**Guía de Volume Activation hospedado por cliente**

**Windows 7 y Windows Server 2008 R2**

Microsoft Corporation

Fecha de publicación: junio de 2009

Resumen

Microsoft® Volume Activation ayuda a los clientes de licencias por volumen a automatizar y administrar el proceso de activación de medios de licencias por volumen. Los clientes de licencias por volumen y los suscriptores de programas especiales, como Microsoft Partner Program, MSDN® y Microsoft TechNet, son elegibles para adquirir medios y software de licencias por volumen. Esta guía está dirigida a los profesionales de TI cuyas organizaciones planean implementar versiones de Volume Activation de los sistemas operativos Windows® 7 y Windows Server® 2008 R2 mediante el Servicio de administración de claves.

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, 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 los contenidos 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. Reservados todos los derechos.

Microsoft, Hyper-V, MSDN, Windows, el logotipo de Windows, Windows NT, Windows 7, Windows Server, Windows Vista y Windows Web Server 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**

[Introducción 1](#_Toc236543928)

[Información sobre KMS 2](#_Toc236543929)

[Requisitos mínimos del equipo 2](#_Toc236543930)

[Umbrales de activación KMS 2](#_Toc236543931)

[Caché de recuento de activación 3](#_Toc236543932)

[Cómo funciona KMS 4](#_Toc236543933)

[Renovación de la activación KMS 4](#_Toc236543934)

[Publicación del servicio KMS 4](#_Toc236543935)

[Detección de clientes del servicio KMS 5](#_Toc236543936)

[Planeación de una implementación de KMS 6](#_Toc236543937)

[Planeación de la configuración del servidor DNS 6](#_Toc236543938)

[Activación del primer host KMS 7](#_Toc236543939)

[Activación de los hosts KMS posteriores 8](#_Toc236543940)

[Actualización de hosts KMS existentes 8](#_Toc236543941)

[Planeación de clientes KMS 8](#_Toc236543942)

[Activación como usuario estándar 9](#_Toc236543943)

[Determinación de las necesidades de claves de producto 10](#_Toc236543944)

[Selección de la clave KMS 10](#_Toc236543945)

[Selección del host KMS 11](#_Toc236543946)

[Implementación de activación KMS 13](#_Toc236543947)

[Configuración de hosts KMS 13](#_Toc236543948)

[Ejecución de Slmgr.vbs de forma remota 15](#_Toc236543949)

[Configuración de Firewall de Windows para operaciones remotas del administrador de licencias de software 15](#_Toc236543950)

[Operaciones remotas dirigidas a equipos de un grupo de trabajo 16](#_Toc236543951)

[Configuración del DNS 16](#_Toc236543952)

[Cambio de los permisos DNS predeterminados para registros SRV 16](#_Toc236543953)

[Publicación en múltiples dominios DNS 17](#_Toc236543954)

[Creación manual de registros SRV en DNS 18](#_Toc236543955)

[Creación manual de registros SRV en un servidor BIND 8.2 o superior 19](#_Toc236543956)

[Deshabilitación de la publicación de registros SRV de KMS en DNS 20](#_Toc236543957)

[Instalación de hosts KMS 21](#_Toc236543958)

[Configuración de clientes KMS 22](#_Toc236543959)

[Especificación manual de un host KMS 22](#_Toc236543960)

[Habilitación de la detección automática de un cliente KMS 23](#_Toc236543961)

[Adición de entradas con sufijo en clientes KMS 23](#_Toc236543962)

[Implementación de clientes KMS 23](#_Toc236543963)

[Activación manual de un cliente KMS 24](#_Toc236543964)

[Conversión de clientes MAK a KMS, y viceversa 24](#_Toc236543965)

[Conversión de ediciones de venta al por menor a Volume Activation 25](#_Toc236543966)

[Reactivación de equipos 26](#_Toc236543967)

# Introducción

Microsoft® Volume Activation es una solución configurable que permite a los profesionales de TI automatizar y administrar el proceso de activación de productos en equipos que ejecutan los sistemas operativos Windows Vista®, Windows® 7, Windows Server® 2008 y Windows Server 2008 R2 otorgados bajo un programa de licencias por volumen de Microsoft y otros programas que ofrecen ediciones de licencias por volumen de Windows.

Esta guía proporciona información para la planeación, la implementación y las operaciones, específicamente para los sistemas operativos Windows 7 y Windows Server 2008 R2. Esta guía es para organizaciones que hospedan sus propias infraestructuras de Volume Activation mediante el Servicio de administración de claves (KMS).

**Nota:** Este documento proporciona una guía de Volume Activation para los sistemas operativos Windows 7 y Windows Server 2008 R2. Para obtener más información sobre la planeación de Volume Activation para Windows Vista y Windows Server 2008, consulte la **Guía técnica de Volume Activation 2.0** en <http://go.microsoft.com/fwlink/?LinkID=75674>. Esta guía aborda la interoperabilidad entre ambas generaciones de productos.

# Información sobre KMS

KMS activa los equipos en una red local, lo que elimina la necesidad de conectar los equipos individuales a Microsoft. Para ello, KMS usa una topología de cliente-servidor. Los equipos cliente KMS pueden ubicar los equipos de host KMS mediante el Sistema de nombres de dominio (DNS) o una configuración estática. Los clientes KMS se conectan con el host KMS mediante una llamada a procedimiento remoto (RPC). KMS se puede hospedar en equipos que ejecutan los sistemas operativos Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008 o Windows Server 2008 R2.

## Requisitos mínimos del equipo

En la planeación de la activación KMS, la red debe alcanzar o superar el umbral de activación, es decir, la cantidad mínima de equipos calificados que requiere KMS. Los profesionales de TI también deben comprender cómo el host KMS realiza un seguimiento de la cantidad de equipos que hay en la red.

### Umbrales de activación KMS

KMS puede activar tanto equipos físicos como virtuales. Para poder obtener acceso a la activación KMS, una red debe alcanzar el umbral de activación: los hosts KMS activan equipos cliente únicamente cuando se alcanza este umbral. A fin de asegurarse de que se alcance el umbral de activación, un host KMS cuenta la cantidad de equipos que solicitan activación en la red. Para los equipos que ejecutan Windows Server 2008 o Windows Server 2008 R2, el umbral de activación es 5. Para los equipos que ejecutan Windows Vista o Windows 7, el umbral de activación es 25. Los umbrales incluyen equipos cliente y servidores que se ejecutan en equipos físicos o virtuales.

Un host KMS responde a cada solicitud de activación válida de un cliente KMS con el recuento de equipos que se conectaron con el host KMS para la activación. Los clientes que reciben un recuento inferior al umbral de activación no se activan. Por ejemplo, si los primeros dos equipos que se conectan con el host KMS ejecutan Windows 7, el primero recibe un recuento de activación 1, y el segundo recibe un recuento de activación 2. Si el equipo siguiente es un equipo virtual de Windows 7, recibe un recuento de activación 3, y así sucesivamente. Ninguno de estos equipos se activa, dado que los equipos que ejecutan Windows 7 deben recibir un recuento de activación igual o superior a 25 para poder ser activados. Los clientes KMS en estado de gracia que no se activan debido a que el recuento de activación es muy bajo se conectan con el host KMS cada dos horas para obtener el recuento de activación actual y se activarán cuando se alcance el umbral.

Si el equipo siguiente que se conecta con el host KMS ejecuta Windows Server 2008 R2, recibe el recuento de activación  4, dado que los recuentos de activación son una combinación de equipos que ejecutan Windows Server 2008 R2 y Windows 7. Si un equipo que ejecuta Windows Server 2008 o Windows Server 2008 R2 recibe un recuento de activación igual o superior a 5, se activa. Si un equipo que ejecuta Windows 7 recibe un recuento de activación igual o superior a 25, se activa.

### Caché de recuento de activación

Para realizar un seguimiento del umbral de activación, el host KMS lleva un registro de los equipos cliente KMS que solicitan la activación. El host KMS proporciona a cada equipo cliente KMS una designación de identificación de equipo cliente (CMID), y el host KMS guarda cada CMID en una tabla. Cada solicitud de activación permanece en la tabla durante 30 días. Cuando un equipo cliente renueva su activación, se quita la CMID almacenada en caché de la tabla, se crea un registro nuevo y comienza nuevamente el período de 30 días. Si un equipo cliente KMS no renueva su activación en un plazo de 30 días, el host KMS quita la CMID correspondiente de la tabla y reduce el recuento de activación a uno.

El host KMS almacena en la memoria caché dos veces la cantidad de CMID que los clientes KMS requieren para garantizar que el recuento de CMID no sea inferior al umbral de activación. Por ejemplo, en una red con equipos cliente que ejecutan Windows 7, el umbral de activación KMS es 25. El host KMS almacena en la memoria caché las CMID de las 50 activaciones más recientes. El umbral de activación KMS para Windows Server 2008 R2 es 5. Un host KMS que solamente se conecta con equipos cliente KMS que ejecutan Windows Server 2008 R2 almacenan en la memoria caché los 10 CMID más recientes. Si un equipo cliente que ejecuta Windows 7 se conecta posteriormente con ese host KMS, KMS aumenta el tamaño de la memoria caché a 50 para adecuarse al umbral más alto. KMS nunca reduce el tamaño de la memoria caché.

## Cómo funciona KMS

La activación KMS requiere conectividad TCP/IP. De forma predeterminada, los equipos cliente y los hosts KMS usan DNS para publicar y buscar el servicio KMS. Se puede usar la configuración predeterminada, que no requiere prácticamente ninguna acción administrativa, o los equipos cliente y los hosts KMS se pueden configurar de forma manual, de acuerdo con los requisitos de seguridad y configuración de la red.

### Renovación de la activación KMS

Las activaciones KMS son válidas durante 180 días: el intervalo de validez de la activación. Para permanecer activados, los equipos cliente 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. Si no se realiza la activación KMS, el cliente intentará realizarla cada dos horas. Una vez que se renueva la activación del equipo cliente, el intervalo de validez de la activación comienza nuevamente.

### Publicación del servicio KMS

El servicio KMS usa registros de recursos (RR) de servicios (SRV) en DNS para almacenar y comunicar las ubicaciones de los hosts KMS. Los hosts KMS usan el protocolo de actualización dinámica DNS, si está disponible, para realizar la publicación de registros de recursos SRV de KMS. Si la actualización dinámica no está disponible o el host KMS no dispone de los derechos para publicar los registros de recursos, los registros de DNS se deben publicar de forma manual, o se deben configurar los equipos cliente para que se conecten con hosts KMS específicos.

**Nota:** Es posible que los cambios de DNS tarden en propagarse a todos los hosts DNS, según la complejidad y la topología de la red.

### Detección de clientes del servicio KMS

De forma predeterminada, los clientes KMS consultan al DNS en busca de la información del servicio KMS. La primera vez que un cliente KMS consulta al servidor DNS respecto de la información del servicio KMS, selecciona al azar un host KMS de la lista de registros de recursos SRV que proporciona el DNS.

La dirección de un servidor DNS que contiene los registros de recursos SRV se puede enumerar como una entrada con sufijo en clientes KMS, lo que permite la publicación de los registros de recursos SRV para que KMS en un servidor DNS y clientes KMS con otros servidores DNS primarios puedan encontrarla.

Los parámetros prioridad e importancia se pueden agregar al valor de registro **DnsDomainPublishList** para KMS. Al establecer agrupaciones de prioridad de hosts KMS y al realizar consideraciones dentro de cada grupo, puede especificar qué host KMS deben probar primero los clientes, y se equilibra el tráfico entre los diversos hosts KMS. Solo Windows 7 y Windows Server 2008 R2 proporcionan los parámetros prioridad e importancia.

Si el host KMS que selecciona un cliente no responde, el cliente KMS quita ese host KMS de la lista de registros de recursos SRV y selecciona de manera aleatoria otro host KMS de la lista. Cuando un host KMS responde, el cliente KMS almacena en la memoria caché el nombre del host KMS y lo usa para los siguientes intentos de activación y renovación. Si el host KMS almacenado en la memoria caché no responde en una renovación posterior, el cliente KMS detecta un nuevo host KMS al consultar al DNS sobre los registros de recursos SRV de KMS.

De forma predeterminada, los equipos cliente se conectan con el host KMS para la activación mediante RPC anónimas a través del puerto TCP 1688 (se puede cambiar el puerto predeterminado). Después de establecer una sesión TCP con el host KMS, el cliente envía un paquete con una sola solicitud. El host KMS responde con el recuento de activación. Si el recuento alcanza o supera el umbral de activación para ese sistema operativo, el cliente se activa y la sesión se cierra. El cliente KMS usa este mismo proceso para las solicitudes de renovación. La comunicación bidireccional es de 250 bytes.

## Planeación de una implementación de KMS

El servicio KMS no requiere un servidor dedicado. El servicio KMS puede hospedarse con otros servicios, como controladores de dominio de solo lectura (RODC) y controladores de dominio de Servicios de dominio de Active Directory® (AD DS). Los hosts KMS también se pueden ejecutar en equipos físicos o virtuales que ejecuten cualquier sistema operativo Windows compatible, incluido Windows Server 2003. Si bien un host KMS que ejecuta Windows Server 2008 R2 puede activar cualquier sistema operativo Windows que sea compatible con Volume Activation, un host KMS que ejecuta Windows 7 solamente puede activar equipos que ejecutan clientes de Windows 7 y Windows Vista. Un solo host KMS puede admitir cantidades ilimitadas de clientes KMS; no obstante, Microsoft recomienda implementar un mínimo de dos hosts KMS en caso de conmutación por error. La mayoría de las organizaciones pueden usar tan solo dos hosts KMS para toda su infraestructura.

**Nota:** KMS no se incluye automáticamente en Windows Server 2003. Para hospedar KMS en equipos que ejecutan Windows Server 2003, descargue e instale KMS de uno de los siguientes sitios:

* Para equipos basados en x86, consulte **Servicio de administración de claves 1.1 (x86) para Windows Server 2003 SP1 y posterior** en <http://go.microsoft.com/fwlink/?LinkID=82964>.
* Para equipos basados en x64, consulte **Servicio de administración de claves 1.1 (x64) para Windows Server 2003 SP1 y posterior** en <http://go.microsoft.com/fwlink/?LinkId=83041>.

### Planeación de la configuración del servidor DNS

La función predeterminada de publicación automática de KMS requiere la compatibilidad con el registro de recursos SRV y el protocolo de actualización dinámica DNS. El comportamiento predeterminado del cliente KMS y la publicación de registros de recursos SRV de KMS se admiten en un servidor DNS que ejecuta el software de Microsoft y cualquier otro servidor DNS que admita los registros de recursos SRV (por Internet Engineering Task Force [IETF] Request for Comments [RFC] 2782) y actualizaciones dinámicas (por RFC 2136). Por ejemplo, las versiones 8.x y 9.x de Berkeley Internet Domain Name (BIND) admiten registros de recursos SRV y actualizaciones dinámicas.

El host KMS se debe configurar de modo tal que tenga las credenciales necesarias para crear y actualizar los registros de recursos SRV, A (Protocolo de Internet versión 4 o IPv4) y AAAA (Protocolo de Internet versión 6 o IPv6) en los servidores DNS, o los registros necesarios para crearlos de forma manual. La solución recomendada para otorgarle al host KMS las credenciales necesarias es crear un grupo de seguridad en AD DS y agregar todos los hosts KMS a dicho grupo. En el servidor DNS que ejecuta el software de Microsoft, asegúrese de otorgar a este grupo de seguridad un control total sobre el registro \_VLMCS.\_TCP en cada dominio DNS que vaya a contener los registros de recursos SRV de KMS.

### Activación del primer host KMS

Los hosts KMS de la red deben instalar una clave KMS y, a continuación, se deben activar con Microsoft. La instalación de una clave KMS habilita el Servicio de administración de claves en el host KMS. Después de instalar la clave KMS, complete la activación del host KMS en línea o por teléfono. Después de esta activación inicial, los hosts KMS no comunican ningún tipo de información a Microsoft.

Las claves KMS solo se instalan en hosts KMS y nunca en clientes KMS individuales. Windows 7 y Windows Server 2008 R2 cuentan con medidas de seguridad para ayudar a evitar la instalación accidental de claves KMS en equipos cliente KMS. Cada vez que los usuarios intenten instalar una clave KMS, aparecerá la advertencia que se muestra en la figura 1.

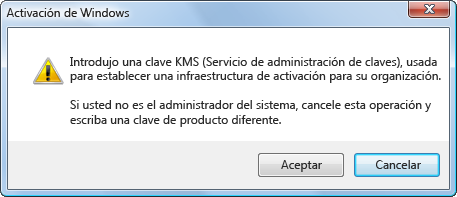


Figura 1. Instalación de una clave KMS

### Activación de los hosts KMS posteriores

Cada clave KMS se puede instalar en hasta seis hosts KMS, que pueden ser equipos físicos o virtuales. Una vez activado un host KMS, es posible volver a activarlo hasta nueve veces más con la misma clave.

Si la organización necesita más de seis hosts KMS, puede solicitar activaciones adicionales para la clave KMS de la organización llamando al Centro de atención telefónica de activaciones para solicitar una excepción. Para obtener más información, visite el sitio web de licencias por volumen en <http://go.microsoft.com/fwlink/?LinkID=73076>.

### Actualización de hosts KMS existentes

Los hosts KMS que ejecutan Windows Server 2003, Windows Vista o Windows Server 2008 se pueden configurar para admitir clientes KMS que ejecutan Windows 7 y Windows Server 2008 R2. Para Windows Vista y Windows Server 2008, es necesario actualizar el host KMS con un paquete con archivos que admitan el cliente KMS expandido. Este paquete está disponible por medio del Centro de descarga de Microsoft en <http://www.microsoft.com/downloads>, o por medio de Windows Update y Windows Server Update Services (WSUS). Una vez instalado el paquete en el host KMS, se puede instalar y activar una clave KMS diseñada para admitir Windows 7 y Windows Server 2008 R2 de la manera descrita anteriormente en esta guía. La clave KMS que admite las versiones nuevas de los sistemas operativos Windows también ofrece compatibilidad con las ediciones anteriores de licencias por volumen de Windows que actúan como clientes KMS.

En el caso de actualización de un host KMS con Windows Server 2003, todos los archivos necesarios se incluyen en el paquete descargable de KMS 1.2, que está disponible por medio del Centro de descarga de Microsoft, en <http://www.microsoft.com/downloads>.

### Planeación de clientes KMS

De forma predeterminada, los equipos que ejecutan las ediciones de licencia por volumen de Windows Vista, Windows 7, Windows Server 2008 y Windows Server 2008 R2 son clientes KMS que no necesitan ninguna configuración adicional. Los clientes KMS pueden localizar un host KMS de manera automática al consultar el servicio de DNS sobre los registros de recursos SRV que publican el servicio KMS. Si el entorno de red no usa registros de recursos SRV, se puede configurar un cliente KMS de forma manual para que use un host KMS determinado.

Para configurar clientes KMS de forma manual, siga los pasos de la sección titulada “Especificación manual de un host KMS”, que aparece más adelante en esta guía.

### Activación como usuario estándar

Windows 7 y Windows Server 2008 R2 no requieren privilegios de administrador para la activación. No obstante, este cambio no permite a las cuentas de usuario estándar quitar del estado activado a Windows 7 o Windows Server 2008 R2. Se requiere una cuenta de administrador para otras tareas relacionadas con la activación o las licencias, como una “reinstalación”.

# Determinación de las necesidades de claves de producto

Los sistemas operativos Windows 7 y Windows Server 2008 R2 se suministran en varias ediciones. Para simplificar Volume Activation y la cantidad de claves de productos que una organización necesita, Microsoft creó *grupos de claves de producto*, en los que las claves de producto se aplican a grupos de productos en lugar de aplicarse a ediciones individuales.

## Selección de la clave KMS

Con KMS, las claves de producto están asociadas con un grupo de productos y pueden activar las ediciones de Windows dentro de ese grupo específico de productos, así como las ediciones en una posición inferior en la jerarquía de productos. El primer grupo menos inclusivo de la jerarquía es el grupo de productos de licencia por volumen de cliente, mientras que el grupo de servidores C es el grupo más inclusivo en la jerarquía de KMS.

Esta jerarquía se extiende a las agrupaciones de claves de producto y las ediciones de licencia por volumen de Windows Vista y Windows Server 2008. Se emitirán claves KMS independientes para cada agrupación de claves de producto, lo que implica que un cliente tendrá acceso a una clave KMS para licencias por volumen de cliente tanto de Windows 7 como de Windows Vista. La clave KMS para los productos Windows más nuevos también activará la generación anterior, lo que implica que un cliente podrá tener una única clave KMS para activar varias ediciones y generaciones de Windows. En la tabla 1, se muestra la correlación entre las agrupaciones de productos.

Tabla 1. Correlación de las agrupaciones de productos

| Grupo de claves de producto con licencia por volumen | Edición de Windows  (Windows 7 y Windows Server 2008 R2) | Edición de Windows  (Windows Vista y Windows Server 2008) |
| --- | --- | --- |
| Licencia por volumen de cliente | * Windows 7 Professional * Windows 7 Enterprise | * Windows Vista Business * Windows Vista Enterprise |
| Grupo de servidores A | * Windows Web Server® 2008 R2 * Windows Server 2008 R2 HPC Edition * Windows HPC Server 2008 R2 | * Windows Web Server 2008 * Windows Compute Cluster Server 2008 |
| Grupo de servidores B | * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise | * Windows Server 2008 Standard * Windows Server 2008 Enterprise * Incluye ediciones sin  Hyper-V™ |
| Grupo de servidores C | * Windows Server 2008 R2 Datacenter * Windows Server 2008 R2 para sistemas basados en Itanium | * Windows Server 2008 Datacenter * Windows Server 2008 para sistemas basados en Itanium * Incluye ediciones sin  Hyper-V |

## Selección del host KMS

Como se mencionó anteriormente en esta guía, KMS puede hospedarse en un sistema operativo cliente o servidor, en un equipo físico o virtual. Al seleccionar el sistema host KMS, tenga en cuenta las ediciones de los sistemas operativos que se activarán con KMS. Un KMS hospedado en Windows 7 puede activar solamente sistemas operativos cliente, pero un KMS hospedado en Windows Server 2008 R2 puede activar equipos cliente y servidor. Consulte la tabla 2 para obtener una explicación de esta jerarquía.

Tabla 2. Jerarquía de KMS

| Grupo de claves de producto | KMS puede hospedarse (la clave KMS activa el host KMS) | Ediciones de productos de Windows activadas por este host KMS |
| --- | --- | --- |
| Licencia por volumen de cliente para Windows 7 | * Windows Vista * Windows 7 * KMS para Windows Server 2003 1.2 | * Windows 7 Professional * Windows 7 Enterprise * Windows Vista Business * Windows Vista Enterprise |
| Grupo de servidores A para Windows Server 2008 R2 | * KMS para Windows Server 2003 1.2 * Windows Web Server 2008 * Windows Web Server 2008 R2 * Windows HPC Server 2008 * Windows HPC Server 2008 R2 | Incluye lo anterior más:   * Windows Web Server 2008 R2 * Windows Web Server 2008 * Windows HPC Server 2008 R2 * Windows HPC Server 2008 |
| Grupo de servidores B para Windows Server 2008 R2 | Incluye lo anterior más:   * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise * Windows Server 2008 Standard * Windows Server 2008 Enterprise | Incluye lo anterior más:   * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise * Windows Server 2008 Standard * Windows Server 2008 Enterprise |
| Grupo de servidores C | Incluye lo anterior más:   * Windows Server 2008 R2 Datacenter * Windows Server 2008 Datacenter * Windows Server 2008 para sistemas basados en Itanium | Incluye lo anterior más:   * Windows Server 2008 R2 Datacenter * Windows Server 2008 Datacenter * Windows Server 2008 para sistemas basados en Itanium |

# Implementación de activación KMS

La activación KMS requiere mínima intervención administrativa. Si el entorno de red tiene el 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. Modifique el Registro bajo su propia responsabilidad.

El resto de esta sección describe las siguientes tareas clave:

* Configuración de hosts KMS
* Configuración del DNS
* Instalación de hosts KMS
* 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 usted puede especificar qué motor de scripts desea usar. 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 ejecute 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 3, 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 3 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 /parameter

Tabla 3. 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, 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 el Firewall de Windows con seguridad avanzada 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, 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 “Publicación 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 AD DS 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 cree 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 AD DS, 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 tiene solamente un dominio DNS, no se requieren más acciones.

Si hay más de un nombre de dominio DNS, puede crear una lista de dominios DNS a fin de que la 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 solamente 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 le permite 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 desee publicar en el valor de Registro de cadena múltiple **DnsDomainPublishList** en la subclave **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** del Registro. 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 subclave del Registro y, luego, impórtela al registro en hosts KMS adicionales. Para comprobar que este procedimiento se haya llevado 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 2.0 en <http://technet.microsoft.com/en-us/library/cc303695.aspx>.

### 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 hosts 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 4, se proporciona una configuración de ejemplo para un registro de recursos SRV.

Tabla 4. Registro de recursos SRV

| Nombre | Configuración |
| --- | --- |
| Servicio | \_VLMCS |
| Protocolo | \_TCP |
| Número de puerto | 1688 |
| Host que ofrece este servicio | Nombre de dominio completo (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 es de Microsoft, se pueden crear los registros de recursos SRV necesarios si el servidor DNS es compatible con BIND 8.2 o superior. Cuando cree el registro, incluya la información que aparece en la tabla 5. La configuración Prioridad e Importancia que se muestra en la tabla 5 solo se usa en Windows 7 y Windows Server 2008 R2.

Tabla 5. 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 posterior 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 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 la subclave **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 la activación de claves de host KMS, consulte la Guía de planeación de Volume Activation 2.0 en <http://technet.microsoft.com/en-us/library/cc303276.aspx>.

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 KmsKey** en un 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 licencias de software.

Windows 7 y Windows Server 2008 R2 muestran la advertencia que aparece en la figura 2 cuando instala 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.

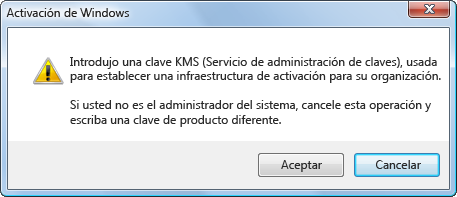


Figura 2. Advertencia de clave KMS

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. También puede 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

Puede 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. Asigne un host KMS a un cliente KMS de forma manual al ejecutar:

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 detectar 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, puede volver a habilitarla al ejecutar **slmgr.vbs /ckms** en un símbolo del sistema.

### Adición de entradas con sufijo en clientes KMS

Si agrega la dirección de un servidor DNS que contiene los registros de recursos SRV como una entrada con sufijo en clientes KMS, puede 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 no se le 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 de demostración para uso interno (por ejemplo: la creación de máquinas virtuales para el departamento de ventas de la organización o para establecer un entorno temporal de aprendizaje), la ejecución del script Slmgr.vbs con la opción de línea de comandos **/rearm** extiende el período de gracia otros 30 días, que a la 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 6. Después de instalar la clave de configuración de KMS, active el cliente KMS. Para ello, ejecute **cscript slmgr.vbs /ato**.

Tabla 6. 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 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 a Volume Activation

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 6 que corresponde a la edición de Windows 7 o Windows Server 2008 R2.

# 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 ha cambiado sustancialmente, 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. Los clientes KMS se centran en los cambios en el disco duro para determinar la necesidad de reactivación.

Las activaciones de los clientes son válidas durante 180 días: el 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.