Управление активацией Windows Vista, Windows 7 и Windows Server 2008 / 2008 R2 в корпоративной сети

Олег Ржевский MVP – Windows Desktop Experience rzhevsky@post.ru



Содержание

- Цели презентации
- Обзор Volume Activation
- Подробности
 - Служба КМЅ
 - Что изменилось в Windows 7 и Windows
 Server 2008 R2
 - Ключи МАК
- Рекомендации
- Источники информации

Цели презентации

- Понятие о Volume Activation (VA)
- Технические требования
- Типичные сценарии и рекомендации
- Если планируется развертывать корпоративные версии Windows, требуется понимание, как работает Volume Activation

Что такое KMS, MAK?

Обзор Volume Activation

Product Activation

- Retail
 - · Вводим Product Key, затем активируем ПО
 - · Стандартный метод для коробочного ПО, например, Vista Home
- · OEM
 - ПО предварительно активировано, от клиента никаких действий не требуется
- · Volume License Key (VLK) для Windows XP/Windows Server 2003
 - Для корпоративных клиентов с большим числом серверов и клиентских систем
 - Специальный ключ, позволяющий обходить активацию
 - Более масштабируемое решение

Volume Activation

- · Существенная переработка Product Activation
- · Ранее один VLK использовался для многих систем
- Теперь ПО, приобретенное по корпоративным каналам лицензирования, должно проходить активацию
- Цель предотвращение распространения за пределы организации
- Для коробочного (Retail) ПО по-прежнему требуются индивидуальные ключи
- Методы активации корпоративного ПО: KMS и MAK

KMS u MAK

- KMS (Key Management Service)
 - · Инфраструктурный сервис (похожий на DHCP 🤤)
 - · Сервер KMS управляет активациями
 - Клиенты запрашивают и получают активацию
- MAK (Multiple Activation Key)
 - МАК похож на ключ от коробочного ПО, но допускает более одной активации
 - · Лимит зависит от типа лицензионного соглашения (Open, Select, Enterprise Agreement и т.д.)
- В обоих вариантах существует Grace Period (льготный период, т.е. допускается временное функционирование неактивированного ПО)

Grace Period (льготный период очке активации

- · Начальный льготный период (Out-Of-Box Grace)
 - 30 дней после установки для всех продуктов, поставляемых по каналам корпоративного лицензирования, за исключением:
 - · Windows Server 2008: 60 дней
- · Можно "обнулить": 'slmgr /rearm' или 'sysprep /generalize' (но только несколько раз)
- После подтверждения лицензии
 - Активирован, но требует периодического обновления (KMS)
 - Активирован, не требует обновления (МАК)

Grace Period

- При ошибке активации
 - 30 дней для всех продуктов, поставляемых по каналам корпоративного лицензирования
 - · Значительно изменилась аппаратная конфигурация активированной системы (Out-Of-Tolerance Grace)
 - Обновление КМS истекло

Сервис KMS, ключи MAK

Подробности

KMS: Key Management Service

- Рекомендуемый метод для корпоративных лицензий
- Клиент-серверная архитектура
 - · Сервер KMS управляет активациями
 - Клиенты запрашивают и получают активации
- Операционная система для хоста КМЅ
 - Windows Vista, Windows 7, Windows Server 2008,
 Windows Server 2008 R2
 - Windows 2003 SP1 + обновление КВ948003
 - http://support.microsoft.com/kb/948003
 - · х86 или х64
 - Может запускаться в виртуальной машине

KMS: Key Management Service

Служба

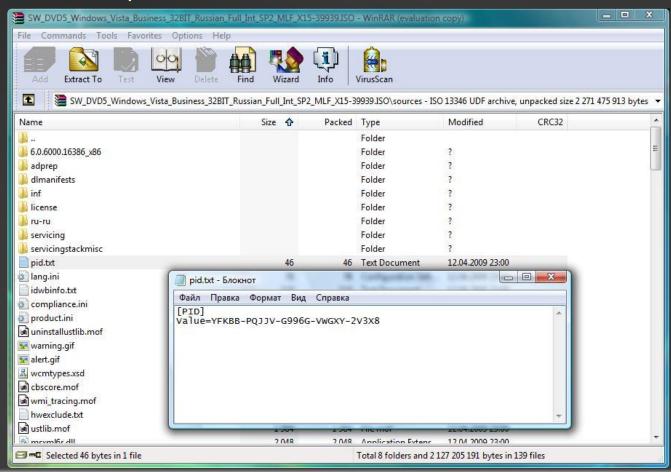
- Одна и та же на сервере КМЅ и на клиентах
- Windows Server 2008, Vista: SLSVC.EXE / "Software Licensing"
- Windows Server 2008 R2, Windows 7, Windows Server 2003 SP1: SPPSVC.EXE / "Software Protection"

KMS и клиенты

- По умолчанию, для ПО, поставляемого по каналам корпоративного лицензирования, требуется инфраструктура КМS
- · KMS не ведет подсчет использованных лицензий

Установка клиентов KMS

 Product Key можно найти в дистрибутиве ОС, поставляемой по корпоративной лицензии, в файле sources\pid.txt



Установка клиентов KMS

Редакция операционной системы	Product Key для KMS-активации
Windows Vista Business	YFKBB-PQJJV-G996G-VWGXY-2V3X8
Windows Vista Enterprise	VKK3X-68KWM-X2YGT-QR4M6-4BWMV
Windows 7 Professional	FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4
Windows 7 Enterprise	33PXH-7Y6KF-2VJC9-XBBR8-HVTHH
Windows Server 2008 Datacenter	7M67G-PC374-GR742-YH8V4-TCBY3
Windows Server 2008 Enterprise	YQGMW-MPWTJ-34KDK-48M3W-X4Q6V
Windows Server 2008 Standard	TM24T-X9RMF-VWXK6-X8JC9-BFGM2
Windows Web Server 2008	WYR28-R7TFJ-3X2YQ-YCY4H-M249D
Windows Server 2008 R2 Datacenter	74YFP-3QFB3-KQT8W-PMXWJ-7M648
Windows Server 2008 R2 Enterprise	489J6-VHDMP-X63PK-3K798-CPX3Y
Windows Server 2008 R2 Standard	YC6KT-GKW9T-YTKYR-T4X34-R7VHC
Windows Web Server 2008 R2	6TPJF-RBVHG-WBW2R-86QPH-6RTM4

Установка сервера KMS

- Получите ключ KMS на портале корпоративного лицензирования Microsoft
- · Установите (если требуется) операционную систему
- Установите ключ КМЅ
 - SLMGR.VBS /ipk <key>
 - · Требуются повышенные привилегии
- Активируйте сервер KMS
 - Онлайн, через Интернет
 - SLMGR.VBS /ato
 - · Или по телефону
 - SLUI.EXE 4
- По умолчанию, каждый ключ KMS может быть использован для установки до 6 серверов KMS
- Ключ КМЅ не предназначен для инсталляции обычных серверов и рабочих станций

Обнаружение сервера КМЅ

- Автообнаружение
 - Клиент просматривает в DNS особую SRV-запись, регистрируемую сервером KMS
 - · KMS регистрирует в своей зоне DNS SRV-запись:
 - _VLMCS._TCP.mydomain.com (_service._protocol)
- Сервер DNS должен поддерживать SRV-записи и динамическое обновление
- Прямое соединение
 - Заставляет клиента просматривать только указанные FQDN или IP-адрес сервера KMS
 - Записи добавляются в реестр на клиентах
 - SLMGR.VBS /skms <KMS_FQDN or IP>[:<port>]

Автообнаружение сервера **KMS** AD / DNS 1. Клиент запрашивает O. KMS регистрирует в DNS SRV-записи SRV-запись _VLMCS 2. DNS возвращает записи KMS-серверов 4. KMS возвращает текущий Кпиент выбирает KMS из (Vista:25, Server:5)

KMS Client

KMS Host

Автообнаружение: особенности

- · Сервер KMS автоматически не регистрирует SRVзаписи в других зонах DNS
 - · например, в дочерних доменах
- Вы должны настроить регистрацию в дочерних доменах вручную
 - HKLM\SOFTWARE\Microsoft\Windows NT \CurrentVersion\SL\DnsDomainPublishList
 - тип REG_MULTI_SZ
 - Введите имена доменов, каждое в отдельной строке
- КМS-хост должен обладать разрешениями на запись в зонах DNS для создания SRV-записей
- Имя сервера КМЅ должно разрешаться из других доменов
 - DNS forwarding или А-запись

Автообнаружение: особенности

- В рабочей группе клиенты используют основной DNS-суффикс или значение DNS domain, назначаемое DHCP (option 15)
 - В Active Directory клиенты используют основной DNS-суффикс или DNS-имя домена

Улучшения для Windows 7 и Windows Server 2008 R2

- · Поиск по списку DNS-суффиксов
 - Достаточно зарегистрировать SRV-запись KMS только в одной зоне DNS
 - Большинство клиентов имеют в настройках протокола TCP/IP список суффиксов DNS
 - redmond.corp.microsoft.com
 - · corp.microsoft.com
 - microsoft.com
- Для леса из многих доменов теперь достаточно одной записи KMS

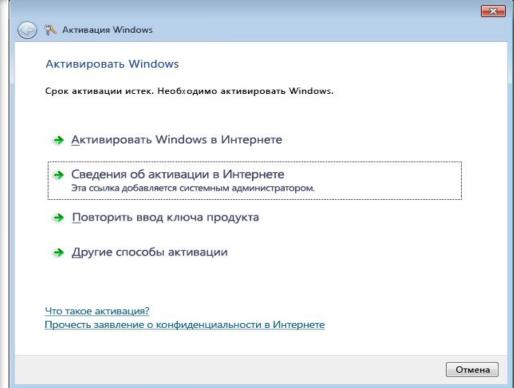
Улучшения для Windows 7 и Windows Server 2008 R2

- Вес и приоритет SRV-записей
 - Сервер KMS выбирается клиентом на основе веса и приоритета SRV-записи
 - Не поддерживается в Windows Server 2008,
 Windows Vista
 - · Сервер KMS выбирается случайным образом из списка
 - Поддерживается в Windows Server 2008 R2, Windows 7
- Запрет кэширования сервера KMS на клиенте (slmgr /ckhc)
 - Клиент всегда обращается к DNS за именем сервера КМS

Улучшения для Windows 7 и Windows Server 2008 R2

Изменения в элементах интерфейса





Группы ключей КМЅ

- КМЅ поддерживает только один ключ
- Можно ли на одном ключе активировать разные продукты?
- Группы ключей
 - Иерархия лицензионных ключей, способных активировать семейства продуктов
- Server Group C
 - Server Group B
 - Server Group A
 - · Client VL

Группы ключей КМЅ

Group C

Windows Server 2008
Datacenter
Windows Server 2008 for
Itanium

+ Group B editions

Windows Server 2008 Enterprise Windows Server 2008 Standard

+ Group A editions

Group A

Windows Web Server 2008
Windows HPC Server 2008
+Client VL editions

Client VL

Windows Vista Enterprise Windows Vista Business

Group C

Windows Server 2008 R2 Datacenter Windows Server 2008 R2 for Itanium

+ Group B & previous editions Group B

Windows Server 2008 Enterprise R2

Windows Server 2008 Standard R2

+ Group A & previous editions

Group A

Windows Web Server 2008 R2 Windows Server 2008 R2 HPC + Client and previous editions

Client VL

Windows 7 Enterprise
Windows 7 Professional
+ previous editions

Группы ключей КМЅ

- КМS-сервер на базе Windows Vista / Windows 7 поддерживает только группу ключей Client VL
- КМS-сервер под управлением любой версии Windows Server 2008 / 2008 R2 поддерживает любые группы ключей
- Установите обновление КВ968912 для поддержки активации Windows 7 / Windows Server 2008 R2 KMS-сервером под управлением Windows Vista / Windows Server 2008

Время действия активации КМS Неактивированные клиенты

- по умолчанию, пытаются соединиться с сервером КМЅ каждые 2 часа
- После активации лицензионный период устанавливается 180 дней (6 месяцев)
- Активированный клиент каждые 7 дней пытается обновить активацию
 - Успешно? лицензионный период вновь устанавливается в 180 дней
 - · Неудачно? клиент ищет другой сервер KMS

Порог активации KMS

- В отличие от клиентов МАК, для клиентов КМЅ требуется регулярное подтверждение активации
- Сервер КМЅ не начинает активацию клиентов, пока их число не достигает предопределенного порога (activation count)
 - Windows Vista / Windows 7: 25 клиентов
 - · Windows 2008 / Windows Server 2008 R2: 5 клиентов
 - Считаются только клиенты, обращавшиеся к серверу КМS в течение последних 30 дней
- Для ОС Vista SP2, Windows Server 2008 SP2 / 2008 R2, Windows 7 считаются как физические, так и виртуальные машины, для остальных – только физические

Достоинства сервиса КМЅ

- Не требуется доступ в Интернет или активация по телефону
- Не требуется резервное копирование
 - · переустановить сервер и KMS-ключ
- Не требователен к ресурсам
 - сосуществует с другими службами
- Обычно не требуется более 2 серверов КМЅ в организации
 - Исключение сложная инфраструктура, юридические ограничения и т.п.

МАК: ключ многократной активации

- Один ключ для многих систем
 - Подходит для нескольких версий ПО
- Число активаций определяется лицензионным соглашением
- В случае компрометации запросите Microsoft закрыть текущий ключ и выпустить новый
- · Требуется соединение с Центром активации Microsoft

МАК: особенности

- Активация клиентов производится один раз
- Требуется прямой (или через анонимный прокси-сервер) доступ в Интернет
 - Активация по телефону также доступна
- Активация по МАК-ключу может быть добавлена в сценарий автоматической установки Windows
- Оставшееся число активаций можно посмотреть:
 - Online: Microsoft Volume Licensing Service Center (VLSC), eOpen, or MSDN
 - VAMT (Options -> Manage MAK Keys)

МАК: замечания

- Не должен быть основным методом активации
 - · предпочтение KMS
 - используйте МАК, если невозможно использовать КМS
- Значительные изменения конфигурации оборудования потребуют повторной активации
 - это отразится на счетчике активаций не в лучшую сторону
- Клонированная система должна пройти отдельную активацию

Утилиты

Volume Activation Management Tool

(УУтМпт)а для автоматизации и управления корпоративной активацией на множестве клиентов

- MAK Independent Activation
 - Устанавливает ключи МАК и позволяет клиентам активироваться
- MAK Proxy Activation
 - Устанавливает ключи МАК на клиенты без доступа в Интернет и активирует их для клиентов
- KMS Activation
 - · Устанавливает и активирует ключи VL по умолчанию
- · Версия 1.1 доступна на сайте Microsoft
- Версия 1.2 (в составе WAIK) добавляет поддержку
 Windows 7 and Windows Server 2008 R2

Утилиты **SLMGR.VBS**

- Основная утилита конфигурации
- Наиболее известные ключи
 - установить ключ защиты ПО · -ipk
 - · -ato активировать
 - · -dli показать лицензионную информацию
 - · -xpr срок окончания лицензионного состояния
 - -skms прямое подключение клиента
 - · -rearm Reset OOB grace period (можно выполнить ограниченное число раз)
- Сценарий находится в папке \System32

УТИЛИТЫ SLUI.EXE

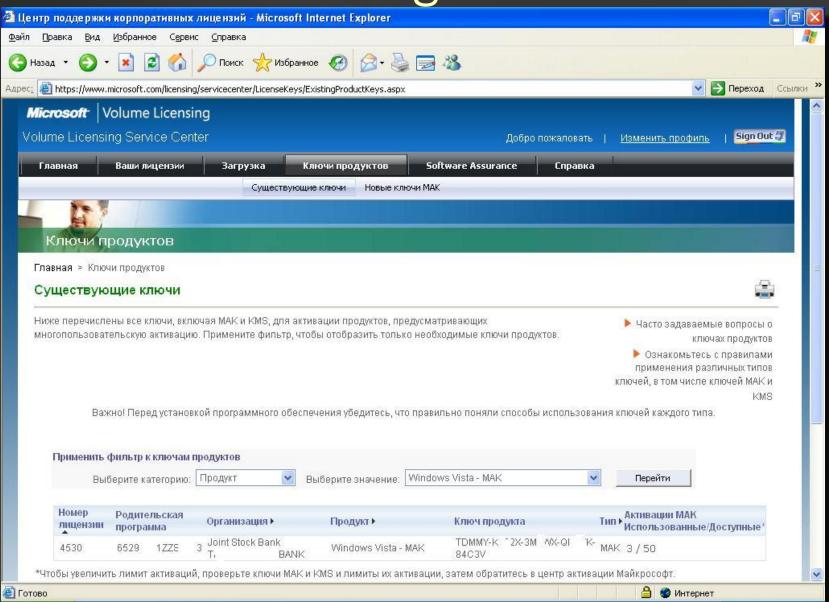
- Графический инструмент Volume Activation
- Наиболее известные ключи
 - 1: Показать статус активации
 - 2: Предпринять активацию
 - 3: Сменить ключ продукта
 - · 4: Предпринять активацию по телефону
 - 0x02a 0x<error code>
 - · Что означает ошибка 0x8007267С, событие 12293?
 - SLUI 0x02a 0x8007267C

Мониторинг активаций и получение ключей KMS и

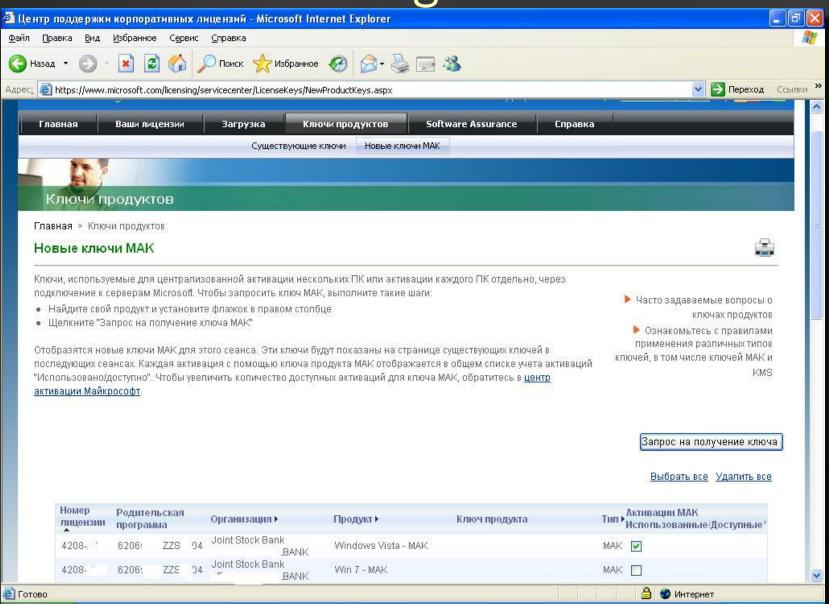
Malkme Licensing Service Center

- зарегистрированные лицензии
- информация по ключам КМЅ
- запрос нового ключа МАК
- счетчик МАК-активаций
- https://www.microsoft.com/licensing/servicece
 nter
- Журнал событий
 - Key Management Service Event Log

Volume Licensing Service Center



Volume Licensing Service Center



Планирование инфраструктуры KMS

Рекомендации

Анализ конфигурации Выберите ваш вариант

- Корпоративная сеть
 - Лес или леса с доверительными отношениями
 - Леса без доверительных отношений (разработчики, учебный центр и т.п.)
 - Рабочие группы
- Сеть, отделенная от корпоративной сети брандмауэром
 - Биржи, закрытые информационные системы
 - Предположение: нет доступа в Интернет

Анализ конфигурации Выберите ваш вариант

- Изолированные сети
 - 25 и более клиентов
 - менее 25 клиентов
- Изолированные клиенты
 - Демонстрационные ноутбуки
 - Компьютеры в удаленных представительствах

Рекомендации Основные принципы

- Простота
 - You can do lots of configuration doesn't mean you should
 - Vista в качестве сервера KMS плохое решение
- Используйте KMS всегда, когда это возможно и минимизируйте число серверов KMS
 - Ограничение в 6 серверов КМЅ для одного ключа можно преодолеть

Основные принципы

- Используйте ключи МАК, только когда невозможно использовать КМЅ
- Как правило, практическое решение задействует оба сценария
- Никогда не открывайте порт КМЅ (1688 по умолчанию) для подключений из Интернета

Простые решения

- Корпоративный лес и доверенные леса
 - · KMS с автообнаружением в DNS
 - Зарегистрировать сервер KMS в других DNSзонах
 - Решение для централизованного управления
- Сети, защищенные брандмауэром, допускающие открытие порта 1688
 - KMS
 - автообнаружение или настройка клиентов на прямое подключение

Рекомендации Решения среднего уровня

- Леса без доверительных отношений
 - KMS
 - Добавить записи SRV и А вручную в каждой зоне DNS
- Рабочие группы
 - KMS
 - Клиенты DHCP будут использовать корпоративный DNS
 - Прописать DNS на клиентах со статической конфигурацией TCP/IP
 - Добавить записи SRV и А в зоне DNS вручную

Решения среднего уровня

- Тестовая лаборатория: операционные системы часто переустанавливаются
 - Не активировать ПО
 - льготный период Out-Of-Box можно "перезапустить" 3 раза
 - Slmgr.vbs –rearm
 - · до 240 дней для Windows Server 2008
 - Даже если льготный период истек, возможно повторно использовать Confirmation ID от первой прокси-активации по ключу МАК

Рекомендации Сложные решения

- Сети без какого-либо внешнего доступа
 - Прокси-активация по ключу МАК
 - требуется потратить время, но выполняется нечасто
 - Если клиентов больше 25, то установите внутренний сервер KMS
 - · Ограничить доступ к ключу KMS
 - · Активировать сервер KMS по телефону
 - Активация ключа МАК по телефону
 - Решение не масштабируемое

Общие решения

- При необходимости настройте клиентов на прямое подключение
 - Slmgr.vbs –skms kms.mydomain.com
 - Игнорируется автообнаружение
 - · Создайте запись CNAME в DNS
 - · kms.mydomain.com
 - По этой записи могут отвечать 1-2 сервера KMS
- Избегайте создания множества серверов КМЅ, если это не продиктовано юридическими требованиями

Итоги

- · Volume Activation технология, с которой удобно работать в корпоративной сети
- · VA следует использовать для всех современных операционных систем Microsoft
- Не все очевидно на первый взгляд
- Создайте правильную инфраструктуру KMS



Информационные ресурсы

- · Техническая информация по Volume Activation
 - http://www.technet.com/volumeactivation
- Мультимедиа-ресурсы
 - http://www.microsoft.com/volumeactivation



Статья Шона Дьюби в
 Windows IT Pro /RE "Активация
 в Windows Server 2008"

http://www.osp.ru/win2000/2009/05/954486

