Обеспечение безопасности серверов, сети и рабочих станций

Семинары TechNet. Осень 2007

Краснодар, Казань, Новосибирск, Санкт-Петербург, Самара, Екатеринбург, Ростов-на-Дону, Н. Новгород, Владивосток, Хабаровск

Microsoft TechNet

Windows Resource Protection -(WRP)

Windows Resource Protection (WRP)

- Во время установки ПО инсталлятор системы Windows Vista не позволяет изменять файлы и папки защищенные Windows Resource Protection (WRP).
- Случайное или намеренное удаление защищенных объектов затруднено.
- Window Resource Protection (WRP) может защищать ключи реестра.

Типы защищаемых файлов:

.acm, .ade, .adp, .app, .asa, .asp, .aspx, .ax, .bas, .bat, .bin, .cer, .chm, .clb, .cmd, .cnt, .cnv, .com, .cpl, .cpx, .crt, .csh, .dll, .drv, .dtd, .exe, .fxp, .grp, .h1s, .hlp, .hta, .ime, .inf, .ins, .isp, .its, .js, .jse, .ksh, .lnk, .mad, .maf, .mag, .mam, .man, .maq, .mar, .mas, .mat, .mau, .mav, .maw, .mda, .mdb, .mde, .mdt, .mdw, .mdz, .msc, .msi, .msp, .mst, .mui, .nls, .ocx, .ops, .pal, .pcd, .pif, .prf, .prg, .pst, .reg, .scf, .scr, .sct, .shb, .shs, .sys, .tlb, .tsp, .url, .vb, .vbe, .vbs, .vsmacros, .vss, .vst, .vsw, .ws, .wsc, .wsf, .wsh, .xsd, and .xsl.

Windows Resource Protection (WRP)

WRP сохраняет файлы необходимые для запуска Windows в кэш папку %Windir%\winsxs\Backup.

Прочие защищаемые файлы хранятся в %systemroot%\system32\dllcache

Windows Resource Protection (WRP)

Типы защищаемых файлов:

.acm, .ade, .adp, .app, .asa, .asp, .aspx, .ax, .bas, .bat, .bin, .cer, .chm, .clb, .cmd, .cnt, .cnv, .com, .cpl, .cpx, .crt, .csh, .dll, .drv, .dtd, .exe, .fxp, .grp, .h1s, .hlp, .hta, .ime, .inf, .ins, .isp, .its, .js, .jse, .ksh, .lnk, .mad, .maf, .mag, .mam, .man, .maq, .mar, .mas, .mat, .mau, .mav, .maw, .mda, .mdb, .mde, .mdt, .mdw, .mdz, .msc, .msi, .msp, .mst, .mui, .nls, .ocx, .ops, .pal, .pcd, .pif, .prf, .prg, .pst, .reg, .scf, .scr, .sct, .shb, .shs, .sys, .tlb, .tsp, .url, .vb, .vbe, .vbs, .vsmacros, .vss, .vst, .vsw, .ws, .wsc, .wsf, .wsh, .xsd, and .xsl.

Windows Resource Protection (WRP)

В случае неавторизованной замены файла Windows восстанавливает его из следующих источников:

- Кэш папки
- Сетевой путь к дистрибутиву
- Windows CD-ROM

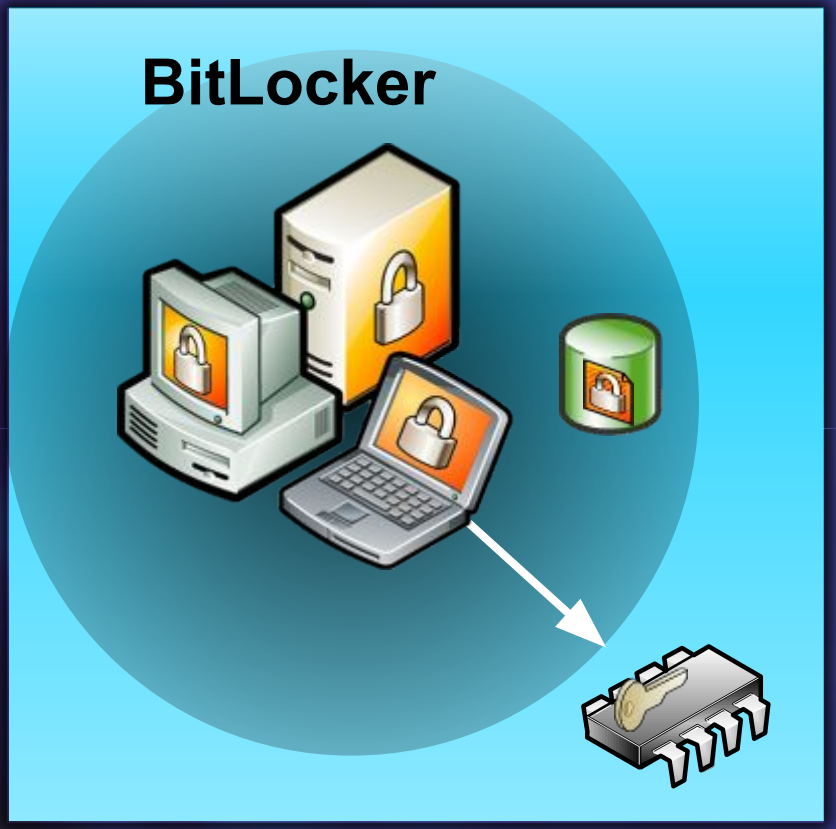
Windows Resource Protection (WRP)

Windows Resource Protection (WRP)

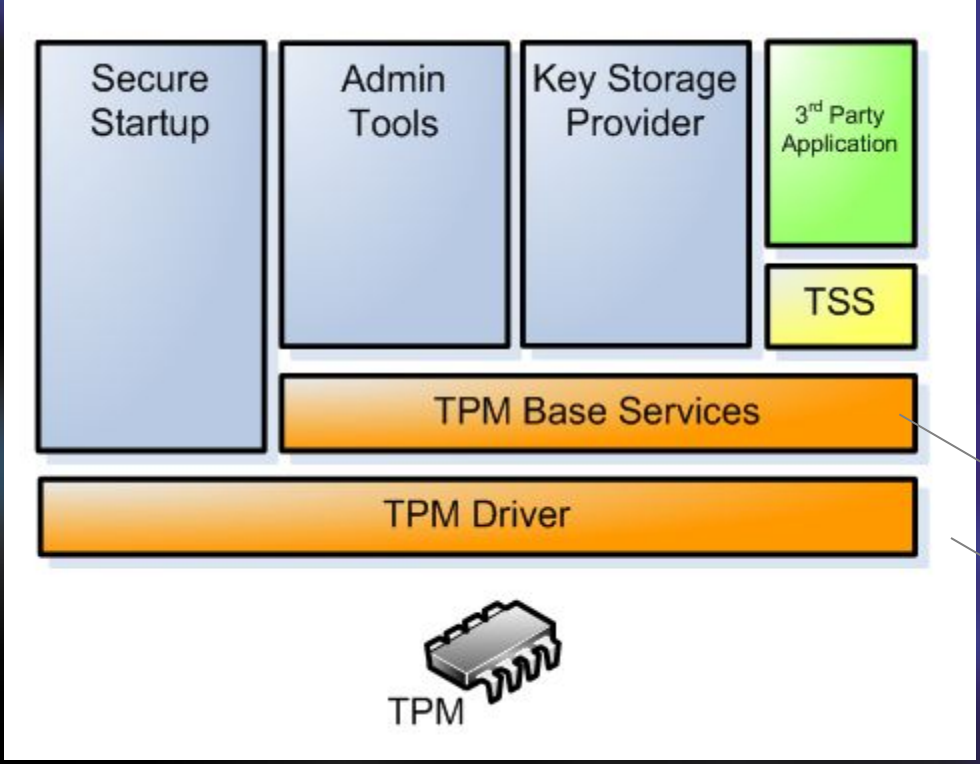
Защита ОС и данных с помощью BitLocker.....

Шифрование дисков с помощью BitLocker™

- Защищает от неавторизованого доступа к данным
- Предназначен для защиты от физической кражи систем
- Позволяет выполнять защищенный старт системы
- Использует TPM или USB диск для хранения ключей



Архитектура TPM



- Оранжевые – сервисы TPM
- Голубые – сервисы Microsoft
- Желтые и зеленые – сервисы сторонних производителей

NT Сервис

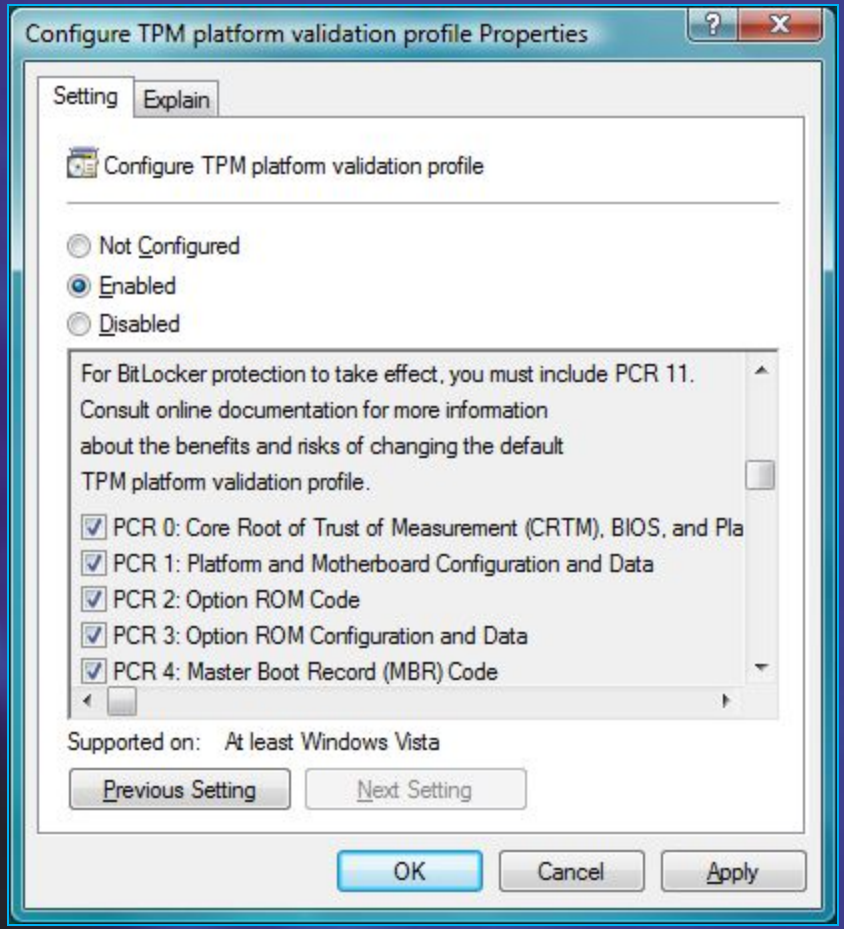
Режим ядра (Kernel Mode)

BitLocker™ и TPM

- Шифрование диска BitLocker™
  - Шифрует полностью том
  - Использует Trusted Platform Module (TPM) v1.2 для проверки pre-OS компонентов
  - Настраиваемые методы защиты и аутентификации
- Защита до запуска ОС
  - USB ключи, PIN, TPM аутентификация
- Единый драйвер TPM от Microsoft
  - Улучшеная стабильность и безопасость
- TPM Base Services (TBS)
  - Позволяет включать в цепочку приложение от сторонних поставщиков
- Active Directory Backup
  - Автоматизированное резервное копирование ключей в AD
  - Поддержка групповых политик
- Скриптовые интерфейсы
  - Управление TPM
  - Управление BitLocker™
  - Инструменты коммандной строки

Варианты применения BitLocker

Policy setting	Description	Windows Vista default
Turn on BitLocker backup to Active Directory Domain Services	Enables the backup of BitLocker recovery information in Active Directory. This recovery information includes the recovery password and some unique identifier data.	Not configured
Control Panel Setup: Configure recovery folder	Configures whether the BitLocker setup wizard asks the user to save the recovery key to a folder. Specifies the default path that displays when the BitLocker Setup Wizard prompts the user to type the location of a folder in which to save the recovery key.	Not configured
Control Panel Setup: Configure recovery options	Configures whether the BitLocker Setup Wizard asks the user to create a recovery password. The recovery password is a randomly generated 48-digit sequence.	Not configured
Control Panel Setup: Enable advanced startup options	Configures whether the BitLocker Setup Wizard asks the user to create a PIN on the computer. The PIN is a 4–20 digit sequence that the user types each time the computer starts. You cannot use policy to set the number of digits.	Not configured
Configure encryption method	Configures the encryption algorithm and key size that BitLocker uses. This policy setting applies to a fully decrypted disk. If the disk is already encrypted or if encryption is in progress, changing the encryption method has no effect.	Not configured
Configure TPM platform validation profile	Configures how the TPM secures the disk volume's encryption key. This policy setting does not apply if the computer does not have a compatible TPM, nor does changing this policy affect existing copies of the encryption key.	Not configured



Требования BitLocker

- Аппаратное обеспечение Trusted Platform Module
  - TPM не ниже версии 1.2
  - Иметь логотип Vista certified
- Не совместимое с TPM оборудование
  - BIOS должен поддерживать загрузку с USB включая считывание данных с USB до загрузки ОС.

Bitlocker - шифрование

Не шифруются:

- загрузочный сектор
- поврежденные сектора, отмеченные как нечитаемые
- метаданные тома
  - состоят из трех избыточных копий данных, включая статистическую информацию о томе
  - защищенные копии некоторых ключей расшифровки*

*Эти элементы не требуют шифрования, поскольку не являются уникальными, ценными или позволяющими определить личность.

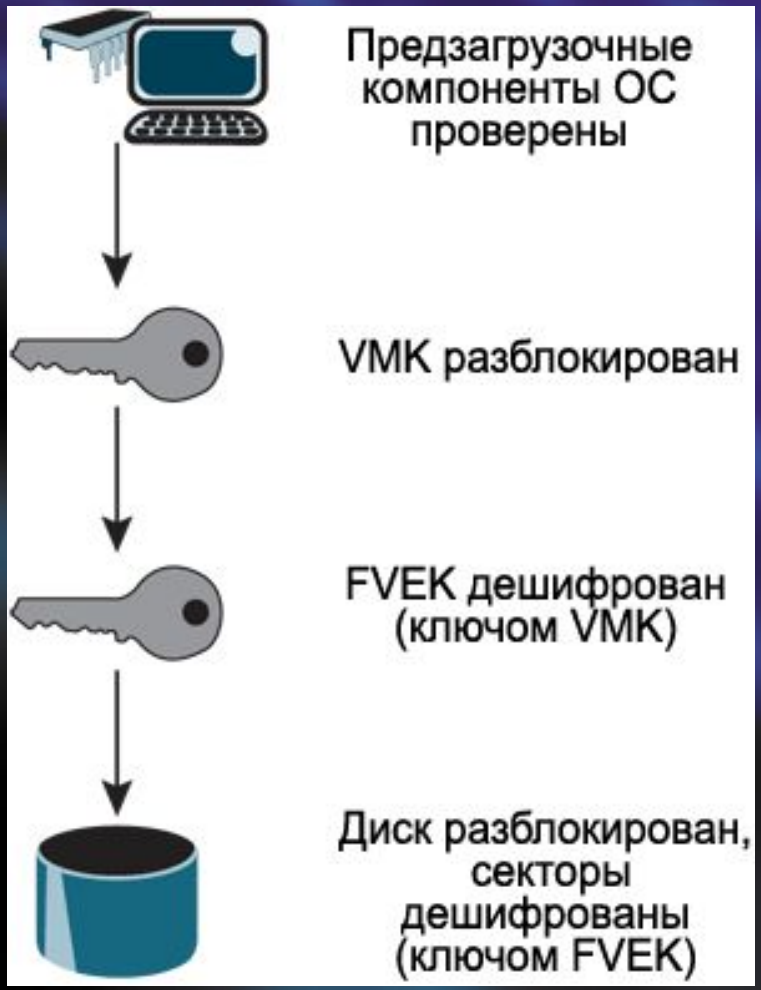
Bitlocker - шифрование

- Используется алгоритм AES с ключом 128 бит. Возможно увеличение длины ключа до 256 бит с помощью GPO или WMI.

- Каждый сектор тома шифруется отдельно, при этом часть ключа шифрования определяется номером этого сектора. В результате два сектора, содержащие одинаковые незашифрованные данные, будут в зашифрованном виде выглядеть по-разному.

- Перед шифрованием данных используется алгоритм, называемый диффузором (diffuser). В результате его применения любое мельчайшее изменение исходных данных приводит к полному изменению всего сектора.

Bitlocker – процесс расшифровки

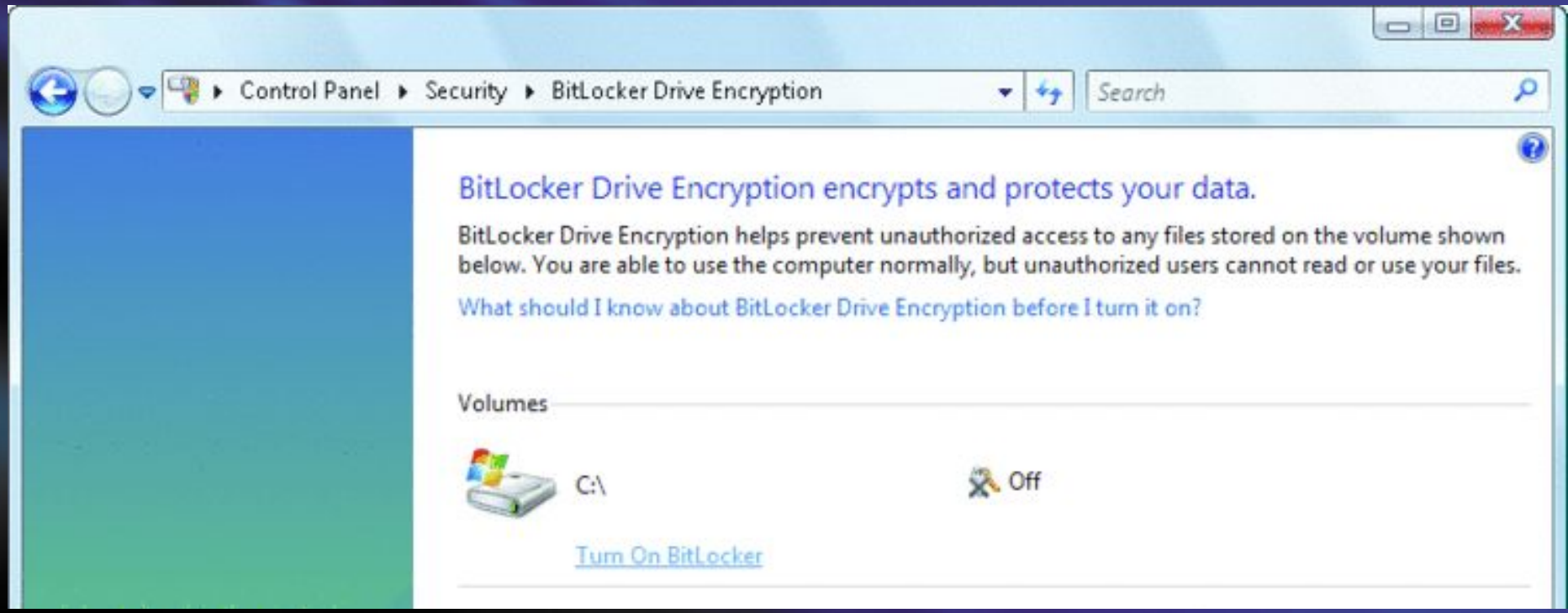


подсчитывает контрольные суммы и сравнивает с эталонными

(volume master key, VMK) – мастер ключ тома разблокируется контрольной суммой предзагрузочных компонентов

(full-volume encryption key, FVEK) – ключ тома защифрован VMK. Пользователи доступа к ключу FVEK не имеют и он никогда не попадает на диск в расшифрованном виде

Bitlocker - настройка



Bitlocker - настройка

Bitlocker запуск

Bitlocker восстановление

Защита информации

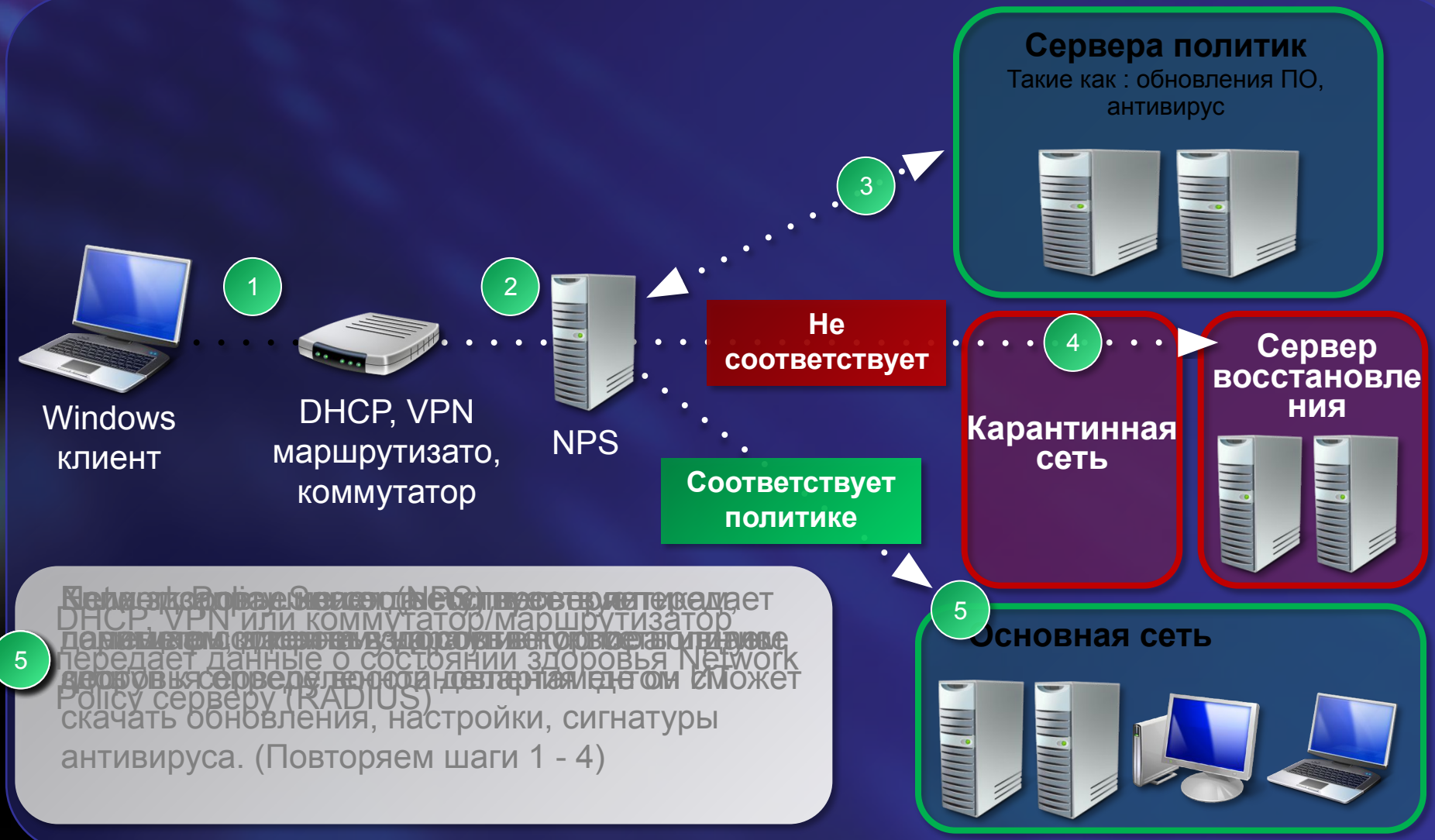
От каких угроз защищаемся?

- От пользователей и Администраторов на этом же PC? (EFS)
- Неавторизованый физический доступ? (BitLocker™)

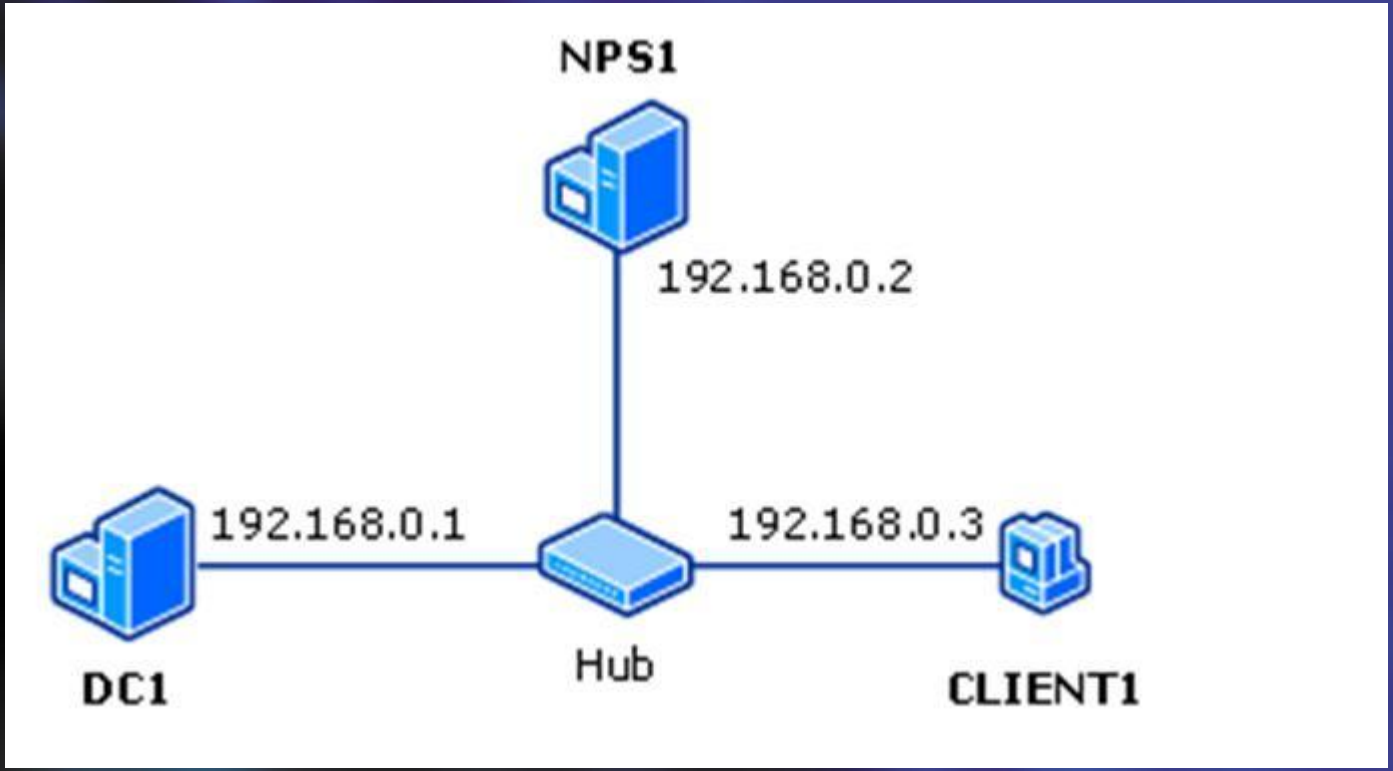
Объект	BitLocker	EFS	RMS
Ноутбук	●		
Сервер филиала	●		
Локальная защина для одного пользователя	●		
Локальная защина для нескольких пользователей		●	
Защита дистанционных файлов		●	
Недовереный администратор сети		●	
Дистанционная политика работы с документами			●

Управление здоровьем систем - Network Access Protection .....

Защита сети с помощью NAP



Архитектура нашего примера NAP



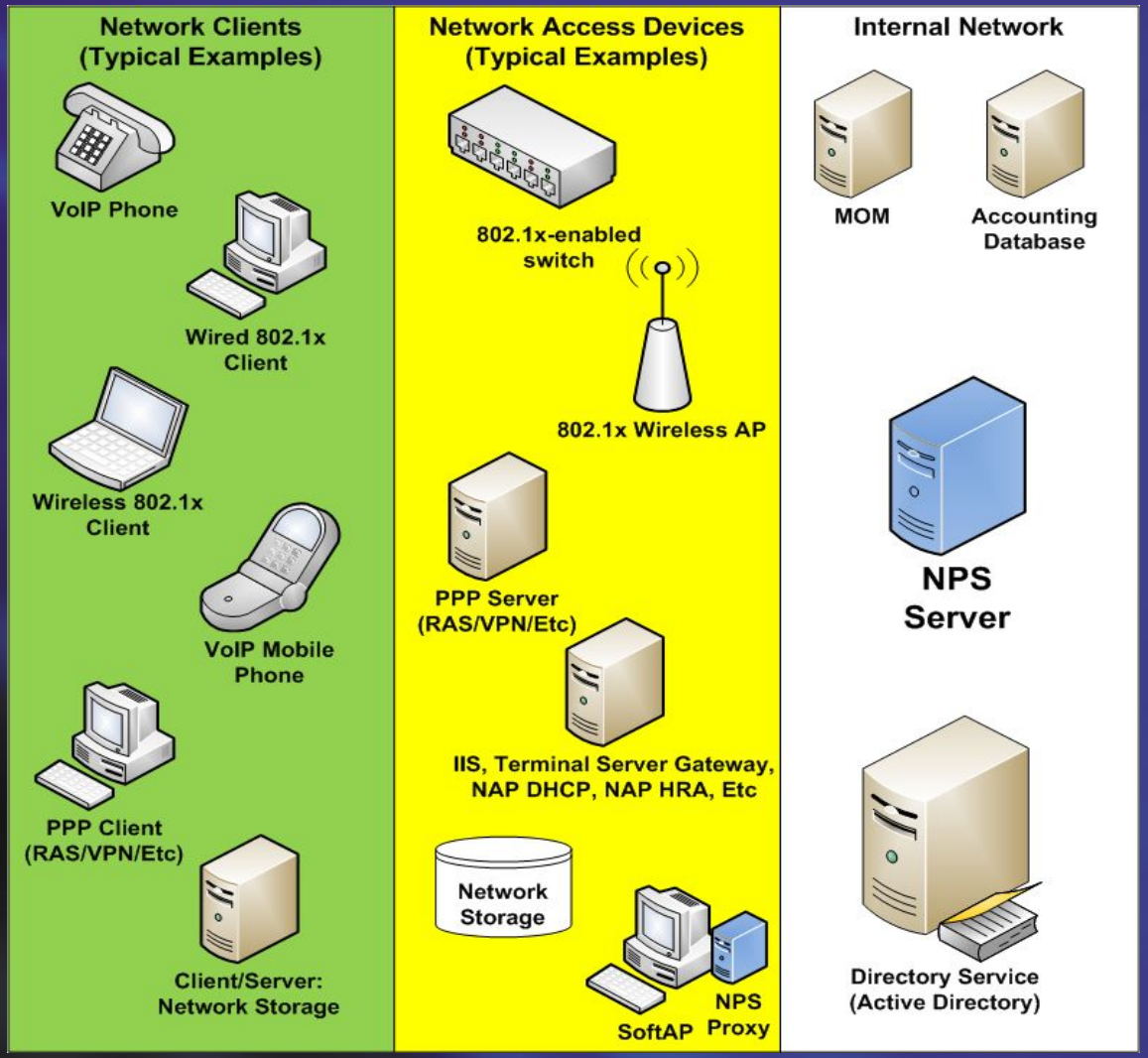
Демонстрация
Network Access Protection

Что такое NPS?

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

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



Преимущества NPS

- NPS в соединении с AD и Windows Vista 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…)

Пример работы NPS

Windows Server
Code Name "Longhorn"

Пользователь запрашивает доступ

Сетевое устойство запрашивает пароль

Устройство передает учетные данные и сведения о соединении в NPS

RADIUS проверяет данные соединения и сравнивает их с политиками; передает учетные данные в AD для аутентификации

Windows
Active Directory

Устройство разрешает доступ

Если политика совпадает, и пользователь предоставил правильные пароли

Advanced Group Policy Management - (AGPM)

Microsoft Advanced Group Policy Management

Улучшаем групповые политики с помощью управления изменениями

- Администрирование основаное на ролях и шаблонах
- Гибкая модель делегирования
- Отслеживание версий, история изменений и возвращение к предыдущей конфигурации

- Ускорение управления за счет более точного административного контроля
- Уменьшает риск глобального сбоя

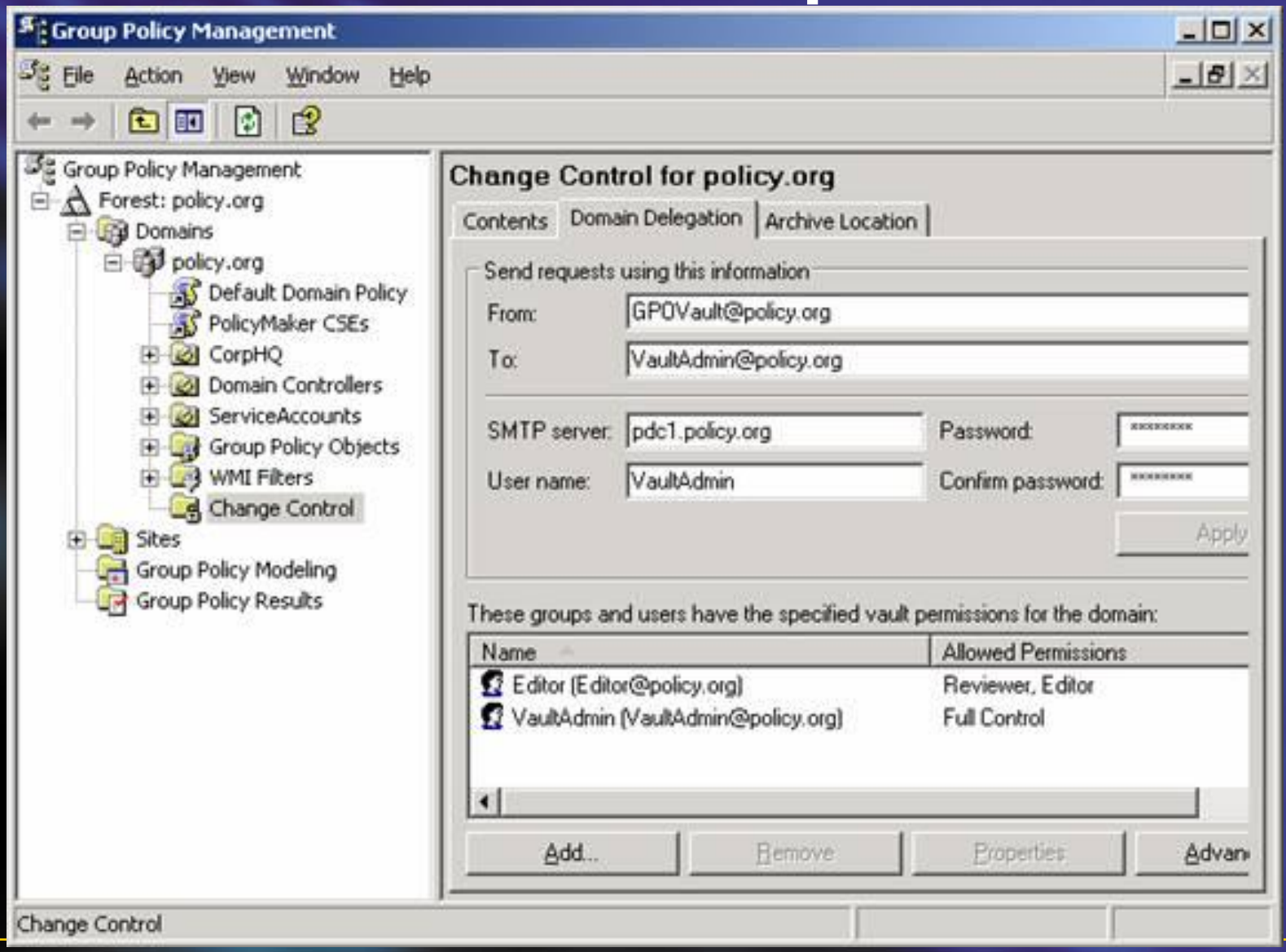
- Управляемость PC
- Диагностика и Help Desk

Advanced Group Policy Management

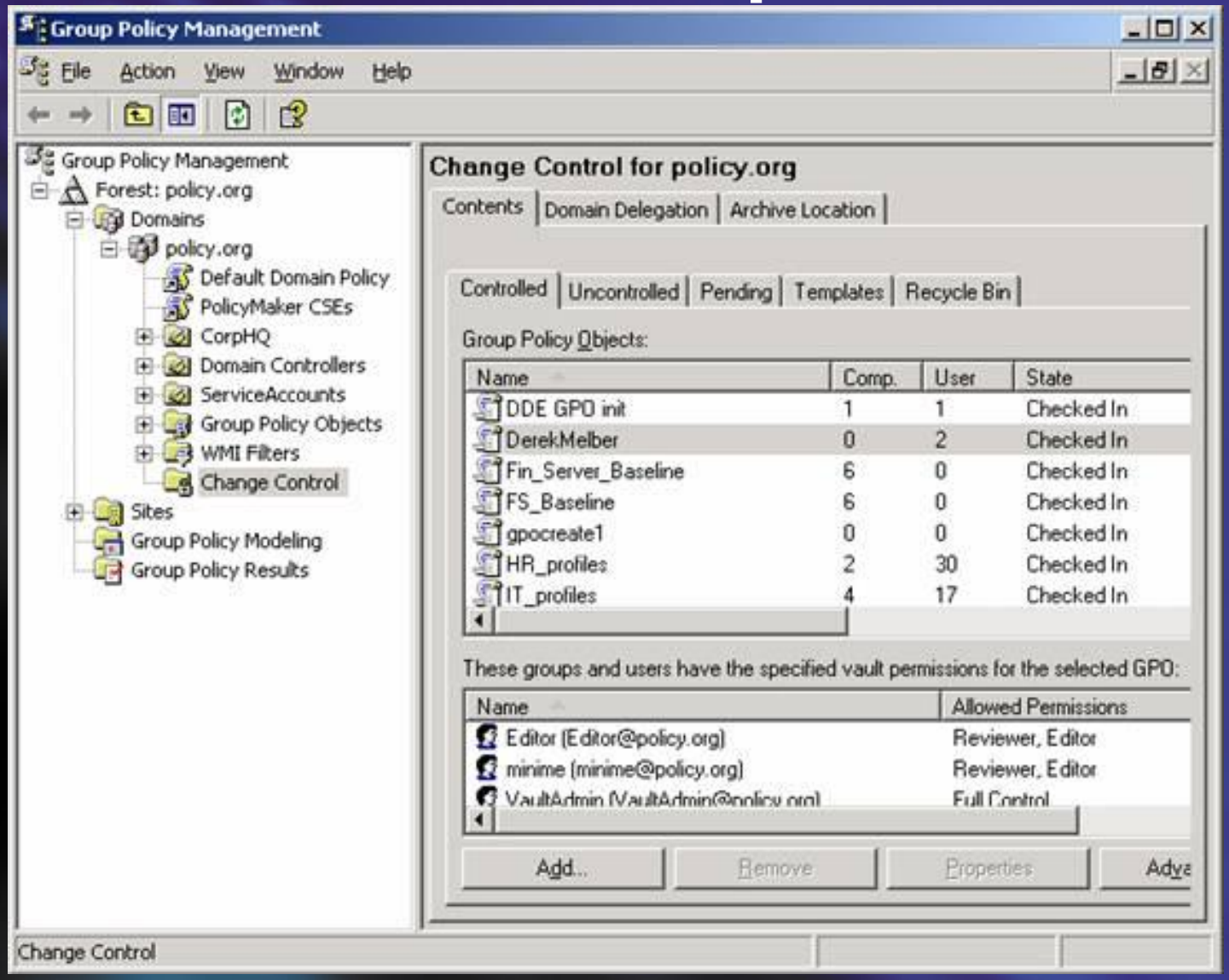
- Простота администрирования всех объектов GPO во всем лесе Active Directory
- Просмотр всех объектов GPO в одном списке
- Редактирование объектов в автономном режиме
- Отчет о настройках GPO, безопасности (security), фильтрах (filter), копировании (delegation) и т.п.
- Контроль наследования GPO inheritance с помощью Block Inheritance (блокировка наследования), Enforce (усиление) и Security Filtering (фильтры безопасности)
- Модель делегирования (Delegation model)
- Создание резервных копий объектов GPO
- Перемещение объектов GPO в различные домены и леса

AGPM – делегирование

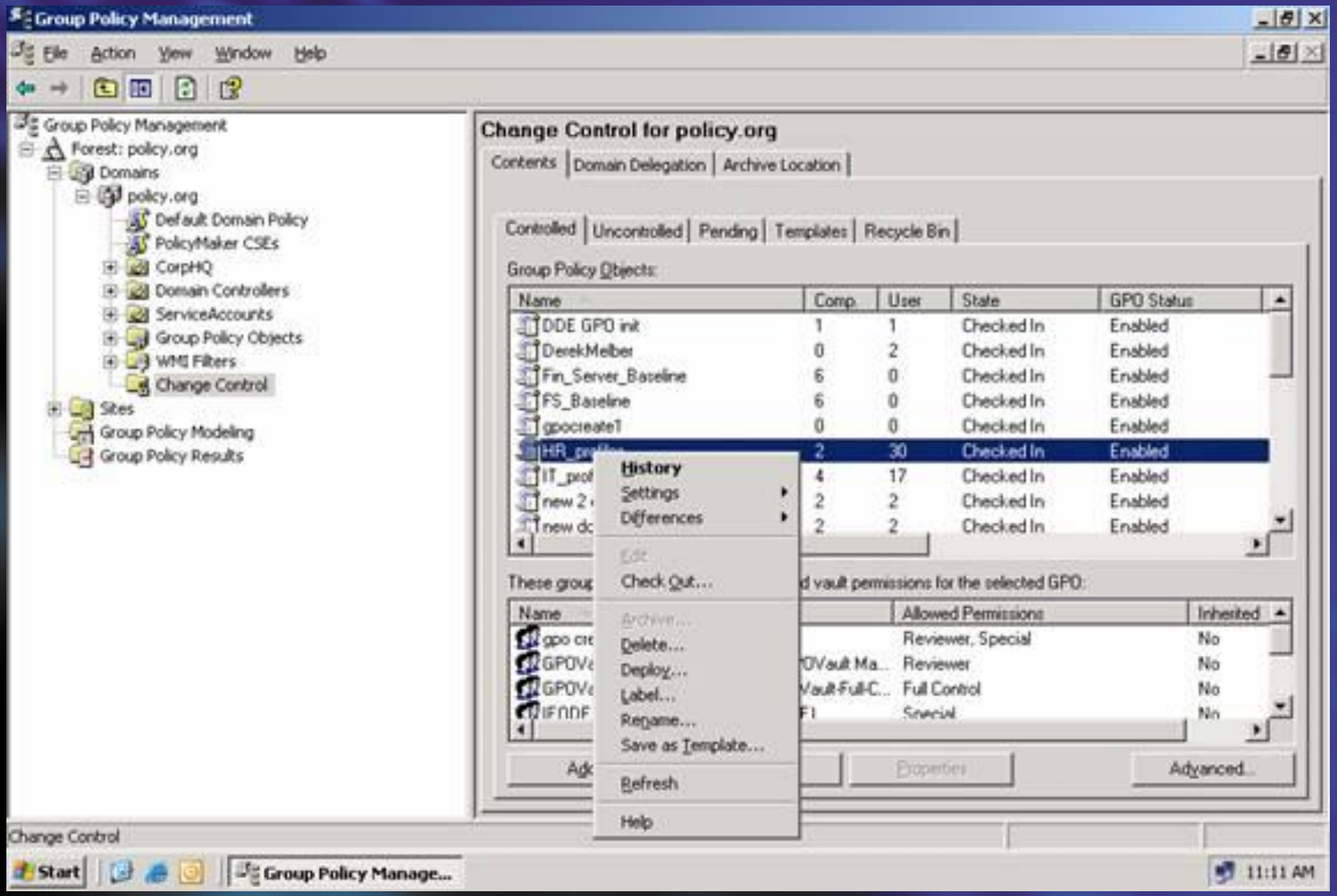
AGPM – делегирование



AGPM – делегирование



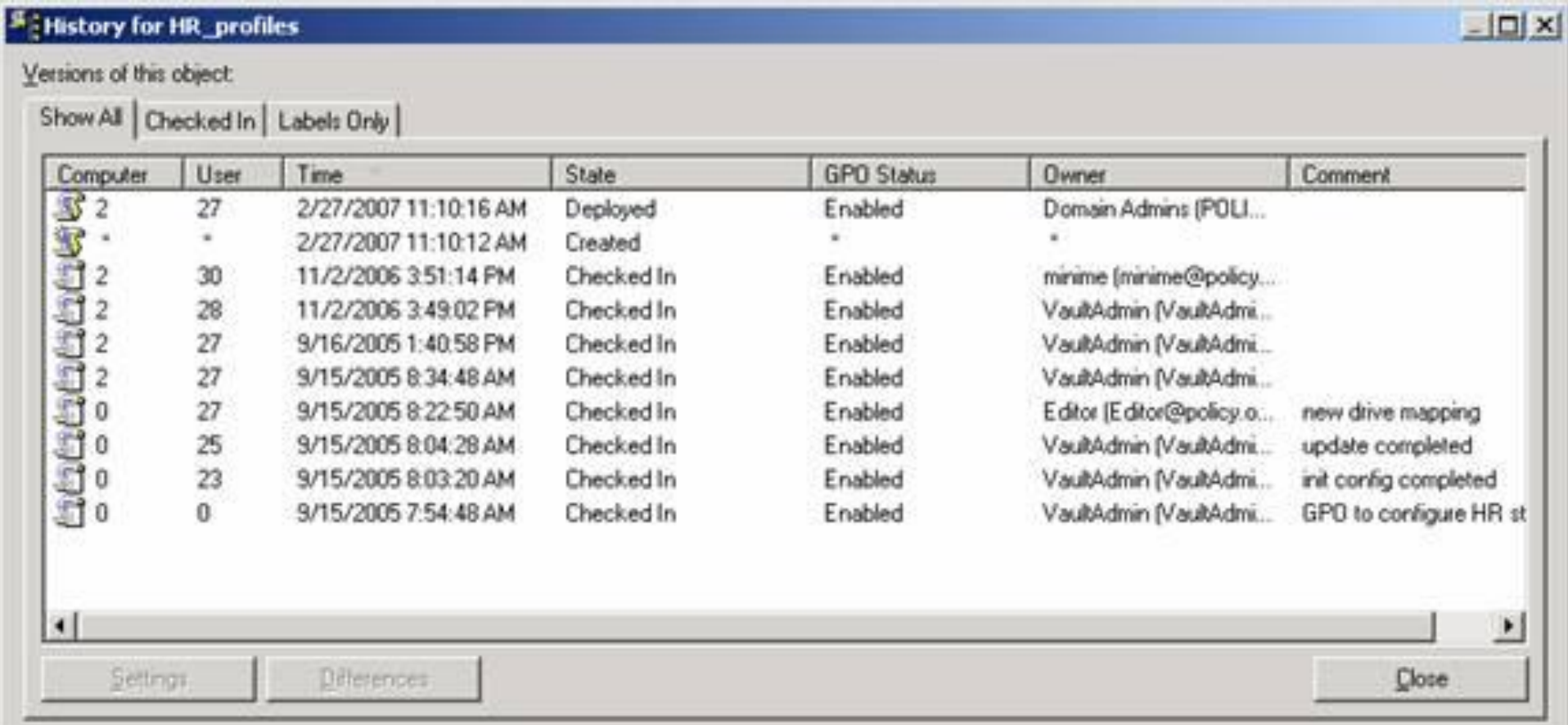
AGPM – автономное редактирование



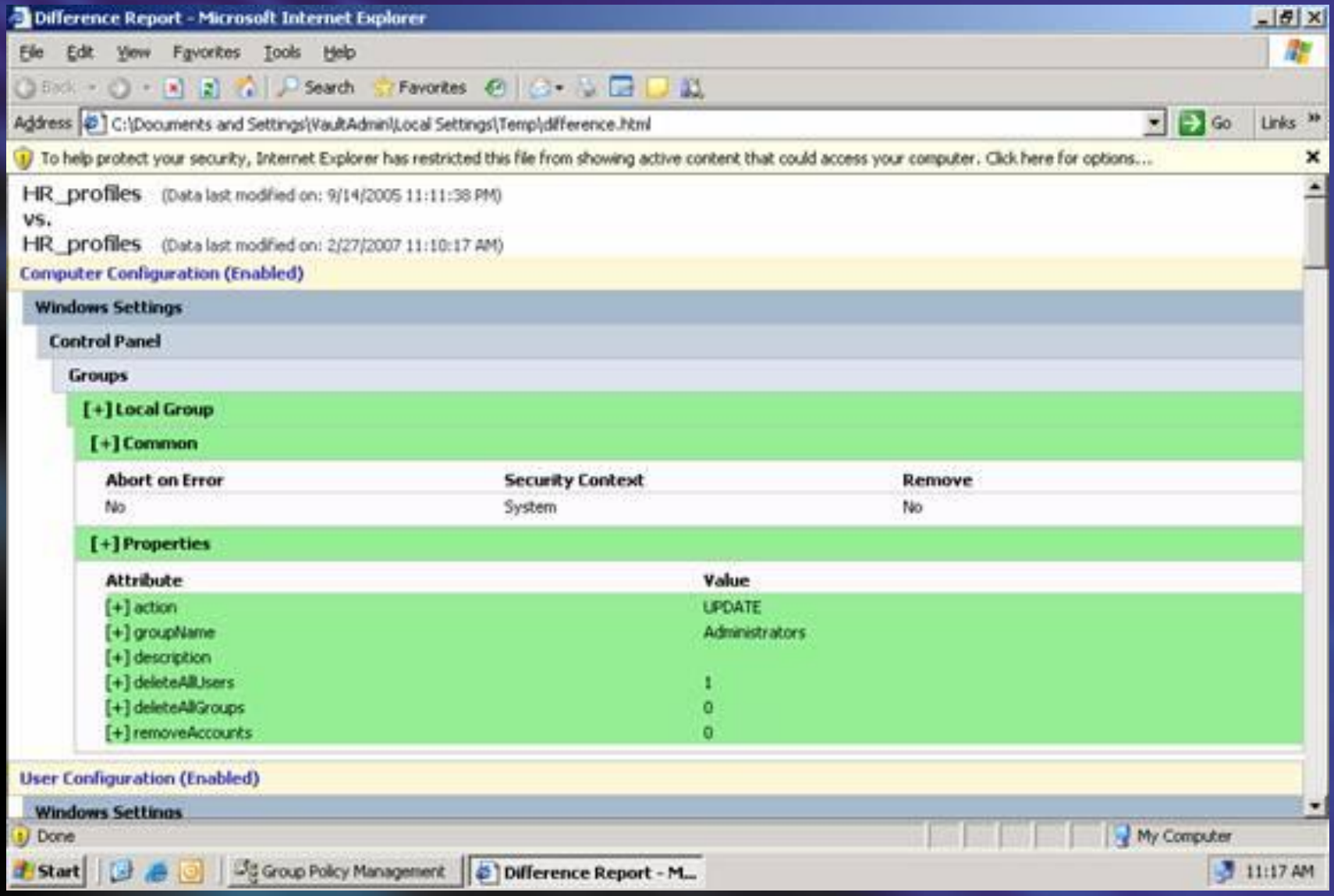
AGPM – управление изменениями

- Кто сделал изменение
- Когда было сделано изменение
- Что затронуло это изменение

AGPM – управление изменениями



AGPM – аудит изменений



Microsoft Advanced Group Policy Management

Создание и управление групповых политик, подерживающих конфигурацию рабочих мест в соответствии с последними требованиями

Проблема:

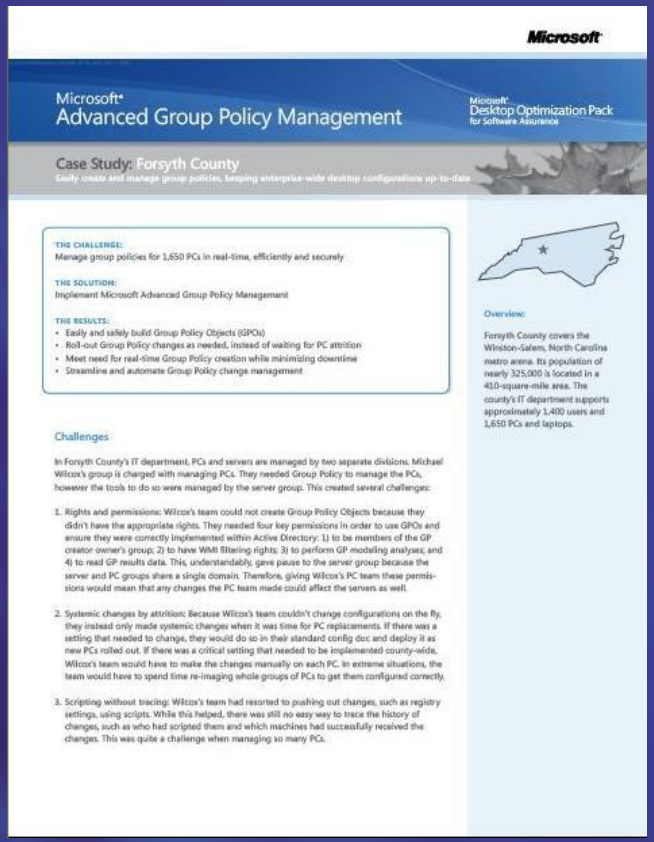
Необходимо управлять групповыми политиками 1,650 компьютеров компании Forsyth County в реальном времени, эффективно и безопасно

Результат:

- Легкость и безопасность построения объектов групповых политик
- Развертование групповых политки в нужный момент вместо ожидания замены PC из-за износа
- Применение групплвых политик в реальном времени и минимизация простоев
- Упрощение и автоматизация процесса управления изменениями групповых политик

“Advanced Group Policy для нас это серебряная пуля. Автоматизация управления изменениями и система делегирования полномочий действительно впечатляют. Я не смог бы управлять групповыми политиками без нее”.

MICHAEL WILCOX
MIS CLIENT SERVICES SUPERVISOR
FORSYTH COUNTY



Microsoft

Microsoft® Advanced Group Policy Management

Microsoft® Desktop Optimization Pack for Software Assurance

Case Study: Forsyth County

Easily create and manage group policies, keeping enterprise-wide desktop configurations up-to-date

THE CHALLENGE:
Manage group policies for 1,650 PCs in real-time, efficiently and securely

THE SOLUTION:
Implement Microsoft Advanced Group Policy Management

THE RESULTS:
- Easily and safely build Group Policy Objects (GPOs)
- Roll-out Group Policy changes as needed, instead of waiting for PC attrition
- Meet need for real-time Group Policy creation while minimizing downtime
- Streamline and automate Group Policy change management

Challenges

In Forsyth County's IT department, PCs and servers are managed by two separate divisions. Michael Wilcox's group is charged with managing PCs. They needed Group Policy to manage the PCs, however the tools to do so were managed by the server group. This created several challenges:

1. Rights and permissions: Wilcox's team could not create Group Policy Objects because they didn't have the appropriate rights. They needed four key permissions in order to use GPOs and ensure they were correctly implemented within Active Directory: 1) to be members of the GP creator owner's group; 2) to have WMI filtering rights; 3) to perform GP modeling analyses; and 4) to read GP results data. This, understandably, gave pause to the server group because the server and PC groups share a single domain. Therefore, giving Wilcox's PC team these permissions would mean that any changes the PC team made could affect the servers as well.

2. Systemic changes by attrition: Because Wilcox's team couldn't change configurations on the fly, they instead only made systemic changes when it was time for PC replacements. If there was a setting that needed to change, they would do so in their standard config doc and deploy it as new PCs rolled out. If there was a critical setting that needed to be implemented county-wide, Wilcox's team would have to make the changes manually on each PC. In extreme situations, the team would have to spend time re-imaging whole groups of PCs to get them configured correctly.

3. Scripting without tracing: Wilcox's team had resorted to pushing out changes, such as registry settings, using scripts. While this helped, there was still no easy way to trace the history of changes, such as who had scripted them and which machines had successfully received the changes. This was quite a challenge when managing so many PCs.

Overview:

Forsyth County covers the Winston-Salem, North Carolina metro area. Its population of nearly 325,000 is located in a 410-square-mile area. The county's IT department supports approximately 1,400 users and 1,650 PCs and laptops.

Дополнительная информация

Документация

- http://www.microsoft.com/windowsserver2008/
- http://msdn2.microsoft.com/en-us/library/aa382503(VS.85).aspx
- http://technet.microsoft.com/en-us/windowsvista/aa905065.aspx
- http://msdn2.microsoft.com/en-us/library/ms723891.aspx

Блоги

- http://blogs.technet.com/abeshkov/
- http://blogs.technet.com/bitlocker/
  http://blogs.technet.com/windowsserver/


Microsoft®
Your potential. Our passion.™
Microsoft TechNet