Microsoft®
Платформа
2008

Windows Server 2008

Совместимость существующих приложений и подготовка к сертификации

Категории несовместимостей

Безопасность	Защищенные компоненты ОС	Новые/Устаревшие функции
• User Account Control • Mandatory Integrity Control • Изоляция сессии 0 • Windows Firewall	• Windows Resource Protection	• Версия операционной системы • Изменения в Active Directory • Новые или измененные серверные роли • Компоненты системы • Server Core • Failover Clustering

Несовместимости

Windows Vista и Windows Server 2008

User Account Control (UAC)

Windows Resource Protection (WRP)

Mandatory Integrity Control (MIC)

Версия операционной системы

Изоляция сессии 0

User Account Control

- Операционная система подвергается существенным рискам когда пользователь работает под учетной записью Administrator
  - Более простая установка вредоносного кода
  - Возможность повышения привилегий
  - Открытость для вредоносного кода
- Случайные повреждения, вносимые пользователем

Windows Resource Protection

- Ключевые файлы операционной системы и ключи реестра могут быть заменены на предыдущие версии или вредоносный код – ущерб стабильности и безопасности системы
- Задача Windows Resource Protection – защита ключевых компонентов операционной системы, увеличение стабильности, предсказуемости и надежности системы

Windows Resource Protection

- Запрещены обновления защищенных ресурсов
  - Только программы установки, известные ОС (Windows Update)
  - ACL для ресурсов
- Распространяется на файлы, папки и ключи реестра
  - Большинство ключевых модулей ОС (EXE и DLL)
  - Большинство ключей реестра (HKCR)
  - Папки, используемые ресурсами ОС

Mandatory Integrity Control (MIC)

- Реализовано в Windows Vista и Windows Server 2008
- Процессы выполняются на одном из четырех уровней целостности (Integrity Levels):
  - Системные процессы – *System* IL
  - Приложения с привилегиями администратора – *High* IL
  - Стандартные приложения – *Medium* IL
  - Приложения с ограничениями – *Low* IL
- Защищаемые объекты (файлы, процессы, очереди сообщений и т.п.) задают минимальный уровенб процесса для доступа к ним
  - Уровень для объектов по умолчанию: *Medium*

Изоляция привилегий интерфейса

- UI Privilege Isolation (UIPI)
- Использует MIC для запрета посылки сообщений между окнами
  - Приложения не могут посылать сообщения приложениям, выполняющися с более высоким IL
  - Приложения с более высоким IL могут разрешить прием сообщений
  - SendMessage() не возвращает ошибок

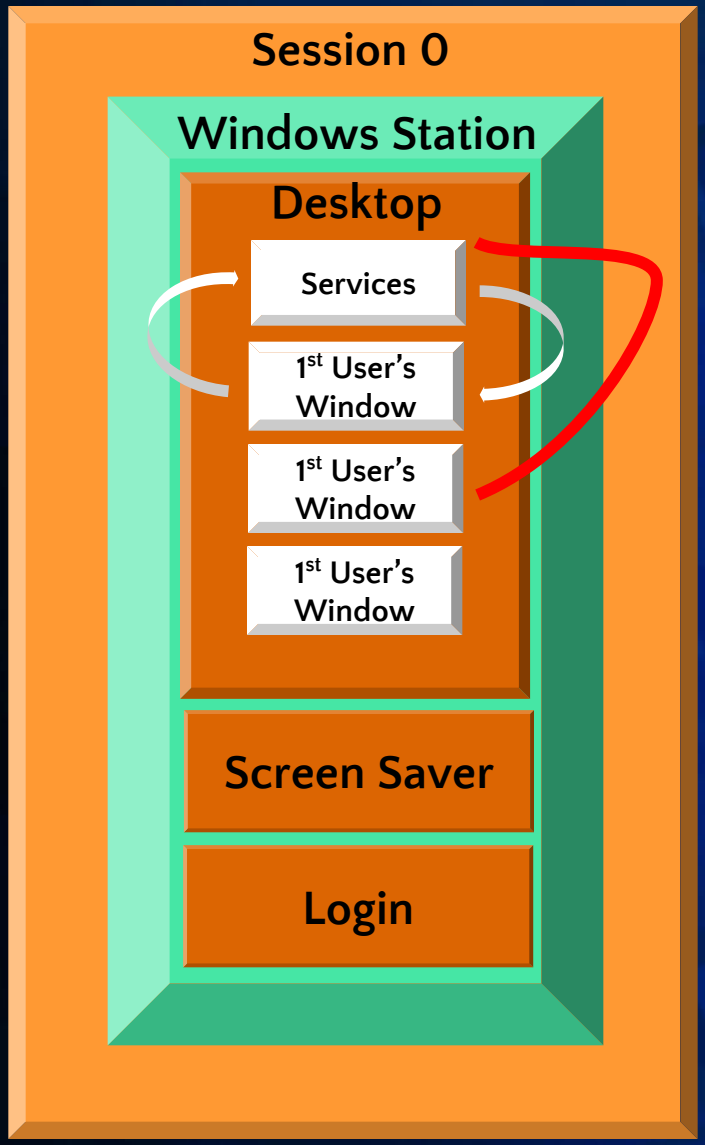
Версия операционной системы

- Внутренний номер версии в Windows Server 2008 (функция GetVersion) = 6

	Windows 2000	Windows XP	Windows Server 2003	Windows Vista	Windows Server 2008
Версия	5.0	5.1	5.2	6.0	6.0

- Версия Internet Explorer – 7.0
  - Версия включена в строку User Agent
  - Строка User Agent включается в заголовок каждого HTTP запроса
- Измените код – нужна проверка типа >= 6

Изоляция сессии 0



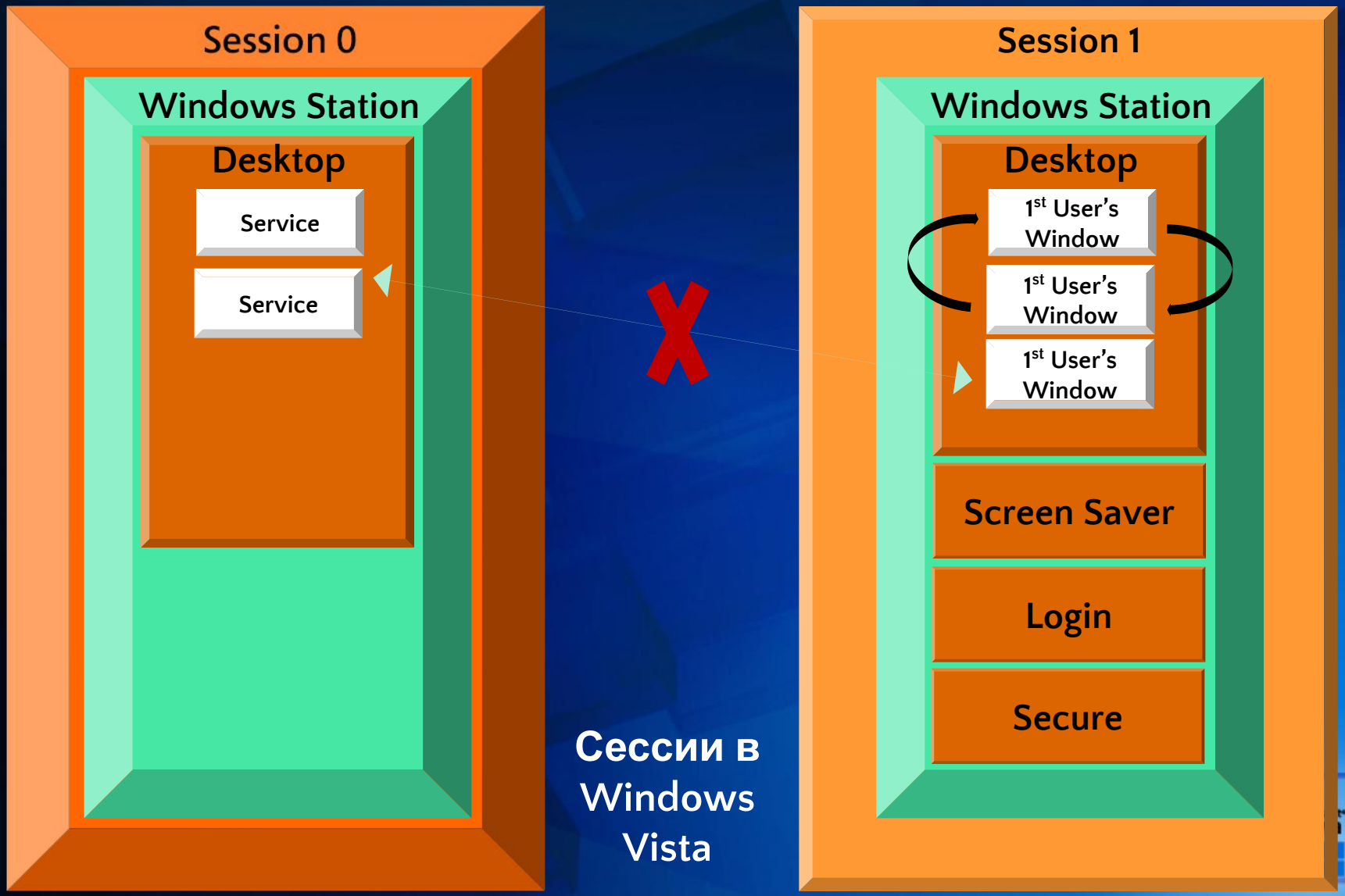
Сессии в Windows XP/2003

Возможность атаки

Изоляция сессии 0

- Выполнение системных сервисов и пользовательских приложений в сессии 0 моежт привести к нарушению безопасности
  - Потенциальная возможность обмена между сервисами и приложениями
  - Потенциальная возможность повышения привилегий
- Выполнение сервисов и приложений в различных сессиях существенно снижает возможность атак, повышает стабильность, надежность и защищенность системы

Изоляция сессии 0



Несовместимости

Уникальные для Windows Server 2008

Изменения в Active Directory	Новые или измененные серверные роли	Компоненты системы
Server Core	Failover Clustering	Windows Firewall

Изменения в Active Directory

- Новая унифицированная модель:
  - Единая архитектура и программная модель
  - Администрирование контроллеров доменов
  - Сервисы каталогов
  - Управление правами
  - Федерация сервисов
  - Интеграция сервисов мета-каталогов (ILM)
  - Доменные контроллеры только для чтения (Read-Only Domain Controllers)

Изменения в Active Directory

- Изменения в названиях

Старое название	Новое название
Active Directory Domain	Active Directory Domain Services
Active Directory App Mode (ADAM)	Active Directory Lightweight Directory Services
Windows Rights Management Services	Active Directory Rights Management Services
Windows Certificate Services	Active Directory Certificate Services
Identity Integration Feature Pack	Active Directory Metadirectory Services

Доменные контроллеры только для чтения

- Безопасность по умолчанию – пароли пользователей/компьютеров не реплицируются и не хранятся в Read Only DC
  - Выборочное разрешение кэширования паролей
- Однонаправленная репликация для AD и SYSVOL
  - Атрибут Read Only Partial для отказа от репликации данных
    - Требует ручной настройки

Доменные контроллеры только для чтения

- Разделение ключей Kerberos – каждый RODC имеет свою учетную запись KDC Krbtgt
- Ограниченные права записи в каталог
  - Учетные записи Workstation;
  - Не члены группы “enterprise domain controller”
  - Не члены группы “domain domain controller”

Доменные контроллеры только для чтения

- Упрощенная система – однонаправленная репликация
- Упрощенная настройка конфигурации
- Большинство настроек включено по умолчанию
- Администратор RODC может не быть администратором домена
  - Предотвращает случайные модификации домена администраторами компьютеров
- Возможность делегирования установки и восстановления RODC

Доменные контроллеры только для чтения

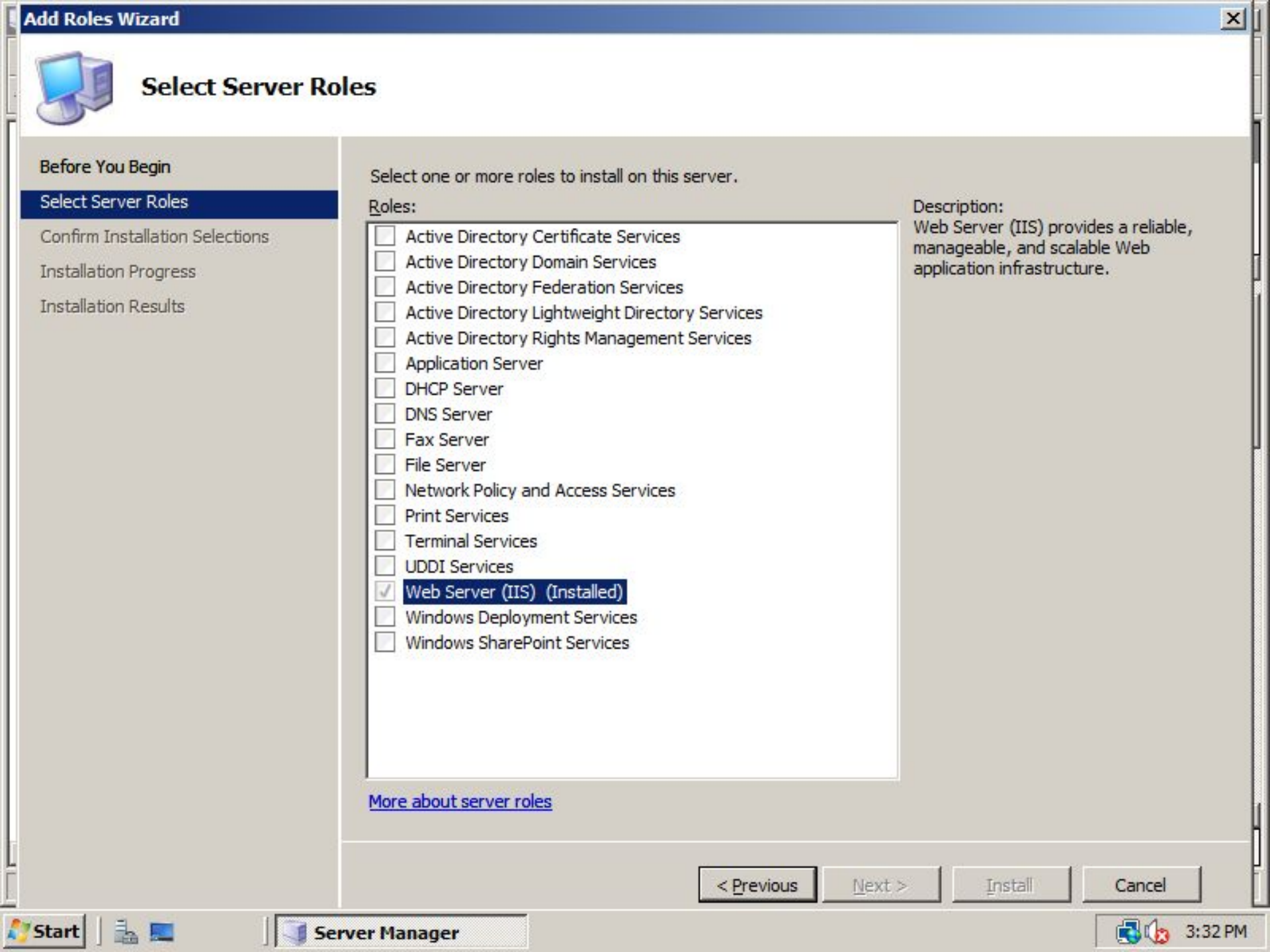
- Работает в существующей инфраструктуре!!!
  - Не требуется изменений для DC или клиентов
  - Требования
    - Наличие режима Windows Server 2003 Forest Functional Mode
    - PDC FSMO на Windows Server 2008
    - Рекомендуется использовать несколько WS2K8 DC на один домент

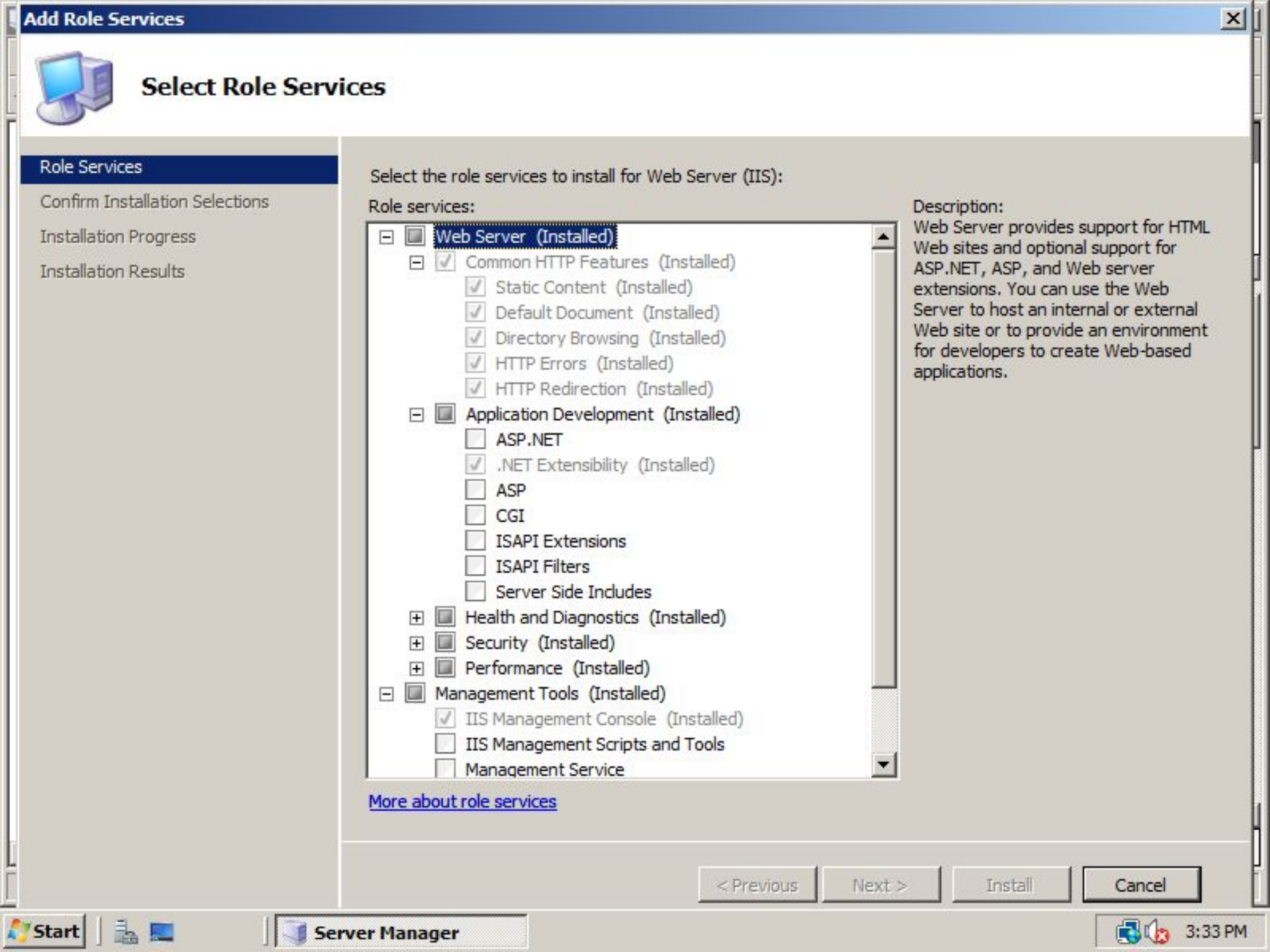
Доменные контроллеры только для чтения

- Возможные проблемы
- Симптомы:
  - Запись в RODC
    - Вызывает ошибку (вызовы RPC и LDAP)
    - Долгие задержки из-за ссылок на контроллер с возможностью записи
- Исправление:
  - Изменение дизайна топологии таким образом, чтобы функции записи не обращались к RODC

Новые или измененные серверные роли

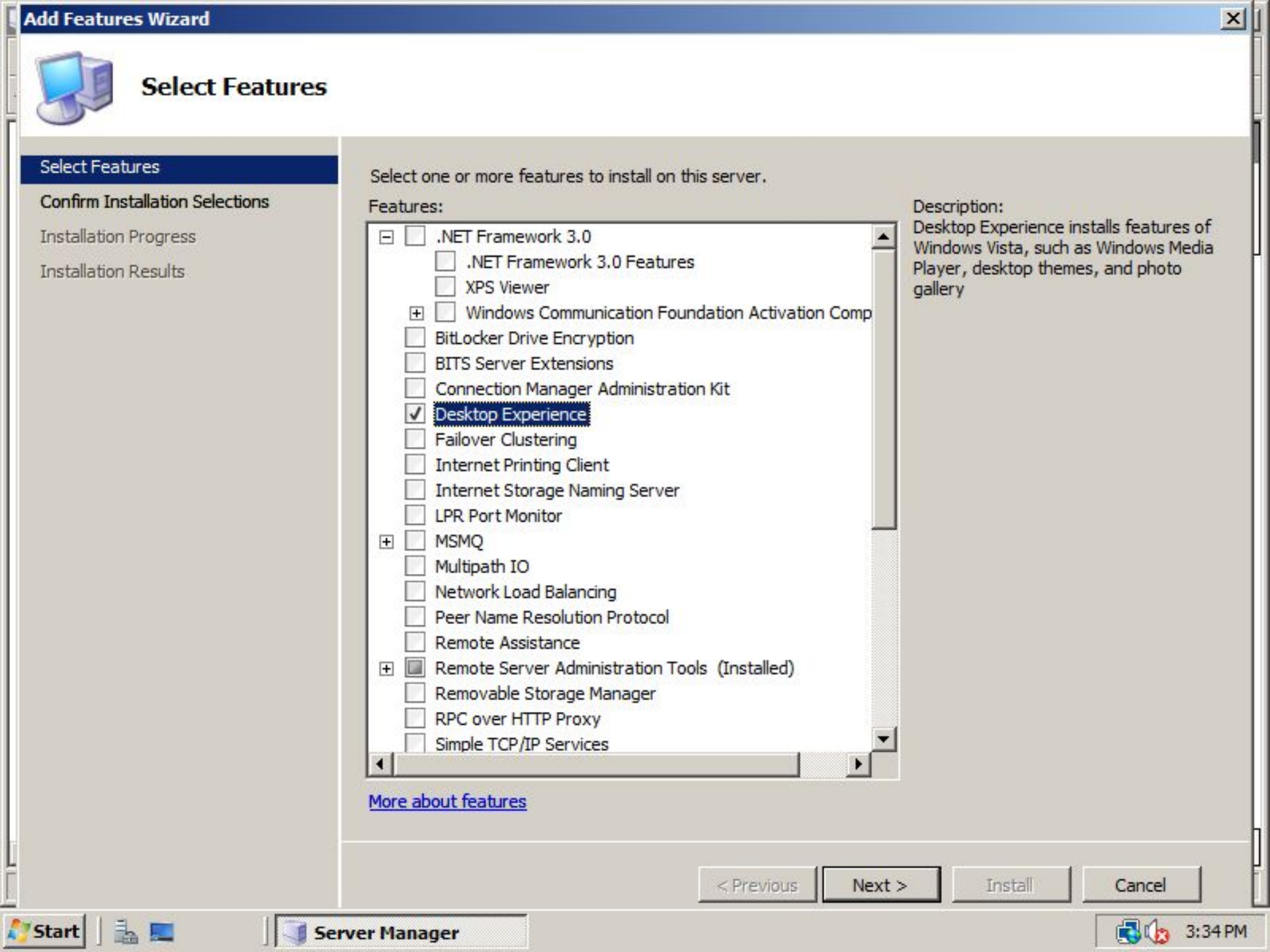
- Полная компонентизация WS2K8
  - Более гранулированные роли
  - По умолчанию роли не активны
  - Роли от предыдущих версий имеют некоторые отличия
  - Программы установки и приложения могут перестать работать, т.к. ожидаемые функции реализованы в новых или измененных ролях
- Из-за этих изменений:
  - После миграции на новую систему необходимо удалить и переустановить приложения
  - Перенос приложений на новую версию не поддерживается


Add Roles Wizard
Select Server Roles
Before You Begin
Select Server Roles
Confirm Installation Selections
Installation Progress
Installation Results
Select one or more roles to install on this server.
Roles:
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server
Fax Server
File Server
Network Policy and Access Services
Print Services
Terminal Services
UDDI Services
Web Server (IIS) (Installed)
Windows Deployment Services
Windows SharePoint Services
Description:
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
More about server roles
< Previous
Next >
Install
Cancel
Start
Server Manager
3:32 PM


Add Role Services
Select Role Services
Role Services
Confirm Installation Selections
Installation Progress
Installation Results
Select the role services to install for Web Server (IIS):
Role services:
Web Server (Installed)
Common HTTP Features (Installed)
Static Content (Installed)
Default Document (Installed)
Directory Browsing (Installed)
HTTP Errors (Installed)
HTTP Redirection (Installed)
Application Development (Installed)
ASP.NET
.NET Extensibility (Installed)
ASP
CGI
ISAPI Extensions
ISAPI Filters
Server Side Includes
Health and Diagnostics (Installed)
Security (Installed)
Performance (Installed)
Management Tools (Installed)
IIS Management Console (Installed)
IIS Management Scripts and Tools
Management Service
Description:
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
More about role services
< Previous
Next >
Install
Cancel
Start
Server Manager
3:33 PM

Компоненты системы

- Desktop Experience Pack
  - Набор приложений, не установленных по умолчанию
  - Отсутствие файлов DirectX/Media
- RPC over HTTP Proxy
- .NET Framework 3.0
- Удаленная поддержка


Add Features Wizard
Select Features
Select Features
Confirm Installation Selections
Installation Progress
Installation Results
Select one or more features to install on this server.
Features:
.NET Framework 3.0
.NET Framework 3.0 Features
XPS Viewer
Windows Communication Foundation Activation Comp
BitLocker Drive Encryption
BITS Server Extensions
Connection Manager Administration Kit
Desktop Experience
Failover Clustering
Internet Printing Client
Internet Storage Naming Server
LPR Port Monitor
MSMQ
Multipath IO
Network Load Balancing
Peer Name Resolution Protocol
Remote Assistance
Remote Server Administration Tools (Installed)
Removable Storage Manager
RPC over HTTP Proxy
Simple TCP/IP Services
Description:
Desktop Experience installs features of Windows Vista, such as Windows Media Player, desktop themes, and photo gallery
More about features
< Previous
Next >
Install
Cancel
Start
Server Manager
3:34 PM

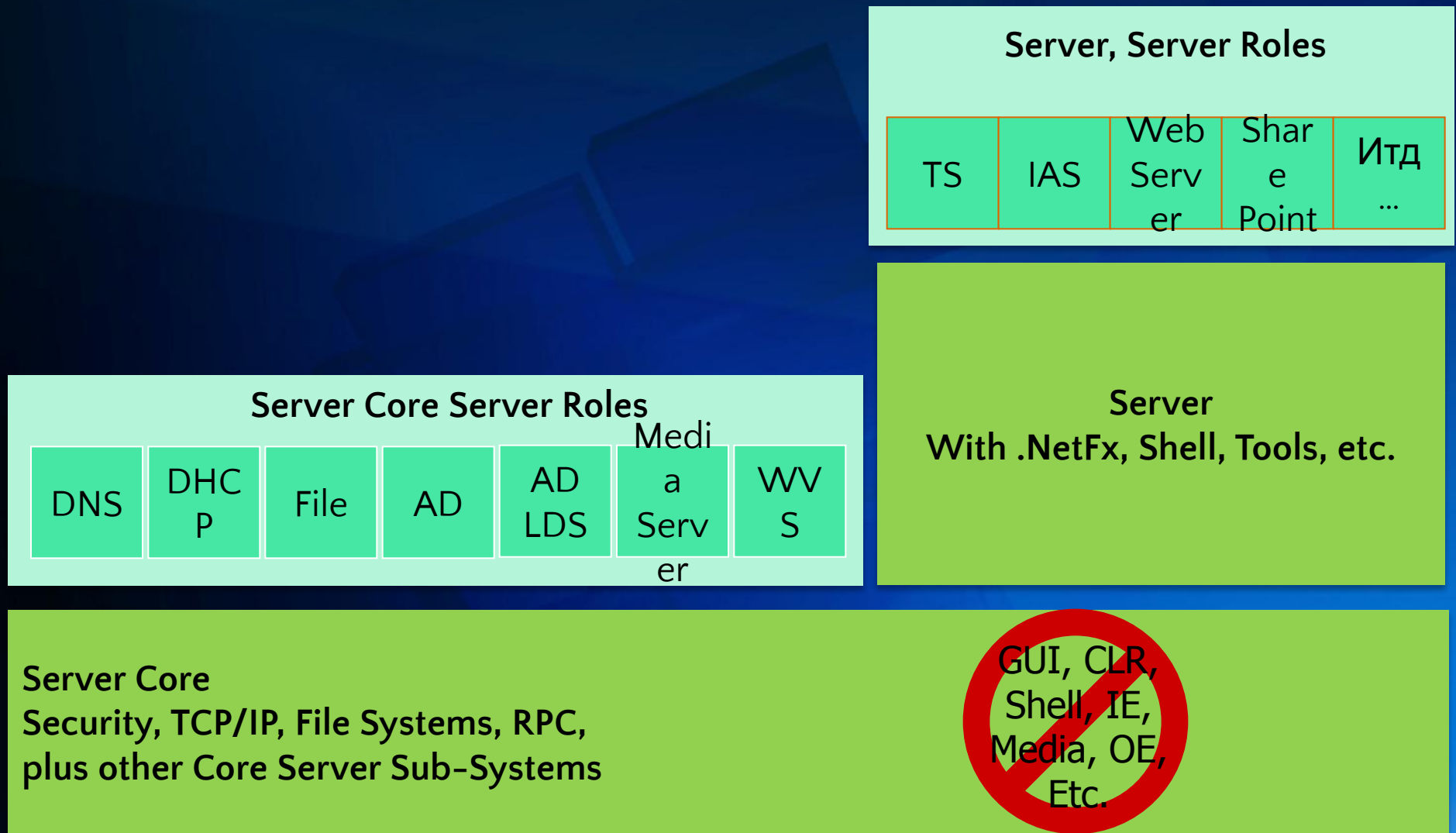
Server Core

- Новинка в Windows Server 2008!
  - Опция минимальной установки для Windows Server 2008
  - Входит в издания Standard, Enterprise и Datacenter
  - Поддерживается на x86 и x64

Server Core

- Включает
  - Фиксированный набор серверных ролей
  - DHCP, File, AD, AD LDS, Media Services, DNS, IIS 7 (минус ASP.Net)
  - Набор дополнительных функций:
    - WINS, Failover Clustering, Subsystem for UNIX-based applications, Backup, Multipath IO, Removable Storage Management, Bitlocker Drive Encryption, SNMP, Telnet Client
  - Интерфейс командной строки, нет графической оболочки
- Снижение области атак
- Базовая функциональность сервера с минимальными требованиями по ресурсам

Server Core – Архитектура



Server Core

- Ограничения
  - Отсутствует Windows PowerShell, минимальный интерфейс – командная строка
  - Отсутствует поддержка управлямого кода – нет .Net Runtime, весь код должен быть только Native Windows API
  - Ограниченная поддержка MSI – только в пакетном режиме
  - Отсутствует поддержка установки приложений
    - Поддержка разработки средств управления, утилит и агентов

Server Core

- Server Core – это не платформа для разработки приложений
  - Требуется отдельное планирование при миграции
- Server Core поддерживает средства управления, утилиты и агентов
- Средства удаленного управления должны работать в большинстве случаев
  - Совет: используйте один из протоколов, поддерживаемых в Server Core, например, RPC

Server Core

- Могут потребоваться изменения для работы агентов под Server Core
  - Требования:
    - Агенты не должны иметь зависимостей от оболочки или GUI
    - Агенты не могут использовать управляемый код
    - Отдельное тестирование агентов под Server Core
  - Советы:
    - В SDK есть список программных интерфейсов, поддерживаемых в Server Core

Отказоустойчивые кластеры

- Новый набор программных интерфейсв
  - Улучшенная функциональность
  - Масштабируемость
  - Управляемость
    - Удаленное управление

Отказоустойчивые кластеры

- Программные изменения
  - В Windows Server 2008 отсутствует Cluster Automation Server (MSClus)
  - Приложения, использующие эти интерфейсы, должны использовать Cluster API или провайдера Cluster WMI
  - Подробно о Cluster Automation Server – см:
    - http://msdn.microsoft.com/library/default.asp?url=/library/en-us/mscs/mscs/programming_with_cluster_automation_server.asp

Отказоустойчивые кластеры

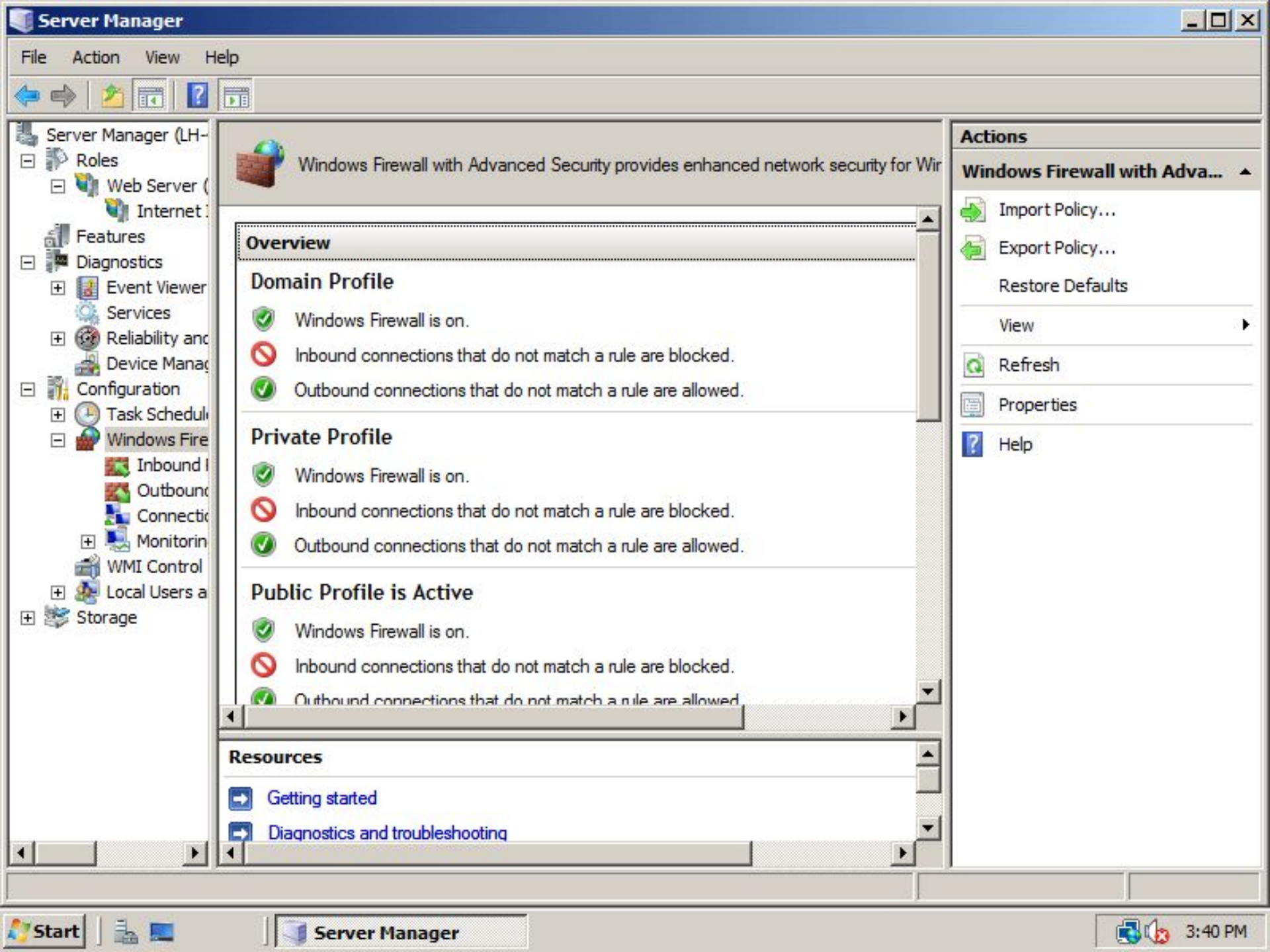
- Новые возможности:
  - Интегрированные средства проверки конфигурации
  - Упрощенная установка кластера
  - Упрощенное управление кластерами
  - Расширения модель Quorum
  - Поддержка Storage Area Networks
  - Расширения в сетевой поддержке
  - Расширения для Stretched Cluster
  - Средства миграции кластеров
  - Поддержка Server Core

Отказоустойчивые кластеры

- Требуется внесение изменений в приложения
  - Приложения должны использовать новые программные интерфейсы
  - Не устанавливайте «старые» приложения на отказоустойчивые кластеры Windows Server 2008
    - Можно получить непредсказуемые результаты

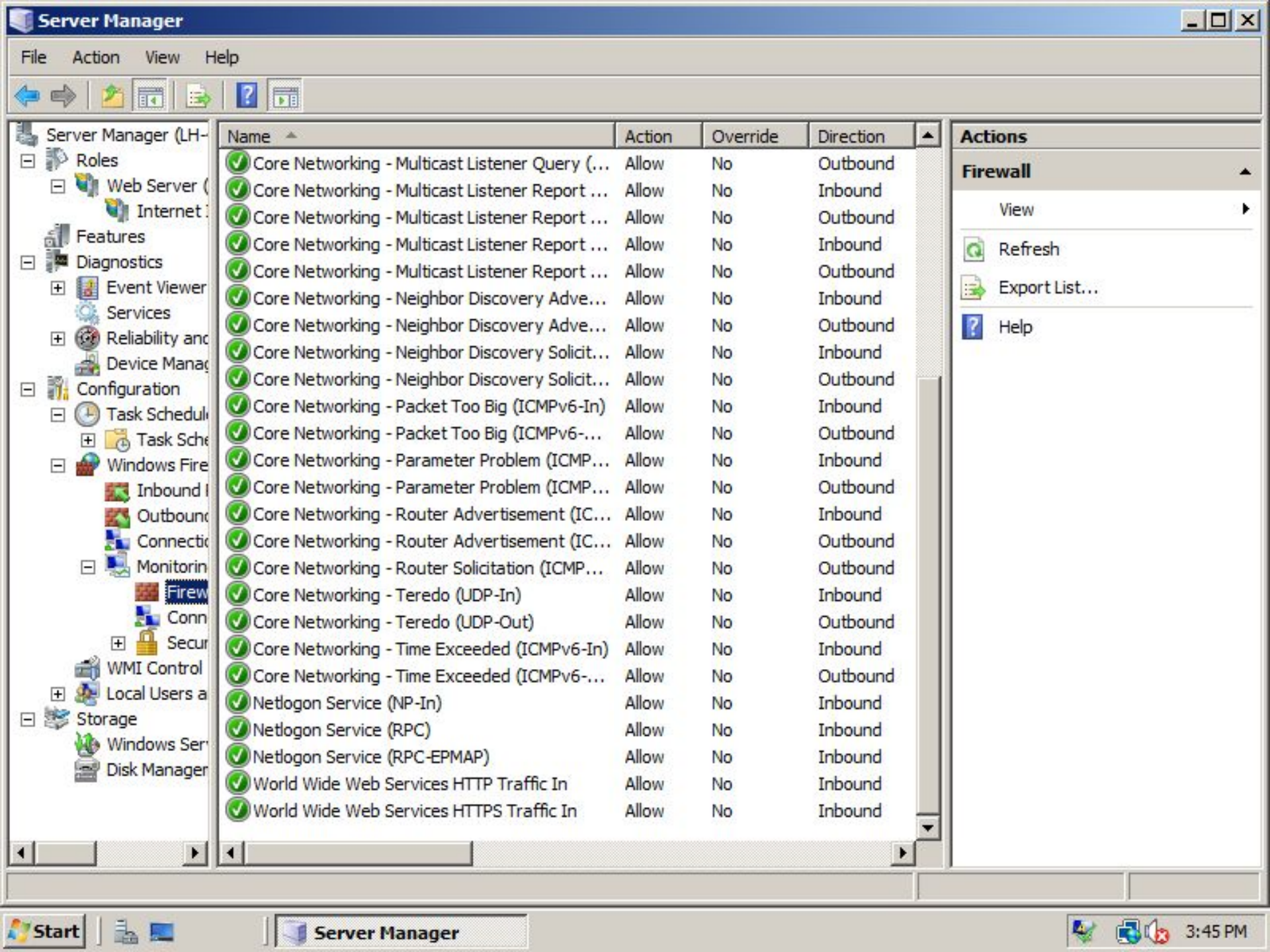
Windows Firewall

- Включен по умолчанию
- Симптомы:
  - Приложения не работают после установки
    - Некоторые порты TCP/IP по умолчанию закрыты
  - Событие аудита безопасности будет занесено в системный журнал – указатель но то, что приложение было заблокировано


Server Manager
File
Action
View
Help
Server Manager (LH-
Roles
Web Server (
Internet I
Features
Diagnostics
Event Viewer
Services
Reliability and
Device Manag
Configuration
Task Schedul
Windows Fire
Inbound R
Outbound
Connectio
Monitorin
WMI Control
Local Users a
Storage
Windows Firewall with Advanced Security provides enhanced network security for Wir
Overview
Domain Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile is Active
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Resources
Getting started
Diagnostics and troubleshooting
Actions
Windows Firewall with Adva...
Import Policy...
Export Policy...
Restore Defaults
View
Refresh
Properties
Help
Start
Server Manager
3:40 PM

Windows Firewall

- Для «старых» приложений администраторы должны открыть требуемые порты
- Возможность отключения Windows Firewall – не рекомендуется
- Администраторы могут использовать:
  - Контекст ‘netsh advfirewall’ для работы с правилами firewall из скриптов
  - Шаблоны мастера Security Configuration для конфигурации серверов
- Разработчики могут использовать программыне интерфейсы INetFwPolicy2 (Firewall APIs) для интеграции инсталляторов с Windows Firewall и Advanced Security


Server Manager
File Action View Help
Server Manager (LH-
Roles
Web Server (
Internet I
Features
Diagnostics
Event Viewer
Services
Reliability and
Device Manag
Configuration
Task Schedul
Task Sche
Windows Fire
Inbound I
Outbound
Connectio
Monitorin
Firew
Conn
Secur
WMI Control
Local Users a
Storage
Windows Ser
Disk Manager
Name
Action
Override
Direction
Core Networking - Multicast Listener Query (... Allow No Outbound
Core Networking - Multicast Listener Report ... Allow No Inbound
Core Networking - Multicast Listener Report ... Allow No Outbound
Core Networking - Multicast Listener Report ... Allow No Inbound
Core Networking - Multicast Listener Report ... Allow No Outbound
Core Networking - Neighbor Discovery Adve... Allow No Inbound
Core Networking - Neighbor Discovery Adve... Allow No Outbound
Core Networking - Neighbor Discovery Solicit... Allow No Inbound
Core Networking - Neighbor Discovery Solicit... Allow No Outbound
Core Networking - Packet Too Big (ICMPv6-In) Allow No Inbound
Core Networking - Packet Too Big (ICMPv6-... Allow No Outbound
Core Networking - Parameter Problem (ICMP... Allow No Inbound
Core Networking - Parameter Problem (ICMP... Allow No Outbound
Core Networking - Router Advertisement (IC... Allow No Inbound
Core Networking - Router Advertisement (IC... Allow No Outbound
Core Networking - Router Solicitation (ICMP... Allow No Outbound
Core Networking - Teredo (UDP-In) Allow No Inbound
Core Networking - Teredo (UDP-Out) Allow No Outbound
Core Networking - Time Exceeded (ICMPv6-In) Allow No Inbound
Core Networking - Time Exceeded (ICMPv6-... Allow No Outbound
Netlogon Service (NP-In) Allow No Inbound
Netlogon Service (RPC) Allow No Inbound
Netlogon Service (RPC-EPMAP) Allow No Inbound
World Wide Web Services HTTP Traffic In Allow No Inbound
World Wide Web Services HTTPS Traffic In Allow No Inbound
Actions
Firewall
View
Refresh
Export List...
Help
Start
Server Manager
3:45 PM

Подготовка к сертификации

1. Принять участие в «**Windows Server 2008 Logo Workshop**»
2. Установить Windows Server 2008 Beta 3/RC0/RCx
3. Получить и изучить «Windows Server 2008 Software Logo Spe
4. Получити
5. Получити
6. Получити Framework
7. Выполнить внутреннее тестирование приложения
8. Передать приложение на пред-тестирование

Успеть к официальному запуску продукта!

Microsoft Платформа 2008

Microsoft®

Your potential. Our passion.™