

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

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 \(Secure Sockets Layer\)](#).

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



Домашняя страница



Обновления



Отчеты



Компьютеры



Параметры

Параметры автоматического одобрения

Справка

Задачи

- Сохранить параметры
- Отмена изменений

Обновления

Можно указать, нужно ли автоматически одобрять установку или обнаружение обновлений и как именно это делать. Одобрение происходит после загрузки обновления или метаданных о нем на сервер Windows Server Update Services.

Примечание: если правила установки и обнаружения противоречат друг другу, используется правило установки.

Одобрено для обнаружения

- Автоматически одобрять обнаружение обновлений по следующему правилу:

Классы: Драйверы, Накопительные пакеты обновления, Обновления, Пакеты обновления

[Добавление и удаление классов...](#)

Группы компьютеров: Все компьютеры

[Добавление или удаление групп компьютеров...](#)

Одобрено для установки

- Автоматически одобрять установку обновлений по следующему правилу:

Классы: Критические обновления, Обновления системы безопасности

[Добавление и удаление классов...](#)

Группы компьютеров: Все компьютеры

[Добавление или удаление групп компьютеров...](#)

Новые редакции обновлений

Иногда выпускаются обновленные версии ранее одобренных обновлений. Можно указать, следует ли автоматически одобрять эти новые редакции. Если не выбрать автоматическое одобрение новых редакций, прежние версии останутся одобренными.

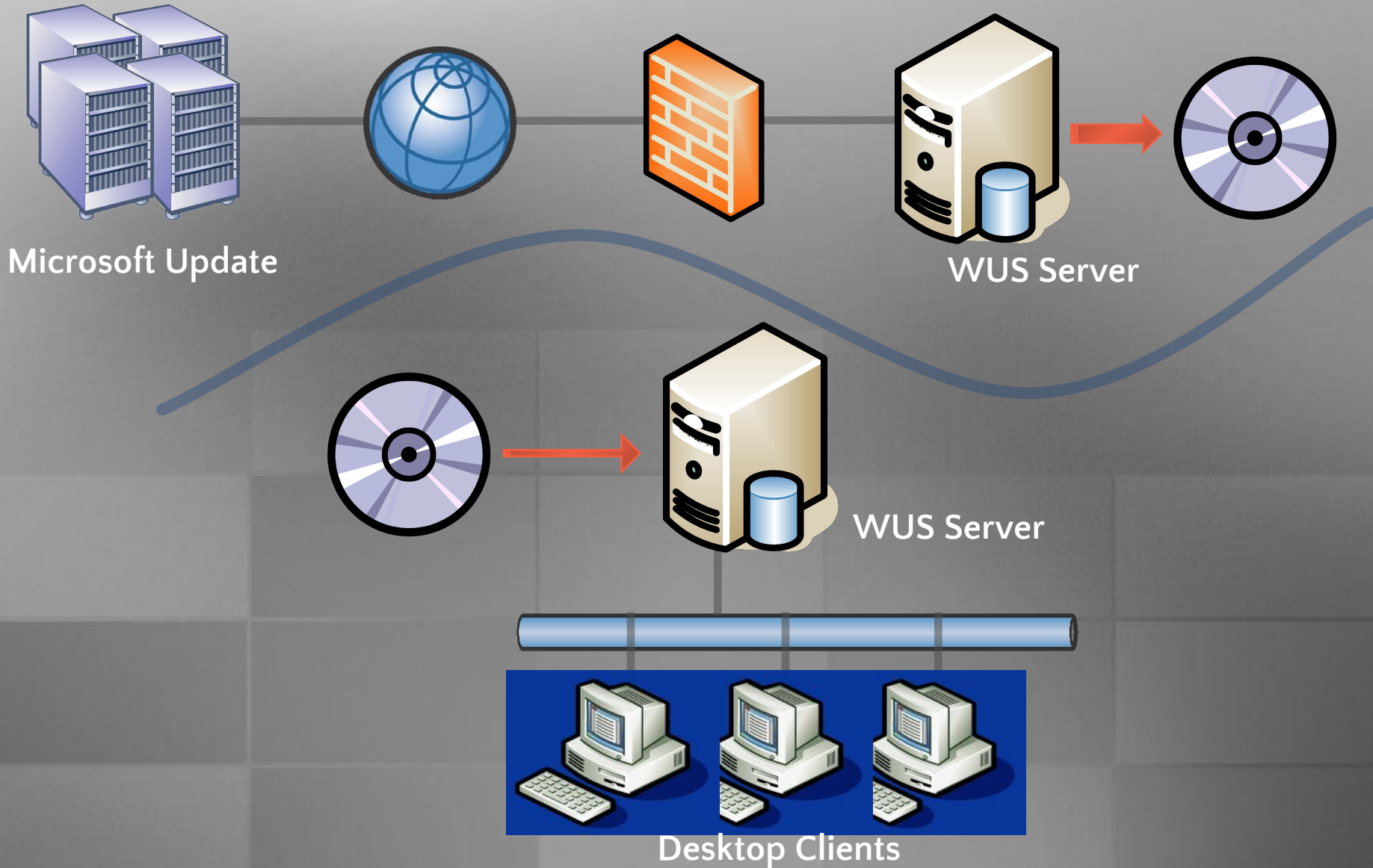
- Автоматически одобрять новейшую редакцию этого обновления
- Продолжать использование прежних редакций и вручную одобрять новые редакции обновлений

Обновления Windows Server Update Services

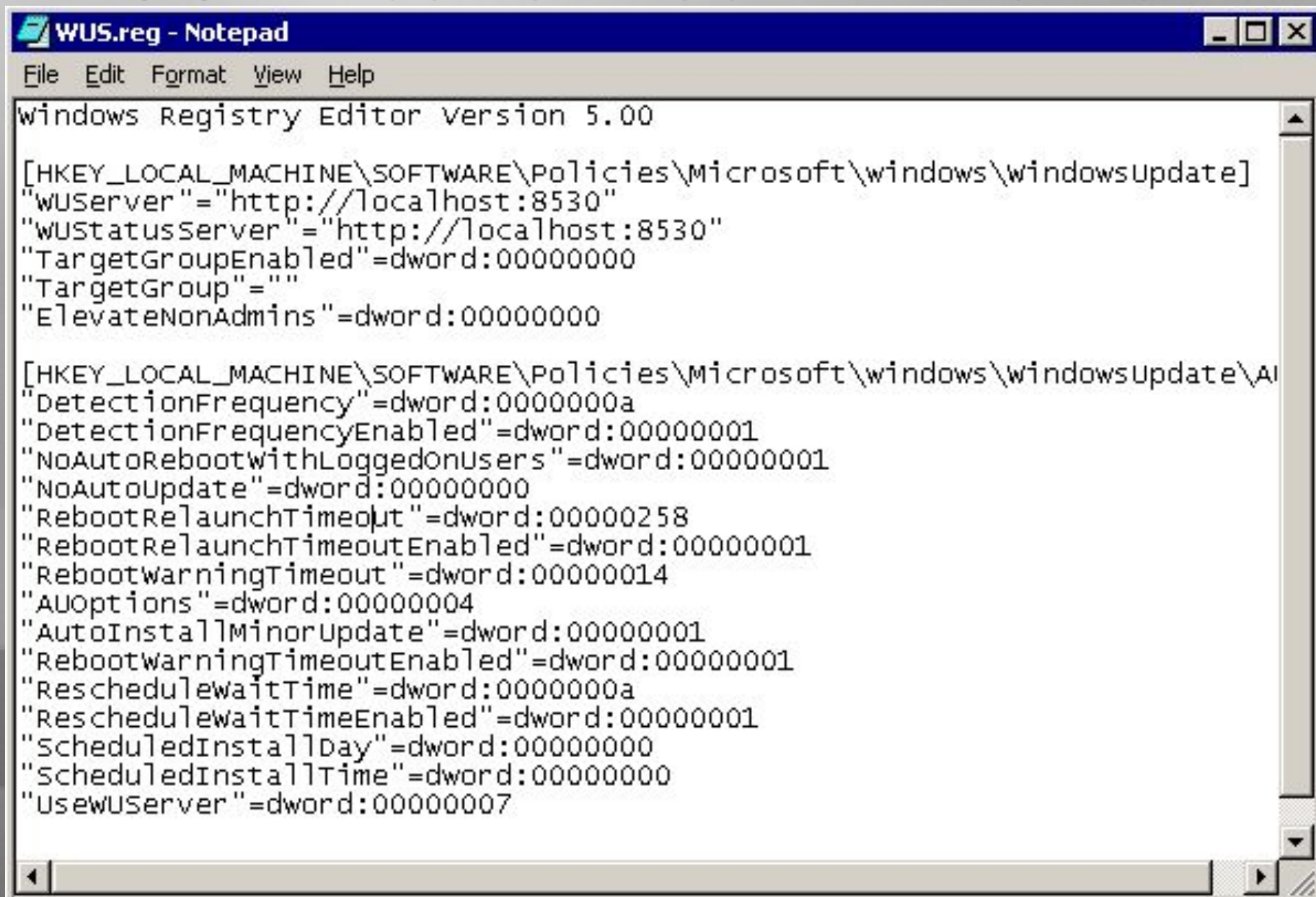
Обновления WSUS необходимы для того, чтобы обеспечить правильное обновление компьютеров. Если обновления WSUS не одобрены, некоторые обновления могут быть не обнаружены компьютерами.

- Автоматически одобрять обновления WSUS

WSUS – disconnected servers



WUS – ВОЗМОЖНОСТИ КЛИЕНТА

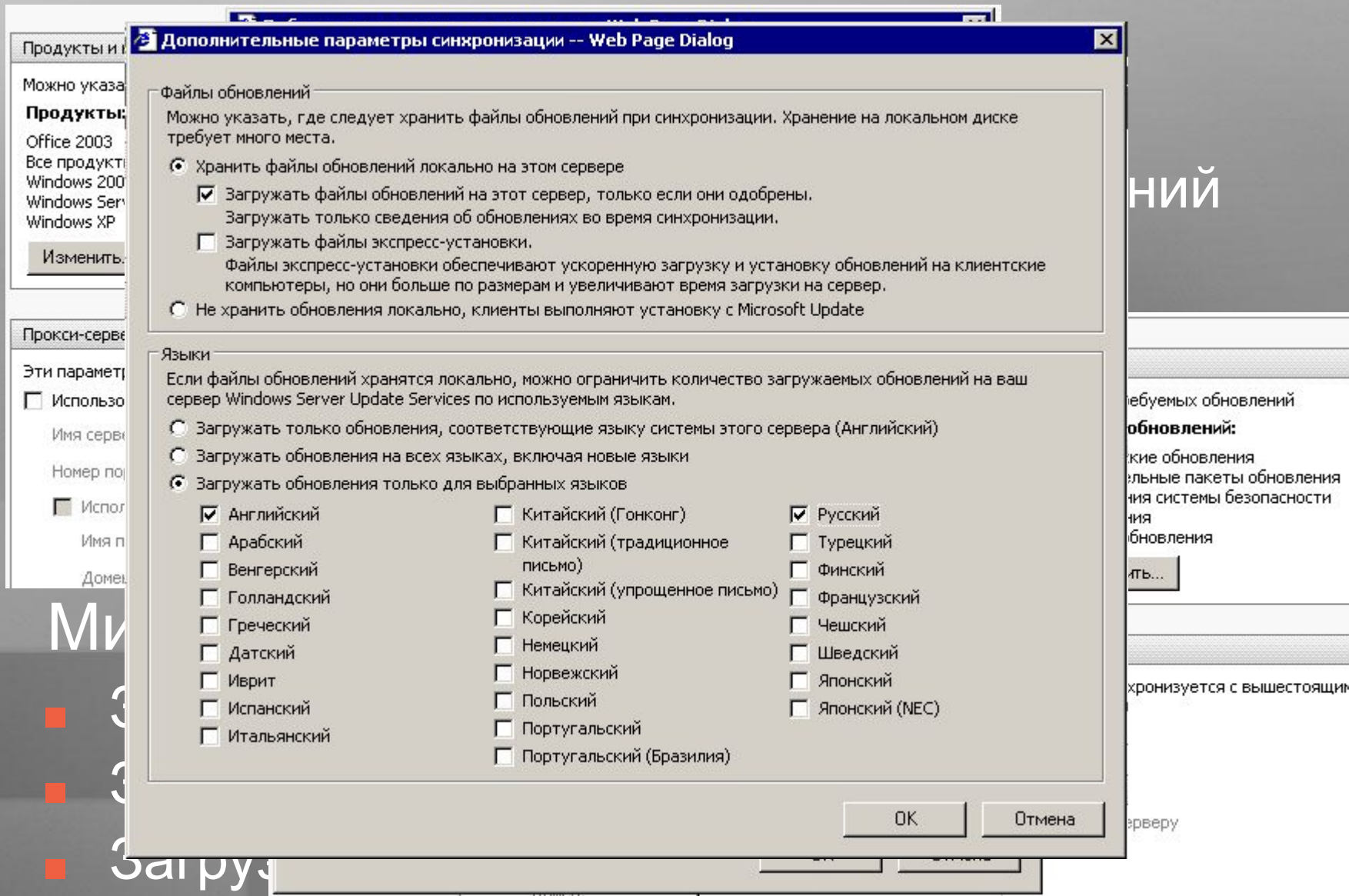


```
WUS.reg - Notepad
File Edit Format View Help
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\windows\windowsupdate]
"WUserver"="http://localhost:8530"
"WUstatusServer"="http://localhost:8530"
"TargetGroupEnabled"=dword:00000000
"TargetGroup"=""
"ElevateNonAdmins"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\windows\windowsupdate\AU]
"DetectionFrequency"=dword:0000000a
"DetectionFrequencyEnabled"=dword:00000001
"NoAutoRebootwithLoggedOnUsers"=dword:00000001
"NoAutoUpdate"=dword:00000000
"RebootRelaunchTimeout"=dword:00000258
"RebootRelaunchTimeoutEnabled"=dword:00000001
"RebootWarningTimeout"=dword:00000014
"AUOptions"=dword:00000004
"AutoInstallMinorUpdate"=dword:00000001
"RebootWarningTimeoutEnabled"=dword:00000001
"ReschedulewaitTime"=dword:0000000a
"ReschedulewaitTimeEnabled"=dword:00000001
"ScheduledInstallDay"=dword:00000000
"ScheduledInstallTime"=dword:00000000
"UseWUserver"=dword:00000007
```


WUS – оптимизация трафика



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 synchronization.

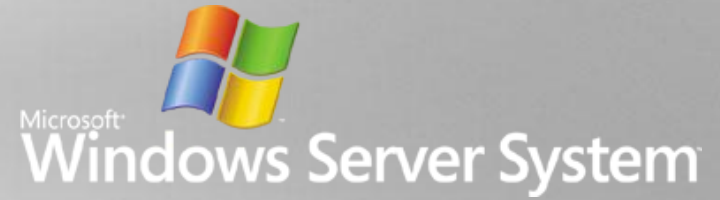


Settings Summary

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'a		✓
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		✓



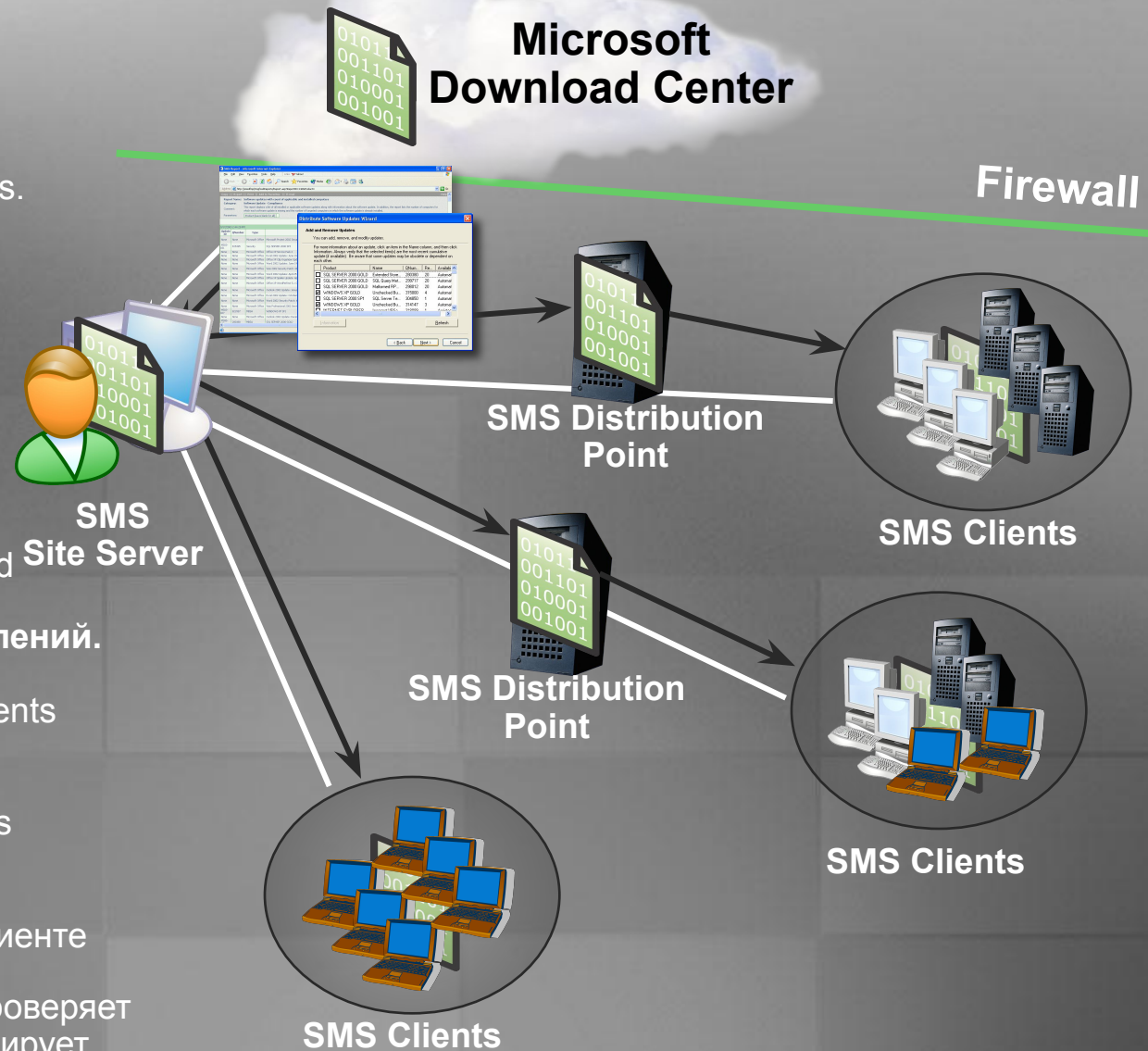
Systems Management Server 2003

SMS: управление обновлениями

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

SMS – схема работы

- Инициализация.**
Загрузка и установка Inventory Tool for Microsoft Updates.
- Распространение.**
Репликация ITMU на клиентов
- Сканирование клиентов.**
Клиенты сканируются и результаты помещаются в Hardware Inventory
- Авторизация обновлений.**
Administrator использует Distribute Software Updates Wizard для авторизации обновлений
- Подготовка к установке обновлений.**
Обновления загружены; packages, programs & advertisements созданы/обновлены; packages реплицированы; programs advertised to SMS clients
- Установка обновлений.**
Software Update Installation Agent устанавливает обновления на клиенте
- 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

Управление обновлениями в Microsoft IT

Microsoft IT Data

- 300,000+ PCs and devices (incl. 10,000 Servers)

- 104,000+ e-mail server accounts

- Single Instance SAP (1.9Tb Db)

Redmond
Tukwila
Silicon Valley

Charlotte

Dublin

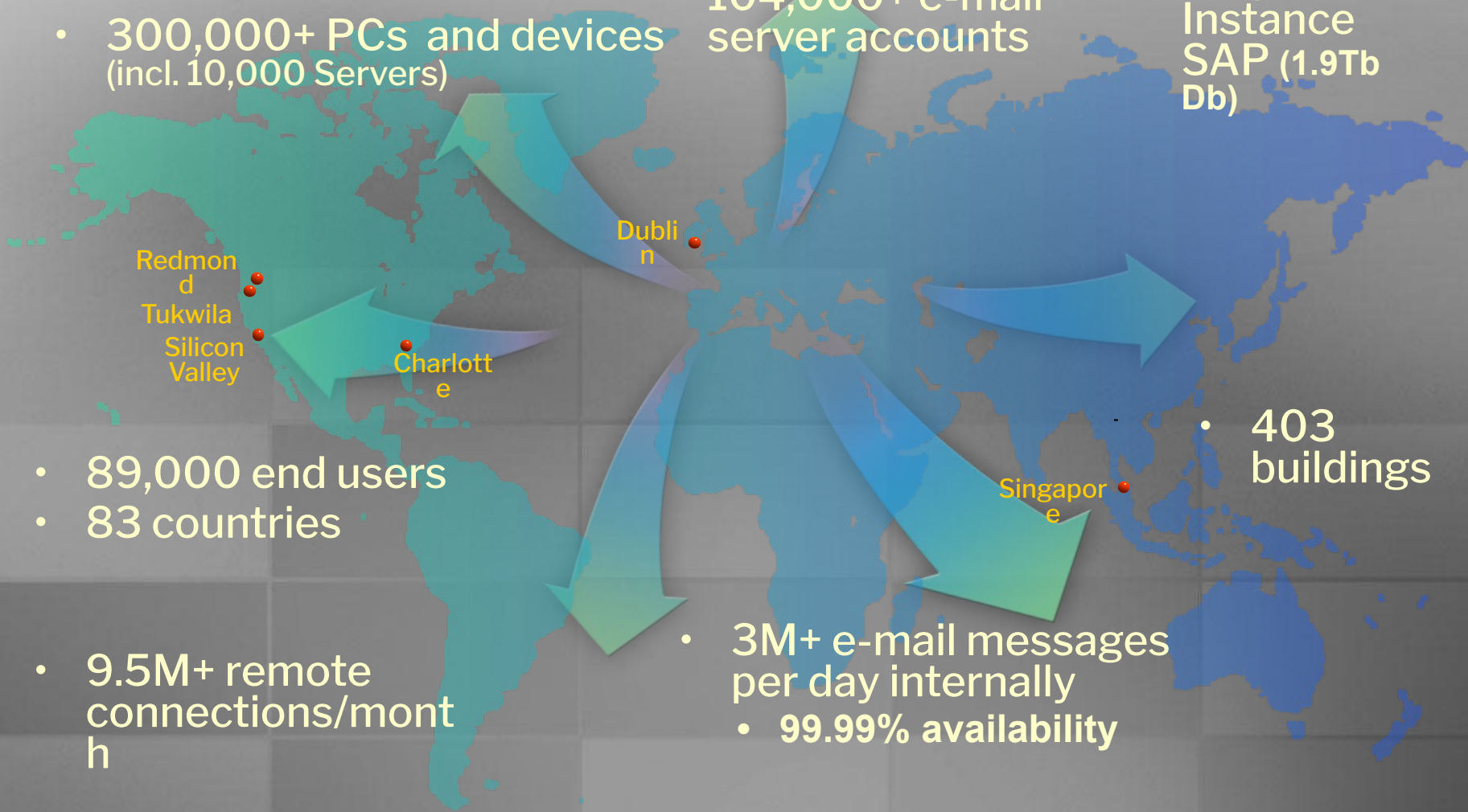
Singapore

- 89,000 end users
- 83 countries

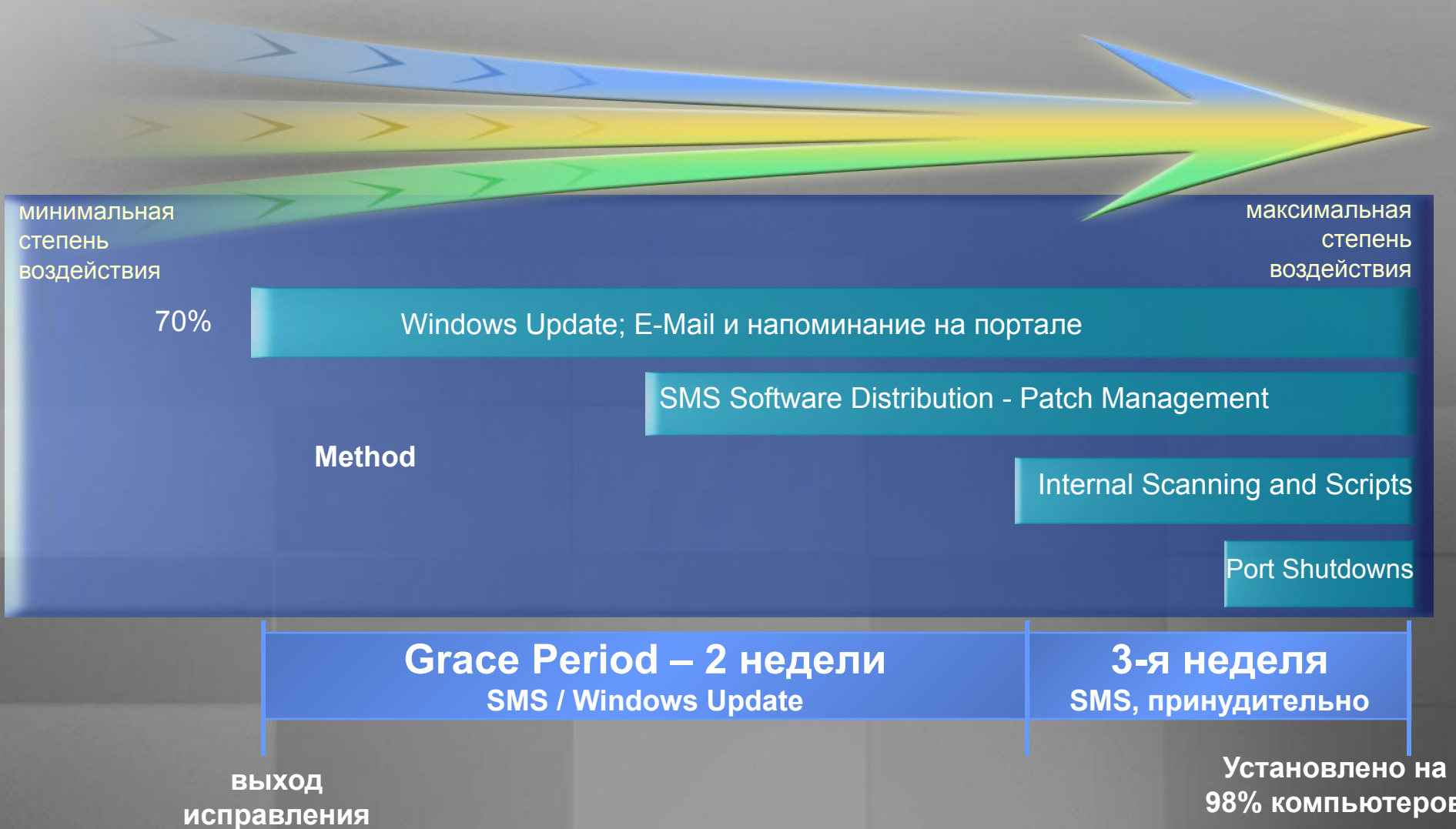
- 9.5M+ remote connections/month

- 3M+ e-mail messages per day internally
 - 99.99% availability

- 403 buildings

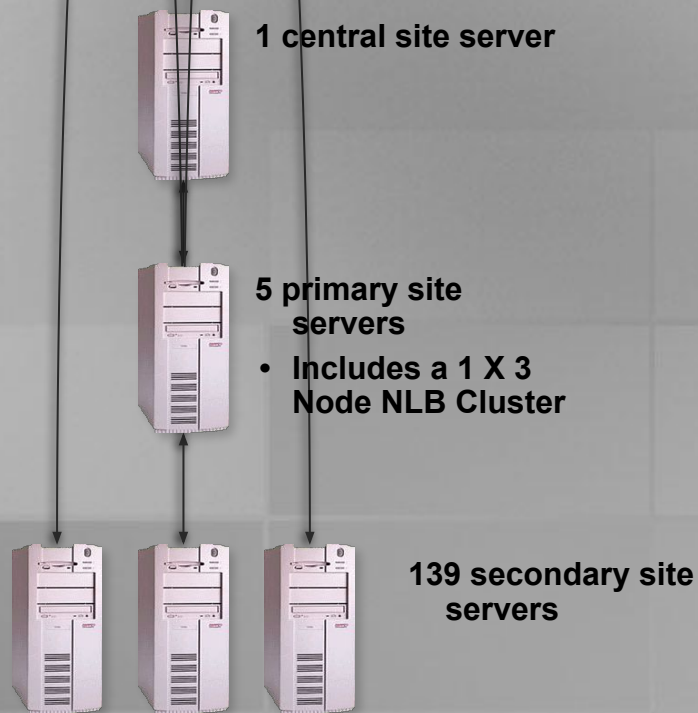


Подход к обновлению рабочих станций пользователей



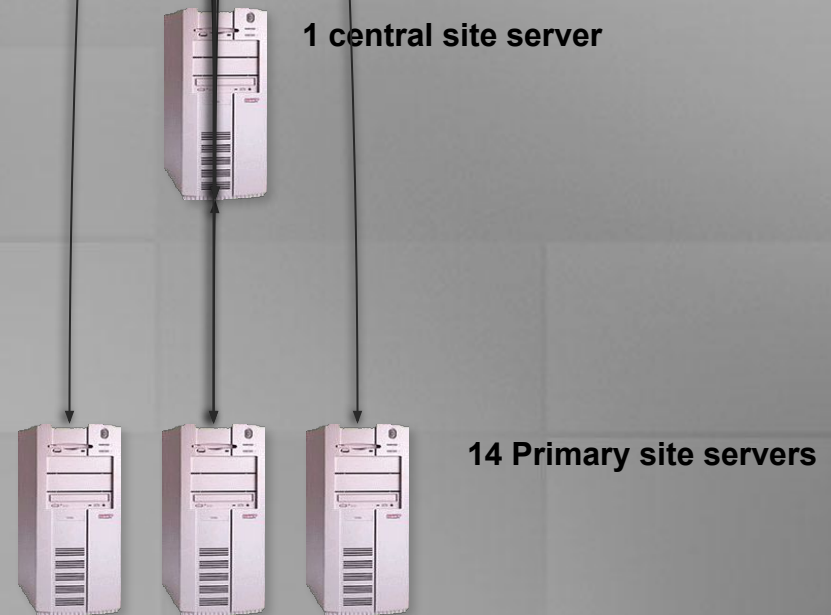
Инфраструктура SMS в Microsoft IT

Client SMS hierarchy



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

Server SMS hierarchy



- 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 аутентичности 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. Анализ результатов



Установка исправлений безопасности

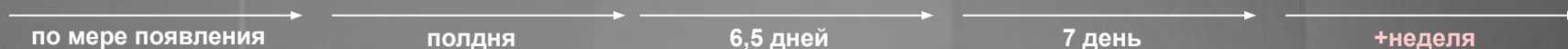
- Важные обновления
 - добровольная установка – сутки
 - обязательная установка – ещё сутки
- Критические исправления
 - добровольная установка – 2 недели
 - обязательная установка – ещё неделя

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)

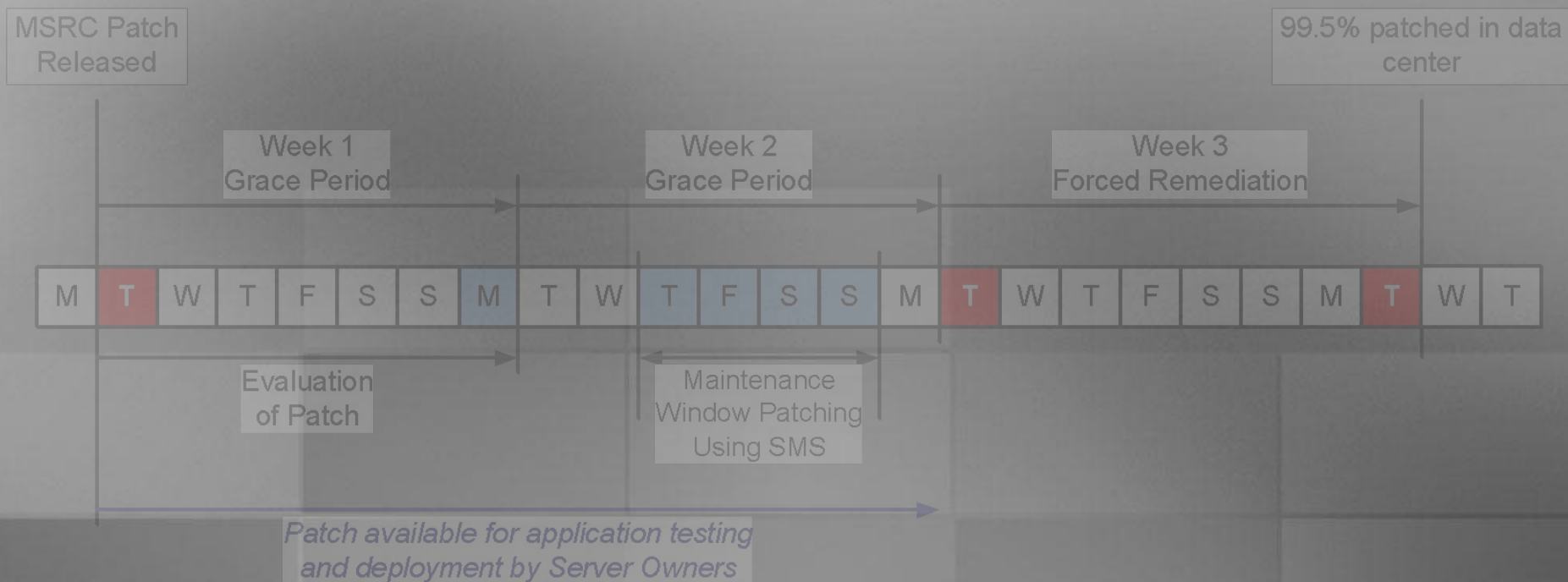
Критические обновления (2 недели)



Важные обновления (24 часа)

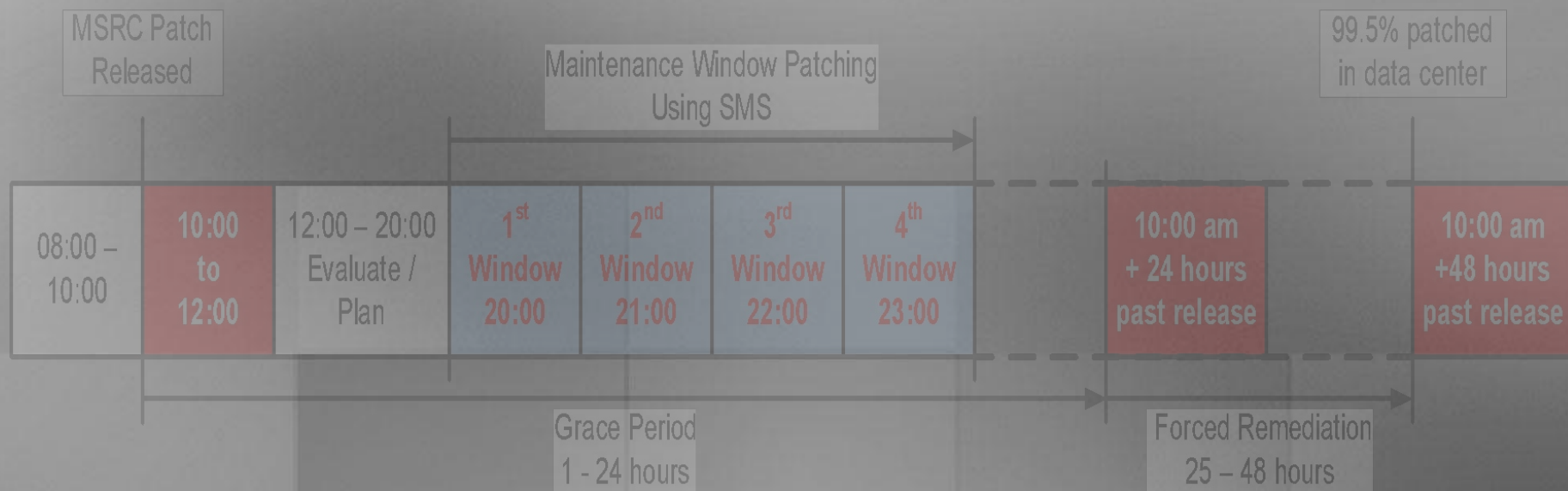


Подход к обновлению серверов критические обновления



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/smsserver/downloads/2003/tools/clienthealth.msp>

user: DOMAIN\USERNAME

server details filters

Server Name:

Data Center: [ALL]

patch ID and compliance filters

vulnID: [ALL]




patch status: [ALL]

organizational filters














BUIT Sponsor: [ALL]

profit code: [ALL]

Get Server List














Total Server Count	
	# of Non-Compliant Servers
	# of Compliant Servers
	# of Servers in Unknown State

Export

Status	ServerName	DataCenter
	SERVER	SAMM-C
	SERVER	SAMM-C
	SERVER	SAMM-C
	SERVER	SAMM-C
	SERVER	SAMM-C
	SERVER	SAMM-C
	SERVER	TUKWILA
	SERVER	119
	SERVER	119
	SERVER	119
	SERVER	119
	SERVER	119
	SERVER	119

Related Team Sites | SPM FAQ |

SERVER1	
SMS Client: Yes	
OS Details	
Maintenance Window Saturday 12:00 AM - 4:00 AM	
Time Last Scanned SMS: 11/4/2004 8:19:00 AM	
Datacenter SAMM-C	
BUIT Sponsor	

Vuln Details	
Vuln ID	SMS
MS04-038	
MS04-037	
MS04-036	
MS04-035	
MS04-034	
MS04-032	
MS04-031	
MS04-028	
MS04-024	
MS04-023	
MS04-022	
MS04-015	
MS04-014	

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

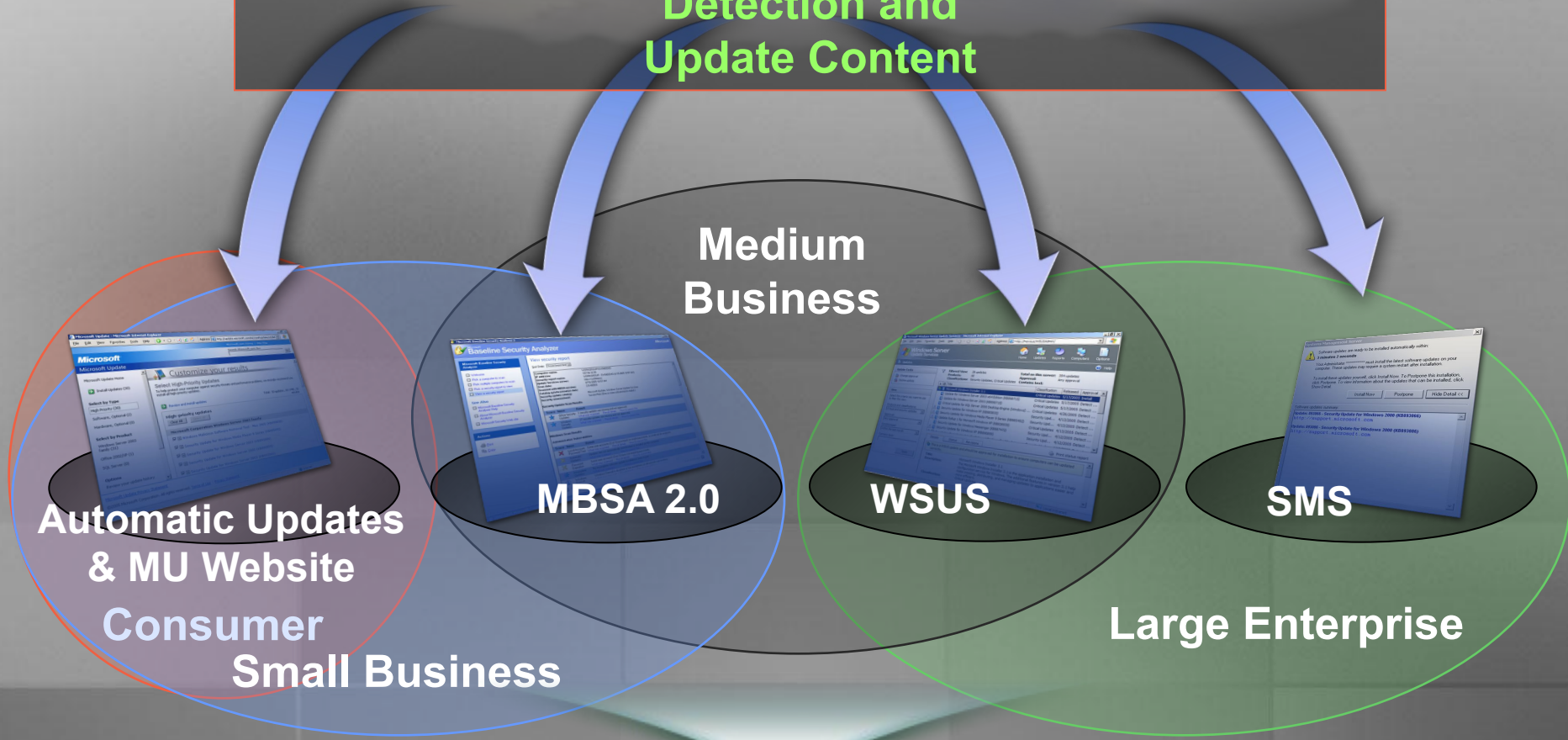
<http://www.microsoft.com/technet/itshowcase>

<http://www.microsoft.com/technet/itsolutions/msit/webc>

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

Microsoft Update Catalog

Detection and Update Content

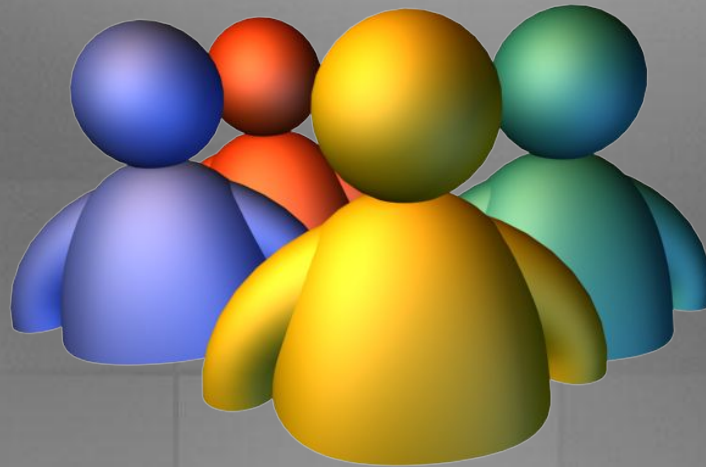


Windows Update Agent

Detection and Installation Infrastructure



Вопросы?



Владислав Кирилин
VKirilin@microsoft.com