**Guía de implementación de
Volume Activation**

**Windows 7 y Windows Server 2008 R2**

Microsoft Corporation

Fecha de publicación: junio de 2009

Resumen

Volume Activation ayuda a los clientes de licencias por volumen a automatizar y administrar el proceso de activación. Este documento está diseñado para implementadores de tecnología de la información (TI) que hayan planeado una implementación de Volume Activation y que estén listos para repasar y llevar a cabo los procedimientos necesarios para este proceso.

Este documento y cualquier otro documento aquí mencionado se proporcionan solo con fines informativos, y Microsoft no establecerá ninguna garantía, expresa o implícita, en este documento. La información de este documento, incluidas las referencias a direcciones URL y a otros sitios web de Internet, está sujeta a cambios sin previo aviso. El usuario será el único responsable del uso o de las consecuencias derivadas del uso que haga de este documento. A menos que se especifique lo contrario, las empresas, las organizaciones, los productos, los nombres de dominio, las direcciones de correo electrónico, los logotipos, las personas, los lugares y los acontecimientos que se describen en este documento a modo de ejemplo son ficticios. No se pretende indicar ni debe deducirse ninguna asociación con compañías, organizaciones, productos, nombres de dominio, direcciones de correo electrónico, logotipos, personas, lugares o acontecimientos reales. El usuario tendrá la responsabilidad de cumplir todas las leyes de derecho de autor aplicables. Sin limitar los derechos de autor aplicables, ninguna parte de este documento se podrá reproducir, almacenar o insertar en un sistema de recuperación, ni transmitir de ninguna forma, por ningún medio (electrónico, mecánico, mediante fotocopias o grabación, o de cualquier otro tipo) o propósito, sin la previa autorización expresa por escrito de Microsoft Corporation.

Microsoft puede ser titular de patentes, solicitudes de patentes, marcas, derechos de autor u otros derechos de propiedad intelectual sobre el contenido de este documento. El suministro de este documento no le otorga ninguna licencia sobre estas patentes, marcas comerciales, derechos de autor u otros derechos de propiedad intelectual, a menos que se prevea en un contrato por escrito de licencia de Microsoft.

© 2009 Microsoft Corporation.

Microsoft, Active Directory, Windows, Windows Server y Windows Vista son marcas registradas del grupo de empresas de Microsoft.

Los nombres de empresas y productos reales mencionados aquí pueden ser marcas comerciales de sus respectivos propietarios.

Contenido

[Contenido 3](#_Toc234138487)

[Introducción 5](#_Toc234138488)

[Activación KMS 6](#_Toc234138489)

[Configuración de hosts KMS 6](#_Toc234138490)

[Ejecución de Slmgr.vbs de forma remota 9](#_Toc234138491)

[Configuración de Firewall de Windows para operaciones remotas del administrador de licencias de software 10](#_Toc234138492)

[Operaciones remotas dirigidas a equipos de un grupo de trabajo 11](#_Toc234138493)

[Configuración del DNS 11](#_Toc234138494)

[Cambio de los permisos DNS predeterminados para registros SRV 12](#_Toc234138495)

[Publicación en múltiples dominios DNS 13](#_Toc234138496)

[Creación manual de registros SRV en DNS 15](#_Toc234138497)

[Creación manual de registros SRV en un servidor BIND 8.2 o superior 16](#_Toc234138498)

[Deshabilitación de la publicación de registros SRV de KMS en DNS 17](#_Toc234138499)

[Instalación de hosts KMS 18](#_Toc234138500)

[Configuración de clientes KMS 19](#_Toc234138501)

[Especificación manual de un host KMS 20](#_Toc234138502)

[Habilitación de la detección automática de un cliente KMS 21](#_Toc234138503)

[Adición de entradas con sufijo en clientes KMS 22](#_Toc234138504)

[Implementación de clientes KMS 23](#_Toc234138505)

[Activación manual de un cliente KMS 24](#_Toc234138506)

[Conversión de clientes MAK a KMS, y viceversa 25](#_Toc234138507)

[Conversión de ediciones de venta al por menor en activaciones de licencia por volumen 26](#_Toc234138508)

[Activación MAK 27](#_Toc234138509)

[Conversión de clientes KMS en activación MAK 27](#_Toc234138510)

[Instalación de una MAK durante la instalación del sistema operativo 28](#_Toc234138511)

[Instalación de una MAK después de la instalación del sistema operativo 29](#_Toc234138512)

[Deshabilitación de la activación automática 30](#_Toc234138513)

[Activación de clientes MAK 30](#_Toc234138514)

[Activación de clientes MAK por Internet 31](#_Toc234138515)

[Activación de clientes MAK mediante un servidor proxy 32](#_Toc234138516)

[Activación de clientes MAK por teléfono 33](#_Toc234138517)

[Activación de clientes MAK mediante la herramienta VAMT 34](#_Toc234138518)

[Deshabilitación de la activación automática 35](#_Toc234138519)

[Integración de claves MAK con Deployment Workbench 35](#_Toc234138520)

[Reactivación de equipos 36](#_Toc234138521)

[Apéndice A: Configuraciones opcionales 37](#_Toc234138522)

[Habilitación de la activación por parte del usuario estándar 37](#_Toc234138523)

[Deshabilitación de las notificaciones de activación 37](#_Toc234138524)

[Modificaciones de claves del registro para funciones de activación 38](#_Toc234138525)

[Apéndice B: Archivo de instalación desatendida de muestra 39](#_Toc234138526)

# Introducción

Esta guía describe conceptos de implementación de Microsoft® Volume Activation. Volume Activation consta de dos tecnologías: el Servicio de administración de claves (KMS) y la Clave de activación múltiple (MAK), que permiten los clientes de licencias por volumen activar las ediciones de licencia por volumen de los sistemas operativos Windows® 7 y Windows Server® 2008 R2. El Centro de servicios de licencias por volumen, disponible en <https://www.microsoft.com/licensing/servicecenter/>, ofrece más información sobre las licencias por volumen.

Cuando una organización planea usar Volume Activation, debe elegir KMS, MAK o una combinación de ambos. Los métodos de activación que se eligen dependen de las necesidades de la organización y de la infraestructura de la red. Para obtener más información sobre la planeación de Volume Activation, consulte la [Guía de planeación de Volume Activation](http://go.microsoft.com/fwlink/?LinkId=155926).

**Nota**   Este documento proporciona una guía de implementación de Volume Activation para los sistemas operativos Windows  7 y Windows Server 2008 R2. Sin embargo, esta guía aborda la interoperabilidad entre ambas generaciones de productos. Para obtener más información sobre la implementación de Volume Activation para Windows Vista® y Windows Server 2008, consulte <http://go.microsoft.com/fwlink/?LinkID=75674>.

**Nota**   Esta guía describe procedimientos que ejecutan scripts y realizan modificaciones en el Registro. Estos derechos pueden delegarse a algunos implementadores de tecnología de la información (TI). Los derechos para cambiar claves de producto y realizar activaciones, incluso, se pueden asignar a usuarios, aunque Microsoft no lo recomienda.

Si se produce un error en la activación, consulte la [Guía de operaciones de Volume Activation](http://go.microsoft.com/fwlink/?LinkId=150084) para obtener ayuda para la solución de problemas. La guía incluye una referencia de códigos de error con los pasos para resolver los problemas comunes.

# Activación KMS

La activación KMS requiere mínima intervención administrativa. Si el entorno de red tiene Sistema de Nombres de Dominio Dinámico (DDNS) y permite a los equipos publicar servicios de forma automática, la implementación de un host KMS puede requerir muy poco esfuerzo. Si la organización tiene más de un host KMS o la red no admite DDNS, es posible que se deban realizar tareas de configuración adicionales.

Advertencia:   Algunos procedimientos de esta sección requieren que se cambie el Registro. Pueden producirse problemas si modifica el Registro de forma incorrecta mediante el Editor del Registro o cualquier otro método, y estos problemas pueden requerir la reinstalación del sistema operativo. Microsoft no garantiza que estos problemas puedan solucionarse. Los profesionales de TI modifican el Registro bajo su propia responsabilidad.

El resto de esta sección describe las siguientes tareas clave:

1. Configuración de hosts KMS
2. Configuración del DNS
3. Instalación de hosts KMS
4. Configuración de clientes KMS

## Configuración de hosts KMS

El administrador de licencias de software, a veces denominado Administrador SL (Slmgr.vbs), es un script que se usa para configurar y recuperar información de Volume Activation. El script puede ejecutarse de forma local en el equipo de destino o de forma remota desde otro equipo, pero debe ejecutarse desde un símbolo del sistema elevado. Si un usuario estándar ejecuta Slmgr.vbs, algunos datos de la licencia pueden faltar o ser incorrectos, y muchas operaciones están prohibidas.

Slmgr.vbs puede usar Wscript.exe o Cscript.exe, y los administradores pueden especificar qué motor de scripts desean utilizar. Si no se especifica un motor de scripts, Slmgr.vbs usa el motor de scripts predeterminado, wscript.exe.

**Nota:**KMS requiere una excepción de firewall en el host KMS. Si usa el puerto TCP predeterminado, habilite la excepción de tráfico de KMS en Firewall de Windows. Si usa otro firewall, abra el puerto TCP 1688. Si usa un puerto no predeterminado, abra el puerto TCP personalizado en el firewall.

Para que los cambios tengan efecto, debe reiniciar el Servicio de licencias de software. Para reiniciar el Servicio de licencias de software, use el complemento Servicios de Microsoft Management Console (MMC), o puede ejecutar el siguiente comando en un símbolo del sistema elevado:

net stop sppsvc && net start sppsvc

Slmgr.vbs requiere, al menos, un parámetro. Si el script se ejecuta sin parámetros, muestra información de ayuda. En la tabla 1, se enumeran las opciones de línea de comandos de Slmgr.vbs con una descripción de cada una. La mayoría de los parámetros de la tabla 1 configura el host KMS. Sin embargo, los parámetros /sai y /sri se pasan a los clientes KMS después de que se conectan con el host. La sintaxis general de Slmgr.vbs es la siguiente:

slmgr.vbs /parámetro

Tabla 1.   Parámetros de Slmgr.vbs

| Parámetro | Descripción |
| --- | --- |
| /sprt NúmerodePuerto | Establece el puerto de comunicaciones TCP en un host KMS. Reemplace NúmerodePuerto con el número de puerto TCP que desee usar. La configuración predeterminada es **1688**. |
| /cdns | Deshabilita la publicación automática de DNS por parte de un host KMS. |
| /sdns | Habilita la publicación automática de DNS por parte del host KMS. |
| /cpri | Baja la prioridad de los procesos del host KMS. |
| /spri | Establece la prioridad de los procesos del host KMS como **Normal**. |
| /sai IntervalodeActivación | Cambia la frecuencia con la que un cliente KMS intenta realizar la activación cuando no puede encontrar un host KMS. Reemplace IntervalodeActivación con la cantidad de minutos. La configuración predeterminada es **120**. |
| /sri IntervalodeRenovación | Cambia la frecuencia con la que un cliente KMS intenta renovar su activación al ponerse en contacto con un host KMS. Reemplace IntervalodeRenovación con la cantidad de minutos. La configuración predeterminada es **10080** (7 días). Esta configuración anula la configuración de cliente KMS local. |
| /dli | Recupera la cantidad actual de activaciones KMS del host KMS. |

### Ejecución de Slmgr.vbs de forma remota

Para ejecutar Slmgr.vbs de forma remota, los administradores deben proporcionar parámetros adicionales. Deben incluir el nombre del equipo de destino, así como el nombre de usuario y la contraseña de una cuenta de usuario que tenga derechos administrativos locales en el equipo. Si se ejecuta de forma remota sin especificar un nombre de usuario ni una contraseña, el script usa las credenciales del usuario que lo ejecuta.

La siguiente sintaxis muestra los parámetros adicionales necesarios para ejecutar Slmgr.vbs de forma remota:

slmgr.vbs NombredeEquipodeDestino [NombredeUsuario] [Contraseña] /parámetro [Opciones]

### Configuración de Firewall de Windows para operaciones remotas del administrador de licencias de software

Slmgr.vbs usa Instrumental de administración de Windows (WMI). Por ello, los administradores deben configurar Firewall de Windows para permitir el tráfico de WMI:

* Para una subred individual, permita la excepción **Instrumental de administración de Windows (WMI)** en Firewall de Windows.
* Para permitir tráfico de WMI en varias subredes, permita la conexión para **Instrumental de administración de Windows (asinc. de entrada)**, **Instrumental de administración de Windows (DCOM de entrada)** e **Instrumental de administración de Windows (WMI de entrada)**. Además, permita el acceso remoto en el ámbito. Establezca esta configuración mediante seguridad avanzada de Firewall de Windows disponible en la carpeta Herramientas administrativas.

Nota:   De forma predeterminada, la opción Excepciones de Firewall de Windows en los perfiles públicos y privados, solamente aplica excepciones al tráfico que se origina en la subred local. Para expandir la excepción de modo que se aplique a varias subredes, cambie la configuración de la excepción en Firewall de Windows con seguridad avanzada, o bien, si es parte de un dominio de AD DS, elija la opción Perfil de dominio.

### Operaciones remotas dirigidas a equipos de un grupo de trabajo

Los administradores pueden permitir que Slmgr.vbs se ejecute de forma remota en los equipos que pertenezcan a un grupo de trabajo. Para ello, cree el valor **DWORD** **LocalAccountTokenFilterPolicy** en la subclave **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** del Registro en los clientes KMS. Establezca este valor en **0x01**.

## Configuración del DNS

En las siguientes secciones, se describen conceptos para configurar el DNS a fin de que funcione con Volume Activation:

* Si se usa más de un host KMS, consulte la sección “Cambio de los permisos DNS predeterminados para registros de SRV”.
* Para permitir que los clientes KMS que usan distintos servidores DNS encuentren hosts KMS, consulte la sección “Publicar en varios dominios DNS”.
* Para agregar manualmente registros de recursos SRV para hosts KMS, consulte las secciones “Creación manual de registros SRV en DNS”, “Creación manual de registros SRV en un servidor DNS BIND 8.2 o posterior” y “Deshabilitación de la publicación de registros SRV de KMS para DNS”.

Nota:   Es posible que los cambios de DNS no se reflejen hasta que todos los servidores DNS se hayan replicado.

### Cambio de los permisos DNS predeterminados para registros SRV

Si está usando un solo host KMS, es posible que no deba configurar los permisos en DNS. El comportamiento predeterminado consiste en permitir que un equipo cree un registro de recursos SRV y, luego, actualizarlo. Sin embargo, si tiene más de un host KMS (caso típico), los demás hosts no podrán actualizar el registro de recursos SRV, a menos que se cambien los permisos predeterminados de este.

El siguiente procedimiento de alto nivel es un ejemplo del entorno de Microsoft. No proporciona pasos detallados, que pueden variar de una organización a otra, y no representa la única forma de lograr el resultado deseado:

1. Cree un grupo de seguridad global en Active Directory® que se usará para los hosts KMS. Un ejemplo es el *Grupo del Servicio de administración de claves*.
2. Agregue todos los hosts KMS a este grupo. Todos deben ser parte del mismo dominio.
3. Una vez que se crea el primer host KMS, creará el registro SRV original. Si el primer host KMS no puede crear el registro de recursos SRV, es posible que se deba a que la organización ha cambiado los permisos predeterminados. En este caso, cree manualmente el registro de recursos SRV como se describe en la sección “Creación manual de registros SRV en DNS”.
4. Establezca los permisos para que el grupo SRV permita actualizaciones por parte de miembros del grupo de seguridad global.

**Nota:** Un administrador de dominio puede delegar la capacidad de realizar los pasos anteriores a los administradores de la organización. Para ello, cree un grupo de seguridad en Active Directory, otórguele permiso para cambiar los registros SRV y, luego, agregue los delegados.

### Publicación en múltiples dominios DNS

De forma predeterminada, el host KMS solamente está registrado en el dominio DNS, al que pertenece el host. Si el entorno de red solo tiene un dominio DNS, no se requieren más acciones.

Si hay más de un nombre de dominio DNS, se puede crear una lista de dominios DNS para que lo use un host KMS para publicar el registro de recursos SRV. Al establecer este valor en el registro se suspende el comportamiento predeterminado del host KMS, que consiste en publicar sólo en el dominio especificado como el sufijo DNS principal.

De forma opcional, agregue los parámetros priority y weight al valor **DnsDomainPublishList** del Registro para KMS. Esta función permite a un administrador establecer agrupaciones de prioridad de hosts KMS y realizar consideraciones dentro de cada grupo para definir qué host KMS probar primero y equilibrar el tráfico entre varios hosts KMS.

Nota:   Es posible que los cambios de DNS no se reflejen hasta que todos los servidores DNS se hayan replicado. Los cambios que se realizan con mucha frecuencia (tiempo < tiempo de replicación) pueden dejar registros anteriores si el cambio se realiza en un servidor que no se ha replicado.

Para publicar KMS automáticamente en varios dominios DNS, agregue el sufijo de cada dominio DNS al KMS que desea publicar en el valor de Registro de cadena múltiple **DnsDomainPublishList in HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform**. Después de cambiar el valor, reinicie el Servicio de licencias de software para crear el registro de recursos de SRV.

Nota:   Esta clave ha cambiado de la ubicación de Windows Vista® en **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL**.

Después de configurar un host KMS para publicar en varios dominios, exporte la clave de registro y, luego, impórtela al registro en host KMS adicionales. Para comprobar que este procedimiento se llevó a cabo correctamente, controle el registro de eventos de aplicaciones de cada host KMS. Un Id. de evento 12294 indica que el host KMS creó correctamente los registros de recursos SRV. Un Id. de evento 12293 indica que el intento de crear los registros de recursos SRV no se realizó correctamente. Para obtener una lista completa de los códigos de error, consulte la [Guía de operaciones de Volume Activation](http://go.microsoft.com/fwlink/?LinkId=150084).

### Creación manual de registros SRV en DNS

Si el entorno no es compatible con DDNS, los registros de recursos SRV se deben crear manualmente para publicar el host KMS. En entornos que no son compatibles con DDNS, se debe deshabilitar la publicación en todos los hosts KMS para evitar que los registros de eventos recopilen eventos de publicación de DNS con error. Para deshabilitar la publicación automática, use el script Slmgr.vbs con la opción de línea de comandos **/cdns**. Consulte la sección “Configuración de KMS” para obtener más información sobre el script Slmgr.vbs.

Nota:   Los registros de recursos de SRV creados de forma manual pueden coexistir con los registros de recursos de SRV que los hosts KMS publican automáticamente en otros dominios, siempre y cuando todos los registros se configuren a fin de evitar conflictos.

Con el Administrador de DNS, en la zona de búsqueda directa apropiada, cree un nuevo registro de recursos SRV. Para ello, utilice la información apropiada para la ubicación. De forma predeterminada, KMS escucha en el puerto TCP 1688, y el servicio es \_VLMCS. En la tabla 2, se proporciona una configuración de ejemplo para un registro de recursos SRV.

Tabla 2.   Registro de recursos SRV

| Nombre | Configuración |
| --- | --- |
| Servicio | \_VLMCS |
| Protocolo | \_TCP |
| Número de puerto | 1688 |
| Host que ofrece este servicio | FQDN del host KMS |

### Creación manual de registros SRV en un servidor BIND 8.2 o superior

Si la organización usa un servidor DNS que no sea de Microsoft, se pueden crear los registros de recursos SRV necesarios si el servidor DNS es compatible con Berkeley Internet Name Domain (BIND) 8.2 o superior. Cuando cree el registro, incluya la información que aparece en la tabla 3. La configuración **Prioridad** e **Importancia** que se muestra en la tabla 3 solo se usa en Windows 7 y Windows Server 2008 R2.

Tabla 3.   Información de registros de recursos SRV

|  |  |
| --- | --- |
| Nombre | Configuración |
| Nombre | \_vlmcs.\_tcp |
| Tipo | SRV |
| Prioridad | 0 |
| Importancia | 0 |
| Puerto | 1688 |
| Nombre de host | FQDN del host KMS |

Para que un servidor DNS BIND  8.2 o superior sea compatible con la publicación automática de KMS, configure el servidor BIND para habilitar las actualizaciones de registros de recursos desde hosts KMS. Por ejemplo, agregue la siguiente línea a la definición de zona en named.conf:

allow-update { any; };

Nota:   También se puede agregar una declaración de allow-update en named.conf.options para permitir el servicio de DDNS para todas las zonas hospedadas en este servidor.

### Deshabilitación de la publicación de registros SRV de KMS en DNS

Los hosts KMS publican su existencia de forma automática y crean registros de recursos SRV en el servidor DNS. Para deshabilitar la publicación automática de un host KMS, use el script Slmgr.vbs con la opción de línea de comandos **/cdns**.

Se prefiere el uso del script Slmgr.vbs para deshabilitar la publicación automática en DNS, pero también puede realizar esta tarea mediante la creación de un nuevo valor **DWORD** llamado **DisableDnsPublishing** en el Registro y la configuración de su valor en **1**. Este valor se encuentra en **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** del Registro. Para volver a habilitar el comportamiento predeterminado para la publicación de registros SRV de KMS en DNS, configure el valor en **0**.

## Instalación de hosts KMS

Para habilitar las funciones de KMS, se instala una clave KMS en un host KMS y, a continuación, se lo activa por Internet o por teléfono mediante los servicios de activación de Microsoft. Los equipos que ejecutan Windows 7 o Windows Server 2008 R2 pueden funcionar como hosts KMS.

Los equipos con Windows Vista, Windows Server 2003 y Windows Server 2008 también pueden funcionar como hosts KMS. Los clientes KMS que se pueden activar con un host KMS dependen de la clave de host que se usa para activar el host KMS. Para obtener más información sobre las claves de host KMS, consulte la *[Guía de planeación de Volume Activation](http://go.microsoft.com/fwlink/?LinkId=155926)*.

Instale y active una clave KMS en un equipo con Windows 7 o Windows Server 2008 R2 mediante un símbolo del sistema elevado:

* Para instalar una clave KMS, escriba **slmgr.vbs /ipk <ClaveKms>** en el símbolo del sistema.
* Para realizar la activación por Internet, escriba **slmgr.vbs /ato** en un símbolo del sistema.
* Para realizar la activación por teléfono, escriba **slui.exe 4** en un símbolo del sistema.

Después de activar la clave KMS, reinicie el servicio de protección de software.

Windows 7 y Windows Server 2008 R2 muestran la advertencia que aparece en la figura 1 cuando los administradores instalan una clave de host KMS mediante el uso de la interfaz de usuario (UI). (Los usuarios no verán esta advertencia si instalan una clave de host KMS mediante el uso del script Slmgr.vbs). Este mensaje evita que se instale de forma accidental una clave KMS en equipos que los administradores no desean que sean hosts KMS.



Figura 1.   Advertencia de clave KMS

Para comprobar que el host KMS se haya configurado correctamente, controle el número de KMS para ver si está aumentando. En la ventana del símbolo de sistema del host KMS, escriba **slmgr.vbs /dli** para ver el número de KMS actual. Los administradores también pueden comprobar el evento con Id. 12290 en el registro del Servicio de administración de claves en la carpeta Registros de aplicaciones y servicios. El registro del Servicio de administración de claves realiza un seguimiento de las solicitudes de activación de los clientes KMS. Con cada evento, se muestra el nombre del equipo y la marca de hora de cada solicitud de activación.

## Configuración de clientes KMS

En esta sección se describen los procedimientos para la instalación y la configuración de equipos como clientes KMS. De forma predeterminada, las ediciones de licencia por volumen de Windows Vista, Windows 7, Windows Server 2008 y Windows Server 2008 R2 son clientes KMS. Si los equipos que la organización desea activar mediante KMS usan cualquiera de estos sistemas operativos y la red permite la detección automática de DNS, no se necesita configuración adicional.

Si un cliente KMS está configurado para buscar un host KMS mediante DNS, pero no recibe registros SRV de DNS, Windows 7 y Windows Server 2008 R2 registran el error en el registro de eventos.

### Especificación manual de un host KMS

Los administradores pueden asignar de forma manual un host KMS a los cliente KMS mediante el uso del almacenamiento en caché del host KMS. La asignación manual de un host KMS deshabilita la detección automática de KMS en el cliente KMS. Para asignar de forma manual un host KMS a un cliente KMS, ejecute:

slmgr.vbs /skms <valor>:<puerto>

donde valor es KMS\_FQDN, IPv4Address o NetbiosName del host KMS y puerto es el puerto TCP en el host KMS.

### Habilitación de la detección automática de un cliente KMS

De forma predeterminada, los clientes KMS intentan descubrir hosts KMS automáticamente. Puede deshabilitar la detección automática si asigna un host KMS a un cliente KMS de forma manual. Esta acción también borra el nombre del host KMS de la caché del cliente KMS. Si deshabilita la detección automática y, luego, desea volver a habilitarla, ejecute **slmgr.vbs /ckms** en un símbolo del sistema.

### Adición de entradas con sufijo en clientes KMS

Si se agrega la dirección de un servidor DNS que contiene los registros de recursos SRV como una entrada con sufijo en clientes KMS, los administradores pueden anunciar los hosts KMS en un servidor DNS y dejar que los clientes KMS con otros servidores DNS primarios la encuentren. Para obtener más información sobre la configuración de una lista de búsqueda de sufijos de dominio en clientes KMS, consulte el artículo de ayuda y soporte de Microsoft “Cómo configurar una lista de búsqueda de sufijos de dominio en clientes KMS” en <http://support.microsoft.com/kb/275553>.

### Implementación de clientes KMS

La información de esta sección es para clientes de licencias por volumen que usan el Kit de instalación automatizada de Windows (Windows AIK) para implementar y activar un sistema operativo Windows. Prepare los clientes KMS para la implementación meditante el uso de la Herramienta de preparación del sistema (Sysprep) o del script Slmgr.vbs:

* **Sysprep.** Antes de capturar una imagen, ejecute Sysprep con la opción de línea de comandos **/generalize** para restablecer el temporizador de activación, el identificador de seguridad (SID) y otras configuraciones importantes. El restablecimiento del temporizador de activación evita que expire el período de gracia de la imagen antes de que se implemente. La ejecución de Sysprep.exe no quita la clave de producto instalada, y a los administradores no se les solicita una nueva clave durante la instalación mínima. Si no se deja ninguna reinstalación, la operación de Sysprep se completa, pero los temporizadores de activación no se cambian, y se devuelve un error que explica la situación.
* **Slmgr.vbs.** Cuando se crean equipos virtuales (VM) de demostración (VM) para uso interno (por ejemplo: la creación de VM para el departamento de ventas de la organización o para establecer un entorno temporal de capacitación), la ejecución del script Slmgr.vbs con la opción de línea de comandos **/rearm** extiende el período de gracia otros 30 días, que a su vez, restablece el temporizador de activación, pero no realiza ningún otro cambio en el equipo. El temporizador de activación puede restablecerse tres veces en los equipos que ejecutan Windows 7 o Windows Server 2008 R2.

### Activación manual de un cliente KMS

De forma predeterminada, los clientes KMS intentan realizar la activación automáticamente a intervalos preestablecidos. Para activar de forma manual clientes KMS (por ejemplo, clientes desconectados) antes de distribuirlos a los usuarios, use el elemento Sistema del Panel de control o ejecute **slmgr.vbs /ato** en un símbolo del sistema elevado. El script Slmgr.vbs informa si la activación se realizó de manera correcta o incorrecta y proporciona un código de resultado. Para realizar la activación, el cliente KMS debe tener acceso al host KMS en la red de la organización.

### Conversión de clientes MAK a KMS, y viceversa

De forma predeterminada, los sistemas operativos Windows 7 y Windows Server 2008 R2 usan KMS para la activación. Para cambiar clientes KMS existentes a clientes MAK, simplemente instale una clave MAK. Del mismo modo, para cambiar clientes MAK a clientes KMS, ejecute:

slmgr.vbs /ipk <ClavedeConfiguracióndeKMS>

ClavedeConfiguracióndeKMS es una de las claves de configuración que aparece en la tabla 4. Después de instalar la clave de configuración de KMS, active el cliente KMS. Para ello, ejecute **cscript slmgr.vbs /ato**.

Tabla 4.   Claves de configuración del cliente KMS

| Edición del sistema operativo | Clave de producto |
| --- | --- |
| Windows 7 |
| Windows 7 Professional | FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4 |
| Windows 7 Professional N | MRPKT-YTG23-K7D7T-X2JMM-QY7MG |
| Windows 7 Enterprise | 33PXH-7Y6KF-2VJC9-XBBR8-HVTHH |
| Windows 7 Enterprise N | YDRBP-3D83W-TY26F-D46B2-XCKRJ |
| Windows 7 Enterprise E | C29WB-22CC8-VJ326-GHFJW-H9DH4 |
| Windows Server 2008 R2 |
| Windows Server 2008 R2 HPC Edition | FKJQ8-TMCVP-FRMR7-4WR42-3JCD7 |
| Windows Server 2008 R2 Datacenter | 74YFP-3QFB3-KQT8W-PMXWJ-7M648 |
| Windows Server 2008 R2 Enterprise | 489J6-VHDMP-X63PK-3K798-CPX3Y |
| Windows Server 2008 R2 para sistemas basados en Itanium | GT63C-RJFQ3-4GMB6-BRFB9-CB83V |
| Windows Server 2008 R2 Standard | YC6KT-GKW9T-YTKYR-T4X34-R7VHC |
| Windows Web Server 2008 R2 | 6TPJF-RBVHG-WBW2R-86QPH-6RTM4 |

### Conversión de ediciones de venta al por menor en activaciones de licencia por volumen

Las ediciones de venta al por menor de Windows 7 Professional y Windows Server 2008 R2 se pueden convertir en clientes KMS, siempre y cuando la organización haya adquirido las licencias por volumen correspondientes y cumpla con las especificaciones de los derechos de uso de productos. Para convertir las ediciones de Windows 7 Professional y todas las ediciones de Windows Server 2008 R2 de venta al por menor en clientes KMS, omita la página **Clave de producto** durante la instalación del sistema operativo. Cuando finalice la instalación, abra una ventana del símbolo del sistema elevado y escriba:

Slmgr.vbs /ipk <ClavedeConfiguración>

donde ClavedeConfiguración es la clave de configuración del cliente KMS de la tabla 4 que corresponde a la edición de Windows 7 o Windows Server 2008 R2.

# Activación MAK

La activación MAK se usa para activaciones individuales mediante los servicios de activación hospedados de Microsoft para los que no se necesitan renovaciones. Para obtener más información sobre la activación KMS, consulte la [Guía de planeación de Volume Activation](http://go.microsoft.com/fwlink/?LinkId=155926).

## Conversión de clientes KMS en activación MAK

Windows 7 y Windows Server 2008 R2 se instalan automáticamente como clientes KMS. Para convertir un cliente KMS en una activación MAK, instale una clave MAK. Las claves MAK se pueden instalar durante la instalación del sistema operativo o en cualquier momento después de haberlo instalado.

Se puede instalar una clave MAK en una imagen de referencia de Windows 7 y Windows Server 2008 R2 para que todas las instalaciones realizadas a partir de esa imagen utilicen la activación MAK en lugar de la activación KMS predeterminada. Así se elimina la necesidad de especificar una clave MAK en un archivo de instalación desatendida.

### Instalación de una MAK durante la instalación del sistema operativo

Los administradores pueden convertir un cliente KMS en cliente MAK durante la instalación inicial de Windows 7 o Windows Server 2008 R2 mediante la inclusión de una clave MAK en un archivo de instalación desatendida (Unattend.xml). El archivo Unattend.xml se puede utilizar con Setup.exe o con los Servicios de implementación de Windows. Para obtener más información, consulte el archivo de ayuda Referencia para la configuración desatendida de Windows en Windows AIK, disponible en <http://go.microsoft.com/fwlink/?LinkId=136976>. Para obtener un archivo de instalación desatendida de muestra, consulte el “Apéndice B: Archivo de instalación desatendida de muestra”.

Nota:   La clave MAK se almacena en texto sin cifrar en el archivo Unattend.xml. Durante una instalación desatendida, se copia el archivo Unattend.xml o AutoUnattend.xml en la carpeta %SystemRoot%\Panther del equipo de destino. Sin embargo, al concluir el proceso de configuración, el programa de configuración la reemplaza por “SENSITIVE\*DATA\*DELETED” (Datos confidenciales eliminados).

### Instalación de una MAK después de la instalación del sistema operativo

Es posible configurar una edición de volumen de Windows 7 o Windows Server 2008 R2 para que utilice la activación MAK desde el elemento Sistema del Panel de control o mediante la ejecución del script Slmgr.vbs:

* Para instalar una clave MAK mediante la aplicación Sistema, haga clic en el vínculo **Cambiar la clave de producto** y, a continuación, escriba la clave MAK en el cuadro de diálogo **Cambie la clave de producto para efectuar la activación**.
* Para instalar una clave MAK mediante Slmgr.vbs, ejecute el siguiente comando en el símbolo del sistema:

slmgr.vbs /ipk <ClavedeActivaciónMúltiple>

ClavedeActivaciónMúltiple es la clave MAK.

Si los usuarios instalan una clave MAK desde la interfaz de usuario, el cliente MAK intentará realizar la activación por Internet una vez. Si los usuarios instalan una clave MAK mediante el script Slmgr.vbs, el cliente MAK no intentará realizar la activación automática.

### Deshabilitación de la activación automática

Para deshabilitar la activación automática en un cliente MAK, configure el valor **DWORD** **Manual** del Registro como **1**. Este valor se encuentra en la subclave **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation** del Registro.

## Activación de clientes MAK

El cliente MAK intenta activarse por Internet en el próximo intervalo programado. Los administradores pueden forzar una activación inmediata por Internet, por teléfono o mediante Volume Activation Management Tool (VAMT).

Para confirmar la activación, seleccione la notificación “Windows está activado” en la bandeja del sistema. También puede escribir **slmgr.vbs /dli** en el símbolo del sistema para ver el estado de activación de un equipo.

### Activación de clientes MAK por Internet

Los clientes MAK se pueden activar por Internet de dos maneras:

* Haga clic en el vínculo **Haga clic aquí para activar Windows ahora** en el elemento Sistema del Panel de control. Windows informa si la activación se realizó correctamente. Si no es posible llevar a cabo la activación, el asistente le mostrará opciones adicionales.
* Ejecute **slmgr.vbs /ato** en el símbolo del sistema. Cuando se utiliza slmgr.vbs, no se muestran opciones adicionales.

### Activación de clientes MAK mediante un servidor proxy

Si el servidor proxy requiere autenticación de usuario, es posible que se bloquee la activación por Internet. En Microsoft Internet Security and Acceleration (ISA) Server, esta configuración se denomina Autenticación básica. Dado que las solicitudes de activación no presentan credenciales de usuario al servidor proxy, Microsoft recomienda no usar la autenticación básica con ISA Server ni otros servidores proxy. Sin embargo, si es necesario utilizar la autenticación básica o un mecanismo comparable en el servidor proxy, agregue las siguientes direcciones URL a la lista **Exclusiones de autenticación de proxy**:

http://go.microsoft.com/\*

https://sls.microsoft.com/\*

https://sls.microsoft.com:443

http://crl.microsoft.com/pki/crl/products/MicrosoftRootAuthority.crl

http://crl.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunications.crl

http://www.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunications.crl

http://crl.microsoft.com/pki/crl/products/MicrosoftProductSecureServer.crl

http://www.microsoft.com/pki/crl/products/MicrosoftProductSecureServer.crl

### Activación de clientes MAK por teléfono

Para activar equipos que están conectados con la red de la organización, pero que no tienen conexión a Internet, use Slmgr.vbs. En la ventana del símbolo de sistema, escriba :

slmgr.vbs NombredeEquipodeDestino <NombredeUsuario> <Contraseña> /dti

a fin de mostrar la información requerida para completar la activación por teléfono. Para obtener el número de teléfono de un Centro de atención telefónica de activaciones en su región, ejecute **slui.exe 4**. Use el sistema de Respuesta interactiva de voz para obtener el identificador de confirmación (CID) y, a continuación, ejecute:

slmgr.vbs NombredeEquipodeDestino <NombredeUsuario> <Contraseña> /atp <CID>

para instalar el CID. Si la activación se realiza con frecuencia o si se activan varios equipos, es posible que sea más útil automatizar el proceso mediante el script Slmgr.vbs.

### Activación de clientes MAK mediante la herramienta VAMT

VAMT permite automatizar la implementación y la activación de claves MAK en la red mediante la distribución de las claves MAK desde una consola centralizada, como se muestra en la figura 2. VAMT consulta los servidores de activación de Microsoft para obtener la cantidad de activaciones restantes en una clave MAK determinada y, a continuación, enumera el estado de activación de todos los sistemas activados con MAK del entorno. Esta cantidad es una instantánea puntual, no se actualiza en tiempo real. Windows AIK incluye VAMT 1.2, que se puede descargar del Centro de descarga de Microsoft en <http://go.microsoft.com/fwlink/?LinkId=136976>.



Figura 2.   Interfaz de usuario de VAMT

### Deshabilitación de la activación automática

La activación automática puede deshabilitarse en cualquier cliente KMS mediante la configuración del valor **DWORD** existente **Manual** en **1**. Este valor se encuentra en la subclave **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation** del Registro.

## Integración de claves MAK con Deployment Workbench

Microsoft Deployment Toolkit (MDT) también incluye una solución para la implementación de claves MAK. En Deployment Workbench, los administradores configuran la clave MAK en secuencias de tareas, lo que hace que la clave MAK se agregue al archivo Unattend.xml que se utiliza durante la instalación. Los administradores pueden preparar la imagen de referencia para la activación KMS y, luego, durante la implementación, MDT activa la instalación mediante una clave MAK si no detecta una infraestructura de KMS. MDT aplica la clave MAK después de instalar la imagen. Para obtener más información sobre MDT, consulte **Deployment TechCenter** en <http://technet.microsoft.com/en-us/deployment/default.aspx>.

# Reactivación de equipos

En forma periódica, Windows 7 y Windows Server 2008 R2 comprueban la configuración de hardware del equipo en que está instalado el sistema operativo. Si el sistema operativo detecta que el hardware es sustancialmente diferente, es necesario llevar a cabo una reactivación. Los factores y los umbrales que se consideran varían, dado que estos valores deben seguir el ritmo del mercado de hardware informático, que se encuentra en evolución constante. En general, los equipos que utilizan la activación MAK usan las mismas reglas de reactivación que las de la activación de ediciones de venta al por menor. Los clientes KMS se centran más en los cambios en el disco duro para determinar la necesidad de reactivación.

Las activaciones cliente son válidas durante 180 días. Este período se denomina intervalo de validez de la activación. Para permanecer activados, los clientes KMS deben renovar su activación conectándose al host KMS al menos una vez cada 180 días. De forma predeterminada, los equipos cliente KMS intentan renovar su activación cada siete días. Una vez que se renueva la activación del cliente, el intervalo de validez de la activación comienza nuevamente.

# Apéndice A: Configuraciones opcionales

Volume Activation es compatible con configuraciones opcionales que pueden funcionar en algunos entornos, pero no son recomendables para la mayoría. Los procedimientos de este apéndice requieren que se reinicie el Servicio de protección de software antes de que tengan efecto.

## Habilitación de la activación por parte del usuario estándar

Para habilitar la activación por parte de usuarios estándar en un cliente KMS, agregue un nuevo valor **DWORD** de Registro denominado **UserOperations** y establezca el valor en **1**. Cree este valor en la subclave **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** del Registro.

Cuando se complete este procedimiento, ya no se requieren derechos administrativos para algunas operaciones, como la instalación de una clave de producto (**slmgr.vbs /ipk**), la instalación de una licencia (**slmgr.vbs /ilc**) o la reinstalación (**slmgr.vbs /rearm**). Esto significa que un usuario estándar podrá cambiar un cliente KMS a la activación MAK, activar un equipo de forma manual y, si es necesario, reemplazar una MAK existente con una nueva. Sin embargo, este procedimiento no es recomendable, dado que disminuye la seguridad del equipo.

Nota:   Si un usuario estándar instala una clave MAK o KMS, los valores del registro correspondientes a **ProductID** no se actualizan. Este comportamiento afecta principalmente al soporte del producto, y los Servicios de soporte al cliente (CSS) de Microsoft están al tanto de la situación.

## Deshabilitación de las notificaciones de activación

Aunque esta acción no se recomienda, las notificaciones de licencias de software se pueden desactivar si agrega un nuevo valor **DWORD** denominado **NotificationDisabled** con un valor de **1** al Registro. Cree este valor en la subclave **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation** del Registro. Este valor deshabilita todas las notificaciones de licencias de software, incluidos los diálogos, los asistentes y los cuadros de diálogo de las tareas.

## Modificaciones de claves del registro para funciones de activación

Windows 7 y Windows Server 2008 R2 incluyen una nueva clave de Plataforma de protección de software (SPP) en el Registro. Para la activación del producto en entornos administrados, configure el cuadro de diálogo **Activar Windows ahora** a fin de que se muestre el vínculo opcional **Información sobre la activación en línea**, como aparece en la figura 3.



Figura 3.   Obtener información sobre la activación en línea

Al hacer clic en este vínculo personalizado, se carga una dirección URL definida por el administrador en el explorador predeterminado del usuario. Esta dirección URL puede ser una página web personalizada u otro archivo almacenado en el equipo local o en un recurso compartido de red. Un cliente de licencias por volumen puede usar este vínculo para proporcionar información específica del cliente sobre la activación. Para poder visualizar este vínculo, se debe configurar el valor **REG\_SZ** **ActivationAlternateURL** para la dirección URL de la página web que se desea mostrar cuando el usuario hace clic en el vínculo. El valor **ActivationAlternateURL** se encuentra en la subclave **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** del Registro.

# Apéndice B: Archivo de instalación desatendida de muestra

<?xml version="1.0" encoding="utf-8"?>

<unattend xmlns="urn:schemas-microsoft-com:unattend">

    <settings pass="windowsPE">

        <component name="Microsoft-Windows-Setup" processorArchitecture="x86" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <UserData>

                <AcceptEula>true</AcceptEula>

            </UserData>

</component>

    </settings>

    <settings pass="specialize">

        <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="x86" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <ProductKey>Clave de producto MAK</ProductKey>

</component>

    </settings>

<cpi:offlineImage cpi:source="" xmlns:cpi="urn:schemas-microsoft-com:cpi" />

</unattend>