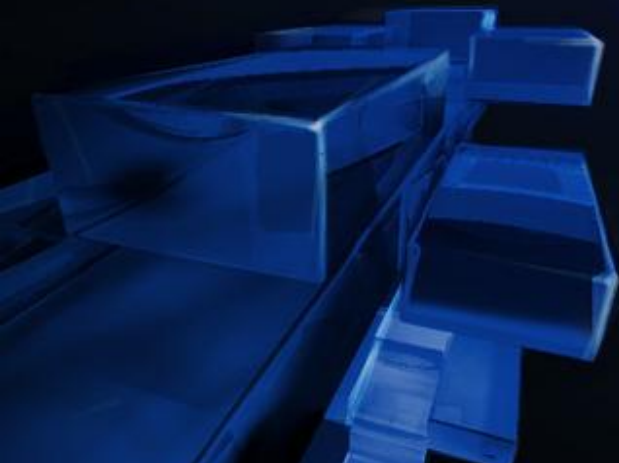




Реализация требуемой политики безопасности серверов и рабочих мест

Бешков Андрей
Microsoft



Содержание

- Поддержка заданных конфигураций – System Center Desired Configuration
- Принудительное исполнение политик здоровья – Network Access Protection

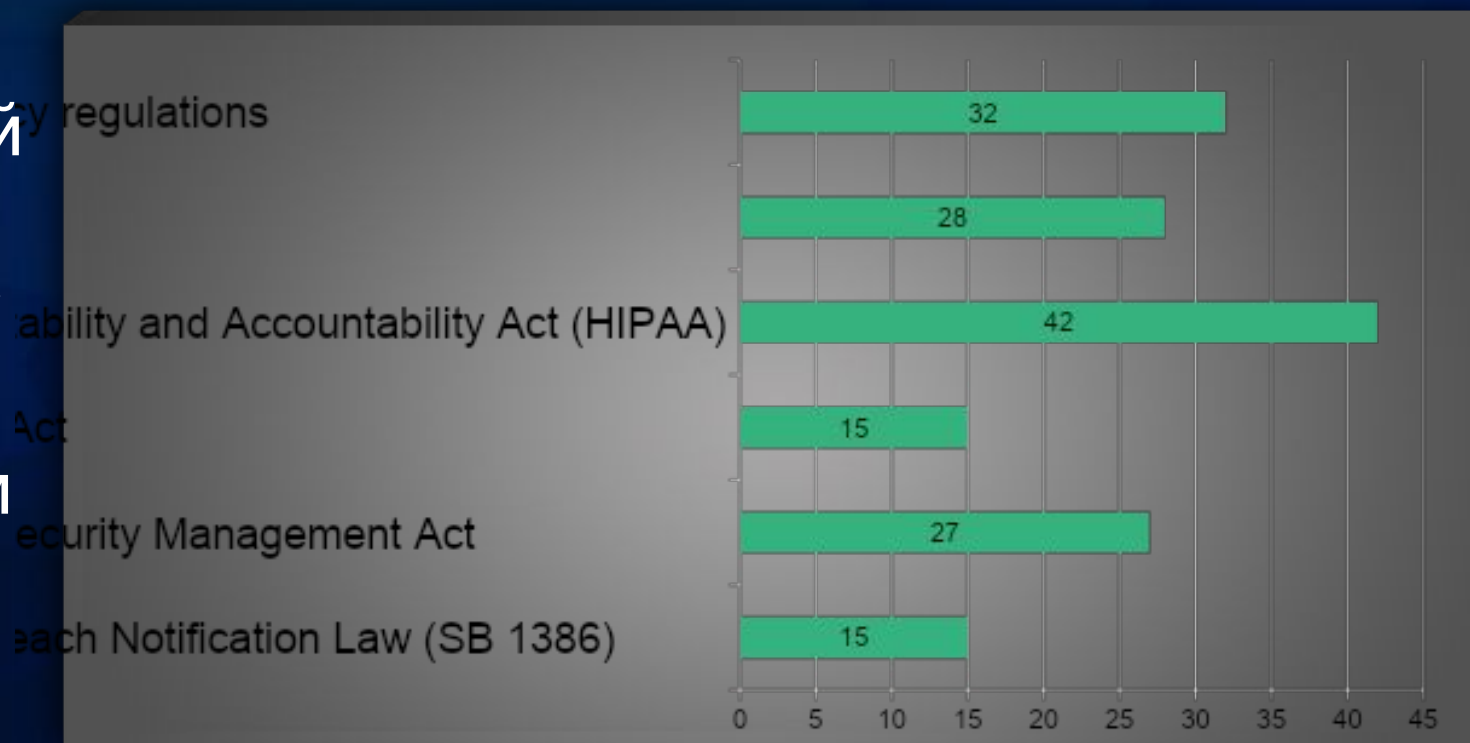
Поддержка заданных
конфигураций System Center
Desired Configuration

Цена соответствия стандартам

- ИТ департаменты ежегодно тратят от 5000 до 20000 человеко часов для поддержания соответствия организации требованиям стандарта Sarbanes-Oxley
 - Survey on Sarbanes-Oxley Compliance Practices Within IT Organizations and Businesses by French Caldwell, Christine Adams, and John Bace (Gartner, Сентябрь 2006)
- Корпоративные стандарты очень непросто

Соответствие стандартам

Процент организаций США не соответствующих отраслевым стандартам



Источник: “The Global State of Information Security 2006”
CIO and PricewaterhouseCoopers
Сентябрь 15, 2006

Что такое Desired Configuration Management?

DCM позволит:

- Определять стандарты корпоративных конфигураций
- Создавать отчеты и отслеживать соответствие стандартам систем Windows®
- Комбинировать данные от DCM с другими полезными функциями Configuration Manager для автоматического приведения клиентов в должное состояние

Основные сценарии применения (1)

- Отчеты о соответствии стандартам
 - Определять политики конфигураций и собирать отчеты о соответствии этим политикам
- Проверка до и после внесения изменений в системы
 - Проверка готовности системы к оказанию сервиса
 - Проверка аккуратности внесенных и эффективности запланированных изменений

Основные сценарии применения (2)

- Поиск серверов с отклонениями от заданой конфигурации
 - Приблизительно $\frac{1}{2}$ незапланированных простое происходит из-за проблем с конфигурацией!
- Уменьшить количество действий необходимое службе Helpdesk для первичного поиска неисправности и уменьшение время затраченого на разрешению проблемы
 - Helpdesk тратит больше всех людских ресурсов в ИТ

DCM термины и концепции

Конфигурационная единица – Configuration Item (CI)

- Конфигурационные единицы могут обнаруживаться, добавляться или удаляться из систем управляемых Configuration Manager
 - Конфигурационные единицы могут представлять:
 - ОС
 - Приложения
 - Общие
 - Обновления ПО

Конфигурационное состояние – Configuration Baseline

- Специальная единица – набор конфигурационных единиц с атрибутами:
 - Требуется
 - Опциональный
 - Запрещен
- Can be assigned to collections for compliance monitoring

Задачи администратора DCM

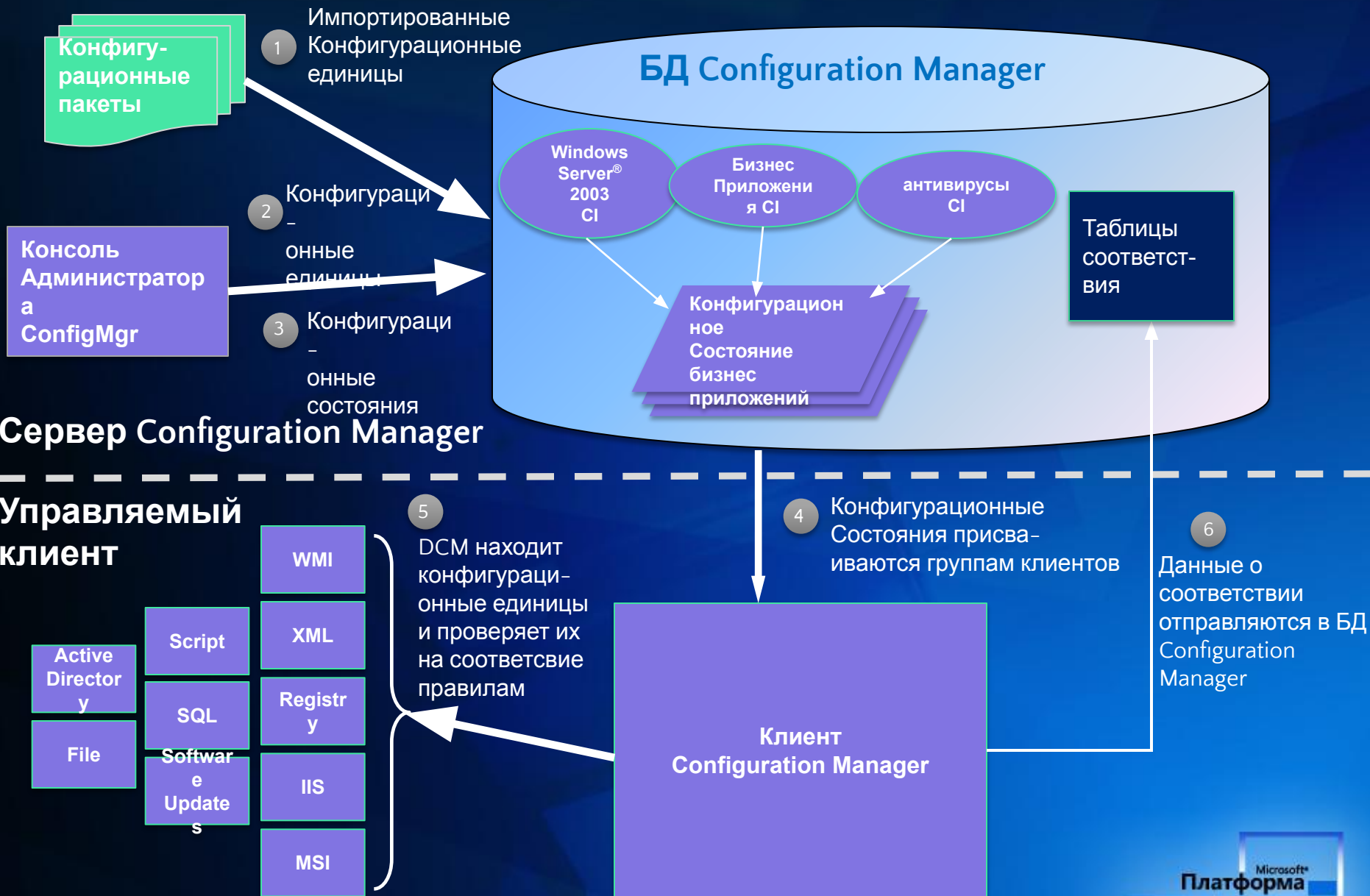
- Создание библиотеки конфигураций
 - Создание новых конфигурационных единиц и состояний через консоль администратора
 - Создание пакетов конфигурационных состояний
 - Импорт эталонных конфигурационных пакетов от Microsoft или партнеров
- Привязывать конфигурационные состояния к группам систем
 - Настраивать частоту проверки систем на соответствие
- Работать с отчетами о соответствии
- Создавать коллекции систем с помощью запросов и сообщений DCM о соответствии стандартам. Работать с набором ПО в системах средствами System Center

Библиотека конфигурационных единиц

Источники знаний:

- Microsoft и другие производители ПО
- Интеграторы
- Консалтиновые компании
- Разработчики приложений
- ИТ персонал

Потоки данных



Управление на основе моделей



Создание конфигурационных единиц

вручную с помощью Configuration Manager

- Конфигурационные единицы с нуля

 - ОС

 - Приложения

 - Общие

 - Конфигурационные состояния

- Создание дочерних конфигурационных единиц

 - Наследование от родительской единицы (или нижних единиц иерархии)

 - Добавление новых правил к унаследованным объектам и настройкам

- Копирование

Создание конфигурационных единиц Родительские/дочерние конфигурационные единицы

Копия

- Нет связи с оригиналом
- Можно редактировать все атрибуты

Копия

- Нет связи с оригиналом



Родительская

- Импортировано из Майкрософт
- Определяет основные настройки/объекты

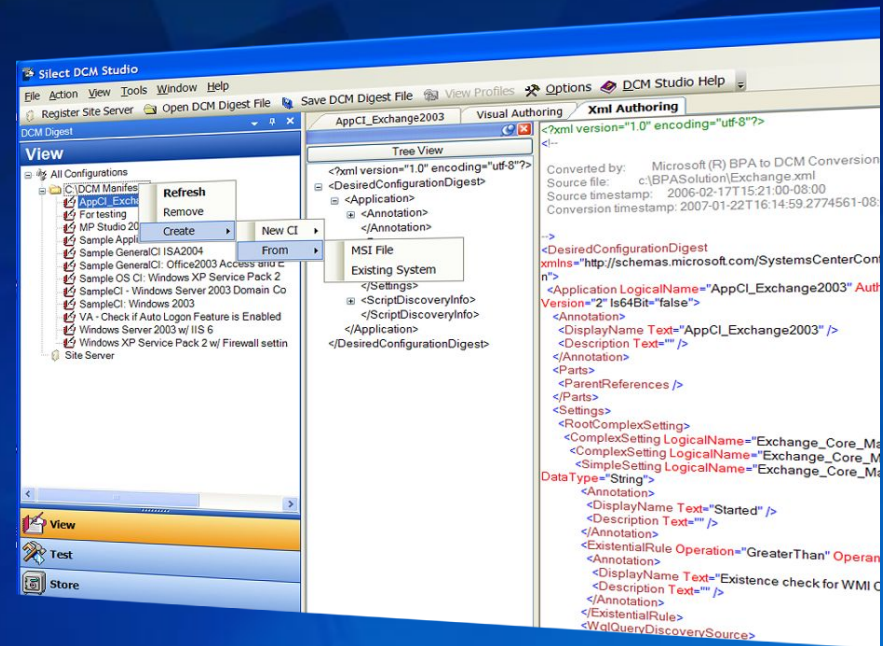
Дочерняя

- Наследует определение от родителя
- Добавляет правила к родительским настройкам и объектам

Добавочные слои наследования.

Silect Software's DCM Studio

- Работает в связке с SCCM для управления жизненным циклом конфигурационных состояний
- Создание конфигурационных состояний :
 - Обследование работающей системы (“золотой мастер”)
 - Обследование одного или нескольких MSI файлов
- Редактирование конфигурационных состояний (включая редактирование XML)
- Новые виды отчетов



Язык моделирования сервисов

- Service Modeling Language (SML) – язык моделирования построенный на основе XML стандартов. Он предоставляет большой набор конструкций для моделирования сложных ИТ систем, включая:
 - Структура системы: объекты и отношения между ними
 - Требуемые конфигурации
 - Административные политики
 - Управляющая информация такая как события, счетчики, правила для определения статуса здоровья систем, и.т.д
- Для работы с SML вам потребуется Microsoft® .Net framework 2.x

DCM 2007 улучшения по сравнению с DCM для SMS 2003

- Улучшилась интеграция компонентов системы отечающих за создании правил, планирование и тестирование
- Увеличилась скорость работы
- Упростилось масштабирование системы
- Работа с моделями и стандартами (SML)
 - Управление типами и повторное использование
 - Контроль версий
 - Наследование конфигурационных единиц
 - Композиция конфигурационных единиц в конфигурационные состояния
- Экосистема для накопления знаний. Готовые конфигурационные пакеты на порталах Microsoft и партнеров
- Инструмент конвертирования данных из DCM 2003 в DCM 2007

В ближайшем будущем

Конфигурационные пакеты от Microsoft

- Microsoft® Exchange Server 2003 и Exchange Server 2007
- Microsoft® SQL Server™ 2000 и SQL Server 2005
- Windows Server® 2003 Active Directory/DNS/ WINS/DHCP
- Microsoft® Office SharePoint® Portal Server 2003 и SharePoint® Server 2007

Конфигурационные пакеты от продуктовых групп

- Роли серверов для Microsoft® System Center Configuration Manager
- Microsoft® System Center Operations Manager 2007
- Microsoft® System Center Virtual Machine Manager 2007
- SharePoint Server 2007

Дополнительная информация

DCM

Официальная документация

<http://www.microsoft.com/systemcenter/configmgr/evaluation/configmgmt.mspx>

- DCM BLOG

<http://blogs.msdn.com/saikodi/>

- DCM Technet

<http://technet.microsoft.com/en-us/library/bb693504.aspx>

- DCM Technet Forum

<http://forums.microsoft.com/TechNet/ShowForum.aspx?ForumID=1817&SiteID=17>

- Веб-трансляции

<http://msevents.microsoft.com/cui/WebCastEventDetails.aspx?EventID=1032345476&EventCategory=4&culture=en-US&CountryCode=US>

Принудительное исполнение политик здоровья – Network Access Protection

Канонический подход к безопасности

- Защитим периметр (межсетевой экран, VPN)
- Вынесем сервера в демилитаризованную зону (DMZ)
- Построим систему управления конфигурациями и изменениями (развертывание и обновления систем, антивирусы)
- Внедрим систему обнаружения вторжений (IDS)

И надеемся что все пойдет
хорошо.....

Реальное положение дел

- 20% инцидентов безопасности происходит по вине внешних злоумышленников
- 80% с участием внутренних сотрудников

Источник: Исследование Национального центра оценки угроз США (National Threats Assessment Center, NTAC) и координационного центра CERT при Университете Карнеги-Меллона. 2004 г.

Проблемы с внутренними пользователями

- Излишние полномочия
- Редкие обновления (мобильные пользователи)
- Недостаточная грамотность в вопросах безопасности
- Неподконтрольность гостевых и домашних рабочих мест

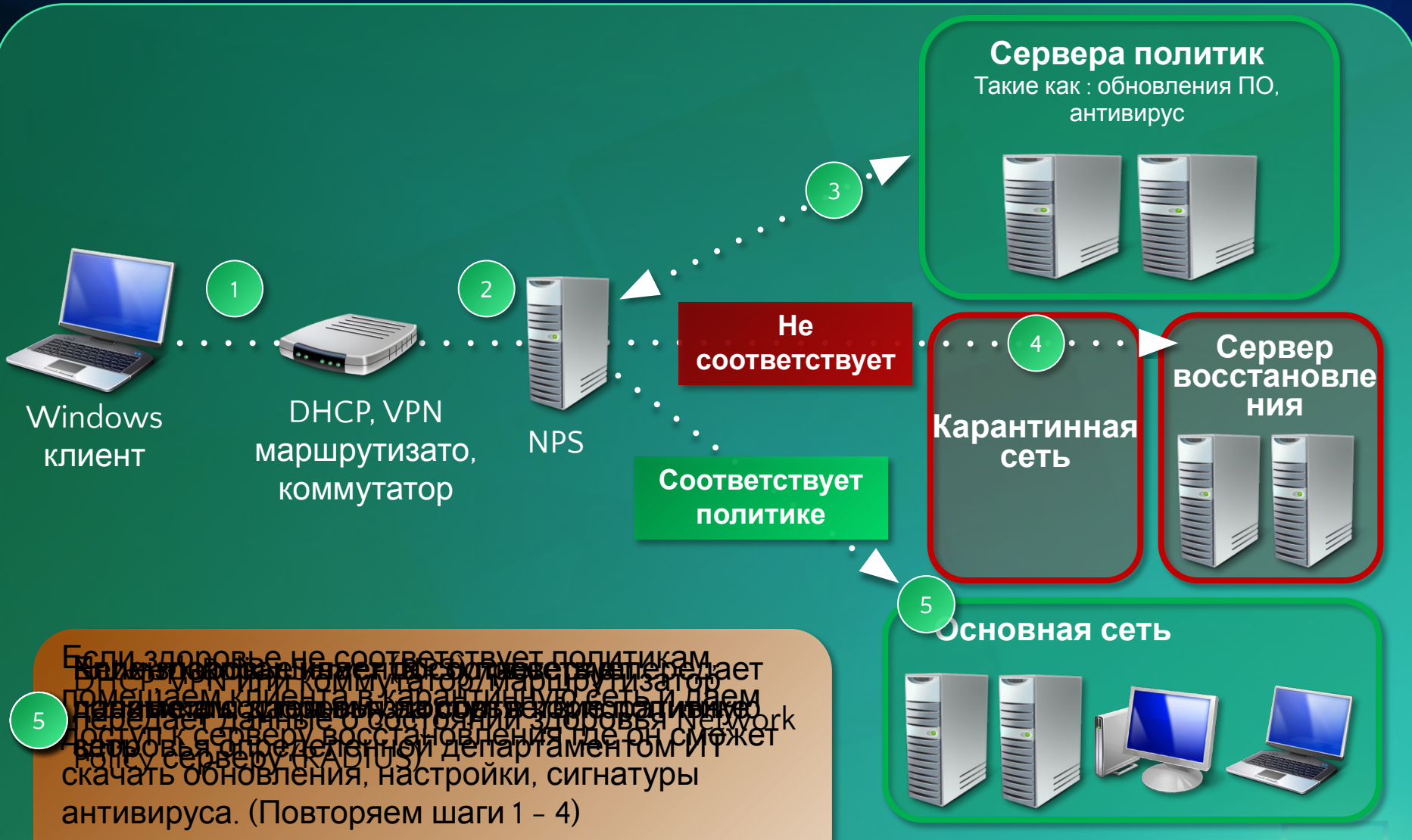
Пожар потушили! Кто виноват?

Нет виновных??!!!!

**Трудно отслеживать
исполнение политик и
регламентов....**

...и реагировать вовремя!!!!

Защита сети с помощью NAP



5

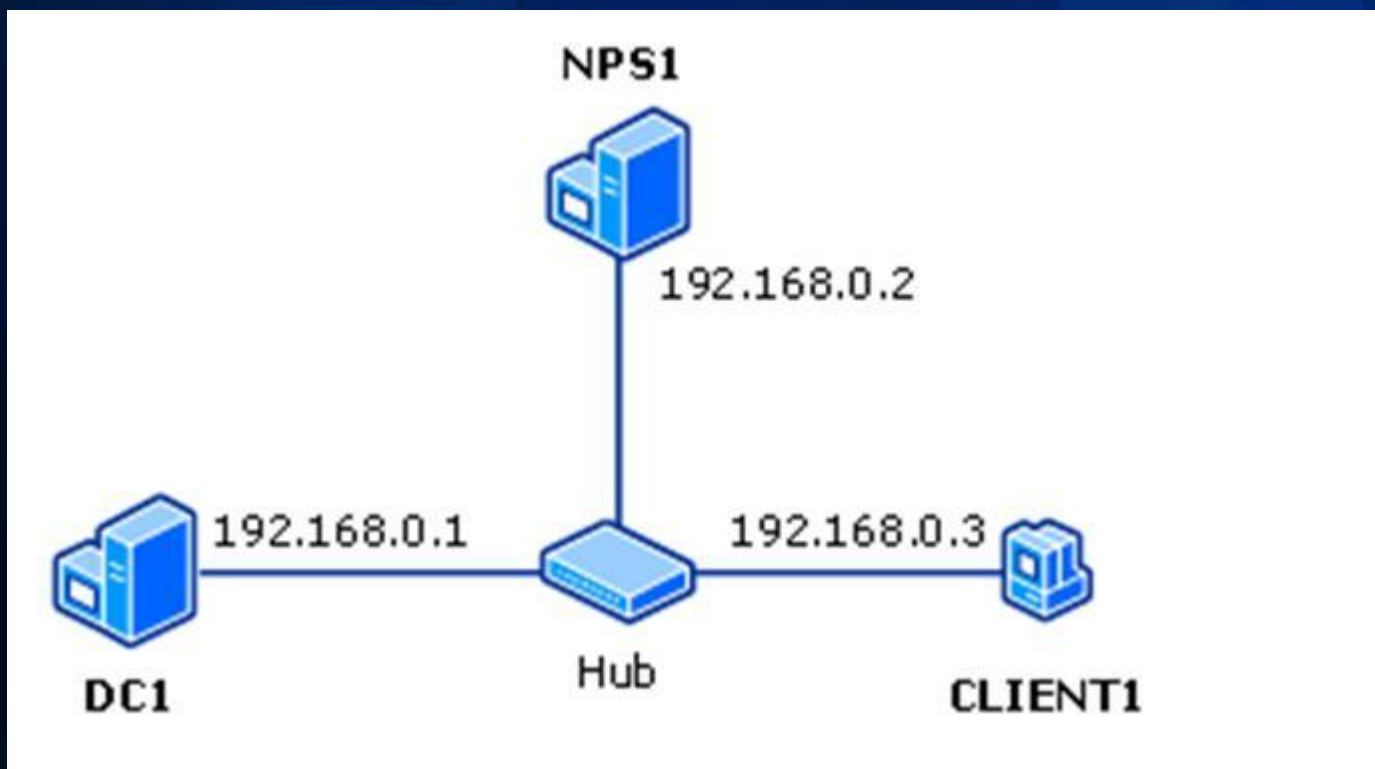
Если здоровье не соответствует политикам, клиент получает уведомление и может перейти в карантинную сеть или к серверу восстановления. Если клиент соответствует политике, он может получить доступ к основной сети. Сервер восстановления предоставляет информацию о состоянии здоровья Network Policy Server (NPS) департаментом ИТ скачать обновления, настройки, сигнатуры антивируса. (Повторяем шаги 1 - 4)



Network Access Protection

ДЕМОНСТРАЦИЯ

Архитектура нашего примера NAP



Что такое NPS?

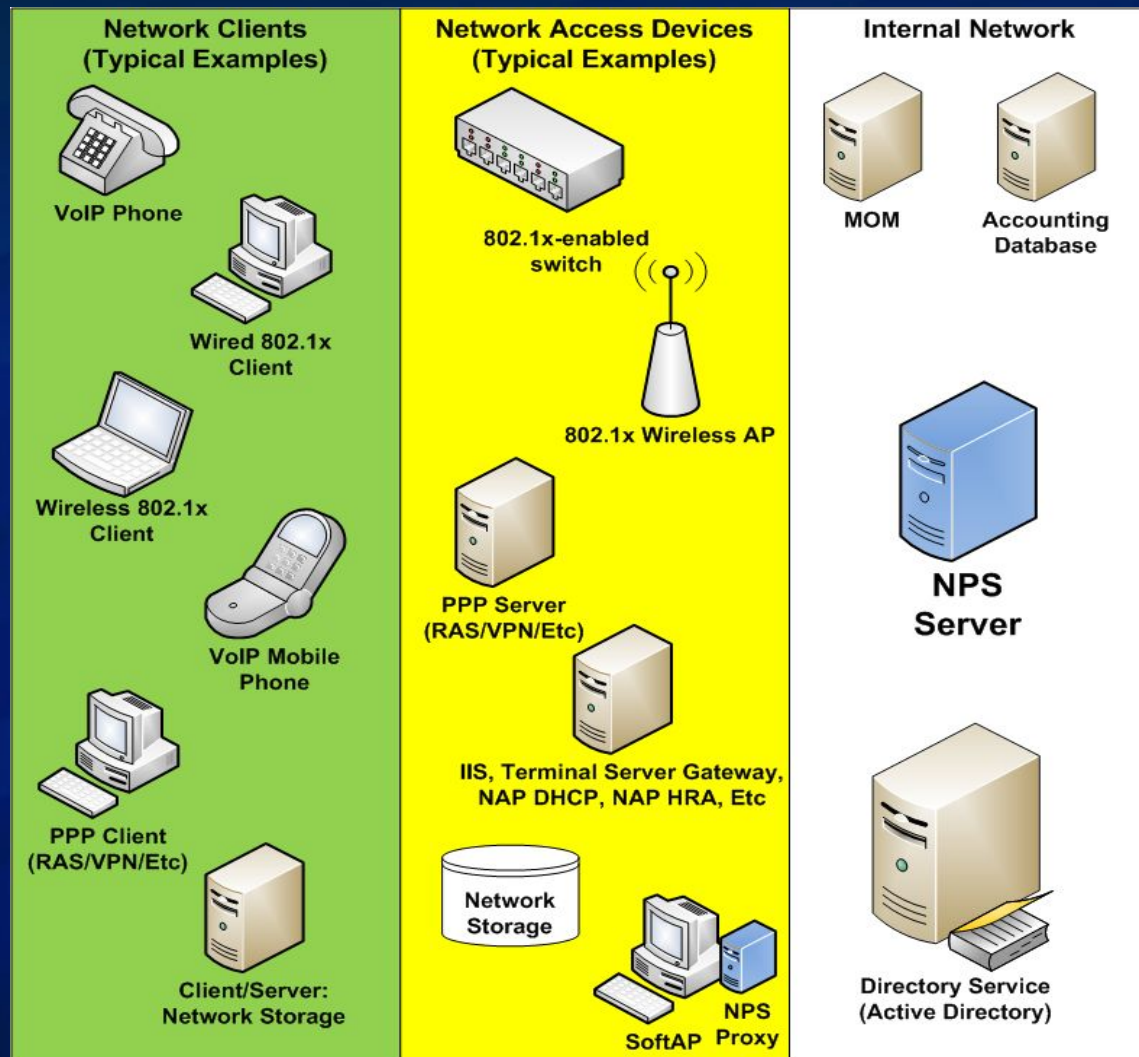
- Network Policy Server новая версия Internet Authentication Services (IAS)
- NPS это реализация RADIUS сервера от Microsoft с поддержкой основных RFC RADIUS и EAP
- NPS работает только на платформе Windows Server 2008

Преимущества NPS

- NPS в соединении с AD и Windows Vista и позволяет предоставлять удобный доступ к сетям и сервисам (single sign-on)
- NPS объединяет в одной точке отчетность и управление доступом для всех способов (802.1x, VPN, DHCP...)
- Определение и принудительное исполнение политик здоровья клиентов

Методы использования NPS

- Аутентификация доступа в сеть
 - 802.1x
 - VPN
 - IPSec
 - NAP
- Определение и принудительное исполнение политик
- Учет доступа в сеть
- Хранение настроек устройств используемых для доступа в сеть
- Прозрачное перенаправление запросов аутентификации в AD



Дополнительная информация NAP

- **Официальная документация**
<http://www.microsoft.com/nap>
- **NAP BLOG**
<http://blogs.technet.com/nap/>
- **NAP Technet Forum**
<http://forums.microsoft.com/TechNet/ShowForum.aspx?ForumID=576&SiteID=17>
- **Channel 9 Interview**
<http://channel9.msdn.com/Showpost.aspx?postid=347154>



ВОПРОСЫ?

Бешков Андрей

Microsoft

abeshkov@microsoft.com

<http://blogs.technet.com/abeshkov/>

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.

