Microsoft Windows Server System

Управление распространением обновлений

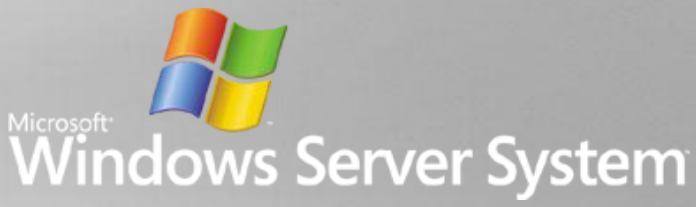
Microsoft Corporation

Владислав Кирилин
VKirilin@microsoft.com

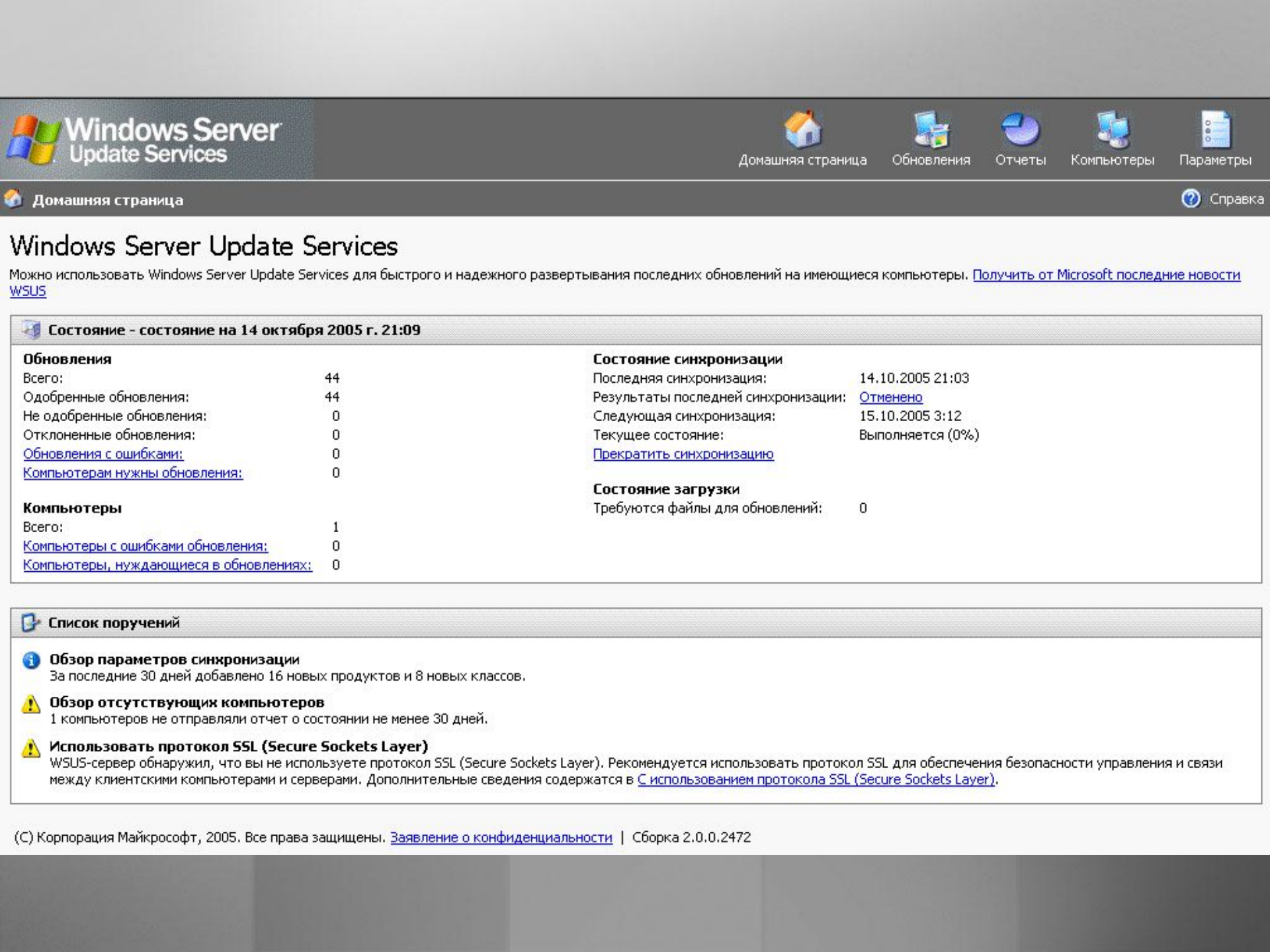
MBSA 2.0

Простейший путь проверить Вашу систему на наличие уязвимостей

- Использует различные каталоги
  - offline / WSUS / MU
- Возможно запускать несколько копий
  - сосуществует с MBSA 1.2.1
- Новые опции командной строки
  - файл со списком компьютеров
- Автоматически устанавливает WU агента



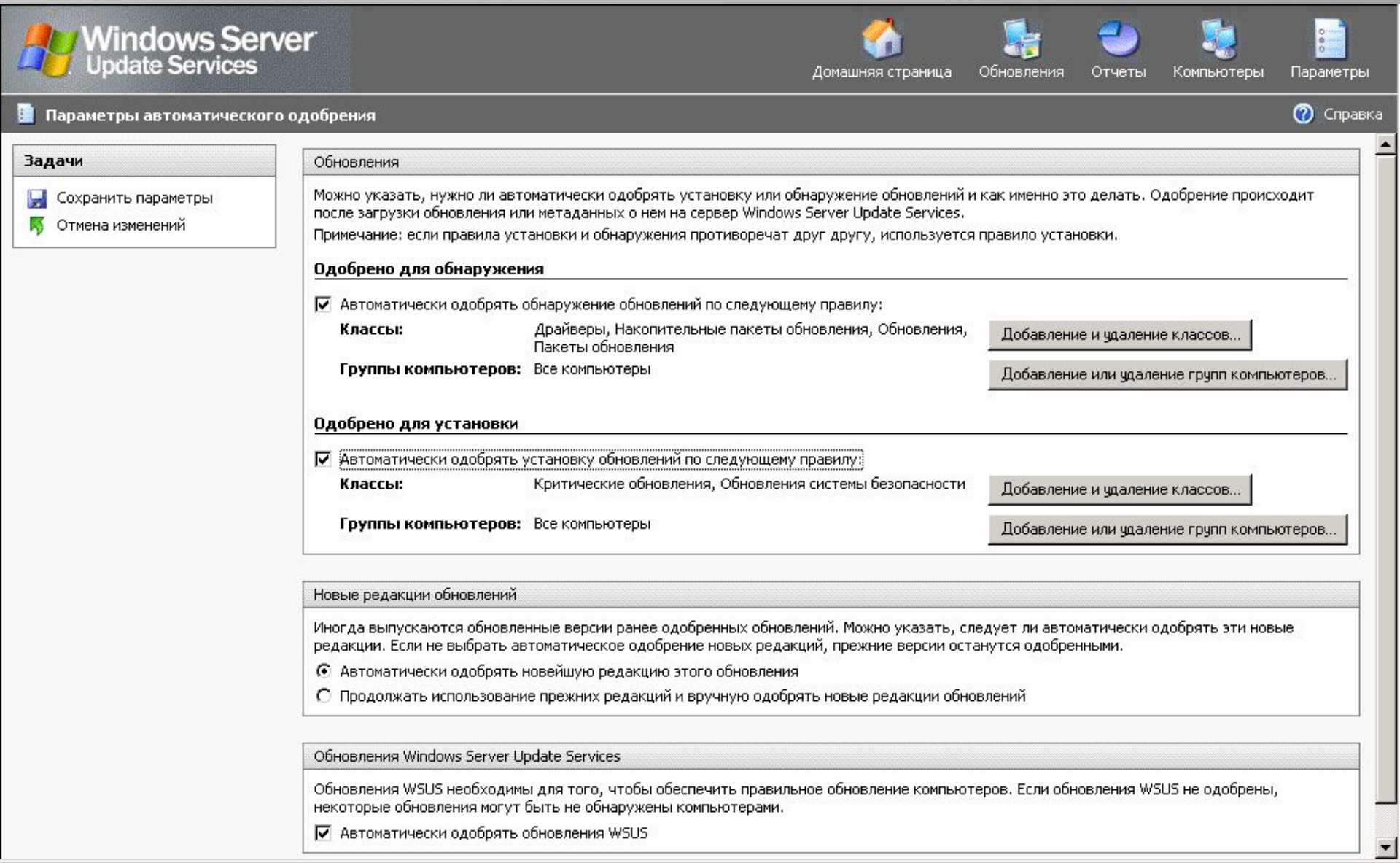
Windows Server Update Services


Windows Server Update Services
Домашняя страница
Обновления
Отчеты
Компьютеры
Параметры
Домашняя страница
Справка
Windows Server Update Services
Можно использовать Windows Server Update Services для быстрого и надежного развертывания последних обновлений на имеющиеся компьютеры. Получить от Microsoft последние новости WSUS
Состояние - состояние на 14 октября 2005 г. 21:09
Обновления
Всего: 44
Одобренные обновления: 44
Не одобренные обновления: 0
Отклоненные обновления: 0
Обновления с ошибками: 0
Компьютерам нужны обновления: 0
Компьютеры
Всего: 1
Компьютеры с ошибками обновления: 0
Компьютеры, нуждающиеся в обновлениях: 0
Состояние синхронизации
Последняя синхронизация: 14.10.2005 21:03
Результаты последней синхронизации: Отменено
Следующая синхронизация: 15.10.2005 3:12
Текущее состояние: Выполняется (0%)
Прекратить синхронизацию
Состояние загрузки
Требуются файлы для обновлений: 0
Список поручений
Обзор параметров синхронизации
За последние 30 дней добавлено 16 новых продуктов и 8 новых классов.
Обзор отсутствующих компьютеров
1 компьютеров не отправляли отчет о состоянии не менее 30 дней.
Использовать протокол SSL (Secure Sockets Layer)
WSUS-сервер обнаружил, что вы не используете протокол SSL (Secure Sockets Layer). Рекомендуется использовать протокол SSL для обеспечения безопасности управления и связи между клиентскими компьютерами и серверами. Дополнительные сведения содержатся в С использованием протокола SSL (Secure Sockets Layer).
(C) Корпорация Майкрософт, 2005. Все права защищены. Заявление о конфиденциальности | Сборка 2.0.0.2472

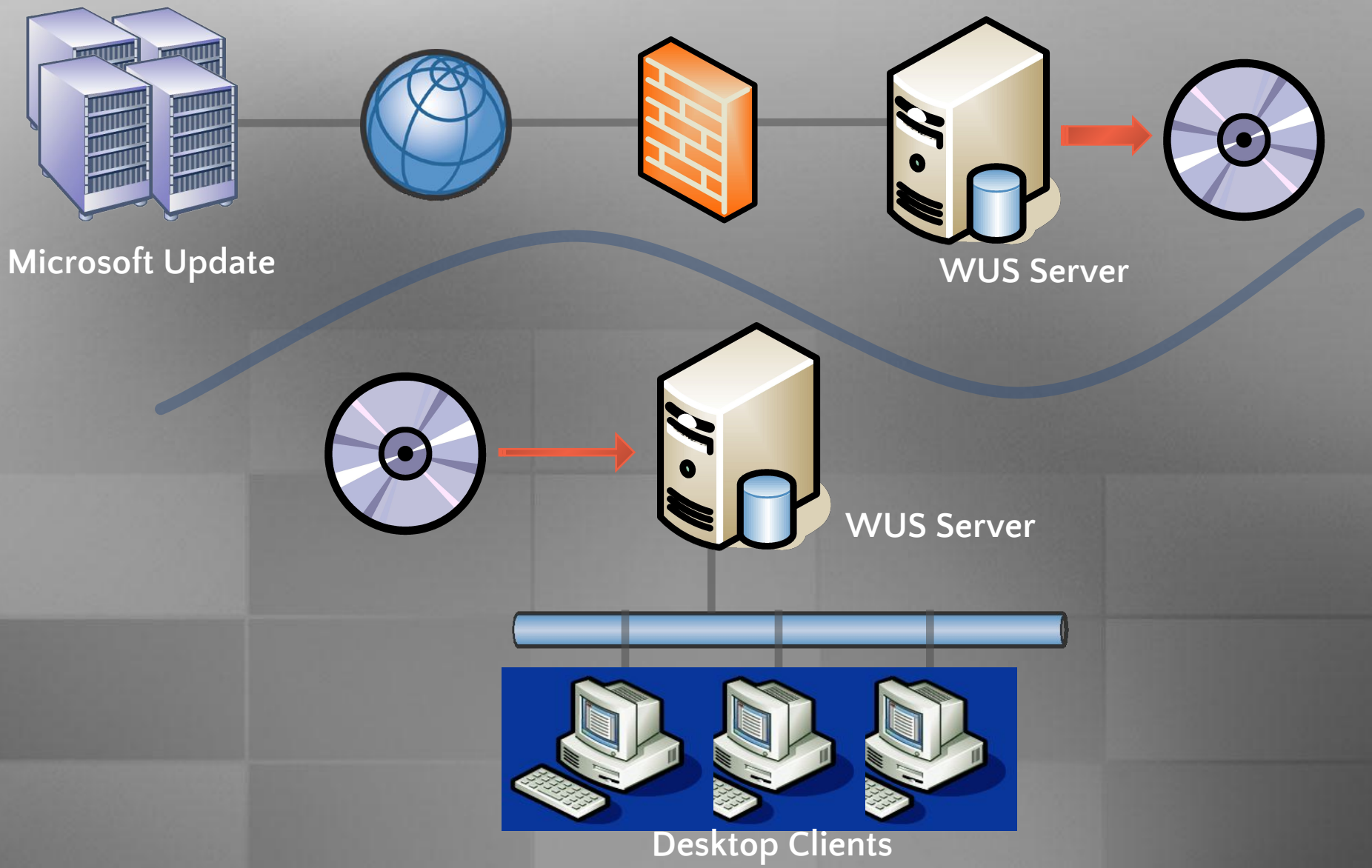
WSUS – клиенты и данные

- Server
  - Windows 2000.SP4 Server
  - Windows Server 2003 Standard / Enterprise
- Client
  - Windows 2000.SP3+ – Server, Professional
  - Windows XP+ – Home, Professional, Embedded
  - Windows Server 2003+ – 32-bit, x64 (SP1), ia64 (SP1)
- Content
  - Windows 2000+, Office XP / 2003
  - SQL / MSDE 2000, Exchange 2003
  - В последствии будет добавлена поддержка всех остальных продуктов
- International
  - Все языки, которые поддерживает Windows

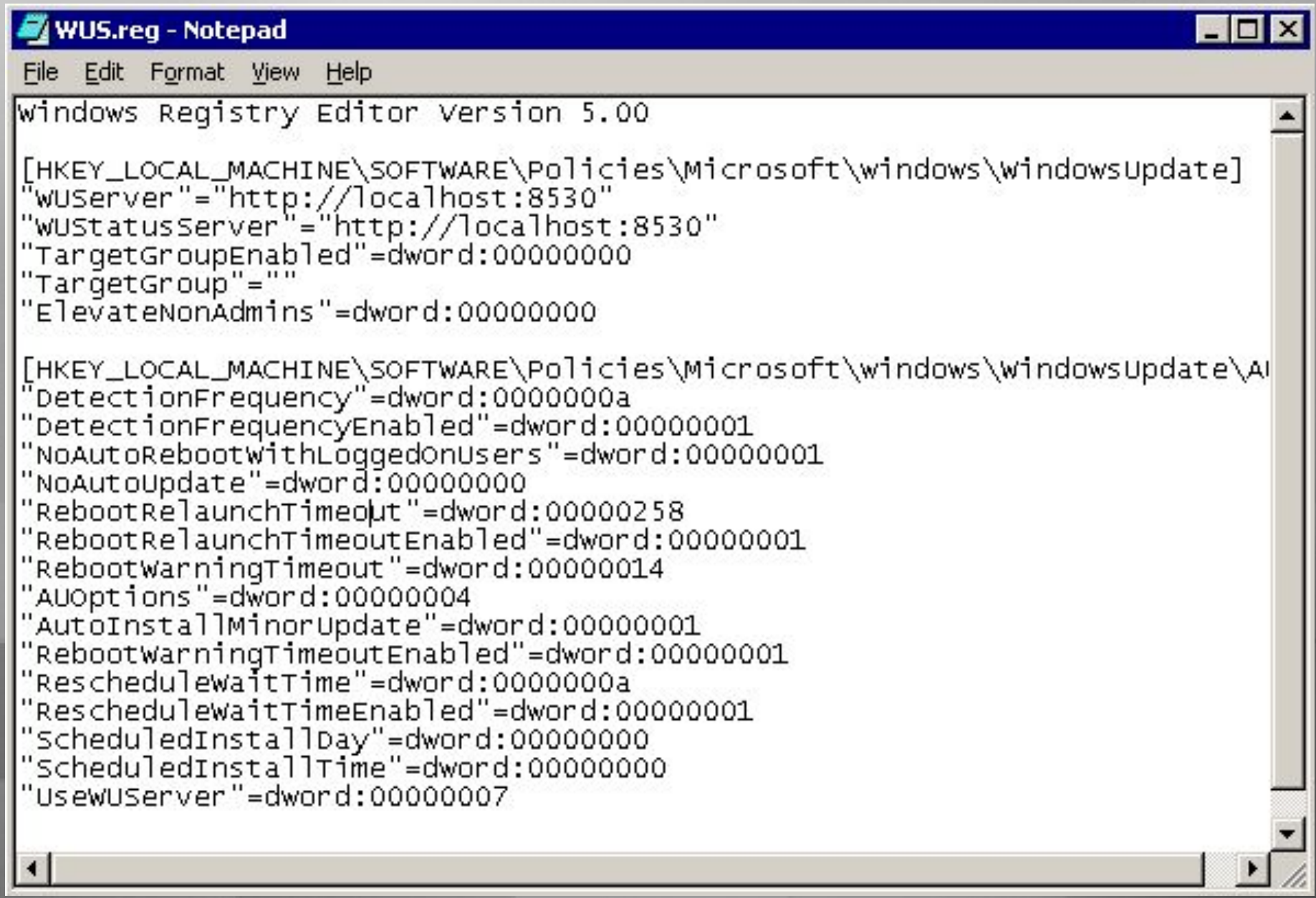
WSUS – возможности



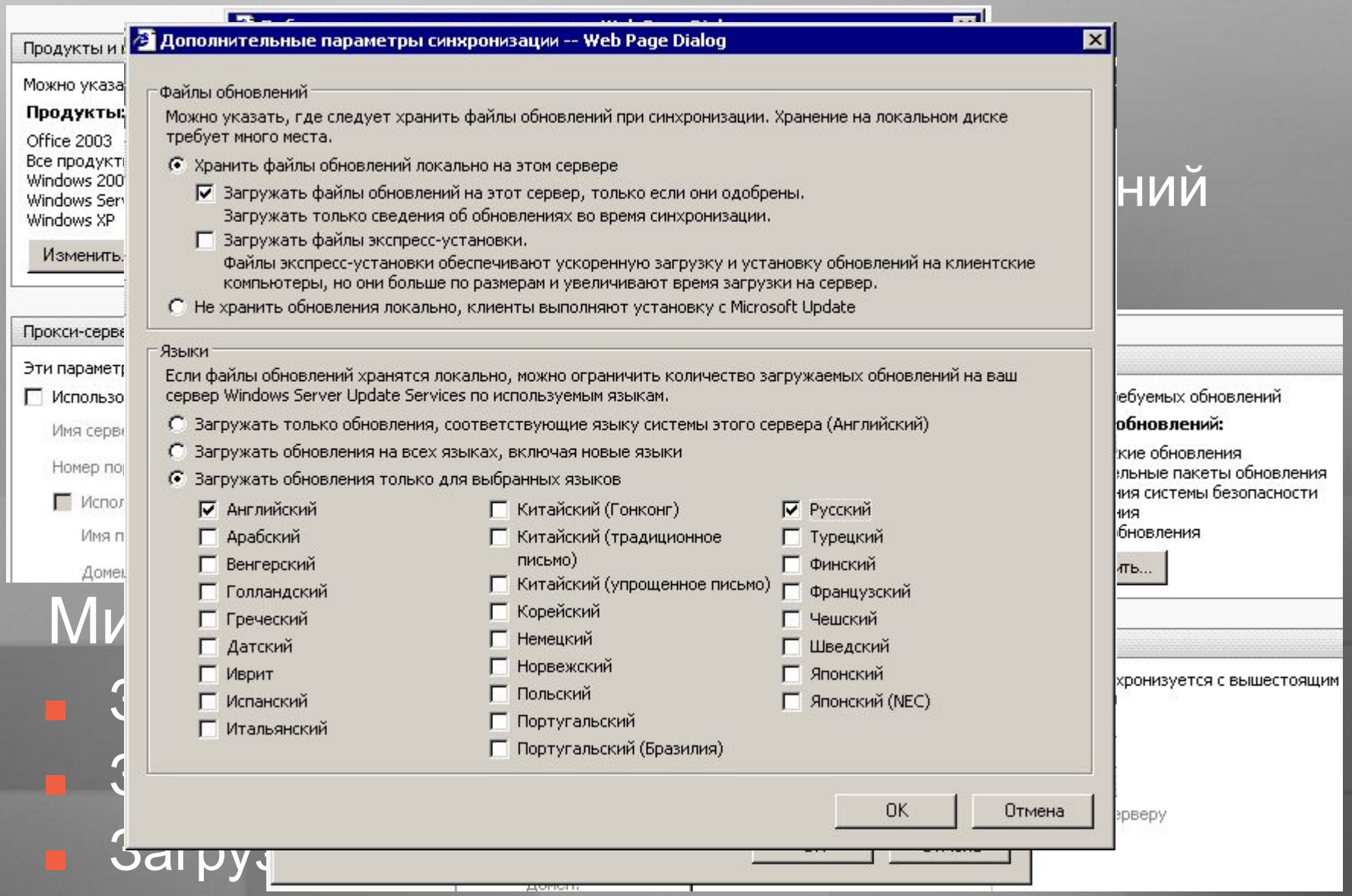
WSUS – disconnected servers



WUS – возможности клиента



WUS – оптимизация трафика



- Ми
  - З
  - З
  - Загру

WSUS – отчётность

Status of Updates for: CRAIGMA-2 Generated: 11/8/2004 10:31 PM

Computer group: All Computers
Approved for: Install

Title	Installed	Needed	Failed	Last Updated
329170: Security Update (Windows 2000)	0	18	0	11/5/2004 8:57 AM
329170: Security Update (Windows XP 64-bit Edition)	0	18	0	11/5/2004 7:04 AM

Computer Group	Approval	Deadline	Installed	Needed	Failed
All Computers	Install	None	0	18	0
Unassigned Computers	Not approved	N/A	0	12	0
Test Group	Same as All Computers group	Same as All Computers group	0	6	0

810565: Critical Update	0	18	0	11/5/2004 7:04 AM
810577: Security Update	0	18	0	11/5/2004 8:57 AM
810833: Security Update (Windows XP 64-bit Edition)	0	18	0	11/5/2004 7:04 AM
811493: Security Update (Windows 2000)	0	18	0	11/5/2004 8:57 AM
811493: Security Update (Windows XP 64-bit Edition)	0	18	0	11/5/2004 7:04 AM
811493: Security Update (Windows XP)	0	18	0	11/5/2004 8:57 AM
811630: Critical Update (Windows XP)	0	18	0	11/5/2004 7:04 AM

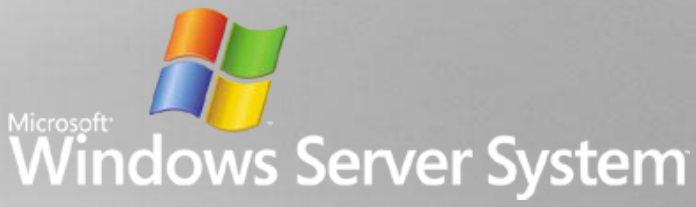
Status of Updates
View the status of all updates for the client computers in various groups.

Synchronization Results
View a list of updates, revisions, and errors that have occurred during synchronizat

Settings Summary
View a printable list of the current Options page settings.

WSUS – итог

feature	SUS	WSUS
установка на контроллер домена	✔	✔
поддержка service pack'ов	✔	✔
поддержка других типов content'а		✔
поддержка других продуктов Microsoft		✔
поддержка собственного и ПО третьих фирм		
возможность выбора загружаемых данных		✔
оптимизация трафика и поддержка плохих каналов		✔
работа при отсутствии связи между офисами		✔
автоматическое утверждение (approval)		✔
категоризация клиентов		✔
поддержка NT 4.0		
работа без прямого соединения с Internet		✔



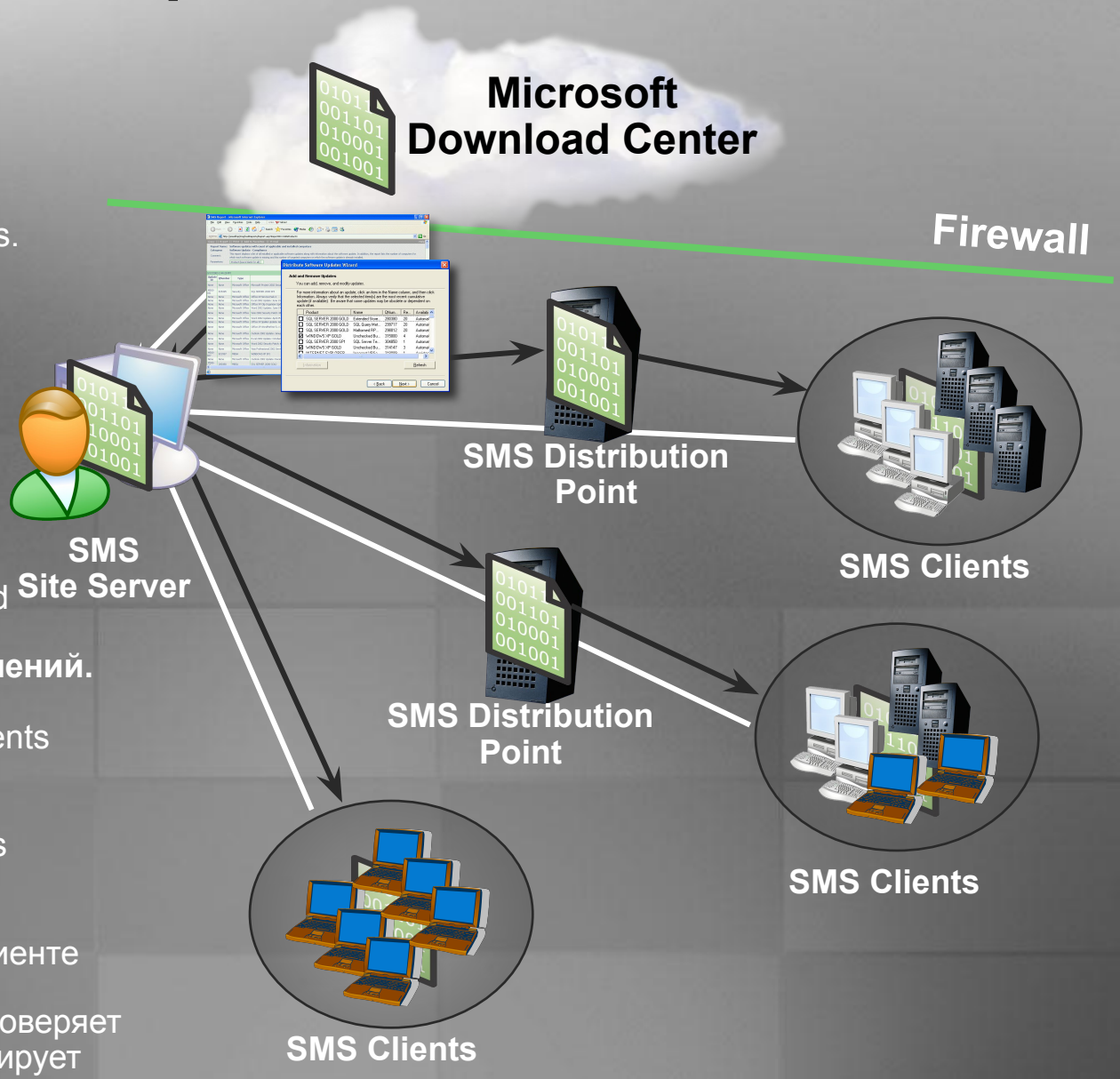
Systems Management Server 2003

SMS: управление обновлнеиями

- Обновление продуктов Microsoft
  - SMS 2003 Inventory Tool for Microsoft Updates
  - *http://www.microsoft.com/smserver/downloads/2003/tools/msupdates.mspx*
- Обновление других продуктов
  - Создание собственных детекторов
    - Пример – SMS 2003 Inventory Tool for Dell Updates
  - Как часть процесса распространения ПО через SMS

SMS – схема работы

1. **Инициализация.**
   Загрузка и установка
   Inventory Tool for Microsoft Updates.
2. **Распространение.**
   Репликация ITMU
   на клиентов
3. **Сканирование клиентов.**
   Клиенты сканируются и
   результаты помещаются в
   Hardware Inventory
4. **Авторизация обновлений.**
   Administrator использует
   Distribute Software Updates Wizard
   для авторизации обновлений
5. **Подготовка к установке обновлений.**
   Обновления загружены;
   packages, programs & advertisements
   созданы/обновлены;
   packages реплицированы;
   programs advertised to SMS clients
6. **Установка обновлений.**
   Software Update Installation Agent
   устанавливает обновления на клиенте
7. **Мониторинг.**
   Sync component периодически проверяет
   наличие новых обновлений, сканирует
   клиентов и распространяет новые обновления



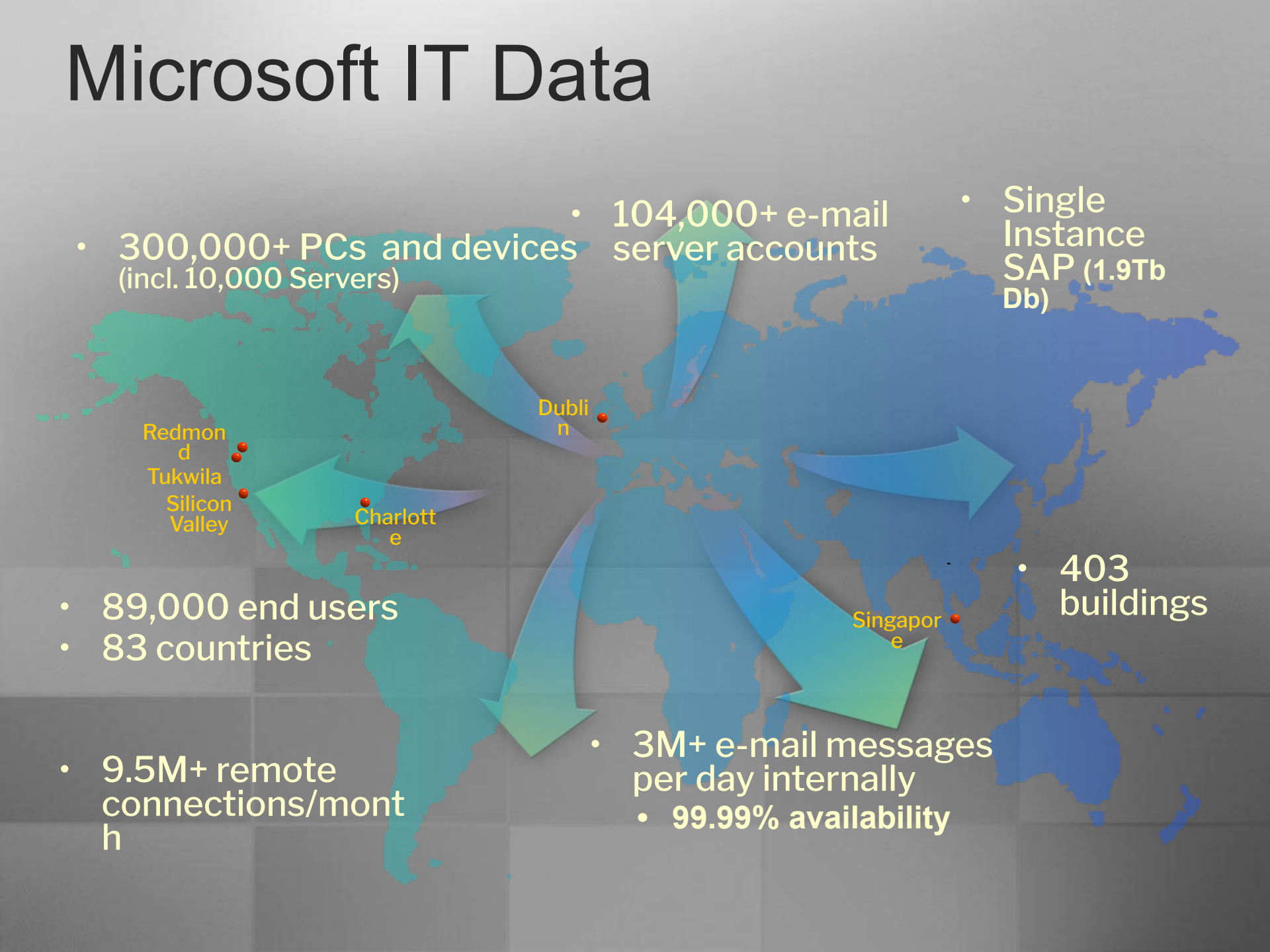
Управление обновлениями через SMS

- Проактивность процесса
  - Устранение уязвимостей до того, как они начнут влиять на производительность труда пользователей
- Автоматическое создание пакетов
  - Не требуется создания дополнительных сценариев и тестирования
  - Самое быстрое время реакции
- Централизованное управление
  - Управление из единого центра
- Использование существующих ресурсов
  - Инфраструктуры серверов SMS
  - Команды SMS Administrator’ов

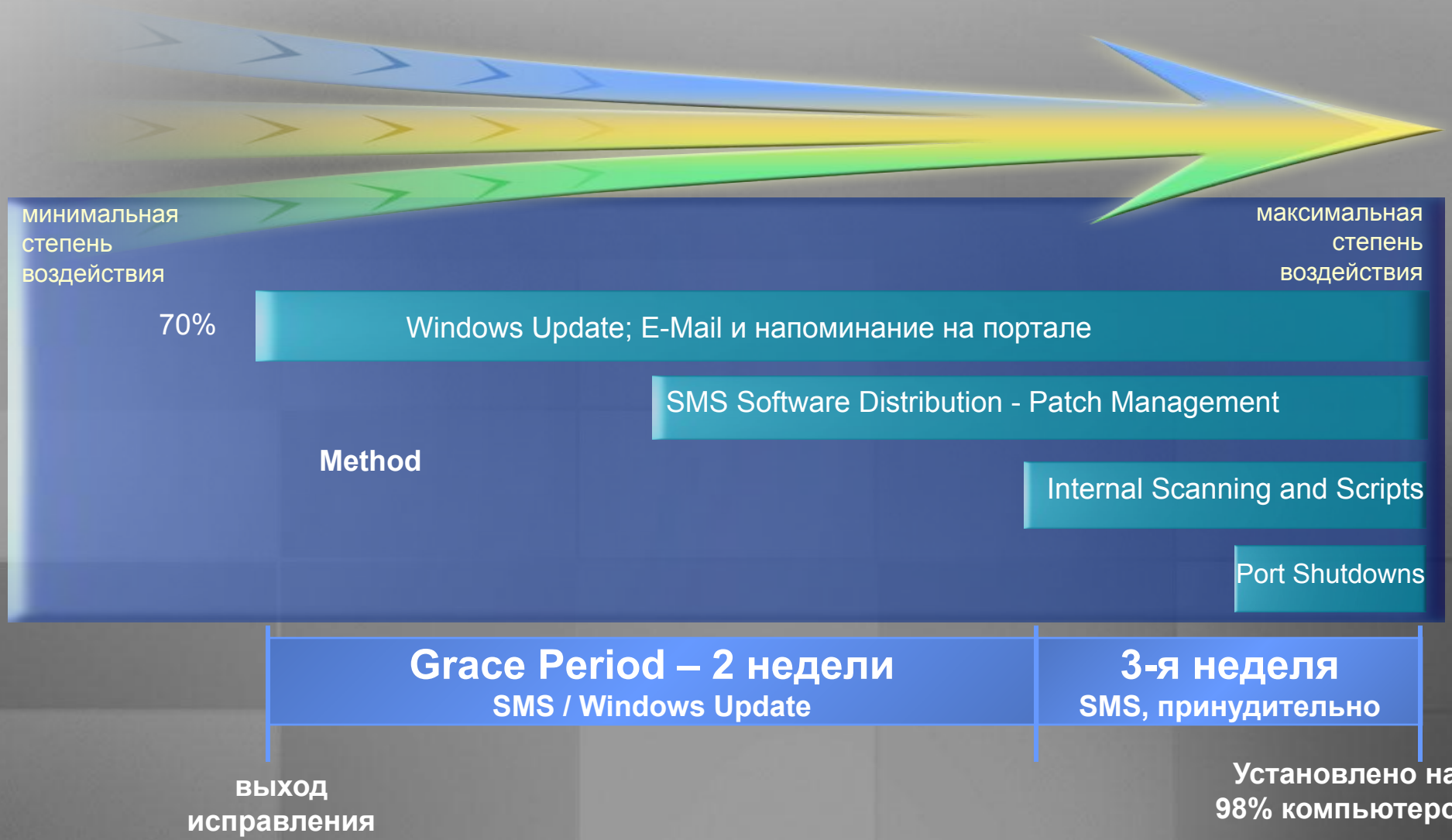
Microsoft Windows Server System

Управление обновлениями в Microsoft IT

Microsoft IT Data

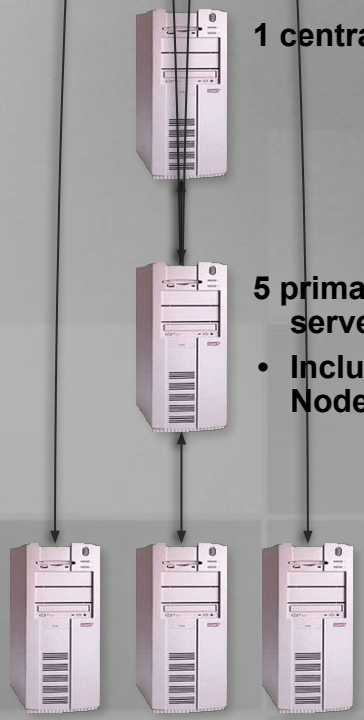


Подход к обновлению рабочих станций пользоватлей



Инфраструктура SMS в Microsoft IT

Client SMS hierarchy



1 central site server

5 primary site servers

- Includes a 1 X 3 Node NLB Cluster

139 secondary site servers

- 180,000 компьютеров
- 4 леса Active Directory
- все компьютеры входят в домены AD

Server SMS hierarchy

1 central site server

14 Primary site servers

- 10,000 компьютеров
- 5 лесов Active Directory
- управление не только членами доменов AD

Клиенты SMS

- “Лёгкая” модель управления
- Большинство пользователей являются администраторами на своих машинах
- Полтора компьютера на человека, без учёта машин для разработки
- В сети используется IPSec
- Членство в домене обязательно
- Около 40,000 пользователей RAS в месяц
- Установка ПО и обновлений через SMS
- Только Advance Client
- Использование Port Shutdown

Процесс обновления

1. Оценка окружения

периодически

A. Создание/модификация стандартов

B. Обновление списка исправлений

C. Контроль инфраструктуры/ конфигурации

регулярно

A. Поиск новых клиентов

B. Инвентаризация

2. Идентификация новых исправлений

по необходимости

A. Определение новых исправлений

B. Определение критичности исправлений

C. Проверка аутеничности и целостности (установка в тестовой лаборатории)

3. Планирование развёртывания

по необходимости

A. Завершение тестирования

B. Получение разрешения на установку

C. Оценка рисков

D. Планирование процесса развёртывания

4. Развёртывание

по необходимости

A. Распространение и установка

B. Отчётность

C. Отработка исключений

D. Аналаиз результатов

Установка исправлений безопасности

- Важные обновления
  - добровольная установка – сутки
  - обязательная установка – ещё сутки
- Критические исправления
  - добровольная установка – 2 недели
  - обязательная установка – ещё неделя

Процесс установки обновлений

оценка	идентификация	планирование	установка	
			Pre-deadline Patching	Deadline Patching
Security Group	Security Group			Security Group
Client Lifecycle Management		Client Lifecycle Management	Client Lifecycle Management	Client Lifecycle Management
Server Lifecycle Management		Server Lifecycle Management	Server Lifecycle Management	Server Lifecycle Management
			System Owners (Server / Desktop)	System Owners (Server / Desktop)

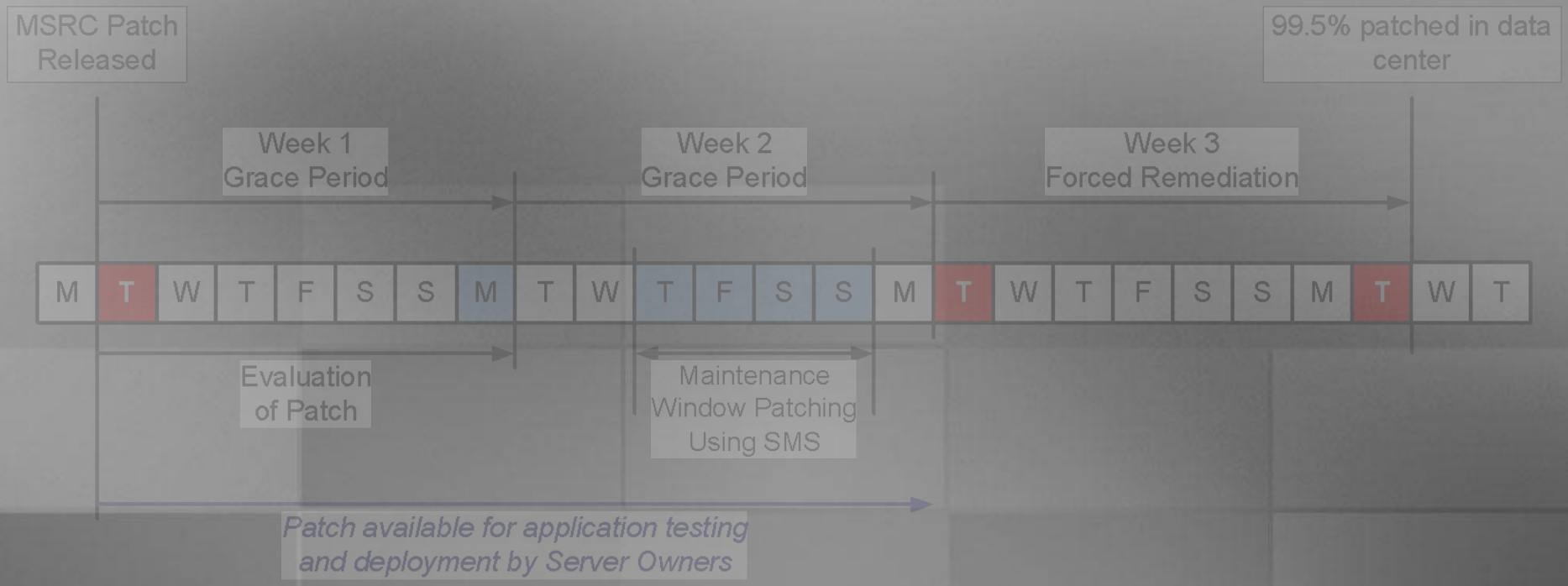
Критические обновления (2 недели)

по мере появления → полдня → 6,5 дней → 7 день → +неделя

Важные обновления (24 часа)

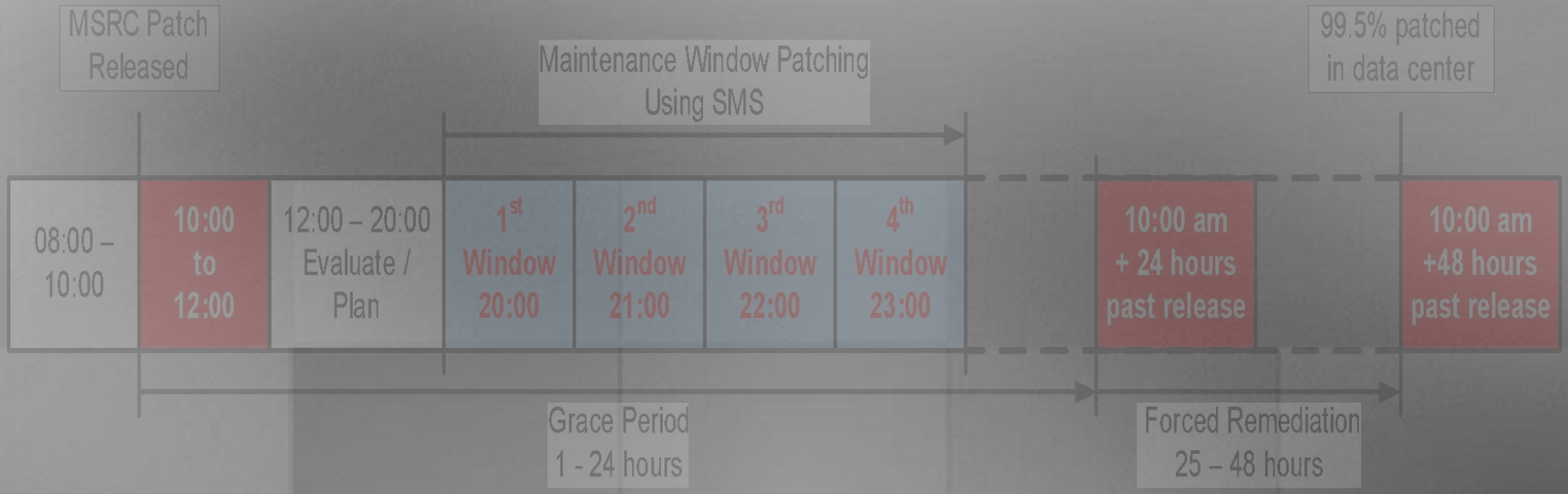
по мере появления → 1 час → 2 час → 21 час → +сутки

Подход к обновлению серверов критические обновления



критические обновления (три недели)

Подход к обновлению серверов важные обновления

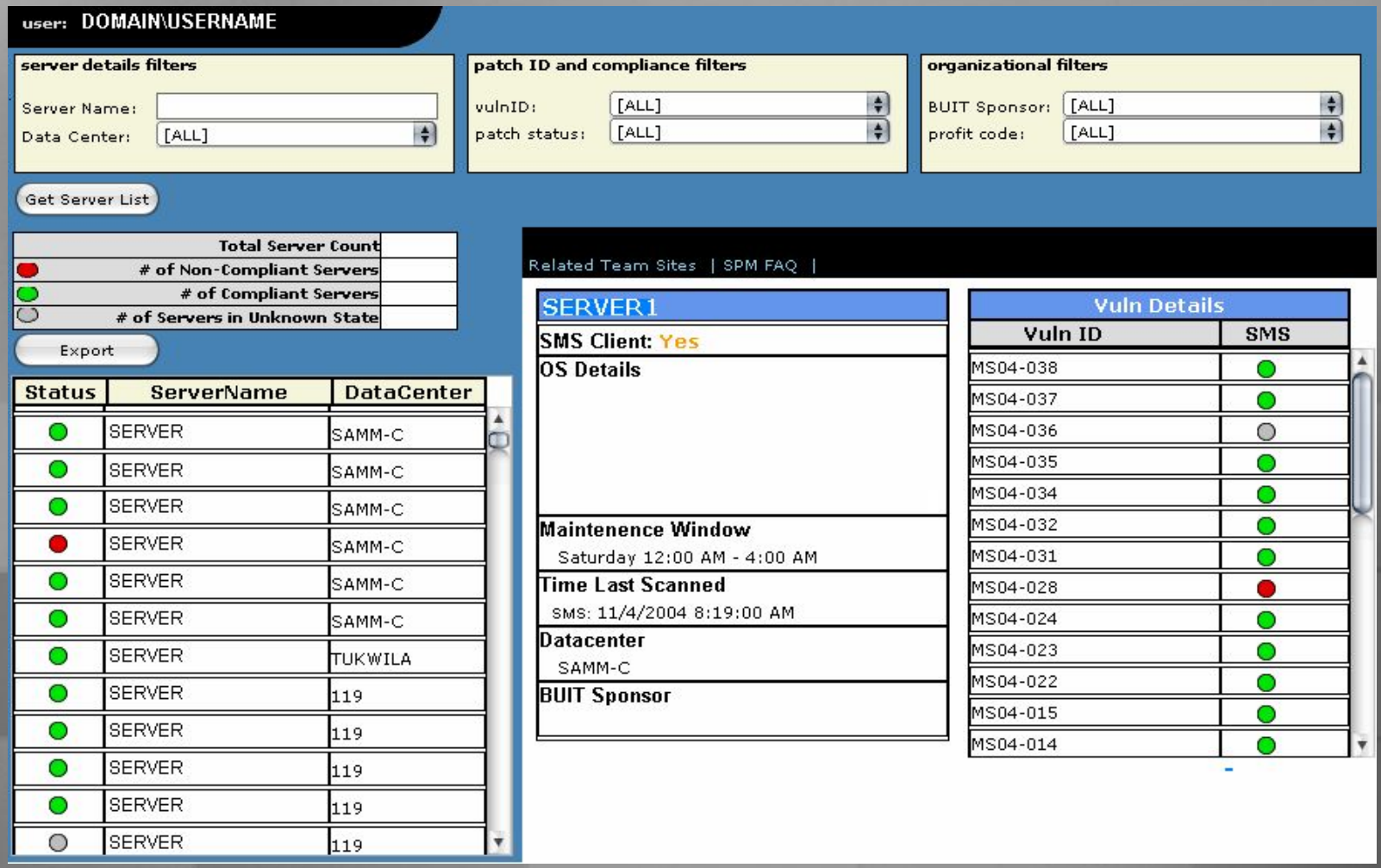


важные обновления (двое суток)

Мониторинг состояния серверов

SMS 2003 Client Health Monitoring Tool

http://www.microsoft.com/smserver/downloads/2003/tools/clienthealth.mspx



Факторы эффективности

- Безопасность – приоритет №1
- Административная поддержка
- Процесс не менее важен чем технология
- Управление окружением
- Корреляция установка обновлений с SMS Client Health
- Ясные и понятные сообщения ответственным за компьютеры

http://www.microsoft.com/technet/itshowcase
http://www.microsoft.com/technet/itsolutions/msit/webc

Windows 2000+
Office XP+
Exchange 2000+
SQL 2000 SP4+

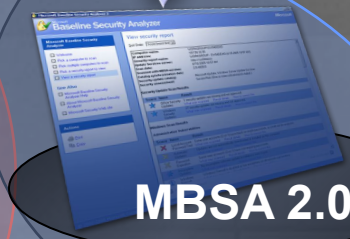
Microsoft Update Catalog

Detection and Update Content

Automatic Updates & MU Website

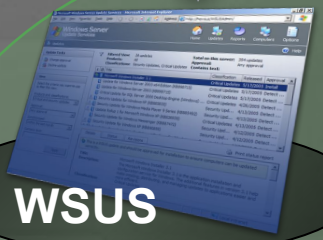
Consumer

Small Business

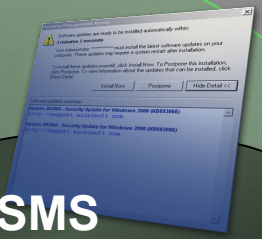


MBSA 2.0

Medium Business



WSUS



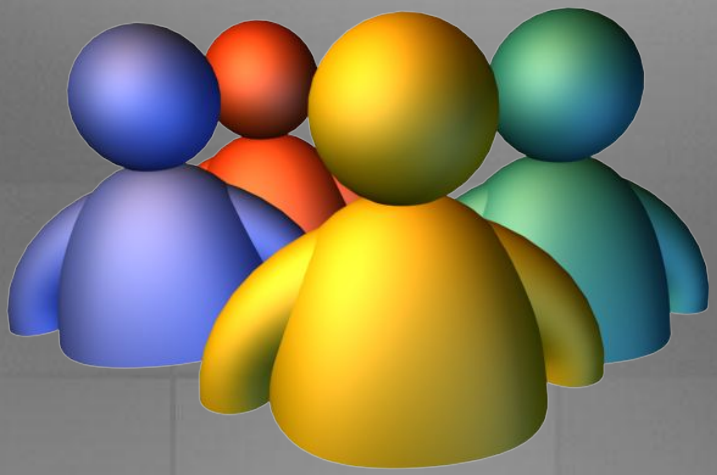
SMS

Large Enterprise

Windows Update Agent

Detection and Installation Infrastructure

Вопросы?



Владислав Кирилин
VKirilin@microsoft.com