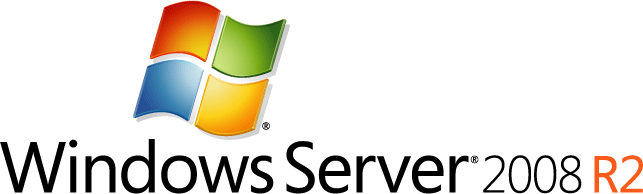
****

****  
  
**批量激活技术参考指南**

**Windows 7 和 Windows Server 2008 R2**

Microsoft Corporation

发布日期：2009 年 7 月

摘要

本参考指南面向其组织计划部署 Windows® 7 和 Windows Server® 2008 R2 操作系统的 Volume Activation 版本的信息技术 (IT) 实施人员。它是 *Volume Activation Planning Guide*（批量激活规划指南）、*Volume Activation Deployment Guide*（批量激活部署指南）和 *Volume Activation Operations Guide*（批量激活操作指南）的姊妹篇。

本文档以及其中引用的任何文档仅供参考，Microsoft 在本文档中未做任何明示或隐含的担保。本文档中的信息（包括 URL 和其他 Internet 网站参考）如有更改，恕不另行通知。使用本文档的全部风险或后果均由用户承担。除非另有说明，否则本文档举例所言公司、组织、产品、域名、电子邮件地址、徽标、人物、地点和事件均为虚构。Microsoft 无意将他们与任何真实的公司、组织、产品、域名、电子邮件地址、徽标、人物、地点或事件相关联，也不应推定为存在任何此类关联。使用者必须遵守所有适用的版权法律。在适用法律不限制版权权利的前提下，未经 Microsoft Corporation 明确书面许可，不得出于任何目的、以任何形式或借助任何手段（电子、机械、影印、录制或其他手段）对本文档任何部分进行复制、存储、引入检索系统或进行传播。

Microsoft 可能拥有本文档所涉及的专利权、专利申请权、商标权、版权或其他知识产权。除非 Microsoft 在任何书面许可协议中明确规定，否则提供本文档并不表示授予您上述专利权、商标权、版权或其他知识产权。

© 2009 Microsoft Corporation。

Microsoft、Active Directory、Hyper-V、Windows、Windows Server 和 Windows Vista 是 Microsoft 集团公司的商标。

此处提及的实际公司和产品的名称可能是其各自所有者的商标。

**目录**

[简介 1](#_Toc236817971)

[用户体验 3](#_Toc236817972)

[Slmgr.vbs 选项 6](#_Toc236817973)

[注册表设置 11](#_Toc236817974)

[组策略对象设置 14](#_Toc236817975)

[KMS 激活计时 15](#_Toc236817976)

[KMS 发现搜索顺序 16](#_Toc236817977)

[激活方案 17](#_Toc236817978)

[KMS 方案 17](#_Toc236817979)

[单站点网络的默认 KMS 实施 17](#_Toc236817980)

[复杂的全局网络中的 KMS 实施 18](#_Toc236817981)

[MAK 方案 20](#_Toc236817982)

[MAK 独立激活 21](#_Toc236817983)

[MAK 代理激活 24](#_Toc236817984)

[VAMT 对 KMS 激活提供的支持 29](#_Toc236817985)

[将 KMS 转换为使用 MAK 激活 30](#_Toc236817986)

[产品的 KMS 主机密钥 32](#_Toc236817987)

[激活策略值 34](#_Toc236817988)

[KMS 客户端安装密钥 35](#_Toc236817989)

[激活错误代码 37](#_Toc236817990)

[Windows 事件日志 43](#_Toc236817991)

[WMI 属性和方法 46](#_Toc236817992)

[术语表 53](#_Toc236817993)

[资源链接 54](#_Toc236817994)

# 简介

本指南为 [Volume Activation Planning Guide](http://go.microsoft.com/fwlink/?LinkId=155926)（批量激活规划指南）、[Volume Activation Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=150083)（批量激活部署指南）和 [Volume Activation Operations Guide](http://go.microsoft.com/fwlink/?LinkId=150084)（批量激活操作指南）提供了技术参考信息。有关 Microsoft® Volume Activation 及其组件的概述信息，请参阅 [Volume Activation Planning Guide](http://go.microsoft.com/fwlink/?LinkId=155926)（批量激活规划指南）。该参考资料包含：

* 用户体验
* Slmgr.vbs 选项
* 注册表设置
* 组策略对象 (GPO) 设置
* 密钥管理服务 (KMS) 激活计时
* KMS 发现搜索命令
* 激活方案
* 产品的 KMS 主机密钥
* 激活策略值
* KMS 客户端安装密钥
* 激活错误代码
* Windows® 事件日志
* Windows Management Instrumentation (WMI) 属性和方法
* 术语表
* 资源

**注：**有关使用 Volume Activation 的其他软件的支持信息，请参考专门为这些应用程序编写的文档。

本指南使用以下惯例：

* 命令行和命令行选项显示为粗体。
* 命令行选项中的占位符两边带有尖括号 (<>)。
* 可选命令行选项的两边带有方括号 ([])。
* 注册表子项和值名称显示为粗体。

# 用户体验

Windows® 7 和 Windows Server® 2008 R2 显示专为特定激活问题定制的通知和对话框。表 1 介绍了这些通知和对话框是如何与各个问题相对应的。

**注：**Windows Server 2008 核心版本不提供通知用户体验。

表 1. 通知状态的气球和对话框

| **问题** | **通知气球** | **相应的对话框** |
| --- | --- | --- |
| 新安装的  Windows 副本在激活宽限期结束时仍未被激活。 |  | C:\Users\Jerry\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\04T7PPNO\AlternateURL.JPG |
| 先前激活的 Windows 副本检测到计算机硬件或基本输入/输出系统 (BIOS) 发生了更改，需要重新激活 Windows。并且，已经激活的 KMS 客户端不会在 180 天内重新自行激活。 |  | 37-HW OOT.jpg |
| 使用 KMS 激活的 Windows  在 180 天外加 30 天的宽限 期内未续订其激活。 |  | 37-KMS OOT.jpg |
| 联机激活失败，或检测 到企图使 Windows  的未授权副 本绕过产品 激活的激活 破解行为。 |  | 37-NG.jpg |
| Windows  检测到某个 Windows  许可组件发 生了更改。 |  | 37 - No Key.jpg |
| Windows  检测到其许 可文件发生 了更改。 |  | 37 - Reinstall.jpg |

# Slmgr.vbs 选项

由于 Windows 7 和 Windows Server 2008 R2 两种系统的 WMI 有所不同，因此 Slmgr.vbs   
脚本不适合跨平台使用。不支持使用 Slmgr.vbs 从 Windows Vista® 操作系统来管理 Windows 7   
或 Windows Server 2008 R2 系统。如果试图管理 Windows 7 或 Windows Server 2008   
R2 中的下层系统，则会生成一个特定的版本不匹配错误。例如，运行 **cscript slmgr.vbs <Vista 计算机名> /dlv** 会产生以下输出结果：

Microsoft (R) Windows Script Host Version 5.8  
Copyright (C) Microsoft Corporation。All rights reserved.

远程计算机不支持此版本的 SLMgr.vbs

要管理远程客户端，请使用批量激活管理工具 (VAMT) 1.2 或更高版本，或创建可识别平台间差异的自定义 WMI 脚本。有关 Volume Activation 的 WMI 属性和方法的更多信息，请参阅本参考指南后面的“”一节。

以下内容介绍了 Slmgr.vbs 脚本的语法，表 2 介绍了各个命令行选项：

slmgr.vbs [计算机名 [用户名] [密码]] [<选项>]

**注：**有关使用 Volume Activation 的其他软件的支持信息，请参阅专门为这些应用程序编写的文档。

表 2. Slmgr.vbs 命令行选项

| **选项** | **说明** |
| --- | --- |
| **[计算机名]** | 远程计算机的名称（默认为本地计算机） |
| **[用户]** | 远程计算机上具有所需特权的帐户 |
| **[密码]** | 远程计算机上具有所需特权的帐户的密码 |
| **全局选项** | |
| **/ipk 产品密钥** | 尝试安装 5×5 产品密钥。此参数提供的产品密钥被确认为有效且适用于已安装的操作系统。否则，将返回错误。  如果密钥有效且适用，则会安装此密钥。如果已安装了密钥，则将以静默方式替换之前的密钥。  为了避免许可证服务中的不稳定情况，应重新启动系统或软件保护服务。  必须通过提升的命令提示符运行此操作，或必须将**标准用户操作**注册表值设置为允许无特权的用户额外访问软件保护服务。 |
| **/ato [激活 ID]** | 对于零售版本和安装了 KMS 主机密钥或多次激活密钥 (MAK) 的批量系统，**/ato** 会提示 Windows 尝试联机激活。  对于安装了通用批量许可证密钥 (GVLK) 的系统，此选项会提示尝试进行 KMS 激活。已经设置为暂停自动尝试 KMS 激活 (**/stao**) 的系统，仍然会在运行 **/ato** 时尝试 KMS 激活。  参数 **[激活 ID]** 扩展了 **/ato** 支持，可识别计算机上安装的  Windows 版本。指定 **[激活 ID]** 参数将隔离此选项对与该激活 ID 相关联的版本产生的影响。运行 **Slmgr.vbs /dlv All** 可获取已安装的 Windows 版本的激活 ID。如果您需要支持其他应用程序，请参阅该应用程序提供的指南以了解详细说明。  KMS 激活不需要提升特权。但是，联机激活需要提升，或必须将**标准用户操作**注册表值设置为允许无特权的用户额外访问软件保护服务。 |
| **/dli [激活 ID | All]** | 显示许可证信息。  默认情况下，**/dli** 会显示已安装的有效 Windows 版本的许可证信息。指定 **[激活 ID]** 参数会显示与此激活 ID 相关联的指定版本的许可证信息。指定参数为 **[All]** 将显示所有适用的已安装产品的许可证信息。  此操作不需要提升特权。 |
| **/dlv [激活 ID | All]** | 显示详细的许可证信息。  默认情况下，**/dlv** 会显示已安装的操作系统的许可证信息。指定 **[激活 ID]** 参数会显示与此激活 ID 相关联的指定版本的许可证信息。指定 **[All]** 参数会显示所有适用的已安装产品的许可证信息。  此操作不需要提升特权。 |
| **/xpr [激活 ID]** | 显示产品的激活过期日期。默认情况下，这涉及当前的 Windows 版本并主要对 KMS 客户端有用，因为 MAK 和零售激活是永久性的。  指定 **[激活 ID]** 参数会显示与此激活 ID 相关联的指定版本的激活过期日期。  此操作不需要提升特权。 |
| **高级选项** | |
| **/cpky** | 某些服务操作要求注册表在全新体验 (OOBE) 操作过程中包含有产品密钥。**/cpky** 选项从注册表中删除了产品密钥，以防止此密钥被恶意代码盗用。  对于部署密钥的零售安装，建议最好运行此选项。MAK 和 KMS 主机密钥不需要运行此选项，因为对于这些密钥来说这是默认行为。只有其他类型的密钥才需要运行此选项，因为在这些情况中，默认行为不是从注册表中清除密钥。  必须通过提升的命令提示符运行此操作。 |
| **/ilc <许可证文件>** | 此选项可安装所需参数指定的许可证文件。这些许可证可能会作为一种疑难解答措施进行安装（以支持基于令牌的激活），或作为手动安装机载应用程序的一部分安装。  此过程中不进行许可证验证：许可证验证超出了 Slmgr 的范围。而是在运行时由软件保护服务进行验证。  必须通过提升的命令提示符运行此操作，或必须将**标准用户操作**注册表值设置为允许无特权的用户额外访问软件保护服务。 |
| **/rilc** | 此选项重新安装存储在 %SystemRoot%\system32\oem 和  %SystemRoot%\System32\spp\tokens 中的所有许可证。这些都是安装过程中存储的“已知良好的”副本。  “受信存储”中任何匹配的许可证都将被替换。但不会替换任何其他许可证，例如，受信任的颁发机构 (TA) 颁发许可证 (IL)（应用程序的许可证）等。  必须通过提升的命令提示符运行此操作，或必须将**标准用户操作**注册表值设置为允许无特权的用户额外访问软件保护服务。 |
| **/rearm** | 此选项会重置激活计时器。**/rearm** 过程也被称作 **sysprep/ generalize**。  如果  HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\SkipRearm 注册表子项等于 **1**，则不会执行此操作。有关此注册表子 项的详细信息，请参阅本指南后面的“” 一节。  必须通过提升的命令提示符运行此操作，或必须将**标准用户操作**注册表值设置为允许无特权的用户额外访问软件保护服务。 |
| **/upk [激活 ID]** | 此选项会卸载当前 Windows 版本的产品密钥。重新启动后，除非安装了新的产品密钥，否则系统将处于未许可状态。  您也可以使用 **[激活 ID]** 参数指定已安装的其他产品。  必须通过提升的命令提示符运行此操作。 |
| **批量许可：KMS 客户端选项** | |
| **/skms 名称[:端口] |:端口 [激活 ID] [激活 ID]** | 此选项可指定要联系的 KMS 主机的名称和端口（可选）。设置此值会禁用 KMS 主机的自动检测。  如果 KMS 主机只使用了 Internet 协议版本 6 (IPv6)，则必须将地址格式指定为 [主机名]：端口。IPv6 地址包含冒号 (:)，这将会被 Slmgr.vbs 脚本错误地解析。  必须通过提升的命令提示符运行此操作。 |
| **/ckms [激活 ID]** | 此选项可删除注册表中指定的 KMS 主机名、地址和端口信息，并还原 KMS 自动发现行为。  必须通过提升的命令提示符运行此操作。 |
| **/skhc** | 此选项会启用 KMS 主机缓存（默认），这会在初次发现运行中的 KMS 主机后阻止使用域名系统 (DNS) **优先级**和**权重**。如果系统不再与运行中的 KMS 主机联系，则会再次尝试发现。  必须通过提升的命令提示符运行此操作。 |
| **/ckhc** | 此选项会禁用 KMS 主机缓存。此设置会在每次尝试 KMS 激活时指示客户端使用 DNS 自动发现（使用**优先级**和**权重**时建议采用此项）。  必须通过提升的命令提示符运行此操作。 |
| **KMS 主机配置** | |
| **/sai <间隔>** | 此选项设置未激活的客户端尝试连接 KMS 的间隔（以分钟为单位）。该激活间隔必须在 15 分钟到 30 天之间，但建议使用默认值（2 小时）。  KMS 客户端最初从注册表获取此间隔，但在收到第一个 KMS 响应后转换为 KMS 设置。  必须通过提升的命令提示符运行此操作。 |
| **/sri <间隔>** | 此选项设置已激活的客户端尝试连接 KMS 的续订间隔（以分钟为单位）。该续订间隔必须在 15 分钟到 30 天之间。此选项最初在 KMS 服务器和客户端上均进行了设置。默认值为 10080 分钟（7 天）。  KMS 客户端最初从注册表获取此间隔，但在收到第一个 KMS 响应后转换为 KMS 设置。  必须通过提升的命令提示符运行此操作。 |
| **/sprt <端口>** | 此选项可设置 KMS 主机上用于侦听客户端激活请求的端口。默认 TCP 端口为 1688。  必须通过提升的命令提示符运行此操作。 |
| **/sdns** | 启用 KMS 主机的 DNS 发布（默认）。  必须通过提升的命令提示符运行此操作。 |
| **/cdns** | 禁用 KMS 主机的 DNS 发布。  必须通过提升的命令提示符运行此操作。 |
| **/spri** | 将 KMS 优先级设置为标准（默认）。  必须通过提升的命令提示符运行此操作。 |
| **/cpri** | 将 KMS 优先级设置为低。  使用此选项可最小化相互托管环境中的 KMS 争用。请注意，这可能导致 KMS 不足，是否会导致 KMS 不足取决于其他哪些应用程序或服务器角色处于活动状态。请谨慎使用。  必须通过提升的命令提示符运行此操作。 |
| **基于令牌的激活配置** | |
| **/lil** | 列出已安装的基于令牌的激活颁发许可证。 |
| **/ril <ILID> <ILvID>** | 删除某个已安装的基于令牌的激活颁发许可证。  必须通过提升的命令提示符运行此操作。 |
| **/stao** | 设置**仅基于令牌激活**的标志，禁用自动 KMS 激活。  必须通过提升的命令提示符运行此操作。 |
| **/ctao** | 清除**仅基于令牌激活**的标志（默认），启用自动 KMS 激活。  必须通过提升的命令提示符运行此操作。 |
| **/ltc** | 列出可激活已安装软件的基于令牌的有效激活证书。 |
| **/fta <证书指纹> [PIN]** | 使用已识别的证书强制进行基于令牌的激活。当使用受硬件（如智能卡）保护的证书时，将提供可选的个人识别号 (PIN) 以解锁没有 PIN 提示的私钥。） |

# 注册表设置

表 3 介绍了 Volume Activation 支持的注册表设置。

表 3. 注册表设置

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **注册表子项：HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\SoftwareProtectionPlatform** | | | | | |
| **值** | **类型** | | **说明** | | **范围** |
| **Activation\AlternateURL** | **REG\_SZ** | | 包含管理员提供的 URL（可选）。如果填充了此密钥，则某些激活对话框将包含一个会在默认浏览器中打开的新链接：**在线了解有关激活的详细信息**。 | | 所有 |
| **DisableDnsPublishing** | **REG\_DWORD** | | 将此值设置为非零值可阻止 KMS 主机自动发布到 DNS。 | | KMS |
| **DnsDomainPublishList** | **REG\_MULTI\_SZ** | | **格式：**域名, <优先级>, <权重>  包含一个 KMS 用以自动发布其 DNS  服务 (SRV) 记录的完全限定域的列表（可选）。KMS 主域会一直使用，因此不必在此处包含该域。这取决于 **DisableDnsPublishing** 值。  **优先级**和**权重**参数可选。如果未提供，则会在 SRV 记录中将这些参数设置为 **0**。 | | KMS |
| **EnableKmsLowPriority** | **REG\_DWORD** | | 将此值设置为非零值可最小化相互托管环境中的 KMS 争用。请注意，在系统繁忙时，这可以避免 KMS 主机维持足够数目。 | | KMS |
| **KeyManagementServiceListeningPort** | **REG\_SZ** | | 在 KMS 主机上设置此值可强制 KMS 侦听指定的 TCP 端口。如果未指定此值，主机将使用 TCP 端口 1688。 | | KMS |
| **KeyManagementServiceName** | **REG\_SZ** | | 设置此值可强制 KMS 客户端使用特定的 KMS 主机。无默认值。  如果指定了 AppID 或 SKU-ID，则会在存储此值的子项中创建以下内容：  ..\SoftwareProtectionPlatform\APPID\_GUID\KeyManagementServiceName | | KMS 客户端 |
| **KeyManagementServicePort** | **REG\_SZ** | | 设置此值可强制 KMS 客户端在与 KMS 通信时使用特定 TCP 端口。如果未指定此值，客户端将使用端口 1688。  如果指定了 AppID 或 SKU-ID，则会在存储此值的子项中创建以下内容：  ..\SoftwareProtectionPlatform\APPID\_GUID\KeyManagementServicePort | | KMS 客户端 |
| **KeyManagementServiceVersion** | **REG\_SZ** | | 设置此值可使 Microsoft Operations  Manager (MOM) 2005 自动发现 KMS。如果 KMS 在计算机上不再可用，请删除此值。 | | KMS |
| **UserOperations** | **REG\_DWORD** | | 默认情况下此值不存在，默认值为 **0**，需要提升。创建此值并将其设置为 **1**，可使标准用户安装产品密钥，且无需提升即可激活并重新装备计算机。  也可通过 GPO 配置此设置，GPO 存储在 **\policies** 注册表子项下。 | | 所有（不仅仅适用于 KMS） |
| **VLActivationInterval** | **REG\_DWORD** | | 此值最初在 KMS 服务器和客户端上均进行了设置。默认值为 120 分钟（2 小时）。KMS 客户端最初从注册表获取此间隔，但在收到第一个 KMS 响应后转换为 KMS 设置。最小值为 15 分钟，最大值为 43,200 分钟（30 天）。 | | KMS 客户端和 服务器 |
| **VLRenewalInterval** | **REG\_DWORD** | | 此值最初在 KMS 服务器和客户端上均进行了设置。默认值为 10,080 分钟（7 天）。KMS 客户端最初从注册表获取此间隔，但在收到第一个 KMS 响应后转换为 KMS 设置。因此，从来不会使用客户端设置。最小值为 15 分钟，最大值为 43,200 分钟（30 天）。 | | KMS 客户端和 服务器 |
| **注册表子项：HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\SoftwareProtectionPlatform\Activation** | | | | | |
| **值** | **类型** | **说明** | | **范围** | |
| **Manual** | **REG\_DWORD** | **0** = 允许自动联机激活（默认）  **1** = 禁用自动激活 | | MAK 和 KMS 主机，而不是 KMS 客户端 | |
| **NotificationDisabled** | **REG\_DWORD** | **0** = 将显示激活通知和气球（默认）  **1** = 隐藏所有与激活相关的通知（如果 Windows 未处于通知或未许可状态）。不推荐。 | | 所有（不仅仅适用于 KMS） | |

# 组策略对象设置

表 4 介绍了组织可用来阻止操作系统在通知状态下将桌面更改为黑色的组策略设置。

表 4. 组策略对象设置

| **策略名称** | **说明** |
| --- | --- |
| **用户配置 -> 管理模板 -> 控制面板 -> 个性化 -> 阻止更改桌面背景** | 阻止用户添加或更改桌面的背景设计。  默认情况下，用户可以使用“个性化”或“显示控制面板”项中的**桌面背景**页面向其桌面添加背景设计（墙纸）。  如果您启用此设置，用户将无法更改任何桌面背景设置。  要为组指定墙纸，请使用**桌面墙纸**设置。  **注**：您还须启用**桌面墙纸**设置以阻止用户更改桌面墙纸。有关详细信息，请参考 <http://support.microsoft.com/kb/Q327998> 上的 Microsoft 帮助和支持文章“管理员在组策略中选择‘阻止更改墙纸’后更改桌面墙纸设置”。  此外，请参见**仅允许使用位图墙纸**设置。 |
| **用户配置 -> 管理模板 -> 桌面 -> 桌面 -> 桌面墙纸** | 指定在所有用户桌面上显示的桌面背景（“墙纸”）。  使用此设置可指定用户桌面上的墙纸，并阻止用户更改图像或其显示。可以将您指定的墙纸存储为位图 (\*.bmp) 文件或 JPEG (\*.jpg) 文件。  要使用此设置，请键入存储墙纸图像的文件的完全限定路径和文件名。您可以键入本地路径（如  C:\Windows\web\wallpaper\home.jpg）或通用命名约定 (UNC) 路径（如 \\Server\Share\Corp.jpg）。如果在用户登录时指定的文件不可用，则不会显示墙纸。用户无法指定备用墙纸。您还可以使用此设置将墙纸图像指定为居中、平铺或拉伸。用户无法更改此指定。  如果您禁用此设置或不对其进行配置，则不会显示墙纸。但是，用户可以自行选择墙纸。  此外，请参见同一位置中的**仅允许使用位图墙纸**设置和“用户配置\管理模板\控制面板”中的**阻止更改墙纸**设置。  **注**：此设置不适用于远程桌面服务器会话。 |
| **用户配置 -> 管理模板 -> 控制面板 -> 个性化 -> 阻止更改桌面图标** | 阻止用户更改桌面图标。  默认情况下，用户可通过“个性化”或“显示控制面板”项中的**桌面图标设置**对话框来显示、隐藏或更改桌面图标。  如果您启用此设置，则用户无法更改任何桌面图标。  对于 Windows Vista 之前的操作系统，此设置还会隐藏“显示控制面板”项中的**桌面**选项卡。 |

# KMS 激活计时

KMS 激活计时可通过两个设置进行控制：激活计时器和续订计时器：

* KMS 激活间隔 确定 KMS 客户端在其被激活之前、在宽限期和通知状态期间尝试激活的频率。通过运行 **slmgr.vbs /sai *间隔***在客户端上设置此值。间隔以分钟为单位，默认值为 120 分  
  钟。有关详细信息，请参阅“”和“”。当系统与 KMS 主机联系后，KMS 主机设置将覆盖本地客户端设置。
* KMS 续订间隔 确定 KMS 客户端尝试在被激活后通过 KMS 进行重新激活的频率。使用 **slmgr   
  /sri *间隔*** 设置此值。间隔以分钟为单位进行设置。默认值为 10,080 分钟（7 天）。可以在客户端上设置此值，但是它将被 KMS 主机提供的值覆盖。

在运行过程中，KMS 客户端会在启动时尝试与 KMS 主机联系，而且会在联系失败后每隔一个激活间隔再次尝试。默认情况下，此操作每两小时执行一次。当 KMS 激活成功后，客户端将收到 KMS 主机的续订间隔并进行存储，Windows 激活状态将持续 180 天。激活续订以滑动窗口的形式运行，类似于动态主机配置协议 (DHCP) 租赁。客户端激活状态将持续 180 天，但是仍然会每隔一个续订间隔（默认为 7 天）尝试重新激活。如果激活成功，则将重置 180 天的周期。如果激活失败，系统将监控网络更改或其他限定的事件以触发下一次尝试。15 分钟后，系统停止监控限定事件，但是仍然会每隔一个激活间隔尝试一次。

如果在 180 天的周期内未成功重新激活，则客户端将转换为容差宽限期外 (OOT)。如果在转换为 OOT 后的 30 天内没有进行激活，则系统将进入通知模式。

# KMS 发现搜索顺序

当启用 KMS 自动发现（默认）且未禁用 KMS 主机缓存时，KMS 客户端将按照以下顺序来确定使用哪个 KMS（它们将尝试每个步骤，直到具有正确密钥的已激活 KMS 主机作出响应）：

* HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\  
  SoftwareProtectionPlatform\AppID\SKUID\KeyManagementServiceName REG\_SZ 注册表值中特定于 SKU 的值
* HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\  
  SoftwareProtectionPlatform\AppID\KeyManagementServiceName REG\_SZ 注册表值中特定于 AppID 的值
* HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\  
  SoftwareProtectionPlatform\KeyManagementServiceName REG\_SZ 注册表值中的全局值
* 特定于 SKU 的缓存 KMS 主机（这是在上次成功激活 KMS 时使用的主机的缓存标识）
* DNS 自动发现（遵照**权重**和**优先级**设置）

如果缓存的 KMS 未作出响应，则会执行搜索。

# 激活方案

以下几节介绍用于 KMS 和 MAK 激活的密钥方案。

## KMS 方案

KMS 可支持简单网络、单站点网络和全局网络。以下方案显示：

* KMS 的默认实施。
* 扩展到支持全局网络的实施。

### 单站点网络的默认 KMS 实施

Contoso 拥有 100 个 Windows 7 Enterprise 客户端和一套包含 Windows Vista、Windows   
Server 2008 和 Windows Server 2008 R2 的混合系统。如图 1 所示，Contoso 是一个扁平的域 (Contoso.com)。DNS 服务器以其默认配置运行 Microsoft DNS。此配置支持动态 DNS 注册和可删除陈旧记录的 DNS 记录清理。



图 1. 单站点网络的默认 KMS 实施

Contoso 购买了一份可提供 KMS B 密钥的许可协议，该密钥将激活 Contoso 的所有系统。信息技术 (IT) 管理员使用在提升的命令提示符下本地运行的以下命令，在两台运行 Windows Server 2008 R2 的 KMS 主机上安装 Contoso 的 KMS 主机密钥 (CSVLK)：

Slmgr.vbs /ipk <KMS 主机密钥>

IT 管理员随后在名为 *KMS 主机* 的 Active Directory® 域服务 (AD DS) 中创建一个安全组。管理员将服务器 KMS\_1 和 KMS\_2 添加为 KMS 主机成员。

通过 Internet 针对 Microsoft 激活主机 KMS\_1：**Slmgr.vbs /ato**。KMS\_1 自动将其 SRV   
资源记录 (RR) 发布到 DNS。IT 管理员访问 DNS 服务器，查找 \_vlmcs.\_tcp.contoso.com 的 RR，并更改它的权限以授予 KMS 主机对该记录的读取、写入和删除权限。现在通过 Internet 针对 Microsoft 激活主机 KMS\_2：**Slmgr.vbs /ato***。*

最后，管理员确认在 Windows 防火墙中启用了 KMS 主机排除。需要启用密钥管理服务防火墙例外。

Contoso 网络上的 KMS 客户端查询 DNS 并接收两台 KMS 主机的 SRV 记录。客户端选择其中一个主机，然后接受激活（一旦 KMS 数量超过了阈值）。有关 KMS 数量要求的详细信息，请参阅“”一节。

### 复杂的全局网络中的 KMS 实施

如图 2 所示，Contoso 扩展到了两个域：east.contoso.com 和 west.contoso.com。通过带有防火墙的广域网 (WAN) 链接，可以在两个网络之间进行私人网络通信。此链接的带宽有限，因此在 WAN 链接的两端复制资源（包括 DNS）以尽可能地减少流量。



图 2. 复杂的全局网络中的 KMS 实施

Contoso 使用基于图像的部署。其客户端系统在 Windows Vista 上是标准的，但是 Windows Vista 系统将被 Windows 7 客户端替换。

用户的地理位置会定期变化，因此他们的网络连接会从一个域更改为另一个域。DHCP 会动态提供客户端的 IP 寻址，包括指定本地 DNS 主机、本地网关地址等。

为了向现有的 Windows Vista 客户端和新的 Windows 7 客户端提供激活支持，Contoso 安装了四个 KMS 主机（使用其 KMS B 密钥）。其中两台 KMS 主机在 east.contoso.com 中配置，另外两台则在 west.contoso.com 中配置。

IT 管理员配置 KMS 主机，以便使 DNS SRV 记录将 east 域中的 Windows 7 和 Windows Server 2008 R2 客户端驱动到 KMS\_E1（如果可用）或 KMS\_E2。如果两个均不可用，则客户端将先尝试 KMS\_W1，然后尝试 KMS\_W2。同样，还会配置 west 域中的 DNS，以便使 west 域中的 Windows 7 客户端会优先联系 KMS\_W1，然后再联系 KMS\_W2，并且只有当这些操作都失败后才会尝试使用 WAN 链接远端的 KMS\_E1 和 KMS\_E2 进行激活。

IT 管理员通过更改以下配置（参见表 5）来完成此操作：

* 将 KMS\_E\* 主机添加到安全组 KMS\_E。该组即获得对记录 \_vlmcs.\_tcp.east.contoso.com 的读取、写入和删除权限。
* 将 KMS\_W\* 主机添加到安全组 KMS\_W。该组即获得对记录 \_vlmcs.\_tcp.west.contoso.com   
  的读取、写入和删除权限
* 配置 DHCP 服务器，以将 east.contoso.com 和 west.contoso.com 添加到所有客户端的 DNS 后缀搜索列表。
* 将 east 和 west 域之间的防火墙配置为允许在端口 1688 上向 KMS 主机进行 RPC 通信。

表 5. KMS 主机配置

| **说明** | **配置** | **主机** |
| --- | --- | --- |
| 配置  east.contoso.com SRV 优先级和权重，以便使客户端在尝试联系 KMS\_W\* 主机之前先联系 KMS\_E\* 主机（如果可用）。通信将分为以下两部分：75% 到 KMS\_\*1 主机，25% 到 KMS\_\*2  主机。 | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform DnsDomainPublishList=  KMS\_E1, 10, 75  KMS\_E2, 10, 25  KMS\_W1, 90, 75  KMS\_W2, 90, 25 | KMS\_E1  KMS\_E2 |
| 配置  west.contoso.com  SRV 优先级和权重，以便使客户端在尝试联系 KMS\_E\* 主机之前先联系 KMS\_W\*  主机（如果可用）。通信将分为以下两部分：75% 到 KMS\_\*1  主机，25% 到  KMS\_\*2 主机。 | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform DnsDomainPublishList=  KMS\_W1, 10, 75  KMS\_W2, 10, 25  KMS\_E1, 90, 75  KMS\_E2, 90, 25 | KMS\_W1  KMS\_W2 |

然后，管理员确认 Windows 防火墙例外是否设置为允许 KMS 客户端通信，并配置客户端计算机（如表 6 所示）。

表 6. KMS 客户端配置

| **说明** | **配置** |
| --- | --- |
| 禁用 KMS 主机缓存 | **Slmgr /ckhc** |
| 设置用户 URL，将有 激活问题的用户直接 转至 Contoso 技术 支持中心 | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation  AlternateURL = http://contoso.com/help |

客户端参考计算机进行 KMS 激活，然后运行 **sysprep /generalize**。关闭系统，并通过 Windows 7 的 Windows 自动安装工具包 (Windows AIK) 中的 ImageX 对其进行映像。Windows AIK 可从 <http://go.microsoft.com/fwlink/?LinkId=136976> 上下载。

## MAK 方案

以下几节介绍了 MAK 激活的各种方案，这些方案均基于图 3 中所示的方案。此图显示了大型企业中的典型网络环境和工作组环境。

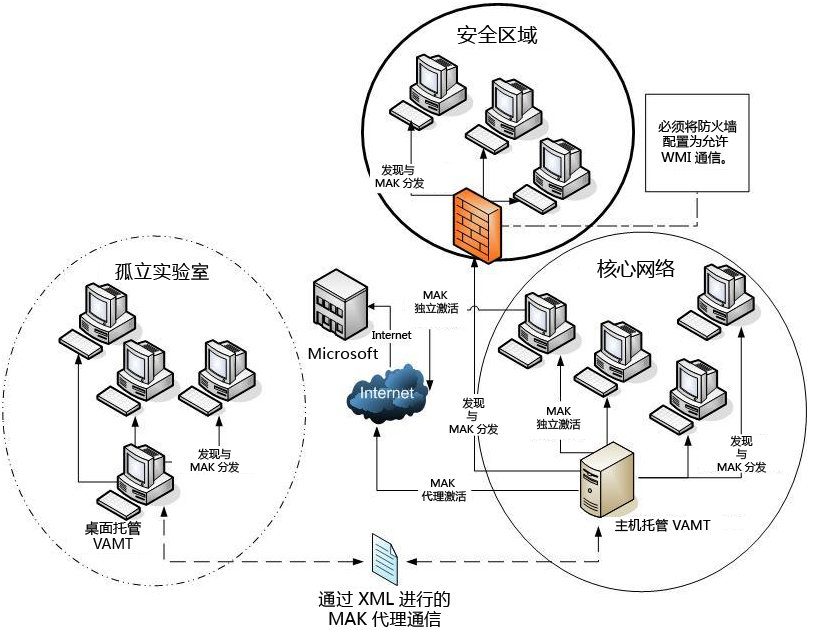


图 3. 企业环境

在核心网络环境中，所有计算机均位于一个由 AD DS 管理的通用网络中。“安全区域”代表具有额外防火墙保护的安全性更高的核心网络计算机。

“隔离实验室”环境是一个物理上与核心网络隔离的工作组，其中的计算机不能访问 Internet。网络安全策略规定，不得将可以识别特定计算机或用户的信息传输到隔离实验室之外。

### MAK 独立激活

VAMT 允许通过从集中控制台分发 MAK 来自动进行 MAK 部署和激活，如图 2 所示。VAMT 会通过查询 Microsoft 激活服务器来获取给定 MAK 的剩余激活次数，然后列出环境中所有使用 MAK 激活的系统的激活状态。此计数是一个即时快照，不是实时计数。VAMT 版本 1.2 包含在 Windows AIK 中。

在此方案中，VAMT 在图 3 所示的核心网络环境中部署。它安装在可通过网络访问所有客户端计算机的中央计算机上。VAMT 主机和客户端计算机均可访问 Internet。以下说明介绍了执行独立激活的步骤：

1. 在已联网的主机上安装 VAMT 并启动：
   1. 在主机上安装 Windows AIK。
   2. 单击“开始”，然后单击 **VAMT** 以打开 VAMT 控制台。
2. 在目标计算机上配置 Windows Management Instrumentation (WMI) 防火墙例外。确保已为所有目标计算机启用了 WMI 防火墙例外（如图 4 所示）。

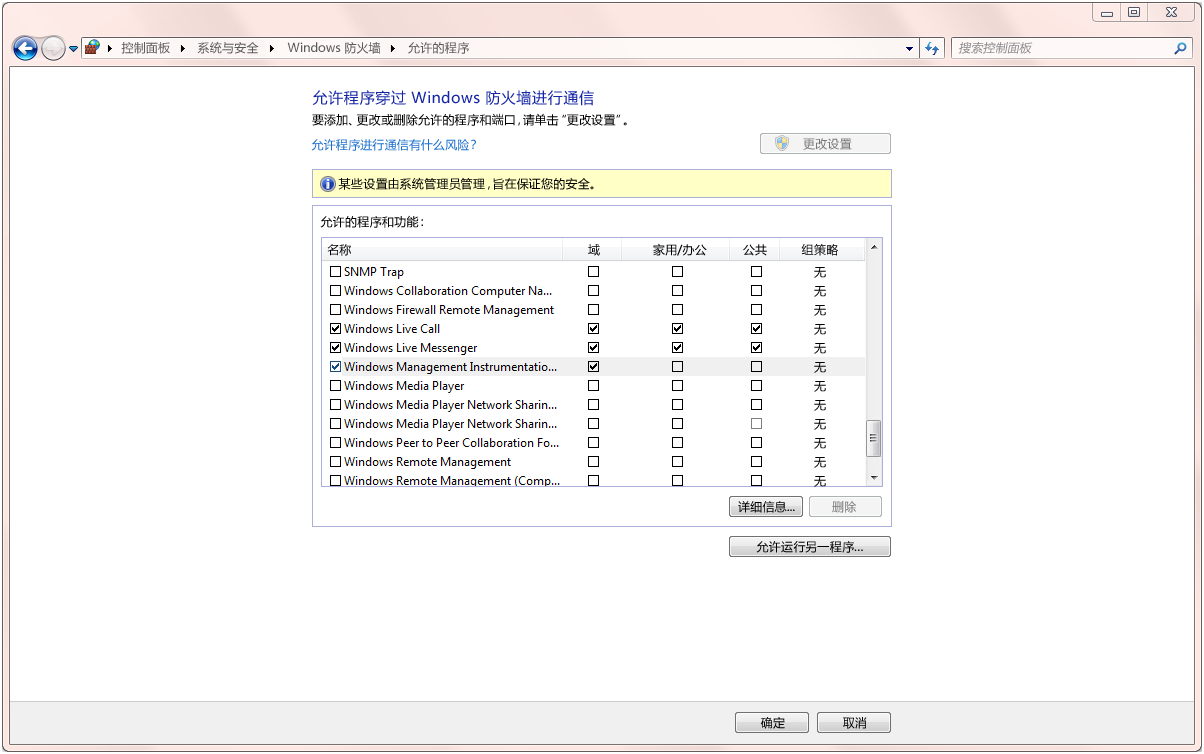


图 4. Windows Management Instrumentation (WMI) 例外

1. 向计算机信息列表 (CIL) 添加计算机：
   1. 在 VAMT 控制台上，单击**操作**，然后单击**添加计算机**以显示**添加计算机**对话框。
   2. 输入计算机组名称（如*核心网络组*），以识别要激活的计算机组。
   3. 单击下拉列表，选择搜索选项。您可以在工作组中或 AD DS 域中搜索计算机，也可以按单个计算机名或 IP 地址搜索计算机。
   4. 如果您要按单个计算机名或 IP 地址进行搜索，请在该下拉列表下的文本框中输入相关  
      信息。
   5. 如果您要在域或工作组中进行搜索，请在针对这些选项显示的其他下拉列表中选择域或工作组。使用**按计算机名筛选**字段可在域或工作组中搜索特定计算机。
   6. 单击**确定**。

VAMT 通过轻型目录访问协议 (LDAP) 来查询 Active Directory 目录服务 (AD DS)，并将其找到的计算机添加到 CIL。

1. 从发现的计算机中收集状态信息：
   1. 如要使 VAMT 在某个计算机上执行一项操作，则其必须具有该计算机的当前许可证状态数据。通过在计算机列表视图窗格中直接选择一台或多台计算机来收集单个计算机的状态信息。要对整个组执行操作，请在树状视图窗格中选择“状态未知”节点或“用户定义组”\“核心网络组”节点。
   2. 右键单击组或所需计算机，然后单击**刷新计算机状态**。
   3. 如果您要激活的计算机要求提供不同于您当前所用凭据的管理员凭据，请选择**使用备用  
      凭据**。
   4. 单击**确定**。
   5. 根据提示，提供域管理员帐户（用来收集该域中所有计算机的状态信息）和密码。

当 VAMT 收集所有所选计算机的状态信息时，将显示**收集计算机信息**对话框。此过程结束后，VAMT 控制台的计算机列表视图窗格中会显示已刷新的各个计算机的状态信息。

**注**：要检索所选计算机的许可状态，VAMT 必须对远程计算机具有管理权限，且必须能够通过 Windows 防火墙访问 WMI。此外，对于工作组计算机，还须创建注册表密钥以在用户帐户控制 (UAC) 下启用远程管理操作。有关配置系统以进行 VAMT 远程管理的详细信息，请参阅 VAMT 帮助。

1. 添加 MAK，并确定其剩余激活计数：
   1. 单击**选项**，然后单击**管理 MAK** 以打开**管理 MAK 密钥**对话框。
   2. 单击**添加**，输入 MAK。
   3. 输入 MAK，然后单击**验证**。

验证后，将自动填充**版本**字段。

* 1. 提供一段有意义的说明，然后单击**添加**。

此时，**管理 MAK 密钥**对话框中将列出 MAK。

* 1. 单击**刷新剩余计数**，以从 Microsoft 中检索列出的 MAK 的剩余激活数量（此步骤需要连接 Internet）。
  2. 单击**退出**，关闭对话框。

1. 安装 MAK 并激活客户端计算机：
   1. 通过单击树状视图窗格中的组或选择列表视图窗格中的单个计算机来选择要激活的计算机。
   2. 右键单击所选组或计算机，然后单击 **MAK 独立激活**以显示 **MAK 独立激活**对话框。
   3. 从**安装 MAK** 列表中选择相应的 MAK。
   4. 选择**安装 MAK (覆盖现有密钥)** 和**立即激活**复选框，以指示所选计算机通过 Internet 联系 Microsoft Windows 激活来立即激活。

如果这些复选框的文本旁显示星号 (\*)，则说明此操作将仅适用于适用的计算机。例如，安装了 Windows Vista 零售版本的计算机无法使用 MAK 激活。

* 1. 如果您要激活的计算机要求提供不同于您当前所用凭据的管理员凭据，请选择**使用备用  
     凭据**。
  2. 单击**确定**。

VAMT 会依次显示**分配产品密钥**对话框和**激活计算机**对话框，直到完成所需的操作。如果您选中了**使用备用凭据**，则系统将在这些对话框显示之前提示您输入凭据。

### MAK 代理激活

在此方案中，VAMT 用于激活隔离实验室环境（如图 3 所示）中的工作组计算机。对于此类与大型网络完全隔离的工作组来说，您可以执行 MAK 代理激活，方法是：在隔离工作组中的计算机上安装第二个 VAMT，并使用可移动介质在该计算机和另一个可以访问 Internet 的 VAMT 主机之间传输 VAMT CIL。有关配置系统以进行 VAMT 远程管理的详细信息，请参阅 VAMT 帮助。以下步骤介绍了如何使用 VAMT 工具进行代理激活：

1. 在隔离实验室中的工作组计算机上安装 VAMT：
   1. 在隔离实验室工作组中的主机上安装 Windows AIK。

该计算机可以运行 Windows XP with Service Pack 2 (SP2)、Windows Server 2003、  
Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2。

* 1. 单击“开始”，然后单击 **VAMT** 以打开 VAMT 控制台。
  2. 在目标计算机上配置 Windows Management Instrumentation (WMI) 防火墙例外。确保已对所有目标计算机启用了 WMI 防火墙例外。

1. 向 CIL 添加计算机：
   1. 在 VAMT 控制台上，单击**操作**，然后单击**添加计算机**以打开**添加计算机**对话框。
   2. 输入组名称（如*隔离实验室组*），以识别要激活的计算机组。
   3. 选择**工作组**选项，指定工作组名称，然后单击**确定**。

VAMT 将在工作组中搜索计算机。

**注**：如要使 VAMT 在工作组中发现客户端计算机，必须启用网络发现 Windows 防火墙例外。

1. 从发现的计算机中收集状态信息：
   1. 如要使 VAMT 在某个计算机上执行一项操作，则其必须具有该计算机的当前许可证状态数据。通过在计算机列表视图窗格中直接选择一台或多台计算机来收集单个计算机的状态信息。要对整个组执行操作，请在左窗格中选择“状态未知”节点或“用户定义组”\“隔离实验室组”节点。
   2. 右键单击组或所需计算机，然后单击**刷新计算机状态**。
   3. 如果您要激活的计算机要求提供不同于您当前所用凭据的管理员凭据，请选择**使用备用  
      凭据**。
   4. 单击**确定**。根据提示，提供在所选工作组计算机上具有本地管理权限的帐户的凭据。

当 VAMT 收集所有所选计算机的状态信息时，将显示**收集计算机信息**对话框。此过程结束后，VAMT 控制台的计算机列表视图窗格中会显示已刷新的各个计算机的状态信息。

**注**：要检索所选计算机的许可状态，VAMT 必须对远程计算机具有管理权限，且必须能够通过 Windows 防火墙访问 WMI。此外，对于工作组计算机，还须创建注册表密钥以在 UAC 下启用远程管理操作。

1. 添加 MAK：
   1. 单击**选项**，然后单击**管理 MAK** 以打开**管理 MAK 密钥**对话框。
   2. 单击**添加**，输入 MAK。
   3. 输入 MAK，然后单击**验证**。

验证后，将自动填充**版本**字段。

* 1. 提供一段有意义的说明，然后单击**添加**。

此时，**管理 MAK 密钥**对话框中将列出 MAK。

* 1. 单击**退出**，关闭对话框。

**注**：由于 VAMT 未安装在可访问 Internet 的计算机上，因此将无法执行**刷新剩余计数**选项。此功能需要连接 Internet。

1. 在隔离实验室计算机上安装 MAK：
   1. 在树状视图窗格中选择“隔离实验室”组。
   2. 右键单击所选组，然后单击 **MAK 代理激活**以显示 **MAK 代理激活**对话框。
   3. 从**安装 MAK** 列表中选择相应的 MAK。
   4. 选择**安装 MAK (覆盖现有密钥)**。

如果此复选框的文本旁边显示星号 (\*)，则说明此操作仅用于适用的计算机。例如，安装了 Windows Vista 零售版本的计算机无法使用 MAK 激活。

* 1. 清除**从 Microsoft 获取确认 ID** 复选框，因为此计算机无法访问 Internet。
  2. 清除**应用确认 ID 并激活**复选框，因为尚未请求确认 ID (CID)。
  3. 如果您要激活的计算机要求提供不同于您当前所用凭据的管理员凭据，请选择**使用备用凭据**，然后单击**确定**。

完成请求的操作后，VAMT 将显示**分配产品密钥**对话框。如果您选中了**使用备用凭据**，则系统将在此对话框显示之前提示您输入凭据。

**注**：选择**安装 MAK (覆盖现有密钥)**复选框将强行在客户端计算机上安装 MAK。必须谨慎进行此操作。如果计算机上已安装 Windows Vista pre-SP1 版本超过 30 天，则说明其初始宽限期已过，如果下次登录前未成功完成激活，计算机将进入功能缩减模式 (RFM)。不过，您可以使用 MAK 代理激活从 RFM 恢复已正确配置的计算机，前提是该计算机能够访问 VAMT 主机。RFM 仅适用于 Windows Vista pre-SP1 版本。Windows Vista SP1 或更高版本、Windows 7、Windows Server 2008 或 Windows Server 2008 R2 无法进入 RFM 模式。

1. 保存 CIL：

在此步骤中，完整的 CIL 保存在本地（即工作组）VAMT 主机上。在 MAK 代理激活中，保持此文件非常重要，因为 VAMT 会用它将 CID 应用到正确的计算机中。

* 1. 使用 VAMT 树状视图或列表视图窗格，选择已成功接收 MAK 的组或单个计算机。
  2. 在**文件**菜单下，单击**保存**，即会显示**保存计算机信息列表**对话框。
  3. 选择一个目录，然后输入 CIL 文件名，如 *IsolatedLabGroup.CIL。*
  4. 单击**保存**。

1. 导出 CIL：

如上所述，企业的安全策略规定，不得将可以标识特定计算机或用户的信息传输到隔离实验室之外。因此，对于此类型数据，必须将其排除在 CIL 文件之外，才能将其转移到核心网络 VAMT 主机。

* 1. 使用 VAMT 树状视图或列表视图窗格，选择已成功接收 MAK 的组或单个计算机。
  2. 右键单击所选组或计算机，然后单击**导出计算机**，即会显示**保存计算机信息列表**对话框。
  3. 选择**排除任何敏感环境数据**。
  4. 单击**浏览**，即会显示**另存为**对话框。
  5. 选择一个目录，然后输入 CIL 文件名，如 *IsolatedLabGroupSecureExport.CIL。*
  6. 单击**保存**。
  7. 将 IsolatedLabGroupSecureExport.CIL 文件复制到可移动介质（磁盘驱动器、CD/DVD   
     或 USB 闪盘 [UFD]）。

**注**：选择**排除任何敏感环境数据**复选框，则可避免将个人身份信息 (PII) 保存在 CIL 中。因此，CIL 必须重新导入此 VAMT 主机和完全保存 CIL 文件，这样 Microsoft 要求的 CID 才能正确分配到“隔离实验室”组中的计算机。

1. 将 CIL 导入到能够访问 Internet 的 VAMT 主机上：
   1. 将 IsolatedLabGroupSecureExport.CIL 从可移动介质复制到能够访问 Internet 的 VAMT 主机上的驱动器上。
   2. 打开 VAMT 控制台。
   3. 在**文件**菜单下，单击**导入**，即会打开**打开计算机信息列表**对话框。
   4. 找到并选择 **IsolatedLabGroupSecureExport.CIL**，然后单击**打开**来将 CIL 加载到 VAMT。
   5. 确认计算机、组和工作组名称不可见。
2. 向 Microsoft 索要 CID：
   1. 右键单击导入的计算机，然后单击 **MAK 代理激活**，即会打开 **MAK 代理激活**对话框。
   2. 清除**安装 MAK (覆盖现有密钥)** 复选框。
   3. 清除**从 Microsoft 获取确认 ID** 复选框。
   4. 清除**应用确认 ID 并激活**复选框，因为此 VAMT 主机与所选计算机不在同一网络上。
   5. 单击**确定**。

VAMT 将显示**在线获取确认 ID** 对话框，同时将联系 Microsoft 并收集 CID。

1. 从已连接到 Internet 的 VAMT 主机导出 CIL：
   1. 为所有计算机检索到 CID 后，保存 CIL 文件。在 VAMT 控制台中，滚动到右侧并确认 **PendingCID** 列有值。
   2. 在**文件**菜单中，单击**另存为**，为文件另起一个名称，如 *IsolatedLabGroupSecureExportwithCID.CIL。*
   3. 将更新后的文件 IsolatedLabGroupSecureExportwithCID.CIL 复制到可移动介质（磁  
      盘驱动器、CD/DVD 或 UFD）。
2. 将 CIL 导入隔离实验室中的原始 VAMT 主机：
   1. 将 IsolatedLabGroupSecureExportwithCID.CIL 从可移动介质复制到隔离实验室中 VAMT 主机上的驱动器中。
   2. 打开 VAMT 控制台。
   3. 单击**文件**菜单中的**打开**，即会显示**打开计算机信息列表**对话框。
   4. 找到并选择 IsolatedLabGroup.CIL，然后单击**打开**，将 CIL 加载到 VAMT 中。

此时，将在计算机列表视图窗格中显示先前搜索到的计算机及其许可证状态。

* 1. 单击**文件**菜单中的**导入**，浏览到包含 CID 的文件 (IsolatedLabGroupSecureExportwithCID.CIL)。

这将启动合并进程，该进程会将 CID 与计算机 IID 相匹配。

* 1. 在**文件**菜单下，单击**保存**，然后输入文件名，如 *IsolatedLabGroupwithCID.CIL*，即会保存此文件（将 IID 与对应的 CID 相关联）。

**重要提示**  保存此文件对重建映像的情况至关重要。极力建议您备份此文件并保护其不被改写。

1. 应用 CID 并激活隔离实验室计算机：
   1. 右键单击树状视图窗格中的“隔离实验室”组，然后单击 **MAK 代理激活**，打开 **MAK 代理激活**对话框。
   2. 清除**安装 MAK (覆盖现有密钥)** 复选框，因为所选计算机已安装了 MAK。
   3. 清除**从 Microsoft 获取确认 ID** 复选框。
   4. 选中**应用确认 ID 并激活**复选框，指示 VAMT 通过安装所选计算机的 CID 来将其激活。
   5. 单击**确定**。

VAMT 将显示**分配确认 ID** 对话框，同时将 CID 安装在所选计算机上。

1. 或者，也可以重新激活隔离实验室中已重建映像的计算机：

如果隔离实验室中的计算机已重建映像，但基础硬件并未更改，VAMT 就可使用 IsolatedLabGroupwithCID.CIL 文件重新激活它们。

* 1. 使用原来使用的计算机名将 Windows 重新部署到每台计算机。
  2. 打开本地（工作组）VAMT 主机上的 VAMT 控制台。
  3. 单击**文件**菜单中的**打开**，然后选择 IsolatedLabGroupwithCID.CIL 文件。
  4. 在树状视图窗格中，右键单击**隔离实验室**组，然后单击**重新应用确认 ID**，即会显示 **MAK 代理重新激活**对话框。
  5. 使**安装 MAK (覆盖现有密钥)** 复选框处于选中状态，确保从列表中选中了先前使用的 MAK。
  6. 使**重新应用确认 ID 并重新激活**复选框处于选中状态，以便从 IsolatedLabGroupwithCID.CIL 文件重新应用存储的 CID。
  7. 如果硬件自初始 MAK 代理激活后并未更改且您正在使用相同的 MAK 重新激活计算机，则使**要求精确的 IID 匹配**复选框处于选中状态。

如果硬件已更改，但您仍希望 VAMT 使用先前存储的 CID 尝试重新激活，则清除此复选框。请注意，在此方案中，Windows 可能无法成功重新激活。

* 1. 如果您要激活的计算机要求提供不同于您当前所用凭据的管理员凭据，请选择**使用备用凭据**复选框。
  2. 单击**确定**。

VAMT 将显示**分配产品密钥**对话框，同时会将 MAK 应用到“隔离实验室”组。

VAMT 将显示**分配确认 ID** 对话框，同时会将 CID 安装到所选计算机上。

**注：**选择**安装 MAK (覆盖现有密钥)** 复选框将强行安装 MAK。必须谨慎进行此操作。如果 Windows Vista pre-SP1 版本已安装了 30 天以上，那么其初始宽限期已过；如果下次登录前未成功完成激活，将进入 RFM 模式。VAMT 可用于从 RFM 恢复正确配置的远程计算机，前提是必须能够通过网络访问要恢复的计算机。RFM 仅适用于 Windows Vista pre-SP1 版本。Windows Vista SP1 或更高版本、Windows 7、Windows Server 2008 和 Windows Server 2008 R2 都无法进入 RFM 模式。

### VAMT 对 KMS 激活提供的支持

在此方案中，VAMT 用于安装并激活核心网络或隔离实验室计算机上的 KMS 客户端密钥。以下所述过程假设已安装了 VAMT 并且计算机已添加到了 CIL 中。方案 1（核心网络）或方案 2（隔离实验室工作组）中的步骤 1–4 描述了这些任务。

1. 打开 VAMT 控制台。
2. 通过单击树状视图窗格中的组或选择列表视图窗格中的单个计算机来选择要激活的计算机。
3. 右键单击所选组或计算机，然后单击**配置 KMS 激活**，即会显示 **KMS 配置**对话框。
4. 选择**安装 KMS 客户端密钥(覆盖现有密钥)**，指示 VAMT 将 KMS 客户端密钥安装到客户端计算机上。
5. 选择相应的激活选项：

* **使用 DNS 自动搜索 KMS 主机。**VAMT 首先将清除目标计算机上的所有先前配置的 KMS 主机，然后指示计算机查询 DNS 以找到 KMS 主机并尝试激活。
* **使用特定 KMS 主机和端口。**VAMT 设置目标计算机上指定的 KMS 主机名和端口，然后指示计算机使用该特定 KMS 主机尝试激活。

1. 如果您要激活的计算机要求提供不同于您当前所用凭据的管理员凭据，请选择**使用备用凭据**复选框，然后单击**确定**。

VAMT 将显示**分配产品密钥**对话框，并且在完成请求的操作后将显示**激活计算机**对话框。如果您选中了**使用备用凭据**复选框，则系统将在这些对话框显示之前提示您输入凭据。

### 将 KMS 转换为使用 MAK 激活

Windows 7 和 Windows Server 2008 R2 自动安装为 KMS 客户端。要将 KMS 客户端转换为使用 MAK 激活，需要安装 MAK。您可以在安装操作系统期间或之后的任何时间安装 MAK。

可以将 MAK 密钥安装到 Windows 7 和 Windows Server 2008 R2 的参考映像中，以使所有从该映像进行的安装都使用 MAK 激活，而不使用默认的 KMS 激活。这样便可以减少在无人参与安装文件中指定 MAK 的需要。

#### 在安装操作系统过程中安装 MAK

通过将 MAK 包含到无人参与安装文件 (Unattend.xml) 中，您可以在 Windows 7 或 Windows   
Server 2008 R2 的初始安装过程中，将 KMS 客户端转换为 MAK 客户端。Unattend.xml 文件可与 Setup.exe 或 Windows 部署服务一起使用。有关详细信息，请参阅 Windows AIK 中的帮助文件 Unattended Windows Setup Reference（无人参与 Windows 安装程序参考），网址为 <http://go.microsoft.com/fwlink/?LinkId=136976>。

**注**：MAK 以明文格式存储在 Unattend.xml 文件中。在无人参与安装过程中，文件 Unattend.xml 或 AutoUnattend.xml 会复制到目标计算机的 %SystemRoot%\Panther 文件夹中。不过，在安装过程结束时，安装程序会将其替换为“SENSITIVE\*DATA\*DELETED”。

#### 在安装操作系统之后安装 MAK

您可以使用控制面板上的“系统”项或通过运行 Slmgr.vbs 脚本将 Windows 7 或 Windows Server 2008 R2 的批量版本配置为使用 MAK 激活。

* 要使用“系统”应用程序安装 MAK，请单击**更改您的产品密钥**链接，然后在**更改您的产品密钥以便激活**对话框中键入 MAK。
* 要使用 Slmgr.vbs 安装 MAK，请在命令提示符下运行以下命令：

slmgr.vbs /ipk <多次激活密钥>

其中，多次激活密钥 为 MAK。

如果用户使用用户界面 (UI) 安装 MAK，则 MAK 客户端会尝试通过 Internet 一次性自行激活。如果用户使用 Slmgr.vbs 脚本安装 MAK 密钥，则 MAK 客户端不会尝试自动激活。用户可以使用 **Slmgr.vbs /ato** 通过 Internet 手动激活 MAK。

# 产品的 KMS 主机密钥

表 7 介绍了每个 KMS 主机可以激活的产品。

表 7. KMS 主机密钥与其激活的产品

| **批量产品组** | **Windows 产品** | **密钥 类型** | **使用密钥类型激活的 产品** |
| --- | --- | --- | --- |
| Windows Vista | Windows Vista Business  Windows Vista Enterprise | KMS | Windows Vista Business  Windows Vista Enterprise |
| Windows 7 | Windows 7 Professional  Windows 7 Enterprise | KMS | Windows Vista Business  Windows Vista Enterprise  Windows 7 Professional  Windows 7 Enterprise |
| Windows Server 2008 R2  服务器组 A | Windows Web Server® 2008 R2  Windows Server 2008 R2 HPC Edition  Windows HPC Server 2008 R2 | KMS\_A | Windows Server 2008 R2 组 A  Windows Server 2008 组 A  Windows Vista 批量版本  Windows 7 批量版本 |
| Windows Server 2008 R2  服务器组 B | Windows Server 2008 R2 Standard  Windows Server 2008 R2 Enterprise | KMS\_B | Windows Server 2008 R2 组 A  Windows Server 2008 组 A  Windows Server 2008 R2 组 B  Windows Server 2008 组 B  Windows Vista 批量版本  Windows 7 批量版本 |
| Windows Server 2008 R2  服务器组 C | Windows Server 2008 R2 Datacenter  用于基于 Itanium 的系统的 Windows Server 2008 R2 | KMS\_C | Windows Server 2008 R2 组 A  Windows Server 2008 组 A  Windows Server 2008 R2 组 B  Windows Server 2008 组 B  Windows Server 2008 R2 组 C  Windows Server 2008 组 C  Windows Vista 批量版本  Windows 7 批量版本 |
| Windows Server 2008 R2 KMS 密钥与 Windows Server 2008 具有相同的层次结构（组 A、B、C），但 Windows Server 2008 R2 增加了 Windows Server 2008 Datacenter（无 Hyper-V™）、Windows Server 2008 Enterprise（无 Hyper-V）和 Windows Server 2 008 Standard（无 Hyper-V）。两者的主要区别在于：Windows Server 2008 R2 KMS 密钥可用来激活一个 KMS 主机，该主机进而将激活 Windows Server 2008、Windows 7 和 Windows Vista。  但 Windows Server 2008 和 Windows Vista 密钥不能激活 Windows 7 或 Windows Server  2008 R2 系统。 | | | |

# 激活策略值

表 8 列出了 Windows 7 和 Windows Server 2008 R2 的策略值。

表 8. Windows 7 和 Windows Sever 2008 R2 策略值

| **元素** | **客户端值** | **服务器值** | **范围** |
| --- | --- | --- | --- |
| 重新装备限制 | 3 | 3 | 不可配置 |
| KMS 客户端计数阈值 | 25 | 5 | 不可配置 |
| KMS 激活持续时间 | 180 天 | 180 天 | 不可配置 |
| KMS 主机侦听端口 | 1688 | 1688 | 任何处于打开状态的 TCP 端口 |
| OOB 宽限期 | 30 天 | 30 天 | 不可配置 |
| OOT 宽限期 | 30 天 | 30 天 | 不可配置 |
| KMS 客户端重新激活（以分钟为单位） | 10,080 分钟  （即 7 天，默 认值） | 10,080 分钟  （即 7 天，默认值） | 15-43,200 分钟  （即 30 天，默认值） |
| 静默 KMS 重试间隔（KMS 激活失败后 便会重试） | 120 分钟 | 120 分钟 | 15-43,200 分钟  （默认值为 120 分钟） |

# KMS 客户端安装密钥

默认情况下，Windows 7 和 Windows Server 2008 R2 操作系统使用 KMS 进行激活。批量安装时，默认情况下将安装安装密钥，这便使系统成了 KMS 客户端。如果要将计算机从 KMS 主机、MAK 或 Windows 的零售版本转换为 KMS 客户端，请使用 **slmgr /ipk <安装密钥>** 安装表 9 中相应的安装密钥 (GVLK)。

表 9. KMS 客户端安装密钥

| **平台** | **操作系统版本** | **产品密钥** |
| --- | --- | --- |
| **Windows 7 和 Windows Server 2008 R2** | | |
| 客户端 | Windows 7 Professional | FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4 |
| 客户端 | Windows 7 Professional N | MRPKT-YTG23-K7D7T-X2JMM-QY7MG |
| 客户端 | Windows 7 Professional E | W82YF-2Q76Y-63HXB-FGJG9-GF7QX |
| 客户端 | Windows 7 Enterprise | 33PXH-7Y6KF-2VJC9-XBBR8-HVTHH |
| 客户端 | Windows 7 Enterprise N | YDRBP-3D83W-TY26F-D46B2-XCKRJ |
| 客户端 | Windows 7 Enterprise E | C29WB-22CC8-VJ326-GHFJW-H9DH4 |
| 服务器 | Windows Server 2008 R2 Web | 6TPJF-RBVHG-WBW2R-86QPH-6RTM4 |
| 服务器 | Windows Server 2008 R2 HPC Edition | FKJQ8-TMCVP-FRMR7-4WR42-3JCD7 |
| 服务器 | Windows Server 2008 R2 Standard | YC6KT-GKW9T-YTKYR-T4X34-R7VHC |
| 服务器 | Windows Server 2008 R2 Enterprise | 489J6-VHDMP-X63PK-3K798-CPX3Y |
| 服务器 | Windows Server 2008 R2 Datacenter | 74YFP-3QFB3-KQT8W-PMXWJ-7M648 |
| 服务器 | 用于基于 Itanium 的系统的 Windows Server 2008 R2 | GT63C-RJFQ3-4GMB6-BRFB9-CB83V |
| **Windows Vista 和 Windows Server 2008** | | |
| 客户端 | Windows Vista Business | YFKBB-PQJJV-G996G-VWGXY-2V3X8 |
| 客户端 | Windows Vista Business N | HMBQG-8H2RH-C77VX-27R82-VMQBT |
| 客户端 | Windows Vista Enterprise | VKK3X-68KWM-X2YGT-QR4M6-4BWMV |
| 客户端 | Windows Vista Enterprise N | VTC42-BM838-43QHV-84HX6-XJXKV |
| 服务器 | Windows Web Server 2008 | WYR28-R7TFJ-3X2YQ-YCY4H-M249D |
| 服务器 | Windows Server 2008 Standard | TM24T-X9RMF-VWXK6-X8JC9-BFGM2 |
| 服务器 | Windows Server 2008 Standard（无 Hyper-V） | W7VD6-7JFBR-RX26B-YKQ3Y-6FFFJ |
| 服务器 | Windows Server 2008 Enterprise | YQGMW-MPWTJ-34KDK-48M3W-X4Q6V |
| 服务器 | Windows Server 2008 Enterprise（无 Hyper-V） | 39BXF-X8Q23-P2WWT-38T2F-G3FPG |
| 服务器 | Windows Server 2008 Datacenter | 7M67G-PC374-GR742-YH8V4-TCBY3 |
| 服务器 | Windows Server 2008 Datacenter（无 Hyper-V） | 22XQ2-VRXRG-P8D42-K34TD-G3QQC |
| 服务器 | 用于基于 Itanium 的系统的 Windows Server 2008 | 4DWFP-JF3DJ-B7DTH-78FJB-PDRHK |

# 激活错误代码

表 10 针对激活 Windows 7 和 Windows Server 2008 R2 操作系统的批量版本时出现的问题提供了疑难解答帮助。

表 10. 错误代码和描述

| **错误代码** | **错误消息** | **激活类型** | **可能的原因** | **解决步骤** |
| --- | --- | --- | --- | --- |
| 0xC004C001 | 激活服务器确定指定的产品密钥无效。 | MAK | 输入的 MAK 无效。 | 验证该密钥是不是 Microsoft 提供的 MAK。  联系 [Microsoft Activation Call Center](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)（Microsoft 激活呼叫中心）以确认 MAK 是否有效。 |
| 0xC004C003 | 激活服务器确定指定的产品密钥被阻止。 | MAK | MAK 在激活服务器上被 阻止。 | 联系 [Microsoft Activation Call Center](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)（Microsoft 激活呼叫中心）以获取新的 MAK 并安装/激活系统。 |
| 0xC004C008 | 激活服务器确定无法使用指定的产品密钥。 | KMS | KMS 密钥 已超过激活 限制。 | KMS 主机密钥最多可在 6 台不同的计算机上激活 10 次。如果需要增加激活次数，  请联系 [Microsoft Activation Call Center](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)（Microsoft 激活呼叫中心）。 |
| 0xC004C020 | 激活服务器报告多次激活密钥已超过其限制。 | MAK | MAK 已超过激活限制。 | 对 MAK 设计了激活次数限制。请联系  [Microsoft Activation Call Center](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)（Microsoft 激活呼叫中心）。 |
| 0xC004C021 | 激活服务器报 告已超过多次 激活密钥扩展 限制。 | MAK | KMS 已超过激活限制。 | 对 MAK 设计了激活次数限制。请联系  [Microsoft Activation Call Center](http://www.microsoft.com/licensing/resources/vol/numbers.mspx)（Microsoft 激活呼叫中心）。 |
| 0xC004F009 | 软件保护服务 报告已超过宽 限期。 | MAK | 激活系统前就已超过了宽限期。现在，系统进入了通知状态。 | 请参阅“” 一节。 |
| 0xC004F00F | 软件授权服务 器报告硬件 ID 界限超过容许 的级别。 | MAK/KMS  客户端/KMS 主机 | 系统上的硬件已变更或驱动程序已更新。 | **MAK：**OOT 宽限期期间，使用联机激活或电话激活重新激活系统。  **KMS：**重新启动，或运行 **slmgr.vbs/ ato**。 |
| 0xC004F014 | 软件保护服务 报告产品密钥 不可用。 | MAK/KMS  客户端 | 系统上未安 装任何产品 密钥。 | 安装 MAK 产品密钥，或者安装在安装介质上的  \sources\pid.txt 中找到的 KMS 安装密钥。 |
| 0xC004F02C | 软件保护服务 报告脱机激活 数据的格式不 正确。 | MAK/KMS  客户端 | 系统已检测到在电话激活过程中输入的数据无效。 | 验证输入的 CID 是否正确。 |
| 0xC004F035 | 此错误代码等同于“软件保护服务报告无法使用批量许可证产品密钥激活该计算机…”。此错误文本是正确的，但意思不明确。  此错误指示计算机的 BIOS 中缺少 Windows 标记，此标记是 OEM 系统中提供的，用来指示计算机在发运时带有合格的  Windows 版本，这是 KMS 客户端激活所必需的。  错误：无效批量许可证密钥  若要激活，您需要将产品密钥更改为有效的多次激活密钥 (MAK)  或有效的零售 密钥。  您必须有合格的操作系统许可证和批量许可的 Windows 7 升级许可证，或者有来自零售源的 Windows 7 完全许可证。  任何其他安装 此软件的行为都将违反您的协 议和适用的著作权法。 | KMS 客户端/KMS 主机 | 只许可升级  Windows 7 批量版本。不支持在没有安装合格操作系统的计算机上安装批量操作系统。 | 安装合格的 Microsoft 操作系统版本，然后使用 MAK 激活。 |
| 0xC004F038 | 软件保护服务 报告无法激活 计算机。密钥 管理服务 (KMS) 报告的数量不足。请联系系 统管理员。 | KMS 客户端 | KMS 主机 的数量不足。KMS 数量 必须大于等 于 5（对于 Windows Server） 或大于等于 25（对于 Windows  客户端）。 | KMS 池中必须有 更多的计算机才能 激活 KMS 客户端。运行 **Slmgr.vbs /dli** 以获取当前的 KMS 主机数量。 |
| 0xC004F039 | 软件保护服务 报告无法激活 计算机。未启 用密钥管理服 务 (KMS)。 | KMS 客户端 | 如果未满足 KMS 请求， 将发生此 错误。 | 解决 KMS 主机和 客户端的网络连接 问题。确保 TCP  端口 1688（默认）未被防火墙或其他 过滤程序阻止。 |
| 0xC004F041 | 软件保护服务 确定密钥管理 服务 (KMS)  未激活。需要 激活 KMS。 | KMS 客户端 | KMS 主机 未激活。 | 通过联机或电话激 活方式激活 KMS  主机。 |
| 0xC004F042 | 软件保护服务 确定无法使用 指定的密钥管 理服务 (KMS)。 | KMS 客户端 | KMS 客户端和 KMS 主机不匹配。 | 当 KMS 客户端与无法激活客户端软件的 KMS 主机联系时，将发生此错误。在某些环境中，比如在包含特定于应用程序和操作系统的 KMS 主机的混合环境中，这种情况可能很常见。 |
| 0xC004F050 | 软件保护服务 报告产品密钥 无效。 | KMS、KMS 客户端、MAK | 这可能由 KMS 密钥中的输入错误引起或者由在已发布的操作系统版本上键入了 Beta 密钥造成。 | 在相应的 Windows 版本中安装适当的 KMS 密钥。检查拼写错误。如果密钥通过复制粘贴输入，请确保密钥中的长划线未被替换成短划线。 |
| 0xC004F051 | 软件保护服务 报告产品密钥 被阻止。 | MAK/KMS | 激活服务器上的产品密钥被 Microsoft  阻止。 | 获取新的 MAK/KMS 密钥，然后将其安装在系统上并激活。 |
| 0xC004F064 | 软件保护服务报告已超过非正版宽限期。 | MAK | Windows 激活工具 (WAT) 已确定该系 统为非正版 系统。 | 请参阅 Volume Activation Operations Guide（批量激活操作 指南）。 |
| 0xC004F065 | 软件保护服务报告应用程序在有效的非正版期限内运行。 | MAK/KMS  客户端 | Windows 激活工具已确定该系统为非正版系统。在非正版宽限期内，该系统将继续运行。 | 获取并安装正版产品密钥并在宽限期内激活系统。否则，宽限期结束后系统将进入通知状态。 |
| 0xC004F06C | 软件保护服务 报告无法激活 计算机。密钥 管理服务 (KMS) 确定请求时间 戳无效。 | KMS 客户端 | 客户端计算机上的系统时间与 KMS 主机上的时间差异太大。 | 出于各种原因，时间同步对于系统和网络安全非常重要。可以通过更改客户端上的系统时间以与 KMS 同步来解决此问题。建议使用网络时间协议 (NTP) 时间源或 Active Directory 域服务进行时间同步。 此问题使用 UTP 时间，独立于时区选择。 |
| 0x80070005 | 访问被拒绝。 请求的操作需 要提升特权。 | KMS 客户端/MAK/KMS 主机 | 用户访问控制 (UAC) 阻止激活进程在未提升的命令提示符中运行。 | 从提升的命令提示符中运行 slmgr.vbs。右键单击 cmd.exe， 然后单击“以管理员身份运行”。 |
| 0x8007232A | DNS 服务器 出现故障。 | KMS 主机 | 系统存在网络或 DNS 问题。 | 解决网络和 DNS  问题。 |
| 0x8007232B | DNS 名称不 存在。 | KMS 客户端 | KMS 客户端无法在 DNS 中找到 KMS SRV RR。  如果网络中不存在 KMS 主机，则应安装 MAK。 | 确认已安装 KMS 主机，且 DNS 发布已启用（默认）。  如果 DNS 不可用，请使用 **slmgr.vbs /skms <*KMS 主机名>*** 将 KMS 客户端指向 KMS 主机。  也可获取并安装 MAK，然后激活系统。  最后，解决 DNS  问题。 |
| 0x800706BA | RPC 服务器不可用。 | KMS 客户端 | KMS 主机上未配置防火 墙设置或 DNS SRV  记录陈旧。 | 确保 KMS 主机上启用了密钥管理服务防火墙例外。  确保 SRV 记录指向有效的 KMS 主机。  解决网络连接问题。 |
| 0x8007251D | 未找到 DNS 查询记录。 | KMS 客户端 | KMS 客户端无法在 DNS 中找到 KMS SRV RR。 | 解决网络连接和 DNS  问题。 |
| 0xC004F074 | 软件保护服务 报告无法激活 计算机。无法 联系任何密钥 管理服务 (KMS)。有关 详细信息，请 参阅应用程序 事件日志。 | KMS 客户端 | 所有 KMS  主机均返回 了错误。 | 解决与激活尝试关 联的每个事件 ID  12288 产生的 错误。 |

# Windows 事件日志

表 11 列出了 KMS 在 Windows 事件日志中记录的事件。下文描述了每个事件的常用数据：

* **所有事件的日志文件名称（除 12290 外）：**Windows 日志\应用程序
* **日志文件名称 12290：**应用程序和服务日志\密钥管理服务
* **事件提供程序名称：** Microsoft-Windows-Security-Licensing-SLC
* **源名称：**软件保护服务

表 11. Windows 事件日志中记录的 KMS 事件

| **事件 ID** | **记录者** | **说明** | **消息** | **参数**  **以逗号分隔的字符串中包含的 字段** | | **示例** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **名称** | **说明** |  |
| 12288 | 客户端 | 请求生成失 败或在 RPC 后提交（客 户端） | 客户端已向密钥管理服务计算机发送了激活请求。%n信息： %n%1 | HRESULT | 返回代码 | 0x0 |
|  | | | | Status | 标志（说明 1） | 0x8 |
| Server:Port | 名称:端口 | kms01.contoso.com:1688 |
| CMID | 客户端计算机 ID | 08c3bda0-c556-4b61-9e4e-7bf6d4df80be, |
| Client Time | 请求时间戳 | 2006/1/14 2:30, |
| VM Info | Unused | 1 |
| Licensing Status | 许可证状态  0 – 未许可  1 – 已许可（已 激活）  2 - OOB 宽限期  3 - OOT 宽限期  4 – 非正版宽限期  5 – 通知  6 – 延长的宽限期 | 2 |
|  | | | | Time to Expiration | 剩余时间 （分钟） | 40123 |
| ActID | 激活 ID – 标识许可证 | cf67834d-db4a-402c-ab1f-2c134f02b700, |
| N-Policy | 需要激活的最小客户端数 | 25 |
| 12289 | 客户端 | KMS 响应 验证后（客 户端） | 客户端已处理密钥管理服务计算机的激活响应。%n信息： %n%1 | HRESULT | 返回代码 | 0x0 |
|  | | | | Status | 标志（说明 1） | 0x4000008 |
| fBound | 已激活标志 | 0 |
| Unused | 未使用 – 忽略 | 0 |
| Count | KMS 当前计数 | 4 |
| Activation Interval | 未激活时的请求间隔（分钟） | 120 |
| Renewal Interval | 激活时的请求间隔（分钟） | 10080 |
| Client Time | 请求时间戳 | 1/14/2006 2:30 |
| 12290 | KMS | 每个请求的 KMS 服务器端日志 | 激活请求已处理。%n信息： %n%1 | HRESULT | 返回代码 | 0x0 |
|  | | | | N-Policy | 需要激活的最小客户端产品数 | 25 |
| Machine | 客户端计算机名称 | kms03.site5.contoso.com |
| CMID | 客户端计算机 ID | e5c98033-aab6-4d0b-9af9-1d399597dd56 |
|  | | | | Client Time | 请求时间戳 | 2006/1/14 22:36 |
| VM Info | 虚拟机中正在 运行客户端操 作系统 | 1 |
| Licensing Status | 许可证状态  0 – 未许可  1 – 已许可（已 激活）  2 - OOB 宽限期  3 - OOT 宽限期  4 – 非正版宽限期  5 – 通知  6 – 延长的宽限期 | 2 |
| Time to Expiration | 剩余时间 （分钟） | 40123 |
| ActID | 激活 ID – 标识许可证 | cf67834d-db4a-402c-ab1f-2c134f02b700 |
| 12291 | KMS | KMS 初始化失败 | 批量许可的客户端 无法初始化密钥管 理服务续订计时器。 %n信息：%n%1 | HRESULT | 返回代码 |  |
| 12292 | KMS | 续订计时器初始化失败 | 密钥管理服务 (KMS)  无法初始化续订计 时器。%n信息： %n%1 | HRESULT | 返回代码 |  |
| 12293 | KMS | DNS RR 发布失败 | 向 '%2' 域中的 DNS 发布密钥管 理服务 (KMS) 失败。%n信息： %n%1 | P1：HRESULT  P2：DNS domain | P1：返回代码  P2：DNS 域名 | |
| 12294 | KMS | DNS RR 发布成功 | 向 '%1' 域中的 DNS 发布密钥管 理服务 (KMS) 成功。%n | DNS domain | DNS 域名 |  |

# WMI 属性和方法

表 12 列出了软件保护平台的 WMI 属性和方法。软件保护平台属性在文件   
%WinDir%\System32\wbem\sppwmi.mof 中进行定义。

表 12. 软件保护平台 WMI 属性和方法

|  |  |
| --- | --- |
| **//属性 SoftwareLicensingService 类** | |
| **Version** | 软件保护服务的版本 |
| **KeyManagementServiceMachine** | KMS 主机名。如果尚未调用 **SetKeyManagementServiceMachine**，则返回空值。 |
| **KeyManagementServicePort** | 客户端用来发送 KMS 激活请求的 TCP 端口。如果尚未调用 **SetKeyManagementServicePort**，则返回 **0**。 |
| **IsKeyManagementServiceMachine** | 指示计算机上是否启用了 KMS：如果为未启用，则为 **0**；如果启用了，则为 **1**。 |
| **VLActivationInterval** | 客户端在获得许可之前与 KMS 主 机联系的频率（以分钟为单位）。 |
| **VLRenewalInterval** | 客户端在获得许可之后与 KMS 主 机联系的频率（以分钟为单位）。 |
| **KeyManagementServiceCurrentCount** | KMS 主机上当前处于活动状态的 KMS 客户端的数量。**-1** 表示未将主机作为 KMS 启用，或主机尚未接收到任何客户端许可请求。 |
| **RequiredClientCount** | 为了启用批量许可而连接到 KMS 主机时所需的最低限客户端数。 |
| **PolicyCacheRefreshRequired** | 指示是否需要更新许可策略缓存：**0**=不需要，**1**=需要刷新。 |
| **ClientMachineID** | 标识 KMS 主机的 KMS 客户端的全局唯一标识符 (GUID)。客户端在其发送给 KMS 的请求中包含此标识符。 |
| **RemainingWindowsReArmCount** | 客户端可成功重新装备的剩余 次数。 |
| **KeyManagementServiceListeningPort** | KMS 主机用来侦听激活请求的 TCP 端口。 |
| **KeyManagementServiceDnsPublishing** | 指示 KMS 主机的 DNS 发布状态：**0**=已禁用，**1**=已启用自动发布（默认）。 |
| **KeyManagementServiceLowPriority** | 指示 KMS 服务的线程优先级状态：**0**=标准优先级（默认），**1**=低优先级。 |
| **KeyManagementServiceHostCaching** | 指示 KMS 主机名和端口的缓存状态：**0**=禁用缓存，**1**=启用缓存（默认）。 |
| **KeyManagementServiceUnlicensedRequests** | 来自许可证状态为 0（未许可）的客户端的 KMS 请求数。 |
| **KeyManagementServiceLicensedRequests** | 来自许可证状态为 1（已许可）的客户端的 KMS 请求数。 |
| **KeyManagementServiceOOBGraceRequests** | 来自许可证状态为 2（OOB 宽限期）的客户端的 KMS 请求数。 |
| **KeyManagementServiceOOTGraceRequests** | 来自许可证状态为 3（OOT 宽限期）的客户端的 KMS 请求数。 |
| **KeyManagementServiceNonGenuineGraceRequests** | 来自许可证状态为 4（非正版宽限期）的客户端的 KMS 请求数。 |
| **KeyManagementServiceNotificationRequests** | 来自许可证状态为 5（通知）的客户端的 KMS 请求数。 |
| **KeyManagementServiceTotalRequests** | 有效 KMS 请求总数。 |
| **KeyManagementServiceFailedRequests** | 无效的 KMS 请求数。 |
| **KeyManagementServiceActivationDisabled** | 指示通过 KMS 的批量激活是否已禁用。 |
| **//方法 SoftwareLicensingProduct 类** | |
| **InstallProductKey** | 安装产品密钥。 |
| **InstallLicense** | 安装许可证。 |
| **InstallLicensePackage** | 为当前产品安装许可证包。 |
| **SetKeyManagementServiceMachine** | 设置用于批量激活的 KMS 主机名。 |
| **ClearKeyManagementServiceMachine** | 清除以前配置的任何 KMS 主机名。 |
| **SetKeyManagementServicePort** | 设置客户端请求 KMS 主机时使用的 TCP 端口。如果未指定，则将使用端口 1688。 |
| **ClearKeyManagementServicePort** | 清除以前指定的任何端口号。 |
| **SetVLActivationInterval** | KMS 客户端在获得许可之前与 KMS 主机联系的激活频率（以分钟为单位）。该频率必须大于等于 15 但小于等于 43,200。如果调用了此方法，但计算机不是 KMS，则会返回错误。 |
| **SetVLRenewalInterval** | KMS 客户端在获得许可之前与 KMS 主机联系的续订频率（以分钟为单位）。该频率必须大于等于 15 但小于等于 43,200。如果调用了此方法，但计算机不是 KMS，则会返回错误。 |
| **ClearProductKeyFromRegistry** | 从注册表清除产品密钥。 |
| **AcquireGenuineTicket** | 执行联机正版验证。调用此方法可能会更改计算机的正版状态。 |
| **ReArmWindows** | 将计算机的许可状态重置为 OOB 宽限期（请参见 **LicenseStatus**）。  **注**：必须重新启动客户端才能使更改 生效。 |
| **RefreshLicenseStatus** | 更新 Windows 的许可状态，以便应用程序可以访问当前许可信息。 |
| **SetKeyManagementServiceListeningPort** | 设置 KMS 主机用来侦听激活请求的 TCP 端口。仅适用于 KMS 主机。如果未指定，则将使用端口 1688。 |
| **ClearKeyManagementServiceListeningPort** | 清除以前指定的任何侦听端口。仅适用于 KMS 主机。 |
| **DisableKeyManagementServiceDnsPublishing** | 在 KMS 主机上启用/禁用 DNS 发布：**0**=启用，**1**=禁用。 |
| **EnableKeyManagementServiceLowPriority** | 启用/禁用以低优先级运行的 KMS  服务：**0**=禁用，**1**=启用。 |
| **DisableKeyManagementServiceHostCaching** | 启用/禁用在批量激活客户端计算机上缓存 KMS 主机名和端口：**0**=启用，**1**=禁用。 |
| **DisableKeyManagementServiceActivation** | 启用/禁用通过 KMS 计算机进行的批量激活：**0**=启用，**1**=禁用。 |
| **DiscoveredKeyManagementServiceMachineName** | 上次通过 DNS 发现的 KMS 主机名。 |
| **DiscoveredKeyManagementServiceMachinePort** | 上次通过 DNS 发现的 KMS 主机端口。 |
| **//属性 SoftwareLicensingService 类** | |
| **ID** | 产品标识符 |
| **名称** | 产品名称 |
| **说明** | 产品描述 |
| **ApplicationID** | 当前产品的应用程序 ID |
| **ProcessorURL** | 处理证书的软件授权服务器 URL |
| **MachineURL** | 绑定证书的软件授权服务器 URL |
| **ProductKeyURL** | 产品证书的软件授权服务器 URL |
| **UseLicenseURL** | 用户许可证的软件授权服务器 URL |
| **LicenseStatus** | 此产品的应用程序的许可证状态：  **0**=未许可， **1**=已许可， **2**=OOB 宽限期， **3**=OOT 宽限期， **4**=非正版宽限期， **5**=通知， **6**=延长的宽限期 |
| **LicenseStatusReason** | 诊断代码，用于指出计算机处于某一特定许可状态的原因。 |
| **GracePeriodRemaining** | 父应用程序进入“通知”模式之前剩余的时间（以分钟为单位）。对于批量客户端，这是需要重新激活之前的剩余时间。 |
| **EvaluationEndDate** | 此产品应用程序的过期日期。自该日期之后，**LicenseStatus** 将变为**未许可**，并且无法激活。 |
| **OfflineInstallationId** | 此产品的应用程序的标示符。它可用于电话激活或脱机激活。如果未安装产品密钥，则返回空值。 |
| **PartialProductKey** | 此产品密钥的最后五个字符。如果未安装产品密钥，则返回空值。 |
| **ProductKeyID** | 产品密钥 ID。如果未安装产品密钥，则返回空值。 |
| **LicenseFamily** | SKU 用于确定许可证添加关系的系列标识符。 |
| **LicenseDependsOn** | SKU 系列用于确定许可证添加关系的依赖标识符。 |
| **LicenseIsAddon** | 如果产品被标识为加载许可证，则返回 **True**。 |
| **VLActivationInterval** | 在产品获得许可之前，客户端与 KMS 主机联系的频率（以分钟为单位）。 |
| **VLRenewalInterval** | 在产品获得许可之后，客户端与 KMS 主机联系的频率（以分钟为单位）。 |
| **KeyManagementServiceProductKeyID** | KMS 产品密钥 ID。如果不适用，则返回空值。 |
| **KeyManagementServiceMachine** | KMS 主机名。如果尚未调用  **SetKeyManagementServiceMachine**，则返回空值。 |
| **KeyManagementServicePort** | 客户端用来发送 KMS 激活请求的 TCP 端口。如果尚未调用  **SetKeyManagementServicePort**，则返回 **0**。 |
| **DiscoveredKeyManagementServiceMachineName** | 上次通过 DNS 发现的 KMS 主机名。 |
| **DiscoveredKeyManagementServiceMachinePort** | 上次通过 DNS 发现的 KMS 主机端口。 |
| **IsKeyManagementServiceMachine** | 指示计算机上是否启用了 KMS：如果启用了，则为 **1**；如果未启用，则为 **0**。 |
| **KeyManagementServiceCurrentCount** | KMS 主机上当前处于活动状态的 KMS 客户端的数量。**-1** 表示没有将计算机作为 KMS 启用，或计算机尚未接收到任何客户端许可请求。 |
| **RequiredClientCount** | 为了启用批量许可而连接到 KMS 主机时所需的最低限客户端数。 |
| **KeyManagementServiceUnlicensedRequests** | 来自许可证状态为 0（未许可）的客户端的 KMS 请求数。 |
| **KeyManagementServiceLicensedRequests** | 来自许可证状态为 1（已许可）的客户端的 KMS 请求数。 |
| **KeyManagementServiceOOBGraceRequests** | 来自许可证状态为 2（OOB 宽限期）的客户端的 KMS 请求数。 |
| **KeyManagementServiceOOTGraceRequests** | 来自许可证状态为 3（OOT 宽限期）的客户端的 KMS 请求数。 |
| **KeyManagementServiceNonGenuineGraceRequests** | 来自许可证状态为 4（非正版宽限期）的客户端的 KMS 请求数。 |
| **KeyManagementServiceTotalRequests** | 有效 KMS 请求总数。 |
| **KeyManagementServiceFailedRequests** | 失败的 KMS 请求数。 |
| **KeyManagementServiceNotificationRequests** | 来自许可证状态为 5（通知）的客户端的 KMS 请求数。 |
| **GenuineStatus** | 此产品应用程序的正版状态。 |
| **ExtendedGrace** | 父应用程序变为未许可状态之前的延长宽限期（以分钟为单位）。 |
| **TrustedTime** | 显示系统中当前存储的受信任 时间。 |
| **DisableKeyManagementServiceHostCaching** | 启用/禁用在批量激活客户端计算机上缓存 KMS 主机名和端口：0=启用，1=禁用。 |
| **// 方法 SoftwareLicensingProduct 类** | |
| **UninstallProductKey** | 卸载当前产品的产品密钥。 |
| **激活** | 激活当前产品。 |
| **DepositOfflineConfirmationId** | 在执行电话激活或脱机激活时通过存储此产品的脱机确认标识符来激活产品。 |
| **GetPolicyInformationDWord** | 获取 DWORD 类型的许可证策略信息。 |
| **GetPolicyInformationString** | 获取字符串类型的政策信息。 |
| **SetKeyManagementServiceMachine** | 设置用于批量激活的 KMS 主 机名。 |
| **ClearKeyManagementServiceMachine** | 清除以前配置的任何 KMS 主 机名。 |
| **SetKeyManagementServicePort** | 设置客户端请求 KMS 主机时使用的 TCP 端口。如果未指定，则将使用端口 1688。 |
| **ClearKeyManagementServicePort** | 清除以前指定的任何端口号。 |

# 术语表

|  |  |
| --- | --- |
| **术语** | **定义** |
| **ACID** | 用于识别软件版本中的激活方法的 GUID。 |
| **AD DS** | Active Directory 域服务。 |
| **AppID** | 为了对一组 SKU ID（例如系列名称）进行分组而定义的 GUID。所有 Windows 版本都具有相同的 AppID。 |
| **DNS** | 域名服务。 |
| **FQDN** | 完全限定域名（例如，phred.microsoft.com）。 |
| **GVLK** | 通用批量许可证密钥，一种特定于版本的产品密钥，默认情况下 Windows 的所有批量版本都安装有该密钥。又称“默认 KMS 客户端安装密钥”。有关详细信息，请参见表 9。 |
| **KMS** | 密钥管理服务。 |
| **KMSID** | KMS 客户端发送的 GUID，供借助 KMS 主机进行激活时使用。可在多个 ACID 之间共享。 |
| **计算机证书存储** | 此证书及其私钥必须能够让尝试进行基于令牌的激活的用户访问。 |
| **MAK** | 多次激活密钥。 |
| **N-policy** | 一种许可证策略，用于指定一个 KMS 返回的计算机的最低限数量，供客户端用来确定是否自行激活。 |
| **PIN** | 个人标识号，与智能卡一起用作身份验证凭据。 |
| **SKU** | 介绍其他版本的 Windows 或其他软件。 |
| **SKUId** | 与上面介绍的 ACID 一样 |
| **SPPSVC** | 软件保护服务，Windows 7 和 Windows Server 2008 R2 中的内置服务平台，用于管理 Windows 和其他应用程序的许可活动。 |
| **SRV** | DNS 中支持的一种资源记录（请参阅“征求意见 [RFC] 2782”） |
| **令牌** | x509 证书及其关联的私钥用于在启用了基于令牌的激活的计算机上激活 Windows。 |
| **VL** | 批量许可。 |
| **WMI** | Windows Management Instrumentation。 |

# 资源链接

* 批量激活：
* TechNet 上的批量激活：<http://go.microsoft.com/fwlink/?LinkId=150083>
* Key Management Service 1.2 for Windows Server 2003 SP1 and Later（适用于 Windows Server 2003 SP1 和更高版本的密钥管理服务 1.2）：  
  <http://go.microsoft.com/fwlink/?LinkId=155083>
* Product Activation and Key Information（产品激活和密钥信息）：  
  <http://go.microsoft.com/fwlink/?LinkId=74008>
* Volume Activation Deployment Guide（批量激活部署指南）：   
  <http://go.microsoft.com/fwlink/?LinkId=150083>
* Volume Activation Operations Guide（批量激活操作指南）：   
  <http://go.microsoft.com/fwlink/?LinkId=150084>
* Volume Activation Planning Guide（批量激活规划指南）：   
  <http://go.microsoft.com/fwlink/?LinkId=155926>
* Volume Activation Technical Reference Guide（批量激活技术参考指南）：   
  <http://go.microsoft.com/fwlink/?LinkId=152550>
* 部署工具：
* Windows Automated Installation Kit (AIK) for Windows 7（适用于 Windows 7 的 Windows 自动安装工具包 (AIK)）：  
  <http://go.microsoft.com/fwlink/?LinkId=136976>
* 管理工具：
* System Center Pack Catalog（System Center 包目录）：  
  <http://go.microsoft.com/fwlink/?LinkID=110332>
* 批量许可：
* Genuine Microsoft Software（正版 Microsoft 软件）：  
  <http://go.microsoft.com/fwlink/?LinkId=151993>
* 正版 Microsoft 软件验证页面：<http://go.microsoft.com/fwlink/?LinkId=64187>
* Microsoft Activation Centers Worldwide Telephone Numbers（Microsoft 激活中心全球电话号码）：<http://go.microsoft.com/fwlink/?LinkId=107418>
* Microsoft Volume Licensing（Microsoft 批量许可）：  
  <http://go.microsoft.com/fwlink/?LinkId=73076>
* Microsoft 批量许可服务中心：<http://go.microsoft.com/fwlink/?LinkId=107544>
* Windows Vista Privacy Notice Highlights（Windows Vista 隐私声明要点）：  
  <http://go.microsoft.com/fwlink/?LinkID=52526>