Active Directory Rights Management Services в Windows Server 2008

Александр Шаповал
Microsoft

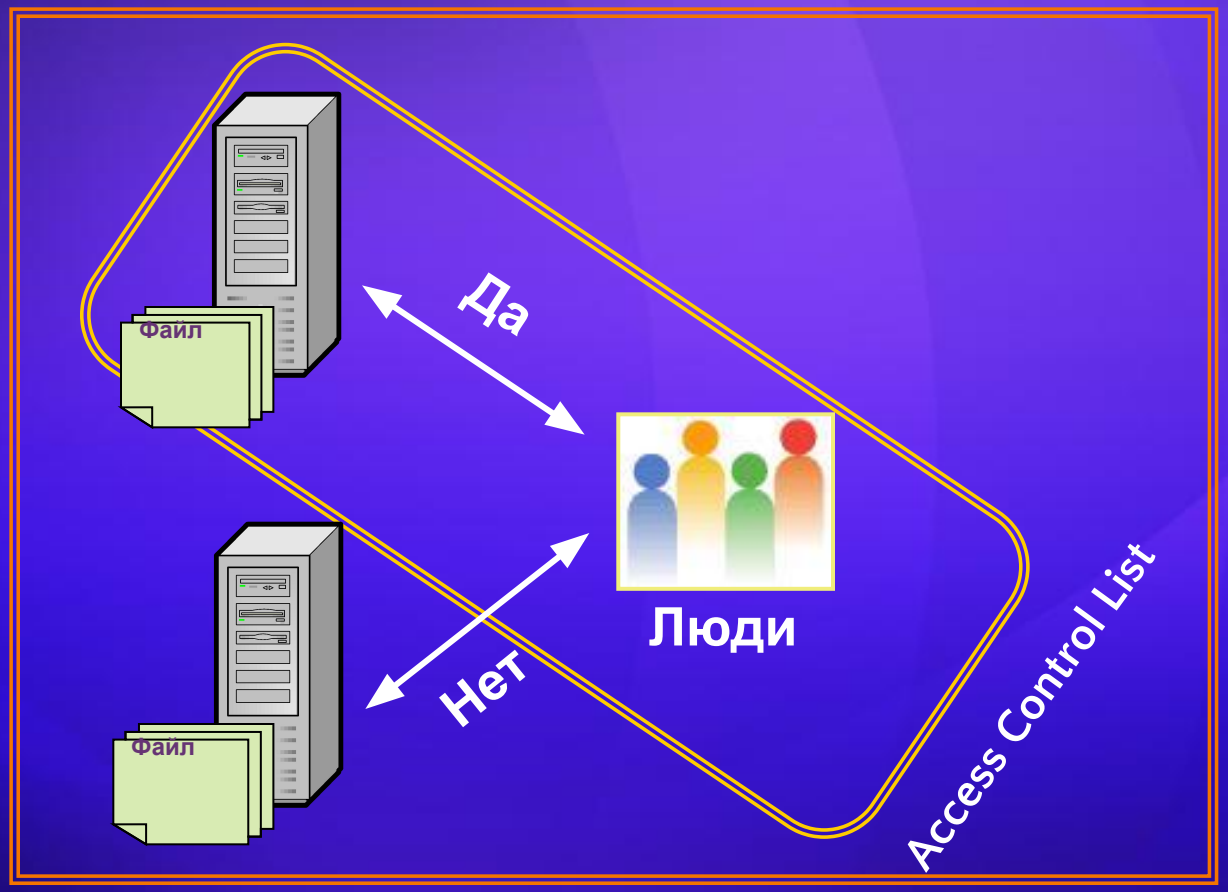
Содержание

- Концепция RMS
- Архитектура RMS
- Новые возможности RMS в Windows Server 2008

Содержание

- Концепция RMS
- Архитектура RMS
- Новые возможности RMS в Windows Server 2008

Классическое управление доступом



Межсетевой экран

Rights Management Services

- RMS позволяет организациям создавать и применять политики использования информации, которой они владеют
  - Для любого приложения
  - В любом формате
- Политика использования «живет» вместе с информацией
  - Куда и каким бы способом ни перемещалась защищенная информация

Rights Management Services

- Данные защищены во время хранения, передачи и обработки
- Защита внутри и снаружи организации

Защита информации

- Постоянный контроль над тем, кто имеет доступ к документу, что он может с ним делать и как долго

Применение политик

- Централизованное управление политиками
- Протоколирование информационных потоков

Контроль на уровне организации

- Доступный программный интерфейс
- Поддержка в приложениях Microsoft и третьих фирм

Расширяемая платформа

Rights Management Services

- Н
во
- Н
не
- Н

ности

Содержание

- Концепция RMS
- Архитектура RMS
- Новые возможности RMS в Windows Server 2008

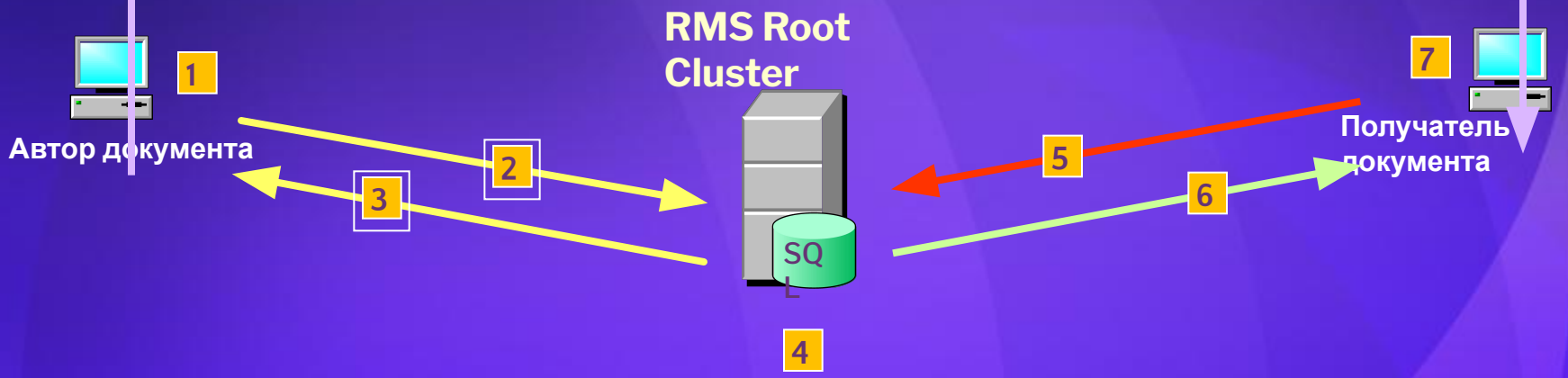
Компоненты

- Active Directory Rights Management Services (RMS)
  - Встроенная компонента (роль) Windows Server 2008
- Клиентская часть RMS
  - Rights Management APIs для всех версий Windows (98SE, 2000, XP, 2003)
  - Встроена в Windows Vista
  - Rights Management Add-on для Internet Explorer
- Software Development Kit
  - Инструментарий разработчика для серверной и клиентской частей
- Приложения, поддерживающие RMS
  - Microsoft Office 2003
    - Word, Excel, Outlook, PowerPoint
  - Microsoft Office 2007
    - + InfoPath
  - Любое приложение, созданное с использованием RM SDK

Инфраструктура

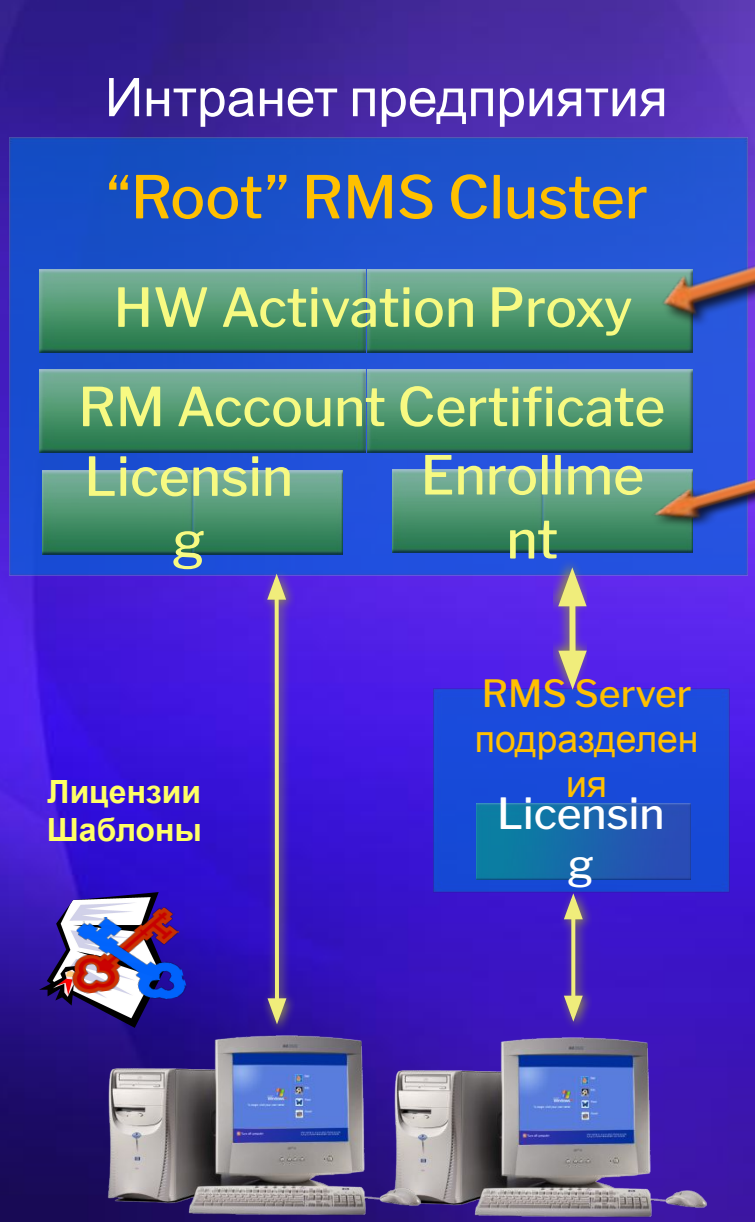
- Active Directory
  - Windows 2000 Server SP3 или выше
- Internet Information Services
  - ASP.NET
- Message Queuing
- SQL Server 2000 SP4 или выше

Рабочий процесс



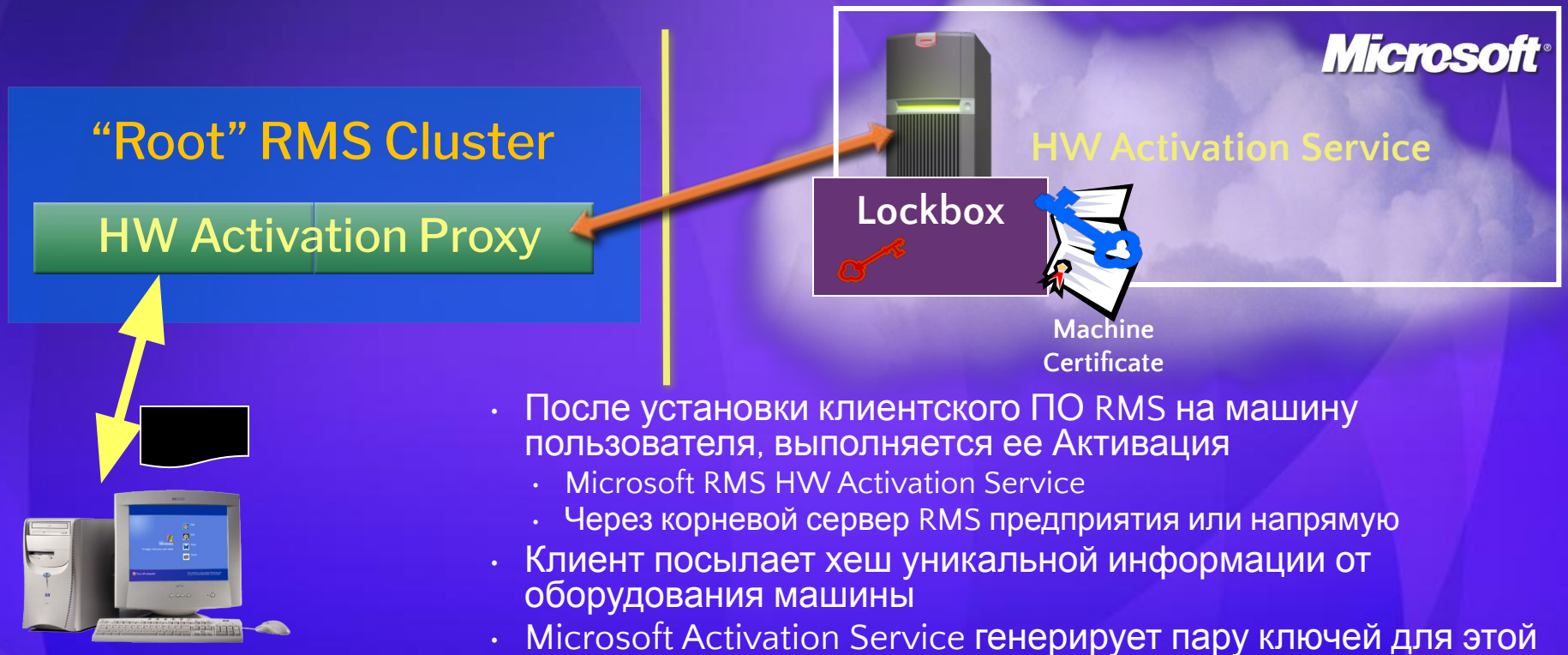
1. Автор создает документ. Автор формирует набор прав и правил для документа (Publishing License). Приложение зашифровывает документ с симметричным ключом
2. Приложение посылает Publishing License серверу RMS на подпись
3. RMS подписывает Publishing License и возвращает ее приложению
4. Автор пересылает файл получателям документа
5. Получатель открывает файл. Приложение посылает серверу RMS запрос на Use License. В этот запрос включаются RM Account Certificate (RAC) получателя и Publishing license документа
6. RMS проверяет запрос и RAC, идентифицирует получателя. При успешной проверке RMS выдает получателю лицензию на работу с документом
7. Приложение получает лицензию от RMS и отрабатывает правила, заложенные в ней. Получатель работает с документом

Топология RMS



- “Root” RMS Cluster
  - Корень структуры доверия RMS предприятия
  - Регистрируется в UDDI Microsoft
- Дополнительный сервер лицензий уровня подразделения. Регистрируется на корневом сервере
- Каждая клиентская машина, участвующая в работе RMS активируется в Microsoft HW Activation Service и получает персональный Lockbox

Сертификат машины



- После установки клиентского ПО RMS на машину пользователя, выполняется ее Активация
  - Microsoft RMS HW Activation Service
  - Через корневой сервер RMS предприятия или напрямую
- Клиент посылает хеш уникальной информации от оборудования машины
- Microsoft Activation Service генерирует пару ключей для этой машины
  - На основе присланной информации создает уникальный Lockbox, в котором зашифрован личный ключ машины
  - Выдает сертификат (Machine Certificate), в котором размещается открытый ключ

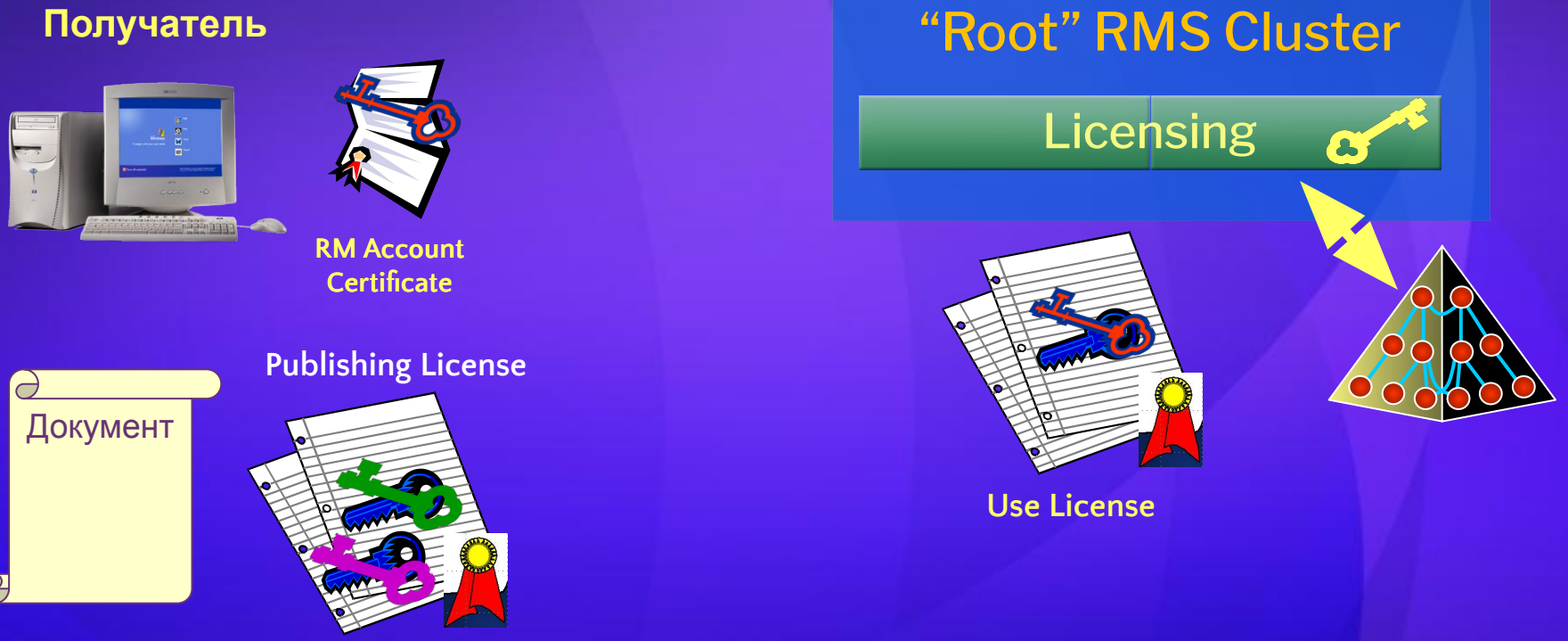
Сертификат пользователя

- После активации машины, пользователь должен получить RM Account Certificate (RAC) для этой машины
  - Бывают Постоянные и Временные сертификаты RAC
- Сертификат RAC выдается корневым сервером RMS
  - Сервер RMS аутентифицирует пользователя в Active Directory
- RAC содержит идентифицирующую информацию пользователя и его пару ключей
  - Открытый
  - Личный, зашифрованный на открытом ключе машины

Лицензия публикации

- Publishing License выдается автору документа сервером RMS и содержит
  - Информацию о правах доступа к информации документа и о правилах ее использования
  - Симметричный ключ для расшифровки документа, зашифрованный на открытом ключе сервера RMS
  - Вторую копию симметричного ключа, зашифрованную на открытом ключе автора документа
- Publishing License подписана личным ключом сервера RMS

Лицензия на работу



- Use License выдается получателю документа на основании Publishing License и его RAC, которые он присылает серверу RMS в запросе
- Лицензия на работу содержит симметричный ключ для расшифровки документа, зашифрованный на открытом ключе получателя

demo

Использование RMS

Содержание

- Концепция RMS
- Архитектура RMS
- Новые возможности RMS в Windows Server 2008

Новые возможности

- Развертывание
  - Не требуется активация в MS Activation Service
  - Устанавливаются все требуемые службы
- Управление и администрирование
  - MMC-консоль для администрирования
  - Реализация всех функций скриптами
  - Генерация отчетов
  - Административные роли
- Взаимодействие с внешними организациями
  - Интеграция RMS со службами ADFS
- Распространение шаблонов

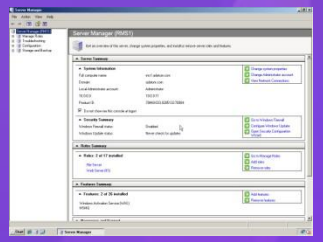
Внедрение

Развертывание инфраструктуры RMS

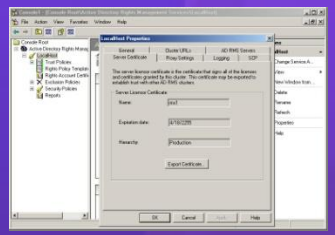
- Упрощенная установка настройка
  - Клиент RMS v2 встроен в Windows Server 2008 и Windows Vista
  - RMS – одна из серверных ролей
    - Автоматическая установка зависимых компонент (SQL Embedded, WPF, IIS, MSMQ, и др…)
  - Новый мастер решает все задачи, связанные с настройкой RMS
  - Автоматическое обнаружение и регистрация RMS-клиентов
- Функциональная независимость
  - Все необходимые сертификаты выдаются автономно, не требуется взаимодействие с сервисами Microsoft
  - Нет ограничения на срок действия корневого сертификата
- Обратная совместимость
  - Обновление сохраняет все защищенные до этого документы
  - Возможно взаимодействие с RMS-серверами предыдущей версии

Интерфейс

Установка RMS



Срок действия сертификата



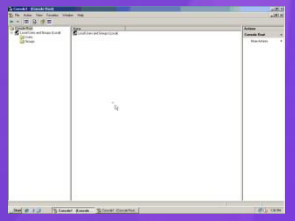
Среда работы

Управление RMS

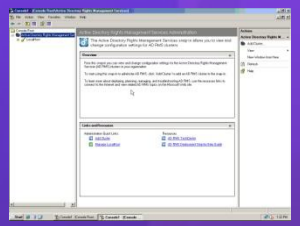
- Улучшения для администратора
  - Отказ от Web-интерфейса версии 1.0
  - Использование оснастки в консоли MMC……
    - Знакомая административная модель
    - Единый подход ко всем серверным ролям
  - Выделение задач (обязательных, рекомендованных, дополнительных)
    - Выполнение «задач под рукой»
  - Ролевое администрирование
    - Администраторы предприятия, шаблонов, аудиторы
- Администрирование с помощью скриптов
  - Задачи управления доступны через Scripting API

Интерфейс

Управление на основе задач



Роли администратора



Эффективность

Основные направления развития

- Усовершенствованные мониторинг и отчетность
- Общее повышение производительности

Модернизация модели «здоровья» RMS

- Управление на основе событий
- Обработка ошибок – более конкретные и подробные
- Метрики
  - Перехват специфичных для RMS событий

MOM 2005 Management Pack

- После Beta 2

Анализ журнала

- Интегрированный инструмент генерации отчетов

Внешнее взаимодействие

Довери-тельные отношения	• Обе организации должны развернуть RMS • Одно- или двусторонний обмен сертификатами для включения доверительных отношений
Extranet-записи	• Добавление записей в AD для внешних пользователей • Прохождение SSL-трафика ко внутр. RMS-серверам • Использование сертификатов для аутентификации • Использование VPN для усиления защиты
Hosted Services	• Использование Windows Live ID • Решения партнеров
Federated RMS	• Двустороннее взаимодействие, развертывание RMS только в одной организации • Обе организации настраивают ADFS

Типовой сценарий

Adatum

Крупная производственная компания

Федеративные отношения с Contoso

Обмен конфиденциальными данными между сотрудниками Adatum **и** Contoso

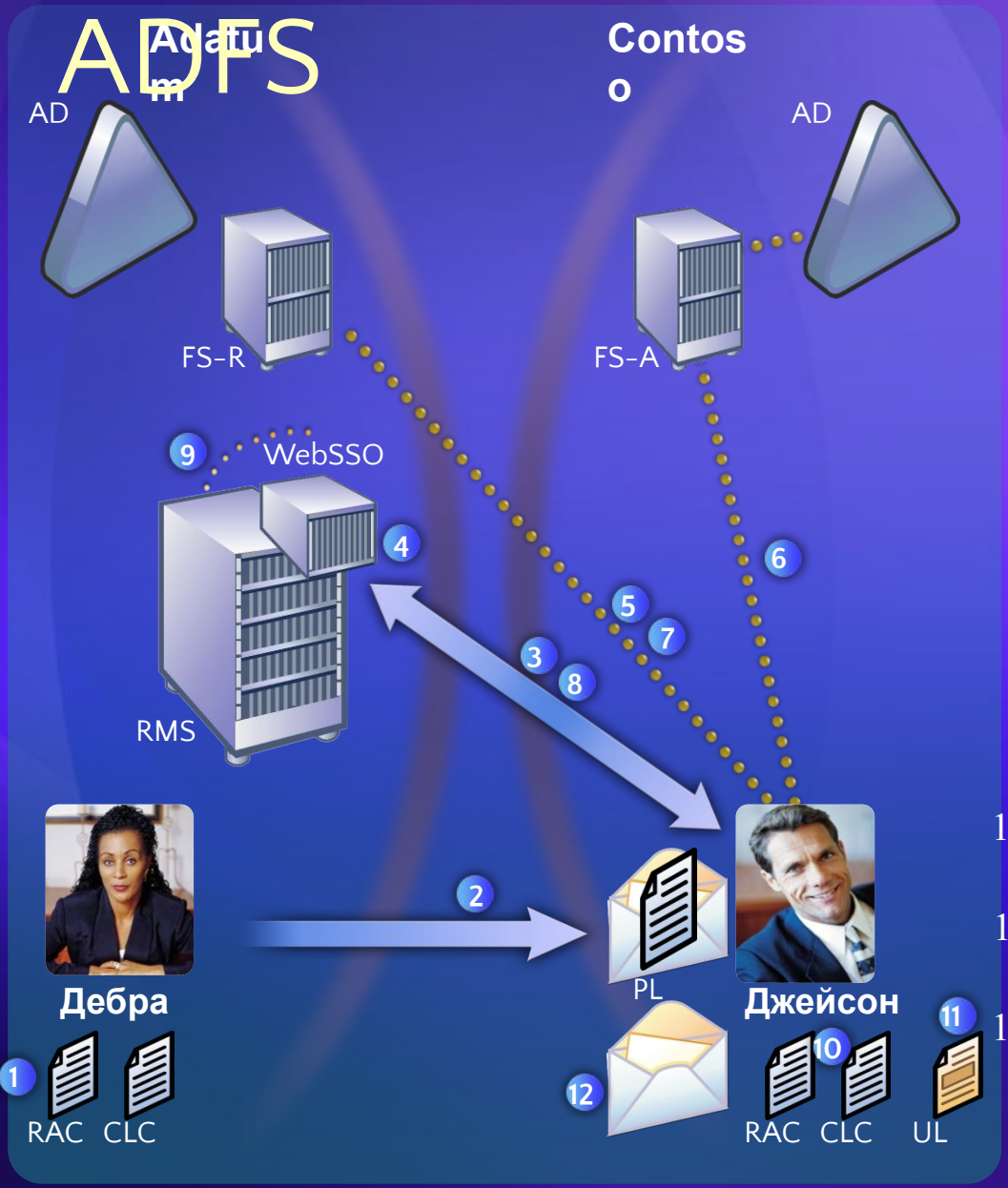
Дебра

Contoso

PR-услуги для Adatum

Джейсон

Взаимодействие на основе ADFS



1. Дебра применяет политику к письму
2. Дебра посылает защищенное письмо Джейсону в Contoso
3. Компьютер Джейсона обращается к RMS-серверу
4. Агент ADFS перехватывает запрос
5. RMS-клиент перенаправляется FS-R для аутентификации
6. RMS-клиент перенаправляется FS-A для аутентификации
7. Сформированная заявка (claim) возвращается к FS-R
8. RMS-клиент запрашивает UL
9. WebSSO-агент перенаправляет запрос RMS-серверу
10. RMS-сервер возвращает сертификат RAC Джейсону
11. RMS-сервер формирует и передает Джейсону UL
12. Джейсон получает доступ к содержимому письма

Требования

- Домен ресурсов
  - Полностью подготовленная инфраструктура RMS
  - Federation Server (Windows Server 2003 R2 или 2008)
  - SSL на вирт. каталогах RMS и на Federation Server
- Домен учетных записей
  - Federation Server (Windows Server 2003 R2 или 2008)
  - SSL на Federation Server

Распространение шаблонов

- Основная проблема: настройка на клиентах вручную
- Новый метод на базе SOAP для получения шаблонов
- RMS-клиент в Vista SP1 поддерживает автоматическое обновление шаблонов с сервера
  - Новый API в клиенте RMS для получения шаблонов
  - WMI-задание по расписанию вызывает API для получения шаблонов

Развитие RMS

Office 2007 Q4 CY06	• SharePoint (MOSS) 2007 • InfoPath 2007 • Усовершенствование пользовательского интерфейса
Windows Vista & XPS Q4 CY06	• RMS “встроен” в Windows Vista • Переход на Windows Presentation Foundation
Windows Mobile 6 Q2 CY07	• Поддержка смартфонов и КПК • Pocket Outlook и Pocket Office
Exchange 2007 SP1 Q4 CY07	• Технология Pre-licensing для RMS-сообщений • Первый шаг в интеграции с Exchange
Решения партнеров	•Система архивации с поддержкой RMS •Защита документации CAD

Вопросы

- http://blogs.technet.com/ashapo
- Внешний доступ к службам RMS
  - Веб-трансляция, 7 ноября
  - http://www.microsoft.com/rus/technet

Microsoft®

Your potential. Our passion.™

© 2007 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

Microsoft Confidential