverte KMS

Lorsque la découverte automatique KMS est activée (par défaut) et que la mise en cache de l’hôte KMS n’est pas désactivée, les clients KMS utiliseront l’ordre suivant pour déterminer le KMS à utiliser (ils tenteront chaque étape jusqu’à ce qu’un hôte KMS activé muni de la clé appropriée réponde) :

* Valeur spécifique à la Référence dans la valeur de registre HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\AppID\SKUID\KeyManagementServiceName REG\_SZ
* Valeur spécifique à l’IdApp dans la valeur de registre HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\AppID\KeyManagementServiceName REG\_SZ
* Valeur globale dans la valeur de registre HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\KeyManagementServiceName REG\_SZ
* Hôte KMS mis en cache spécifique à la Référence (Il s’agit de l’identité mise en cache de l’hôte utilisé dans la dernière activation KMS réussie.)
* Découverte automatique DNS (**pondération** et **priorité** respectées)

Si un KMS mis en cache ne répond pas, la découverte est effectuée.

# Scénarios d’activation

Les sections suivantes décrivent des scénarios clés pour l’activation MAK et KMS.

## Scénarios KMS

Le KMS peut prendre en charge des réseaux simples, de site unique et globaux. Les scénarios suivants indiquent :

* L’implémentation par défaut du KMS.
* L’implémentation étendue pour prendre en charge un réseau global.

### Implémentation KMS par défaut pour un réseau de site unique

Contoso compte 100 clients Windows 7 Entreprise et un ensemble de systèmes Windows Vista, Windows Server 2008 et Windows Server 2008 R2. Contoso est un domaine plat (Contoso.com), comme indiqué en Figure 1. Le serveur DNS exécute le DNS Microsoft dans sa configuration par défaut. Cette configuration prend en charge l’enregistrement dynamique DNS ainsi que le nettoyage des enregistrements DNS pour supprimer les enregistrements périmés.



Figure 1. Implémentation KMS par défaut pour un réseau de site unique

Contoso achète un contrat de licence qui fournit une clé B KMS, qui activera tous ses systèmes. L’administrateur informatique (IT) installe la clé hôte KMS de Contoso (CSVLK) sur deux hôtes KMS exécutant Windows Server 2008 R2 à l’aide de la commande suivante exécutée localement à partir d’une invite de commandes avec élévation de privilèges :

Slmgr.vbs /ipk <clé\_hôte\_KMS>

L’administrateur IT crée ensuite un Groupe de sécurité dans les services de domaine Active Directory® (AD DS) appelé *Hôtes\_KMS.* L’administrateur ajoute les serveurs KMS\_1 et KMS\_2 aux hôtes KMS.

L’hôte KMS\_1 est activé auprès de Microsoft par Internet : **Slmgr.vbs /ato**. KMS\_1 publie automatiquement ses enregistrements de ressources SRV dans le DNS. L’administrateur IT accède au serveur DNS, localise l’enregistrement de ressources de \_vlmcs.\_tcp.contoso.com, et modifie ses autorisations pour accorder à l’enregistrement l’autorisation de lecture, d’écriture et de suppression des hôtes KMS. L’hôte KMS\_2 est désormais activé auprès de Microsoft par Internet : **Slmgr.vbs /ato***.*

Enfin, l’administrateur confirme que l’exclusion des hôtes KMS est activée dans le pare-feu Windows. L’exception de pare-feu du service Gestionnaire de clés doit être activée.

Les clients KMS sur le réseau Contoso demandent le DNS et reçoit les enregistrements SRV pour les deux hôtes KMS. Les clients prennent l’un ou l’autre hôte et sont activés (dès que le nombre de clients KMS dépasse le seuil). Reportez-vous à la section, «  », pour plus d’informations sur les exigences en matière de nombre de clients KMS.

### Implémentation KMS dans un réseau global complexe

Contoso s’est étendu à deux domaines, est.contoso.com et ouest.contoso.com, comme indiqué en Figure 2. Le trafic réseau peut passer de manière privée entre les deux réseaux via une liaison de réseau étendu (WAN) derrière un pare-feu. Cette liaison présente une bande passante limitée. Ainsi, les ressources (notamment DNS) sont répliquées des deux côtés de la liaison WAN afin de réduire le trafic dans toute la mesure du possible.



Figure 2. Implémentation KMS dans un réseau global complexe

Contoso utilise un déploiement basé sur une image. Ses systèmes clients sont standardisés sur Windows Vista, mais les systèmes Windows Vista sont remplacés par des clients Windows 7.

Les utilisateurs se déplacent régulièrement, et leur connexion réseau passe d’un domaine à un autre. L’adressage IP des clients est fourni dynamiquement par DHCP, notamment la spécification de l’hôte DNS local, de l’adresse de la passerelle locale, etc.

Pour assurer la prise en charge de l’activation des clients Windows Vista existants et des nouveaux clients Windows 7, Contoso installe quatre hôtes KMS (à l’aide de sa clé B KMS). Deux hôtes KMS sont configurés dans est.contoso.com, et deux autres sont configurés dans ouest.contoso.com.

L’administrateur IT configure les hôtes KMS de sorte que les enregistrements SRV DNS amènent les clients Windows 7 et Windows Server 2008 R2 dans le domaine Est vers KMS\_E1, si disponible, ou vers KMS\_E2. Si aucun des deux n’est disponible, les clients feront une tentative avec KMS\_W1, puis KMS\_W2. De même, le DNS dans le domaine Ouest est configuré de sorte que les clients Windows 7 du domaine Ouest préféreront contacter KMS\_W1, puis KMS\_W2, et lorsque ceux-ci seront défaillants uniquement, tenteront une activation avec KMS\_E1 et KMS\_E2 du côté le plus éloigné de la liaison WAN.

L’administrateur IT effectue cette opération en procédant aux modifications de configuration suivantes (voir Tableau 5) :

* Les hôtes KMS\_E\* sont ajoutés au groupe de sécurité KMS\_E. Ce groupe dispose de droits de lecture, d’écriture et de suppression pour l’enregistrement \_vlmcs.\_tcp.east.contoso.com.
* Les hôtes KMS\_W\* sont ajoutés au groupe de sécurité KMS\_W. Ce groupe dispose de droits de lecture, d’écriture et de suppression pour l’enregistrement \_vlmcs.\_tcp.west.contoso.com.
* Les serveurs DHCP sont configurés pour ajouter les domaines est.contoso.com et ouest.contoso.com à la liste de recherche de suffixes DNS pour tous les clients.
* Les pare-feux entre les domaines Est et Ouest sont configurés pour permettre le trafic RPC vers les hôtes KMS sur le port 1688.

Tableau 5. Configuration des hôtes KMS

| **Description** | **Configuration** | **Hôte** |
| --- | --- | --- |
| Configurez la pondération et la priorité SRV du domaine est.contoso.com de sorte que les clients contactent les hôtes KMS\_E\* s’ils sont disponibles avant d’essayer les hôtes KMS\_W\*. Le trafic sera divisé : 75 % sur les hôtes KMS\_\*1 et 25 % sur les hôtes KMS\_\*2. | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform DnsDomainPublishList=  KMS\_E1, 10, 75  KMS\_E2, 10, 25  KMS\_W1, 90, 75  KMS\_W2, 90, 25 | KMS\_E1  KMS\_E2 |
| Configurez la pondération et la priorité SRV du domaine ouest.contoso.com de sorte que les clients contactent les hôtes KMS\_W\* s’ils sont disponibles avant d’essayer les hôtes KMS\_E\*. Le trafic sera divisé : 75 % sur les hôtes KMS\_\*1 et 25 % sur les hôtes KMS\_\*2. | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform DnsDomainPublishList=  KMS\_W1, 10, 75  KMS\_W2, 10, 25  KMS\_E1, 90, 75  KMS\_E2, 90, 25 | KMS\_W1  KMS\_W2 |

Puis, l’administrateur confirme que les exceptions du pare-feu Windows sont définies pour permettre le trafic des clients KMS, et configure les ordinateurs clients, comme décrit au Tableau 6.

Tableau 6. Configuration des clients KMS

| **Description** | **Configuration** |
| --- | --- |
| Désactiver la mise en cache de l’hôte KMS | **Slmgr /ckhc** |
| Une URL client est définie pour diriger les utilisateurs ayant des problèmes d’activation vers l’assistance Contoso | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation  Autre URL = http://contoso.com/help |

L’ordinateur de référence client est activé par le KMS, puis la commande **sysprep /generalize** est exécutée. Le système est arrêté et imagé à l’aide de ImageX du kit d’installation automatisée Windows (Windows AIK) de Windows 7. Windows AIK est téléchargeable à l’adresse suivante : <http://go.microsoft.com/fwlink/?LinkId=136976>.

## Scénarios MAK

Les sections suivantes décrivent des scénarios pour l’activation MAK, qui sont basés sur le scénario illustré en Figure 3. Cette figure schématise des environnements de groupes de travail et de réseaux types de grandes entreprises.

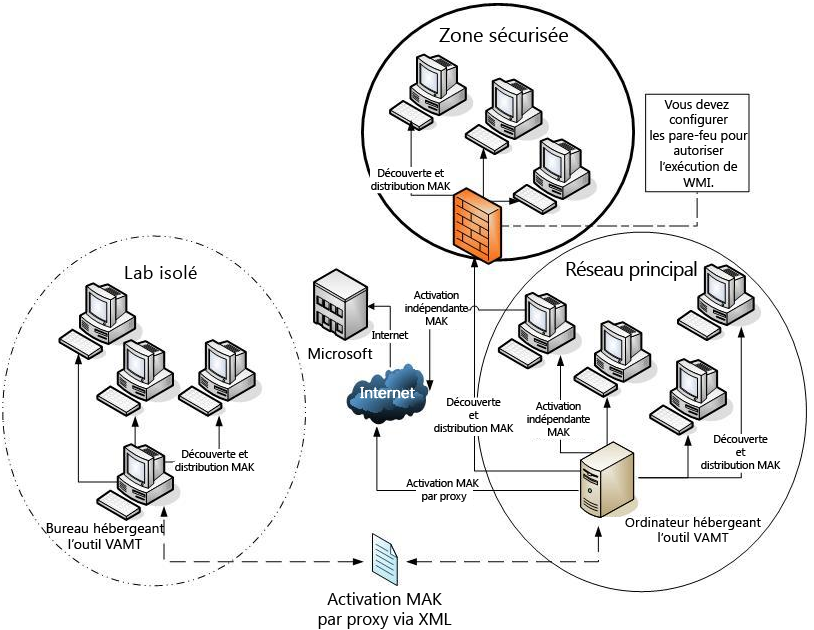


Figure 3. Environnements d’entreprise

Dans l’environnement du réseau principal, tous les ordinateurs se trouvent dans un réseau commun géré par AD DS. La zone sécurisée représente des ordinateurs du réseau principal de sécurité plus élevée qui disposent d’une protection de pare-feu supplémentaire.

L’environnement de laboratoire isolé est un groupe de travail physiquement isolé du réseau principal, et ses ordinateurs ne disposent pas d’accès Internet. La stratégie de sécurité réseau stipule qu’aucune information pouvant identifier un utilisateur ou un ordinateur spécifique ne peut être transférée en dehors du laboratoire isolé.

### Activation indépendante MAK

L’outil VAMT permet d’automatiser le déploiement et l’activation de MAK sur le réseau en distribuant les clés MAK à partir d’une console centralisée, comme illustré à la Figure 2. VAMT interroge les serveurs d’activation Microsoft pour obtenir le nombre d’activations restantes pour une clé MAK donnée, puis indique l’état d’activation de tous les systèmes activés par MAK dans l’environnement. Ce décompte est un instantané capturé à un instant t, et non un décompte en temps réel. L’outil VAMT version 1.2 est inclus dans Windows AIK.

Dans ce scénario, le VAMT est déployé dans l’environnement du réseau principal illustré en Figure 3. Le VAMT est installé sur un ordinateur central disposant d’un accès réseau à tous les ordinateurs clients. L’hôte VAMT et les ordinateurs clients ont un accès Internet. Les instructions suivantes décrivent la procédure d’activation indépendante :

1. Installez et lancez le VAMT sur un ordinateur hôte en réseau :
   1. Installez Windows AIK sur l’ordinateur hôte.
   2. Cliquez sur Démarrer, puis sur **VAMT** pour ouvrir la console VAMT.
2. Configurez l’exception de pare-feu WMI (Windows Management Instrumentation) sur les ordinateurs cibles. Assurez-vous que l’exception de pare-feu WMI a été activée pour tous les ordinateurs cibles, comme indiqué en Figure 4.

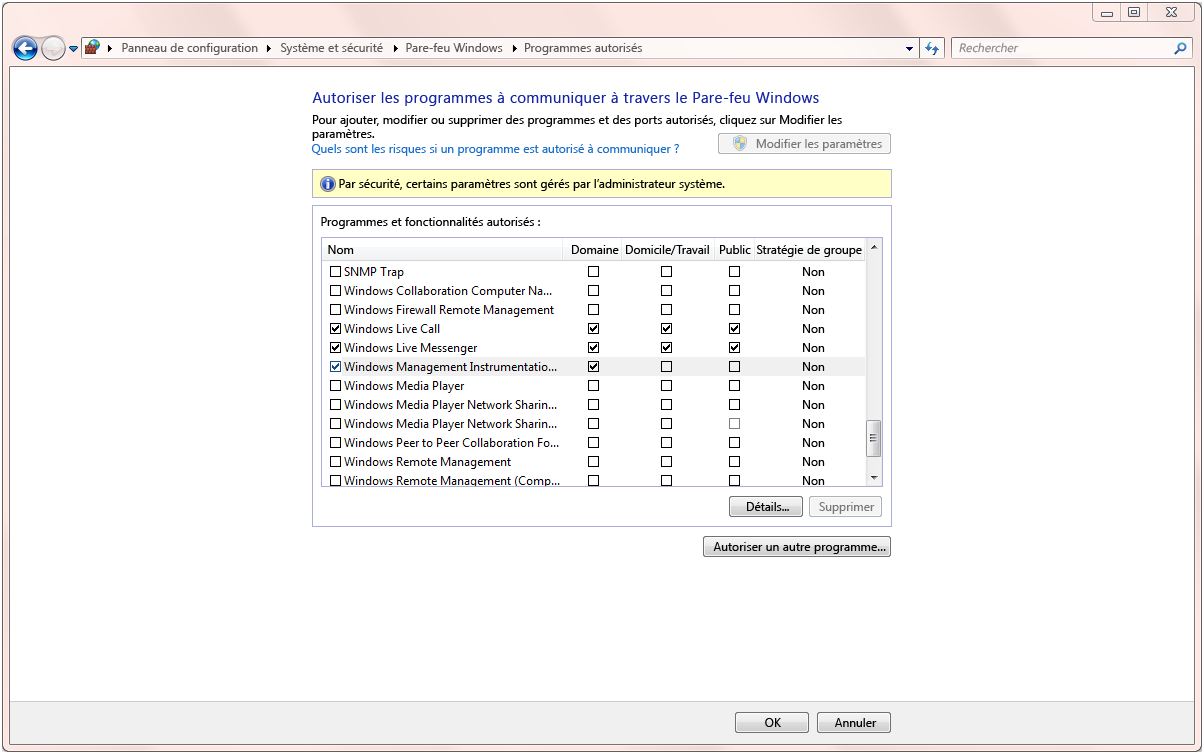


Figure 4. Exception WMI (Windows Management Instrumentation)

1. Ajoutez des ordinateurs à la liste d’informations sur l’ordinateur (CIL) :
   1. Dans la console VAMT, cliquez sur **Action**, puis sur **Ajouter des ordinateurs** pour afficher la boîte de dialogue **Ajouter des ordinateurs**.
   2. Entrez un nom de groupe d’ordinateurs tel que *Groupe du réseau principal* pour identifier le groupe d’ordinateurs que vous activez.
   3. Cliquez dans la liste déroulante pour sélectionner une option de recherche. Vous pouvez rechercher des ordinateurs dans un groupe de travail, dans un domaine AD DS, ou par nom d’ordinateur individuel ou adresse IP.
   4. Si vous effectuez une recherche par nom d’ordinateur individuel ou adresse IP, entrez ces informations dans la zone de texte située sous la liste déroulante.
   5. Si vous recherchez un domaine ou un groupe de travail, sélectionnez le domaine ou le groupe de travail à partir de la liste déroulante qui s’affiche pour ces options. Utilisez le champ **Filtrer par nom d’ordinateur** pour recherche un ordinateur spécifique dans le domaine ou le groupe de travail.
   6. Cliquez sur **OK**.

Le VAMT interroge les services de domaine Active Directory (AD DS) via le protocole LDAP (Lightweight Directory Access Protocol) et ajoute les ordinateurs qu’il trouve à la CIL.

1. Collectez les informations d’état des ordinateurs trouvés :
   1. Pour que le VAMT effectue une action sur un ordinateur, il doit disposer de données d’état de licence actuelles pour cet ordinateur. Collectez l’état des ordinateurs individuels en sélectionnant directement un ou plusieurs ordinateurs dans le volet d’affichage de liste des ordinateurs. Pour effectuer des opérations pour un groupe entier, dans le volet de l’arborescence, sélectionnez le nœud État inconnu ou le nœud Groupes définis par l’utilisateur\Groupe du réseau principal.
   2. Cliquez avec le bouton droit de la souris sur le groupe des ordinateurs de votre choix, puis cliquez sur **Actualiser l’état des ordinateurs**.
   3. Si vous activez des ordinateurs qui requièrent des informations d’identification de l’administrateur différentes de celles que vous utilisez actuellement, sélectionnez **Utiliser d’autres informations d’identification**.
   4. Cliquez sur **OK**.
   5. Indiquez un compte Administrateur de domaine (pour collecter l’état de tous les ordinateurs du domaine) et le mot de passe afférent lorsque vous y êtes invité.

Le VAMT affiche la boîte de dialogue **Collecte des informations sur l’ordinateur** pendant qu’il collecte l’état de tous les ordinateurs sélectionnés. Une fois le processus terminé, l’état actualisé de chaque ordinateur apparaît dans le volet d’affichage de liste des ordinateurs de la console VAMT.

**Remarque**   Pour connaître l’état de licence des ordinateurs sélectionnés, le VAMT doit disposer des autorisations administratives sur les ordinateurs distants, et WMI doit être accessible via le pare-feu Windows. En outre, pour les ordinateurs du groupe de travail, une clé de registre doit être créée pour permettre des actions administratives distantes sous contrôle de compte d’utilisateur (UAC). Pour plus d’informations sur la configuration des systèmes pour la gestion distante du VAMT, reportez-vous à l’aide du VAMT.

1. Ajoutez une MAK, et déterminez son nombre d’activations restantes :
   1. Cliquez sur **Options**, puis sur **Gérer les MAK** pour ouvrir la boîte de dialogue **Gérer les clés MAK**.
   2. Cliquez sur **Ajouter** pour entrer une MAK.
   3. Entrez la MAK puis cliquez sur **Valider**.

Une fois validée, le champ **Édition** est automatiquement renseigné.

* 1. Entrez une description détaillée puis cliquez sur **Ajouter**.

La MAK apparaît désormais dans la boîte de dialogue **Gérer les clés MAK**.

* 1. Cliquez sur **Actualiser le nombre restant** pour connaître le nombre d’activations restantes des MAK répertoriées de Microsoft. (Cette étape requiert une connexion Internet.)
  2. Cliquez sur **Quitter** pour fermer la boîte de dialogue.

1. Installez la MAK et activez les ordinateurs clients :
   1. Sélectionnez les ordinateurs à activer soit en cliquant sur un groupe dans le volet d’affichage de l’arborescence, soit en sélectionnant des ordinateurs individuels dans le volet d’affichage de liste.
   2. Cliquez avec le bouton droit de la souris sur le groupe ou les ordinateurs sélectionné(s), puis cliquez sur **Activation indépendante MAK** pour afficher la boîte de dialogue **Activation indépendante MAK**.
   3. Sélectionnez la MAK appropriée à partir de la liste **Installer une MAK**.
   4. Cochez les cases **Installer une MAK (remplacer la clé existante)** et **Activer maintenant** pour demander aux ordinateurs sélectionnés de procéder immédiatement à l’activation en contactant le service d’activation Microsoft Windows via Internet.

Si un astérisque (\*) apparaît près du texte de ces cases, l’action s’appliquera uniquement aux ordinateurs applicables. Par exemple, un ordinateur doté d’une version commerciale de Windows Vista ne peut pas être activé à l’aide d’une MAK.

* 1. Si vous activez des ordinateurs qui requièrent des informations d’identification de l’administrateur différentes de celles que vous utilisez actuellement, sélectionnez **Utiliser d’autres informations d’identification**.
  2. Cliquez sur **OK**.

VAMT affiche la boîte de dialogue **Attribution de clés de produit**, puis la boîte de dialogue **Activation d’ordinateurs** jusqu’à ce qu’il termine l’action demandée. Si vous avez sélectionné **Utiliser d’autres informations d’identification**, vous serez invité à entrer les informations d’identification avant ces boîtes de dialogue.

### Activation MAK par proxy

Dans ce scénario, le VAMT est utilisé pour activer les ordinateurs du groupe de travail dans l’environnement de laboratoire isolé illustré en Figure 3. Pour des groupes de travail tels que celui-ci, qui sont complètement isolés du réseau plus important, vous pouvez effectuer une activation MAK par proxy en installant un deuxième VAMT sur un ordinateur dans le groupe de travail isolé et en utilisant un support amovible pour transférer les CIL du VAMT entre cet ordinateur et un autre hôte VAMT disposant d’un accès Internet. Pour plus d’informations sur la configuration des systèmes pour la gestion distante du VAMT, reportez-vous à l’aide du VAMT. Les étapes suivantes décrivent la procédure d’utilisation de l’outil VAMT pour une activation par proxy :

1. Installez un VAMT sur un ordinateur du groupe de travail dans le laboratoire isolé :
   1. Installez Windows AIK sur un ordinateur hôte dans le groupe de travail du laboratoire isolé.

Cet ordinateur peut exécuter Windows XP Service Pack 2 (SP2), Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2.

* 1. Cliquez sur Démarrer, puis sur **VAMT** pour ouvrir la console VAMT.
  2. Configurez l’exception de pare-feu WMI (Windows Management Instrumentation ) sur les ordinateurs cibles. Assurez-vous que l’exception de pare-feu WMI a été activée pour tous les ordinateurs cibles.

1. Ajoutez des ordinateurs à la CIL :
   1. Dans la console VAMT, cliquez sur **Action**, puis sur **Ajouter des ordinateurs** pour ouvrir la boîte de dialogue **Ajouter des ordinateurs**.
   2. Entrez un nom de groupe tel que *Groupe du laboratoire isolé* pour identifier le groupe d’ordinateurs que vous activez.
   3. Sélectionnez l’option **Groupe de travail**, et spécifiez le nom du groupe de travail puis cliquez sur **OK**.

Le VAMT recherche le groupe de travail des ordinateurs.

**Remarque**   Pour que le VAMT trouve les ordinateurs clients dans un groupe de travail, l’exception du pare-feu Windows de découverte du réseau doit être activée.

1. Collectez l’état des ordinateurs trouvés :
   1. Pour que le VAMT effectue une action sur un ordinateur, il doit disposer de données d’état de licence actuelles pour cet ordinateur. Collectez l’état des ordinateurs individuels en sélectionnant directement un ou plusieurs ordinateurs dans le volet d’affichage de liste des ordinateurs. Pour effectuer des opérations pour un groupe entier, dans le volet de gauche, sélectionnez le nœud État inconnu ou le nœud Groupes définis par l’utilisateur\Groupe du laboratoire isolé.
   2. Cliquez avec le bouton droit de la souris sur le groupe des ordinateurs de votre choix, puis cliquez sur **Actualiser l’état des ordinateurs**.
   3. Si vous activez des ordinateurs qui requièrent des informations d’identification de l’administrateur différentes de celles que vous utilisez actuellement, sélectionnez **Utiliser d’autres informations d’identification**.
   4. Cliquez sur **OK**. Lorsque vous y êtes invité, fournissez les informations d’identification d’un compte disposant de droits administratifs locaux pour les ordinateurs du groupe de travail sélectionnés.

Le VAMT affiche la boîte de dialogue **Collecte des informations sur l’ordinateur** pendant qu’il collecte l’état de tous les ordinateurs sélectionnés. Une fois le processus terminé, l’état actualisé de chaque ordinateur apparaît dans le volet d’affichage de liste des ordinateurs de la console VAMT.

**Remarque**   Pour connaître l’état de licence des ordinateurs sélectionnés, le VAMT doit disposer des autorisations administratives sur les ordinateurs distants, et WMI doit être accessible via le pare-feu Windows. En outre, pour les ordinateurs du groupe de travail, une clé de registre doit être créée pour permettre des actions administratives distantes sous UAC.

1. Ajoutez une MAK :
   1. Cliquez sur **Options**, puis sur **Gérer les MAK** pour ouvrir la boîte de dialogue **Gérer les clés MAK**.
   2. Cliquez sur **Ajouter** pour entrer une MAK.
   3. Entrez la MAK puis cliquez sur **Valider**.

Une fois validée, le champ **Édition** est automatiquement renseigné.

* 1. Entrez une description détaillée puis cliquez sur **Ajouter**.

La MAK apparaît désormais dans la boîte de dialogue **Gérer les clés MAK**.

* 1. Cliquez sur **Quitter** pour fermer la boîte de dialogue.

**Remarque**   Dans la mesure où le VAMT n’est pas installé sur un ordinateur disposant d’un accès Internet, l’option **Actualiser le nombre restant** ne fonctionnera pas. Cette fonctionnalité requiert un accès Internet.

1. Installez la MAK sur les ordinateurs du laboratoire isolé :
   1. Sélectionnez le groupe du laboratoire isolé dans le volet de l’arborescence.
   2. Cliquez avec le bouton droit de la souris sur le groupe sélectionné, puis cliquez sur **Activation MAK par proxy** pour afficher la boîte de dialogue **Activation MAK par proxy**.
   3. Sélectionnez la MAK appropriée à partir de la liste **Installer une MAK**.
   4. Sélectionnez **Installer une MAK (remplacer la clé existante)**.

Si un astérisque (\*) apparaît près du texte de cette case, l’action s’appliquera uniquement aux ordinateurs applicables. Par exemple, un ordinateur doté d’une version commerciale de Windows Vista ne peut pas être activé à l’aide d’une MAK.

* 1. Décochez la case **Obtenir un ID de confirmation de Microsoft**, car cet ordinateur ne dispose pas d’accès Internet.
  2. Décochez la case **Appliquer l’ID de confirmation et activer**, car les ID de confirmation (CID) n’ont pas encore été demandés.
  3. Si vous activez des ordinateurs qui requièrent des informations d’identification de l’administrateur différentes de celles que vous utilisez actuellement, sélectionnez **Utiliser d’autres informations d’identification**, puis cliquez sur **OK**.

VAMT affiche la boîte de dialogue **Attribution de clés de produit** jusqu’à ce qu’il termine l’action demandée. Si vous avez sélectionné **Utiliser d’autres informations d’identification**, vous serez invité à entrer les informations d’identification avant cette boîte de dialogue.

**Remarque**   La sélection de la case **Installer une MAK (remplacer la clé existante)** entraîne l’installation d’une MAK sur un ordinateur client. Cette opération doit être effectuée avec précaution. Si la version antérieure au SP1 de Windows Vista a été installée sur l’ordinateur pendant plus de 30 jours, alors sa période de grâce initiale a expiré, et l’ordinateur entrera en mode de fonctionnalités réduites (RFM) si aucune activation n’est effectuée avant la prochaine ouverture de session. Toutefois, vous pouvez utiliser une activation MAK par proxy pour restaurer les ordinateurs correctement configurés du mode de fonctionnalités réduites tant que les ordinateurs sont accessibles à l’hôte VAMT. Le mode RFM ne s’applique qu’à la version antérieure au SP1 de Windows Vista. Windows Vista SP1, ou version ultérieure, Windows 7, Windows Server 2008 ou Windows Server 2008 R2 n’entrera pas en mode RFM.

1. Enregistrez la CIL :

Dans cette étape, la CIL entière est enregistrée sur l’hôte local (à savoir, le groupe de travail). Dans une activation MAK par proxy, il est essentiel de conserver ce fichier car le VAMT l’utilise pour appliquer les CID aux ordinateurs correspondants.

* 1. À l’aide du volet d’affichage de liste ou d’arborescence du VAMT, sélectionnez le groupe ou les ordinateurs individuels qui ont bien reçu une MAK.
  2. À partir du menu **Fichier**, cliquez sur **Enregistrer** pour afficher la boîte de dialogue **Enregistrer la liste d’informations sur l’ordinateur**.
  3. Sélectionnez un répertoire puis entrez le nom d’un fichier CIL tel que *GroupeLaboratoireIsolé.CIL.*
  4. Cliquez sur **Enregistrer**.

1. Exportez la CIL :

Comme précédemment mentionné, la stratégie de sécurité d’entreprise stipule qu’aucune information pouvant identifier un utilisateur ou un ordinateur spécifique ne peut être transférée en dehors du laboratoire isolé. Ainsi, ce type de données doit être exclu du fichier CIL pour être transféré vers l’hôte VAMT du réseau principal.

* 1. À l’aide du volet d’affichage de liste ou d’arborescence du VAMT, sélectionnez le groupe ou les ordinateurs individuels qui ont bien reçu une MAK.
  2. Cliquez avec le bouton droit de la souris sur le groupe ou les ordinateurs sélectionné(s), puis cliquez sur **Exporter des ordinateurs** pour afficher la boîte de dialogue **Enregistrer la liste d’informations sur l’ordinateur**.
  3. Sélectionnez **Exclure toutes les données d’environnement sensibles**.
  4. Cliquez sur **Parcourir** pour afficher la boîte de dialogue **Enregistrer sous**.
  5. Sélectionnez un répertoire puis entrez le nom d’un fichier CIL tel que *ExportSécuriséGroupeLaboratoireIsolé.CIL.*
  6. Cliquez sur **Enregistrer**.
  7. Copiez le fichier ExportSécuriséGroupeLaboratoireIsolé.CIL sur un support amovible (lecteur de disque, CD/DVD ou lecteur flash USB [UFD]).

**Remarque**   Le fait de cocher la case **Exclure toutes les données d’environnement sensibles** exclut les informations personnellement identifiables (PII) d’être enregistrées dans la CIL. Par conséquent, la CIL doit être ré-importée dans cet hôte VAMT et dans le fichier CIL d’enregistrement complet de sorte que les CID demandés auprès de Microsoft puissent être correctement attribués aux ordinateurs dans le groupe Laboratoire isolé.

1. Importez la CIL sur un hôte VAMT disposant d’un accès Internet :
   1. Copiez le fichier ExportSécuriséGroupeLaboratoireIsolé.CIL du support amovible sur un lecteur sur un hôte VAMT disposant d’un accès Internet.
   2. Ouvrez la console VAMT.
   3. À partir du menu **Fichier**, cliquez sur **Importer** pour ouvrir la boîte de dialogue **Ouvrir la liste d’informations sur l’ordinateur**.
   4. Repérez et sélectionnez le fichier **ExportSécuriséGroupeLaboratoireIsolé.CIL**, puis cliquez sur **Ouvrir** pour charger la CIL dans le VAMT.
   5. Confirmez que les noms de l’ordinateur, du groupe et du groupe de travail ne sont pas visibles.
2. Demandez les CID auprès de Microsoft :
   1. Cliquez avec le bouton droit de la souris sur les ordinateurs importés, puis cliquez sur **Activation MAK par proxy** pour ouvrir la boîte de dialogue **Activation MAK par proxy**.
   2. Désélectionnez **Installer une MAK (remplacer la clé existante)**.
   3. Décochez la case **Obtenir un ID de confirmation de Microsoft**.
   4. Décochez la case **Appliquer l’ID de confirmation et activer**, car cet hôte VAMT ne se trouve pas sur le même réseau que les ordinateurs sélectionnés.
   5. Cliquez sur **OK**.

Le VAMT affiche la boîte de dialogue **Acquisition d’un ID de confirmation en ligne** pendant qu’il contacte Microsoft et collecte les CID.

1. Exportez la CIL de l’hôte VAMT connecté à Internet :
   1. Une fois les CID récupérés de tous les ordinateurs, enregistrez le fichier CIL. Dans la console VAMT, faites défiler vers la droite et vérifiez que la colonne **CID en attente** contient des valeurs.
   2. À partir du menu **Fichier**, cliquez sur **Enregistrer sous**, et indiquez un nouveau nom pour le fichier, tel que *ExportSécuriséGroupeLaboratoireIsoléAvecCID.CIL.*
   3. Copiez le fichier ExportSécuriséGroupeLaboratoireIsoléAvecCID.CIL sur un support amovible (lecteur de disque, CD/DVD ou UFD).
2. Importez la CIL sur l’hôte VAMT original dans le Laboratoire isolé :
   1. Copiez le fichier ExportSécuriséGroupeLaboratoireIsoléAvecCID.CIL du support amovible sur un lecteur sur l’hôte VAMT dans le Laboratoire isolé.
   2. Ouvrez la console VAMT.
   3. À partir du menu **Fichier**, cliquez sur **Ouvrir** pour afficher la boîte de dialogue **Ouvrir la liste d’informations sur l’ordinateur**.
   4. Repérez et sélectionnez le fichier GroupeLaboratoireIsolé.CIL, puis cliquez sur **Ouvrir** pour charger la CIL dans le VAMT.

Cette opération permet d’afficher les ordinateurs précédemment découverts ainsi que leurs états de licence dans le volet d’affichage de liste des ordinateurs.

* 1. À partir du menu **Fichier**, cliquez sur **Importer** et recherchez le fichier contenant les CID (ExportSécuriséGroupeLaboratoireIsoléAvecCID.CIL).

Cette opération déclenche le processus de fusion qui associe les CID aux IID des ordinateurs.

* 1. À partir du menu **Fichier**, cliquez sur **Enregistrer**, puis entrez un nom de fichier tel que *GroupeLaboratoireIsoléAvecCID.CIL* pour enregistrer ce fichier qui associe les IID aux CID correspondants.

**Important**   L’enregistrement de ce fichier est essentiel pour les scénarios de réimagerie. Il vous est fortement recommandé de faire une copie de ce fichier et de protéger celle-ci en écriture.

1. Appliquez les CID, et activez les ordinateurs du Laboratoire isolé :
   1. Cliquez avec le bouton droit de la souris sur le groupe Laboratoire isolé dans le volet d’affichage de l’arborescence, puis cliquez sur **Activer une MAK par proxy** pour ouvrir la boîte de dialogue **Activer une MAK par proxy**.
   2. Décochez la case **Installer une MAK (remplacer la clé existante)**, car une MAK est déjà installée sur les ordinateurs sélectionnés.
   3. Décochez la case **Obtenir un ID de confirmation de Microsoft**.
   4. Cochez la case **Appliquer l’ID de confirmation et activer** pour demander au VAMT d’activer les ordinateurs sélectionnés en installant leurs CID.
   5. Cliquez sur **OK**.

Le VAMT affiche la boîte de dialogue **Attribution des ID de confirmation** pendant qu’il installe les CID sur les ordinateurs sélectionnés.

1. En outre, réactivez les ordinateurs réimagés dans le Laboratoire isolé :

Si les ordinateurs dans le Laboratoire isolé ont été réimagés mais que le matériel sous-jacent n’a pas changé, le VAMT peut les réactiver à l’aide du fichier GroupeLaboratoireIsoléAvecCID.CIL.

* 1. Redéployez Windows sur chaque ordinateur à l’aide des mêmes noms d’ordinateurs qu’auparavant.
  2. Ouvrez la console VAMT sur l’hôte VAMT local (groupe de travail).
  3. À partir du menu **Fichier**, cliquez sur **Ouvrir**, puis sélectionnez le fichier GroupeLaboratoireIsoléAvecCID.CIL.
  4. Dans le volet d’affichage de l’arborescence, cliquez avec le bouton droit de la souris sur le groupe **Laboratoire isolé**, puis cliquez sur **Réappliquer l’ID de confirmation** pour afficher la boîte de dialogue **Réactivation MAK par proxy**.
  5. Laissez la case **Installer une MAK (remplacer la clé existante)** cochée, et assurez-vous que la MAK précédemment utilisée est sélectionnée dans la liste.
  6. Laissez la case **Réappliquer l’ID de confirmation et réactiver** cochée pour réappliquer les CID stockés du fichier GroupeLaboratoireIsoléAvecCID.CIL.
  7. Laissez la case **Requérir la correspondance IID exacte** cochée si le matériel n’a pas changé depuis l’activation MAK par proxy initiale et si vous utilisez la même MAK pour réactiver l’ordinateur.

Décochez cette case si le matériel a changé mais que vous souhaiteriez encore que VAMT tente une réactivation à l’aide du CID précédemment stocké. Notez que la réactivation de Windows peut échouer dans ce scénario.

* 1. Si vous activez un ordinateur qui requiert des informations d’identification de l’administrateur différentes de celles que vous utilisez actuellement, cochez la case **Utiliser d’autres informations d’identification**.
  2. Cliquez sur **OK**.

Le VAMT affiche la boîte de dialogue **Attribution de clés de produit** pendant qu’il applique la MAK au Groupe de Laboratoire isolé.

Le VAMT affiche la boîte de dialogue **Attribution des ID de confirmation** pendant qu’il installe les CID sur les ordinateurs sélectionnés.

**Remarque**La sélection de la case **Installer une MAK (remplacer la clé existante)** entraîne l’installation d’une MAK. Cette opération doit être effectuée avec précaution. Si la version antérieure au SP1 de Windows Vista a été installée pendant plus de 30 jours, alors sa période de grâce initiale a expiré, et l’ordinateur entrera en mode RFM si aucune activation n’est effectuée avant la prochaine ouverture de session. Le VAMT peut être utilisé pour restaurer les ordinateurs distants correctement configurés du mode RFM tant qu’ils sont accessibles sur le réseau. Le mode RFM ne s’applique qu’à la version antérieure au SP1 de Windows Vista. Windows Vista SP1, ou version ultérieure, Windows 7, Windows Server 2008 ou Windows Server 2008 R2 n’entrera pas en mode RFM.

### Prise en charge du VAMT pour l’activation KMS

Dans ce scénario, le VAMT est utilisé pour installer et activer des clés de clients KMS sur les ordinateurs du réseau principal ou du Laboratoire isolé. La procédure décrite ci-après suppose que le VAMT a été installé et que les ordinateurs ont été ajoutés à la CIL. Ces tâches sont décrites dans les étapes 1 à 4 dans le Scénario 1 (pour le réseau principal) ou le Scénario 2 (pour le groupe de travail du Laboratoire isolé).

1. Ouvrez la console VAMT.
2. Sélectionnez les ordinateurs à activer soit en cliquant sur un groupe dans le volet d’affichage de l’arborescence, soit en sélectionnant des ordinateurs individuels dans le volet d’affichage de liste.
3. Cliquez avec le bouton droit de la souris sur le groupe ou les ordinateurs sélectionné(s), puis cliquez sur **Configuration pour l’activation KMS** pour afficher la boîte de dialogue **Configuration KMS**.
4. Sélectionnez **Installer une clé de client KMS (remplacer la clé existante)** pour demander au VAMT d’installer une clé de client KMS sur un ordinateur client.
5. Sélectionnez l’option d’activation appropriée :

* **Découverte automatique d’hôte KMS à l’aide de DNS.** Le VAMT supprime dans un premier temps tout hôte KMS précédemment configuré sur l’ordinateur cible, puis demande à l’ordinateur d’interroger DNS pour repérer un hôte KMS et tenter une activation.
* **Utilisation d’un port et d’un hôte KMS spécifiques.** Le VAMT définit le port et le nom d’hôte KMS spécifiques sur l’ordinateur cible, puis demande à l’ordinateur de tenter une activation avec cet hôte KMS spécifique.

1. Si vous activez des ordinateurs qui requièrent des informations d’identification de l’administrateur différentes de celles que vous utilisez actuellement, cochez la case **Utiliser d’autres informations d’identification**, puis cliquez sur **OK**.

Le VAMT affiche la boîte de dialogue **Attribution de clés de produit**, puis la boîte de dialogue **Activation d’ordinateurs** jusqu’à ce qu’il termine l’action demandée. Si vous avez coché la case **Utiliser d’autres informations d’identification**, vous serez invité à entrer les informations d’identification avant ces boîtes de dialogue.

### Conversion de clients KMS en activation MAK

Windows 7 et Windows Server 2008 R2 s’installent automatiquement en tant que clients KMS. Pour convertir un client KMS en activation MAK, installez une clé MAK. Vous pouvez installer une clé MAK pendant l’installation du système d’exploitation ou à tout moment par la suite.

Vous pouvez installer une clé MAK sur une image de référence de Windows 7 et de Windows Server 2008 R2 pour que toutes les installations effectuées depuis cette image utilisent l’activation MAK plutôt que l’activation KMS par défaut. Cette opération élimine la nécessité de spécifier une clé MAK dans un fichier d’installation sans assistance.

#### Installation d’une clé MAK pendant l’installation du système d’exploitation

Vous pouvez convertir un client KMS en client MAK pendant l’installation initiale de Windows 7 ou de Windows Server 2008 R2 en incluant une clé MAK dans un fichier d’installation sans assistance (Unattend.xml). Le fichier Unattend.xml est utilisable avec Setup.exe ou avec les services de déploiement Windows. Pour plus d’informations, reportez-vous au fichier d’aide (en anglais) Unattended Windows Setup Reference (Guide de référence de l’installation sans assistance utilisateur de Windows) de Windows AIK, accessible à l’adresse <http://go.microsoft.com/fwlink/?LinkId=136976>.

**Remarque**   La clé MAK est stockée en texte clair dans le fichier Unattend.xml. Lors d’une installation sans assistance, le fichier Unattend.xml ou AutoUnattend.xml est copié dans le dossier %SystemRoot%\Panther de l’ordinateur cible. Toutefois, à la fin du processus d’installation, le programme remplace cette information par la mention « SENSITIVE\*DATA\*DELETED ».

#### Installation d’une clé MAK après l’installation du système d’exploitation

Vous pouvez configurer une édition en volume de Windows 7 ou de Windows Server 2008 R2 pour utiliser l’activation MAK à l’aide de l’option Système du Panneau de configuration ou en exécutant le script Slmgr.vbs :

* Pour installer une clé MAK à l’aide de l’application Système, cliquez sur le lien **Changer la clé du produit**, puis tapez la clé MAK dans la boîte de dialogue **Changer de clé de produit pour l’activation**.
* Pour installer une clé MAK par le biais du script Slmgr.vbs, exécutez la commande ci-après à partir d’une invite de commandes :

slmgr.vbs /ipk <CléActivationMultiple>

où CléActivationMultiple correspond à la clé MAK.

Si les utilisateurs installent une clé MAK à l’aide de l’interface utilisateur, le client MAK tente de s’activer une seule fois sur Internet. En cas d’installation d’une clé MAK au moyen du script Slmgr.vbs, le client MAK ne tente pas de s’activer automatiquement. L’utilisateur peut utiliser **Slmgr.vbs /ato** pour activer manuellement la MAK sur Internet.

# Clés d’hôte KMS de produits

Le tableau 7 décrit les produits que chaque hôte KMS peut activer.

Tableau 7. Clés d’hôtes KMS associées aux produits qu’elles activent

| **Groupe de produits en volume** | **Produits Windows** | **Type de clé** | **Produits activés par type de clé** |
| --- | --- | --- | --- |
| Windows Vista | Windows Vista Professionnel  Windows Vista Entreprise | KMS | Windows Vista Professionnel  Windows Vista Entreprise |
| Windows 7 | Windows 7 Professionnel  Windows 7 Entreprise | KMS | Windows Vista Professionnel  Windows Vista Entreprise  Windows 7 Professionnel  Windows 7 Entreprise |
| Windows Server 2008 R2  Groupe de serveurs A : | Windows Web Server® 2008 R2  Windows Server 2008 R2 Édition HPC  Windows HPC Server 2008 R2 | KMS\_A | Groupe A pour Windows Server 2008 R2  Groupe A pour Windows Server 2008  Éditions en volume de Windows Vista  Éditions en volume de Windows 7 |
| Windows Server 2008 R2  Groupe de serveurs B | Windows Server 2008 R2 Standard  Windows Server 2008 R2 Entreprise | KMS\_B | Groupe A pour Windows Server 2008 R2  Groupe A pour Windows Server 2008  Groupe B pour Windows Server 2008 R2  Groupe B pour Windows Server 2008  Éditions en volume de Windows Vista  Éditions en volume de Windows 7 |
| Windows Server 2008 R2  Groupe de serveurs C | Windows Server 2008 R2 Datacenter  Windows Server 2008 R2 pour les systèmes Itanium | KMS\_C | Groupe A pour Windows Server 2008 R2  Groupe A pour Windows Server 2008  Groupe B pour Windows Server 2008 R2  Groupe B pour Windows Server 2008  Groupe C pour Windows Server 2008 R2  Groupe C pour Windows Server 2008  Éditions en volume de Windows Vista  Éditions en volume de Windows 7 |
| Les clés KMS de Windows Server 2008 R2 suivent la même hiérarchie (groupes A, B, C) que Windows Server 2008 avec en plus Windows Server 2008 Datacenter sans Hyper-V™, Windows Server 2008 Enterprise sans Hyper-V, et Windows Server 2008 Standard sans Hyper-V. La principale différence est que les clés KMS de Windows Server 2008 R2 peuvent être utilisées pour activer un hôte KMS qui activera à son tour Windows Server 2008, Windows 7 et Windows Vista.  Les clés de Windows Server 2008 et Windows Vista ne peuvent pas activer les systèmes Windows 7 ou Windows Server 2008 R2. | | | |

# Valeurs de stratégie d’activation

Le tableau 8 répertorie les valeurs de stratégie pour Windows 7 et Windows Server 2008 R2.

Tableau 8. Valeurs de stratégie Windows 7 et Windows Server 2008 R2

| **Élément** | **Valeur Client** | **Valeur Serveur** | **Champ d’application** |
| --- | --- | --- | --- |
| Limite de réarmement | 3 | 3 | Non configurable |
| Seuil du nombre de clients KMS | 25 | 5 | Non configurable |
| Durée d’activation KMS | 180 jours | 180 jours | Non configurable |
| Port d’écoute de l’hôte KMS | 1688 | 1688 | Tout port TCP ouvert |
| Période de grâce OOB | 30 jours | 30 jours | Non configurable |
| Période de grâce OOT | 30 jours | 30 jours | Non configurable |
| Réactivation du client KMS (en minutes) | 10 080 minutes  (7 jours - par défaut) | 10 080 minutes  (7 jours - par défaut) | 15-43 200 minutes  (30 jours - par défaut) |
| Intervalle avant nouvelle tentative, en cas d’échec d’activation KMS | 120 minutes | 120 minutes | 15-43 200 minutes  (120 minutes - par défaut) |

# Clés d’installation de client KMS

Par défaut, les systèmes d’exploitation Windows 7 et Windows Server 2008 R2 utilisent KMS pour l’activation. Dans les installations en volume, la clé d’installation est installée par défaut, faisant du système un client KMS. Si vous convertissez un ordinateur d’un hôte KMS, d’une MAK ou d’une version commerciale de Windows en un client KMS, installez la clé d’installation applicable (GVLK) indiquée au Tableau 9 à l’aide de **slmgr /ipk <clé d’installation>**.

Tableau 9. Clés d’installation de client KMS

| **Plateforme** | **Édition du système d’exploitation** | **Clé de produit** |
| --- | --- | --- |
| **Windows 7 et Windows Server 2008 R2** | | |
| Client | Windows 7 Professionnel | FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4 |
| Client | Windows 7 Professionnel N | MRPKT-YTG23-K7D7T-X2JMM-QY7MG |
| Client | Windows 7 Professionnel E | W82YF-2Q76Y-63HXB-FGJG9-GF7QX |
| Client | Windows 7 Entreprise | 33PXH-7Y6KF-2VJC9-XBBR8-HVTHH |
| Client | Windows 7 Entreprise N | YDRBP-3D83W-TY26F-D46B2-XCKRJ |
| Client | Windows 7 Entreprise E | C29WB-22CC8-VJ326-GHFJW-H9DH4 |
| Serveur | Windows Web Server 2008 R2 | 6TPJF-RBVHG-WBW2R-86QPH-6RTM4 |
| Serveur | Windows Server 2008 R2 Édition HPC | FKJQ8-TMCVP-FRMR7-4WR42-3JCD7 |
| Serveur | Windows Server 2008 R2 Standard | YC6KT-GKW9T-YTKYR-T4X34-R7VHC |
| Serveur | Windows Server 2008 R2 Entreprise | 489J6-VHDMP-X63PK-3K798-CPX3Y |
| Serveur | Windows Server 2008 R2 Datacenter | 74YFP-3QFB3-KQT8W-PMXWJ-7M648 |
| Serveur | Windows Server 2008 R2 pour les systèmes Itanium | GT63C-RJFQ3-4GMB6-BRFB9-CB83V |
| **Windows Vista et Windows Server 2008** | | |
| Client | Windows Vista Professionnel | YFKBB-PQJJV-G996G-VWGXY-2V3X8 |
| Client | Windows Vista Professionnel N | HMBQG-8H2RH-C77VX-27R82-VMQBT |
| Client | Windows Vista Entreprise | VKK3X-68KWM-X2YGT-QR4M6-4BWMV |
| Client | Windows Vista Entreprise N | VTC42-BM838-43QHV-84HX6-XJXKV |
| Serveur | Windows Web Server 2008 | WYR28-R7TFJ-3X2YQ-YCY4H-M249D |
| Serveur | Windows Server 2008 Standard | TM24T-X9RMF-VWXK6-X8JC9-BFGM2 |
| Serveur | Windows Server 2008 Standard sans Hyper-V | W7VD6-7JFBR-RX26B-YKQ3Y-6FFFJ |
| Serveur | Windows Server 2008 Entreprise | YQGMW-MPWTJ-34KDK-48M3W-X4Q6V |
| Serveur | Windows Server 2008 Entreprise sans Hyper-V | 39BXF-X8Q23-P2WWT-38T2F-G3FPG |
| Serveur | Windows Server 2008 Datacenter | 7M67G-PC374-GR742-YH8V4-TCBY3 |
| Serveur | Windows Server 2008 Datacenter sans Hyper-V | 22XQ2-VRXRG-P8D42-K34TD-G3QQC |
| Serveur | Windows Server 2008 pour les systèmes Itanium | 4DWFP-JF3DJ-B7DTH-78FJB-PDRHK |

# Codes d’erreur d’activation

Le tableau 10 fournit une aide pour résoudre des problèmes survenant lors de l’activation d’éditions en volume de systèmes d’exploitation Windows 7 et Windows Server 2008 R2.

Tableau 10. Codes d’erreur et descriptions

| **Code d’erreur** | **Message d’erreur** | **Type d’activation** | **Cause possible** | **Mesures de dépannage** |
| --- | --- | --- | --- | --- |
| 0xC004C001 | Le serveur d’activation a déterminé que la clé de produit spécifiée n’est pas valide. | MAK | La clé MAK saisie est non valide. | Vérifiez que la clé est bien la clé MAK fournie par Microsoft.  Contactez le [Centre d’appels d’activation Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx) pour vérifier la validité de la clé MAK. |
| 0xC004C003 | Le serveur d’activation a déterminé que la clé de produit spécifiée est bloquée. | MAK | La clé MAK est bloquée au niveau du serveur d’activation. | Contactez le [Centre d’appels d’activation Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx) pour obtenir une nouvelle clé MAK et installer / activer le système. |
| 0xC004C008 | Le serveur d’activation a déterminé que la clé de produit spécifiée ne pouvait pas être utilisée. | KMS | La clé KMS a dépassé la limite d’activation. | Les clés hôtes KMS permettent 10 activations au maximum, sur six ordinateurs différents. Si des activations supplémentaires sont requises, contactez le [Centre d’appels d’activation Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx). |
| 0xC004C020 | Le serveur d’activation a signalé que la limite de la clé d’activation multiple a été dépassée. | MAK | La clé MAK a dépassé la limite d’activation. | Les clés MAK disposent d’un nombre limité d’activations. Contactez le [Centre d’appels d’activation Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx). |
| 0xC004C021 | Le serveur d’activation a signalé que la limite de l’extension de la clé d’activation multiple a été dépassée. | MAK | La clé MAK a dépassé la limite d’activation. | Les clés MAK disposent d’un nombre limité d’activations. Contactez le [Centre d’appels d’activation Microsoft](http://www.microsoft.com/licensing/resources/vol/numbers.mspx). |
| 0xC004F009 | Le service de protection logicielle a signalé que la période de grâce a expiré. | MAK | La période de grâce a expiré avant activation du système. Ce dernier est à présent dans l’état de notification. | Voir la section «  ». |
| 0xC004F00F | Le service de licences logicielles a signalé que la liaison d’ID du matériel dépasse le niveau de tolérance. | Client MAK/KMS / hôte KMS | Le matériel a été modifié ou les pilotes ont été mis à jour sur le système. | **MAK :** Réactivez le système pendant la période de grâce Hors tolérance en recourant à une activation en ligne ou par téléphone.  **KMS :** Redémarrez, ou exécutez **slmgr.vbs /ato**. |
| 0xC004F014 | Le service de protection logicielle a signalé que la clé de produit n’est pas disponible. | Client MAK/KMS | Aucune clé de produit n’est installée sur le système. | Installez une clé de produit MAK ou une clé d’installation KMS disponible dans le fichier \sources\pid.txt du support d’installation. |
| 0xC004F02C | Le service de protection logicielle a signalé que le format des données d’activation hors connexion est incorrect. | Client MAK/KMS | Le système a détecté que les données saisies au cours de l’activation par téléphone ne sont pas valides. | Vérifiez que l’ID de confirmation (CID) est correctement saisi. |
| 0xC004F035 | Ce code d’erreur signifie « Le service de protection logicielle a signalé que l’ordinateur n’a pas pu être activé avec une clé de produit de licence en volume ». Le message d’erreur est correct mais ambigu.  Cette erreur indique qu’il manque un marqueur Windows dans le BIOS, fourni sur des systèmes OEM pour identifier les ordinateurs livrés avec des éditions qualifiantes de Windows, qui constitue une exigence pour l’activation de clients KMS.  Erreur : Clé de licence en volume non valide  Afin de procéder à l’activation, vous devez changer la clé de votre produit et passer à une clé d’activation multiple (MAK) ou à une clé de produit commercialisé.  Vous devez avoir une licence éligible pour le système d’exploitation ET une licence de mise à niveau en volume vers Windows 7 ou bien une licence complète provenant d’un revendeur.  TOUTE AUTRE INSTALLATION DE CE LOGICIEL CONSTITUE UNE VIOLATION DE VOTRE CONTRAT ET DE LA RÉGLEMENTATION RELATIVE AUX DROITS D’AUTEUR. | Client KMS / hôte KMS | Les éditions en volume de Windows 7 disposent de licence pour une mise à niveau uniquement. L’installation d’un système d’exploitation en volume sur un ordinateur qui ne possède pas un système d’exploitation éligible n’est pas prise en charge. | Installez une version éligible d’un système d’exploitation Microsoft, puis activez-la à l’aide d’une MAK. |
| 0xC004F038 | Le service de protection logicielle a signalé que l’ordinateur n’a pas pu être activé. Le compte indiqué par votre service Gestionnaire de clés (KMS) est insuffisant. Contactez votre administrateur système. | Client KMS | Le compte indiqué sur l’hôte KMS n’est pas assez élevé. Il doit être ≥ 5 pour Windows Server et ≥ 25 pour le client Windows. | Un nombre d’ordinateurs supérieur est requis dans le pool KMS afin que les clients KMS soient activés. Exécutez **Slmgr.vbs /dli** pour obtenir le nombre actuel sur l’hôte KMS. |
| 0xC004F039 | Le service de protection logicielle a signalé que l’ordinateur n’a pas pu être activé. Le service Gestionnaire de clés (KMS) est désactivé. | Client KMS | Cette erreur survient lorsqu’une demande KMS ne reçoit aucune réponse. | Résolvez les problèmes au niveau de la connexion réseau entre l’hôte KMS et le client. Assurez-vous que le port TCP 1688 (port par défaut) n’est pas bloqué par un pare-feu ou filtré d’une autre manière. |
| 0xC004F041 | Le service de protection logicielle a déterminé que le service Gestionnaire de clés (KMS) n’est pas activé. KMS doit être activé. | Client KMS | L’hôte KMS n’est pas activé. | Activez l’hôte KMS par téléphone ou en ligne. |
| 0xC004F042 | Le service de protection logicielle a déterminé que le service Gestionnaire de clés (KMS) spécifié ne peut pas être utilisé. | Client KMS | Incompatibilité entre le client KMS et l’hôte KMS. | Cette erreur survient lorsqu’un client KMS contacte un hôte KMS qui ne peut pas activer le logiciel client. Ce peut être courant dans des environnements mixtes contenant par exemple des hôtes KMS spécifiques à la fois au système d’exploitation et aux applications. |
| 0xC004F050 | Le service de protection logicielle a signalé que la clé de produit n’est pas valide. | KMS, client KMS, MAK | Cette erreur peut être due à une faute de frappe dans la clé KMS ou à la saisie dans une clé bêta sur une version finale du système d’exploitation. | Installez la clé KMS appropriée sur la version correspondante de Windows. Vérifiez l’orthographe. Si la clé est copiée-collée, assurez-vous que les tirets cadratins n’ont pas été substitués par des tirets dans la clé. |
| 0xC004F051 | Le service de protection logicielle a signalé que la clé de produit est bloquée. | MAK/KMS | La clé de produit sur le serveur d’activation est bloquée par Microsoft. | Obtenez une nouvelle clé MAK/KMS, installez-la sur le système, puis procédez à l’activation. |
| 0xC004F064 | Le service de protection logicielle a signalé que la période de grâce de version non validée a expiré. | MAK | Le WAT a détecté que le système n’est pas authentique. | Voir le Guide des opérations de Volume Activation. |
| 0xC004F065 | Le service de protection logicielle a détecté que l’application s’exécute pendant la période de grâce de version non validée. | Client MAK/KMS | Le WAT a détecté que le système n’est pas authentique. L’exécution du système se poursuivra pendant la période de grâce non validée. | Obtenez et installez une clé de produit authentique et activez le système pendant la période de grâce. Sinon, le système passera en état de notification à l’issue de la période de grâce. |
| 0xC004F06C | Le service de protection logicielle a signalé que l’ordinateur n’a pas pu être activé. Le service Gestionnaire de clés (KMS) a déterminé que l’horodatage de la demande n’est pas valide. | Client KMS | L’heure du système sur l’ordinateur client diffère trop de l’heure sur l’hôte KMS. | La synchronisation des heures est essentielle à la sécurité du système et du réseau pour plusieurs raisons. Résolvez ce problème en modifiant l’heure du système sur le client pour la synchroniser à celle du KMS. L’utilisation d’une source de temps NTP ou AD DS pour la synchronisation des heures est recommandée. Ici, l’heure utilisée est de source UTP et est indépendante du choix de fuseau horaire. |
| 0x80070005 | Accès refusé. L’action demandée exige des privilèges plus élevés. | Client KMS / hôte KMS/MAK | Le contrôle de compte d’utilisateur (UAC) empêche l’exécution de processus d’activation dans une invite de commandes à privilèges non élevés. | Exécutez slmgr.vbs depuis une invite de commandes à privilèges élevés. Cliquez avec le bouton droit de la souris sur cmd.exe, puis cliquez sur Exécuter en tant qu’administrateur. |
| 0x8007232A | Défaillance du serveur DNS. | Hôte KMS | Le système contient des erreurs DNS ou de réseau. | Résolvez ces problèmes au niveau du réseau et du DNS. |
| 0x8007232B | Le nom DNS n’existe pas. | Client KMS | Le client KMS ne trouve pas les enregistrements de ressource SRV KMS dans le DNS.  Si un hôte KMS n’existe pas sur le réseau, une MAK doit être installée. | Confirmez qu’un hôte KMS a été installé et que la publication DNS est activée (par défaut).  Si DNS est indisponible, dirigez le client KMS vers l’hôte KMS à l’aide de **slmgr.vbs /skms <*nom\_hôte\_kms>***.  En outre, obtenez et installez une MAK puis activez le système.  Enfin, résolvez les problèmes au niveau du DNS. |
| 0x800706BA | Le serveur RPC n’est pas disponible. | Client KMS | Les paramètres de pare-feu ne sont pas configurés sur l’hôte KMS ou les enregistrements SRV DNS sont caducs. | Assurez-vous que l’exception de pare-feu du service Gestionnaire de clé est activée sur l’ordinateur hôte KMS.  Assurez-vous que les enregistrements SRV renvoient bien à un hôte KMS valide.  Résolvez les problèmes au niveau des connexions réseau. |
| 0x8007251D | Aucun enregistrement trouvé pour la requête DNS donnée. | Client KMS | Le client KMS ne trouve pas les enregistrements de ressource SRV KMS dans le DNS. | Résolvez les problèmes au niveau des connexions réseau et du DNS. |
| 0xC004F074 | Le service de protection logicielle a signalé que l’ordinateur n’a pas pu être activé. Aucun service Gestionnaire de clés (KMS) n’a pu être contacté. Veuillez consulter le journal d’événements d’applications pour plus d’informations. | Client KMS | Tous les systèmes hôtes KMS ont renvoyé une erreur. | Résolvez les erreurs de chaque ID d’événement 12288 associé à la tentative d’activation. |

# Journal des événements Windows

Le tableau 11 répertorie les événements que KMS inscrit dans le journal des événements Windows. Vous trouverez ci-après les données communes pour chaque événement :

* **Nom du fichier journal (sauf 12290) :** Journaux Windows\Application
* **Nom du fichier journal (12290) :** Journaux des applications et des services\Service Gestionnaire de clés
* **Nom du fournisseur d’événements :** Microsoft-Windows-Security-Licensing-SLC
* **Nom de la source :** Service de protection logicielle

Tableau 11. Événements KMS inscrits dans le journal des événements Windows

| **ID d’événement** | **Journalisé par** | **Description** | **Message** | **Paramètres**  **Champs inclus dans la chaîne de valeurs séparées par des virgules** | | **Exemples** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Nom** | **Description** |  |
| 12288 | Client | Échec de génération de requête ou après soumission RPC (client) | Le client a envoyé une demande d’activation à l’ordinateur du service Gestionnaire de clés.%nInfos :%n%1 | HRESULT | Code de retour | 0x0 |
|  | | | | Status | Indicateurs (note 1) | 0x8 |
| Server:Port | Nom : port | kms01.contoso.com:1688 |
| CMID | ID d’ordinateur client | 08c3bda0-c556-4b61-9e4e-7bf6d4df80be, |
| Client Time | Horodatage de la demande | 2006/1/14 2:30, |
| VM Info | Non utilisé | 1 |
| Licensing Status | État de la licence  0 - Sans licence  1 - Avec licence (activé)  2 - Grâce hors boîte  3 - Grâce hors tolérance  4 - Grâce non validée  5 - Notifications  6 - Grâce étendue | 2 |
|  | | | | Time to Expiration | Temps restant (en minutes) | 40123 |
| ActID | ID d’activation - identifie la licence | cf67834d-db4a-402c-ab1f-2c134f02b700, |
| N-Policy | Nombre minimum requis pour que le client soit activé | 25 |
| 12289 | Client | Après validation de la réponse KMS (client) | Le client a traité une réponse d’activation de l’ordinateur du service Gestionnaire de clés.%nInfos :%n%1 | HRESULT | Code de retour | 0x0 |
|  | | | | Status | Indicateurs (note 1) | 0x4000008 |
| fBound | Indicateur activé | 0 |
| Unused | Non utilisé - ignorer | 0 |
| Count | Nombre KMS actuel | 4 |
| Activation Interval | Intervalle entre les demandes en cas de non-activation (en minutes) | 120 |
| Renewal Interval | Intervalle entre les demandes en cas d’activation (en minutes) | 10080 |
| Client Time | Horodatage de la demande | 1/14/2006 2:30 |
| 12290 | KMS | Journal côté serveur KMS pour chaque demande | Une demande d’activation a été traitée.%nInfos :%n%1 | HRESULT | Code de retour | 0x0 |
|  | | | | N-Policy | Nombre minimum de produits client requis pour l’activation | 25 |
| Machine | Nom de l’ordinateur client | kms03.site5.contoso.com |
| CMID | ID d’ordinateur client | e5c98033-aab6-4d0b-9af9-1d399597dd56 |
|  | | | | Client Time | Horodatage de la demande | 2006/1/14 22:36 |
| VM Info | Le SE client est exécuté sur un ordinateur virtuel | 1 |
| Licensing Status | État de la licence  0 - Sans licence  1 - Avec licence (activé)  2 - Grâce hors boîte  3 - Grâce hors tolérance  4 - Grâce non validée  5 - Notifications  6 - Grâce étendue | 2 |
| Time to Expiration | Temps restant (en minutes) | 40123 |
| ActID | ID d’activation - identifie la licence | cf67834d-db4a-402c-ab1f-2c134f02b700 |
| 12291 | KMS | Échec d’initialisation KMS | Un client avec licence en volume n’a pas pu initialiser la temporisation de renouvellement du service Gestionnaire de clés.%nInformations :%n%1 | HRESULT | Code de retour |  |
| 12292 | KMS | Échec d’initialisation de la temporisation de renouvellement | Le Service Gestionnaire de clés (KMS) n’a pas pu initialiser la temporisation de renouvellement.%nInfos :%n%1 | HRESULT | Code de retour |  |
| 12293 | KMS | Échec de publication de RR DNS | Échec de la publication du service Gestionnaire de clés (KMS) dans DNS dans le domaine %2.%nInfo :%n%1 | P1 : HRESULT  P2 : DNS domain | P1 : code de retour  P2 : nom de domaine DNS | |
| 12294 | KMS | Réussite de publication de RR DNS | Réussite de la publication du service Gestionnaire de clés (KMS) dans DNS dans le domaine %1.%n | DNS domain | Nom de domaine DNS |  |

# Méthodes et propriétés WMI

Le tableau 12 répertorie les méthodes et propriétés WMI de la plateforme de protection logicielle. Les propriétés de la plateforme de protection logicielle sont définies dans le fichier %WinDir%\System32\wbem\sppwmi.mof.

Tableau 12. Méthodes et propriétés WMI de la plateforme de protection logicielle

|  |  |
| --- | --- |
| **//Propriétés du service de gestion de licences des logiciels** | |
| **Version** | Version du service de protection logicielle |
| **KeyManagementServiceMachine** | Nom de l’hôte KMS. Renvoie la valeur Null si **SetKeyManagementServiceMachine** n’a pas été appelé. |
| **KeyManagementServicePort** | Port TCP utilisé par les clients pour envoyer des demandes d’activation du service Gestionnaire de clés. Renvoie **0** si **SetKeyManagementServicePort** n’a pas été appelé. |
| **IsKeyManagementServiceMachine** | Indique si le service Gestionnaire de clés est activé sur l’ordinateur : **0** signifie non, **1** oui. |
| **VLActivationInterval** | Fréquence, en minutes, à laquelle un client contactera l’hôte KMS avant de recevoir une licence. |
| **VLRenewalInterval** | Fréquence, en minutes, à laquelle un client contactera l’hôte KMS après avoir reçu une licence. |
| **KeyManagementServiceCurrentCount** | Nombre de clients KMS actuellement actifs sur l’hôte KMS. **-1** indique que l’hôte n’est pas activé en tant que service Gestionnaire de clés ou qu’il n’a reçu aucune demande de licence de la part des clients. |
| **RequiredClientCount** | Nombre minimal de clients devant se connecter à un hôte KMS afin d’activer les licences en volume. |
| **PolicyCacheRefreshRequired** | Indique si le cache de stratégie de licence doit être mis à jour : **0**=actualisation non requise, **1**=actualisation requise. |
| **ClientMachineID** | Identificateur global unique (GUID) identifiant un client KMS auprès d’un hôte KMS. Le client inclut ce GUID dans les demandes qu’il envoie au service Gestionnaire de clés. |
| **RemainingWindowsReArmCount** | Nombre de fois où le client peut encore être réarmé. |
| **KeyManagementServiceListeningPort** | Port TCP utilisé par l’hôte KMS pour écouter les demandes d’activation. |
| **KeyManagementServiceDnsPublishing** | Indique l’état de publication DNS d’un hôte KMS : **0**=désactivé, **1**=publication automatique activée (par défaut). |
| **KeyManagementServiceLowPriority** | Indique l’état de la priorité de thread du service Gestionnaire de clés : **0**=Priorité normale (par défaut), **1**=priorité basse. |
| **KeyManagementServiceHostCaching** | Indique l’état de la mise en cache du nom et du port d’hôte KMS : **0**=mise en cache désactivée, **1**=mise en cache activée (par défaut). |
| **KeyManagementServiceUnlicensedRequests** | Nombre de demandes reçues par le service Gestionnaire de clés provenant de clients avec l’état de licence = 0 (Sans licence). |
| **KeyManagementServiceLicensedRequests** | Nombre de demandes reçues par le service Gestionnaire de clés provenant de clients avec l’état de licence = 1 (Avec licence). |
| **KeyManagementServiceOOBGraceRequests** | Nombre de demandes reçues par le service Gestionnaire de clés provenant de clients avec l’état de licence = 2 (Grâce initiale). |
| **KeyManagementServiceOOTGraceRequests** | Nombre de demandes reçues par le service Gestionnaire de clés provenant de clients avec l’état de licence = 3 (Grâce hors tolérance). |
| **KeyManagementServiceNonGenuineGraceRequests** | Nombre de demandes reçues par le service Gestionnaire de clés provenant de clients avec l’état de licence = 4 (Grâce pour version non authentique). |
| **KeyManagementServiceNotificationRequests** | Nombre de demandes reçues par le service Gestionnaire de clés provenant de clients avec l’état de licence = 5 (Notification). |
| **KeyManagementServiceTotalRequests** | Nombre total de demandes valides reçues par le service Gestionnaire de clés. |
| **KeyManagementServiceFailedRequests** | Nombre total de demandes non valides reçues par le service Gestionnaire de clés. |
| **KeyManagementServiceActivationDisabled** | Indique si l’activation en volume via le service Gestionnaire de clés est désactivée. |
| **//Méthodes du service de gestion de licences des logiciels** | |
| **InstallProductKey** | Installe une clé de produit. |
| **InstallLicense** | Installe une licence. |
| **InstallLicensePackage** | Installe un package de licence pour le produit actuel. |
| **SetKeyManagementServiceMachine** | Définit le nom d’hôte KMS à utiliser pour l’activation en volume. |
| **ClearKeyManagementServiceMachine** | Efface, le cas échéant, le nom d’hôte KMS configuré antérieurement. |
| **SetKeyManagementServicePort** | Définit le port TCP utilisé par un client pour effectuer des demandes auprès d’un hôte KMS. Si ce paramètre n’est pas spécifié, le port 1688 est utilisé. |
| **ClearKeyManagementServicePort** | Efface, le cas échéant, le numéro de port spécifié antérieurement. |
| **SetVLActivationInterval** | Fréquence d’activation, en minutes, à laquelle les clients KMS contacteront l’hôte KMS avant de recevoir une licence. Cette fréquence doit être supérieure ou égale à 15 et inférieure ou égale à 43 200. Une erreur est renvoyée si la méthode est appelée alors que l’ordinateur n’est pas un service Gestionnaire de clés. |
| **SetVLRenewalInterval** | Fréquence de renouvellement, en minutes, à laquelle les clients KMS contacteront l’hôte KMS après avoir reçu une licence. Cette fréquence doit être supérieure ou égale à 15 et inférieure ou égale à 43 200. Une erreur est renvoyée si la méthode est appelée alors que l’ordinateur n’est pas un service Gestionnaire de clés. |
| **ClearProductKeyFromRegistry** | Efface la clé de produit du registre. |
| **AcquireGenuineTicket** | Effectue la validation de l’authenticité en ligne. L’appel de cette méthode peut modifier l’état d’authenticité de l’ordinateur. |
| **ReArmWindows** | Réinitialise l’état de la licence de l’ordinateur à Grâce initiale (voir **État de la licence**).  **Remarque**   vous devez redémarrer le client pour que les modifications soient prises en compte. |
| **RefreshLicenseStatus** | Met à jour l’état de la licence de Windows afin que les applications aient accès aux informations de licence actuelles. |
| **SetKeyManagementServiceListeningPort** | Définit le port TCP utilisé par un hôte KMS pour écouter les demandes d’activation. S’applique uniquement aux hôtes KMS. Si ce paramètre n’est pas spécifié, le port 1688 est utilisé. |
| **ClearKeyManagementServiceListeningPort** | Efface, le cas échéant, le port d’écoute spécifié antérieurement. S’applique uniquement aux hôtes KMS. |
| **DisableKeyManagementServiceDnsPublishing** | Active/désactive la publication DNS sur un ordinateur hôte KMS : **0**=Activer, **1**=Désactiver. |
| **EnableKeyManagementServiceLowPriority** | Active/désactive le service Gestionnaire de clés s’exécutant avec une priorité basse : **0**=Désactiver, **1**=Activer. |
| **DisableKeyManagementServiceHostCaching** | Active/désactive la mise en cache du nom et du port d’hôte KMS sur un ordinateur client de l’activation en volume : **0**=Activer, **1**=Désactiver. |
| **DisableKeyManagementServiceActivation** | Active/désactive l’activation en volume via un ordinateur KMS : **0**=Activer, **1**=Désactiver. |
| **DiscoveredKeyManagementServiceMachineName** | Dernier nom d’hôte KMS découvert par le biais de DNS. |
| **DiscoveredKeyManagementServiceMachinePort** | Dernier port d’hôte KMS découvert par le biais de DNS. |
| **//Propriétés du service de gestion de licences des logiciels** | |
| **ID** | Identificateur du produit |
| **Nom** | Nom du produit |
| **Description** | Description du produit |
| **ApplicationID** | ID de l’application du produit en cours |
| **ProcessorURL** | URL du serveur de gestion de licence des logiciels pour le certificat de processus |
| **MachineURL** | URL du serveur de gestion de licence des logiciels pour le certificat de liaison |
| **ProductKeyURL** | URL du serveur de gestion de licence des logiciels pour le certificat de produit |
| **UseLicenseURL** | URL du serveur de gestion de licence des logiciels pour la licence d’utilisateur |
| **LicenseStatus** | État de la licence de l’application de ce produit :  **0**=Sans licence, **1**=Avec licence, **2**=Grâce initiale, **3**=Grâce hors tolérance, **4**=Grâce pour version non authentique, **5**=Notification, **6**=Grâce étendue |
| **LicenseStatusReason** | Code de diagnostic qui indique pourquoi un ordinateur présente un état de licence spécifique. |
| **GracePeriodRemaining** | Temps restant (en minutes) avant que l’application parent passe en mode Notification. Pour les clients en volume, il s’agit du temps restant avant qu’une réactivation soit nécessaire. |
| **EvaluationEndDate** | Date d’expiration de l’application de ce produit. Après cette date, l’**état de la licence** sera **Sans licence** et ne pourra pas être activé. |
| **OfflineInstallationId** | Identificateur pour l’application de ce produit qui peut être utilisé pour l’activation par téléphone ou hors connexion. Renvoie la valeur Null si aucune clé de produit n’est installée. |
| **PartialProductKey** | Cinq derniers caractères de la clé de ce produit. Renvoie la valeur Null si aucune clé de produit n’est installée. |
| **ProductKeyID** | ID de clé de produit. Renvoie la valeur Null si aucune clé de produit n’est installée. |
| **LicenseFamily** | Identificateur de famille de la référence (SKU) utilisée pour déterminer les relations de licence pour les composants additionnels. |
| **LicenseDependsOn** | Identificateur de dépendance de la famille de références (SKU) utilisée pour déterminer les relations de licence pour les composants additionnels. |
| **LicenseIsAddon** | Renvoie la valeur **True** si le produit est identifié en tant que licence de composant additionnel. |
| **VLActivationInterval** | Fréquence, en minutes, à laquelle un client contactera l’hôte KMS avant l’attribution d’une licence au produit. |
| **VLRenewalInterval** | Fréquence, en minutes, à laquelle un client contactera l’hôte KMS après l’attribution d’une licence au produit. |
| **KeyManagementServiceProductKeyID** | ID de clé de produit du service Gestionnaire de clés. Renvoie la valeur Null si non applicable. |
| **KeyManagementServiceMachine** | Nom de l’hôte KMS. Renvoie la valeur Null si **SetKeyManagementServiceMachine** n’a pas été appelé. |
| **KeyManagementServicePort** | Port TCP utilisé par les clients pour envoyer des demandes d’activation du service Gestionnaire de clés. Renvoie **0** si **SetKeyManagementServicePort** n’a pas été appelé. |
| **DiscoveredKeyManagementServiceMachineName** | Dernier nom d’hôte KMS découvert par le biais de DNS. |
| **DiscoveredKeyManagementServiceMachinePort** | Dernier port d’hôte KMS découvert par le biais de DNS. |
| **IsKeyManagementServiceMachine** | Indique si le service Gestionnaire de clés est activé sur l’ordinateur : **1** signifie oui, **0** non. |
| **KeyManagementServiceCurrentCount** | Nombre de clients KMS actuellement actifs sur l’hôte KMS. **-1** indique que l’ordinateur n’est pas activé en tant que service Gestionnaire de clés ou qu’il n’a reçu aucune demande de licence de la part des clients. |
| **RequiredClientCount** | Nombre minimal de clients devant se connecter à un hôte KMS afin d’activer les licences en volume. |
| **KeyManagementServiceUnlicensedRequests** | Nombre de demandes reçues par le service Gestionnaire de clés provenant de clients avec l’état de licence = 0 (Sans licence). |
| **KeyManagementServiceLicensedRequests** | Nombre de demandes reçues par le service Gestionnaire de clés provenant de clients avec l’état de licence = 1 (Avec licence). |
| **KeyManagementServiceOOBGraceRequests** | Nombre de demandes reçues par le service Gestionnaire de clés provenant de clients avec l’état de licence = 2 (Grâce initiale). |
| **KeyManagementServiceOOTGraceRequests** | Nombre de demandes reçues par le service Gestionnaire de clés provenant de clients avec l’état de licence = 3 (Grâce hors tolérance). |
| **KeyManagementServiceNonGenuineGraceRequests** | Nombre de demandes reçues par le service Gestionnaire de clés provenant de clients avec l’état de licence = 4 (Grâce pour version non authentique). |
| **KeyManagementServiceTotalRequests** | Nombre total de demandes valides reçues par le service Gestionnaire de clés. |
| **KeyManagementServiceFailedRequests** | Nombre total de demandes infructueuses reçues par le service Gestionnaire de clés. |
| **KeyManagementServiceNotificationRequests** | Nombre de demandes reçues par le service Gestionnaire de clés provenant de clients avec l’état de licence = 5 (Notification). |
| **GenuineStatus** | État authentique pour l’application de ce produit. |
| **ExtendedGrace** | Temps de grâce étendu, en minutes, avant que l’application parente ne perde sa licence. |
| **TrustedTime** | Affiche l’heure approuvée stockée actuellement dans le système. |
| **DisableKeyManagementServiceHostCaching** | Active/désactive la mise en cache du nom et du port d’hôte KMS sur un ordinateur client de l’activation en volume : 0=Activer, 1=Désactiver. |
| **//Méthodes du service de gestion de licences des logiciels** | |
| **UninstallProductKey** | Désinstalle une clé de produit pour le produit actuel. |
| **Activate** | Active le produit actuel. |
| **DepositOfflineConfirmationId** | Active un produit en déposant un identificateur de confirmation hors connexion pour ce produit lors de l’activation par téléphone ou hors connexion. |
| **GetPolicyInformationDWord** | Obtient des informations de stratégie de licence de type DWORD. |
| **GetPolicyInformationString** | Obtient des informations de stratégie de type chaîne. |
| **SetKeyManagementServiceMachine** | Définit le nom d’hôte KMS à utiliser pour l’activation en volume. |
| **ClearKeyManagementServiceMachine** | Efface, le cas échéant, le nom d’hôte KMS configuré antérieurement. |
| **SetKeyManagementServicePort** | Définit le port TCP utilisé par un client pour effectuer des demandes auprès d’un hôte KMS. Si ce paramètre n’est pas spécifié, le port 1688 est utilisé. |
| **ClearKeyManagementServicePort** | Efface, le cas échéant, le numéro de port spécifié antérieurement. |

# Glossaire

|  |  |
| --- | --- |
| **Terme** | **Définition** |
| **ACID** | GUID utilisé pour identifier une méthode d’activation dans une édition logicielle. |
| **AD DS** | Services de domaine Active Directory. |
| **AppID** | GUID défini pour regrouper une collecte d’IDRéf comme un nom de famille. Toutes les éditions Windows ont le même IDApp. |
| **Banque d’informations de certificats de l’ordinateur** | Ce certificat et sa clé privée doivent être accessibles par l’utilisateur tentant une activation basée sur les jetons. |
| **DNS** | Service de noms de domaine. |
| **FQDN** | Nom de domaine complet (par exemple : phred.microsoft.com). |
| **GVLK** | Clé de licence en volume générique, clé de produit spécifique à une édition qui installe toutes les éditions en volume de Windows par défaut. Également connue comme la clé d’installation de client KMS par défaut. Pour plus d’informations, voir le Tableau 9. |
| **IDRéf** | Voir ACID |
| **Jeton** | Certificat x509, associé à une clé privée, utilisé pour activer Windows sur des ordinateurs permettant une activation basée sur les jetons. |
| **KMS** | Service gestionnaire de clés. |
| **KMSID** | GUID envoyé par le Client KMS pour activation avec un hôte KMS. Peut être partagé entre plusieurs ACID. |
| **MAK** | Clé d’activation multiple. |
| **N-policy** | Stratégie de licence qui spécifie le nombre minimum d’ordinateurs renvoyés par un KMS qu’un client utilisera pour décider d’une auto-activation ou non. |
| **PIN** | Code confidentiel, utilisé par une carte à puce comme information d’identification d’authentification. |
| **Réf** | Désigne une édition distincte de Windows ou d’autres logiciels. |
| **SPPSVC** | Service de protection logicielle, plateforme de service intégrée à Windows 7 et Windows Server 2008 R2 qui gère les activités de licence pour Windows et d’autres applications. |
| **SRV** | Type d’enregistrement de ressource pris en charge dans le DNS (voir RFC 2782) |
| **VL** | Licence en volume. |
| **WMI** | Infrastructure de gestion Windows WMI. |

# Liens de ressources

* Volume Activation :
* Volume Activation sur TechNet : [http://go.microsoft.com/fwlink/?LinkId=150083 (éventuellement en anglais)](http://go.microsoft.com/fwlink/?LinkId=150083%20(éventuellement%20en%20anglais))
* Service Gestionnaire de clés 1.2 pour Windows Server 2003 SP1, et versions ultérieures : [http://go.microsoft.com/fwlink/?LinkId=155083 (éventuellement en anglais)](http://go.microsoft.com/fwlink/?LinkId=155083%20(éventuellement%20en%20anglais))
* Informations sur l’activation et les clés de produits : [http://go.microsoft.com/fwlink/?LinkId=74008 (éventuellement en anglais)](http://go.microsoft.com/fwlink/?LinkId=74008%20(éventuellement%20en%20anglais))
* Guide de déploiement de Volume Activation : [http://go.microsoft.com/fwlink/?LinkId=150083 (éventuellement en anglais)](http://go.microsoft.com/fwlink/?LinkId=150083%20(éventuellement%20en%20anglais))
* Guide des opérations de Volume Activation : <http://go.microsoft.com/fwlink/?LinkId=150084>
* Guide de planification de Volume Activation : <http://go.microsoft.com/fwlink/?LinkId=155926>
* Guide de référence technique de Volume Activation : [http://go.microsoft.com/fwlink/?LinkId=152550 (éventuellement en anglais)](http://go.microsoft.com/fwlink/?LinkId=152550%20(éventuellement%20en%20anglais))
* Outils de déploiement :
* Kit d’installation automatisée Windows (AIK) pour Windows 7 : <http://go.microsoft.com/fwlink/?LinkId=136976>
* Outils de gestion :
* Catalogue de packs System Center : <http://go.microsoft.com/fwlink/?LinkID=110332>
* Licences en volume :
* Logiciels Microsoft authentiques : [http://go.microsoft.com/fwlink/?LinkId=151993 (éventuellement en anglais)](http://go.microsoft.com/fwlink/?LinkId=151993%20(éventuellement%20en%20anglais))
* Page de validation de logiciels Microsoft authentiques : <http://go.microsoft.com/fwlink/?LinkId=64187>
* Numéros de téléphone des Centres d’activation Microsoft dans le monde : <http://go.microsoft.com/fwlink/?LinkId=107418>
* Licences en volume Microsoft : [http://go.microsoft.com/fwlink/?LinkId=73076 (éventuellement en anglais)](http://go.microsoft.com/fwlink/?LinkId=73076%20(éventuellement%20en%20anglais))
* Centre de gestion des licences en volume Microsoft : <http://go.microsoft.com/fwlink/?LinkId=107544>
* Déclaration de confidentialité de Windows Vista : [http://go.microsoft.com/fwlink/?LinkID=52526 (éventuellement en anglais)](http://go.microsoft.com/fwlink/?LinkID=52526%20(éventuellement%20en%20anglais))