Грейсон Митчем
Полное руководство по терминальным службам Windows Server 2003

Глава 1: Введение в Windows Server 2003 Terminal Services

В этой книге описываются новые возможности и улучшения WS2K3 Terminal Services. Здесь также будет обсуждаться наилучшая практика настройки и управления терминальными службами с точки зрения новых технологий, доступных системным администраторам в WS2K3. С помощью Remote Desktop Protocol (RDP) 5.2, интерфейса ADSI для доступа к атрибутам объекта пользователя, относящихся к терминальным службам, новых элементов управления групповыми политиками, каталога сеансов, мы можем использовать Terminal Services для решения сложных задач предоставления пользователям рабочих столов на базе терминальных служб.

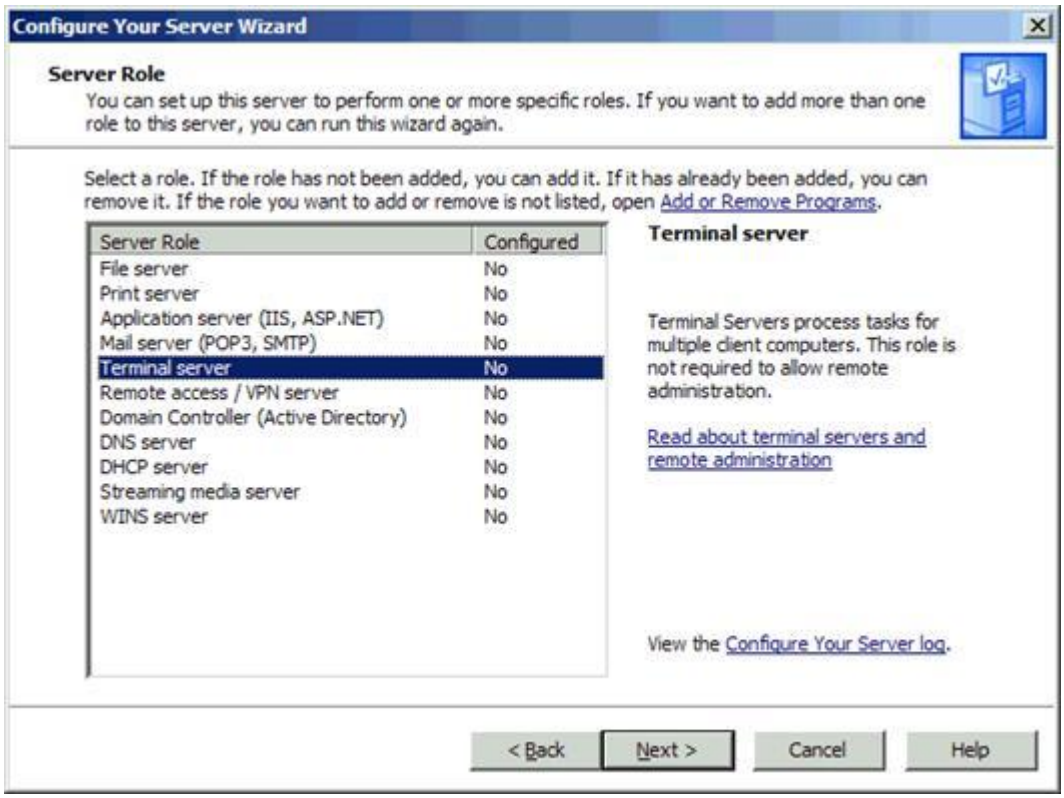
Роли сервера

При установке WS2K3 большая часть второстепенных подсистем не активируется или не устанавливается. Это сделано по причинам безопасности. Поскольку система по умолчанию защищена, системные администраторы могут сосредоточиться на проектировании системы, которая будет выполнять исключительно возложенные на нее функции и ничего лишнего. Для помощи при включении нужных функций, Windows теперь предлагает выбрать роль сервера (Server Role):

Роль - это функция сервера (например, почтовый сервер, контроллер домена). Один сервер может играть несколько ролей. При регистрации администратора на сервере, мастер "Manage Your Server" помогает добавить новые роли и изменять существующие.

При добавлении новой роли, мастер Manage Your Server включает нужные службы и осуществляет необходимые изменения в безопасности. Вы также можете добавлять и удалять службы старым способом - через Add/Remove Windows Components и оснастку Services, но мастер Manage Your Server очень полезен.

После добавления роли, мастер Manage Your Server создает ссылки для доступа к инструментам и настройкам каждой роли.



- **File Server**
  Добавление роли файлового сервера оптимизирует сервер для поддержки общих папок и хранения файлов. После добавления роли файл-сервера, вы сможете назначать пользователям дисковые квоты, использовать службу индексации для поиска файлов и даже делать поиск документов в разных форматах на разных языках, используя в меню Start интрумент Search или новый веб-интерфейс поиска. WS2K3 предлагает массу новых возможностей для улучшения обслуживания файлов:
    - Теневое копирование (Shadow copy) - Резевное побайтовое копирование ранних версий документов, позволяющее пользователям отменять сделанные изменения в документах, хранящихся на сервере.
    - Улучшенная распределенная файловая система DFS - позволяет создавать единое логическое именованное пространство для множества общих папок, расположенных на разных серверах. Теперь пользователям не нужно запоминать, на каких серверах расположены часто используемые ими общие папки. DFS в WS2K3 также предоставляет службу репликации файлов с выбором топологии, что было недоступно в Win2K. Кроме того, серверы WS2K3 могут обслуживать несколько корней DFS.
    - Служба теневого копирования томов (Volume shadow copy service) - Создает копию оригинальных общих данных на заданный момент времени. Программы резервного копирования могут использовать эту копию,чтобы сделать папку общего доступа статической, пока меняются текущие документы. Кроме того, вы можете перемещать теневые копии на другие сервера для резервного хранения,

тестирования и анализа данных
.

- **Print Server**
  Серверы печати используются для предоставления и управления доступом к принтерам. Роль сервера печати позволяет управлять принтерами через веб-броузер, печатать на URL принтера, используя протокол IPP, а также подключать принтеры, используя Point and Print. Microsoft сделала ряд расширений службы печати в WS2K3:
  - Поддержка кластеров печати - автоматичекая репликация драйверов принтеров по всем серверам в кластере.
  - Расширения в Active Directory - Администраторы могут публиковать принтеры в AD, чтобы пользователи могли искать принтеры в зависимости от месторасположения, цвета и скорости.
  - Улучшение безопасности - Включены новые групповые политики, позволяющие администратору предотвращать доступ клиентов к спулеру, если сервер не ослуживает печать.

- **Application Server**
  Когда вы настраиваете сервер в качестве сервера приложений, вы устанавливаете Internet Information Services (IIS) 6.0 и целый ряд компонентов, например, COM+ и ASP.NET. Microsoft оптимизировала IIS 6.0 с точки зрения стабильности, управляемости, быстрой разработки приложений и безопасности.
  Роль сервера приложений WS2K3 обеспечивает поддержку новых веб-служб и платформы .NET, включая службы Universal Description, Discovery and Integration (UDDI), а также Simple Object Access Protocol (SOAP) и Web Services Description Language (WSDL). Серверы приложений часто конфигурируют включая следующее:
  - Слияние ресурсов (Resource pooling)
  - Управление распределенными транзакциями
  - Встроенная защита
  - Отказоустойчивость

- **Mail Server**
  WS2K3 теперь включает серверы POP3 и SMTP. Это позволяет обслуживать базовые почтовые ящики ваших пользователей и позволяет принимать и отправлять почту с сервера. Почтовые серверы обеспечивают прием и отправку почты. Входящая почта может хранится на сервере, а потом забираться пользователем по протоколу POP3. Для роли почтового сервера вы должны иметь:
  - Активное соединение с интернет
  - Зарегистрированное доменное имя
  - Запись MX у провайдера для вашего почтового домена

- **Terminal Server**
  После инсталляции роли терминального сервера, вы можете разрешить пользователям подключаться к серверу и запускать на нем приложения так, как будто эти приложения были инсталлированы на рабочей станции клиента. Мы рассмотрим установку, конфигурирование и новые возможности терминального сервера позже. В отличие от Win2K, которая автоматически разрешает пользователям доступ после установки Terminal Services, WS2K3 ограничивает доступ только администраторами. Вы должны добавить пользователей или их группы в группу Remote Desktop Users.

- **Remote Access/VPN Server**
  Серверы удаленного доступа и VPN предоставляют точку входа в вашу сеть для удаленных пользователей. Используя роль *Remote Access/VPN Server*, вы можете реализовать протоколы маршрутизации для сред LAN и WAN. Эта роль поддерживает модемные соединения и VPN через интернет.

- **Domain Controller**
  Контроллер домена содержит базу данных Active Directory. Контроллеры домена предоставляют службы аутентификации для пользователей и компьютеров, а также управляют доступом к сетевым ресурсам. Роль контроллера домена заменяет инструмент DCPROMO, который был в Win2K. Эта роль позволяет добавить контроллер домена к существующему домену, создать новый домен, создать новое дерево.

- **DNS Server**
  Служба DNS позволяет преобразовывать доменные имена (FQDN) в адреса IP. Версия DNS в WS2K3 включает службу динамического DNS (DDNS), которая позволяет компьютерам самим регистрироваться в базе данных DNS. Версия DNS в WS2K3 также позволяет интергрировать DNS с WINS.

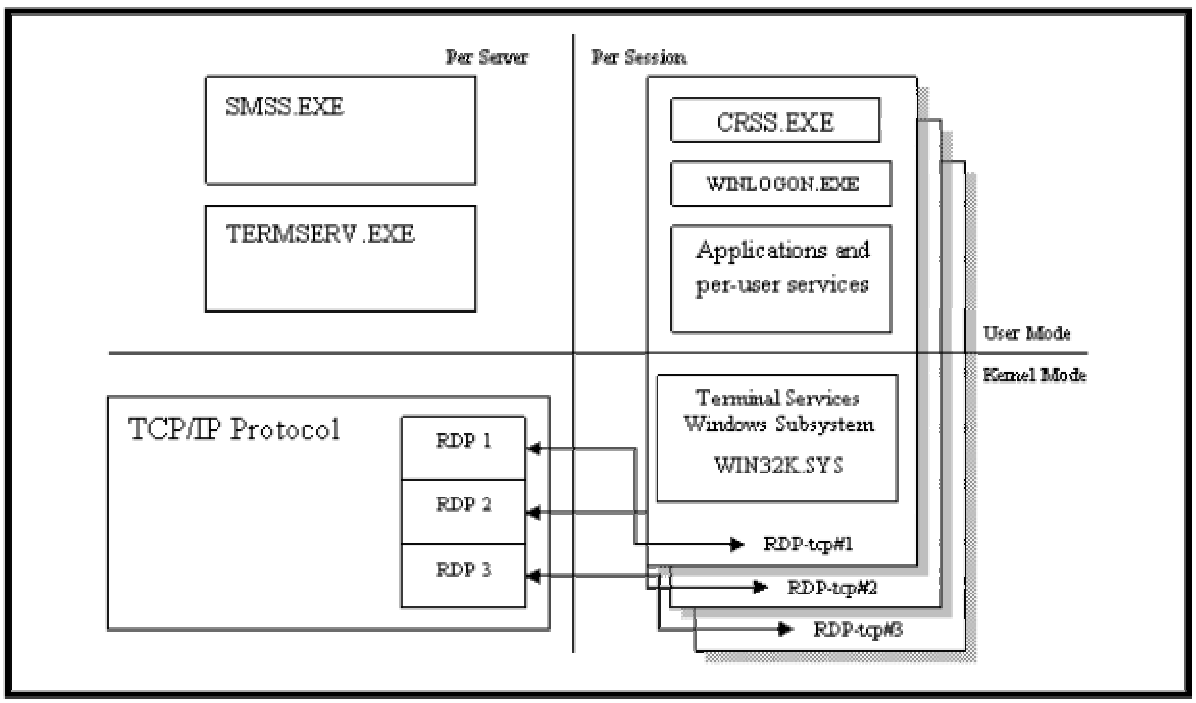
- **DHCP Server**
  Сервер DHCP позволяет клиентам получать свой IP по мере необходимости. Сервер DHCP также предоставляет дополнительную информацию для конфигурации сети - адрес серверов DNS, WINS и т.п.

- **Streaming Media Server**
  Потоковый сервер предоставляет службы Windows Media Services сетевым клиентам. Windows Media Services используются для управления и доставки мультимедийного контента - потокового видео и аудио - через интранет или интернет.

- **WINS Server**
  WINS позволяет клиентам NetBIOS преобразовывать имена компьютеров в адреса IP. В отличие от DNS, требующего доменные имена, WINS спроектирована для внутренней интрасети для разрешения простых имен NetBIOS.
  Хотя можно иметь сеть Windows без NetBIOS и WINS, многие утилиты все еще зависят от базы данных WINS. Многие типы записей, имеющиеся в WINS, отсутствуют в DNS. Эти типы позволяют легко находить в сети серверы, выполняющие специфические службы (включая Terminal Services). Такой утилитой является Terminal Server Administration. Без WINS вам придется вручную указывать сервер для управления.

Технология Terminal Services

Что такое терминальный сервер? Windows спректирована как однопользовательская операционная система, т.е. в один и тот же момент времени в ней может интерактивно работать только один пользователь. Служба Terminal Services ломает эту модель, внедряя между слоями системы и пользователя слой сеанса. Session Manager для каждого сеанса создает отдельный экземпляо подсистемы Win32, WIN32K.SYS. Затем Session Manager внутри сеанса запускает рабочий процесс подсистемы клиент-сервер, CRSS.EXE, и службу входа WINLOGON.EXE, как показано на следующем рисунке.



Этот процесс позволяет нескольким пользовательским сеансам параллельно выполняться на одной системе Windows. Session Manager работает аналогично распорядителю в ресторане - он провожает новых посетителей (клиентов) к их столикам (сеансам), а затем дает указания персоналу (приложениям, службам и ресурсам) обслужить стол. Session Manager присваивает каждому сеансу уникальный идентификатор (ID) и адресное пространство.

Еще одним важным компонентом Terminal Services является протокол RDP, который позволяет пользователям взаимодействовать с сеансами, выполняющимся на терминальном сервере. Без RDP каждому пользователю потребовалась бы консоль, непосредственно подключенная к серверу.

RDP функционирует как виртуальный дисплей, клавиатура и мышь на сервере. Вместо того, чтобы посылать видеовывод в порт VGA, терминальный сервер перенаправляет его в видеоканал стека RDP. Это позволяет передавать видеоинформацию по сети и отображать ее на экране рабочей станции клиента. RDP также принимает нажатия клавиш и перемещения мыши удаленного клиента и передает их на терминальный сервер, который обрабатывает их так, как будто они происходили от локальных клавиатуры и мыши.

Используя Terminal Services, вы можете инсталлировать приложения на небольшом количестве серверов, а не на сотнях рабочих станций. Вы также можете получить выгоду от использования недорогих "тонких клиентов", чем от рабочих станций. Даже если вам необходимо иметь персональные компьютеры для пользователей, вы все равно можете получить выгоду от использования терминальных серверов за счет централизации сетевого траффика.

Многие компании также используют терминальные серверы для удаленного доступа. Это позволяет закрыть большую часть сети и разрешить удаленные соединения с лишь с отдельными серверами. На таких серверах легко можно поддерживать последние пакеты обновлений, антивирусы и пр.

Новые ответы на старые вопросы

Если вы уже знакомы с современными терминальными серверами, то уже сталкивались с проблемами, связанными с ними - конфигурация учетных записей пользователей, управление перемещаемыми профилями, распределение нагрузки, настройка протоколов, управление печатью. В WS2K3 многие из этих задач существенно упрощены.

Remote Desktop

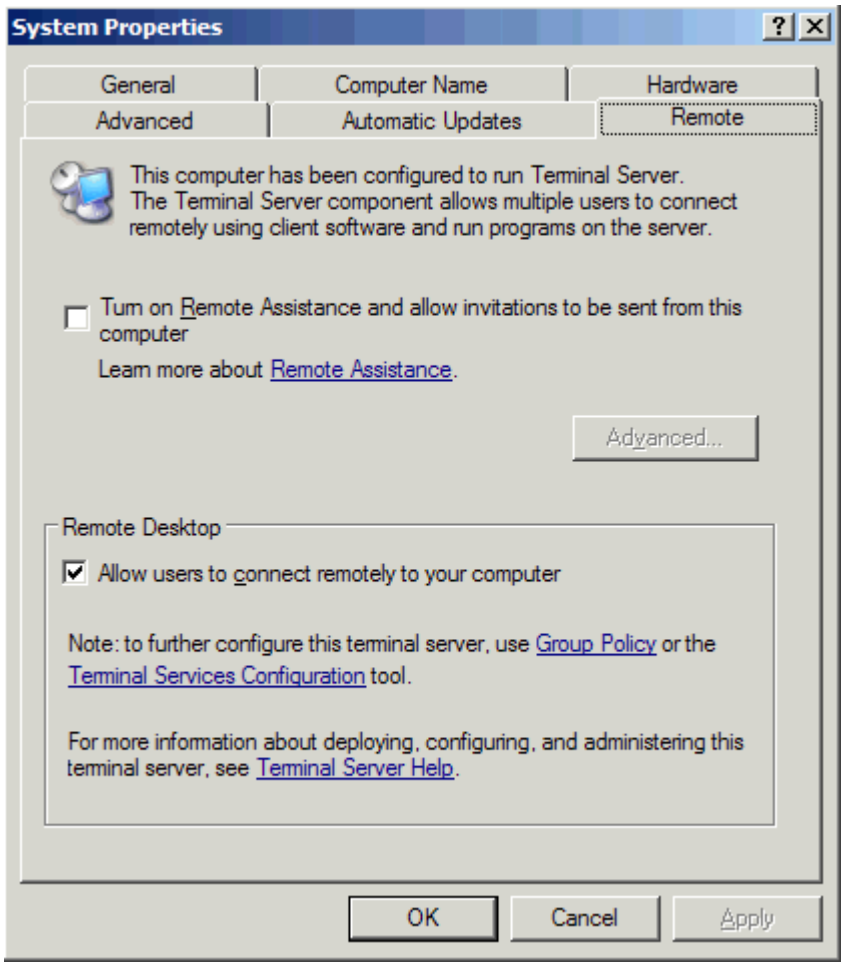
Первое изменение, которое бросается в глаза, состоит в устранении режима Remote Administration. В Win2K этот режим разрешал два удаленных сеанса для системного администрирования. Эта терминология сбивала с толку администраторов, поскольку включение Terminal Services не обязательно делало сервер терминальным сервером. Кроме того, Remote Administration Mode заставляла сервер регистрироваться в WINS и появляться в утилите Terminal Server Administration. Это поведение затрудняло поиск терминальных серверов Win2K.

Но не пугайтесь. Вы можете удаленно администрировать серверы WS2K3. Однако, вместо установки Terminal Services вы просто включаете Remote Desktop. Если вы используете Windows XP, то уже знакомы с Remote Desktop. В WS2K3, Remote Desktop позволяет создать два виртуальных сеанса RDP, а также удаленное подключение к консольному сеансу сервера (этого требовали многие администраторы Win2K). Кроме того, в отличие Remote Administration Mode в Win2K, WS2K3 Remote Desktop препятствует появлению сервера в списке утилиты Terminal Server Administration.

Чтобы сервер с Remote Desktop был виден в Terminal Server Administration, измените в реестре значение TSAdvertise с 0 на 1 в следующем ключе: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server.

Для включения Remote Desktop откройте System Control Panel, выберите вкладку *Remote* и установите флажок *Allow users to remotely connect to your computer*. По умолчанию удаленное соединение разрешено только локальным администраторам, но вы можете добавить

пользователей в группу *Remote Desktop Users*. Учтите, что включение Remote Desktop не активирует систему совместимости приложений, поэтому приложения могут работать некорректно.



Microsoft добавила возможность подключаться и удаленно управлять консольным сеансом. Для подключения к консольному сеансу вы можете либо использовать Remote Desktop Administration, либо запустить клиента Remote Desktop Connection с опцией /console. Для удаленного управления консольным сеансом используйте Terminal Server Administration.

Для быстрого установления удаленного управления консоли сервра, к которому вы подключены через RDP, запустите с командной строки:
```
SHADOW 0
```

Режимы совместимости

Как и Win2K, WS2K3 предлагает два режима совместимости для Terminal Services: Полная безопасность (Full Security) и Ослабленная безопасность (Relaxed Security). Режимы совместимости позволяют выполнять старые приложения, которые не могут работать в условиях более строгих ограничений на файловую систему и реестр со стороны WS2K3

Улучшения в протоколе RDP 5.2

Самое большое количество изменений в WS2K3 Terminal Services сделано в RDP. Теперь он поддерживает некоторые новые возможности перенаправления ресурсов. Новые расширения значительно приблизили RDP к протоколу Citrix ICA.

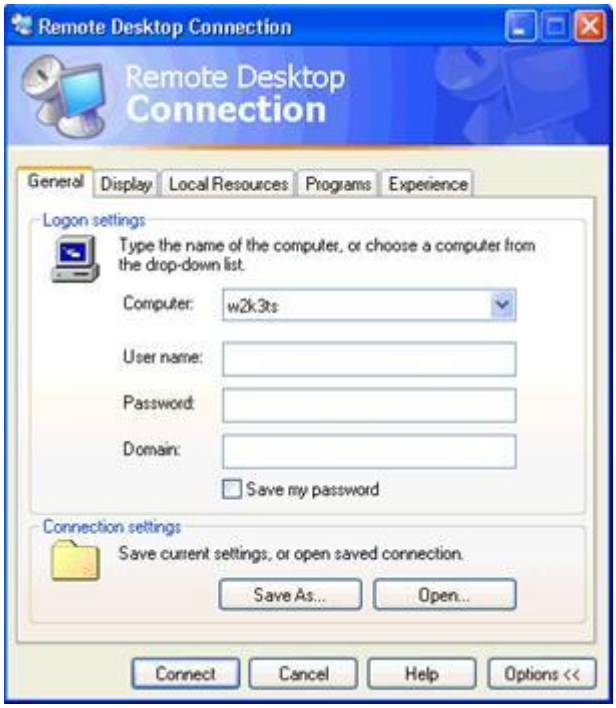
Теперь можно переназначать драйвы клиентов, аудио, буфер обмена, порты, часовые пояса, клавиши Windows (например, ALT+TAB). RDP 5.2 даже поддерживает аутентификацию с помощью смарт-карт. Все эти функции включаются и отключаются администратором. RDP 5.2 добавляет поддержку 24-разрядного цвета и разрешение экрана до 1600x1600.

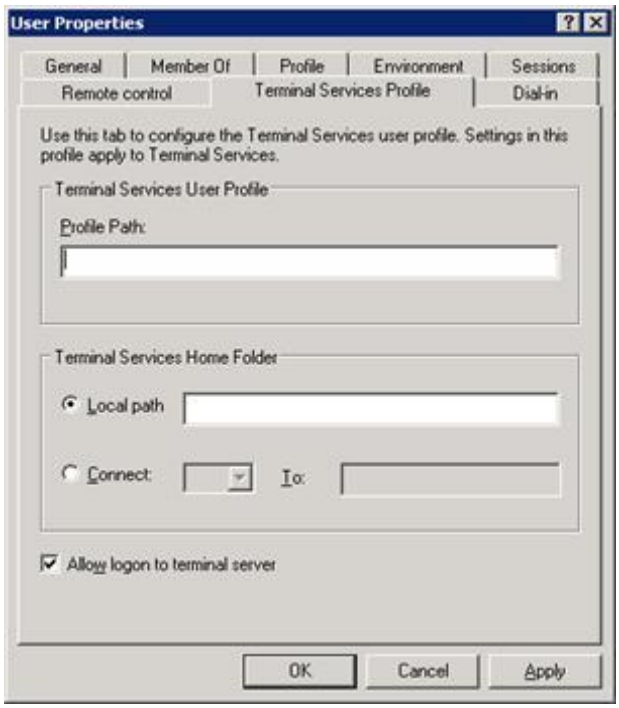
Функция	RDP 5.2	ICA
Отображение драйва клиента	Автоматически подключается ко всем локальным и сетевым драйвам клиента	Автоматически подключается ко всем локальным драйвам клиента
Отображение буфера обмена	Автоматически	Автоматически
Теневые сеансы	Есть	Есть
Отображение локальных принтеров клиента	Автоматически	Автоматически
Отображение сетевых принтеров клиента	Автоматически	Автоматически
Смарт-карты	Есть	Есть
Восстановление разъединенных сеансов	Автоматически	Автоматически
Звук	Есть	Есть
Шифрование	До 128 bit	До 128 bit
Сжатие	Автоматически	Автоматически
Отображение временных зон	Есть	Есть
Клавиши Windows	Автоматически	Требует альтернативных комбинаций клавиш
Отображение последовательных и параллельных портов клиента	Автоматически	Автоматически
Поддерживаемые ОС клиента	Win32, Win16, Windows CE, CE.NET, PocketPC, Macintosh	Win32, Win16, Windows CE, PocketPC, MS-DOS, UNIX, Macintosh, Linux, Java
Протокол передачи	TCP/IP	TCP/IP, IPX/SPX, NetBEUI
Seamless Windows	Нет	Автоматически

Клиент Remote Desktop Connection

Remote Desktop Connection - это новый клиент для RDP 5.2. Remote Desktop Connection поддерживает все новые возможности RDP 5.2. Он устраняет необходимость в Connection Manager и больше не хранит данные о соединениях в реестре. Вместо этого, Remote Desktop Connection поддерживает файлы RDP - текстовые файлы, содержащие информацию о параметрах соединений к терминальному серверу или к Windows XP Remote Desktop. С помощью файлов RDP можно легко распространять или централизованно хранить общую информацию о соединениях для ваших пользователей.

С помощью интерфейса Remote Desktop Connection вы можете управлять опциями соединения (см. рисунок ниже). Новая опция Experience позволяет включить или отключить интерфейс Aqua в Windows XP и WS2K3 - обои, темы и анимацию меню - чтобы повысить производительность на низкоскоростных соединениях.





Конфигурация через групповые политики

В WS2K3 вы можете централизованно настраивать и управлять всеми параметрами Terminal Services посредс помощью групповых политик:

Доступ к параметрам пользователя через ADSI

В Win2K с комадной строки для объекта пользователя был доступен единственный атрибут - Terminal Services Profile Path; для доступа к другим атрибутам требовался TSPROF. WS2K3 предоставила доступ ко всем атрибутам через ADSI. Используя Windows Script Host (WSH) и ваш любимый скриптовый язык, вы можете легко конфигурировать пользовательские терминальные настройки. Вот список доступных атрибутов:

```
objUser.ConnectClientDrivesAtLogon
objUser.ConnectClientPrintersAtLogon
objUser.DefaultToMainPrinter
objUser.TerminalServicesInitialProgram
objUser.TerminalServicesWorkDirectory
objUser.TerminalServicesProfilePath
objUser.TerminalServicesHomeDirectory
objUser.TerminalServicesHomeDrive
objUser.AllowLogon
objUser.MaxDisconnectionTime
objUser.MaxConnectionTime
objUser.MaxIdleTime
objUser.BrokenConnectionAction
objUser.ReconnectionAction
```

Каталог сеансов

При использовании в качестве терминального сервера WS2K3 Enterprise Edition в среде с балансировкой нагрузки, вы можете использовать новую службу Session Directory для предоставления единой точки входа в ферму терминальных серверов. Session Directory выступает не только в роли распределителя нагурзки, но также поддерживает базу данных активных сеансов в ферме. Это позволяет пользователю возобновить разъединенный сеанс на том же сервере, от которого он отключился.

Лицензирование терминальных служб

Чтобы терминальный сервер продолжал принимать соединения по истечении 120 дней, вы должны сконифгурировать Terminal Services Licensing. WS2K3 добавляет новые опции и новые уровни сложности к лицензированию Terminal Services. Для подключения к WS2K3 клиентам понядобятся новые маркеры лицензий WS2K3. Эти маркеры (tokens) выдаются только сервером WS2K3 Terminal Services License - серверы лицензий Win2K не могут выдавать новые маркеры WS2K3. Поэтому если в вашей среде уже есть сервер лицензий Win2K, вам нужно как можно быстрее обновить его до WS2K3 или активировать отдельный сервер лицензий WS2K3.

Компоненты лицензирования Terminal Server

Лицензирование Terminal Services включает в себя Microsoft Clearinghouse, один или несколько серверов WS2K3 Terminal Services Licensing и один или несколько терминальных серверов. Вы используете Microsoft Clearinghouse (через интернет, Web или по телефону) для активирования серверов лицензий и для получения пакетов лицензий, которые инсталлируются на серверах лицензирования.

Сервер Terminal Services Licensing может быть сервером WS2K3 любой редакции с инсталлированной службой Terminal Services Licensing. Terminal Services Licensing хранит все маркеры CAL и следит за маркерами, которые были выданы компьютерам или пользователям. Все терминальные серверы должны иметь возможность связаться с сервером Terminal Services Licensing для выдачи постоянных маркеров. Если сервер лицензирования не активирован, он будет выдавать только временные лицензии.

Терминальный сервер - это сервер WS2K3 любой редакции с инсталлированной ролью Terminal Server. При подключении клиента к терминальному серверу, сервер определяет, требуется ли выдать клиенту маркер лицензии. Если да, то он обращается к серверу лицензий и запрашивает у того маркер от лица клиента, а затем передает маркер клиенту. При первом подключении клиента, если используется модель лицензирования "на устройство" (per-device), клиент получает временный маркер. Временные лицензии хранятся на сервере Terminal Services Licensing в течении 90 дней. Только при втором подключении (в течении 90 дней) для устройства выдается постоянная лицензия.

Термин "постоянный" не совсем правильный, поскольку лицензия на устройство истекает через случайное число дней (от 52 до 89). Это сделано затем, что если устройство больше не

используется для доступа к терминальному серверу (или переинсталлирована ОС), лицензия возвращается назад. Впервые это реализовано в Win2K Service Pack 3 (SP3).

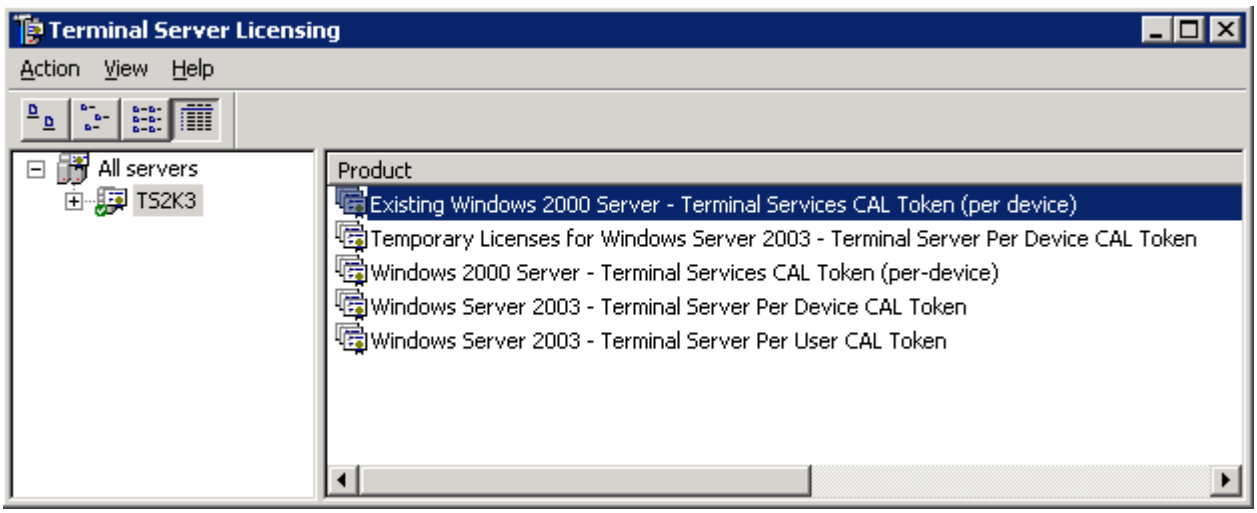
Типы лицензий

WS2K3 Terminal Services Licensing может поддерживать семь типов маркеров лицензий. Помимо CAL, необходимых для подключения к терминальным серверам Win2K, есть четыре новых типа CAL, специфичных для WS2K3 Terminal Services

Встроенных лицензий для WS2K3 Terminal Services больше не существует. Вам необходимо покупать CAL для всех устройств или пользователей, подключающихся к таким серверам, независимо от используемой операционной системы клиента.

- WS2K3 Terminal Server Device CAL - Эти лицензии запрашиваются у сервера лицензий терминальными серверам WS2K3, лицензируемыми в режиме "Per Device"
- WS2K3 Terminal Server User CAL - Для терминальных серверов WS2K3, лицензируемых в режиме "Per User"
- Лицензии WS2K3 Terminal Server External Connector - Эти лицензии разрешают неограниченное число соединений внешних пользователей к терминальному серверу. Эти лицензии еще не доступны.
- Win2K Terminal Services CAL - Терминальные серверы Win2K запрашивают эти лицензии у сервера лицензий для клиентов, выполняющих ОС, отличную от Win2K Professional или Windows XP. Эти лицензии нужны только если у вас есть серверы Win2K.
- Лицензии Win2K Terminal Services Internet Connector - Эти лицензии разрешают до 200 одновременных соединений к терминальному серверу Win2K через интернет для не-сотрудников вашей организации.
- Встроенные лицензии Win2K - Клиенты, выполняющие Win2K Pro или Windows XP получают маркер лицензии из встроенного пула маркеров лицензий при подключении к терминальному серверу Win2K.

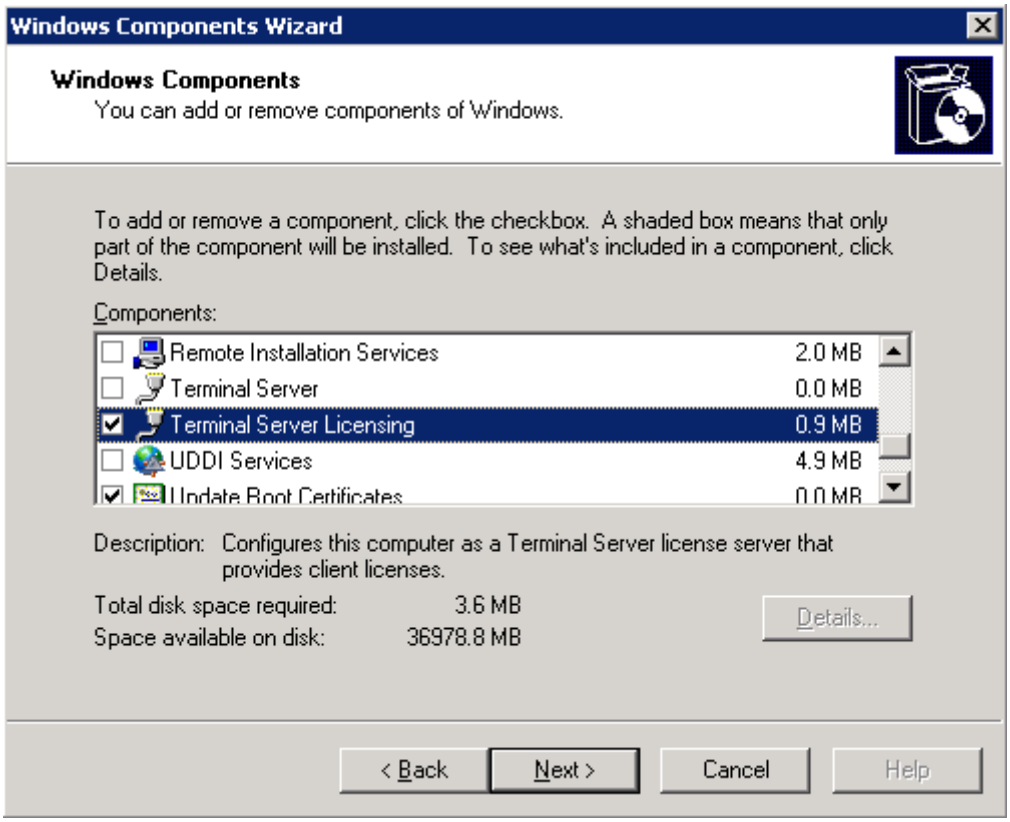
На следующем рисунке показаны лицензии, доступные в Terminal Server Licensing. Обратите внимание, что лицензии для пользователей обрабатываются отдельно от лицнзий для устройств. Пользовательские лицензии - новые в WS2K3. Теперь терминальные серверы можно перевести в режим лицензирования *Per Device* или *Per User*. Один сервер Terminal Services Licensing может обслуживать разные маркеры в любой комбинации, если установлены соответствующие лицензии.



Инсталляция Terminal Server Licensing

Если у вас несколько серверов, то Terminal Server Licensing следует установить на сервере, отличном от терминального. Если вы используете домены, то должны установить службу лицензирования на контроллере домена.

Для установки Terminal Server Licensing, откройте в панели управления апплет *Add/Remove Programs*, выберите *Add/Remove Windows Components*. В мастере установки компонентов выберите *Terminal Server Licensing* .



Если вы устанавливаете Terminal Server Licensing на сервер в AD, вы можете выбрать один из вариантов установки: *Domain/Workgroup* и *Enterprise*. Эти режимы определяют, как служба лицензирования будет оповещать о себе для терминальных серверов. Если вы находитесь в рабочей группе или домене, отличном от AD, опция *Enterprise* будет недоступна.

Я объясню процесс обнаружения в следующем разделе, а пока вы должны понять, что сервер лицензирования *Enterprise* будет обнаруживаться терминальными серверами из любого доверительного домена, но только в пределах того же сайта AD, что и сервер лицензирования.

После установки Terminal Server Licensing, сервер лицензирования необходимо активировать, обратившись в Microsoft Clearinghouse. Запустите утилиту администрирования Terminal Server Licensing из меню Start, щелкните правкой кнопкой мыши на сервере и выберите *Activate Server*. Появится мастер активации сервера лицензирования:

- *Automatic connection* - Это самый простой метод активации. Он требует, чтобы сервер Terminal Server Licensing имел подключение к интернет через порт 443 (SSL). Заполните информацию о компании и щелкните *Activate*.

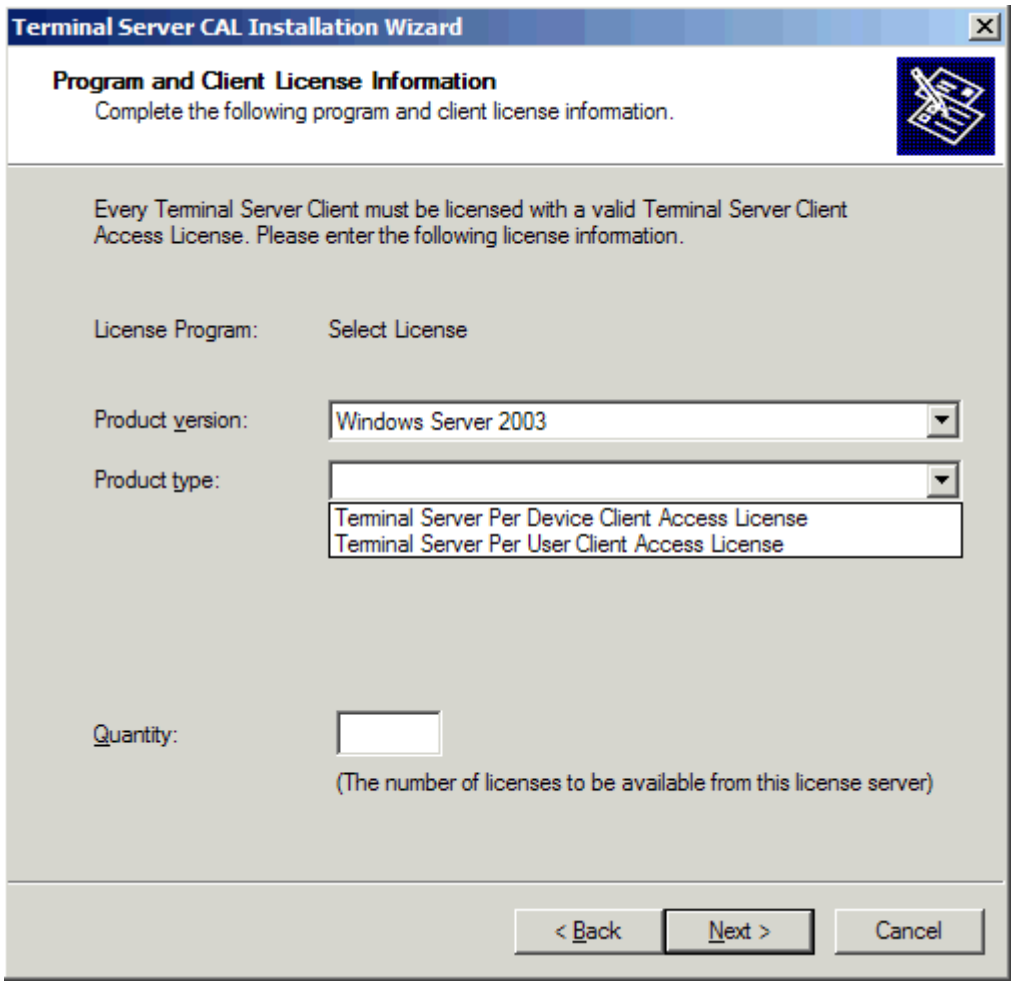
- *Web Browser* - Если сервер Terminal Server Licensing не подключен к интернет, вы все равно можете активировать сервер через веб с другого компьютера. Для этого откройте в веб-броузере сайт https://activate.microsoft.com, заполните информацию о компании, а также укажите уникальный идентификатор Terminal Server Licensing ID, который формирует мастер активации. Веб-сервер даст код активации, который вы должны ввести в службу лицензирования.

- *Telephone* - Если у вас вообще нет интернета, то позвоните в Microsoft Clearinghouse по телефону. Выберите вашу страну в мастере активации, и вы получите номер телефона. Сообщите службе поддержки имя компании, контакную информацию, идентификатор сервера, и вам сообщат код активации. Активируйте сервер во время разговора по телефону или очень внимательно запишите код на бумаге.

После активации сервера лицензирования он немедленно начинает выдавать временные лицензии для серверов Win2K и WS2K3, которые дают администратору 90-дневный период, в течении которого необходимо установить постоянные CAL на сервер лицензирования.

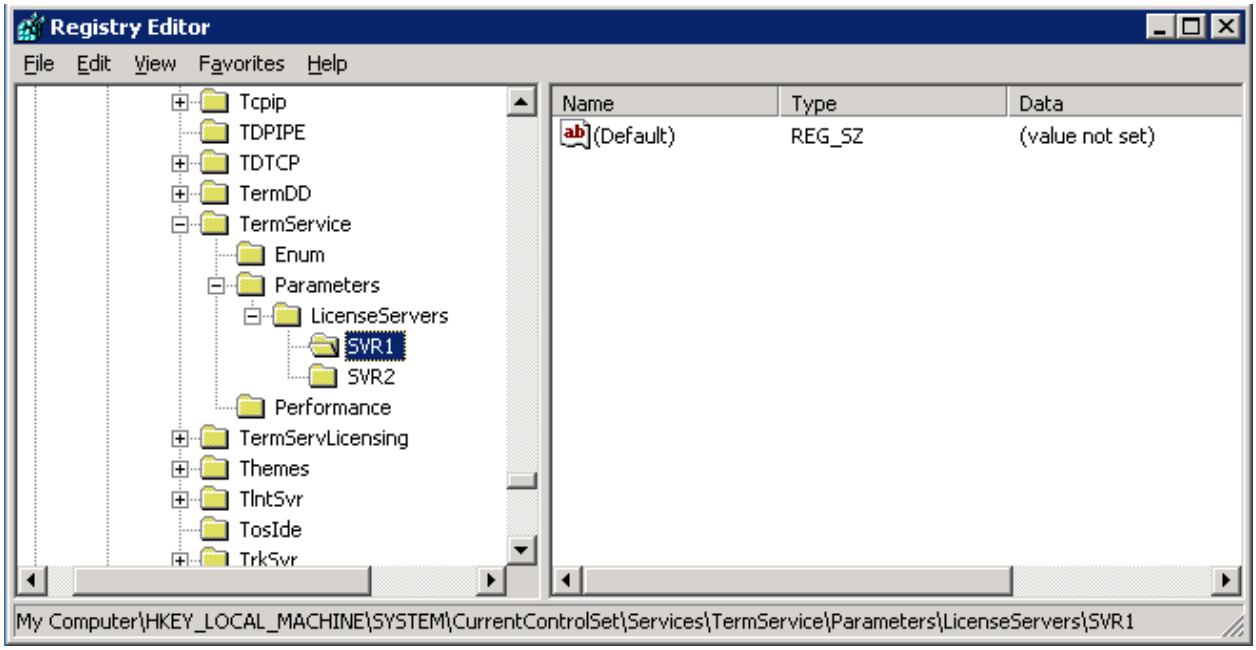
Если вы обновляете сервер Win2K с установленной службой Terminal Server Licensing до WS2K3, вам необходимо повторно активировать службу лицензирования. Для этого выберите *Re-Activate Server* в Advanced в меню Actions в утилите администрирования Terminal Server Licensing

Для добавления пакета лицензий, щелкните правой кнопкой в утилите администрирования Terminal Server Licensing и выберите *Install Licenses*. Вам будет представлен тот же выбор, как при активации сервера. Если вы устанавливаете розничные лицензии, этот тип лицензий будет выбран автоматически. Однако, если вы устанавливаете лицензии через Select, Open или другие соглашения Microsoft, то вам следует выбрать тип добавляемой лицензии:



Обнаружение сервера лицензирования

При запуске терминального сервера, он пытается найти сервер лицензирования. Метод поиска зависит от среды сервера и режима работы сервера лицензирования. Вы можете переопределить процесс обнаружения, явно указав в реестре серверы лицензирования. В Win2K вы могли указать только один сервер лицензирования, а WS2K3 позволяет указать несколько. Добавьте подключи в ключ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService\Parameters\LicenseServers. Каждый подключ должен быть назван по имени сервера лицензирования.



Если вы не укажите явно серверы лицензирования в реестре, то процесс их нахождения работает следующим образом: терминальные серверы в рабочей группе или в домене, отличном от AD, посылают широковещательные запросы mailslot. Соответственно, таким образом могут быть обнаружены только серверы, находящиеся в той же подсети.

Терминальные серверы AD сначала ищут серверы лицензирования в режиме лицензирования Enterprise. Для этого они делают запрос LDAP в поиске записи CN TS-Enterprise-License-Server, указывая свой сайт. Затем терминальный сервер обращается к каждому контроллеру домена в сайте в поиске доменного сервера лицензирования. Наконец, терминальный сервер будет обращаться ко всем контроллерам в своем домене.

После обнаружения терминальный сервер кеширует все найденные серверы лицензирования в реестре в ключах:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSLicensing\Parameters\EnterpriseServerMulti и
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSLicensing\Parameters\DomainLicenseServerMulti.

Важно заметить, что если найдены корпортивный (Enterprise) и доменный серверы лицензирования, то терминальный сервер всегда предпочтет использовать доменный сервер, даже если для этого необходимо перейти границы сайта. Если ни одного сервера лицензирования не найдено, терминальный сервер будет продолжать процесс поиска каждый час. Как только обнаружен один или несколько серверов лицензирования, процесс обнаружения не повторяется до тех пор, пока в реестре доступны данные о кешированных серверах.

Назначение лицензий

Всякий раз при подключении клиента к терминальному серверу, последний обращается к серверу лицензирования для подтверждения существующей лицензии или выдачи новой лицензии. Тип лицензии, который выдает терминальный сервер, зависит от режима лицензирования - Per Device или Per User. Вы можете установить режим в утилите Terminal Services Configuration или групповыми политиками. По умолчанию используется режим Per Device, но если вы обновили терминальный сервер Win2K, который был в режиме Internet Connector, то режим лицензирования будет Per User.

Чтобы поддерживать маркеры лицензий как Per User, так и Per Device, терминальный сервер должен быть в режиме Per User.

Для каждого соединения клиента сервер выполняет следующие действия:

1. Независимо от режима лицензирования, терминальный сервер сначала запрашивает устройство клиента чтобы определить, есть ли в реестре маркер устройства. Если маркер найден, терминальный сервер обращается к серверу лицензирования, который указан в маркере, для подтверждения лицензии. Если это временная лицензия, сервер лицензирования назначит постоянную лицензию, которая будет сохранена в реестре клиента.

2. Если устройство клиента не имеет маркера, то следующий шаг зависит от режима лицензирования терминального сервера:

- a. Режим лицензирования *Per-User* - Терминальный сервер запрашивает учетные данные пользователя и осуществляет аутентификацию. Затем он запрашивает сервер лицензирования либо проверить, либо выдать лицензию для пользователя. Маркер лицензии сохраняется на сервере лицензирования.

- b. Режим лицензирования *Per-Device* - Терминальный сервер запрашивает временный маркер у сервера лицензирования и записывает его в реестр клиента. После аутентификации пользователя терминальный сервер указывает серверу лицензирования пометить временный маркер как проверенный. Если пользователь не аутентифицировался, маркер немедленно возвращается в пул доступных лицензий.

3. В любом случае, если сервер лицензирования не имеет свободных маркеров, производится обращение к другому серверу лицензирования. Если первый сервер лицензирования знает, что другой сервер лицензирования имеет доступные лицензии, он запросит маркер от лица терминального сервера. Если сервер лицензирования не знает об остальных серверах лицензирования, то терминальный сервер запрашивает следующий сервер лицензирования, кешированный в его реестре.

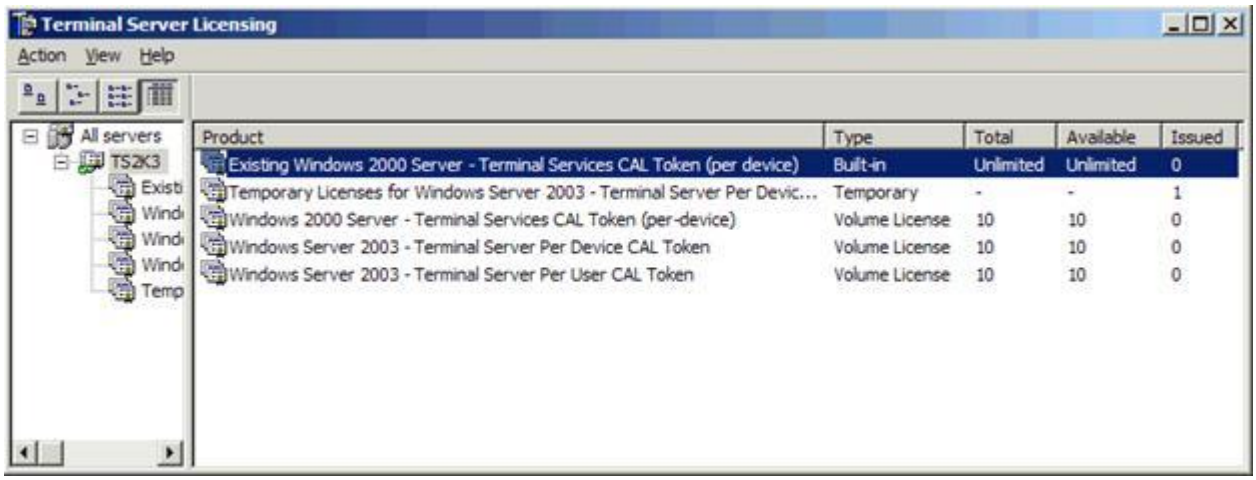
В большинстве случаев серверы лицензирования информируют друг друга о том, какие лицензии добавлены или удалены их их пулов. Этот процесс называется "уведомлением о лицензиях" (License Token Announcement) и происходит в следующих случаях:

- Между доменными серверами лицензирования в пределах одного домена
- Между корпоративными серверами лицензирования внутри одного сайта и домена
- От корпоративных серверов лицензирования к доменным серверам лицензирования
- От серверов лицензировния Win2K к серверами лицензирования WS2K3

License Server Administration

После того, как вы активировали ваши серверы лицензирования и инсталлировали лицензии, дальнейшее администрирование почти не требуется. Однако, вам следует ознакомиться с несколькими утилитами, чтобы выявлять и устранять возможные проблемы с лицензированием.

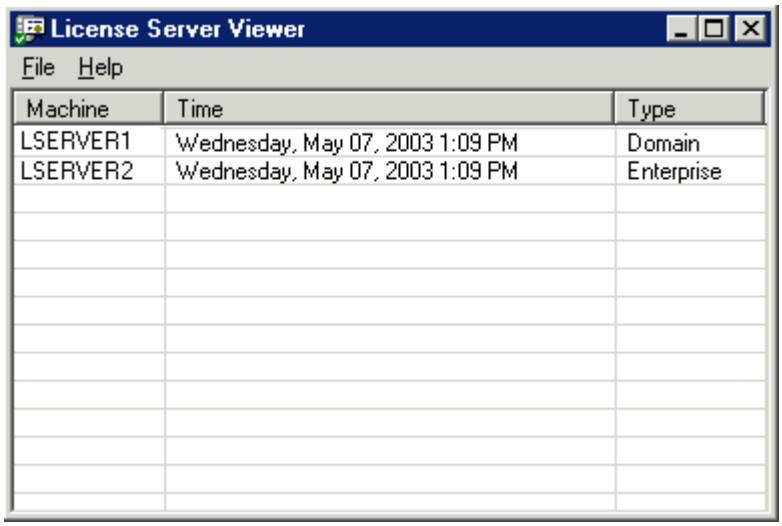
Утилита Terminal Sever Licensing является основной утилитой управления лицензиями. Она используется для активирования сервера лицензирования, установки лицензий и просмотра доступных маркеров лицензий. С ее помощью вы можете видеть, какие пользователи и устройства получили маркеры лицензий и когда истекает срок их действия.



WS2K3 Resource Kit содержит утилиту командной строки LSREPORT.EXE. С ее помощью вы можете получить список маркеров, назначенных сервером лицензирования.

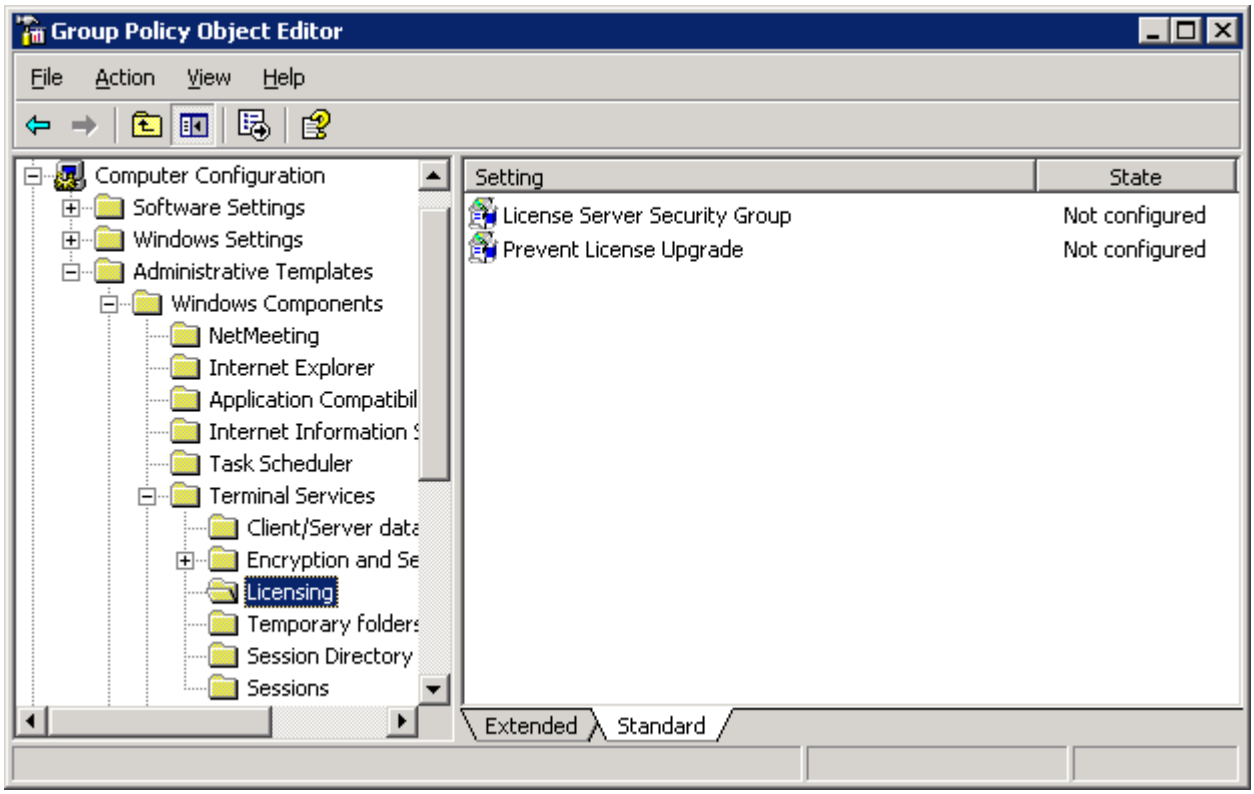
Есть еще одна утилита, Client License Test Tool, TSCTST.EXE. Она используется для запроса подробной информации относительно маркеров устройств, инсталлированных на указанном устройстве. В выводе утилиты содержится имя сервера лицензирования, выдавшего маркер, диапазон, пользователь, который аутентифицировался при выдаче маркера, идентификатор лицензии, срок действия. Если указать опцию /A, утилита также покажет версию сертификата сервера, версию лицензированного продукта, идентификатор аппаратуры, идентификатор платформы клиента, имя компании.

Утилита License Server Viewer - LSVIEW.EXE - также содержится в Resource Kit. Она осуществляет поиск серверов лицензирования и выводит все серверы лицензирования терминальных служб. Она также определяет тип сервера лицензирования - Domain or или Enterprise - и создает журнал с диагностической инфрмацией.



Групповые политики для сервера лицензирования

WS2K3 включает несколько политик для управления лицензированием. С их помощью можно легко централизованно настроить серверы лицензирования и поддерживать ихз целостность.



- *License Server Security Group* - По умолчанию, сервер лицензирования выдает маркеры клиентам, подключающимся к любым терминальным серверам. Если вы включите эту настройку, то сервер лицензирования будет отвечать на запросы только тех терминальных серверов, которые находятся в локальной группе *Terminal Services Computers*. Если сервер лицензирования является контроллером домена, это локальная доменная группа. Включение этой настройки предотвращает нежелательным терминальным серверам запрашивать лицензии и заставляет использовать отдельный пул лицензий для групп серверов. Если у вас есть несколько серверов лицензирования для некоторой группы терминальных серверов, добавьте серверы лицензирования в эту группу.

- *Prevent License Upgrade* - Как вы знаете, сервер лицензирования WS2K3 может раздавать терминальные лицензии как Win2K, так и WS2K3. Если терминальный сервер Win2K запрашивает маркер, а сервер лицензирования не имеет доступных Win2K TS CAL, он будет автоматически выдавать макркер лицензии WS2K3 Per-Device (если они доступны). Это поведение можно запретить политикой. Если настройка разрешена, то сервер лицензирования будет выдвать только временные маркеры клиентам, подключающимся к терминальным сервам Win2K. Если срок действия лицензии истек, в подключении отказывается.

Группа Terminal Services Computers по умолчанию пустая; добавьте в нее серверы перед тем, как включить политику, чтобы предотвратить отказы в соединении.

Глава 2: Установка и настройка терминального сервера

Сценарии развертывания терминальных служб

Что вам необходимо учитывать в первую очередь при управлении рабочими столами Windows? Честно говоря, я уверен, что на первом месте будут следующие факторы:

- Развертывание программного обеспечения
- Защита от вирусов
- Обновление ПО

Используя Terminal Services вы можете значительно снизить сложность этих задач. Роль терминального сервера WS2K3 позволяет вам централизировать программное обеспечение, уменьшить число систем Windows в вашей среде и снизить риск заражения вирусами, централизованно обновляя антивирусное ПО и создавая единую точку входа для удаленных пользователей.

Существует три основные модели использования Terminal Services:

- Замена рабочего стола - Убрать со стола пользователя ПК с Windows и заменить его устройством тонкого клиента.
- Удаленный доступ - Обеспечение доступа удаленных пользователей к рабочему столу или индивидуальным приложениям через глобальные сети или RAS
- Провайдер приложений (Application service provider, ASP) - Предоставление доступа пользователей к индивидуальным приложениям, не инсталлируя эти приложения на рабочих столах пользователей.

Замена рабочего стола

Одной из распстраненных причин внедрения Terminal Services является стремление персонала служб автоматизации предприятия полностью убрать у пользователей персональные компьютеры. Эта модель дает много преимуществ, включая избавление от сопровождение конечных ПК, быстрое развертывание и обновление программного обеспечения, уменьшение энергопотребления, повышенная защищенность. В зависимости от вашей корпоративной архитектуры, замена рабочего стола может также снизить потребляемую пропускную способность и устранить необходимость в серверах в удаленных офисах.

- **Устранение поддержки конечных узлов**. Если у пользователей не будет ПК, то больше не надо бегать к рабочим станциям для настройки системы, установки и ремонта программ, помощи в настройке приложений, замены сломанных деталей. Устройства тонкого клиента имеют операционную систему, зашитую в ROM, а приложения устанавливаются на сервере терминалов. Служба техподдержки может помогать пользователям посредством удаленного управления их терминальными сеансами, а пользователи могут сами заменить поврежденное устройство, просто установив новое. Большинство устройств тонкого клиента поддерживают автоматическую конфигурацию через DHCP и FTP. Вы добавляете URL к расширению DHCP, и при загрузке клиента он загружает свою конфигурацию с указанного FTP.

- **Быстрое развертывание и обновление приложений**. Если вы работаете в большой компании, то знаете, насколько тяжело распространять программное обеспечение для множества пользователей. Используя Terminal Services и тонкие клиенты, вы просто устанавливаете новое ПО на серверах, и оно становится доступным тысячам пользователей.

- **Уменьшение энергопотребления**. Устройства тонких клиентов не имеют движущихся частей, они потребляют всего 10% мощности обычного ПК Wintel. С учетом постоянного роста цен на электроэнергию, это может дать существенную экономию для вашей компании.

- **Повышенная безопасность**. Если украдут обычный компютер, вы рискуете потерять важные конфиденциальные данные, хранящиеся на нем, и должны выложить деньги для его замены. В случае тонкого клиента данные на конечном устройстве не хранятся, а стоимость замены составляет приблизительно половину стоимости обычного ПК.

На рынке устройств тонкого клиента есть много игроков, включая Wyse Technologies' Winterm и Neoware EON. Эти устройства могут использовать любую встроенную ОС (Windows CE, embedded Linux и т.п.).

Однако, в модели замены рабочих столов есть и потенциальные недостатки, включая ограниченную приспособляемость одноразовых приложений, ограничения в персонализации пользовательских настроек и повышенная стоимость внедрения:

- Ограниченная приспособляемость одноразовых приложений. Если у вас небольшое число пользователей, нуждающихся в приложении, то в модели замены рабочего стола вы не будете иметь свободы в установке приложения только на выбранных пользовательских ПК. Вам придется интегрировать все приложения в инфраструктуру Terminal Services. По этой причине модель замены рабочего стола лучше всего подходит для однородной среды.

- Ограничения в персонализации пользовательских настроек. Если ваши пользователи персонализируют свои рабочие станции обоями, хранителями экрана, или имеют возможность сами устанавливать программное обеспечение, вам придется бороться с ними, когда они столкнутся с ограничениями.

- Повышенная начальная стоимость внедрения. Если у вас уже есть большое число пользователей и компьютеров, начальные затраты при покупке устройств тонких клиентов и надежных серверов могут быть очень велики. Однако, в долгосрочной перспективе снижение стоимости владения (TCO) даст больше, чем покрытие начальных затрат. Открытие нового офиса или центра обработки заказов - удобные случаи для внедрения модели замены рабочего стола.

Удаленный доступ

Если эти недостатки или корпоративная культура мешают внедрению модели замены рабочего стола, то модель удаленного доступа может быть отличной альтернативой. Многие большие компании имеют удаленные офисы или разъездных пользователей - надомных работников, коммивояжеров, курьеров и т.п. Хотя ноутбуки и КПК дают возможность удаленной работы, они ничего не могут сделать с медленными соединениями или с удаленной поддержкой. Кроме того, ноутбуки очень дорогие.

Модель удаленного доступа предоставляет удаленным пользователям возможность иметь доступ к индивидуальным приложениям или даже к целому корпоративному рабочему столу через интернет (используя Remote Desktop Web Connection, веб-версию клиента Remote Desktop Connection) с их домашних компьютеров. Кроме того, невысокие требования RDP к пропускной способности повышают производительность работы по сравнению с работой на ноутбуке через медленные каналы связи.

Использование терминального сервера в качестве портала в корпоративную локальную сеть может защитить вашу сеть от вирусов, присутствующих на удаленных компьютерах.

При любой стратегии удаленного доступа вы должны ставить вопрос безопасности на первое место. Найдите время для обучения ваших сетевых инженеров особенностям протоколов терминальнх серверов. Обеспечьте стратегию, предотвращающую злоупотребления в терминальной среде.

ASP

Рассматривая масштабное внедрение вертикального приложения, следует учитывать много факторов:

- Метод развертывания (Sneakernet, Systems Management Server—SMS, IntelliMirror)
- Требования к рабочим станциям (RAM, диски, процессор)
- Поддержка и план отката в случае неудачного внедрения
- Требования к пропускной способности для приложений

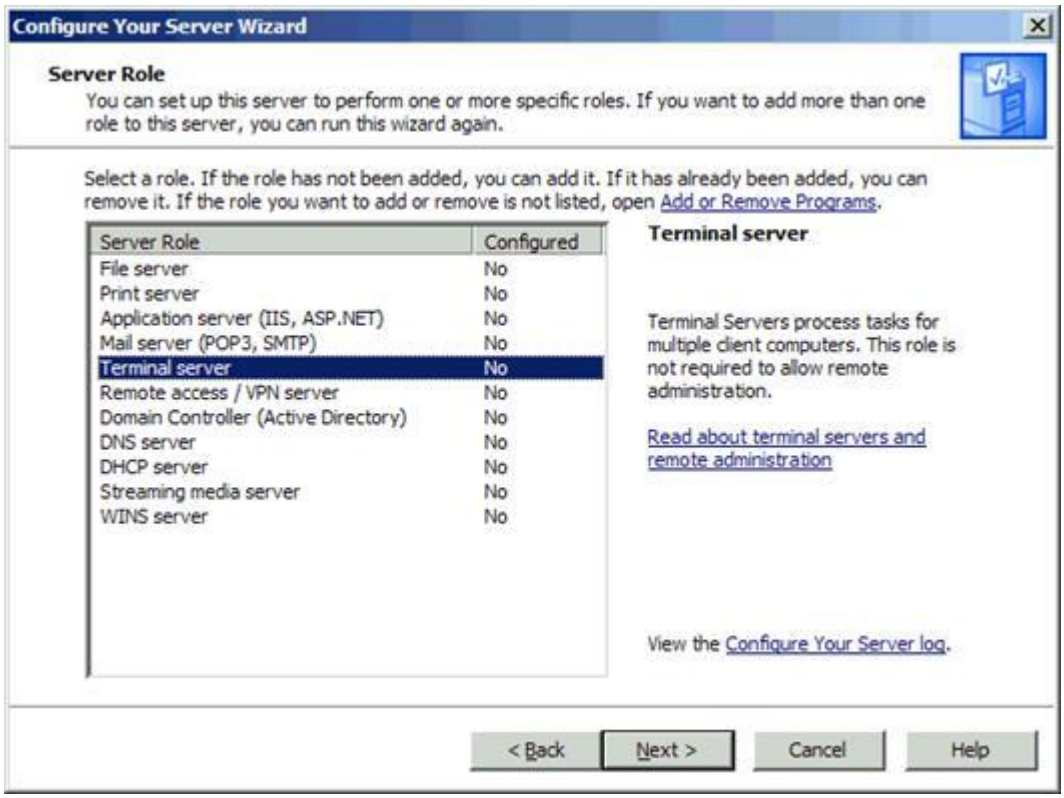
Если приложение не имеет сложной интеграции OLE с другими приложениями на рабочих столах пользователей, вам может подойти модель ASP. Терминальные серверы, особенно вместе с TSAC или другими продуктами публикации приложений, могут быстро и легко предоставлять пользователям необходимые им приложения, не требуя установки и настройки на рабочих

станциях. В этой модели приложения инсталлируются на терминальных серверах, а пользователи запускают их из клиентского приложения или веб-браузера.

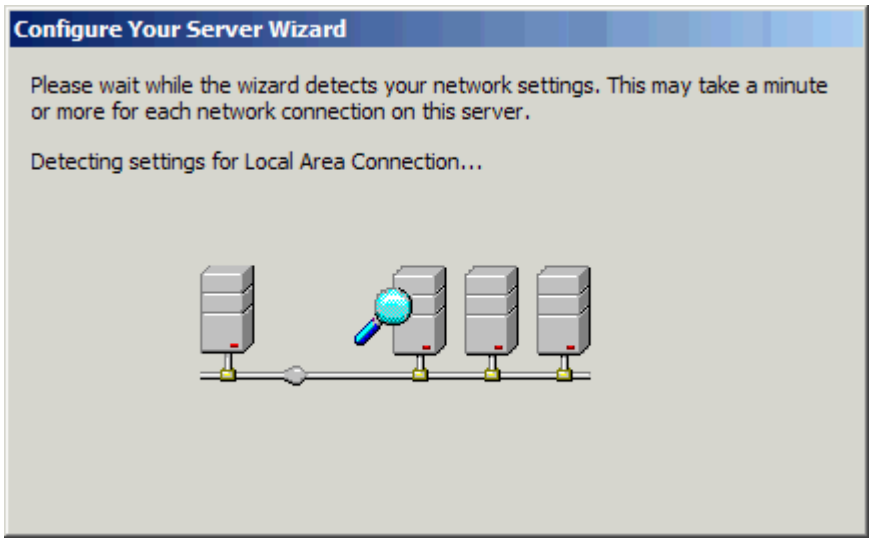
Установка роли терминального сервера

При входе администратора на сервер WS2K3, появляется мастер Manage Your Server:

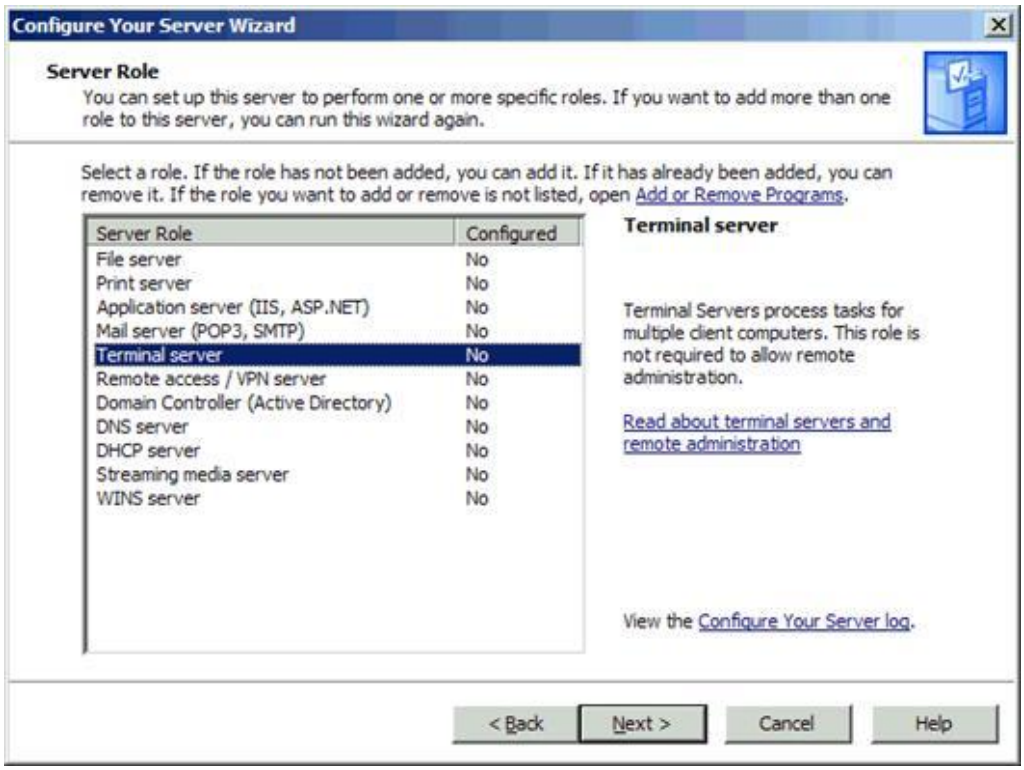
Щелкните ссылку *Add or remove a role* для запуска мастера "Configure Your Server":



Затем мастер начнет сканирование ваших сетевых соединений, чтобы определить совместимые роли, а затем выдаст список доступных ролей.



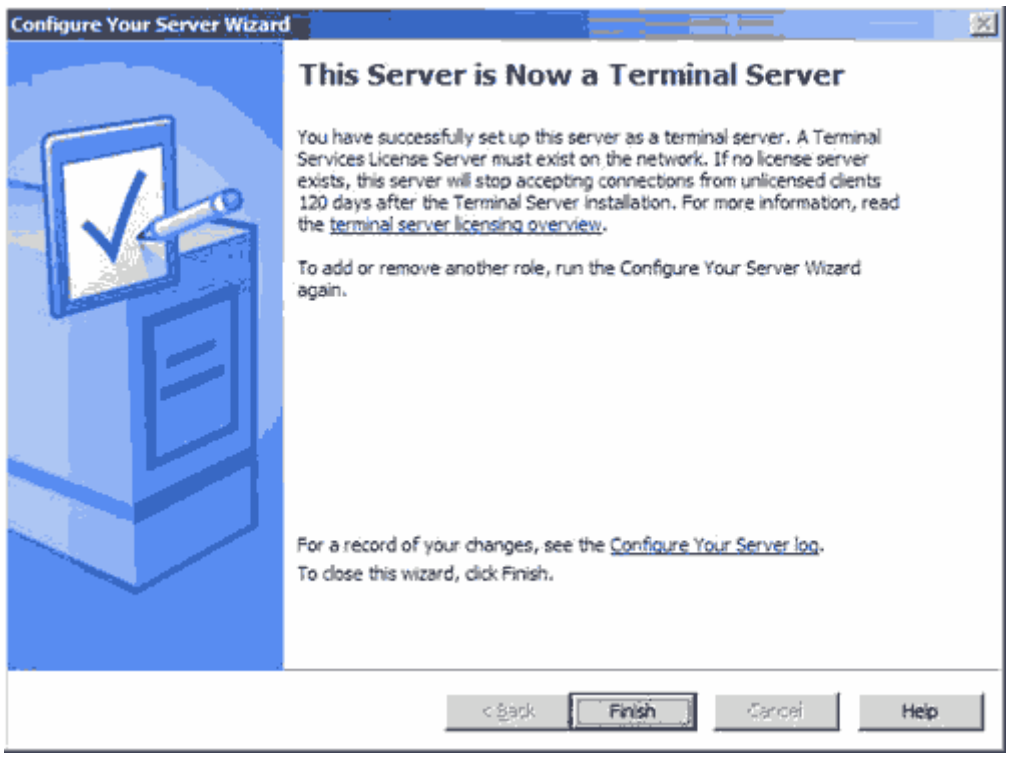
В окне, появившемся после сканирования, выберите роль терминального сервера и щелкните Next.



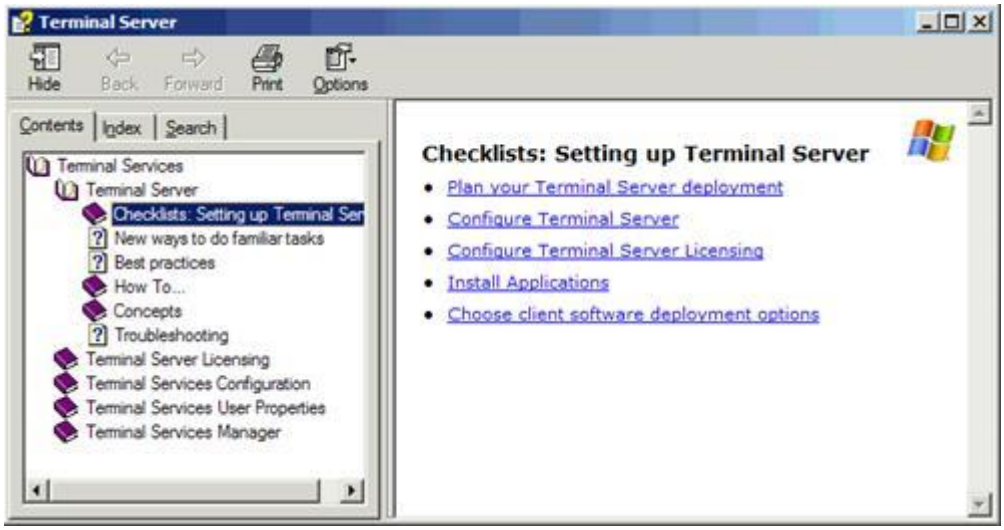
Мастер предупредит, что после добавления роли сервер будет перезагружен, и запустит апплет *Add/Remove Windows Components* для добавления нужных служб. По завершении сервер перезагрузится.

При добавлении роли вы не можете отложить перезагрузку.

После перезагрузки зарегистрируйтесь в системе и вы увидите два окна. Одно из них сообщает о том, что роль терминального сервера успешно установлена.



Второе окно содержит весьма полезный список дальнейших шагов, которые вы должны предпринять для завершения настройки.



Настройка роли терминального сервера

Как видно из рисунка, после установки терминального сервера вы должны сделать ряд шагов. Мы уже обсуждали лицензирование в Главе 1. В этом разделе мы обсудим настройку терминального сервера.

Справочный материал содержится в разделе *Plan your Terminal Server Deployment*, внимательно ознакомьтесь с ним.

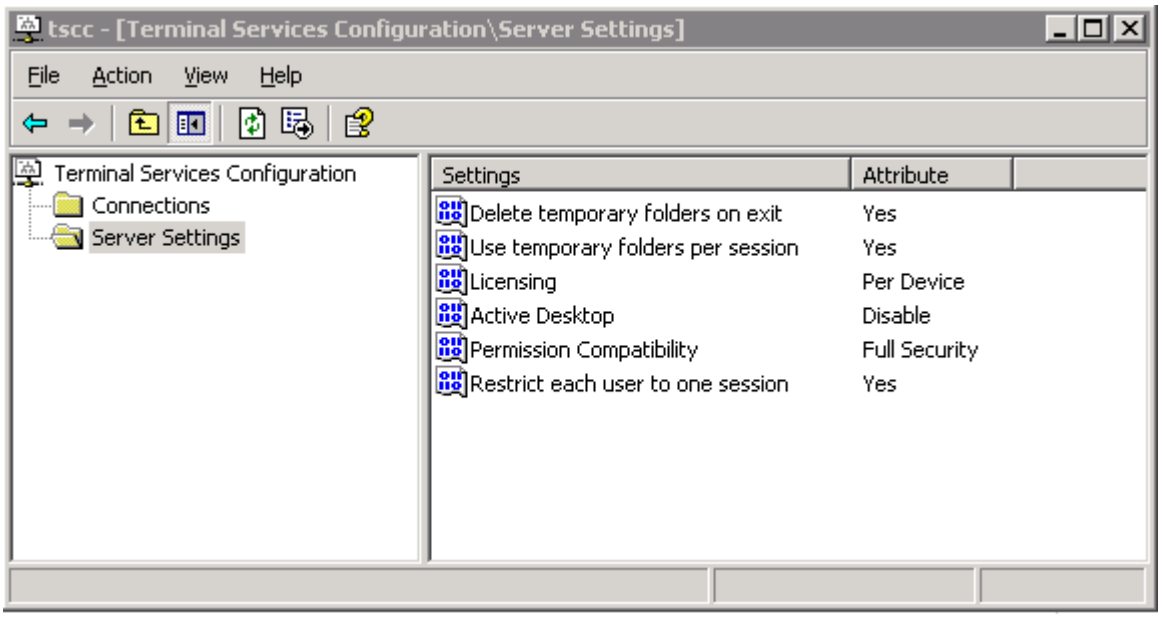
Есть два основных инструмента конфигурирования терминального сервера: утилита Terminal Services Configuration и редактор групповых политик.

Terminal Services Configuration

Это основной инструмент настройки терминального сервера. С его помощью вы можете устанавливать режим полномочия для сервера, настраивать опции производительности, настраивать RDP. Вы можете запустить Terminal Services Configuration тремя способами:

- Из меню Start в разделе Administrative Tools
- Из мастера Configure Terminal Server
- Из мастера Manage Your Server

В Server Settings вы видите шесть опций:



Три из этих опций - *Delete temporary folders on exit* , *Use temporary folders per session (использовать в сеансе временные папки)* и *Active Desktop* - лучше оставить по умолчанию

- *Delete temporary folders on exit (удалять временные файлы при выходе)*. Каждому пользователю на терминальном сервере предоставляется временный каталог. Он находится в `C:\Documents and Settings\<username>\local settings\temp`. Если эта опция включена, то содержимое этого каталога удаляется при выходе пользователя. Если вы используете перемещаемые профили и включили политику *Delete cached copies of roaming profiles* (обычная практика на терминальных серверах), то настройка *Delete temporary folders on exit* становится бессмысленной. Однако, лучше оставить эту опцию включенной, если у вас нет приложений, которые требуют наличия временных файлов со старого сеанса - в этом случае вам также придется изменить групповую политику.

- *Use temporary folders per session* (*отдельный временный каталог для каждого сеанса*). Если включено, то для каждого сеанса пользователя создается отдельный временный каталог. Эти каталоги именуются \temp\0, \temp\1 и т.д. Это не дает разным сеансам мешать друг другу.

- *Active Desktop* - Начиная с Windows 98, на рабочий стол стало возможным внедрять активное содержимое (веб-страницы, анимацию, новостные тикеры и т.п.). Для уменьшения прорисовок экрана, посылаемых с терминального сервера клиенту, эта настройка по умолчанию запрещена.

Оставшиеся три настройки — *Licensing*, *Permission Compatibility* и *Restrict each user to one session* — требуют чуть большего внимания и понимания.Они зависят от вашей среды и приложений, которые вы инсталлируете на терминальном сервере.

Совместимость разрешений (Permission Compatibility)

В Win2K при установке Terminal Services вам предлагалось выбрать режим совместимости - разрешения, совместимые с Windows 2000 или с Terminal Server 4.0. В Windows 2003 Microsoft сосредоточилась на безопасности, теперь в WS2K3 по умолчанию режим Full Security. В этом режиме в W2K3 пользователи, отличные от администраторов, не могут изменять ключ реестра HKEY_LOCAL_MACHINE и записывать файлы в любое место диска, кроме каталога своего профиля.

Если вам попалось приложение, которое не может выполняться в режиме Full Security, вам может потребоваться изменить режим на Relaxed Security (ослабленная безопасность). Используйте этот режим в крайнем случай, поскольку он открывает сервер для нежелательных изменений со стороны обычных пользователей.

Лицензирование (Licensing)

Следующая настройка относится к режиму лицензирования. Она контролирует, какие типы лицензий термнальный сервер будет запрашивать у сервера лицензирования от имени клиентов. В большинстве случаев значение по умолчанию Per Device, это означает, что вы должны установить на сервере лицензирования лицензии "Per Device" для WS2K3 Terminal Server. Однако, если вы обновляете терминальный сервер Win2K, использующий Internet Connector Licensing, то вам нужно установить лицензирование Per User.

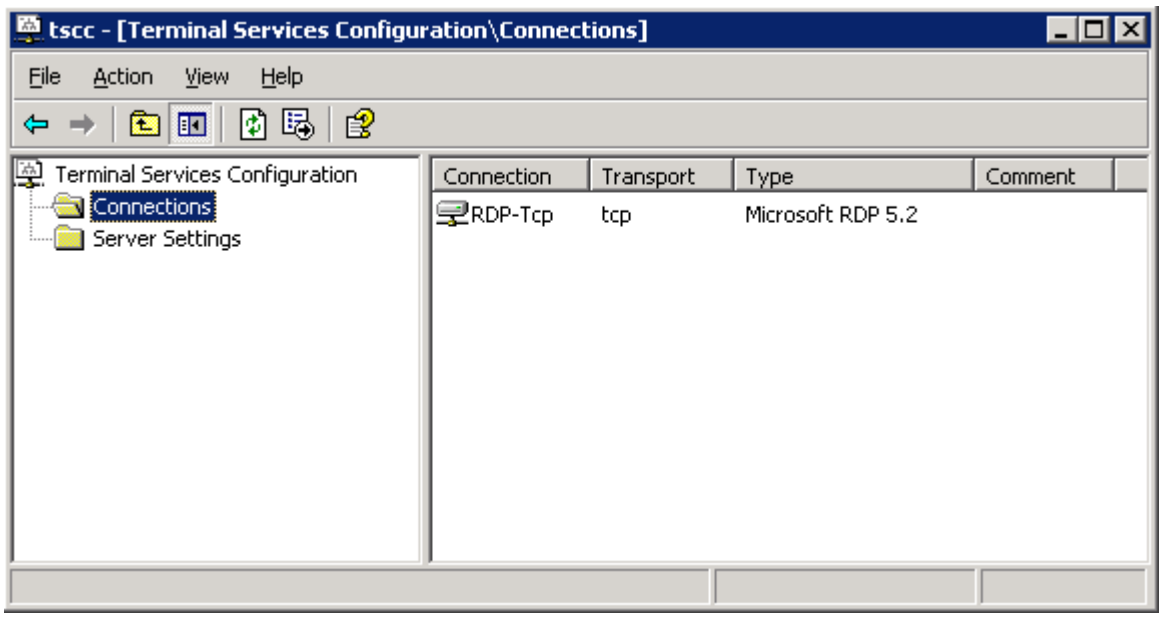
Выбор режима зависит от вашей среды. Если у вас есть пользователи, которые имеют несколько устройств, с которых они могут подключаться, то оптимальным будет выбор лицензирования Per User. Если же одним компьютером пользуются несколько разных пользователей, то лучше Per Device - например, если компьютер стоит в службе круглосуточной поддержки и используется тремя пользователями в три смены. Лицензирование Per Device означает, что вам понадобится только один маркер лицензии для всех троих пользователей. Если вы установите режим лицензирования Per User, то сервер также будет проверять и принимать соединения с устройств, уже получивших маркер Per Device.

Ограничить пользователя одним сеансом (Restrict Each User to One Session)

Включение этой опции предотвращает устанавливать пользователями несколько сеансов на одном сервере, что позволяет экономить его ресурсы, разрешая одному пользователю установить только один сеанс и запускать приложения только в этом сеансе. Учтите, если вы собираетесь предоставлять прямой доступ к индивидуальным приложениям за пределами рабочего стола, то пользователям может потребоваться запустить более одного приложения одновременно.

Citrix MetaFrame поддерживает совместное использование сеанса (session sharing). Это позволяет пользователю запускать несколько опубликованных приложений на том же сервере без создания отдельного сеанса для каждого из них.

На следующем рисунке показан узел соединений. В этом узле вы можете настраивать тайм-ауты, безопасность и перенаправление ресурсов клиента.

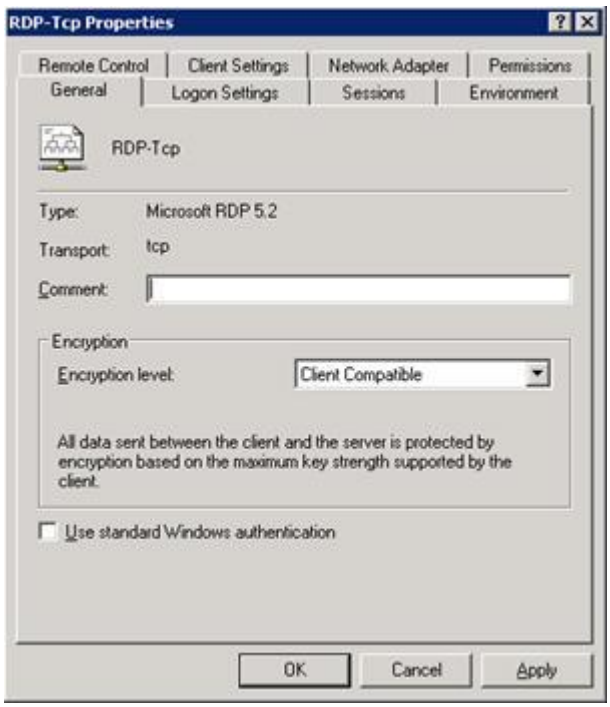


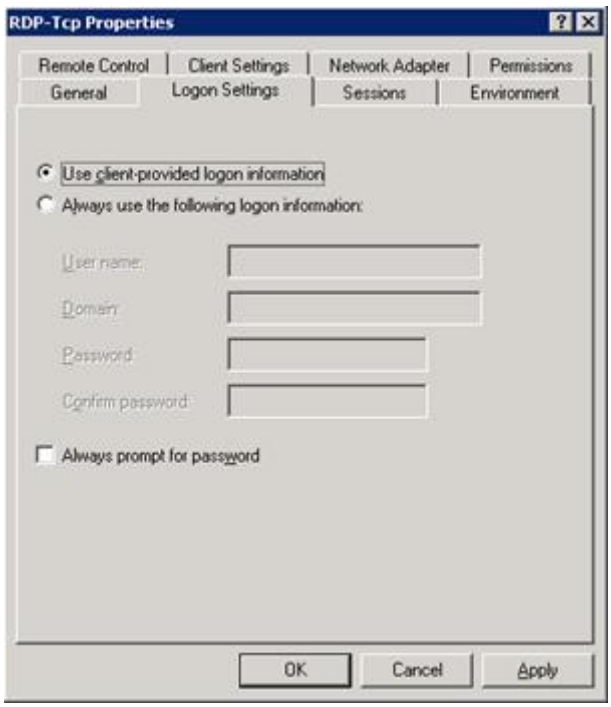
По умолчанию вы видите только одно соединение RDP-Tcp. Если у вас многоадресный (multihomed) севрер, то вы можете изменить определение соединения по умолчанию так, чтобы оно применялось только к одному сетевому интерфейсу, а затем создать новое соединение для другого интерфейса. Если вы инсталлировали Citrix MetaFrame, то увидите здесь еще и соединения ICA; но их лучше настраивать с помощью Citrix Connection Configuration.

Щелкнув правой кнопкой на соединении, вы можете целиком его запретить, переименовать или получить доступ к свойствам. Если вы знакомы с Win2K Terminal Services Configuration, то интерфейс WS2K3 покажется вам знакомым, с добавлением новых особенностей RDP 5.2 и новой модели "полной безопасности".

Вкладка *General* свойств RDP-Tcp позволяет добавить комментарии к соединению и установить уровень шифрования. WS2K3 предлагает новые уровни шифрования:

- *Low* - Все данные от клиента к серверу защищаются 56-битным алгоритмом.
- *Client Compatible* (по умолчанию) - Все данные между сервером и клиентом шифруются используя максимальную силу ключа, поддерживаемую клиентом.
- *High* - Все данные между сервером и клиентом шифруются используя максимальную силу ключа, поддерживаемую сервером. Клиенты, не способные поддерживать заданный уровень шифрования, не смогут подключиться.
- *FIPS Compliant* - Все данные между сервером и клиентом шифруются, используя методы Federal Information Processing Standard (FIPS) 140-1





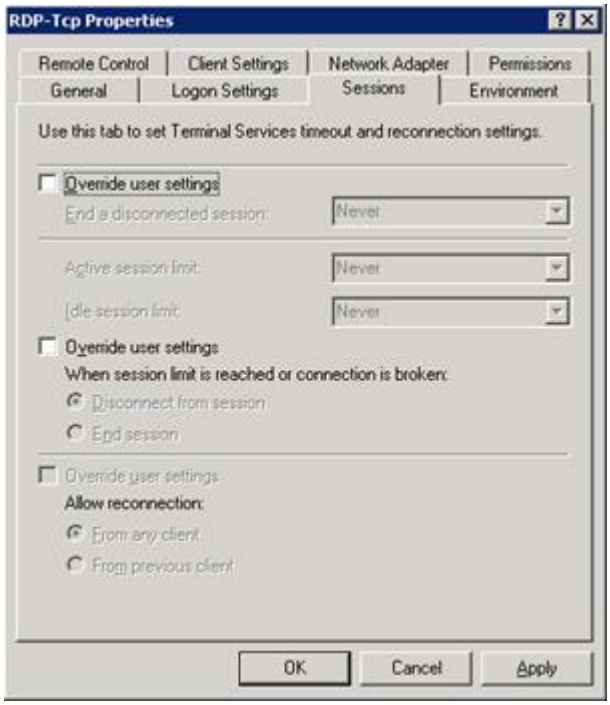
На вкладке *Logon Settings* вы можете указать, чтобы пользователи регистрировались под своими именами или указать единую учетную запись для автоматического входа.

Будьте аккуратными с учетной записью для автоматического входа, поскольку это предотвращает вход под администратором.

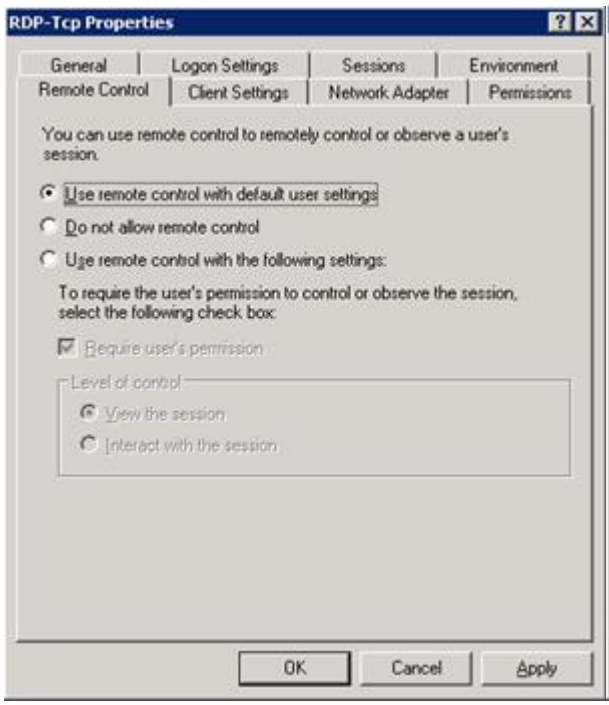
Ниже показаны вкладки *Sessions* и *Environment*. В этих окнах указываются тайм-ауты, опции переподключения, а также начальная программа. По умолчанию значения наследуются из параметров пользователя, подключающегося к серверу. Если вы хотите переопределить значения, сделайте это здесь.

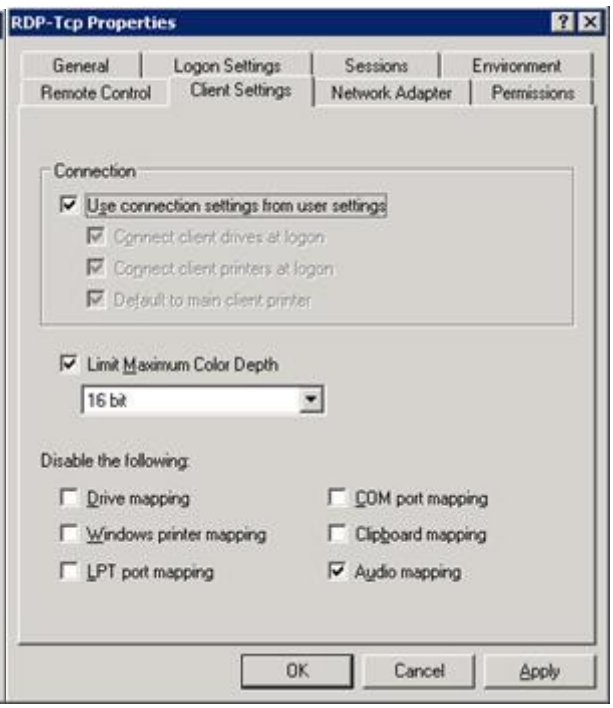
Вкладка *Sessions* содержит тайм-ауты для разъединенных, холостых и активных сеансов. Разъединенный сеанс - это такой сеанс, в котором пользователь активно отключился от сервера, закрыв окно соединения, но не выбрав из меню Start опцию "Disconnect". Холостой (idle) сеанс - это сеанс с открытым окном, но пользователь не нажимал клавиши и не двигал мышью в течении заданного периода времени. Если сеанс теряет сетевое соединение или наступает тайм-аут холостого сеанса, то вы можете выбрать, как поступать в этом случае - завершить сеанс или считать сеанс разъединенным.

Вкладка *Environment* позволяет указать некоторую программу, запускаемую при подключении клиента к серверу. Вы должны указать как путь, так и имя исполняемого файла. При подключении любого пользователя, включая администратора, вместо Windows Explorer будет запущена указанная программа. Многие администраторы ошибаются, думая что настройка здесь аналогична папке "Автозагрузка" (Startup) меню Start, которая автоматически запускает программу при регистрации пользователя. Это не так - указанная здесь программа *заменяет* оболочку Explorer.



Следующие закладки - это *Remote Control* и *Client Settings*.





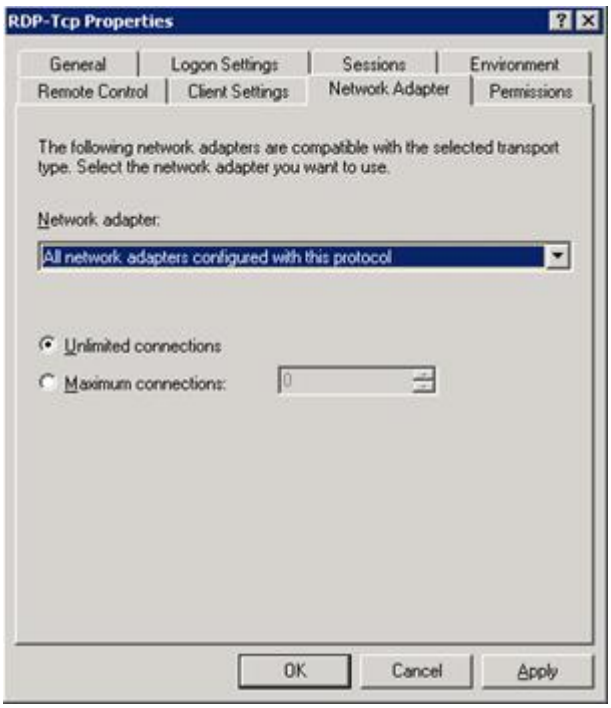
Когда администратор хочет удаленно подключиться к существующему пользовательскому сеансу, то это называется *shadowing*, или *удаленное управление*. На вкладке *Remote Control* вы можете настроить значения по умолчанию для наследования настроек из пользовательских настроек, или можете указать здесь свои собственные для этого сервера. Если вы указываете настройки здесь, то можете разрешить или запретить, чтобы пользователь давал согласие на удаленное

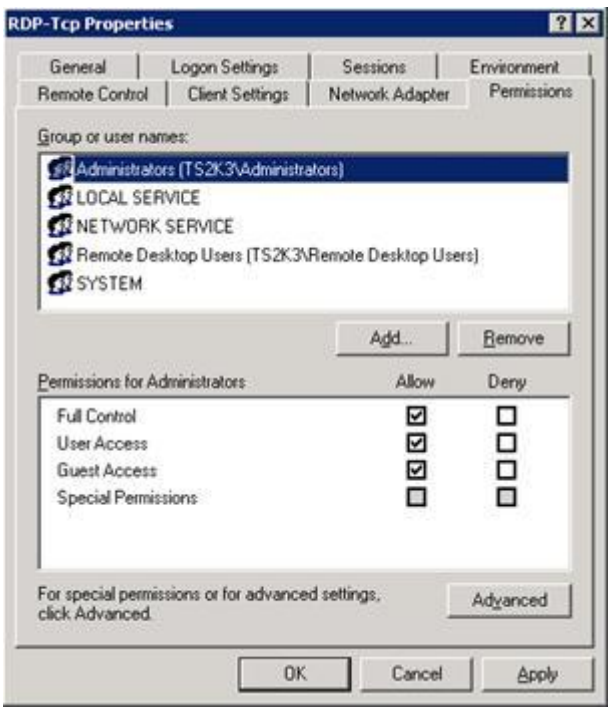
управление (через всплывающее окно), а также можете установить уровень взаимодействия с пользовательским сеансом - только наблюдение или взаимодействие. Если вы выбрали взаимодействие (interact with the session), то администратор может управлять мышью и клавиатурой пользователя от лица пользователя. Вы также можете вообще запретить удаленное управление.

Вкладка *Client Settings* позволяет переопределить перенаправление следующих ресурсов клиента:

- Драйвы
- Принтеры
- Порты LPT
- Порты COM
- Буфер обмена
- Аудио

Вкладки *Network Adapter* и *Permissions* служат для настройки параметров сервера. На вкладке *Network Adapter* вы можете указать, что настройки относятся ко всем сетевым адаптерам или только к указанному. На вкладке *Permissions* вы указываете, кто имеет право подключения к серверу по протоколу RDP, а также уровень их привилегий:





Вкладка *Network Adapter* также позволяет ограничить максимальное число соединений, допустимое для указанного сетевого адаптера или для всего сервера, если установлено "*All network adapters configured with this protocol*".

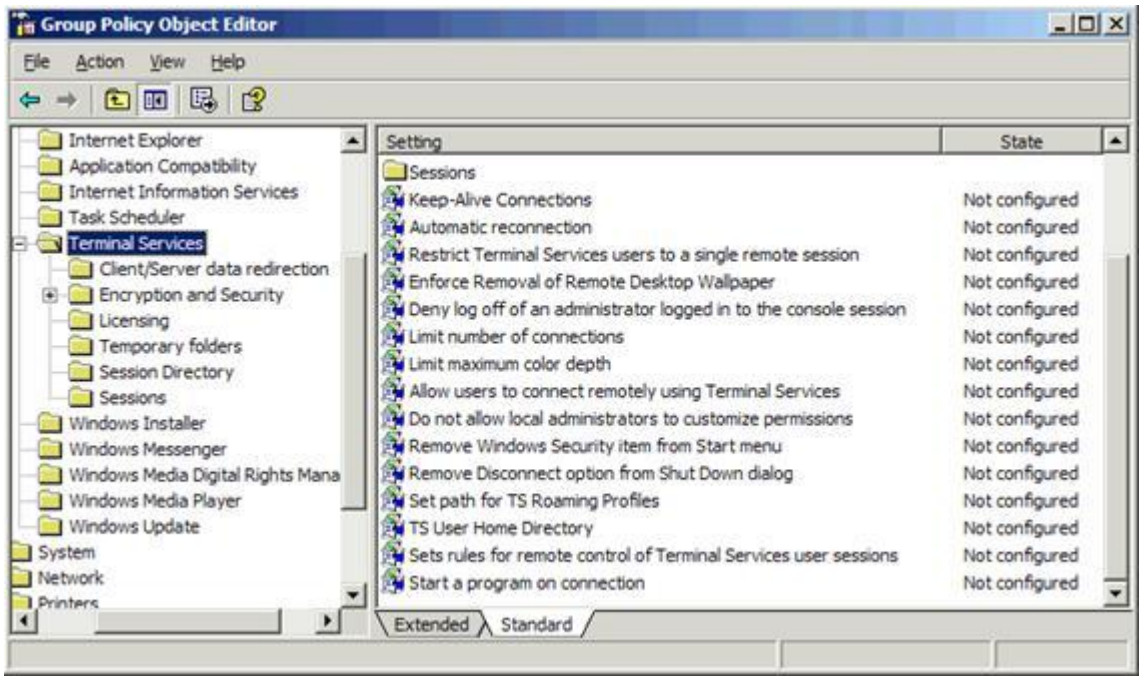
Вкладка *Permissions* несколько отличается от той, что была в Win2K. В Win2K, привилегии по умолчанию позволяли всем пользователям всех доверительных доменов подключаться к терминальному серверу сразу после его установки. В WS2K3 безопасность прежде всего, и подключение разрешено только администраторам и членам группы *Remote Desktop Users*. Учтите, что группа *Remote Desktop Users* изначально пустая, поэтому чтобы ваши пользователи могли подключаться к терминальному серверу, вы должны их добавить в эту группу.

Если вы находитесь в домене AD, то для управления членами группы Remote Desktop Users вы можете использовать настройку *Managed Group* в групповой политике

Основная настройка групповых политик

В WS2K3 в редактор групповых политик добавлено большое количество новых параметров, недоступных в Win2K. Если терминальный сервер находится в среде AD, вы получите большое преимущество от групповых политик; но даже если он находится в рабочей группе или в домене NT 4.0, настройки терминального сервера все равно доступны через политику локальной машины. Эти настройки доступны через редактор групповых политик (Group Policy Editor).

Для доступа к локальному редактору групповых политик, запустите с комадной строки `GPEDIT.MSC`. Откройте узел *Terminal Services* в разделе *Computer Configuration, Administrative Templates, Windows Components, Terminal Services*.



Настройки разбиты на несколько категорий: Encryption (шифрование), Licensing (лицензирование), Sessions (сеансы) и т.д. Вы обнаружите, что некоторые настройки идентичны тем, что находятся в Terminal Services Configuration. Это сделано для того, чтобы вы могли централизованно управлять настройками серверов без необходимости конфигурировать каждый сервер вручную. Вот некотрые из настроек:

- *Set path for TS Roaming Profiles* (установить маршрут для перемещаемых профилей) - Эта настройка позволяет указать сервер и папку общего доступа, в которой следует хранить перемещаемые профили пользователей. Вы также можете указать путь к терминальному профилю для каждой учетной записи пользователя. Эта настройка позволяет не только переопределить пользовательские настройки в зависимости от сервера, но и позволяет указать другой профиль для терминального сервера для группы терминальных серверов. Это полезно, если вы имеете географически распределенную ферму терминальных серверов и пользователи перемещаются между ними.

- *TS User Home Directory* (домашний каталог терминального пользователя) - Эта настрока аналогична предыдущей, но указывает сервер и папку для создания домашнего каталога для пользователей, регистрирующихся на терминальных серверах.

Настраивая один из вышеуказанных параметров, не пытайтесь указывать каталог для каждого пользователя. Сервер автомтически добавит %username% к маршруту.

- *Do not allow local administrators to customize permissions* (не давать локальным администраторам менять привилегии) - Эта настройка запрещает вкладку *Permissions* в утилите Terminal Services Configuration. Поскольку RDP в WS2K3 по умолчанию ограничен и предпочтительный метод предоставления пользователям доступа к терминальному серверу состоит в добавлении их в группу Remote Desktop Users (вместо добавления новых групп в привилегиях RDP), вы можете целиком запретить эту вкладку.

Узел Licensing внутри Terminal Services используется для настройки сервера лицензирования терминальных служб, назначая ему группу безпасности или запрещая обновление лицензий. Группа безопасности принуждает сервер лицензирования выдавать маркеры лицензий только тем терминальным серверам, которые являются членами группы безопасности *Terminal Services Computers*. Запрет обновлений лицензий предотвращает выдачу маркеров терминальных лицензий WS2K3 клиентам, подключающимся к терминальным серверам Win2K. По умолчанию, если сервер лицензирования не имеет доступных лицензий для серверов W2K, он выдает лицензию WS2K3.

Узел *Session Directory* используется для конфигурирования терминальных серверов, являющихся членами кластера каталога сеансов. В этом узле вы можете указать имя кластера и сервер каталога сеансов, а также поведение при подключении клиентов существующему сеансу в кластере.

Есть также несколько настроек для администраторов терминального сервера. В *Computer Configuration, Administrative Templates, System, User Profiles* есть опция *Allow only local user profiles* (разрешить только локальные профили пользователей). Эта настройка предотвращает сервер от загрузки перемещаемых профилей, даже если они сконфигурированы в учетных записях пользователей. Это полезно, если у вас есть терминальный сервер в другом сайте, чем сервер профиля, и вы не хотите создавать отдельный профиль для этого сайта. Если вы разрешите эту политику, то при входе пользователя будет создаваться локальный профиль и сохраняться на сервере.

Узел *User Profiles* также содержит политику *Delete cached copies of roaming profiles*. Эта политика указывает серверу удалять локальную копию перемещаемого профиля после выхода пользователя. Это позволяет экономить место на диске и предотвращает объединение старой версии профиля с сетевой, если пользователь некоторое время не регистрировался на терминальном сервере.

Если вы заглянете в User Configuration, Administrative Templates, Windows Components, Terminal Services, то увидите настройки для удаленного управления, среды, тайм-аутов сеансов, аналогично Computer Configuration. Такой двойной доступ позволяет настраивать политики на пользовательском уровне.

В большиснтве случаев, если вы настраиваете одинаковые параметры в Computer Configuration и в User Configuration, побеждают настройки компьютера.

Дополнительные параметры

Помимо настроек, делаемых в Terminal Services Configuration и в редакторе групповых политик, есть несколько параметров, которые администраторы могут устанавливать в реестре. Эти параметры позволяют улучшить производительность серверов, увеличивая число холостых сеансов RDP и запрещая разнообразные украшения дисплея.

- Холостые соединения RDP - По умолчанию, сервер создает два холостых сеанса, отвечающих на запросы при открытии клиентом соединения. После подключения пользователя эти сеансы немедленно заменяются новыми холостыми сеансами. Для предотвращения крайне редкого случая, когда два соединения устанавливаются в один и тот же момент времени, вы можете увеличить число холостых сеансов. Я рекомендую увеличить это число до 5, установив значение параметра IdleWinStationPoolCount в ключе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server.

- Переопределение настроек рабочего стола пользователей - Эти настройки могут повысить производительность при работе через RDP, уменьшив число обновлений экрана. Для отключения анимации при изменении размеров окна установите значние MinAnimate в ключе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\UserOverride\Control Panel\Desktop\WindowMetrics в 0. Кроме того, вы также можете установить следующие значения параметров в ключе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\UserOverride\Control Panel\Desktop subkey.

Имя параметра	Значение	Описание
AutoEndTasks	1	Автоматическое завершение программы, если она не отвечает
CursorBlinkRate	-1	Немигающий курсор - уменьшает число прорисовок экрана.
DragFullWindows	0	Не показывать содержимое окна при перетаскивании.
MenuShowDelay	10	Задержка при отображении вложенных меню.
WaitToKillAppTimeout	20000	Число миллисекунд ожидания до завершения приложения, если оно не отвечает.
SmoothScroll	Значение типа DWORD 00000000	Запрет плавной прокрутки
Wallpaper	(none)	Запрет обоев

Есть также другие настройки, которые вы можете сделать для улучшения общей производительности:

- Настроить журнал событий - В Event Viewer настройте свойства каждого журнала так, чтобы ограничить его размер 16Мб (или больше) и перезаписывать журнал при превышении объема.

- Настройте сбор отладочной информации - В панели управления, в Advanced Startup and Recovery Options настройте параметры Write Debugging Information для записи дампа отладки в нужное место (или запретите отладку совсем), и установите автоматическую перезагрузку сервера.

- Проверьте в реестре ключ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, в котором содержатся программы, запускаемые при создании каждого сеанса. Некоторые приложения (включая некоторые антивирусы, сетевые утилиты, утилиты распределения нагрузки) добавляют туда записи для создания иконок в панели задач. Обычно эти иконки используются лишь для упрощения доступа к панели управления или утилитам конфигурации и не требуют запуска всякий раз. Удалив эти записи, вы уменьшите нагрузку, связанную с запуском этих апплетов для каждого терминального сеанса.

Установка и настройка клиента Remote Desktop Connection

После установки и настройки терминального сервера вы можете предоставлять доступ к серверу через интерфейс клиента. Существуют две версии клиента Remote Desktop Connection: локальная версия, доступная для 32-разрядных Windows, Macintosh и PocketPC; и Remote Desktop Web Connection, элемент управления ActiveX, используемый для подключения к терминальному серверу из окна Internet Explorer.

Выбор клиента зависит от ваших нужд. Если вы хотите поддерживать конфигурацию соединений к терминальным серверам на клиентах (распространяя файлы RDP или разрешая пользователям самим указывать имена серверов), то лучшим выбором будет Remote Desktop Connection. Однако, если вы хотите централизованно управлять соединением (именами серверов, начальными программами и пр.), лучшим выбором будет Remote Desktop Web Connection.

Клиент Remote Desktop Connection

Клиент Remote Desktop Connection входит в состав WindowsXP. Если вы хотите установить его на других ОС, то можете загрузить его с сайта http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.mspx. Этого клиента можно установить на следующие ОС: Windows 95, Windows 98, Windows 98 Second Edition, Windows Me, Windows NT 4.0, Windows 2000 и Macintosh. Вы также можете загрузить Terminal Services Client для PocketPC с http://www.microsoft.com/mobile/pocketpc/downloads/default.asp. На следующей иллюстрации показан интерфейс клиента Remote Desktop Connection:

В интерфейсе вы можете настроить следующие опции:

- Имя или адрес IP терминального сервера
- Имя и пароль, используемые для соединения
- Размер экрана
- Глубина цвета
- Отображение звука, драйвов, принтера, портов
- Поведение комбинаций клавиш Windows (интерпретация клиентом или сервером)
- Начальная программа
- Разрешение или запрещение визуальных эффектов

Установив опции, вы можете сохранить конфигурацию в файле RDP. Это текстовый файл, который может быть запущен для упрощения подключения к некоторому серверу или приложению. Администраторы могут заранее создать файлы RDP и раздать их пользователям по электронной почте.

Если вы скопировали файл RDP, содержащий пароль для другого компьютера, пароль не будет вводиться при подключении. Это важно учитывать при распространении файлов RDP с предустановленными учетными данными.

Если администратор настроил любую из этих опций в Terminal Services Configuration и Group Policy Object Editor на сервере, то настройки сервера будут переопределять настройки клиента. Настройки групповой политики будут переопределять настройки как Terminal Services Configuration, так и клиента.

Вы можете запустить клиента Remote Desktop Connection с командной строки, используя синтакис:

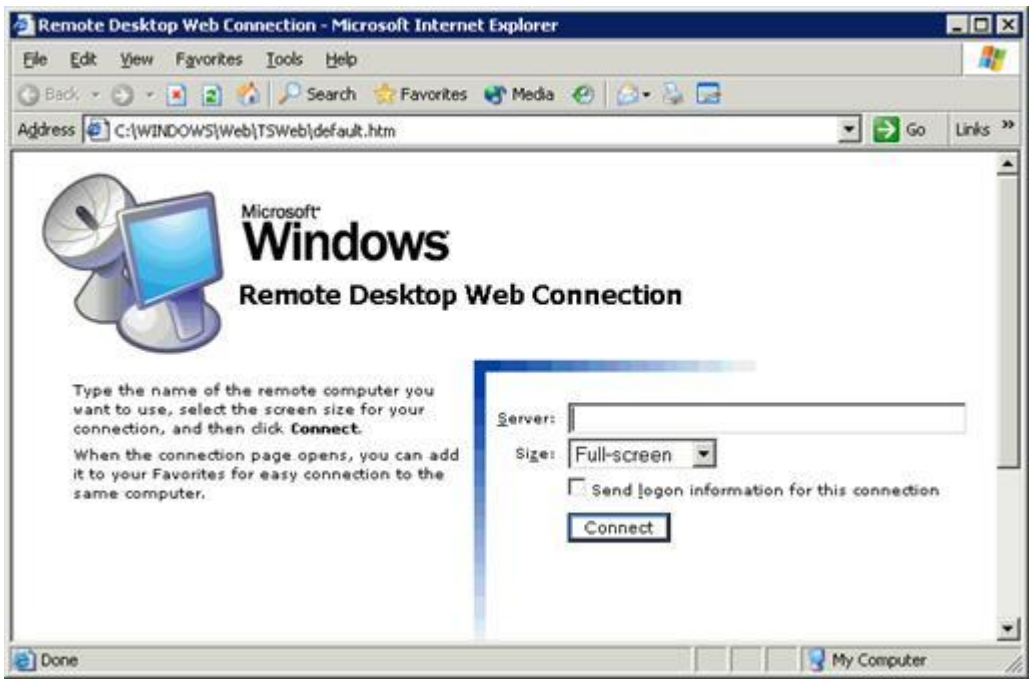
MSTSC [<*Connection File*>][/v:<*server*[:*port*]>] [/console] [[/f[ullscreen]|[/w:<*width*> /h:<*height*>]]|[/Edit"*connection file*"][/Migrate]

- <C*onnection File*> - имя файла RDP
- /v:<*server*[:*port*]> - имя или адрес сервера
- /console – подключение к консоли сервера Windows Server 2003
- /f[ullscreen] – запуск клиента в полноэкранном режиме
- /w:<*width*> /h:<*height*> - ширина и выоста окна соединения
- /edit – открывает файл RDP для редактирования
- /Migrate – мигрировать старые настройки Client Connection Manager из реестра в файлы RDP.

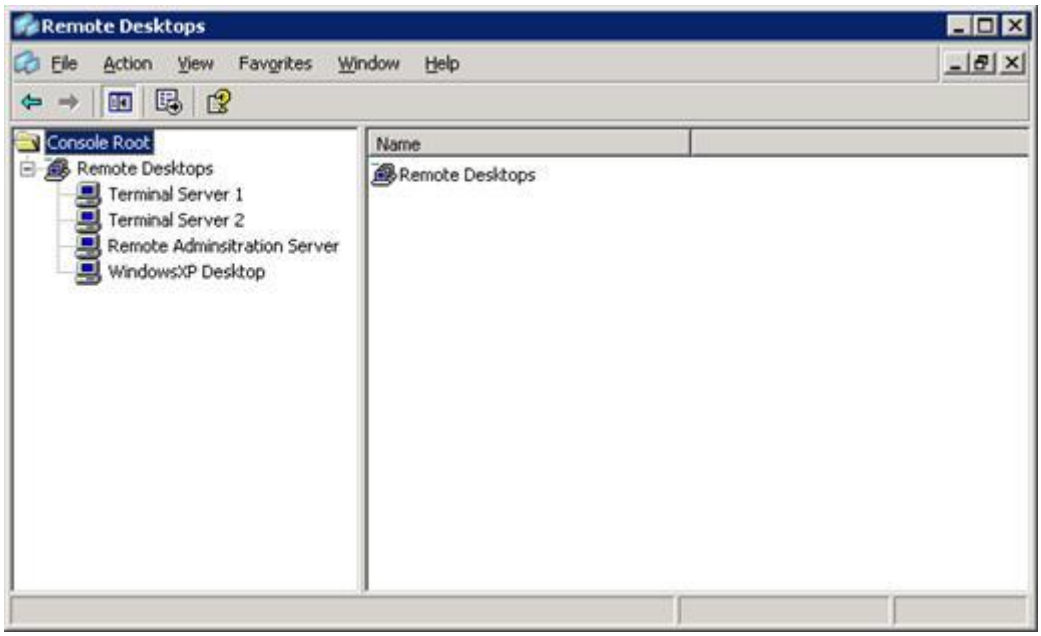
Клиент Remote Desktop Web Connection

Remote Desktop Web Connection инсталлируется на Internet Information Server (IIS) или на сервер WS2K3, на котором разрешена роль терминального сервера. Пакет Remote Dekstop Web Connection доступен на Microsoft для установки на Win2K IIS или может быть установлен на WS2K3 путем выбора Add/Remove Windows Components, Application Server (details), IIS (details), World Wide Web Service (details), Remote Desktop Web Connection. Старая инсталляция устанавливалась в C:\inetpub\wwwroot\tsweb, новая - в C:\windows\web\tsweb.

Как видно на следующем рисунке, единственные доступные опции - это имя сервера, размер окна и информация для входа (имя и пароль). Сценарий ActiveX на самом деле поддерживает полный диапазон настроек, доступных в локальном клиенте, просто вам необходим некоторый наывык в программировании, чтобы получить преимущества от них. Поищите на http://MSDN.Microsoft.com по ключевым словам Desktop ActiveX Control Interfaces.



WS2K3 также включает новую версию старого клиента Terminal Services Connections от Win2K. Теперь он называется Remote Desktops и находится в меню Start, Administrative Tools. Вы можете установить его на WindowsXP, используя пакет adminpak.msi, находящийся на CD-ROM с WS2K3.



Глава 3. Каталог сеансов и распределение нагрузки

Если у вас есть больше пользователей, чем может поддерживать один терминальный сервер, или если вы хотите иметь возможность отключить сервер для профилактики, но продолжать предоставлять доступ к приложениям, то вы можете использовать распределение нагрузки, которая встроена в архитектуру Terminal Services. В этой главе мы рассмотрим службу Microsoft Network Load Balancing (NLB), а также новую особенность WS2K3 - каталог сеансов (Session Directory), который позволяет следить за сеансами пользователей на нескольких серверах.

Я начну с введения в основы конфигурации аппаратного обеспечения терминального сревера, а затем рассмотрю процесс масштабирования. Это фундаментальная информация поможет вам определить, сколько серверов вам необходимо для поддержки пользователей.

Конфигурация аппаратного обеспечения терминального сервера

Вообще говоря, терминальные серверы больше похожи на рабочие станции, чем на серверы. Много ли вы встречали серверов, на которых инсталлирован Microsoft Office? Системные интеграторы должны учитывать это при конфигурировании аппаратных средств для терминального сервера.

Большинство файловых серверов, веб-серверов и серверов печати оптимизированы для дисковых операций, чтобы улучшить производительность при чтении и записи файлов пользователями. Однако, терминальные серверы не хранят данные; они обслуживают приложения. Поэтому оптимизировать их надо для обслуживания приложений. Оптимизация необходима не только для дисковых операций, но и для приложений и DLL, к которым осуществляется доступ из пользовательских сеансов. Поэтому обычными факторами, ограничивающими производительность терминальных серверов, являются память и мощность процессора,а не не дисковое пространство.

Необходимо также учитывать прикладные программы - большинство приложений написано для рабочих станций, поэтому они подразумевают установку на диск C в каталог Program Files. Даже сегодня все еще есть популярные приложения, не понимающие при инсталляции других дисков,

кроме C. Поэтому если на сервере диск D используется для данных, то разбиение диска на разделы будет пустой тратой времени.

Если вы хотите отделить приложения от операционной системы, переместив папку Program Files на диск D и измените в реестре значение HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir, чтобы он отражал новое место.

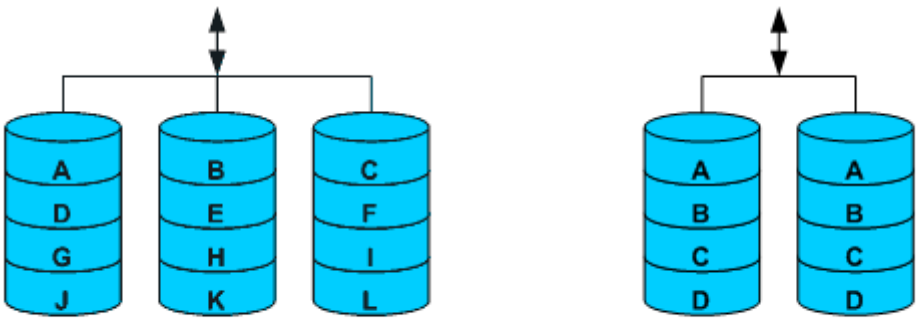
Конфигурация жесткого диска

Из всего этого следует, что я рекомендую терминальные серверы с одним локальным жестким диском. Это упрощает инсталляцию приложений, делает параллель ближе к рабочим станциям и позволяет избежать пустых дисковых разделов. Но даже с конфигурацией с одним диском вы можете рассмотреть варианты RAID.

RAID0 - это простое чередование дисков без контроля четности. Он не является отказоустойчивым - потеря одного диска вызовет потерю всех данных и остановку сервера. Основным достоинством RAID0 является высокая скорость чтения и записи. Производительность можно еще повысить, разместив диски на разных контроллерах.

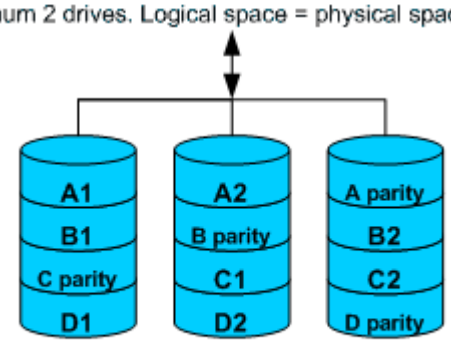
RAID1, или зеркалирование, встречается наиболее часто. Его просто реализовать, он требует всего 2 диска, а также является отказоустойчивым . RAID1 удваивает скорость чтения, но не увеличивает скорость записи, поскольку данные пишутся на оба диска. Если один из дисков выходит из строя, сервер продолжает работу, используя второй диск. Это хороший выбор, если у вас ограниченное число дисков.

RAID5, чередование дисков с паритетом, также часто используется. Как и в RAID0, данные распределяются по дискам, но в RAID5 добавляются контрольные блоки. Эти контрольные блоки позволяют вычислить пропущенный блок в случае выхода одного из дисков из строя. Поэтому RAID5 является отказоустойчивым при выходе из строя одного диска. Поскольку данные разнесены по разным дискам, скорость чтения данных очень высокая, но скорость записи небольшая, поскольку помимо записи самих данных надо вычислить и записать контрольный блок. Для RAID5 необходимо минимум 3 диска; это хороший выбор для терминальных серверов.



RAID 0 = Fast Disk Read & Write. No fault tolerance. Minimum 2 drives. Logical space = physical space

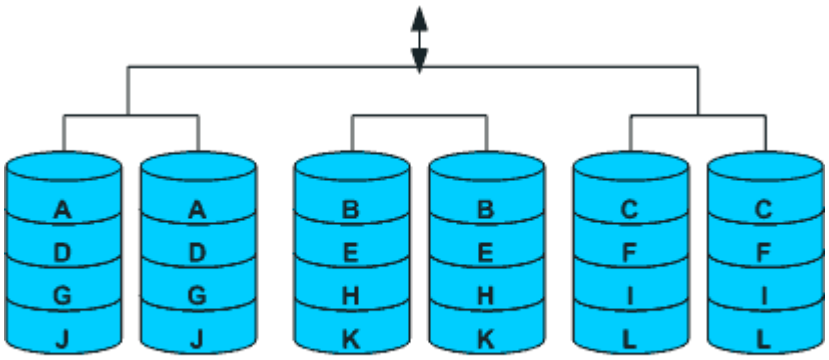
RAID 1 = Fast Disk Read. Single drive fault tolerance. Minimum 2 drives. Logical space = ½ physical space



RAID 5 = Very Fast Disk Read. Single drive fault tolerance.
Minimum 3 drives. Logical space = physical space - 1 disk

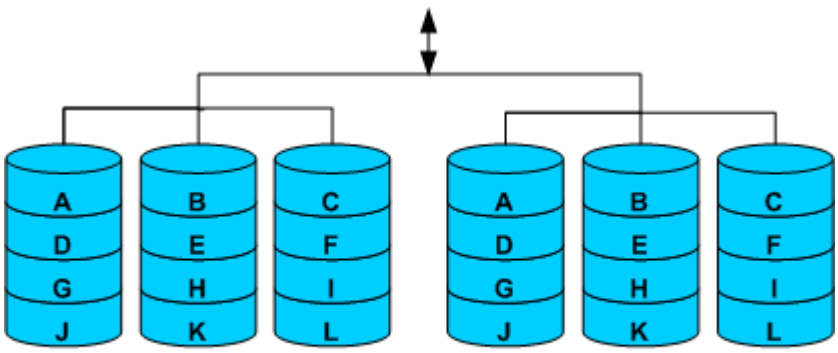
Если в используете RAID 5 и потеряли диск, сервер будет продолжать работу, но скорость чтения сильно замедлится, поскольку контроллер вынужден вычислять пропущенный блок для каждого сегмента данных.

RAID 10 (иногда называемый RAID 1+0) комбинирует скорость RAID0 и отказоустойчивость RAID1. В нем каждым элементом массива RAID0 является зеркало из двух дисков. RAID 10 обеспечивает самый быстрый доступ к данным из всех RAID, одновременно поддерживая отказоустойчивость. Вы даже можете потерять несколько дисков, и сервер все равно будет продолжать функционировать (если эти диски не формируют одно зеркало). Недостатком RAID 10 является то, что вы теряете половину дискового пространства под отказоустойчивость; однако, поскольку для терминального сервера не требуется большого дискового пространства, этот потенциальный недостаток можно не принимать во внимание. RAID 10 является лучшим выбором для терминальных среверов, имеющих минимум 4 диска.



RAID 10 = Very Fast Disk Read & Write. Multiple drive fault tolerance.
Minimum 4 drives. Logical space = ½ physical space

На первый взгляд, RAID 0+1 выглядит аналогичным RAID 10. Разница состоит в том, как контроллер обрабатывает массив. Вместо того, чтобы считать его массивом RAID0 зеркальных дисков, RAID 0+1 считает зеркалом весь массив. Поэтому, в отличие от RAID 10, RAID 0+1 может потерять только один диск и продолжать функционировать. Это прекрасный выбор для терминального сервера, поскольку позволяет значительно повысить скорость дисковых операций, одновременно обеспечивая отказоустойчивость.



RAID 0+1 = Very Fast Disk Read & Write. Single drive fault tolerance.
Minimum 4 drives. Logical space = ½ physical space

Память

Когда RAM была более дорогой, она часто была ограничивающим фактором в масштабировании терминальных серверов. Сегодня не редкость встретить терминальные серверы с 4Гб памяти - достаточно для поддержки сотен пользовательских сеансов. Объем памяти на сервере чаще ограничивается операционной системой и аппаратурой сервера, чем бюджетом.

В первую очередь вам необходимо учесть ограничения материнской платы и BIOS. Также примите во внимание число доступных слотов памяти. На максимальный объем памяти влияет также редакция WS2K3:

Редакция	Максимум RAM	Максимальное число процессоров
Standard Edition	4GB	4
Enterprise Edition (32-bit)	32GB	8
Datacenter Edition (32 bit)	64GB	32

Перед тем, как устанавливать в сервер память, необходимо определить, сколько ее нужно для ваших пользователей. Для этого есть несколько ресурсов, которые помогут вам оценить требуемый объем RAM:

- Windows 2000 Terminal Services Capacity and Scaling
- The HP ProLiant Sizer for Citrix MetaFrame XP and Windows Server 2003 Terminal Services

Microsoft рекомендует начать отсчет памяти с 128MB RAM для ОС. После этого определите тип работы, которая будет осуществляться на терминальном сервере. Пользователей можно разбить на три категории:

- Обычные пользователи - обычно выполняют одновременно только одно приложение. Их работа обычно связана с набором текста (обработка жалоб, прием заказов или служба работы с покупателями).
- Опытные пользователи - Используют одновременно несколько приложений, переключаясь между ними. В основном, это администраторы, менеджеры, аналитики.
- Ввод данных - пользователи вводят данные в компьютер, например, переводчики, клерки службы обработки заказов и т.п.

Определив типы пользователей, вы можете оценить объем требуемой памяти, воспользовавшись следующей таблицей:

Тип пользователя	Объем памяти	Системная память
Обычный пользователь	9.3MB	128MB
Опытный пользователь	8.5MB	128MB
Ввод данных	3.5MB	128MB

Hewlett Packard рекомендует увеличить объем памяти, если используются 16-разрядные приложения. 16-разрядные приложения требуют дополнительной памяти - на 25% больше, чем 32-разрядные.

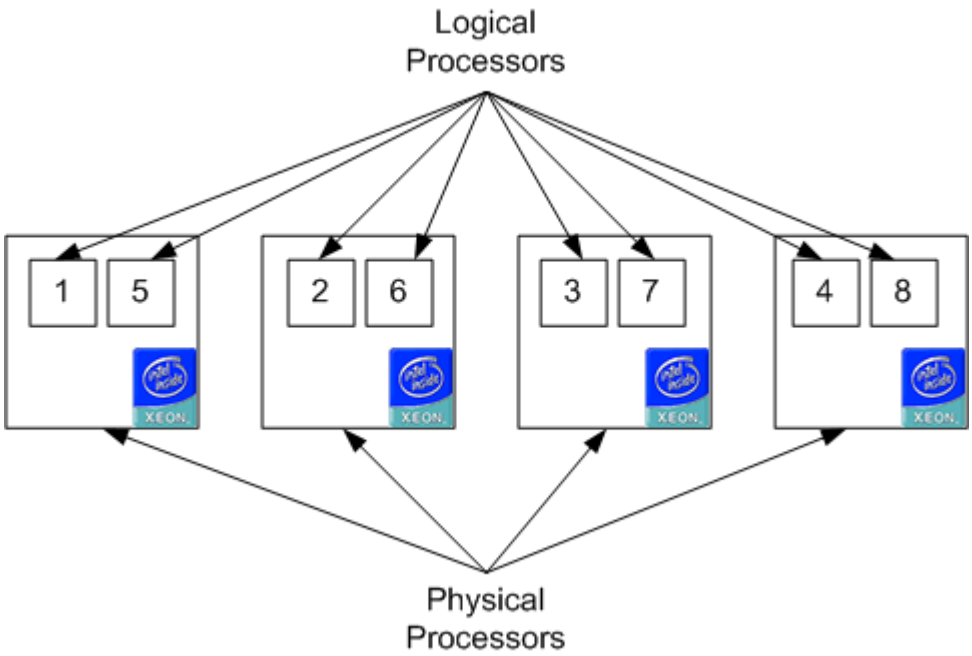
Процессор

Терминальные серверы поддерживают несколько параллельных пользователей, что означает параллельное выполнение нескольких процессов. Поэтому требования к процессору терминального сервера высоки. Возможность одновременной обработки множества задач значительно увеличивает производительность терминального сервера. Поэтому большинство терминальных серверов являются многопроцессорными.

Как вы видели ранее, разные редакции WS2K3 поддерживают разное число процессоров. Эти ограничения такие же, как и для Win2K Server, но в W2K3 встроена поддержка технологии Intel HyperThreading. Эта технология позволяет одним процессором параллельно обрабатывать два потока (threads), виртуально удваивая вычислительную мощность процессора.

WS2K3 может корректно различать физические процессоры и виртуальные, создаваемые HyperThreading. При загрузке Windows, она подсчитывает количество процессоров в системе. Если

процессоров больше, чем поддерживает эта лицензированная ОС, то отсчет заканчивается на лимите ОС. Это важно, поскольку BIOS подсчитывает физические процессоры перед виртуальными. Такое поведение предотвращает Win2K использовать виртуальные процессоры, если есть доступные физические. На рисунке показан порядок, в котором процессоры подсчитываются в ОС при использовании HyperThreading.



Давайте сравним процессорные ограничения стандартной редакции каждой ОС - каждая из них ограничена 3 процессорами. Поскольку Win2K не может различать физические и логические процессоры, ОС останавливается на четвертом процессоре. В нашем примере есть 4 физических процессора с HyperThreading, Win2K остановится на 4-м процессоре и будет размещять на каждом процессоре по одному потоку. Если бы было только 2 процессора с HyperThreading, то Win2K тоже остановилась бы на четвертом, но в этом случае разместила бы по два потока на каждый процессор, используя преимущества HyperThreading.

Однако, WS2K3 может различать физические и логические процессоры, и применяет лимит только к физическим процессорам. Поэтому в нашем сценарии WS2K3 получила бы преимущества от всех восьми логических процессоров, удвоив вычислительную мощность по сравнению с Windows 2000 Server.

Что это означает для терминальных серверов? В большинстве случаев, поддержка HyperThreading в WS2K3 позволит вам повысить производительность без добавления процессоров в систему или обновления ОС до Enterprise Edition.

Нижняя граница

Собрав всю информацию, вы можете задаться вопросом - сколько пользователей может поддерживать мой терминальный сервер? Ответ зависит от многих факторов - числа приложений, используемых каждым пользователем на сервере, потребления приложением памяти и процессора, частоты переключения между приложениями. Давайте рассмотрим пример на основе современной аппаратуры сервера.

Начнем с двухпроцессорной системы 2.4GHz Xeon с включенным HyperThreading. Добавим 2GB RAM и 4 диска SCSI в конфигурации RAID 10. Такой сервер будет стоить около $6000 и будет поддерживать до 200 обычных пользователей. Если вы используете этот же сервер для предоставления доступа не к рабочему столу, а к одиночному опубликованному приложению, то он может поддерживать и 400 параллельных пользователей (в зависимости от требований приложения).

Если ваш терминальный сервер содержит стандартный набор приложенй - Microsoft Office, Outlook, Internet Explorer (IE) и т.д. - то ограничивающим фактором будет память; два процессора с HyperThreading не будут полностью загружены. Поэтому удвоив память до 4GB вы сможете удвоить число поддерживаемых пользователей.,

Есть утилиты, например, Wyse Expedian (http://www.wyse.com), которые оптимизируют использование памяти на терминальных серверах, позволяя еще больше увеличить емкость вашего сервера.

Отказоустойчивость

Отказоустойчивоть *— Способность системы продолжать функционировать в случае сбоя одного из ее компонентов.*

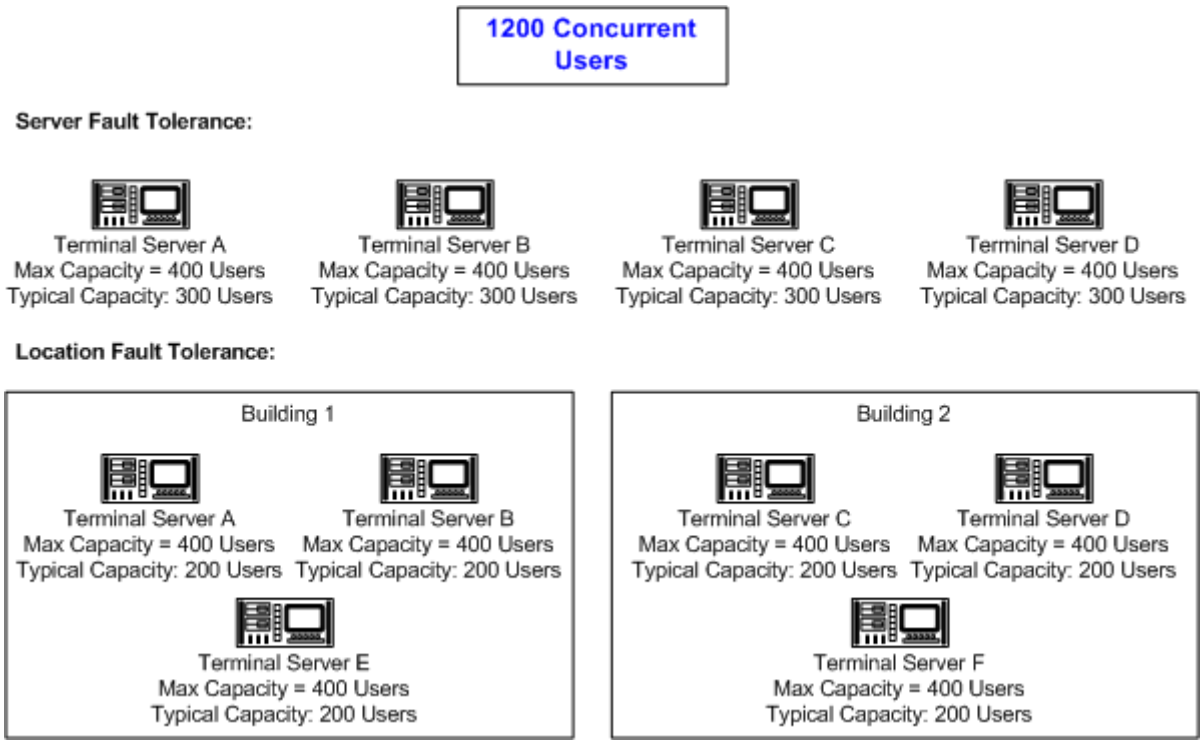
Я уже говорил об отказоустойчивости жесткого диска при использовании RAID, и большинство серверного оборудования содержат опции отказоустойчивости электропитания и сетевых адаптеров. Помимо отказоустойчивости оборудования сервера, вы должны рассмотреть ее на других уровнях.

- Отказоусточивость сервера - Этот уровень определяет способность продолжать поддерживать пользователей в случае потери одного из серверов. Для этого определите число необходимых серверов и добавьте еще один - запасной.

- Отказустойчивость размещения - Способность поддерживать пользователей после потери всех серверов в некотором месте. Эта потеря может быть вызвана сбоем сети, пожаром в здании или природной катастрофой. Для обеспечения отказоустойчивости этого рода вы должны подсчитать число серверов, необходимых для поддержки ваших пользователей, разбить их по местам и добавить запасные серверы в каждом месте. Запасные серверы также размещаются в разных местах.

В большинстве случаев нет необходимости поддерживать отказоустойчивость для *всех* пользователей, достаточно только для *критических*. Для принятия правильного решения вам необходимо собрать адекватные данные.

Допустим, есть 1200 критических пользователей. Для обеспечения отказоустойчивости сервера, это число пользователей требуют 4 сервера, каждый из которых может поддерживать 400 пользователей. В обычных условиях на каждом сервере по 300 пользователей, но в случае поломки сервера остальные серверы способны вынести нагрузку. Для обеспечения отказоустойчивости метоположения с 4 серверами в двух зданиях, вам потребуется 6 x 400 серверов. Если здание 1 будет недоступным, три сервера в здании 2 продолжат поддерживать пользователей.
(Прим. перев.: наверное, навеяно событиями 11 сентября)



Вам также следует рассмотреть вопрос регламента работы. Если пользователи работают 14 часов 7 дней в неделю, вам понадобится адекватная емкость, чтобы иметь возможность отключить один из серверов для профилактики или установки нового ПО. Если же пользователи работают 8 часов и есть два выходных, то эти работы можно выполнить в нерабочие часы, сэкономив на дополнительных серверах.

После того, как вы определились с количеством серверов, вам нужен способ распределения сеансов пользователей по серверам. Мы подошли к расределению нагрузки.

Распределение нагрузки

В базовом варианте распределение нагрузки делается вручную. Вы создаете файлы соединений для каждого из ваших серверов и распространяете их среди пользователей, указывая определенному проценту пользователей их предпочтительное соединение. Вернемся к нашему примеру. Если у вас есть 1200 пользователей и 4 сервера, вы создаете 4 файла и распространяете их среди пользователей, но инструктируете 400 пользователей подключаться к серверу A, еще 400 - к серверу B и т.д. Если один из серверов перестает функционировать, пользователи могут использовать другой файл соединения в качестве резерва. Если вы хотите сделать автоматическое распределение нагрузки и отказоустойчивость без вмешательства пользователя, вам нужно реализовать распределение нагрузки.

Microsoft Network Load Balancing (NLB)

NLB позволяет разместить группу серверов за виртуальным адресом IP (VIP). NLB распределяет соединения, делаемые к VIP, среди серверов кластера и поддерживает межсерверные коммуникации, чтобы в случае выхода одного из серверов из строя NLB прекратила направлять к нему клиентов.

В WS2K3 Microsoft улучшила балансировщик нагрузки. В Win2K, NLB был доступен только в редакции Advanced или Datacenter. WS2K3 включает NLB во все редакции. Microsoft сделала следующие улучшения:

- NLB Manager - В Win2K вы должны вручную конфигурировать каждый сервер в кластере. WS2K3 включает новый инструмент администрирования, который позволяет централизованно создавать, конфигурировать и управлять кластерами NLB.

- Виртуальные кластеры - При использовании NLB для кластеризации веб-серверов, вы можете создавать множественные кластеры на одном и том же наборе серверов, используя несколько адресов IP на каждом сервере . Каждому виртуальному кластеру присваивается свой VIP.
- Подержка нескольких сетевых адаптеров - WS2K3 позволяет привязать NLB к каждому сетевому адаптеру сервера. Win2K позволяла привязать NLB только к одному адаптеру.
- Поддержка широковещания - Кластеры WS2K3 можно настроить на использование multicast для межсерверных коммуникаций.

Но даже со всеми этими улучшениями NLB все еще имеет ограничения, которые вы должны учитывать. Во первых, все члены кластера NLB должны находиться в одной подсети. Во вторых, NLB считает только число активных соединений с сервером при определении того сервера, к которому следует направить соединение; он не учитывает потребление памяти или процессора. В третьих, при использовании совместно с Каталогом Сеансов, NLB требует, чтобы адреса IP терминальных серверов должны быть видимыми клиенту. И NLB ограничен 32 узлами в кластере.

В NLB Manager, Microsoft называет группу серверов, связанных распределением нагрузки, кластером. Не путайте этот термин с настоящим кластером, который позволяет серверам совместно использовать процессы и запоминающие устройства как единый сервер. Во многих документах о распределении нагрузки, включая статьи Microsoft, группы серверов с распределением нагрузки называются *фермами*. Тем не менее, в этой книге я буду использовать термин "кластер", чтобы не противоречить NLB Manager.

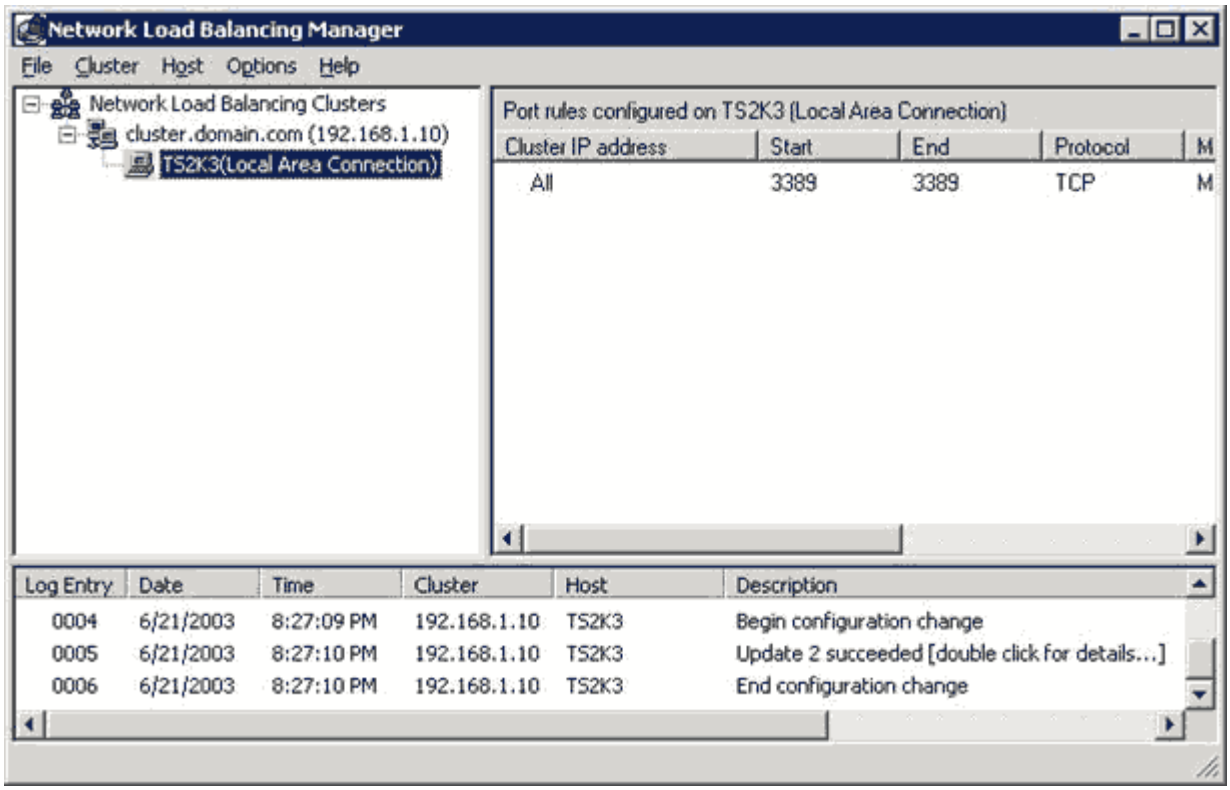
Настройка NLB

После того, как вы сконфигурировали ваши терминальные серверы и установили приложения, вы готовы приступить к конфигурированию их для NLB. Но сначала вы должны собрать следующую информацию:

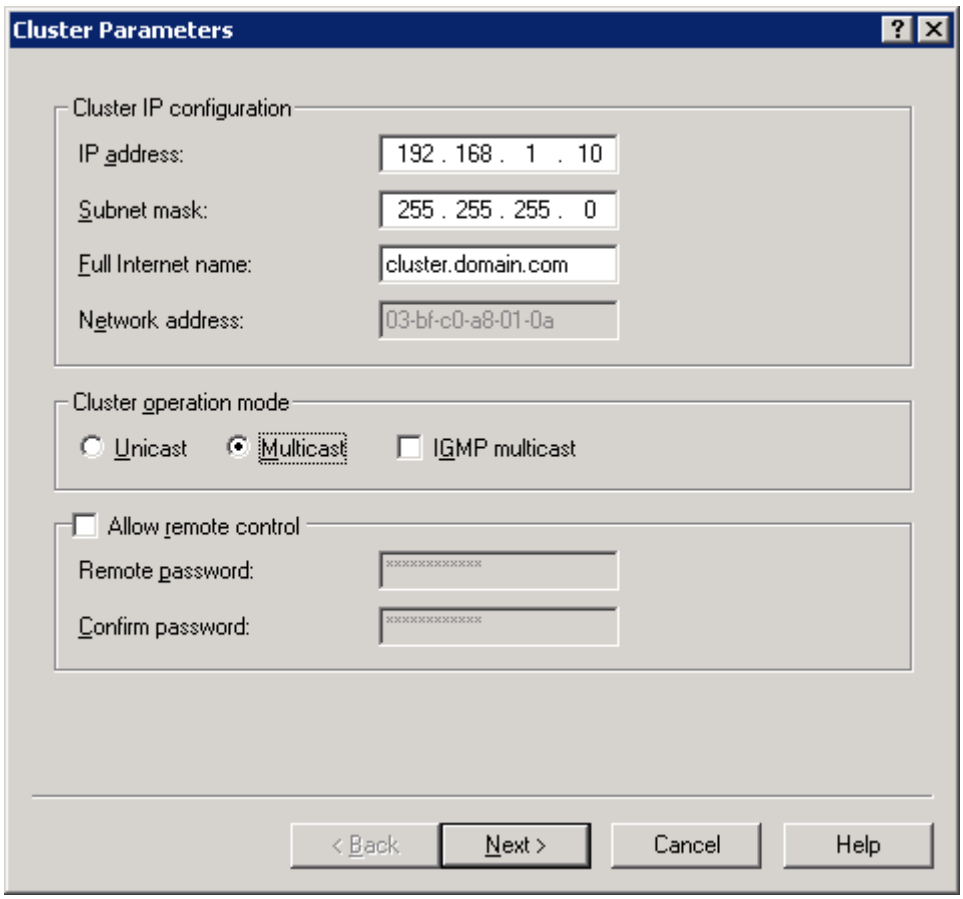
- Адрес VIP, который вы выбрали для кластера
- Уникальные адреса IP каждого из серверов фермы
- Алиас DNS, который вы хотите использовать для кластера
- Сетевой протокол и порт, который вы хотите использовать для распределения нагрузки (для RDP это TCP и порт 3389).
- Доменная учетная запись с правами администратора ко всем серверам кластера, или локальные учетные записи администраторов каждого сервера

Собрав эту информацию, вы должны запустить NLB Manager. Вы можете это сделать с любой системы WS2K3 или с клиента Windows XP, на котором установлен WS2K3 Administrative Tools.

NLB Manager позволяет создавать, конфигурировать и управлять кластерами NLB в сети. Для создания нового кластера выберите *New* из меню *Cluster*.



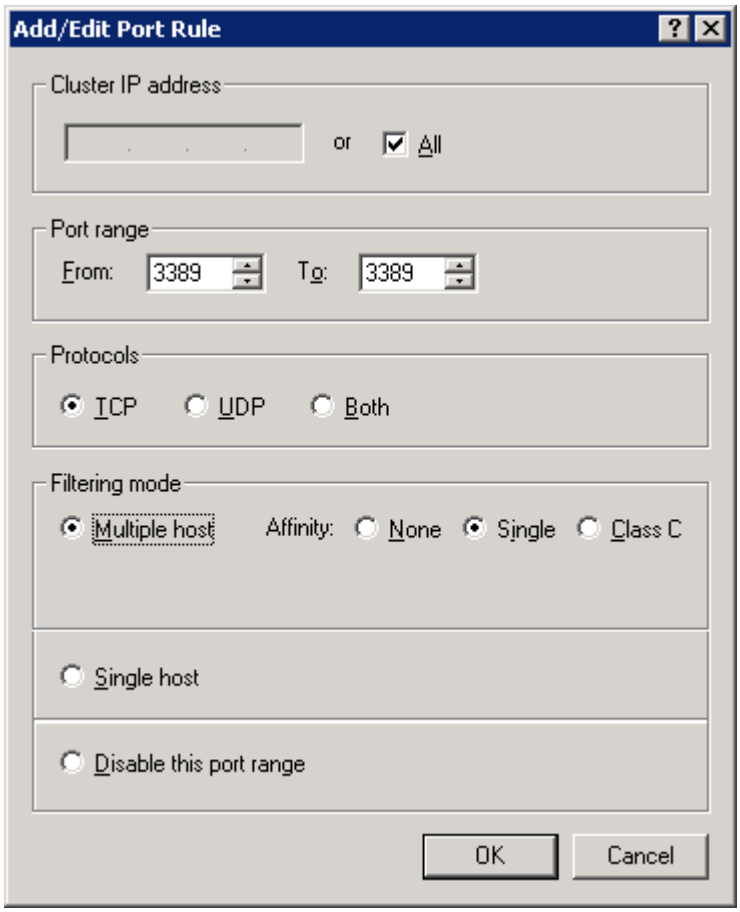
В окне *Cluster Parameters* введите адрес VIP и имя DNS нового кластера. Если вы планируете администрировать кластер с помощью NLB Manager, то не нужно разрешать удаленное управление или устанавливать пароль. NLB Manager использует Windows Management Interface (WMI), т.е. использует учетную запись пользователя.



Вы также можете выбрать, какой режим должна использовать межсерверная коммуникация - однонаправленный (unicast) или широковещательный (multicast). Если ваши терминальные серверы имеют по одному сетевому адаптеру, и ваша сеть поддерживает мультикастинг в подсети, вы должны разрешить широковещательный режим (multicast). Это позволит вам управлять кластером с помощью NLB Manager с любого сервера кластера. Заполнив параметры кластера, щелкните *Next*.

Дополнительную информацию см. статью "Technical Overview of Windows Server 2003 Clustering Services"

Следующее окно NLB Manager предлагает ввести дополнительные адреса IP, используемые в кластере. Эта информация обычно используется веб-серверами с распределением нагрузки, когда каждый сервер обслуживает несколько веб-сайтов, каждый из которых представлен уникальным адресом IP. Для терминальных серверов вы можете оставить это окно пустым и щелкнуть *Next* для вызова окна *Port Rules*.



Правила портов определяют, как должны обрабатываться соединения к VIP. По умолчанию весь траффик TCP и UDP равномерно распределяется по узлам кластера. Для терминальных серверов вам необходимо балансировать только RDP, поэтому подсветите правило default и щелкните *Remove* для его удаления. Затем щелкните *Add* для вызова окна *Add/Edit Port Rule.*

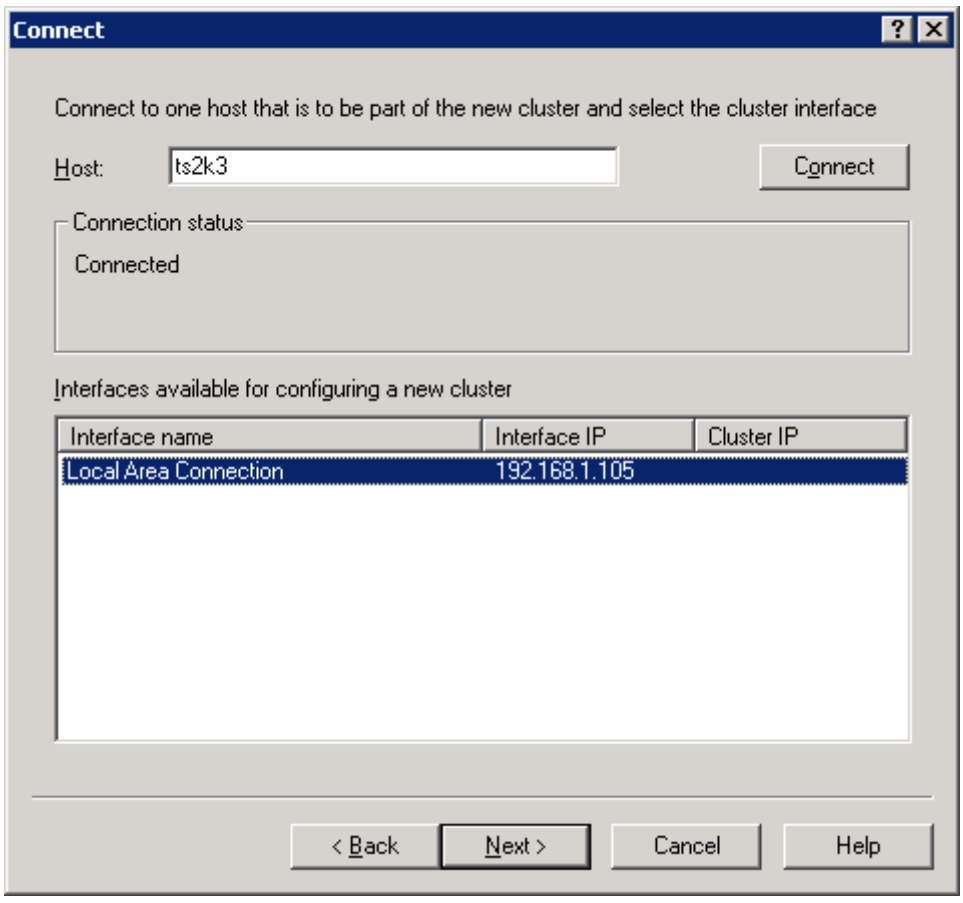
В этом окне укажите диапазон портов с 3389 по 3389 и выберите протокол TCP. Эта конфигурация создаст распределение нагрузки только для протокола RDP. Ограничив правила только протоколом RDP, вы снизите нагрузку на службу NLB и на серверы, защитив их от ошибочных запросов, посылаемых на адрес VIP на другие порты.

Оставьте режим фильтрации по умолчанию (multiple host, single affinity), смысл остальных опций следующий:

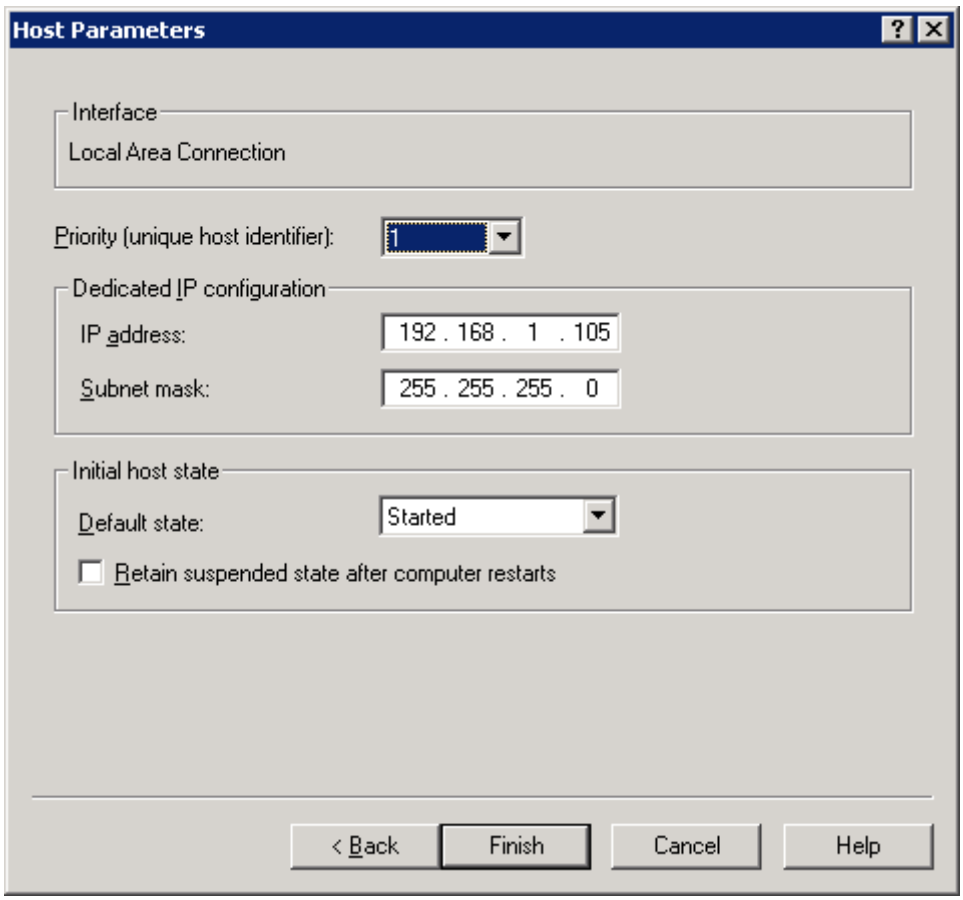
- Multiple host — Если выбрано, то соединение, выполняемое на указанный диапазон портов, будет распределяться среди нескольких узлов. В этом случае вы должны выбрать режим родственности (affinity). Родственность обеспечивает, что после того, как клиент будет направлен на указанный узел, клиент в течении сеанса будет продолжать направляться на тот же узел во всех коммуникациях.
  Опции родственности:
  - None - родственность не используется
  - Single - Родственность основывается на адресе IP клиента, балансировка выполняется на базе клиента
  - Class C - Родственность основана на подсети класса C клиентов. Когда один клиент устанавливает соединение к некоторому узлу, все соединения от той подсети будут направлены на тот же узел.
  - Single host - Соединения на указанынй диапазон портов будут направлены на один узел, а если этот узел недоступен - то на следующий узел, вычисляемый по номеру Handling Priority (приоритет обработки). Приоритет присваивается узлу при добавлении сервера в кластер.

Вы также можете запретить правило в этом окне. Это временно отключит разпределение нагрузки для указанного диапазона портов..

После настройки правил портов, щелкните *Next* для перехода к окну *Connect*. Введите в нем имя первого сервера, добавляемого к кластеру. NLB Manager установит соединение с этим сервером и выдаст список сконфигурированных сетевых адаптеров. Вы должны выбрать адаптер, на котором вы хотите принимать входящие соединения с VIP, и щелкнуть*Next*.



В последнем окне, *Host Parameters*, вы настраиваете конкретный сервер, выбранный для присоединения к кластеру. Здесь вы сначала должны установить номер приоритета, который одновременно используется как уникальный идентификатор узла. Вы можете изменить физический адрес IP сервера и маску подсети, а также установить начальное значение состояния службы распределения нагрузки после загрузки сервера.



После щелчка *Finish*, NLB Manager подключится к серверу через WMI и сконфигурирует службу NLB. После создания кластера вы вернетесь в основное окно NLB Manger, в котором увидите новый кластер. В этом окне вы можете щелкнуть правой кнопкой мыши на кластере для добавления к нему узлов. Всякий раз при добавлении сервера вам необходимо выбрать сетевой инерфейс и установить приоритет.

Завершив добавление терминальных серверов в кластер, вы можете опробовать NLB, используя клиент Remote Desktop Connection, указав в нем адрес VIP или имя DNS кластера. Ваше соединение должно быть направлено на один из серверов кластера.

Для подключения с использованием имени DNS кластера, вы должны либо разрешить в своей сети динамический DNS (DDNS), который позволяет службе NLB регистрировать имя кластера, или вручную добавить алиас кластера в базу данных DNS.

Другие балансировщики нагрузки

Хотя служба Microsoft NLB проста в настройке и администрировании, а также бесплатна во всех редакциях WS2K3, есть много причин присмотреться к балансировщикам нагрузки других производителей. Особенно если ваши серверы находятся в разных подсетях или вам необходимо поддерживать более 32 серверов.

Одним из важнейших факторов, которые следует учитывать при выборе балансировщика, является то, как балансировщик определяет нагрузку. Многие балансировщики, включая Microsoft NLB, просто подсчитывают число активных соединений к узлу. В среде терминальных серверов этот метод не всегда адекватен.

Некоторые балансировщики могут размещать на серверах метрики и определять нагрузку на основе доступной памяти, использования процессора и других коэффициентов производительности. Такие продукты имеют большое преимущество при распределении нагрузки терминальных среверов, поскольку отслеживают их текущую производительность.

Помимо балансировщиков нагрузки есть продукты, специально предназначенные для расширения возможностей Terminal Services. Эти продукты не только включают в себя средства распределение нагрузки, но и позволяют публиковать приложения, позволяя пользователям подключаться к приложениям, а не к рабочему столу. Лидерами в этой области являются Citrix MetaFrame (http://www.citrix.com) и New Moon Canaveral iQ (http://www.newmoon.com).

Каталог Сеансов (Session Directory)

Один из вопросов, возникающих при распределении нагрузки, состоит в том, что делать с разъединенными сеансами. Как мы обсуждали в главе 2, администраторы могут настроить на терминальных серверах тайм-ауты для холостых и разъединенных сеансов. Вы можете либо указать эти тайм-ауты очень низкими, давая возможность пользователю повторно соединиться с того же клиентского устройства и адресом IP в случае сбоя в сети, или вы можете установить большой тамй-аут, чтобы пользователи могли отключиться от сеанса, оставив приложение работать, а затем воссоединиться с ним позже.

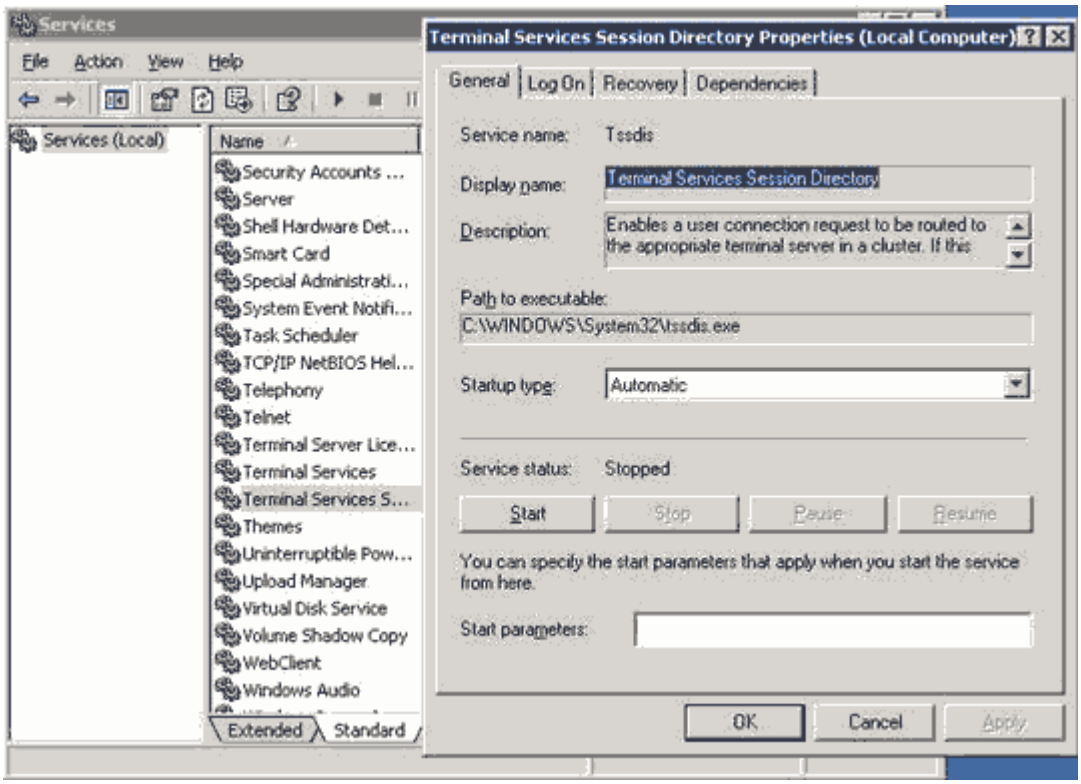
Эти настройки хорошо работают в среде с одним сервером. При повторном подключении пользователя, Session Manager подключает его к существующему сеансу. Однако, в случае кластера с распределением нагрузки, Session Manager ничего не знает о сеансах на других серверах. Поэтому Microsoft ввела понятие Каталога Сеансов (Session Directory).

Каталог Сеансов поддерживает динамическую базу данных, которая хранит соответствия имен пользователей и открытых сеансов на всех терминальных серверах кластера. Это позволяет пользователям подключаться к своим сеансам на любом сервере в кластере, независимо от того, на какой сервер его изначально направила служба NLB.

Настройка каталога сеансов

Чтобы получить преимущества каталога сеансов, все терминальные серверы в кластере должны иметь редакцию Enterprise или Datacenter. Session Directory может использовать любую редакцию WS2K3. Вы даже можете создать Session Directory на одном терминальном сервере в кластере, хотя это не рекомендуется, поскольку остановка этого сервера для осблуживания или установки ПО может затронуть весь кластер.

Для настройки Каталога Сеансов, начните с сервера, на котором будет храниться база данных сеансов. На этом сервере откройте Computer Management or Services для доступа к Terminal Services Session Directory. Откройте свойства службы, настройте ее на автоматический запуск и запустите ее.



При первом запуске службы Session Directory она создает новую локальную группу Session Directory Computers. Чтобы терминальные серверы информировали сервер каталога сеансов о своих сеансах или запрашивали каталог сеансов с других серверов, терминальный сервер должен быть членом этой группы. Вы можете добавить в эту группу индивидуальные компьютеры в кластере или создать доменную группу, содержащую терминальные серверы, и добавить эту группу в Session Directory Computers.

После того, как вы создали сервер каталога сеансов, необходимо настроить терминальные серверы. Вы можете использовать либо утилиту Terminal Services Configuration, либо редактор групповых политик. В редакциях WS2K3 Enterprise или Datacenter, узел Server Settings в Terminal Services Configuration имеет дополнительную опцию - Session Directory.

Здесь вы вводите имя кластера NLB, к которому принадлежит терминальный сервер, и имя хоста или адрес IP сервера каталога сеансов. Если терминальный сервер имеет несколько сетевых адаптеров, вы должны выбрать один из них для направления на него клиентов. Вы также должны указать, следует ли подключать клиента к уникальному адресу IP этого сервера , выбрав редирект адреса IP, или использовать редирект маркеров маршрутизации, если адрес сервера невидим клиентам.

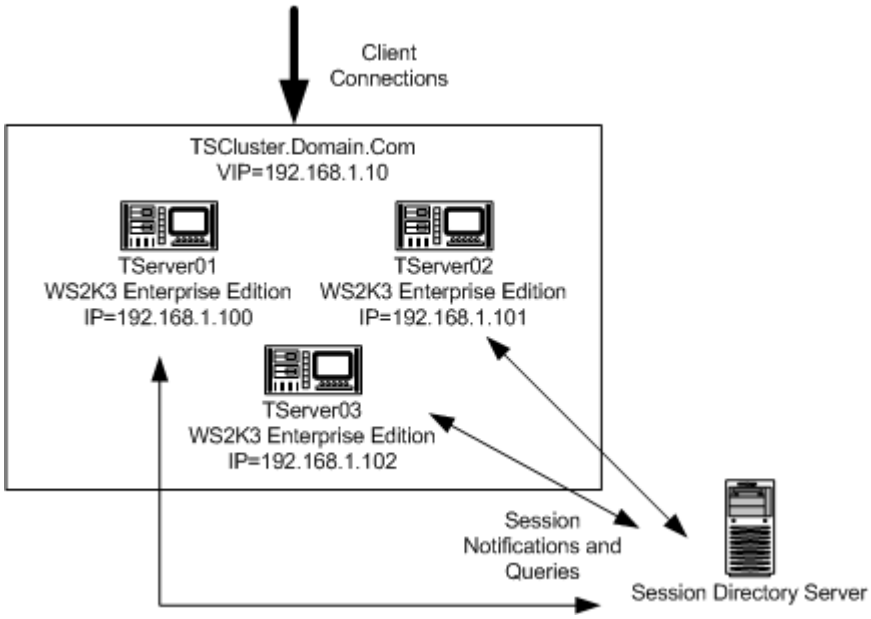
При использовании Microsoft NLB вы должны выбрать редирект адреса IP, поскольку NLB не поддерживает маркеры маршрутизации.

Если вы решили использовать Terminal Services Configuration, то вам необходимо сделать эти настройки вручную на всех терминальных серверах. Если вы используете Active Directory, то используйте групповые политики. Для этого создайте или отредактируйте GPO и примените их ко всем серверам кластера. Затем откройте редактор групповых политик, найдите Computer Configuration, Administrative Templates, Windows Components, Terminal Services, Session Directory. Там содержатся все настройки, доступные в Terminal Services Configuration. Разрешите все четыре параметра и введите необходимую информацию. При следующем обновлении политик все серверы кластера будут использовать каталог сеансов.

При использовании Session Directory, сервер, содержащий базу данных, становится критическим для функционирования терминальных серверов. Вы можете использовать кластеры Windows, чтобы сделать каталог сеансов отказоустойчивым. Microsoft написала инструкции для этого в статье “Session Directory and Load Balancing Using Terminal Server”

Как работает каталог сеансов

Здесь приведен пример работы каталога сеансов. Утром пользователь Joe User использует клиента Remote Desktop Connection для подключения к TSCluster.Domain.Com. Служба NLB направляет это соединение на сервер TServer02, наименее загруженный сервер в это время. Джо регистрируется на TServer02, и поскольку он еще не имеет существующего сеанса на TServer02, сервер запрашивает службу Session Directory на предмет существующих сеансов, принадлежащих Joe User на любом сервере в кластере. Joe не имеет никаких других сеансов, поэтому TServer02 принимает соединение и Джо начинает работу.



В 3:00, Джо решает поехать домой и продолжить работу оттуда. Он уже напечатал половину документа и открыл три окна веб-браузера со справочным материалом, поэтому от отключился, но не завершил сеанс, чтобы продолжить работу с того места, где он ее оставил. Когда Джо отключается от сеанса, TServer02 информирует сервер каталога сеансов о разъединенном сеансе. Сервер каталога сеансов создает запись в своей базе данных, включая имя пользователя и домен для Джо, имя сервера, время создания и отключения сеанса, а также разрешение и глубину цвета сеанса.

Придя домой, Joe устанавливает соединение VPN с корпоративной сетью. Он запускает на своем домашнем компьютере клиента Remote Desktop Connection и указывает имя TSCluster.Domain.Com. Служба NLB направляет соединение на уникальный адрес IP сервера с наименьшим числом соединений - на этот раз это TServer01. Джо вводит свое имя и пароль для TServer01.

TServer01 сначала проверяет свои разъединенные сеансы Джо. Если таковых не найдено, он запрашивает базу данных каталога сеансов. База данных находит сеанс Джо на сервере TServer02 и сообщает клиенту Remote Desktop Connection адрес IP сервера TServer02, а также шифрованные имя и пароль Джо. Клиент Remote Desktop Connection автоматически подключается к TServer02 и посылает учетные данные. TServer02 находит существующий сеанс Джо и подключает к нему Джо, который начинает продолжать работу над своим документом.

Глава 4. Администрирование терминального сервера

Как и при любом внедрении технологии, процесс инсталляции и конфигурирования терминального сервера - это всего лишь половина работы. Вы должны также спланировать администрирование и сопровождение, а также поддержание цикла жизни программного обеспечения. В этой главе я сфокусируюсь на администрировании терминальных служб, включая конфигурацию учетных записей пользователей. Кроме того, я объясню настроку групповых политик с точки зрения Active Directory.

Требования для доступа к терминальному серверу

WS2K3 имеет три различных уровня защиты, которые позволяют контролировать доступ к терминальному серверу. Чтобы пользователь мог зарегистрироваться на терминальном сервере, необходимо соблюдение следующих трех условий:

- Право *Allow log on through Terminal Services* (разрешен вход через службу терминалов) — В Windows 2000 вам необходимо было давать право *Log on locally* всем пользователям, которым требовался доступ терминальному серверу. Это создавало потенциальную брешь в безопасности, поскольку позволяло регистрироваться на консоли сервера, обходя ограничения, которые вы сделали для RDP. WS2K3 разделяет право локального входа и право входа через службу терминалов. По умолчанию, на WS2K3 право *Allow log on through Terminal Services* дается только администраторам и членам группы Remote Desktop Users.

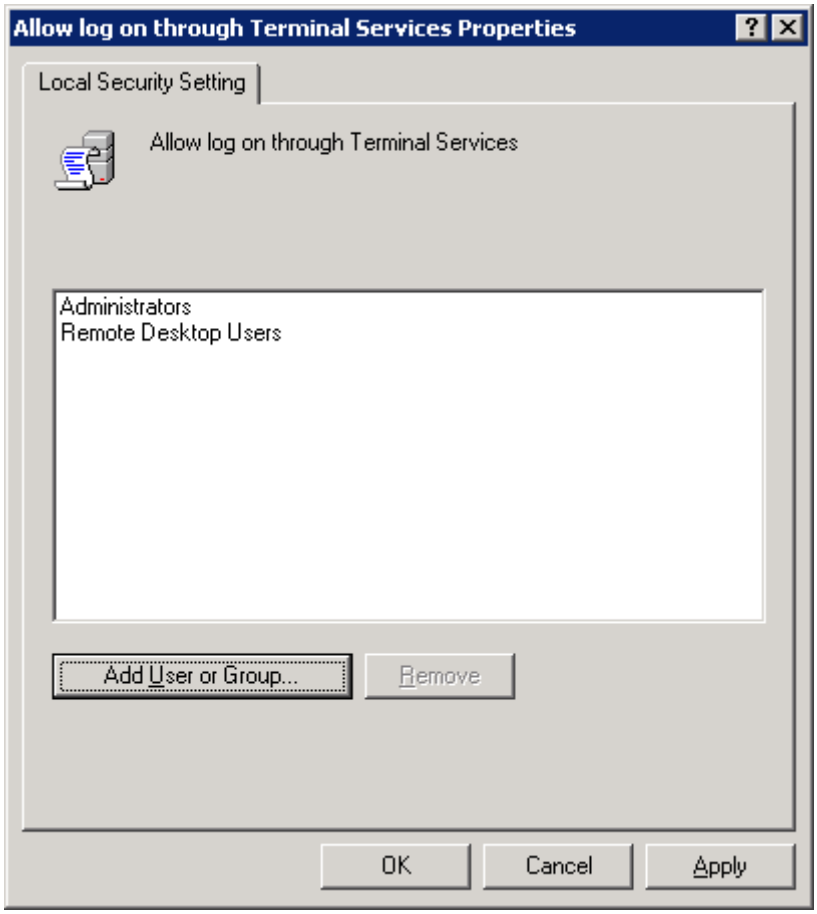
- Права использовать RDP — Администратор может установить разрешения RDP с помощью Terminal Services Configuration. Как уже упоминалось, Microsoft изменила разрешения по умолчанию для протокола в WS2K3. Если в Win2K локальной группе Users был разрешен доступ к RDP, то в WS2K3 этот доступ ограничен только локальной группой Remote Desktop Users. Поэтому чтобы пользователи могли регистрироваться на терминальном сервере, вы должны поместить их в эту группу.

- Опция *Allow logon to terminal (разрешен вход на терминальный сервер)* — В свойствах каждого пользователя в AD есть опция *Allow logon to terminal server*, которая определяет, разрешено ли пользователю регистрироваться на терминальном сервере. По умолчанию эта опция включена.

Два из этих условий зависят от членства в группе *Remote Desktop Users*. Если пользователь получает сообщение *You do not have permission to access this session*, то одно из этих трех условий не соблюдается.

Allow Log On Through Terminal Services

Доступ к привилегии *Allow log on through Terminal Services* (разрешен вход через Terminal Services) осуществляется либо из Local Security Policy, либо из редактора групповых политик (`GPEDIT.MSC`), в Security Settings, Local Policies, User Rights Assignment. После установки роли Terminal Services, эта привилегия дается локальной группе пользователей Remote Desktop Users.

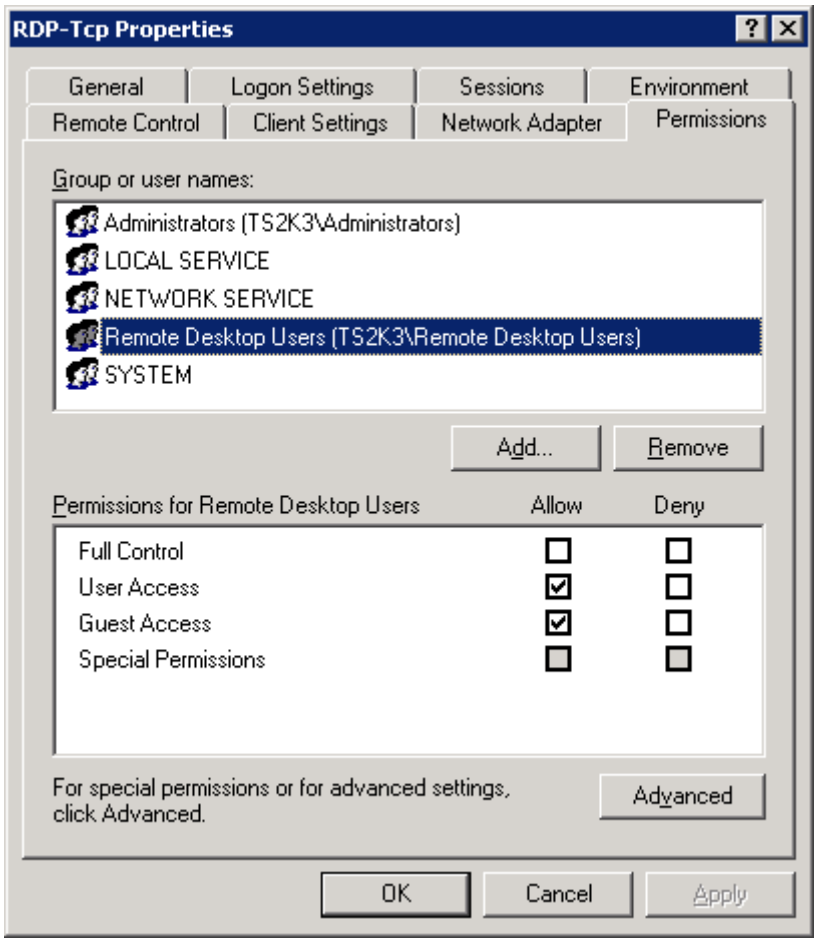


Если терминальный сервер находится в домене AD, редактор Local Security Policy показывает как локальные настройки, так и эффективные, поскольку права могут назначаться доменными групповыми политиками. Если вы обнаружили, что эффективные права не дают достаточных привилегий нужным пользователям, вам следует использовать инструмент Resultant Set of Policy (RSOP.MSC) для определения того, какой объект GPO отзывает право.

Даже в WS2K3 право *Log on locally* открыто как администраторам, так и пользователям. Если терминальный сервер находится в незащищенной среде, вы можете ограничить это право только для администраторов, а пользователям разрешить доступ только через службу терминалов.

Разрешения для RDP

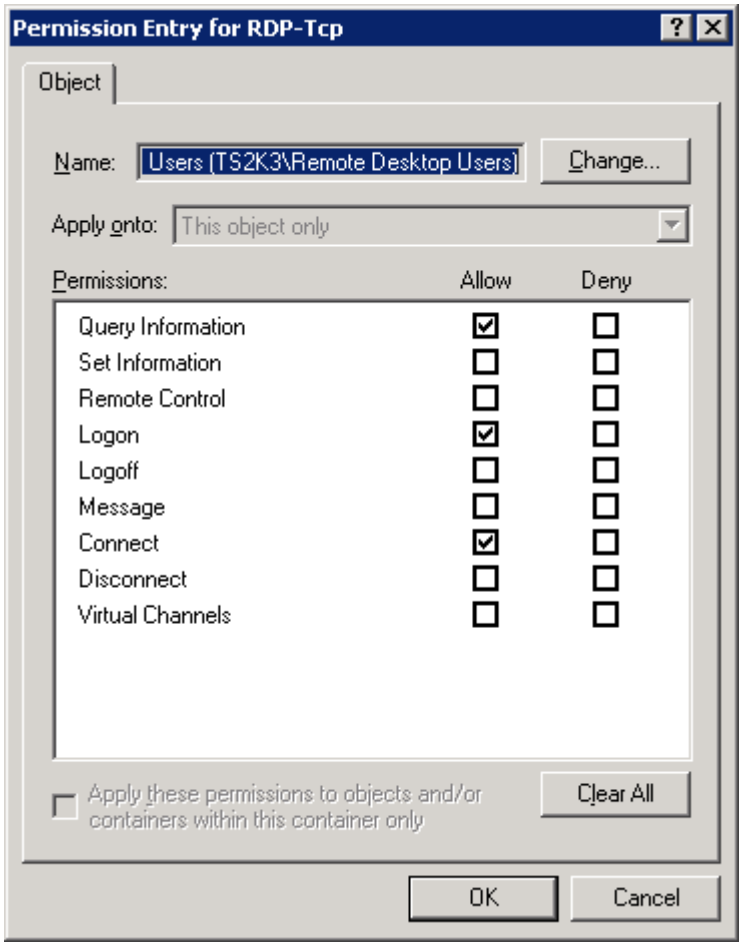
Вкладка *Permissions* свойств соединения RDP-Tcp показывает, что право использовать RDP разрешено администраторам и членам группы Remote Desktop Users. По умолчанию группа Remote Desktop Users пустая, поэтому чтобы позволить пользователям подключаться к терминальному серверу, вам необходимо добавить их в эту группу.



Как видно из рисунка, группа Remote Desktop Users по умолчанию разрешает доступ User Access. Каждый уровень доступа - гость, пользователь, полный контроль - идет с разным набором разрешений к сеансам на терминальном сервере. Чтобы полностью использовать мощь этих разрешений, вы должны понять, что предоставляет каждый из этих уровней доступа и какие доступны дополнительные опции.

Уровни доступа RDP

RDP предоставляет три основных уровня доступа: Guest Access (гость), User Access (пользователь) и Full Control (полный доступ). Уровень, назначенный группе, определяет возможности группы при подключении к терминальному серверу через RDP. Давайте разберемся с доступными разрешениями, а затем ассоциируем их с базовыми уровнями доступа. На следующем рисунке показан базовый список разрешений, а в таблице показано, как они относятся к пользователям.



Разрешение	Описание
Query Information	Запрос информации через Terminal Services Administrator или с комадной строки утилитой QUERY.
Set Information	Изменение настроек и разрешений RDP.
Remote Control	Просмотр или удаленное управление сеансом другого пользователя
Logon	Вход на сервер
Logoff	Принудительное завершение сеанса другого пользователя
Message	Отправка сообщений в другие сеансы на сервере используя консоль Terminal Services Manager или с комадной строки командой MSG
Connect	Подключение к разъединенному сеансу того же пользователя
Disconnect	Принудительное отключение сеанса другого пользователя, оставляя сеанс на сервере в активном состоянии.
Virtual Channels	Использование виртуальных каналов - коммуникационных каналов, которые разрабочики могут использовать для расширения возможностей RDP. Пока System имеет это разрешение, пользователи могут использовать приложения, использующие виртуальные каналы.

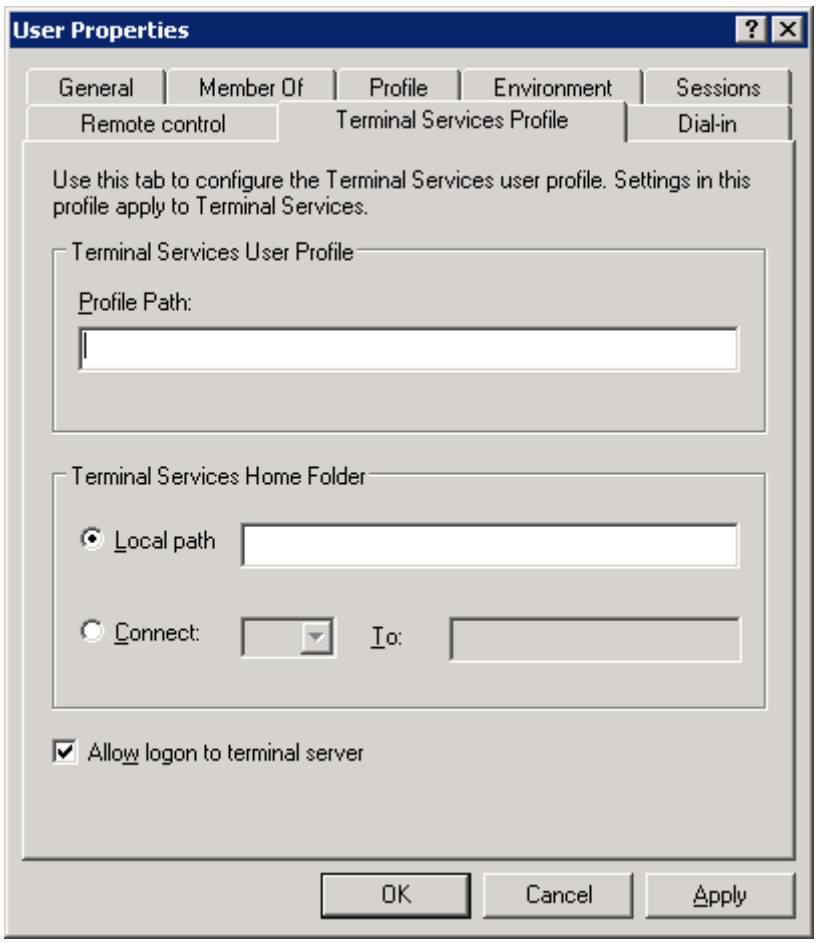
В следующей таблице показано, какие разрешения назначены уровням доступа. Вы можете использовать редактор ACL для создания особых наборов разрешений. Например, вы можете дать сотрудникам справочного стола почти все разрешения Full Control, кроме Set Information.

Permission	Guest Access	User Access	Full Control

Query Information		X	X
Set Information			X
Remote Control			X
Logon	X	X	X
Logoff			X
Message			X
Connect		X	X
Disconnect			X
Virtual Channels			X

Allow Logon to Terminal Server

Последнее требование для регистрации на терминальном сервере делается на уровне пользователей. В свойствах пользователей есть четыре вкладки, относящиеся к настройкам терминального сервера. Большинство из них затрагивают поведение сеанса при подключении пользователя к терминальному серверу. Вы можете использовать опцию *Allow logon to terminal server* чтобы целиком ограничивать способность пользователя подключаться к терминальному серверу. По умолчанию эта опция включена.



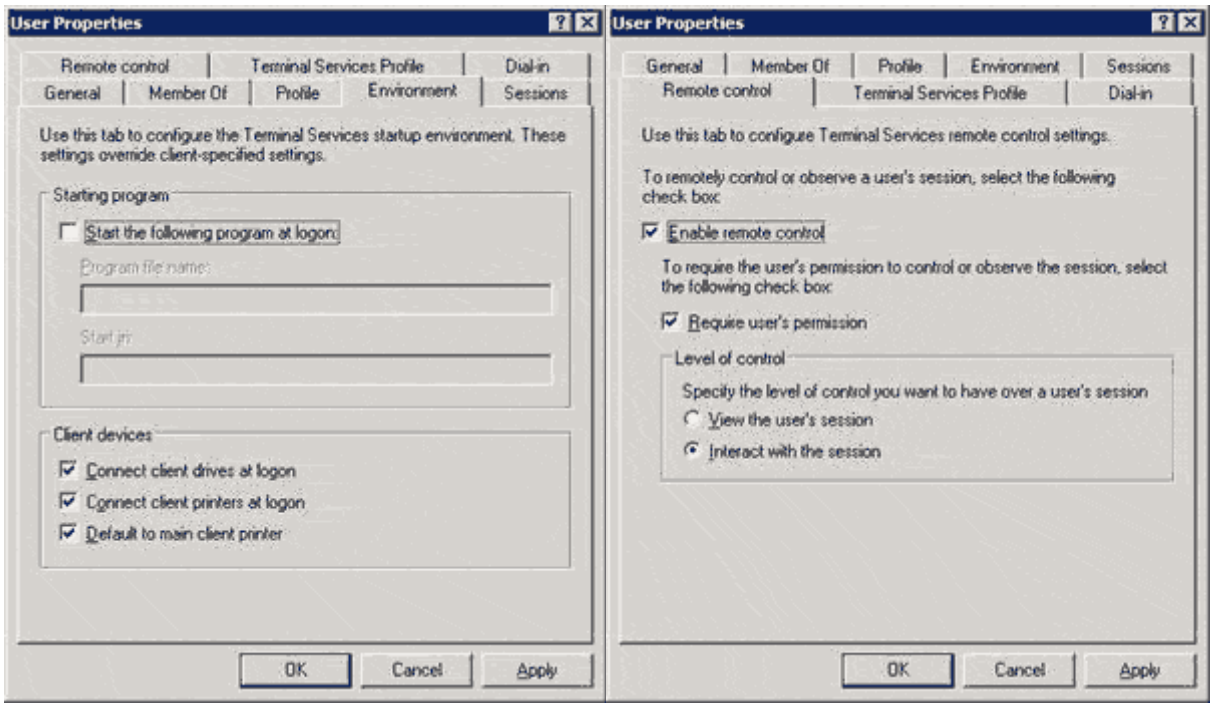
Настройка учетных записей пользователей

Пока мы рассматриваем интерфейс User Properties, я хотел бы обсудить остальные настройки терминального сервера. Большинство из этих настроек доступны в Terminal Services Configuration. Вы сами решаете, на каком уровне их применять - для отдельных пользователей или для сервера. Учтите, что настройки пользователя переопределяют настройки сервера. Для доступа к

пользовательским настройкам используйте один из следующих инструментов: для доменов AD используйте инструмент Active Directory Users and Computers; для доменов NT 4.0 используйте User Manager for Domains, а для рабочих групп - Computer Management.

Вкладка Terminal Services, показанная в этом разделе, не видна в версии User Manager for Domains для NT 4.0; вы должны использовать версию этого инструмента для Win2K, WS2K3 или NT 4.0 Terminal Server Edition.

Независимо от используемого инструмента, вам доступны одни и те же опции. На следующем рисунке показаны вкладки *Environment* и *Remote control.*

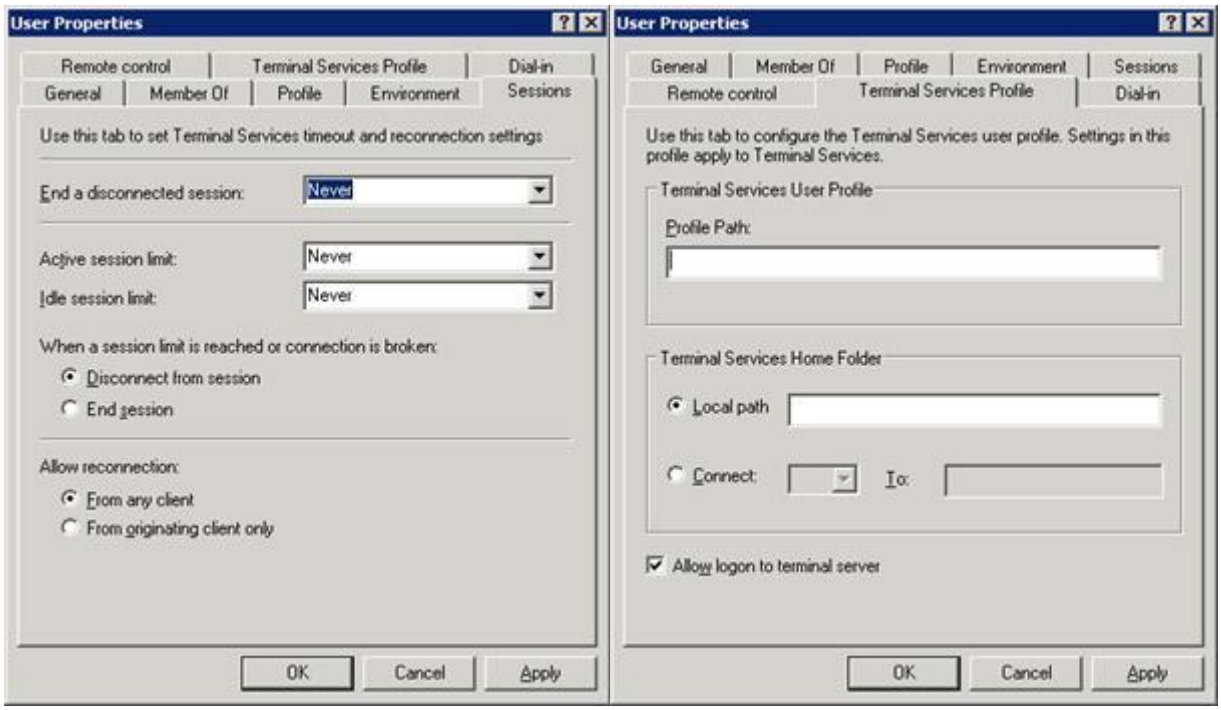


Вкладка *Environment* используется для указания начальной программы и настроек переназначения ресурсов клиента. Если вы разрешите опцию *Start the following program at logon* setting, то при каждом подключении пользователя вместо рабочего стола будет запущена указанная программа.

В этом разделе настройки сервера переопределяют настройки пользователя. Так, если вы указали начальную прогорамму и в настройках пользователя, и в настройках сервера (с помощью Terminal Services Configuration), то будет запущена программа, указанная в настройках сервера.

На вкладке *Remote control* вы можете разрешить или запретить возможность удаленного управления сеансом этого пользователя. Если вы разрешаете удаленное управление, вы также можете указать требовать от пользователя разрешения, а также установить уровень управления. Эти настройки будут переопределены, если удаленный доступ сконфигурирован на сервере с помощью Terminal Services Configuration.

Вкладка *Sessions* позволяет установить тайм-ауты для терминальных сеансов. На этой вкладке вы можете установить тайм-ауты для активных, холостых и разъединенных сеансов. Вы можете выбрать поведение при потере соединения или превышении лимита времени сеанса - отключить сеанс или завершить его. Вы также можете выбрать, может ли пользователь подключаться к разъединенному сеансу с любого клиентского устройства или только с того, с которого инициировал сеанс.



На вкладке *Terminal Services Profile* вы можете установить профиль и домашний каталог, используемый при регистрации пользователя на терминальном сервере. Здесь также находится опция *Allow logon to terminal server*, определяющая, может ли вообще пользователь регистрироваться на терминальном сервере. В отличие от других настроек в этом разделе, она не дублируется в Terminal Services Configuration.

Домашний каталог и каталог профиля

Будучи системным администратором, вы вероятно знакомы с сетевыми домашними каталогами и перемещаемыми профилями. Эти особенности Windows позволяют поддерживать центральное хранилище для пользовательских документов и настроек профиля, чтобы они были доступны независимо от компьютера, за которым сидит пользователь.

Terminal Services может поддерживать разные хранилища для домашних данных и профилей пользователей.

Путь к профилю Terminal Services

При регистрации пользователя на рабочей станции, система проверяет атрибут Profile Path объекта пользователя. Если пользователь имеет централизованно хранящийся профиль, и этот профиль новее, чем его локально кешированная копия, то профиль загружается для этого пользователя. Аналогично, когда пользователь регистрируется на терминальном сервере, система запрашивает атрибут UserParameters и ищет Terminal Services Profile Path.

Это разделение позволяет поддерживать разные профили пользователей в зависимости от того, какой тип компьютера они используют. В большинстве случаев вы захотите получить преимущества профилей Terminal Services, поскольку некоторые функции Terminal Services осложняют жизнь, если вы не используете профили Terminal Services. Позвольте мне объяснить, что я имею ввиду. Если вы не используете перемещаемые профили для ваших пользовательских рабочих станций, то вы зависите от поддержки компьютером копии пользовательского профиля. Если пользователь не регистрируется на нескольких ПК, эта настройка работает прекрасно. Однако, на терминальном сервере отказ от использования перемещаемых профилей означает, что терминальный сервер должен поддерживать профили для *всех* пользователей, что требует много дискового пространства. Кроме того, если вы хотите использовать распределение нагрузки и каталог сеансов для распределения пользователей по нескольким терминальным серверам, вам придется поддерживать профили пользователей на каждом сервере.

Использование профилей Terminal Services позволяет пользователю получать одинаковые настройки независимо от того, к какому серверу он подключается. Для избежания проблем с дисковым пространством вы можете разрешить системную политику, которая удаляет локальные кешированные копии перемещаемых профилей.

Если вы не указали терминальный профиль, но указали перемещаемый профиль Windows, терминальный сервер будет использовать перемещаемый профиль Windows. Кроме того, если терминальный профиль указан, но недоступен, система вернется к профилю Windows. Это поведение может вызвать нежелательные результаты, если вы используете на сервере сценарии совместимости приложений.

Если вы используете перемещаемые профили Windows, использование профилей Terminal Services может стать еще более важным, поскольку если система не находит путь к терминальному профилю в учетной записи пользователя, она ищет путь к профилю Windows. В главе 5 вы познакомитесь со скриптами совместимости приложений, которые позволяют приложениям корректно работать на терминальном сервере. Эти скрипты вносят изменения в реестр в раздел HKEY_CURRENT_USER, чтобы помочь в настройке приложений для нескольких пользователей. Если эти изменения делаются в пользовательском профиле Windows, то пользователь может столкнуться с проблемами, когда в следующий раз зарегистрируется на рабочей станции.

География также может стать причиной разделения профилей. Скорее всего, вы захотите хранить пользовательские профили Windows на файловых серверах поближе к рабочим станциям, но терминальные серверы из-за их невысоких требований к пропускной способности могут находиться в центрах данных. Вы не хотите, чтобы профили закачивались по медленным каналам связи.

WS2K3 имеет две новые политики, которые управляют пользовательскими профилями. *Allow only local user profiles* предотвращает указанному компьютеру загружать перемещаемые профили, даже если они сконфигурированы для пользователей. *Set Path for TS Roaming Profiles* позволяет указать специфический файловый сервер, который будет использоваться для перемещаемых профилей всех пользователей, регистрирующихся на терминальном сервере.

Домашние каталоги

Вы можете настроить учетные записи пользователей так, чтобы при регистрации на терминальном сервере они использовали другие домашние каталоги. Как вы увидите в главе 5, система использует пользовательский домашний каталог на драйве ROOTDRIVE и хранит там скрипты совместимости приложений. Отдельные домашние каталоги для терминалов позволяют держать файлы вне домашнего каталога Windows пользователя. Проблема состоит в том, что если ваш пользователь сохранил свои документы в домашнем каталоге Windows, то пользователю необходим доступ к тому же каталогу при регистрации на терминальном сервере. Если вы определили маршрут к домашнему каталогу Terminal Services, этот маршрут будет прменяться вместо домашнего каталога Windows. Если вы не указали домашний каталог Terminal Services, то будет использоваться домашний каталог Windows.

Настройка свойств пользователей через интерфейсы Active Directory Service

Использование графических утилит для конфигурации пользователей удобно, если у вас мало пользователей. Но если вам необходимо конфигурировать большое число пользователей, то легче это делать с использованием интерфейса службы активного каталога (Active Directory Service Interfaces, ADSI). По сравнению с Win2K эта особенность значительно улучшена.

Доступ к ADSI осуществляется через Windows Script Host (WSH), поэтому вы можете использовать скрипты на Visual Basic Script (VBScript) или Java Script. Примеры, приведенные далее, написаны на VBScript.

Конфигурирование пользователей через ADSI состоит из трех этапов. Сначала вы должны открыть соединение с учетной записью пользователя, затем установить свойства, и наконец записать изменения в учетную запись пользователя. Для открытия соединения вы используете либо

провайдера WinNT, либо LDAP. Провайдер WinNT используется записями Security Accounts Manager (SAM) - либо локальными учетными записями на терминальном сервере, либо записями в домене NT 4.0. LDAP используется для учетных записей пользователей в AD.

Хотя вы можете использовать эти скрипты для конфигурирования как учетных записей домена NT 4.0, так и Win2K AD, вы можете запустить их только на сервере WS2K3; они не будут работать на Win2K и даже на Windows XP.

Синтаксис для соединения:

```
Set objUser = GetObject("WinNT://<domain name>/<username>,user"
```

или

```
Set obUser = Get Object("LDAP://<distinguished name of user>")
```

Как видно, для использования LDAP вы должны знать отличительное имя объекта пользователя (например, cn=joe.user,ou=users,dc=example,dc=domain,dc=com), что нелегко, если ваши пользователи расположены в нескольких OU. Для облегчения этого Microsoft разрешила использовать провайдера WinNT также для учетных записей AD. Контроллер домена автоматически транслирует вызовы WinNT в вызовы LDAP.

Открыв учетную запись, вы устанавливаете параметры, которые хотите изменить. Имена параметров Terminal Services и синтаксис их использования приведены ниже:

```
objUser.ConnectClientDrivesAtLogon = [1,0]
objUser.ConnectClientPrintersAtLogon = [1,0]
ObjUser.DefaultToMainPrinter = [1,0]
objUser.TerminalServicesInitialProgram = ["path to program"]
objUser.TerminalServicesWorkDirectory = ["path to directory"]
objUser.TerminalServicesProfilePath = ["path to directory"]
objUser.TerminalServicesHomeDirectory = ["path to directory"]
objUser.TerminalServicesHomeDrive = ["drive letter:"]
objUser.AllowLogon = [1,0]
objUser.MaxDisconnectionTime = [minutes, 0 for never]
objUser.MaxConnectionTime = [minutes, 0 for never]
objUser.MaxIdleTime = [minutes, 0 for never]
objUser.BrokenConnectionAction = [1,0]
      1 = end session, 0 = disconnect the sesion
objUser.ReconnectionAction = [1.,0]
      1 = original client only, 0 = any client
objUser.EnableRemoteControl = [0,1,2,3,4]
0 = Disable Remote Control
     1 = Enable Notify & Enable Interact
     2 = Disable Notify & Enable Interact
     3 = Enable Notify & Disable Interact
     4 = Disable Notify & Disable Interact
```

Наконец, вы должны сохранить изменения в учетной записи пользователя:

```
objUser.SetInfo
```

Теперь объединим все это вместе и настроим параметры для одной учетной записи пользователя:

```
Set objUser =
GetObject("LDAP://cn=joe.user,ou=users,dc=example,dc=domain,dc=com")
' илиr: Set objUser = GetObject("WinNT://example/joe.user,user")
objUser.ConnectClientDrivesAtLogon = 1
objUser.ConnectClientPrintersAtLogon = 1
objUser.DefaultToMainPrinter = 1
objUser.TerminalServicesInitialProgram = "C:\windows\notepad.exe"
```

```
objUser.TerminalServicesWorkDirectory = “c:\windows”
objUser.TerminalServicesProfilePath = “\\server\tsprofiles\joe.user”
objUser.TerminalServicesHomeDirectory = “\\server\home\joe.user”
objUser.TerminalServicesHomeDrive = “H:”
objUser.AllowLogon = 1
objUser.MaxDisconnectionTime = 15
objUser.MaxConnectionTime = 0
objUser.MaxIdleTime = 180
objUser.BrokenConnectionAction = 0
objUser.ReconnectionAction = 0
objUser.EnableRemoteControl = 1
objUser.SetInfo
```

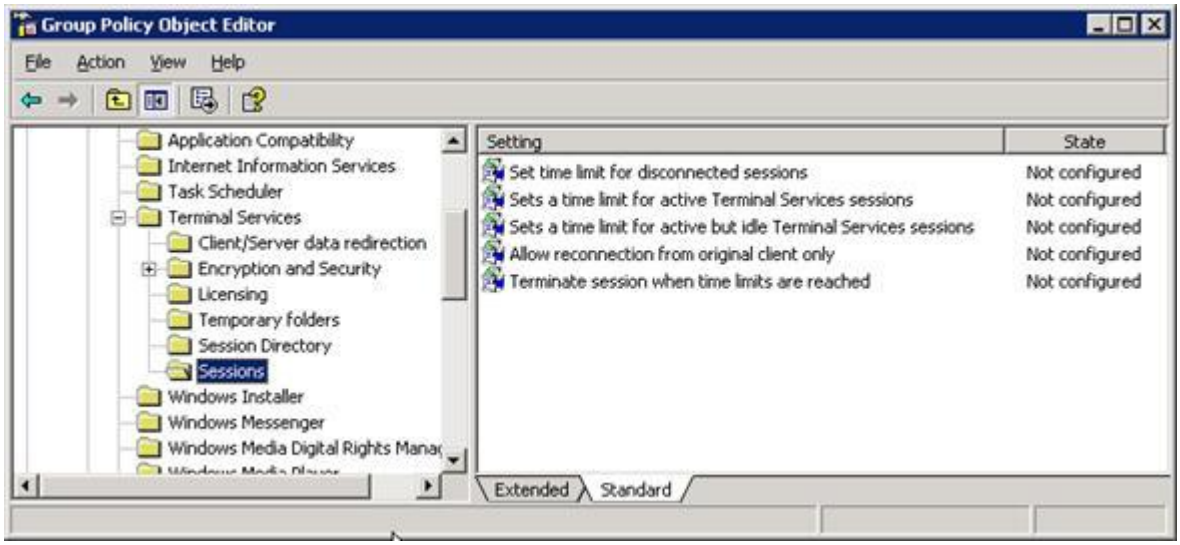
Конечно, если вам нужно сконфигурировать одну учетную запись, то быстрее и проще это сделать графической утилитой, но ADSI удобен для одновременного конфигурирования свойств для множества пользователей.

Microsoft TechNet Script Center (http://www.microsoft.com/technet/scriptcenter) - отличный ресурс для административных скриптов. Даже с небольшим знанием программирования вы можете изменить примеры скриптов, приспособив их для своих нужд.

Групповые политики

WS2K3 включает новый уровень гибкости при конфигурировании пользовательских сеансов - групповые политики. Как вы уже знаете, вы можете конфигурировать тайм-ауты сеансов, настройки ресурсов клиента, опции восстановления соединения для индивидуальных пользователей или отдельных серверов. С помощью групповых политик WS2K3 вы также можете управлять всеми этими опциями с помощью GPO.

Для повышения гибкости эти настройки можно конфигурировать для пользователей и для компьютеров. Поэтому вы можете устанавливать все опции для всех серверов с центрального места. Вы даже можете применять GPO к отдельным группам безопасности, чтобы администраторы имели доступ к другим опциям, чем обычные пользователи; вам не нужно делать настройку индивидуальных пользователей.



Если вам необходимо установить опции в нескольких местах, или вы мигрируете из существующей терминальной инфраструктуры Win2K и уже сконфигурировали ваших пользователей и серверы, вы должны знать приоритет этих опций:

1. Настройки Computer Configuration Group Policy
2. Настройки User Configuration Group Policy
3. Настройки утилиты Terminal Services Configuration
4. Настройки пользовательской учетной записи

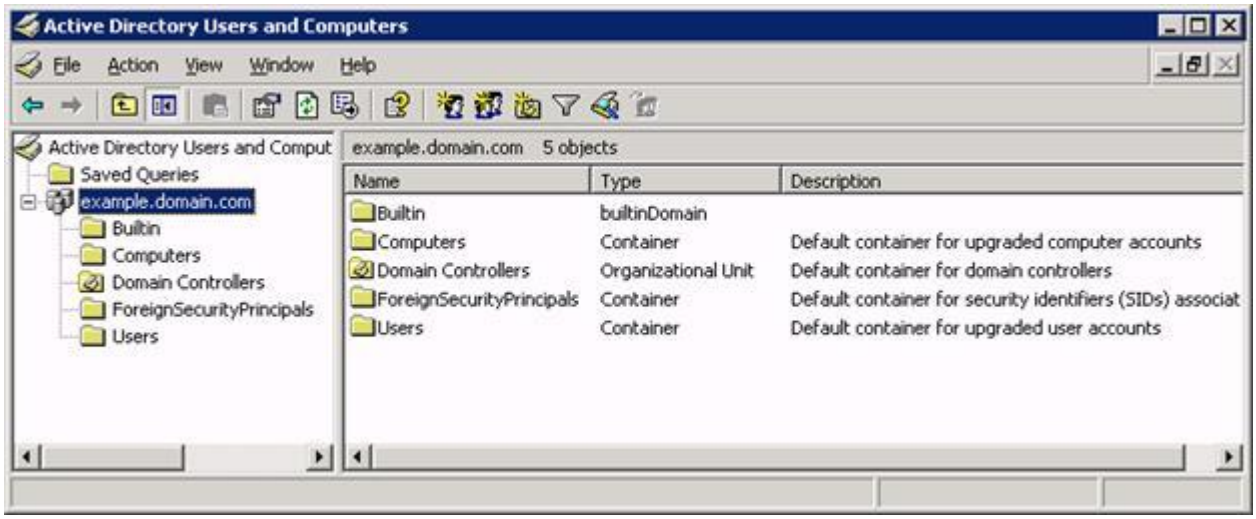
Будут побеждать настройки с более высоким приоритетом, поэтому настройки в Computer Configuration будут переопределять настройки User Configuration и т.п.

Управление терминальными серверами в среде AD

При работе в среде AD вы имеете возможность централизовать конфигурацию ваших терминальных серверов, облегчая ввод новых серверов в ферму. В этом разделе мы сосредоточимся на инструментах, используемых для настройки и управления терминальнми серверами в AD.

Active Directory Users and Computers

Active Directory Users and Computers - это административная утилита, используемая для управления OU, пользователями, компьютерами и группами в AD. На следующем рисунке показан интерфейс Active Directory Users and Computers.



В конфигурации по умолчанию объекты AD разделены в 5 основных категорий:

- *Users* - Контейнер по умолчанию для объектов пользователей, содержит встроенных пользователей, таких как Administrator и Guest, а также всех пользователей, которые находились в домене NT 4.0 при обновлении. Этот контейнер также содержит доменные глобальные группы, такие как Domain Admins и Domain Users.
- *Computers* - Контейнер по умолчанию для объектов типа компьютер, включает в себя все рабочие станции и серверы-члены, которые находились в домене NT 4.0 при обновлении.
- *Domain Controllers* - Контейнер по умолчанию для контроллеров доменов
- *Builtin* - Этот контейнер содержит встроенные доменные локальные группы, которые система использует для управления родными правами, как Server and Account Operators and Administrators.
- *ForeignSecurityPrincipals* - Этот контейнер используется системой для хранения ссылок на пользователей и компьютеры из других доверенных доменов.

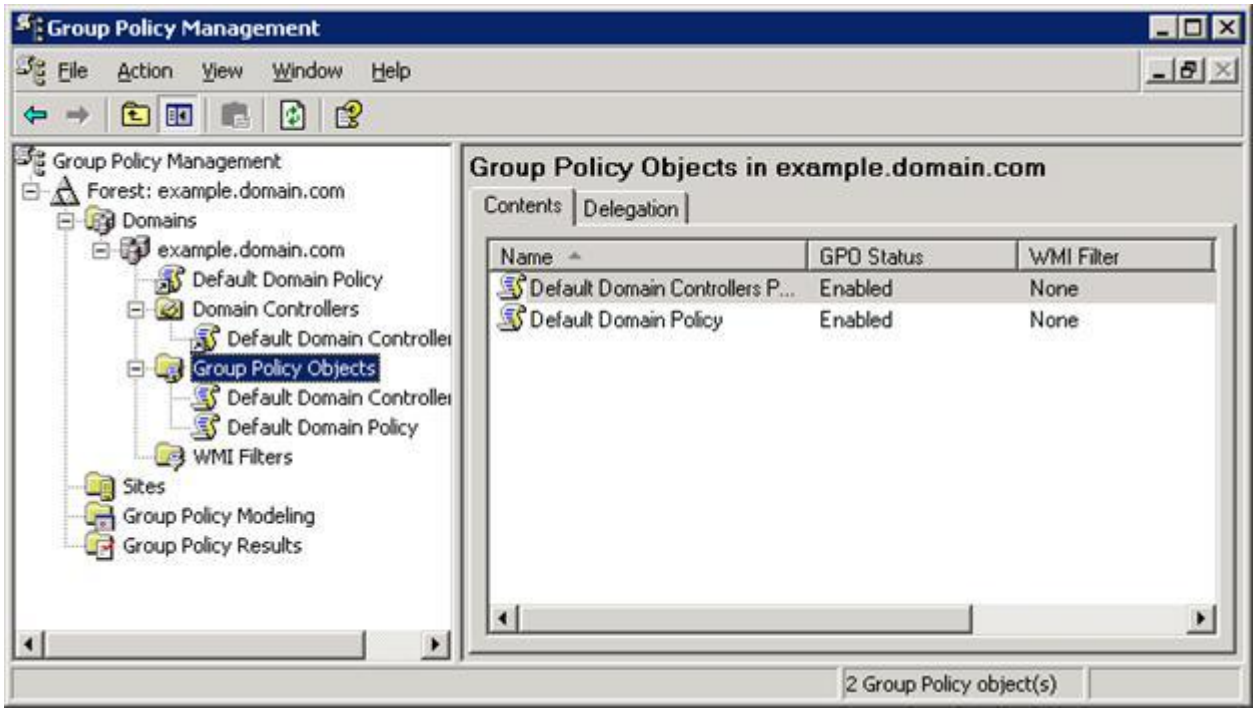
Если вы управляете небольшим или средним доменом, этих контейнеров достаточно для удовлетворения ваших нужд. Однако, если вам необходимо организовать ваших пользователей, вы можете создать новые контейнеры OU для хранения объектов. Затем вы применяете разрешения к этим OU, чтобы группы администраторов могли управлять пользователями и компьютерами в своих собственных OU.

При интеграции терминальных серверов в AD, желательно создать новый OU специально для терминальных серверов. Это позволит применять объекты групповых политик (GPO) ко всем серверам этого OU, не заботясь о добавлении серверов в группу безопасности, чтобы они получали настройки из политик. Исключение из этого пожелания - если вы используете

исключительно тонкие клиенты; в этом случае вам не нужно создавать отдельные GPO для рабочих станций и терминальных серверов.

Group Policy Management Console

В WS2K3 включен новый инструмент для управления групповыми политиками — Консоль управления политиками (Group Policy Management Console, GPMC). Используя GPMC, вы можете создавать и редактировать GPOs; связывать GPO с OU, сайтами и доменами; настраивать безопасность; делегировать администрирование; делать резервные копии и восстанавливать GPO; создавать отчеты в формате HTML; и даже запускать сценарии Resultant Set of Policy для помощи в проектировании ваших GPO.



По умолчанию GPMC не инсталлируется. Вы можете загрузить ее отсюда: http://www.microsoft.com/windowsserver2003/gpmc/default.mspx.

Настройка терминальных серверов при помощи групповых политик

После того, как вы подняли AD и добавили в домен терминальные серверы, вы готовы начать проектировать свои GPO для конфигурирования терминальных серверов и пользовательских сеансов. В главе 2 содержался краткий обзор политик, которые вы можете сконфигурировать для серверов. В предыдущих разделах я упоминал, что вы можете использовать GPO для конфигурирования настроек пользователей и сеансов, например, тайм-аутов, редиректа ресурсов и т.д. Вы также можете использовать GPO для управления пользовательским интерфейсом Windows и для ограничения доступа к инструментам и функциям, которые злонамеренные пользователи могут использовать для дестабилизации работы сервера.

Настройки интерфейса пользователя

Большинство настроек, доступных в GPO, предназначены для конфигурирования и блокировки интерфейса пользователя. Это весьма скользкая тема, поскольку пользователи часто привыкли использовать особенности Windows, которые администраторы часто удаляют или запрещают использовать на терминальных серверах (например, командная строка, команда Run, Task Manager и т.п.). Я рекомендую прочесть статью Microsoft “How to Lock Down a Win2K Terminal Server Session”. Затем вы можете добавлять или удалять ограничения в зависимости от требований пользователей.

Ниже приведен список политик, которые рекомендует Microsoft (настройки разделены на Computer Configuration и User Configuration):

Настройки Computer Configuration:

- Do not display last user name in logon screen (Не выводить имя последнего пользователя на экране входа)
- Restrict CD-ROM access to locally logged-on user only (Ограничить доступ к CD-ROM только для локально вошедших пользователей)
- Restrict floppy access to locally logged-on user only (Ограничить доступ к FDD только для локально вошедших пользователей)
- Disable Windows Installer—Always (Запретить Windows Installer - Насовсем)

Настройки User Configuration:

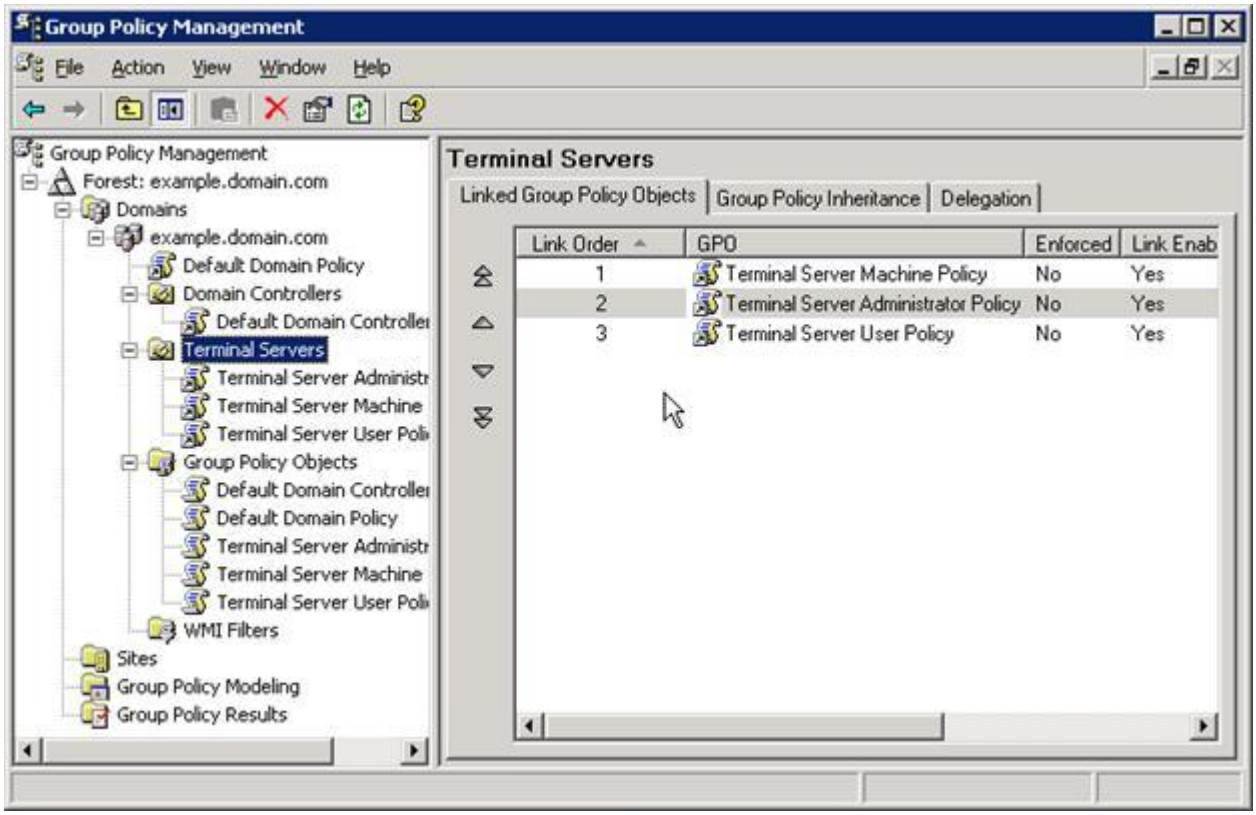
- Folder Redirection: Application Data
- Folder Redirection: Desktop
- Folder Redirection: My Documents
- Folder Redirection: Start Menu
- Remove Map Network Drive and Disconnect Network Drive (Удалить команды Map Network Drive и Disconnect Network Drive)
- Remove Search button from Windows Explorer (Удалить кнопку Search из Windows Explorer)
- Disable Windows Explorer's default context menu (Запретить контекстное меню в Windows Explorer)
- Hide the Manage item on the Windows Explorer context menu (Спрятать команду Manage в контекстном меню Windows Explorer)
- Hide these specified drives in My Computer (enable this setting for A through D) (Спрятать следующие диски в My Computer - от A до D)
- Prevent access to drives from My Computer (enable this setting for A through D) (Запретить доступ к этим дискам в My Computer - от A до D)
- Hide Hardware Tab (Запретить вкладку Hardware)
- Prevent Task Run or End (Запретить запуск и завершение задач)
- Disable New Task Creation (Запретить создание новых задач)
- Disable and remove links to Windows Update (Запретить и удалить ссылки на Windows Update)
- Remove common program groups from Start Menu (Удалить группу общих программ из меню Start)
- Disable programs on Settings Menu (Запретить программы в меню Start)
- Remove Network and Dial-up Connections from Start Menu (Убрать пункт Network and Dial-up Connections из меню Start)
- Remove Search menu from Start Menu (Убрать пункт Search из меню Start)
- Remove Help menu from Start Menu (Убрать пункт Help из меню Start)
- Remove Run menu from Start Menu (Убрать пункт Run из меню Start)
- Add Logoff to Start Menu (Добавить понкт Logoff в меню Start)
- Disable and remove the Shut Down command (Запретить и удалить команду Shut Down)
- Disable changes to Taskbar and Start Menu Settings (Запретить изменения в панель задач и настройки меню Start)
- Hide My Network Places icon on desktop (Спрятать иконку My Network Places на рабочем столе)
- Prohibit user from changing My Documents path (Запретить пользователю менять путь My Documents)
- Disable Control Panel (Запретить Панель Управления)
- Disable the command prompt (Set Disable scripts to No) (Запретить командную строку)
- Disable registry editing tools (Запретить инструменты редактирования реестра)
- Disable Task Manager (Запретить Task Manager)
- Disable Lock Computer (Запретить Lock Computer)

Очевидно, что если вы используете все эти политики, то получите крайне строгую среду, почти не пригодную к использованию. Например, Microsoft рекомендует удалить команду Map Network Drive, но если вы находитесь в распределенной среде, ваши пользователи могут потребовать этой

возможности для доступа к своим документам. Тем не менее этот список может служить хорошей отправной точкой.

Я рекомендую начать с крайне ограничительной политики, а затем протестировать и при необходимости разрешить отдельные настройки. Вы не должны полагаться только на политики при защите вашего сервера, поскольку они оставляют множество лазеек для злонамеренных пользователей. Например, если вы используете *Prevent access to drives in My Computer* в качестве единственного метода защиты файлов на сервере, злоумышленник может легко создать пакетный файл. Вместо этого вы должны применить ограничения NTFS для защиты файловой системы и использовать политику *Prevent access to drives in My Computer* для предотвращения использования диска C сервера в качестве диска C своего клиентского устройства. Если вы запускаете сервер в режиме Full Security, то большинство ключевых областей файловой системы и реестра по умолчанию защищены.

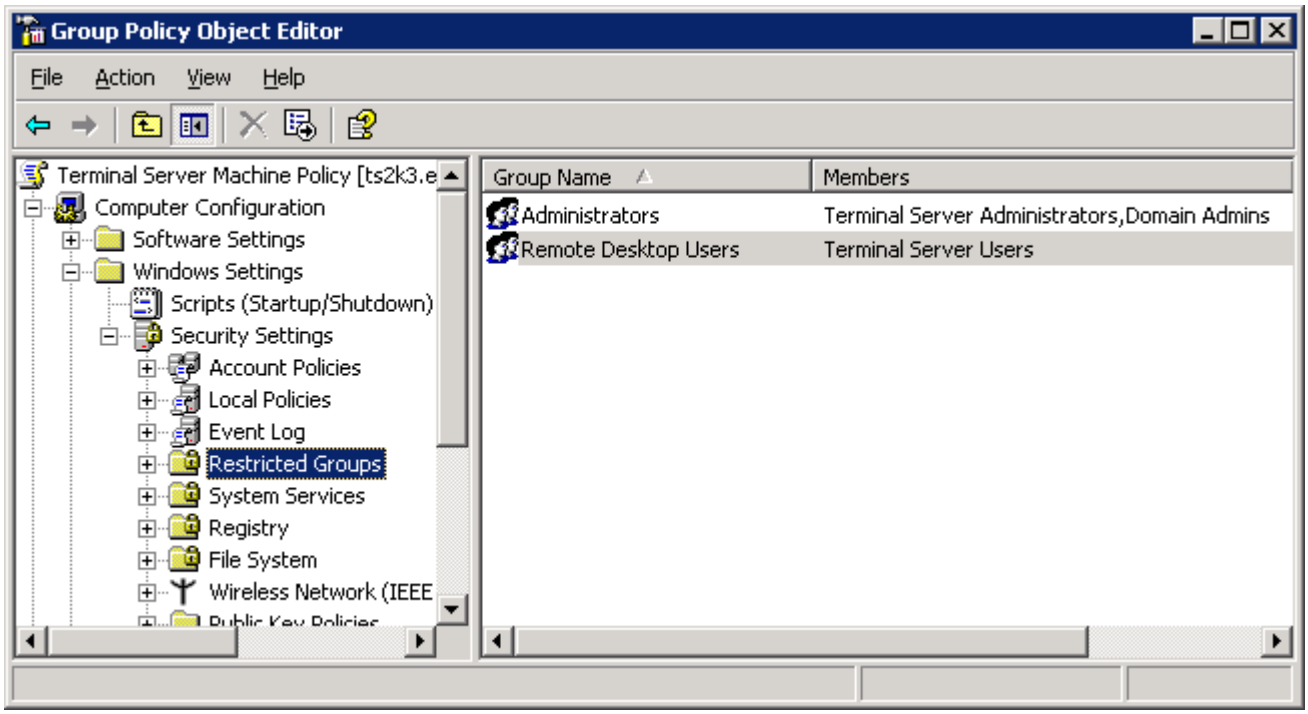
Вам следует быть осторожными, создавая разные политики для пользователей и системных администраторов. Очевидно, что администраторам требуются некоторые функции, которые не нужны пользователям. Для создания отдельных политик, создайте два объекта GPO, один для пользователей, которые включает все ограничения, которые вы хотите реализовать, а второй - для администраторов, в котором ограничения запрещены. Установите делегирование на пользовательскую политику для применения ее к Authenticated Users, а администраторскую политику примените только к доменной группе, содержащей учетные записи администраторов. Наконец, поместите в порядке применения администраторскую политику перед пользовательской.



Ограниченные группы

Вы уже знаете, что для доступа к терминальному серверу необходимо членство в групе Remote Desktop Users . По этой причине управление этой группой рекомендуется осуществлять посредством групповых политик.

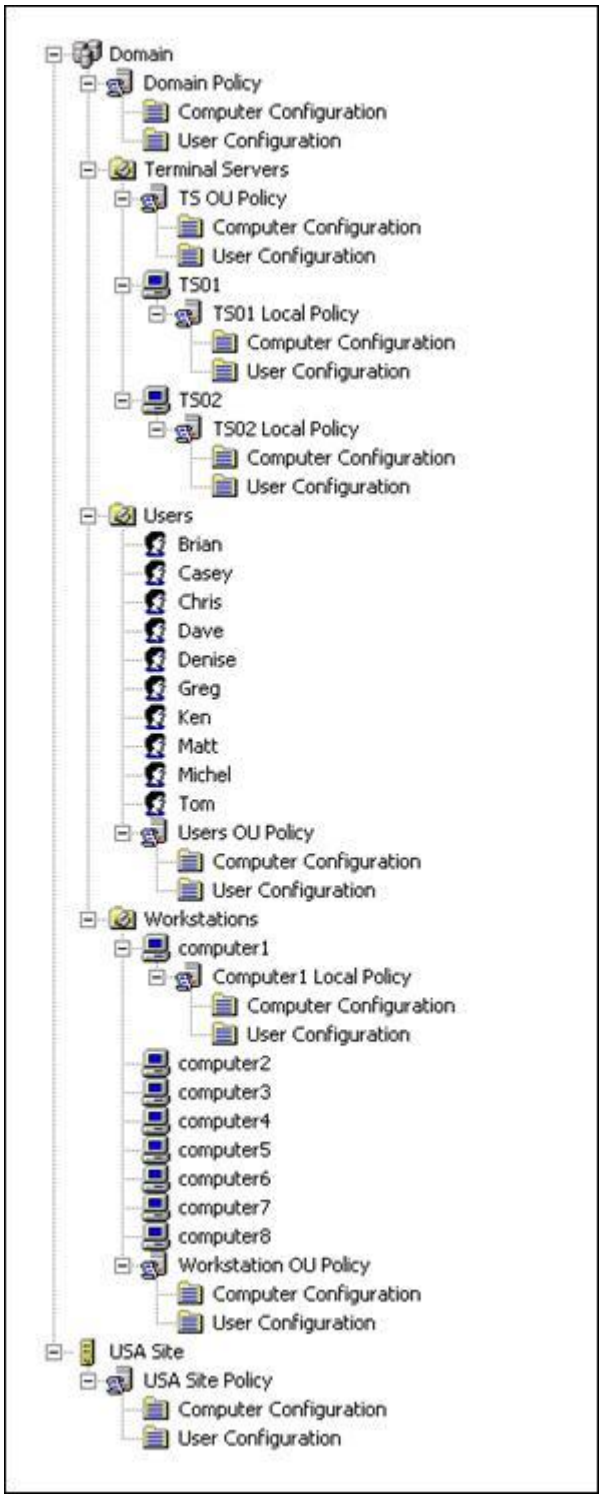
Ограниченные группы (Restricted Groups) позволяют вам управлять членами локальной машинной группы через доменные GPO. Тогда при добавлении в домен нового терминального сервера, сервер немедленно наследует надлежащие доменные группы в свою группу Remote Desktop Users. Таким же способом вы можете управлять локальной группой Administrators.



Порядок обработки политик

Очень важен порядок применения объектов GPO. Поскольку для данного пользователя или компьютера у вас может быть несколько политик, в конечном счете эффект настроек определяет результирующий набор политик (Resultant Set of Policy). Чтобы определить конечные настройки, которые применяются к пользователям, вы должны просмотреть все GPO, которые применяются к этому пользователю. GPO применяются в фиксированном порядке: локальные, сайтовые, доменные, OU. Машинные и пользовательские настройки применяются раздельно, хотя они оба идут из одного GPO.

Для понимания порядка обработки GPO, давайте взглянем на инфраструктуру теоретического домена и проследим применение политик. На рисунке показан примерный домен и его GPO. Для простоты я применил только по одному GPO на каждом уровне. В большинстве случаев у вас будет одновременно несколько GPO на уровнях сайта, домена и OU. Эти GPO будут обрабатываться все, чтобы получить Результирующий набор политик.



Начнем с обрабоки GPO при загрузке компьютера computer1. Во время загрузки настройки безопасности применяются к этому компьютеру в следующем порядке:

1. Local — Применяются настройки Computer Configuration из локальной политики cComputer1 Local Policy.
2. Site — Применяются настройки Computer Configuration из USA Site Policy.
3. Domain — Применяются настройки Computer Configuration из Domain Policy.
4. OU — Применяются настройки Computer Configuration из Workstation OU Policy. Политики OU определяются OU, в которой находится объект. В нашем случае computer1 находится в OU "Workstations", поэтому обрабатываются политики, связанные с этой OU.

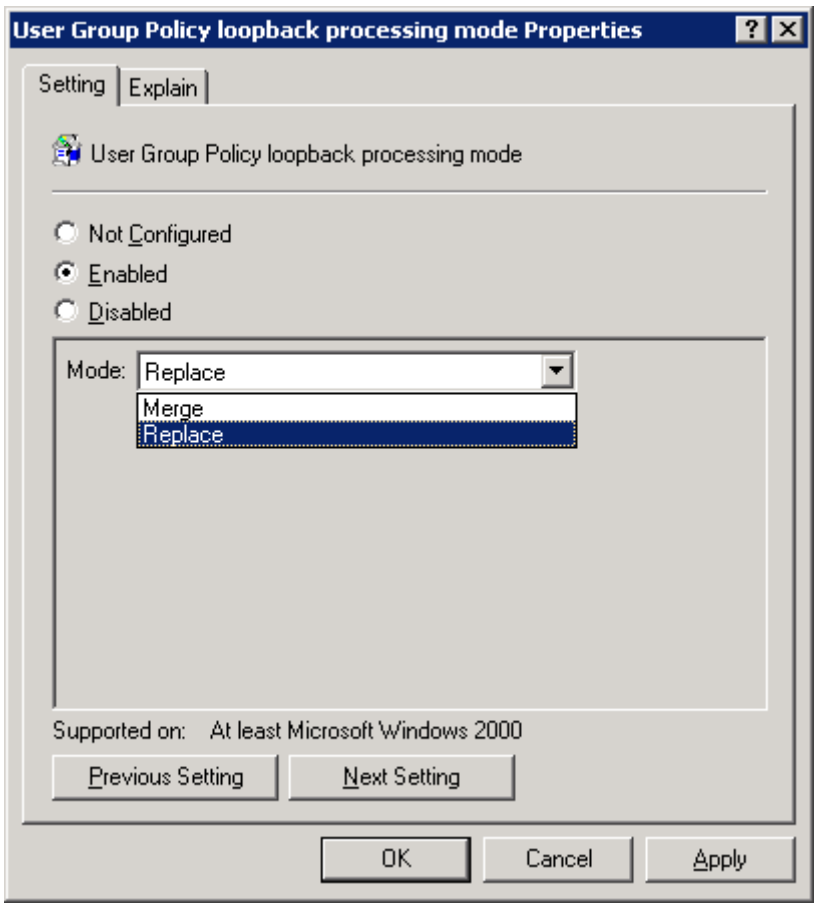
Теперь, когда computer1 имеет полную конфигурацию, заставим на нем зарегистрроваться пользователя Greg, чтобы обработались политики User Configuration:

1. Local — Применяются настройки User Configuration из Computer1 Local Policy
2. Site — Применяются настройки User Configuration из USA Site Policy
3. Domain — Применяются настройки User Configuration из Domain Policy
4. OU — Применяются настройки User Configuration из Users OU Policy для OU "Users". В стандартном режиме обработки, Грег всегда получит свою конфигурацию User Configuration из политики, независимо от того, в какой OU находится компьютер, на котором он регистрируется.

В стандартном режиме обработки, поскольку в OU "Workstation" нет пользователей, политика User Configuration из Workstation OU Policy никогда не применяется. Кроме того, в стандартном режиме обработки, Грег получит одинаковый результирующий набор пользовательских политик независимо от того, на каком компьютере он регистрируется. Эта особенность важна в больших доменах со множеством рабочих станций, где Грег может использовать компьютеры из других OU. Однако, если вы хотите, чтобы Грег получил более ограничительную политику при регистрации на некотором компьютере (например, на терминальном сервере), вам необходимо реализовать обратную обработку политик.

Обратный порядок обработки политик

Обратный порядок обработки политик позволяет получить преимущества настроек User Configuration из GPO, связанного с OU, которая содержит компьютер. Как показано на следующем рисунке, есть два режима обратной обработки: Замена (Replace) и Слияние (Merge). Режим слияния предписывает системе сначала применить User Configuration из политики OU "Users" (стандартный режим обработки), затем применить User Configuration из политики OU "Computers". Результирующий набор политик будет представлять собой комбинацию обоих наборов GPO. Режим замены предписывает системе целиком игнорировать объекты GPO из OU "Users" и применять только настройки User Configuration из политики OU "Computers".



В нашем примере мы можем включить обратную обработку политик в режиме слияния для терминального сервера TS01. В этом сценарии Computer Configuration применяется как обычно, но когда Грег подключается к TS01, его User Configuration применяется в следующем порядке:

1. Local — Применяются настройки User Configuration из политики Computer1 Local Policy
2. Site — Применяются настройки User Configuration из политики USA Site Policy
3. Domain — Применяются настройки User Configuration из политики Domain Policy
4. OU — Применяются настройки User Configuration из политики Users OU Policy для OU "Users"
5. OU Loopback — Применяются настройки User Configuration из политики TS OU Policy из OU "Terminal Servers"

В этом режиме Грег получает настройки прокси для его Internet Explorer из политики "Users OU Policy", но не имеет доступа к команде Shut Down в меню Start, т.к. она удалена политикой "TS OU Policy". Режим слияния имеет преимущество в том, что можно поместить глобальные настройки в политику "Users OU Policy", а запрещения применять только в политике "TS OU Policy". Недостатком этого режима является то, что вам необходимо следить за пользовательскими настройками в двух объектах GPO.

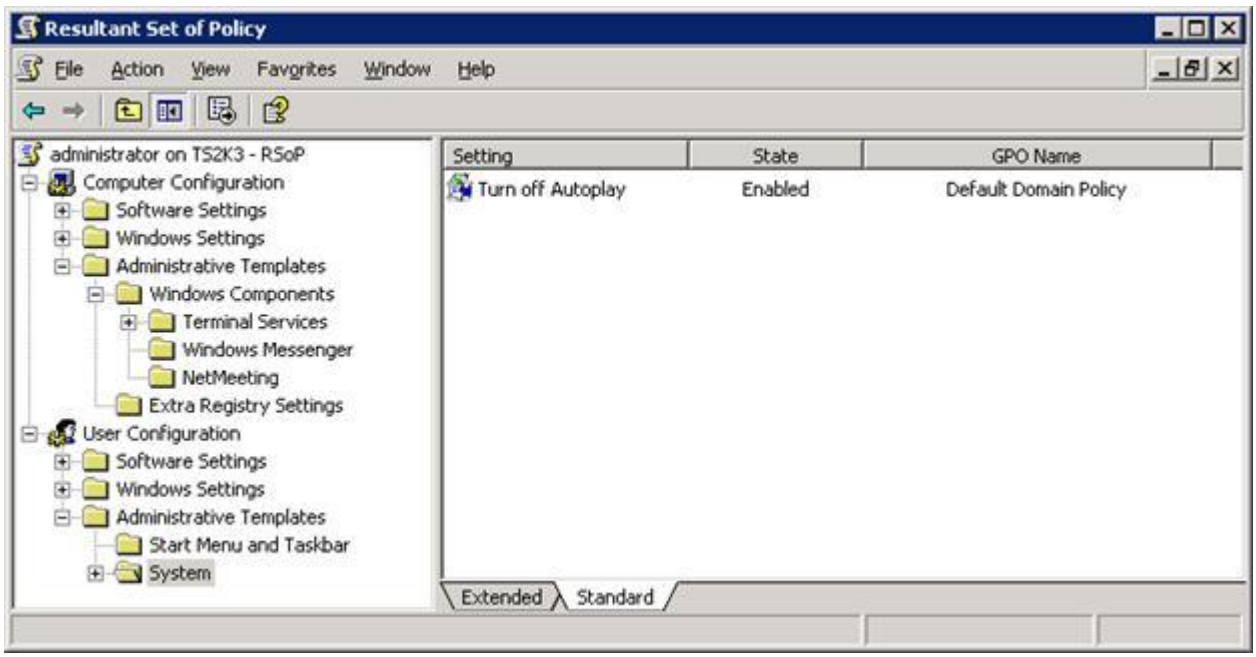
В режиме замены, User Configuration из политики "Users OU Policy" игнорируется :

1. Local — Применяются настройки User Configuration из Computer1 Local Policy
2. Site — Применяются настройки User Configuration из USA Site Policy
3. Domain — Применяются настройки User Configuration из Domain Policy
4. OU Loopback — Применяются настройки User Configuration из TS OU Policy

Этот режим упрщает обработку GPO, помещая все настройки в политику TS OU Policy, но требует синхронизации с изменениями, вносимыми в политику "Users OU Policy". Например, если вы настроили прокси для IE с помощью групповых политик, то необходимо, чтобы значения, применяемые в объектах GPO, связанных с OU "Users", соотвествовали значениям в объектах GPO, связанным с OU "Terminal Servers" (подразумевая, что настройки прокси одинаковы для сервера и рабочих станций). Если меняется адрес прокси-сервера, то вам следует изменить обе политики.

Разрешение обратного порядка

Обратный порядок разрешается в разделе Computer Configuration редактора Group Policy Object Editor (см. рисунок). Вы можете включить обратный порядок либо в локальной машинной политике на терминальном сервере, либо через любой объект GPO, примененный к терминальным серверам.

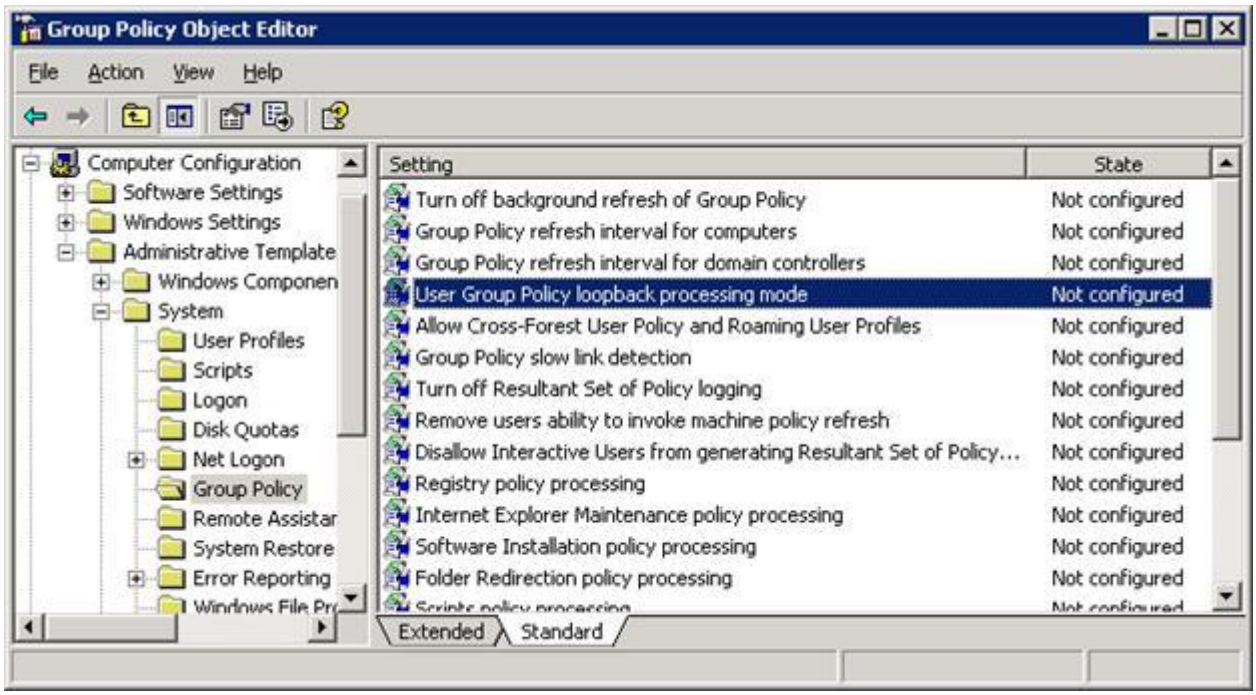


Результирующая политика

В сложных доменах со множеством групповых политик и комбинаций стандартной и обратной обработки довольно сложно отслеживать суммарный эффект объектов GPO и точно предсказывать результат перемещения пользователя или компьютера из одного OU в другой. Для помощи в этом Microsoft предлагает утилиту Resultant Set of Policy (RSOP.MSC).

Вы можете запустить ее с помощью команды Run для получения информации для текущего пользователя или компьютера, или из GPMC для тестирования сценариев регистрации пользователей на отдельных компьютерах. GPMC также предоставляет доступ к инструменту Group Policy Modeling, который вы можете использовать для тестирования "что будет, если..." перед внесением изменений в групповые политики или перемещением объектов.

RSOP.MSC не только показывает конечный эффект применения всех политик к пользователю или компьютеру, но также позволяет получить доступ к отдельным настройкам и увидеть все сконфигурированные политики.



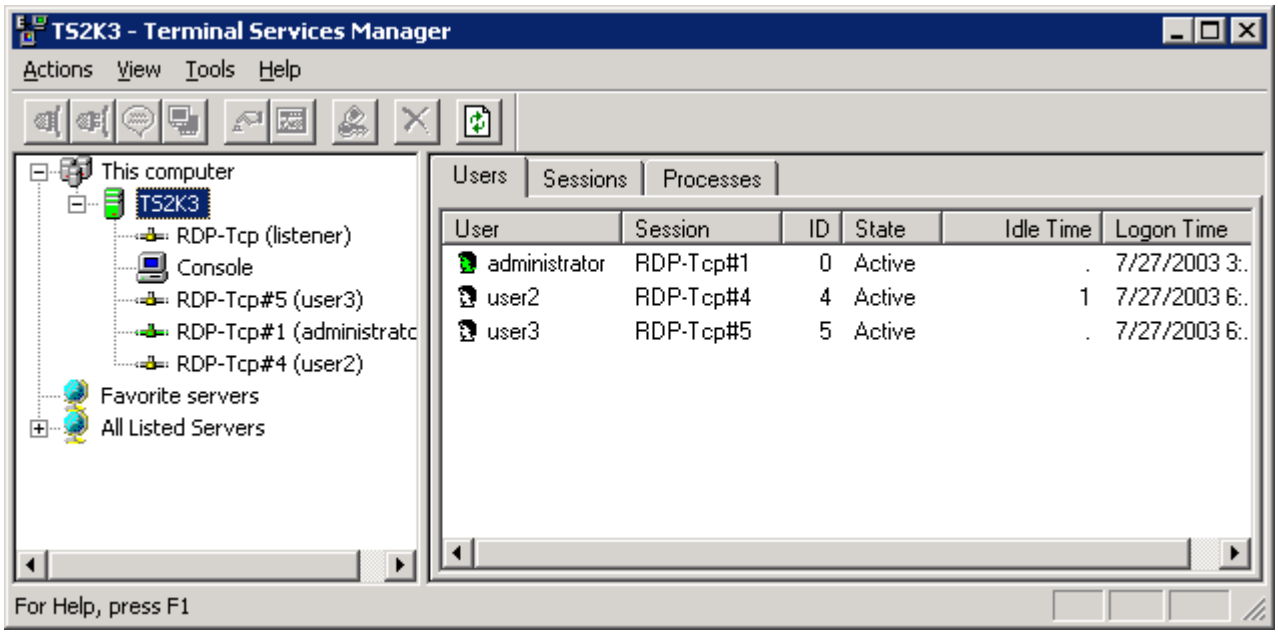
Управление сеансами пользователей

Если у вас инфраструктура ориентирована на рабочие станции, то вы знаете, как трудно удаленно диагностировать и устранять проблемы ваших пользователей. Вероятно, вы используете такие средства, как Microsoft Systems Management Server (SMS) и Windows XP Remote Support для работы на пользовательском ПК и вы знаете, как удаленно подключиться к сетевому реестру для изменения настроек ваших пользователей.

В среде Terminal Services эти задачи упрощаются. Вместо того, чтобы разыскивать некоторую рабочую станцию на удаленном узле вашей сети, вы и ваши пользователи оба зарегистрированы на одном и том же компьютере. А поскольку вы оба используете RDP для передачи данных KVM, вы легко можете вмешаться. Чтобы показать разную технику поддержки, сначала познакомимся с утилитами поддержки.

Terminal Services Manager

При запуске утилиты Terminal Services Manger выводится список всех серверов, на которых установлены терминальные службы. С помощью этой утилиты вы можете легко видеть, к каким серверам подключены пользователи и с каких клиентских устройств, какие процессы и приложения работают в их сеансах.

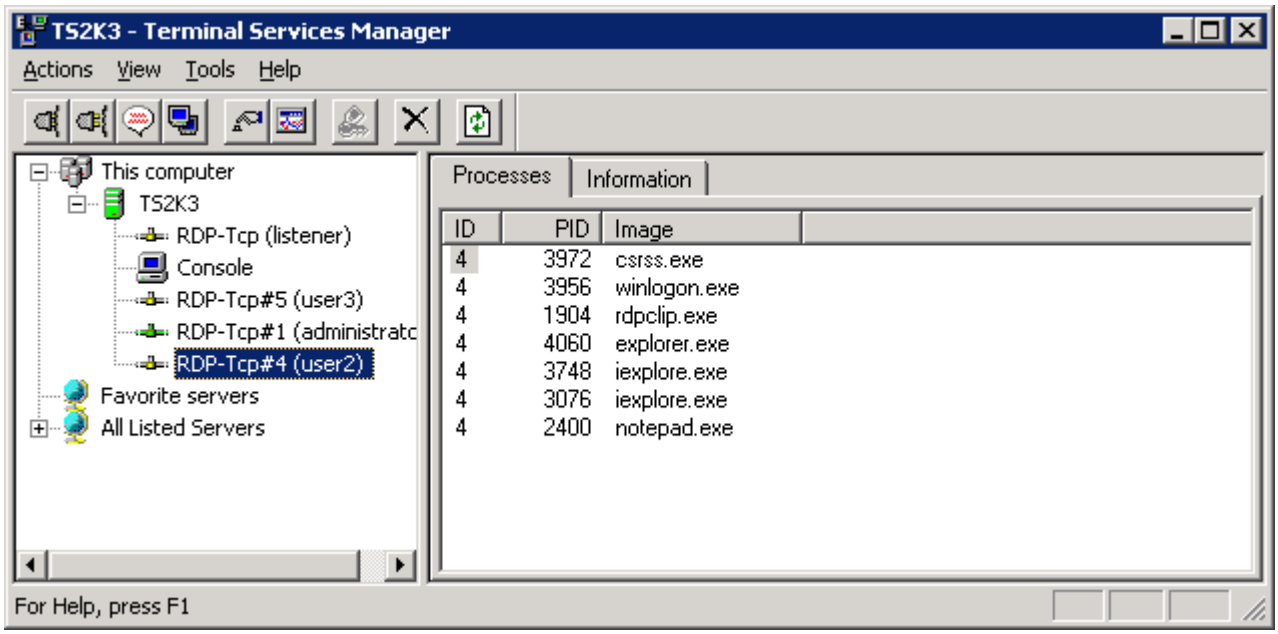


Если вы знакомы с Win2K Terminal Services Manager, то заметите несколько улучшений в версии, включенной в состав WS2K3. Во-первых, новая версия содержит узел *This computer*, дающий быстрый доступ к сеансам сервера, на котором вы зарегистрированы. Во-вторых, есть узел *Favorite Servers*, который позволяет получить доступ к некоторым терминальным серверам, которые вы чаще всего администрируете. Наконец, узел *All Listed Servers* изначально не раскрыт, поэтому вам не нужно долго ждать поиска всех терминальных серверов перед началом использования этой утилиты.

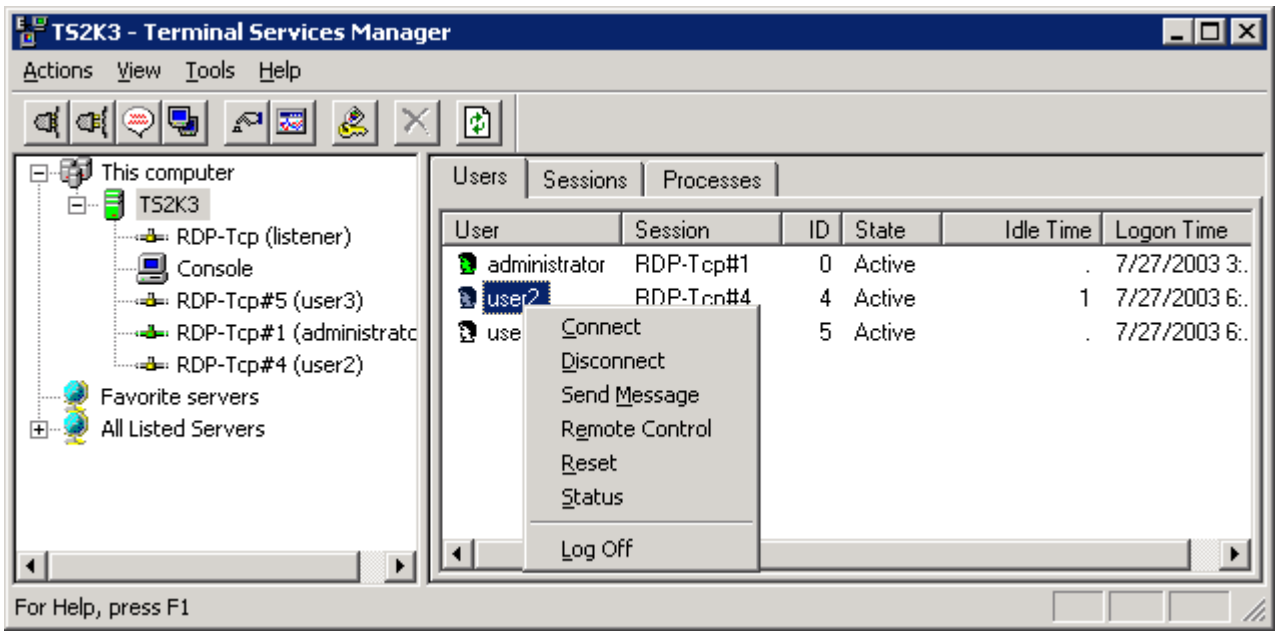
Если вы выделите некоторый сервер, утилита покажет список всех пользовательских сеансов на этом сервере. Также показывается состояние каждого сеанса:

- Active (активный) — Пользователь в настоящий момент посылает на сервер информацию от клавиатуры или мыши
- Idle (холостой) — Пользователь не перемещал мышь и не нажимал клавиш в течении определенного промежутка времени
- Disconnected (разъединенный) — Пользователь отключился от сервера, но оставил сеанс работать для дальнейшего подключения.

Если вы в левой панели выберите сеанс пользователя, то в правой панели будет показан список всех процессов, выполняемых пользователем на сервере. В этой панели вы можете завершить зависший процесс.



Вкладка *Information* в правой панели сообщает имя устройства клиента и адрес IP, а также версию клиента RDP, разрешение экрана и уровень шифрования. Эта информация поможет в устранении проблем. Если вы щелкните правой кнопкой на пользовательском сеансе, появится контекстное меню:



- Connect — Прозволяет подключиться к другому сеансу, который вы установили на сервере
- Disconnect — Отключает пользователя от сеанса, но оставляет сеанс работать на сервере
- Remote Control — Позволяет просмотреть или взаимодействовать с сеансом пользователя, не отключая пользователя. Пользователь видит любые выполняемые вами действия, а вы в свою очередь можете наблюдать за действиями пользователя.
- Reset — Убить сеанс
- Status — Выводит окно состояния, показывающее сетевую активность между сервером и клиентом.
- Log Of f— Принудительное завершение сеанса

Опция *Log Off* аккуратно завершает сеанс и выгружает профиль пользователя в центральный каталог профиля. Однако она не оставляет пользователю возможности сохранить свою работу.

Удаленное управление

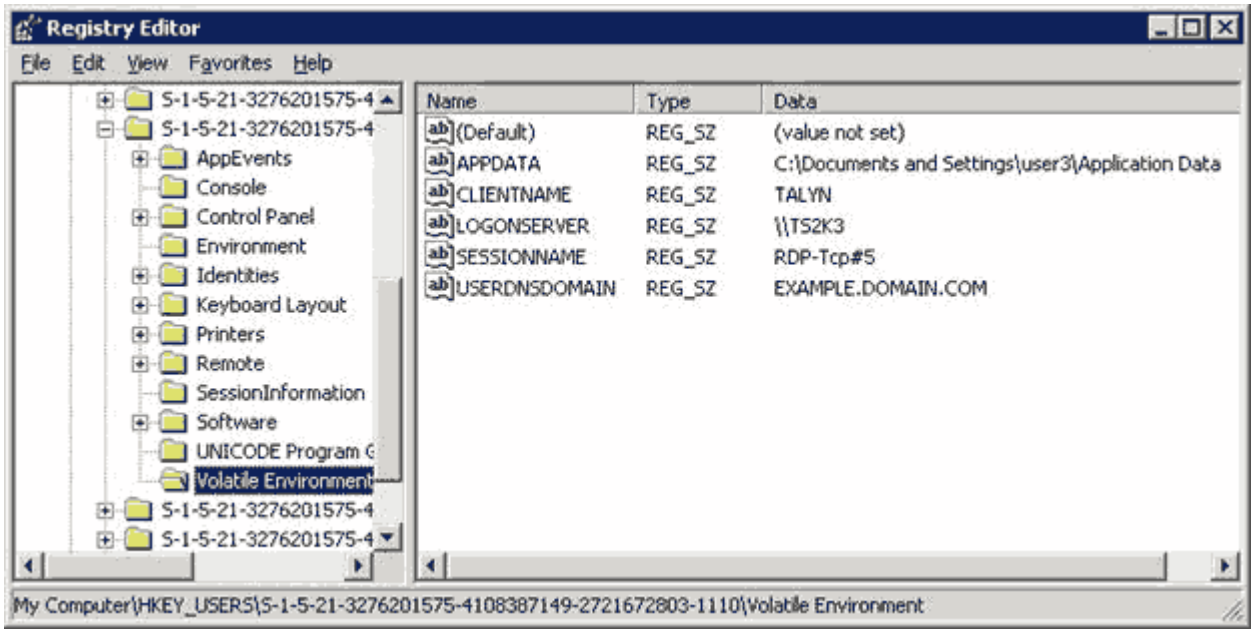
При выборе опции Remote Control вы временно отключаетесь от своего сеанса и подключаетесь к пользовательскому сеансу. Теперь RDP посылает всю видеоинформацию как на вашу машину, так и на клиентское устройство пользователя, и получает нажатия клавиш и перемещения мыши от вас обоих (если вы настроили интерактивное удаленное управление).

Во время удаленного управления пользователь может наблюдать, как вы запускаете приложения, меняете настройки и т.п., а вы можете наблюдать за действиями пользователя. Важно помнить, что любые ограничения, которые вы применили пользователю с помощью групповых политик, будут работать и при удаленном управлении, поэтому если вы запретили редактирование реестра, то не сможете запустить `REGEDIT` во время удаленного управления.

Редактирование реестра

Иногда необходимо отредактировать реестр пользователя. В случае с рабочими станциями, вам необходимо было подключаться к удаленному реестру пользовательского компьютера. На терминальном сервере вы совместно с вашими пользователями используете один и тот же реестр. Есть только один ключ HKEY_LOCAL_MACHINE для всех пользователей, а ключ HKEY_CURRENT_USER для каждого сеанса может быть найден в HKEY_USERS.

Каждый реестр пользователя имеет свой SID. Самый быстрый способ найти нужного пользователя, если вы не знаете его SID, заключается в просмотре подключа *Volatile Environment* для каждого пользователя. Этот подключ содержит переменную APPDATA, в которой содержится имя пользователя. Любые сделанные изменения становятся немедленно видимыми для пользователя.



Утилиты командной строки

Есть несколько утилит комадной строки, которые могут помочь в администрировании сервера. Большинство из них дублируют функции Terminal Services Manager, но версии командной строки удобны при написании скриптов.

- `CHANGE USER {/Install /Execute}` - Команда `CHANGE USER` используется для переключения сервера между режимами инсталляции и исполнения.
- `CHANGE LOGON {/Enable /Disable}` - запрещает прием новых соединений сервером
- `Query {Process | Session | Termserver | User}` - Команда Query дает ту же информацию, что и Terminal Services Manager; она перечисляет активные процессы в сеансе, доступные терминальные серверы и текущих пользователей.

- TSSHUTDN - TSSHUTDN используется для выключения или перезагрузки терминального сервера. Эта команда, в отличие от команды Shut Down в меню Start, предупреждает пользователей о выключении, чтобы они смогли сохранить свою работу. Затем осуществляется завершение каждого сеанса и в конце концов полное выключение сервера.

Вы можете сократить команду Query User до QUSER для быстрого получения списка активных сеансов на терминальном сервере.

Есть также другие инструменты, которые могут помочь в управлении и блокировке терминального сервера, в управлении групповыми политиками, профилями пользователей и печатью. Например, triCerat Simplify Profiles позволяет сохранять, восстанавливать, создавать и удалять настройки реестра конечных пользователей.

Глава 5. Установка приложений и совместимость

Мы рассмотрели, как разрешить роль Terminal Services, создавать и управлять фермой Session Directory, как интегрировать терминальные серверы в среду AD. Все эти факторы жизненно важны для успешной инфраструктуры Terminal Services, но именно пользовательские приложения определяют успех или неуспех развертывания вашего терминального сервера.

После установки Terminal Services вам также необходимо установить пользовательские приложения. Сегодня большинство приложений можно установить на терминальный сервер и они будут работать в многопользовательской среде без модификации. Однако, всегда найдутся важные программы, которые либо старые, либо не следуют спецификациям Microsoft Windows Logo, поэтому важно ознакомиться с особенностями Windows Server 2003, связанных с совместимостью приложений.

В этой главе описывается установка, развертывание и управление приложениями в среде Terminal Services. Вы узнаете, как настроить приложения для параллельной работы пользователей, писать скрипты совместимости и использовать флаги реестра для управления старыми приложениями.

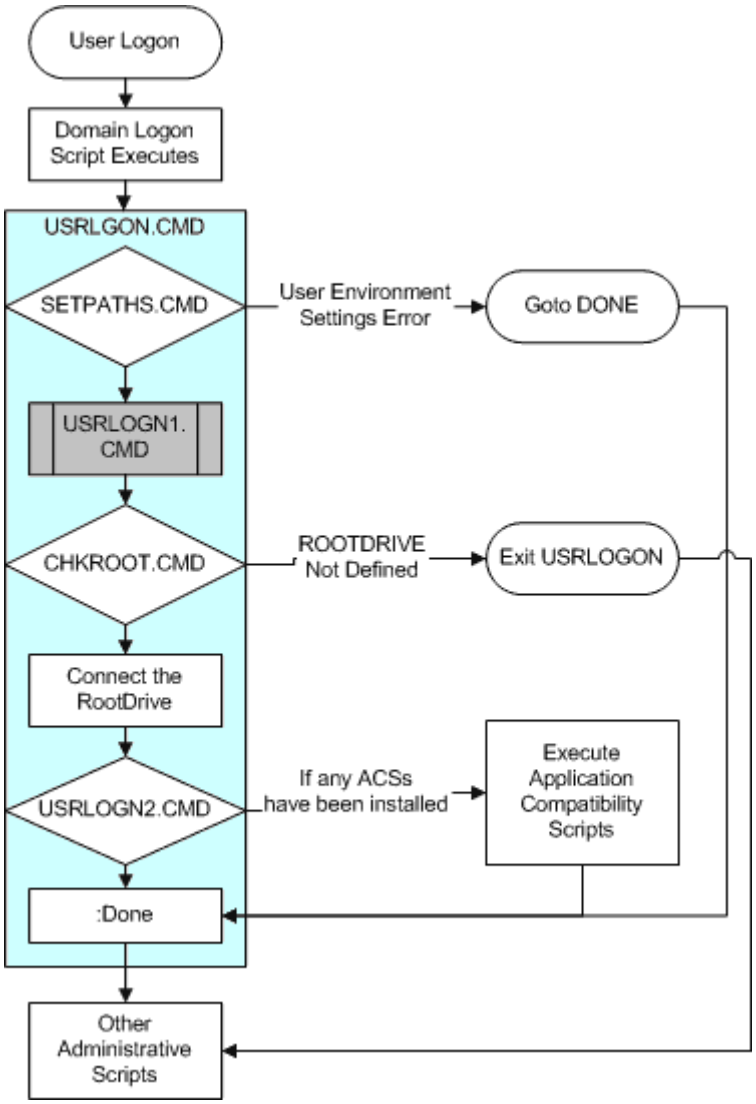
Механизмы совместимости приложений

Перед тем, как мы погрузимся в процесс инсталляции приложений, давайте рассмотрим механизмы, которые позволяют запускать приложения, изначально не рассчитанные для работы в терминальной среде. Эти механизмы включают скрипты входа, скрипты совместимости, режимы установки и исполнения, отображение реестра и отображение файлов INI.

Если приложение имеет логотип *Designed for Microsoft Windows XP*, оно обычно совместимо с Terminal Services. Программа сертификации Microsoft гарантирует, что приложение в процессе своей инсталляции и в хранении и обработки своих данных и настроек следует определенным правилам и совместимо с особенностями WS2K3. Подробнее о программе сертификации см. http://www.microsoft.com/winlogo/software/windowsxp-sw.mspx.

Скрипты входа

Помимо доменных скриптов входа, Terminal Services использует последовательность скриптов, которые запускаются при входе пользователя, чтобы помочь вам скорректировать приложения так, чтобы они работали в многопользовательской среде. На следующем рисунке показан процесс входа пользователя.



При инсталляции Terminal Services, система добавляет вход в ключ реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Appsetup, который запускает скрипт `USRLOGON.CMD`, находящийся в каталоге `System32`. `USRLOGON.CMD` - это сердце процесса входа Terminal Services, внутри него вызываются дополнительные скрипты.

Все скрипты, предоставляемые Microsoft, написаны на языке комадного интрпретатора, но WS2K3 также может использовать VBScript и JavaScript с помощью Windows Script Host (WSH).

USRLOGON.CMD

Первая часть `USRLOGON.CMD` вызывает скрипт `SETPATHS.CMD`

```
REM USRLOGON.CMD
@Echo Off
Call "%SystemRoot%\Application Compatibility Scripts\SetPaths.Cmd"
If "%_SETPATHS%" == "FAIL" Goto Done
```

Скрипт `SETPATHS.CMD` проверяет, что ключи реестра для пользовательского окружения находятся на месте. Ключи реестра для текущего пользователя находятся в HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, а ключи для всех пользовательских переменных находятся в таком же подключе в HKEY_LOCAL_MACHINE. Если ни одна из этих переменных не определена, появляется предупреждающее сообщение и выполнение `USRLOGON.CMD` прекращается. В следующей таблице показаны переменные окружения:

Компонент среды	Значение реестра
All Users: Startup	COMMON_STARTUP
All Users: Start Menu	COMMON_START_MENU
All Users: Start Menu\Programs	COMMON_PROGRAMS
Current User: Start Menu	USER_START_MENU
Current User: Startup	USER_STARTUP
Current User: Start Menu\Programs	USER_PROGRAMS
Current User: My Documents	MY_DOCUMENTS
Current User: Templates	TEMPLATES
Current User: Application Data	APP_DATA

Затем скрипт проверяет существование скрипта USRLOGN1.CMD и если он есть, то выполняет его. По умолчанию этого скрипта нет, и он нужен лишь в том случае, если у вас есть приложение, которое требует скрипт совместимости, не использующий ROOTDRIVE. Этот тип скрипта может вносить изменения в HKEY_CURRENT_USER безотносительно к размещению файлов, специфичных для пользователя.

```
If Not Exist "%SystemRoot%\System32\Usrlogn1.cmd" Goto cont0
Cd /d "%SystemRoot%\Application Compatibility Scripts\Logon"
Call "%SystemRoot%\System32\Usrlogn1.cmd"
:cont0
```

ROOTDRIVE - это буква драйва, которую администратор зарезервировал в качестве абсолютного пути к домашнему каталогу пользователя - сетевому или локальному - который одинаков для всех пользователей..

Следующий раздел скрипта создает ROOTDRIVE. Концепция ROOTDRIVE создана потому, что большинство ключей реестра не могут ссылаться на переменные окружения. Например, MyApplication.EXE может иметь в реестре значение UserTemplates, которое определяет путь для хранения модифицируемых пользователем шаблонов. Лучшей опцией для такого маршрута было бы указание %HOMEDRIVE%%HOMEPATH%\MyTemplates, чтобы каждый пользователь мог быть направлен на свой сетевой домашний каталог (если он есть) или в профиль на терминальном сервере. Поскольку вы не можете использовать переменные окружения в значениях реестра, вам необходимо указать абсолютный маршрут, который можно было бы разрешить для всех пользователей. Поэтому на терминальном сервере вы определяете ROOTDRIVE.

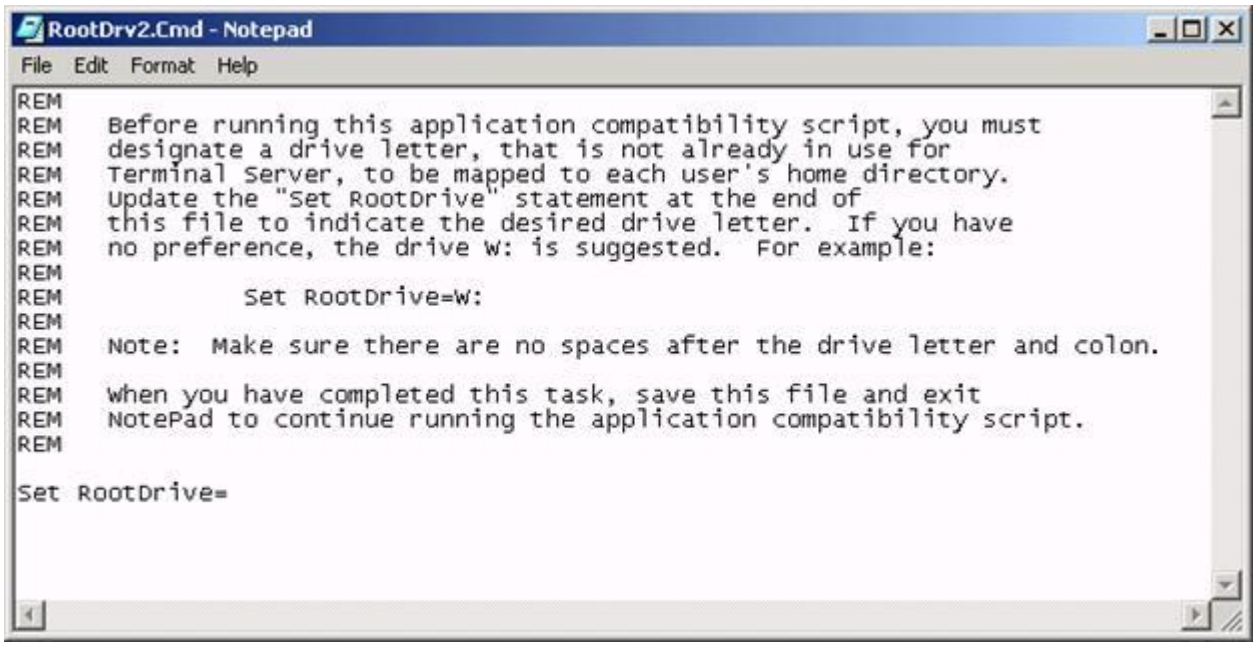
USRLOGON.CMD использует команду SUBST для подключения буквы ROOTDRIVE к пользовательскому каталогу во время входа.

```
Cd /d %SystemRoot%\"Application Compatibility Scripts"
Call RootDrv.Cmd
If "A%RootDrive%A" == "AA" End.Cmd

Rem
Rem Отобразить домашний каталог пользователя на букву драйва
Rem

Net Use %RootDrive% /D >NUL: 2>&1
Subst %RootDrive% "%HomeDrive%%HomePath%"
if ERRORLEVEL 1 goto SubstErr
goto AfterSubst

:SubstErr
Subst %RootDrive% /d >NUL: 2>&1
Subst %RootDrive% "%HomeDrive%%HomePath%"
```

```
:AfterSubst
```

Команда SUBST используется в Windows для назначения буквы драйва абсолютному маршруту - в отличие от NET USE, которая назначает букву драйва для пути в формате UNC. Так, `SUBST W: C:\WINNT\FONTS` сделает драйв W: ссылкой на каталог шрифтов.

Как выбирается и определяется буква для ROOTDRIVE? Когда администратор инсталлирует скрипт совместимости, который ссылается на ROOTDRIVE, скрипт инсталляции автоматически предлагает администратору изменить пакетный файл `ROOTDRV2.CMD`, указав в нем букву, которую администратор хотел бы зарезервировать. После этого эта буква не может быть использована в других отображениях драйвов на терминальном сервере.



Пример 1

Пользователь Joe User имеет домашний каталог, определенный в его учетной записи \\Server01\Home\Joe.User. При входе на терминальный сервер, буква H отображается на \\Server01\Home. В сеансе Джо, переменная %HOMEDRIVE% имеет значение H, а переменная %HOMEPATH% - значение \Joe.User.

Джо использует приложение, которое позволяет ему использовать персональные шаблоны для его документов, и есть ключ реестра, который определяет путь к этим шаблонам. Реестр не может ссылаться на переменные окружения, а только на аболютные маршруты, поэтому мы не можем использовать %HOMEDRIVE%%HOMEPATH%. Если мы попытаемся использовать H для UserTemplates, шаблоны Джо будут создаваться в корне домашней папки, а не в его каталоге.

Если администратор использовал `ROOTDRV2.CMD` для установки переменной ROOTDRIVE в W, то USRLOGON.CMD использует команду SUBST для отображения W на %HOMEDRIVE%%HOMESHARE% или H:\Joe.User. Теперь путь W:\ является ссылкой на H:\Joe.User, и значения реестра могут ссылаться на W:\, если им необходим доступ к домашнему каталогу Джо. Кроме того, этот путь может использоваться для размещения его файлов шаблонов.

Пример 2

У Jane Doe нет сетевого домашнего каталога, поэтому ее шаблоны должны храниться в ее профиле. В сеансе Джейн, переменная %HOMEDRIVE% указывает на C, а %HOMEPATH% указывает на \WTSRV\Profiles\Jane.Doe. Опять, мы не можем использовать переменные окружения в ключах реестра, поэтому у нас нет легкого способа сылаться на каталог профиля Джейн.

Администратор установил в скрипте ROOTDRIVE=W:, поэтому USRLOGON.CMD подключает W напрямую к каталогу профиля Jane, и мы можеи использовать в реестре W:\.

В примере с Джо пришлось использовать обходной путь, поскольку NT 4.0 не может отображать сетевой драйв на подкаталог папки общего доступа, поэтому

```
Net Use H: \\Server01\Share\Directory
```

подключит H к \\Server01\Share. Но WS2K3 может отображать подкаталог, что позволяет использовать домашний каталог в ROOTDRIVE.

Однако, без модификации `USRLOGON.CMD` всегда сбрасывает текущее значение ROOTDRIVE перед выполнением команды SUBST, поэтому он не получает преимущества от расширенных возможностей переназначения драйвов в WS2K3. Зачем нужны оба драйва, которые указывают на один и тот же каталог? Лучше изменить `USRLOGON.CMD` так, чтобы он использовал преимущества WS2K3.

Подробнее о ROOTDRIVE см. статью Microsoft “How and why ROOTDRIVE is used on Windows Terminal Server”

Допустим, вы используете сетевые домашние каталоги и назначили их на драйв H. Если вы установили ROOTDRIVE тоже на H, то вы можете избежать назначения двух драйвов. Ниже показаны изменения, которые вы можете сделать в USRLOGON.CMD (изменения выделены красным)

```
Cd /d %SystemRoot%\"Application Compatibility Scripts"
Call RootDrv.Cmd
If "A%RootDrive%A" == "AA" goto done
REM If the user has a network Home Directory already mapped
REM on the ROOTDRIVE, we do not need to do anything.
if /I "%rootdrive%" == "%homedrive%"        goto NoSubst
:DoSubst
Net Use %RootDrive% /D >NUL: 2>&1
Subst %RootDrive% "%HomeDrive%%HomePath%"
if ERRORLEVEL 1 goto SubstErr
goto AfterSubst
:SubstErr
Subst %RootDrive% /d >NUL: 2>&1
Subst %RootDrive% "%HomeDrive%%HomePath%"
:AfterSubst

:NoSubst
```

Если вы не инсталлируете приложения, требующие скриптов совместимости, то ROOTDRIVE никогда не будет создан, а процесс входа существенно упростится.

После установки ROOTDRIVE, скрипт USRLOGON.CMD вызывает любые установленные скрипты совместимости:

```
Rem Invoke each Application Script.  Application Scripts are automatically
Rem added to UsrLogn2.Cmd when the Installation script is run.
Rem

If Not Exist %SystemRoot%\System32\UsrLogn2.Cmd Goto Cont1
Cd Logon
Call %SystemRoot%\System32\UsrLogn2.Cmd
:Cont1
:Done
```

При установке скрипта совместимости, его вызов добавляется в `USRLOGN2.CMD`, чтобы все скрипты совместимости могли вызываться без модификации `USRLOGON.CMD`.

Дополнительные административные скрипты

Помимо `USRLOGON.CMD` и скриптов совместимости, вы можете запускать при входе пользователя дополнительные скрипты. Например, вы можете создать скрипт, котрый отображает дополнительные сетевые драйвы или подключает к принтерам. Если вы находитесь в среде AD, то можете добавить скрипты входа в объект групповой политики User Group Policy Object (GPO).

Если терминальный сервер находится в рабочей группе, вы можете заставить систему выполнить дополнительный скрипт, скопировав файл скрипта в каталог \System32 и изменив значение AppSetup в подключе реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. По умолчанию в этом ключе находится только USRLOGON.CMD, но вы можете добавить другие скрипты, отделив их друг от друга запятыми.

Подробнее о добавлении скриптов см. статью Microsoft “How to Set Up a Logon Script Only for Terminal Server Users”

Вместо редактирования ключа реестра AppSetup, вы можете вызывать дополнительные скрипты из USRLOGON.CMD. Если вы не используете ROOTDRIVE, встаьте вызов после метки `:Cont0`. Если вы используете ROOTDRIVE, вставьте вызов в конец скрипта.

Инсталляция приложений

Теперь, когда вы поняли процесс создания среды на терминальном сервере, мы можем приступить к рассмотрению процесса инсталляции программ на терминальном сервере. В идеальном случае, все приложения должны следовать спецификациям "Designed for Microsoft Windows XP".

Эта спецификация требует от программистов использовать преимущества некоторых компонентов Windows, которые делают приложение совместимым с WS2K3 и Terminal Services. В следующем списке содержатся некоторые из них, которые представляют интерес для администраторов Terminal Services:

- *Не читать и не писать в файлы Win.ini, System.ini, Autoexec.bat или Config.sys на любой ОС Windows, основанной на технологии NT* - Программы, которые не подчинаются этому правилу могут хранить пользовательские настройки в этих файлах.

- *Инсталлироваться используя пакеты Windows Installer* и *Принять меры, чтобы приложение поддерживало анонсирование.* - Служба Windows Installer использует процесс, называемым анонсированием (*advertising*), чтобы ключи реестра и файлы устанавливались для всех пользователей данного компьютера, а не только для того, кто запустил инсталляцию.

- *Хранить пользовательские данные в My Documents* - Пользовательские файлы (документы, макросы, шаблоны и пр.) должны храниться в каталогах пользователя, а не в каталоге программы.

В реальном мире системным адмнистраторам приходиться иметь дело с множеством приложений - как современных, так и устаревших, которые не следуют этим правилам или которые написаны до того, как эти правила были установлены. Для облегчения интеграции таких приложений Terminal Services использует отображение реестра, отображение файлов INI и скрипты совместимости приложений.

Отображение реестра

Реестр Windows разделен на два основных раздела: HKEY_CURRENT_USER и HKEY_LOCAL_MACHINE. HKEY_LOCAL_MACHINE используется для хранения глобальной

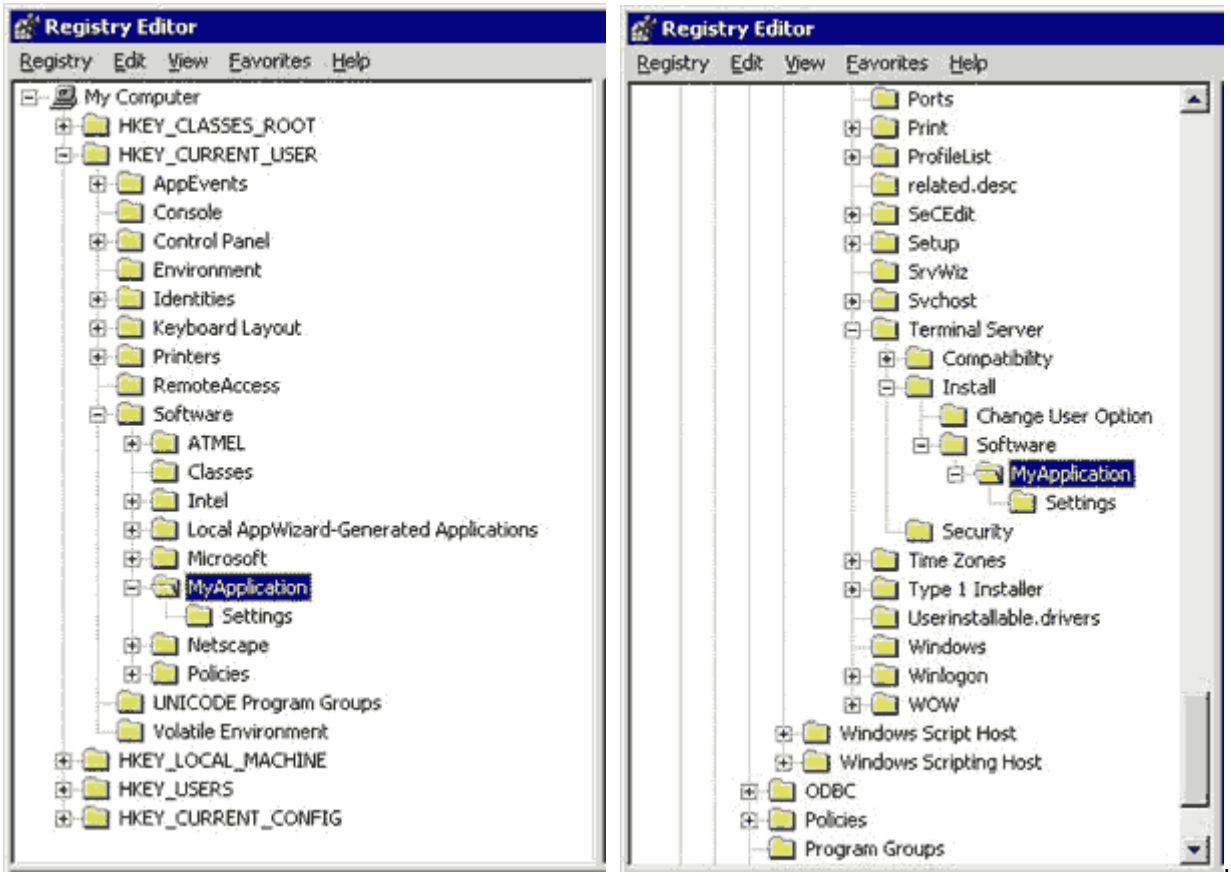
конфигурационной информации = такой, как сетевые настройки, аппаратная конфигурация, настройки программного обеспечения, одинаковые для всех пользователей. HKEY_CURRENT_USER хранит пользовательские настройки, например, косметические настройки, предпочтения пользователя, пользовательские настройки приложений. Каждый пользователь, зарегистрировавшийся в Windows, имеет свой собственный узел HKEY_CURRENT_USER.

При установке приложения ключи HKEY_CURRENT_USER создаются программой инсталляции. Когда другой пользователь регистрируется на компьютере, он также требует эти же ключи HKEY_CURRENT_USER для запуска приложения. Некоторые приложения используют саморегистрацию для создания этих ключей. При запуске приложения оно ищет ключи в HKEY_CURRENT_USER. Если ключей не существует, программа создает их и заполняет значениями по умолчанию.

Если приложение использует службу Windows Installer, приложение может использовать *advertising* для создания ключей HKEY_CURRENT_USER. Если такое приложение запускается из меню Start, то запускается служба Windows Installer и делает пользовательскую подстройку приложения. При этом создаются все необходимые ключи и специфические для пользователя файлы, необходимые для приложения.

Приложения, не использующие саморегистрацию или advertising, лишь пишут информацию HKEY_CURRENT_USER в узел, принадлежащий пользователю, инсталлирующему приложение, проэтому важные значения реестра могут не войти в HKEY_CURRENT_USER. Этот недостаток не заметен на рабочей станции, поскольку компьютер, как правило, используется одним человеком. Но терминальный сервер по своей природе предназначен для множества пользователей.

Чтобы гарантировать, что все пользователи получат правильные значения реестра, Terminal Services использует процесс, называемый *отображением реестра* (registry mapping). При инсталляции приложения, терминальный сервер переводится в режим инсталляции. В этом режиме сервер наблюдает за всеми изменениями, вносимыми программой установки в HKEY_CURRENT_USER. Как показано на следующем рисунке, все ключи, которые записываются в HKEY_CURRENT_USER, автоматически копируются в особое место в HKEY_LOCAL_MACHINE - в подключ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software



Отображение реестра работает только в том случае, если программа для записи в реестр использует стандартные вызовы API. Всегда проверяйте реестр после установки приложения и до первого его запуска, чтобы убедиться, что зеркало создано. Если нет, вам следует вручную скопировать ключи.

По завершении установки приложения сервер переводится в режим исполнения. В этом режиме, если приложение пытается прочитать ключ реестра из HKEY_CURRENT_USER, а ключа там нет, система автоматически проверит, есть ли такой ключ в подключе HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software. Если он там найден, то система скопирует его в HKEY_CURRENT_USER.

Отображение файлов INI

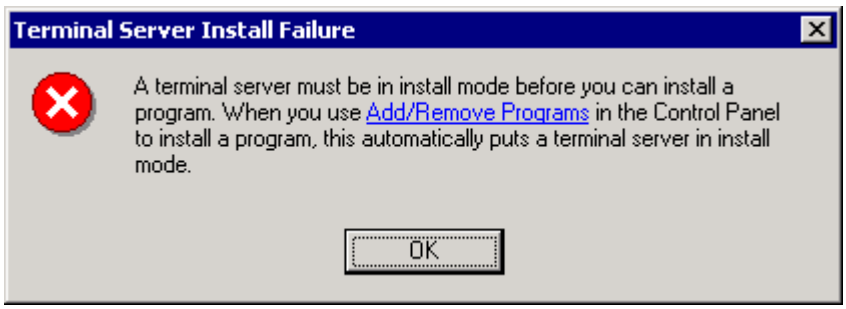
До Windows 95 все настройки системы и приложений хранились в файлах INI (инициализационных файлах). Старые приложения до сих пор их используют. В отличие от реестра, который отделяет пользовательские настройки от машинных, файлы INI являются глобальными, поэтому изменения, сделанные одним пользователем, затрагивают всех пользователей на терминальном сервере. Кроме того, большинство терминальных серверов настроены так, что обычные пользователи не имеют достаточных прав для изменения этих системных файлов, поэтому приложения, использующие файлы, не будут работать в пользовательском контексте.

Для компенсации такого поведения, Terminal Services создает копии системных файлов INI и сохраняет их в домашнем каталоге каждого пользователя. Если приложение пытается читать или записать в системный файл INI, Terminal Services переадресуют вызов на пользовательскую копию вместо оригинала.

В режиме инсталляции все изменения, которые программа установки делает в этих файлах INI, она делает в оригинальных копиях в каталоге %SYSTEMROOT%. При входе пользователя, система сверяет пользовательские копии системных файлов INI с теми, что находятся в каталоге WINNT, и если пользовательские файлы старее, система их обновляет. Вы можете запретить такую проверку, изменив значение реестра.

Режимы инсталляции и исполнения

Для работы переназначения реестра и файлов INI, система во время инсталляции приложения и во время его работы должна находиться в соотвествтующем режиме. Для переключения сервера в режим инсталляции просто запустите мастер Add New Programs в апплете панели управления Add/Remove Programs. Для переключения обратно в режим исполнения закройте мастер. Если вы попытаетесь запустить программу SETUP.EXE за пределами панели управления, терминальный сервер выдаст сообщение об ошибке:



Терминальный сервер не может перехватывать все программы установки, поэтому выработайте привычку всегда использовать панель управления для установки новых программ.

В качестве альтернативы вы можете переключаться между режимами с комадной строки, используя следующие команды:

```
CHANGE USER /INSTALL

CHANGE USER /EXECUTE
```

Эти команды полезны, если вы хотите заскриптовать процесс инсталляции приложения.

Скрипты совместимости приложений

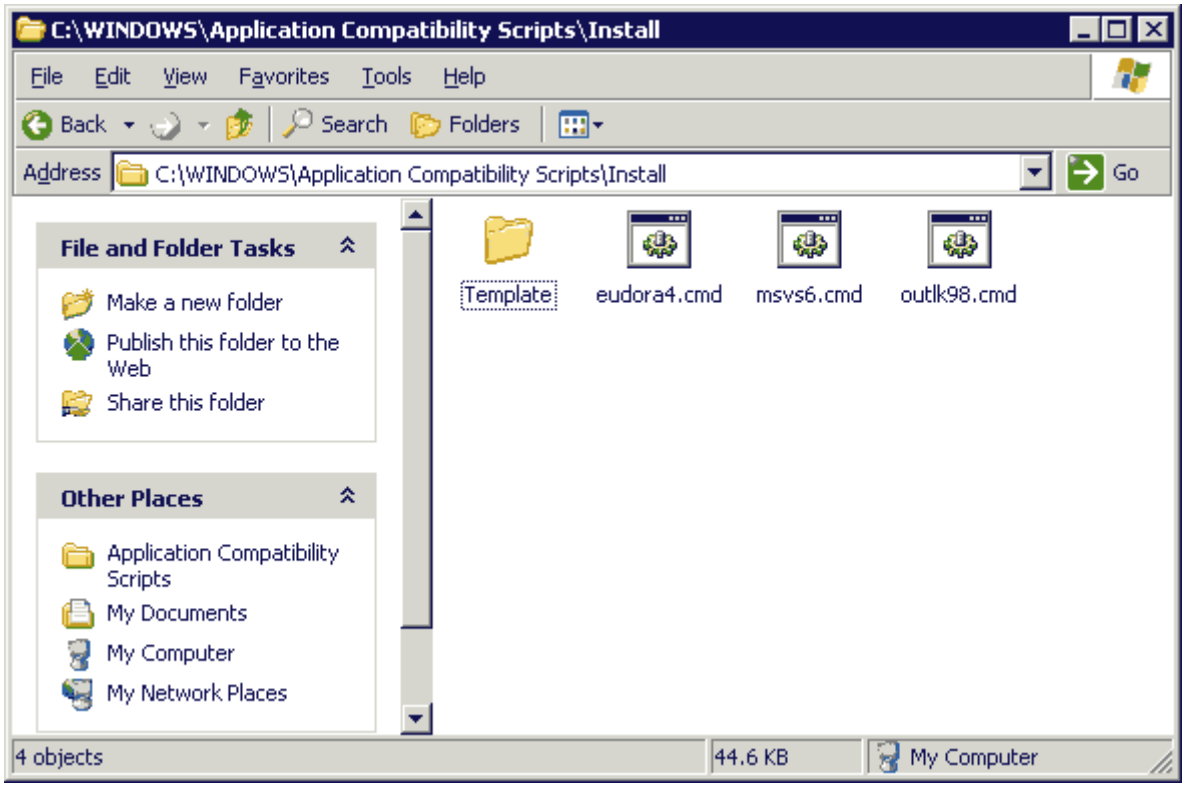
Многие приложения не учитывают особенностей Terminal Services и сохраняют свои компоненты на диске C компьютера. Эти компоненты могут включать в себя макросы, шаблоны, всяческие файлы. На рабочей станции, если пользователь модифицирует один из таких файлов, изменения затронут любого пользователя, который зарегистрируется на этом компьютере. Но на терминальном сервере изменения также затронут всех пользователей, одновременно зарегистрированных на нем. Это может создать проблемы, когда такие файлы будут использоваться одним пользователем и будут недоступны другому экземпляру приложения, запущенному в другом сеансе другим пользователем.

Скрипты совместимости компенсируют эту проблему, копируя эти компоненты в каталоги, уникальные для каждого пользователя (обычно в домашний каталог), а затем указывая приложению, где найти новые копии. Вы также можете использовать скрипты совместимости для предоставления пользователю прав доступа к отдельным файлам и разделам реестра, которые ограничены на терминальном сервере.

Тот факт, что многие современные приложения следуют спецификации Windows Logo, заметен по уменьшению количества скриптов совместимости, включенных в Windows. Вы можете найти эти скрипты в C:\WINNT\Application Compatibility Scripts. Скрипты разбиты на три группы:

- Install — Эти скрипты вносят изменения на системном уровне и добавляют строки в USRLOGON2.CMD, если приложение также требует скрипт совместимости для каждого пользователя при входе
- Logon — Эти скрипты вызываются из USRLOGON2.CMD при входе пользователя; они копируют пользовательские компоненты на ROOTDRIVE и вносят изменения в реестр HKEY_CURRENT_USER.

- Uninstall — Эти скрипты удаляют вызов скриптов из USRLGON2.CMD, если отпадает необходимость в запуске скрипта совместимости.



Как видно, Microsoft включает лишь скрипты для Eudora 4, Visual Studio 6 и Outlook 98. Если вы используете старые приложения (например, Office 97, Project 95 и т.п.), вы можете скопировать скрипты с терминального сервера Win2K.

При инсталляции приложения, требующего скрипта совместимости, вы запускаете инсталляционный скрипт после установки приложения. Этот инсталляционный скрипт делает все необходимые системные изменения и указывает USRLOGN2.CMD выполнить скрипт входа при регистрации пользователя.

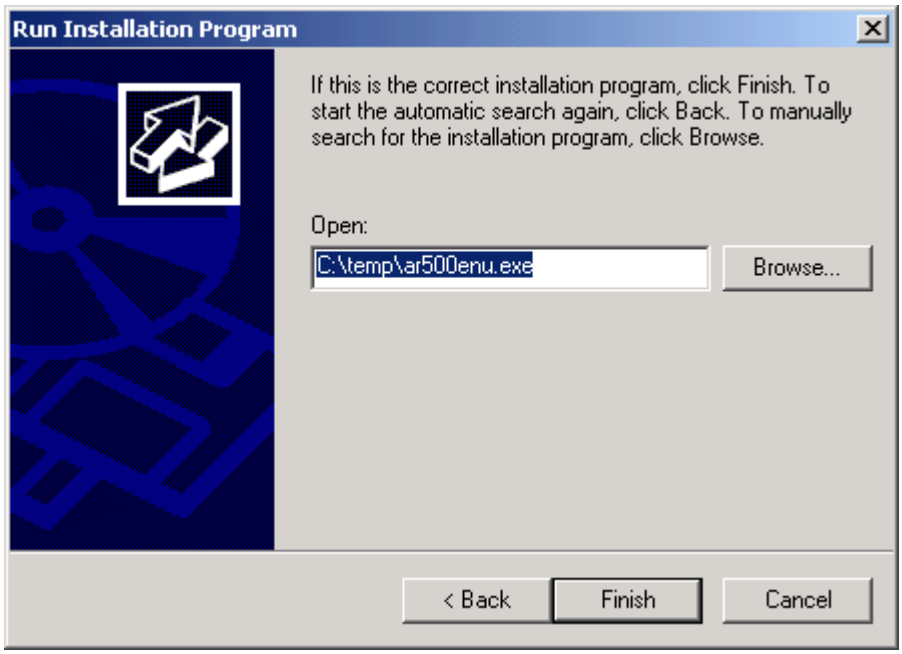
Если вы устанавливаете приложение, не удовлетворяющее спецификациям Microsoft и не имеющее скрипта совместимости, см. раздел "Установка недокументированных приложений".

Примеры инсталляции приложений на терминальном сервере

Давайте рассморим процесс инсталляции трех разных приложений. Одно не имеет проблем с Terminal Services, другое требует специального метода установки для Terminal Services, а третье требует скрипта совместимости. Это "старые" приложения - Acrobat Reader 5, Netscape Navigator 4 и Office 2000 - но многие организации до сих пор их используют.

Простая инсталляция

Adobe Acrobat Reader - это бесплатная утилита для чтения файлов PDF. Она без проблем работает на терминальном сервере. Для ее установки просто используйте мастре Add New Programs в апплете Add/Remove Programs панели управления, как показано на рисунке. Мастер автоматически переводит сервер в режим инсталляции.



По завершении инсталляции щелкните кнопку *Finish*. Сервер вернется в режим исполнения и Acrobat Reader готов для ваших терминальных пользователей. В качестве упражнения откройте редактор реестра и сравните значения в HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Adobe с аналогичными в HKEY_CURRENT_USER\Software\Adobe, чтобы убедиться, что сработало отображение реестра. Когда пользователь первый раз запустит Acrobat, система скопирует ключи в пользовательский узел HKEY_CURRENT_USER.

Уже вышел Acrobat Reader 6. Эта версия упакована в MSI и также не требует особых шагов для установки на терминальном сервере.

Заказная инсталляция

Некоторые производители ПО учитывают Terminal Services при написании программ и предоставляют инструкции по установке их на терминальном сервере. В качестве примера рассмотрим процесс установки приложения, которое проектировалось с учетом Terminal Services - Microsoft Office 2000. Office 2000 в чистом виде имеет ряд проблем при работе на терминальном сервере.

- *Install on First Use*. Поскольку пользователи не имеют права инсталлировать компоненты на терминальном сервере, опция *Install on First Use* непригодна. Вместо этого нужно установить все компоненты либо *Run from My Computer,* либо *Not Available*.

- *Имя и инициалы пользователя* - Инсталлятор запрашивает у пользователя его имя и инициалы, поэтому эти данные достанутся всем пользователям терминального сервера. Вам необходимо разрешить переключатель NOUSERNAME, чтобы Office запрашивал у пользователя его имя при первом запуске.

- *Анимация* - Частые прорисовки экрана крайне нежелательны в терминальной среде, поэтому анимации следует избегать. Главный преступник здесь - это Помощник, его не следует устанавливать.

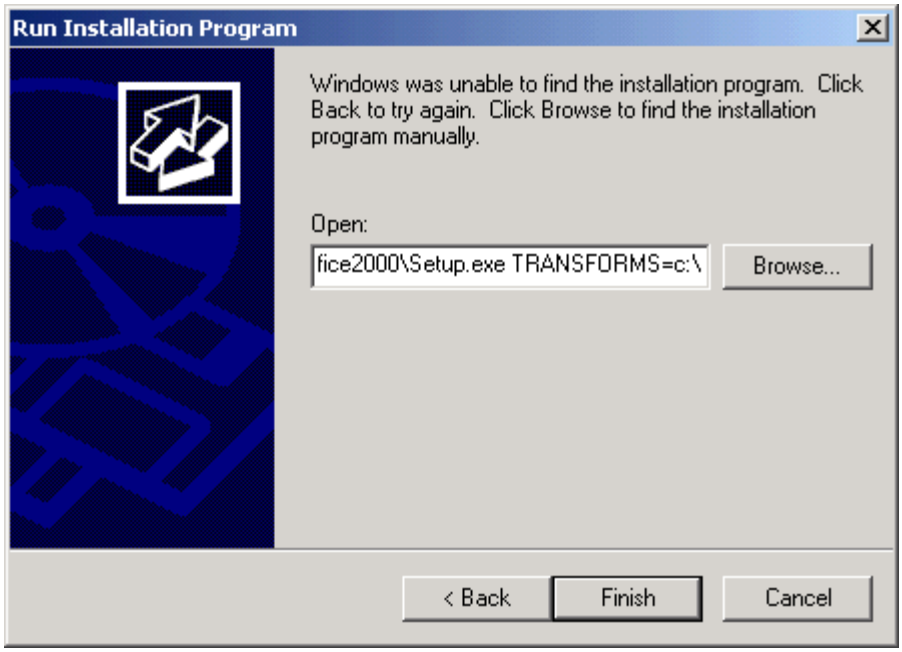
Эти проблемы решаются применением трансформы для Office 2000 - файла `TermSrvr.mst`. Трансформа - это специальный файл, который предписывает Windows Installer настроить Office для Terminal Services и исключить пролематичные возможности Office 2000.

Трансформы для Terminal Services можно найти в Office Resource Kit, который вы можете загрузить по ссылке http://www.microsoft.com/office/ork/2000/appndx/toolbox.htm#orktools. Есть также

подробная статья об установке Office на терминальном сервере: http://www.microsoft.com/office/ork/2000/two/30t3_2.htm.

Раздобыв файл MST, вы готовы к установке Office 2000. Откройте в панели управления апплет *Add/Remove Programs*, выберите *Add New Programs*. Щелкните *CD or Floppy*, найлите файлы Office и выберите SETUP.EXE. Теперь вы должны указать инсталлятору использовать трансформу. Для этого добавьте к команде

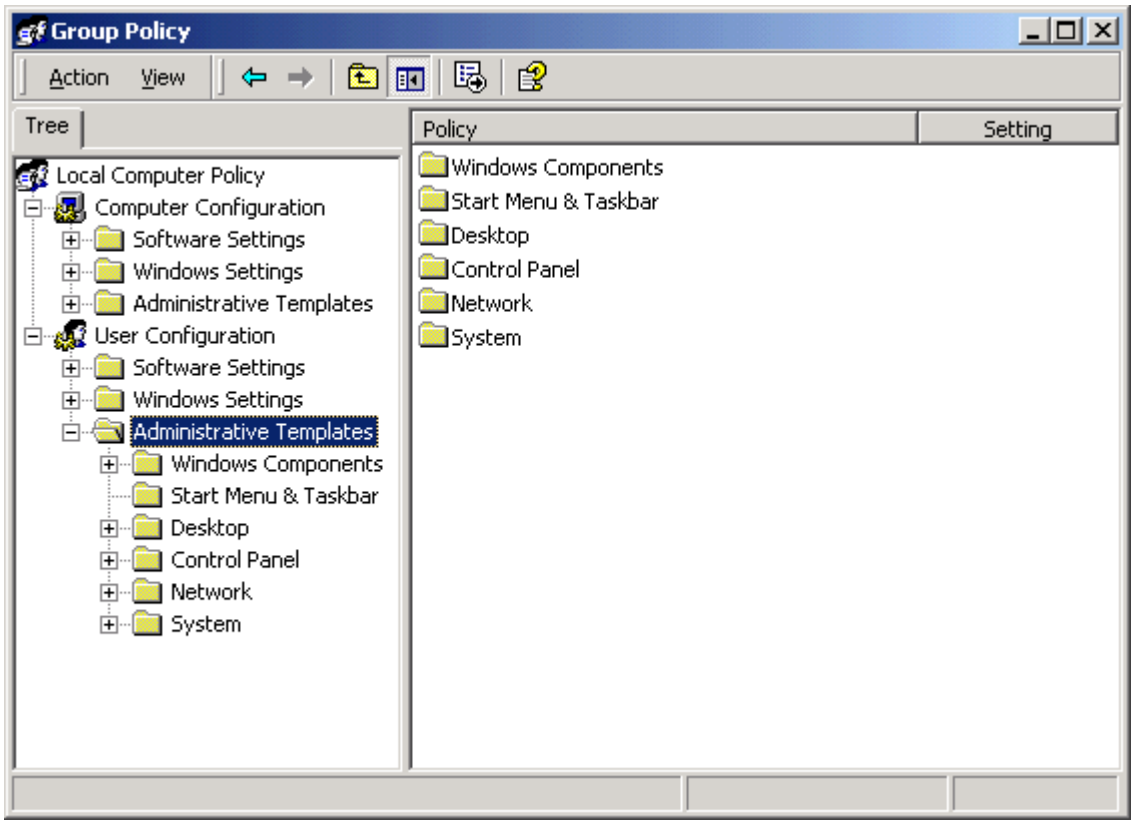
```
TRANSFORMS=path\TermSrvr.mst
```



По завершении установки щелкните Finish для перевода Terminal Services обратно в режим исполнения. Я рекомендую устанавливать последний релиз Office, поскольку в них исправлены некоторые ошибки, затрагивающие пользователей Terminal Services.

Теперь следует добавить кое-какие настройки для ваших пользователей. Вы можете это сделать с помощью Office Profile Wizard или файлов ADM для Office 2000 совместно с редактором локальных или доменных групповых политик. Если вы хотите использовать Office Profile Wizard, следуйте документации, которую предлагает Microsoft. Если вы находитесь в домене AD или используете групповые политики для управления пользовательскими настройками, см. Главу 4. Для использования локальной политики, найдите файлы ADM, входящие в состав Resource Kit, затем запустите редактор политик:

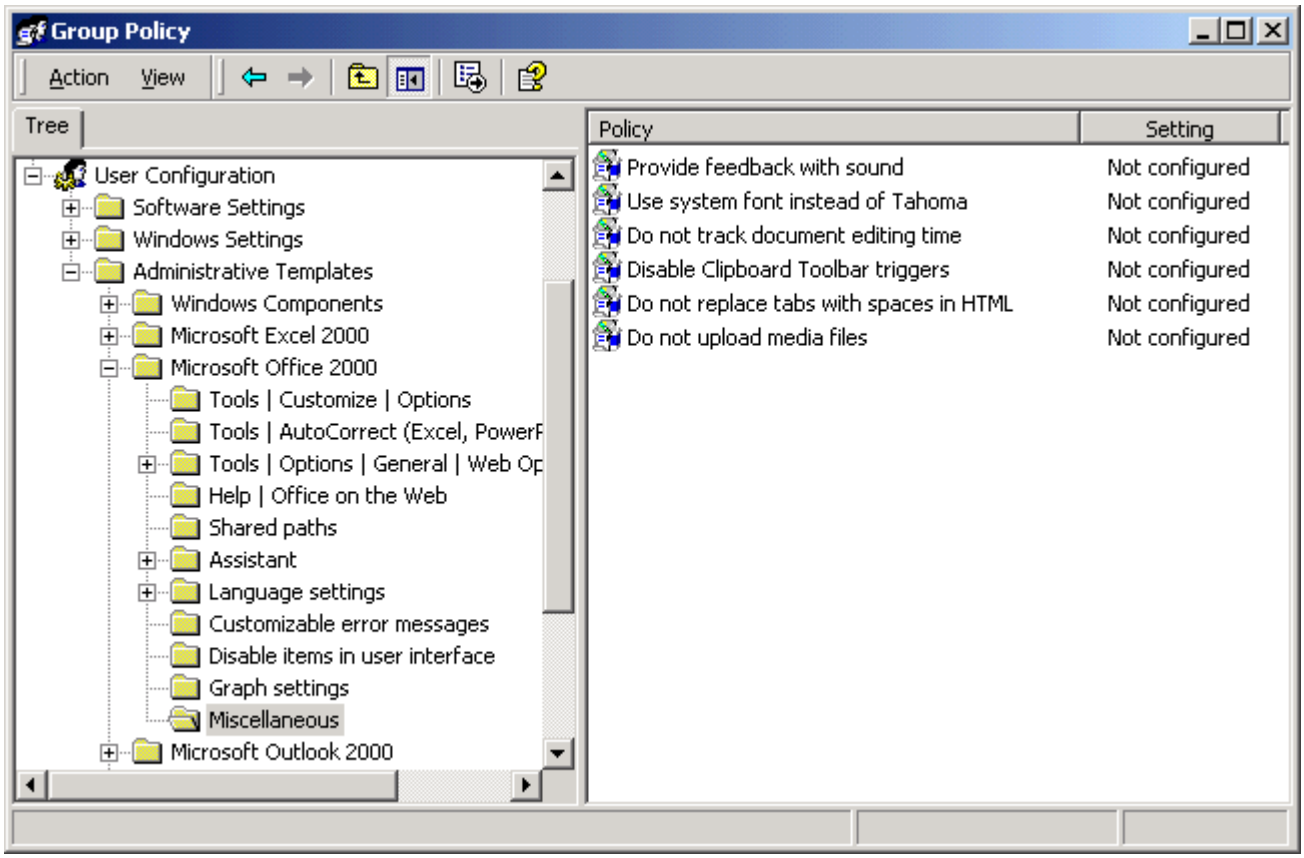
```
GPEDIT.MSC
```



Щелкните правой кнопкой на *Administrative Templates*, выберите *Add/Remove Templates*. Добавьте файлы ADM для программ, которые вы инсталлировали. В следующей таблице перечислены файлы ADM, ассоциированные с программами Office.

Компонент Office	**Файл ADM**
Общие настройки Office	OFFICE9.ADM
Word 2000	WORD9.ADM
Excel 2000	EXCEL9.ADM
PowerPoint 2000	PPOINT9.ADM
Outlook 2000	OUTLK.ADM
FrontPage 2000	FRONTPG4.ADM
Access 2000	ACCESS9.ADM
Publisher 2000	PUB9.ADM

После добавления файлов ADM, вы получаете доступ к огромному числу настроек, которые вы можете сконфигурировать или запретить для ваших пользователей.



Вы должны проверить все значения и настроить Office для ваших пользователей. Вам следует запретить любые особенности, использующие звуки и анимацию. Удалите из всех продуктов команду *Detect and Repair*. Вы можете также запретить проверку правописания и грамматики при вводе (*Check Spelling as you Type* и *Check Grammar as you Type*), поскольку эти операции сильно загружают процессор.

Вы должны учитывать, что если вы используете для настройки локальную машинную политику, то настройки будут применены ко всем пользователям, включая администраторов.

С выпуском Windows XP, Microsoft включила необходимые модификации для терминальных серверов внутрь инсталляционного пакета MSI. При инсталляции Office XP на терминальном сервере, Windows Installer обнаруживает наличие терминального сервера и автоматически применяет необходимые изменения. Трансформы больше не нужны.

Даже с этими новыми улучшениями в установке Office XP все равно необходимо сделать пост-инсталляционную настроку, используя файлы ADM для Office XP. Подробнее см. http://www.microsoft.com/office/ork/xp/one/deph02.htm.

Инсталляция с использованием скриптов совместимости

Некоторые приложения требуют модификации после инсталляции или внесения изменений "на лету" во время входа пользователя. Эти изменения осуществляются скриптами совместимости. В качестве примера мы рассмотрим установку Netscape Communicator 4.5.

Как и для других приложений, мы начнем с мастера *Add New Programs*. Сделайте инсталляцию Netscape как обычно, затем щелкните *Finish* для закрытия мастера. Теперь надо установить скрипт совместимости. Перед этим давайте разберемся, почему он необходим для Navigator 4.5:

- Профили пользователей - по умолчанию, Navigator 4.x хранит профили пользователей (избранное, настройки, историю) в каталоге программы. Пользователи на сервере терминалов не имеют доступа к каталогу Program Files, поэтому нам надо указать Netscape

хранить профили пользователей в их домашних каталогах, а не на терминальном сервере, и автоматизировать настройку профиля при каждом входе пользователя.

- Менеджер профилей - Navigator включает менеджер профилей, который позволяет пользователям изменять и удалять чужие профили на терминальном сервере. Нам нужно ограничить доступ к этой утилите.

- Панель быстрого запуска - Пользователи хотят иметь иконку Netscape в панели быстрого запуска. Скрипт совместимости может ее создать для них во время входа.

Для запуска скрипта откройте каталог C:\WINNT\Appliation Compatibility Scripts\Install и запустите `NETCOM40.CMD`. Скрипт выполняет следующие действия:

- Проверяет, установили ли вы ROOTDRIVE и предлагает это сделать, если эта переменная пустая
- Копирует иконку Quick Launch из вашего профиля в каталог программы Netscape в качестве шаблона для будущих пользователей.
- Копирует каталог профиля Netscape, созданный программой установки, в качестве шаблона для будущих пользователей.
- Применяет ограничительные разрешения для утилиты управления профилями для предотвращения запуска ее не-администраторами
- Меняет скрипт входа для Netscape, чтобы он отражал ROOTDRIVE
- Добавляет вызов дополнительного скрипта в USRLOGN2.CMD, чтобы скрипт совместимости выполнялся для всех пользователей.

При входе пользователя запускается `COM40USR.CMD` (скрипт входа для Netscape), и выполняет слудющие действия:

- Копирует шаблон User Profile в пользовательский ROOTDRIVE, если его еще нет
- Модифицирует раздел Netscape в ключе реестра HKEY_CURRENT_USER, указывая на новый профиль на ROOTDRIVE.
- Создает иконку в панели быстрого запуска, если ее еще там нет.

Теперь Netscape готов для работы на терминальном сервере.

Установка недокументированных приложений

Что делать, если вам попалось приложение, которое не содержит документации по работе с Terminal Services? Вам небходимо научиться определять, требует ли приложение настройки после инсталляции и нужны ли ему скрипты совместимости. Этот навык очень важен, хотя многие современные приложения следуют спецификациям Microsoft.

Начните с веб-сайта производителя программы, поищите в разделе технической поддержки по ключеым словам “terminal server” или “Citrix” (даже если вы используете только Terminal Services без MetaFrame, вы можете найти много полезной информации, проиндексированной для Citrix, поскольку это давний лидер в области терминальных служб). Если вы ничего не нашли, поспрашивайте в форумах, поищите по ключевым словам, указав имя вашего приложения AND “terminal server” OR “Citrix.”

В поиске недокументированных приложений полезны следующие сайты :

http://www.thethin.net

http://www.thinplanet.com

Собрав любую информацию о вашем приложении, инсталлируйте его на пилотном сервере. Ваш пилотный сервер должен иметь такую же конфигурацию, что и рабочий - с теми же патчами, сервис-паками, скриптами и пр.

Никогда не инсталлируйте непроверенные приложения на рабочий сервер!!!

Как и в случае с другими приложениями, для установки используйте мастер *Add New Programs*. Если приложение после установки требует перезагрузки, сделайте это. Перед первым запуском приложения проверьте реестр. Начните с HKEY_LOCAL_MACHINE\SOFTWARE и найдите подключ для приложения. Проверьте значения, уделяя особое внимание данным, соежржащим абсолютные маршруты. Значения типа InstallPath или ApplicationSource нормальные, поскольку они одинаковы для всех пользователей, но значения, относящиеся к пользовательским настройкам, например, UserDictionary или UserHome, могут вызвать проблемы. Запишите эти ключи на бумаге.

Затем проверьте в HKEY_CURRENT_USER\Software, что приложение сконфигурировало ключи реестра. Если так, найдите здесь те же типы значений и запишите то, что вы нашли. Проверьте, создано ли зеркало ключей в улее HKEY_LOCAL_MACHINE. Если нет, создайте файл .REG для ключа приложения HKEY_CURRENT_USER\Software, выбрав в regedit опцию *Export Registry File* из меню Registry. Этот файл понадобится позже, если вам понадобится вручную синхронизировать ключи.

Сделайте экспорт ключа приложения HKEY_CURRENT_USER\Software до того, как запустите приложение в первый раз. Вам не следует захватывать настройки, которые сгенерируются при первом запуске.

Теперь запустите приложение под той учетной записью, под которой оно установлено. Пройдитесь по всем функциям приложения в поиске потенциальных проблем - сообщений об ошибках, неверного поведения и пр. Затем войдите на терминальный сервер под тестовой учетной записью. Эта учетная запись не должна быть администратором, а должна быть сконфигурирована как обычный пользователь. Запустите приложение и выполните те же тесты. Если ошибок не обнаружено, закройте приложение и проверьте реестр для этого пользователя.

Убедитесь, что ключи приложения из HKEY_CURRENT_USER корректно скопировались из ключа Terminal Server в HKEY_LOCAL_MACHINE или были автоматически созданы приложением. Если ключи отсуствуют при сравнении их с теми, что находятся в учетной записи пользователя, установившего приложение, вы должны вручную их синхронизировать. Для этого:

1. Откройте в Notepad файл .REG, созданный ранее, и выберите *Replace* из меню *Edit* для замены всех вхождений HKEY_CURRENT_USER\Software на HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software.
2. Импортируйте файл .REG в реестр

Теперь удалите профиль (локальный и перемещаемый) тестовой учетной записи и зарегистрируйтесь еще раз. Запустите приложение и убедитесь, что отраженные ключи скопировались. Если они там, и вы решили внести для ваших пользователей какие-то изменения в реестре, сделайте их в HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software, и новые настройки будут скопированы, когда ваши пользователи запустят приложение в первый раз.

Теперь обратитесь к вашим записям ключей реестра, относящихся к пользовательским настройкам. Если вы обнаружили ссылки на пользовательские файлы, хранящиеся на локальных драйвах терминального сервера, вы должны попробовать скопировать эти файлы в подкаталог вашего драйва ROOTDRIVE, затем изменить значение реестра так, чтобы оно указывало на новое место. Если эти ключи находятся в HKEY_LOCAL_MACHINE, то просто измените их там. Если они находятся в HKEY_CURRENT_USER, измените их там и в подключе HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software. Задокументируйте все изменения, которые вы делаете в реестре, чтобы повторить их позже на рабочем терминальном сервере. Запустите приложение и убедитесь, что оно не испытывает проблем с новыми каталогами.

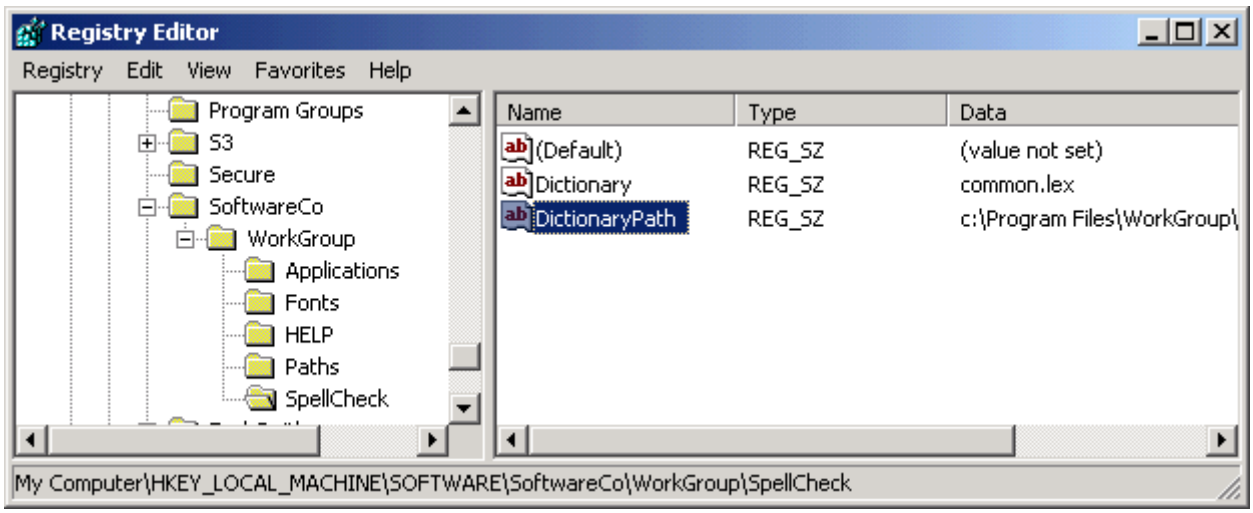
Это процесс - метод проб и ошибок, он отличается для каждого устанавливаемого вами приложения. К счастью, его следует применять только для приложений, не сертифицированных для Windows.

Пример из реального мира

Давайте рассмотрим пример приложения, требующего модификации для использования на терминальном сервере. Допустим, ваша компания использует некую программу, называемую WorkGroup, для управления проектами. Эта программа использует базу данных SQL для хранения описаний проекта, сроков, замечаний членов проекта и пр. Вы хотите инсталлировать WorkGroup на ваш терминальный сервер, чтобы позволить пользователям запускать его через веб-браузеры (используя клиент Remote Desktop Web connection).

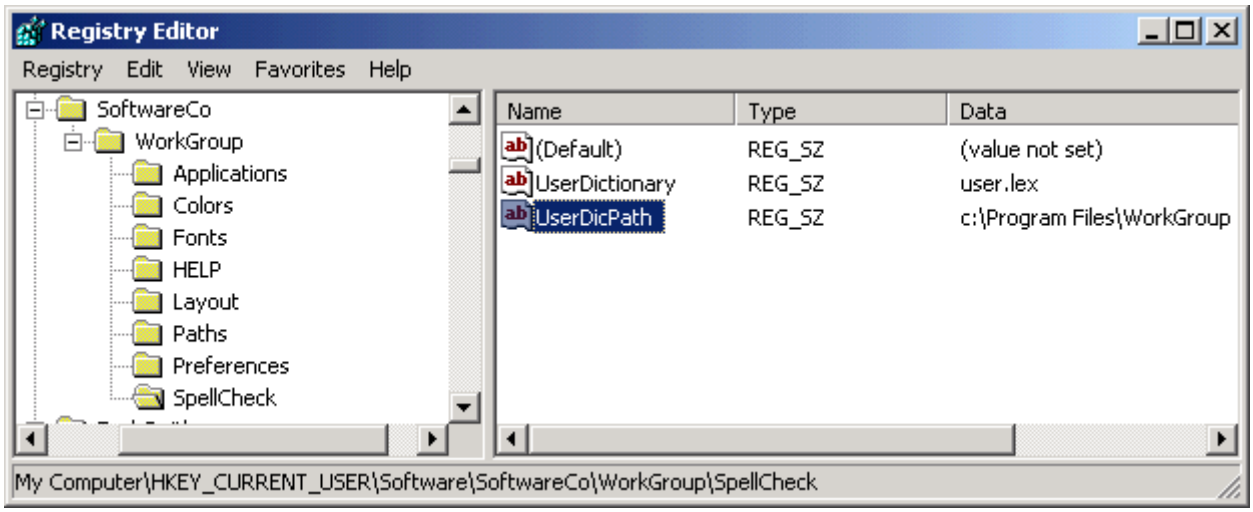
Вы ничего не нашли на веб-сайте производителя про терминальный сервер, а когда позвонили в службу технической поддержки компании, то услышали, что продавец не поддерживает приложение на терминальном сервере. Вы просмотрели группы новостей, но это редкое приложение и никто его не упоминает. Вам необходимо самим проверить приложение, чтобы убедиться, что оно совместимо с Terminal Services и требует ли оно скрипты совместимости.

Начните с мастера Add New Programs для запуска SETUP.EXE для установки WorkGroup. инсталлятор не требует перезагрузки, поэтому немедленно запустите regedit и поищите в HKEY_LOCAL_MACHINE\SOFTWARE абсолютные маршруты в ключе WorkGroup:



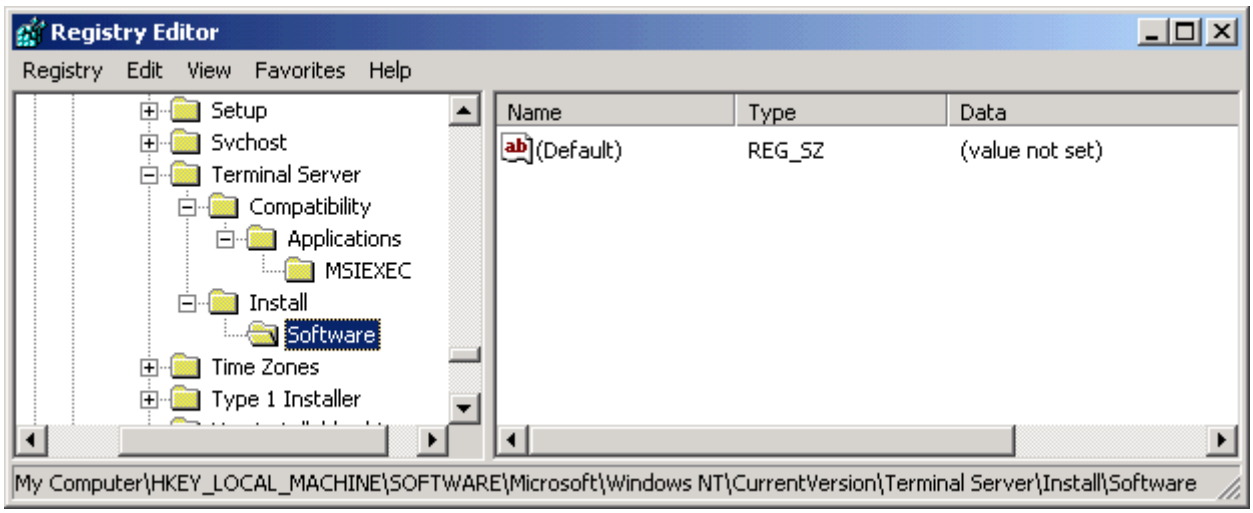
В ключе Paths вы обнаружили размещение базы данных SQL, которая является общей для всех пользователей, поэтому она не будет представлять проблем для Terminal Services. Однако, в SpellCheck вы нашли значение, которое может создать проблемы - DictionaryPath. После внимательного изучения, это значение выглядит как файл словаря, который совместно используется всеми пользователями. На всякий случай запишите на бумаге значение этого ключа.

Затем поищите аналогичные значения в HKEY_CURRENT_USER\Software. Здесь вы находите еще один ключ SpellCheck, который содержит размещение пользовательского словаря - C:\Program Files\Workgroup:



Этот ключ поднимает красный флаг для Terminal Services. Каждый пользователь должен иметь свой файл USER.LEX для WorkGroup, но этот файл по умолчанию хранится на терминальном сервере, а не в пользовательском домашнем каталоге. К счастью, WorkGroup позволяет изменить ключ реестра для размещения файла, поэтому проблему можно легко решить.

Затем определите, сработало ли отображение реестра, сравнив этот ключ HKEY_CURRENT_USER с HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server, как показано на следующем рисунке.



Как видно, отражение не сработало, поэтому вы должны сделать отражение раздела реестра вручную (если вы решили, что вам нужно предварительно сделать настройки в HKEY_CURRENT_USER для ваших пользователей). В этом случае вы должны создать файл .REG для ключа HKEY_CURRENT_USER\Software\SoftwareCo\WorkGroup.

Теперь запустите WorkGroup и убедитесь, что программа работает под учетной записью пользователя, инсталлировавшего ее. Допустим, что все работает. Вы можете подключиться к базе данных, считывать и вводить данные, делать запросы. Теперь сделайте то же самое под обычным тестовым пользователем. Приложение запускается без проблем, но при попытке добавить слово в пользовательский словарь программа выдает ошибку - тестовый пользователь не имеет прав записи в файл USER.LEX, находящийся на диске C. Вам необходимо устранить этот дефект.

Сначала проверьте, позволяет ли WorkGroup переместить файл USER.LEX в другое место. Снова зарегистрируйтесь под администратором и скопируйте файл из C:\Program Files\WorkGroup в H:\WorkGroup, а затем измените значение UserDicPath в HKEY_CURRENT_USER на H:\WorkGroup. Теперь запустите WorkGroup и попробуйте добавить слово в словарь. Проверив временные метки,

вы можете подтвердить, что слово добавлено в копию на драйве H, поэтому изменения сделаны успешно.

Чтобы реплицировать эти изменения для всех пользователей, вам нужно сделать следующее:

- Изменить значение UserDicPath для каждого пользователя
- Копировать файл USER.LEX на ROOTDRIVE всякий раз при входе пользователя.

Вы могли бы сделать это с помощью отображения реестра, но, как мы выяснили, это отображение придется сделать вручную. Копирование файла потребует скрипта совместимости. Давайте рассмотрим эти задачи по очереди.

Для создания отображения реестра, отредактируйте файл .REG, созданный из HKEY_CURRENT_USER, щелкнув на нем правой кнопкой и выбрав *Edit*. Используйте команду *Replace* для замены всех вхождений "HKEY_CURRENT_USER\Software" на "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software".

Кроме того, найдите значение UserDicPath и измените его на "H:\WorkGroup". Сохраните измененный файл в каталоге C:\WINNT\Application Compatibility Scripts\Install.

Для копирования файла вам нужно написать два скрипта совместимости - один для инсталляции, а второй для входа. Для нашего приложения оба скрипта очень просты. Для копирования файла в нужное место вам необходимо определить переменную ROOTDRIVE. Затем инсталляционный скрипт должен импортировать ваш файл .REG и добавить вызов скрипта совместимости для входа в USRLOGN2.CMD.

Ручной импорт файла .REG и редактирование USRLOGN2.CMD может быть проще, но использованием инсталляционного скрипта совместимости вы делаете этот процесс легко повторяемым при инсталляции приложения на рабочем сервере. Убедитесь, что вы поддерживаете центральное хранилище для всех скриптов совместимости, которых вы создаете, чтобы вы могли реплицировать их на новых серверах.

WorkGroup.cmd - Notepad

File Edit Format Help

```
@Echo off

Rem ##########################################################################

Rem
Rem Verify that %RootDrive% has been configured and set it for this script.
Rem

Call "%SystemRoot%\Application Compatibility Scripts\ChkRoot.Cmd"
If "%_CHKROOT%" == "FAIL" Goto Done

Rem ##########################################################################

REM
REM Import the WorkGroup.REG file into the registry to establish
REM the mirror and update th User Dictionary location
REM

REGEDIT /S WorkGroup.REG


Rem
Rem Add WorkGroupUSR.Cmd to the UsrLogn2.Cmd script
Rem

FindStr /I WorkGroupUSR| %SystemRoot%\System32\UsrLogn2.Cmd >Nul: 2>&1
If Not ErrorLevel 1 Goto Skip1
Echo Call WorkGroupUSR.Cmd >> %SystemRoot%\System32\UsrLogn2.Cmd
:Skip1


:Done
```

Перед запуском инсталляционного скрипта совместимости, вам необходимо создать скрипт совместимости для входа, который будет делать копирование файла для каждого пользователя. Этот скрипт будет вызываться всякий раз при входе пользователя, но он должен копировать файл лишь в том случае, если его не существует на пользовательском ROOTDRIVE. Этот скрипт должен быть сохранен в каталоге C:\WINNT\Applicaiton Compatibility Scripts\Logon. Ниже показан пример скрипта совместимости для входа:

WorkGroupUSR.cmd - Notepad

File Edit Format Help

```
Rem
Rem Copy the User Dictionary file for WorkGroup
Rem

If Exist "%RootDrive%\WorkGroup" Goto Skip1

MD| "%RootDrive%\WorkGroup"
copy "c:\Program Files\WorkGroup\User.lex" "%RootDrive%\WorkGroup" /Y >Nul: 2>&1


:Skip1
```

Теперь, когда все части собраны, запустите инсталяционный скрипт совместимости для WorkGroup. Теперь вы должны проверить скрипт совместимости, войдя под тестовым пользователем. Не забудьте удалить профиль этого пользователя - как перемещаемый, так и локальный - перед входом, чтобы получить чистое окружение.

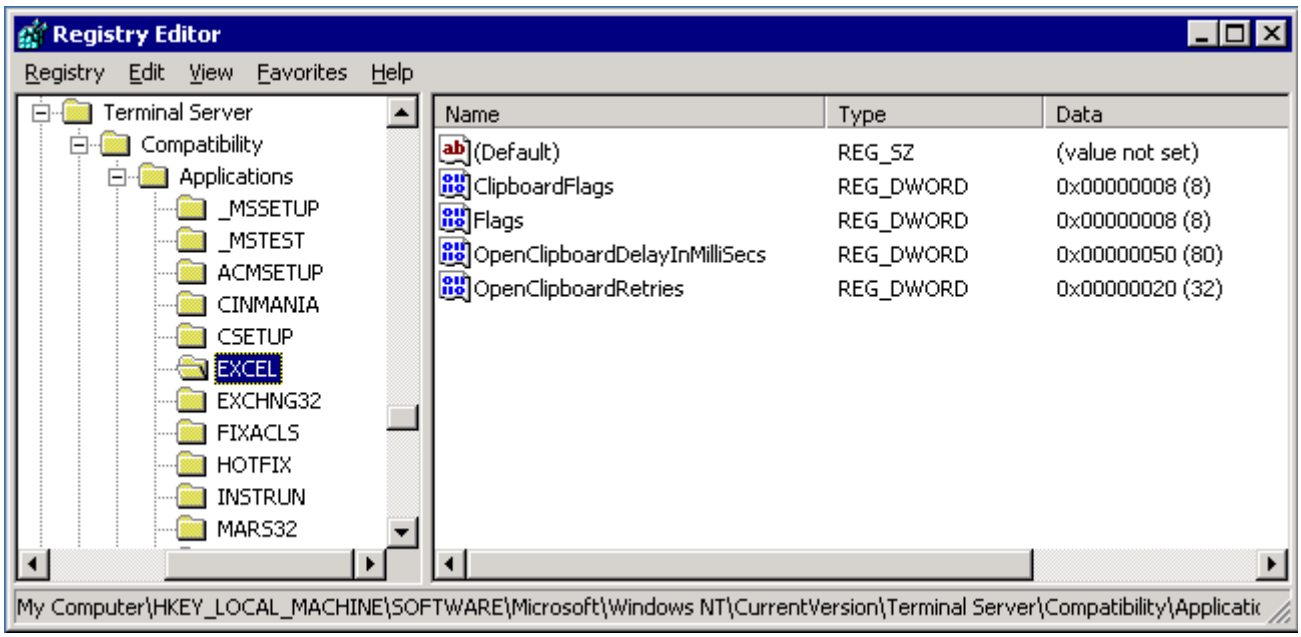
После входа в первую очередь поищите в домашнем каталоге файл USER.LEX, созданный в подкаталоге WorkGroup. Если файла нет, вернитесь назад и убедитесь, что ваш скрипты совместимости для инсталляции правильно добавил вызов команды в USRLOGN2.CMD, а затем проверьте скрипт совместимости для входа.

Теперь запустите WorkGroup и убедитесь, что все ключи реестра, особенно измененное значение UserDicPath, скопировались в HKEY_CURRENT_USER для тестового пользователя. Добавьте слово в пользовательский словарь тестового пользователя и убедитесь, что это слово добавлено в словарь, находящийся в домашнем каталоге.

Завершив этот процесс, вы должны проверить WorkGroup, запустив ее одновременно несколькими пользователями. Если вы удовлетворены производительностью, вы готовы повторить инсталляцию на рабочем сервере.

Флаги совместимости Terminal Services

При установке приложения, Terminal Services создает в реестре ключ для флагов совместимости, которые сообщают терминальному серверу тип приложения (MS-DOS, 16-bit, 32-bit). Если вы инсталлируете старое приложение, которое не будет работать на терминальном сервере, вы можете изменить этот флаг так, чтобы терминальный сервер сделал определенные настройки при запуске этого приложения.



Эти флаги затрагивают выделение памяти, отображение реестра и файлов INI. Их также можно использовать, чтобы Terminal Services возвращал значение %USERNAME%, если приложение запрашивает %COMPUTERNAME%. Эта особенность полезна, если приложение использует имя машины в качестве уникального идентификатора.

Если ваша программа не хочет работать под Terminal Services, прочтите статью Microsoft “Terminal Server Registry Settings for Applications”

Инсталляция приложений с помощью групповых политик

Если вы управляете большой фермой терминальных серверов или нуждаетесь в быстром расширении фермы, вы можете использовать технологию автоматизированной установки программного обеспечения. В среде AD вы можете использовать групповые политики для назначения приложений вашим серверам. При загрузке сервера обрабатываются машинные политики и инсталлируются все назначенные приложения.

Чтобы использовать групповые политики, приложения должны быть в формате MSI. Групповые политики также поддерживают скрипты в формате ZAP, которые могут запускать инсталляторы, отличные от MSI. Однако, использование этого формата на терминальных серверах не рекомендуется, поскольку такие приложения не поддерживают advertising, и ваши пользователи не получат необходимые ключи реестра HKEY_CURRENT_USER.

Вы можете переупаковать приложение в MSI используя сторонние утилиты, например, Wise for Windows Installer. Обязательно проверьте приложение на терминальном сервере до и после перепаковки, чтобы выяснить, нужны ли какие-то модификации для обеспечения совместимости с Terminal Services.

Основные шаги, требуемые для инсталляции программ с помощью групповых политик, таковы:

- Создайте папку общего доступа для хранения ваших пакетов MSI.
- Создайте административные инсталляции ваших пакетов MSI и поместите их в эту общую папку.
- Добавьте пакеты в GPO, котрые применяются к компьютерам терминальных серверов в AD.
- Модифицируйте права доступа к пакетам в GPO, если вы хотите, чтобы пакеты инсталлировались на отдельных серверах.
- Перезагрузите терминальные серверы.

Создание папки общего доступа

Для назначения или публикации приложений с помощью групповых политик вам необходимо центральное место для исходных файлов приложений. Путь к этому месту должен быть доступен для всех компьютеров, к которым применяется данная политика. Простейший способ состоит в создание папки общего доступа на файловом сервере и копировании в нее исходных файлов.

Убедитесь, учетные записи машин ваших терминальных серверов имеют право чтения и выполнения в этой папке. Группы Authenticated Users и Everyone включают машинные учетные записи.

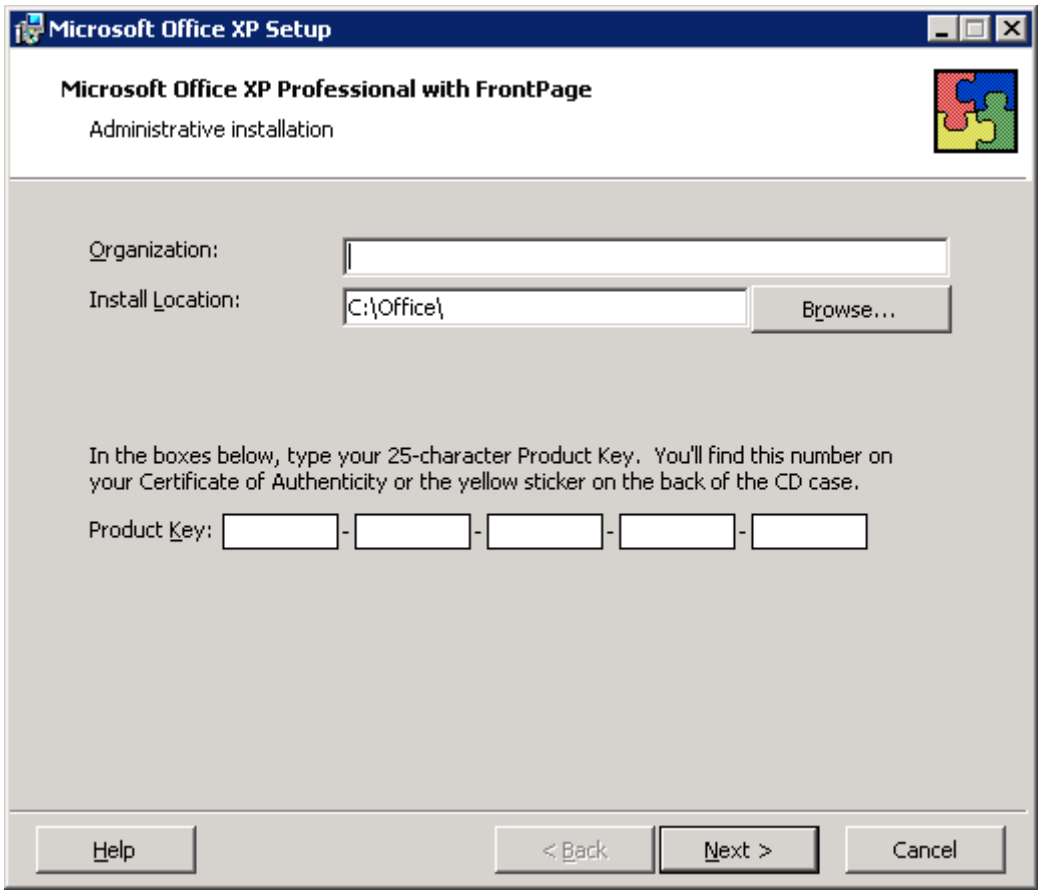
Создание административных инсталляций

Пакеты MSI обычно включают в себя все требуемые файлы, упакованные в файлы CAB. Для оптимизации установки программ, заблаговременно распакуйте эти файлы, создав административную инсталляцию.

Для создания административной инсталляции, запустите Windows Installer Service с опцией “/a” и укажите путь к пакету MSI, который вы хотите распаковать.:

```
msiexec /a d:\proplus.msi
```

Появится мастер, похожий на рисунке, который запрашивает каталог для административной инсталляции. Если приложение требует лицензионного ключа, мастер его запросит. Ключ будет зашифрован и включен в административную инсталляцию, поэтому в дальнейшем он не будет спрашиваться.

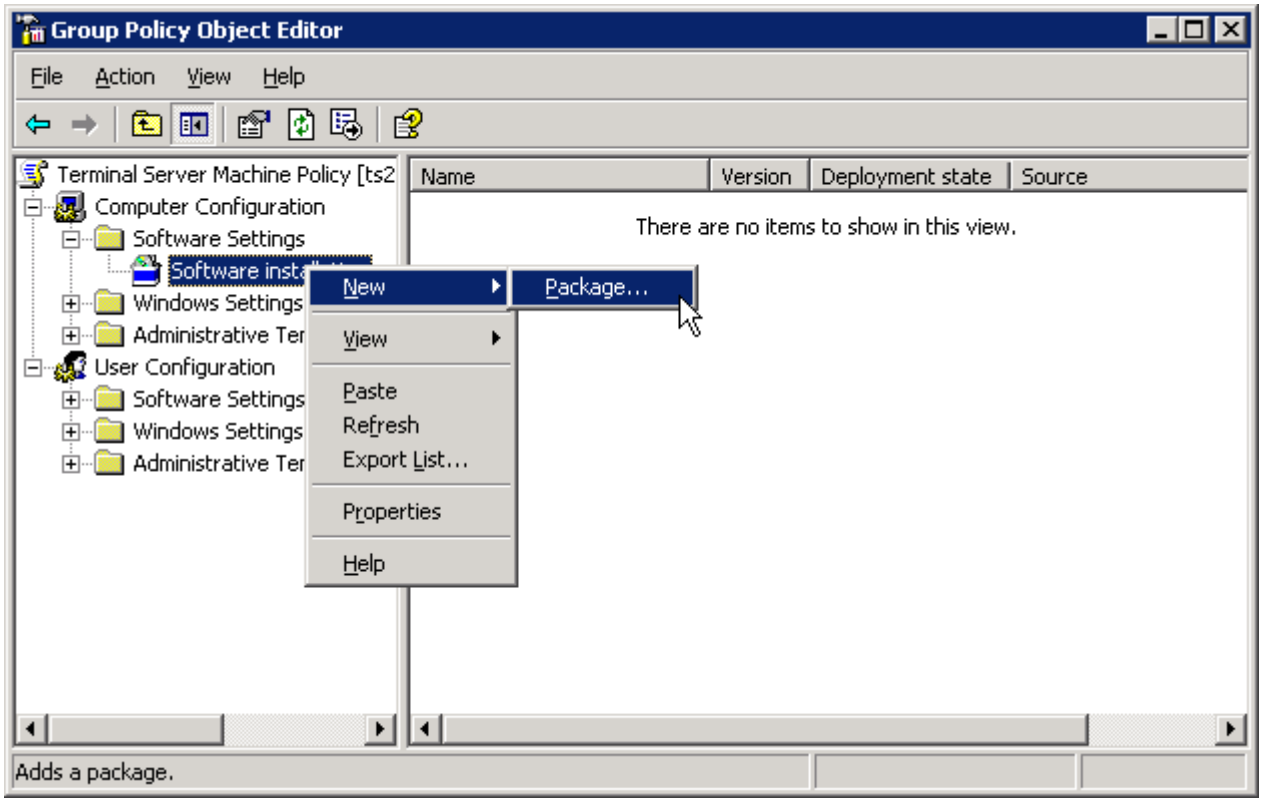


По завершении административной инсталляции, скопируйте новые исходные файлы в общую папку.

Добавление пакетов в GPO

В главе 4 мы создали OU для терминальных серверов и прикрепили к ней три объекта групповых политик. Один из них - это Terminal Server Machine Policy. Этот объект содержит машинную конфигурацию ваших терминальных серверов, поэтому он уже готов для применения к терминальным серверам. Вы можете добавить программные пакеты к этому GPO, и они будут проинсталлированы на всех компьютерах, входящих в OU "TerminalServers".

Для добавления пакета в GPO, откройте редактор политик, раскройте Computer Configuration, Software Settings. Щелкните правой кнопкой на *Software installation*, и выберите *New*, *Package*:

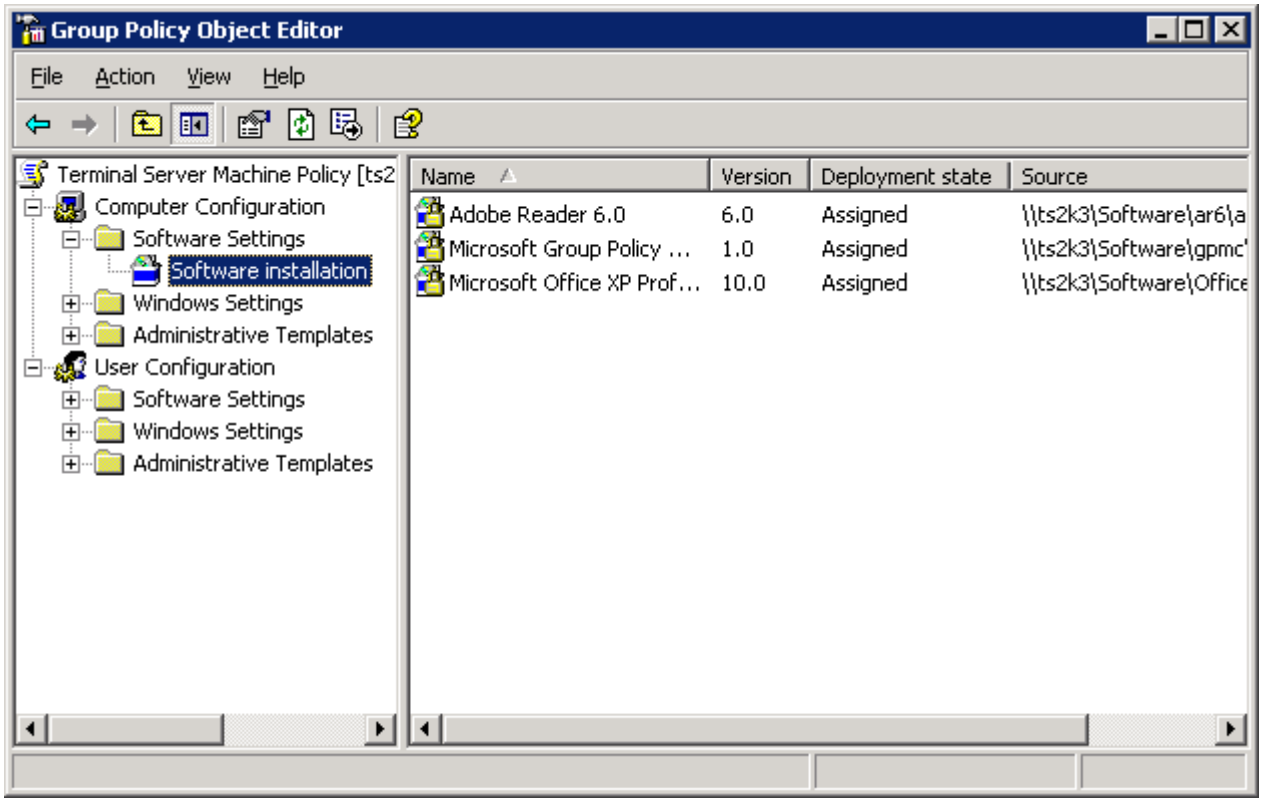


Укажите имя пакета MSI, который вы хотите добавить. Затем у вас спросят, хотите ли вы назначить пакет или открыть интерфейс расширенных настроек. В большинстве случаев вы можете выбрать *Assign* и принять опции по умолчанию. Однако, если вам необходимо указать трансформу, выберите *Advanced*.

Транформа (файл MST) определяет опции или вносит изменения в значения по умолчанию файла пакета Windows Installer (файла MSI). Вы можете создать трансформы используя Microsoft Office Custom Installation Wizard или другую утилиту.

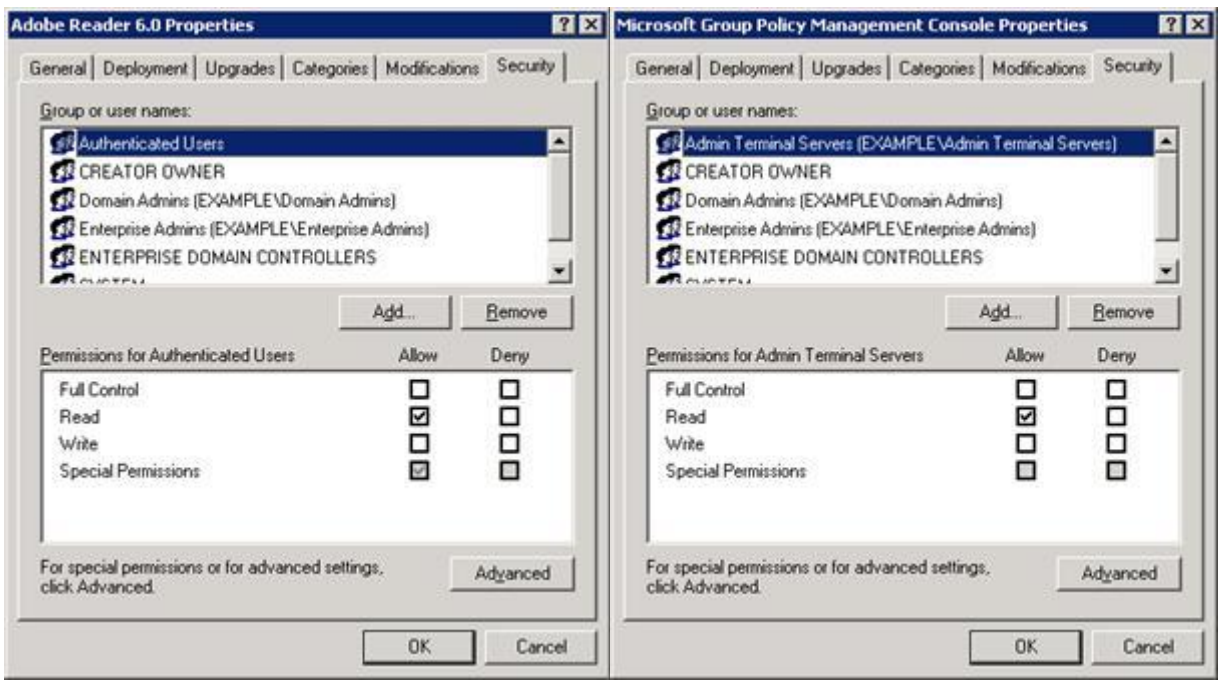
Фильтрация приложений

Вы можете использовать единый GPO, который применяется ко всем серверам, но отфильтровать приложения, которые будут установлены на каждый сервер, используя фильтры безопасности на пакетах в GPO. Следующий рисунок показывает GPO, содержащий три пакета - Adobe Acrobat Reader 6, Office XP и Microsoft Group Policy Management Console.



Допустим, что вы хотите инсталлировать Acrobat Reader и Office XP на всех терминальных серверах, к которым применяется GPO, а консоль - только на тех серверах, которые используются администраторами. По умолчанию пакеты наследуют настройки безопасности из GPO, поэтому все компьютеры, которые имеют право чтения на этот GPO будут также иметь право чтения пакета, и как следствие, установят приложение при загрузке.

Вы можете изменить права к пакету и ограничить право чтения только для отдельной группы компьютеров. Тогда все компьютеры в OU смогут обрабатывать политику, но только те, которые имеют право чтения для пакета, смогут его установить.



Чтобы этот фильтр безопасности мог работать, вы должны создать группу Domain Security - например, Admin Terminal Servers, - и поместить в нее те серверы, на которых хотите установить консоль.

Для изменения разрешений к пакету, вы должны отключить наследование разрешений GPO. Для этого щелкните *Advanced* и уберите флажок *Allow inheritable permissions*. Вы можете затем выбрать копирование существующих разрешений и использовать их в качестве отправной точки для модификаций.

Перезагрузка терминальных серверов

Основной недостаток инсталляции при помощи групповых политик состоит в том, что они обрабатываются только во время загрузки. Если вы добавляете новый пакет, то для его инсталляции вы должны перезагрузить сервер. Преимуществ инсталляции с помощью GPO состоит в том, что новые серверы, помещенные в OU "Terminal Servers", автоматически проинсталлируют необходимые пакеты, экономя ваше время и усилия.

Вы можете использовать GPO и для деинсталляции программ. Подробнее см. книгу Darren MarElia's *The Definitive Guide to Windows 2000 Group Policy* (http://www.realtimepublishers.com)

Существуют также системы управления программным обеспечением, позволяющие устанавливать программы по расписанию и не требующие перезагрузки. К ним относятся Microsoft Systems Management Server и компонент Installation Manager в Citrix MetaFrame XPe.

Развертывание приложений для конечных пользователей

Если вы используете Terminal Services для замены рабочих столов, развертывание приложений для ваших пользователей состоит просто в добавлении иконки программ в All Users в меню Start на терминальном сервере. Если же вы хотите развернуть единственное приложение в модели Application Service Provider (ASP), тип развертывания будет зависеть от типа используемого клиента.

Если пользователи подключаются к приложениям на терминальном сервере с помощью локального клиента Remote Desktop Connection, вам необходимо создать файл RDP, который содержит имя сервера и начальное приложение, а затем раздать этот файл пользователям.

Если вы хотите предоставлять доступ к приложениям через клиент Remote Desktop Web Connection, чтобы пользователи запускали программы по ссылке URL, вы должны обратиться к документации, которую предлагает Microsoft вместе с клиентом, чтобы создать веб-страницы для хостинга приложений. Клиент Web Connection Client очень мощный и настраиваемый, поэтому при небольшом знании HTML и ActiveX вы можете создать мощный портал для ваших приложений

Глава 6: Безопасность и защита от вирусов

Blaster, Love Bug, Nimda, Melissa - это компьютерные вирусы, распространенные в наши дни, поэтому инфраструктура Windows должна их учитывать. Анитивирусное ПО, брэндмауэры и управление заплатами должно быть частью крохотных вычислительных сред. Если пользователи на терминальном сервере пользуются почтой или выходят в интернет, вы должны быть бдительными и содержать сервер в безопасности. К счастью, ограничительные разрешения на терминальном сервере затрудняют занесение вирусов в систему, тем не менее вы должны быть готовы ко всему.

В этой главе мы рассмотрим доступные варианты содержания сервера в безопасности с использованием технологий Microsoft Automatic Updates и Software Update Services, а также практику применения этих вариантов.

Вирусы, черви, трояны...

Существует несколько типов вредоносного кода, от которого необходимо защищать систему. Хотя такой код обобщенно называют "вирусами", существует разница между вирусами, троянами и червями.

Вирус - это небольшая программа, которая написана с целью изменения - без ведома пользователя - функционирования компьютера. Вирусы имеют исполняемый код либо в виде смостоятельной программы, либо в виде макроса, содержащегося в другом файле, и он дожен иметь возможность копировать самого себя, чтобы продолжать работу после завершения начальной программы или макроса. Примеры вирусов:

- Загрузочные вирусы, например, Michelangelo и Disk Killer, устанавливают себя в загрузочный сектор жесткого диска, чтобы выполняться перед запуском операционной системы.
- Макровирусы, например, Melissa и Nice Day, которые находятся внутри документов Office. Эти вирусы запускаются при открытии документа и пытаются инфицировать другие документы Office или шаблоны, чтобы новые создаваемые документы также оказались зараженными.

Червь - это программа, которая использует ошибки в проектировании или брешь в безопасности ОС. Черви способны распространяться с одного компьютера на другой без помощи файла, хотя некоторые могут распространяться посредством копирования зараженного файла с одного компьютера на другой. Типичный пример такого червя - это Blaster, который использует брешь в RPC и позволяет удаленно исполнять код на других компьютерах сети для саморазмножения.

Троян - это программа, которая содержится внутри другой внешне безобидной программы. При запуске такой программы (например, хранителя экрана, поздравительной открытки, shareware-программы) в систему инсталлируется троян. Трояны могут выполнять роль spyware (шпионских программ), отправляя конфиденциальную информацию третьей стороне или могут использоваться для атак типа DoS. Основное отличие троянов от вирусов состоит в том, что трояны сами не размножаются - для инфицирования системы они должны быть запущены вручную.

Атака DoS посылает большое количество запросов на некоторый сервер или URL, вызывая сильную загрузку сервера и предотвращая обслуживанием им других запросов. Распределенная атака DoS использует вирусы, трояны или червей для подчинения нескольких компьютеров в Интернет, приказывая им одновременно атаковать некоторый сервер.

Вы должны защищать сервер от любого вредного кода. Вы можете это делать с помощью комбинации разрешений файловой системы, настроек групповых политик, антивирусного ПО, заплат безопасности, распространяемых Microsoft.

Если вы используете разрешения по умолчанию и храните пользователей в группе Users (не в Power Users), то ваша система защищена от большей части вирусов и троянов, которые пытяются заразить системные файлы или файлы в каталоге Program Files. Кроме того, вы можете использовать групповые политики для дополнительных ограничений, например, ограничить пользователей процессами и приложениями, которые они могут выполнять, запретить запись на диск С сервера и т.п.

Даже с улучшенной безпасностью файловой системы WS2K3 и дополнительными ограничениями, которые могут быть наложены групповыми политиками, полезно установить антивирусное ПО и систему управленяи патчами - авторы вирусов постоянно изобретают новые способы навредить вашей системе.

Настройка безопасности в Internet Explorer

В WS2K3 включен новый инструмент, называемый Internet Explorer Enhanced Security Configuration. После его установки, он меняет настройки безопасности в Internet Explorer, уменьшая подверженность потенциально вредному коду, который может быть найден в Web и прикладных скриптах.

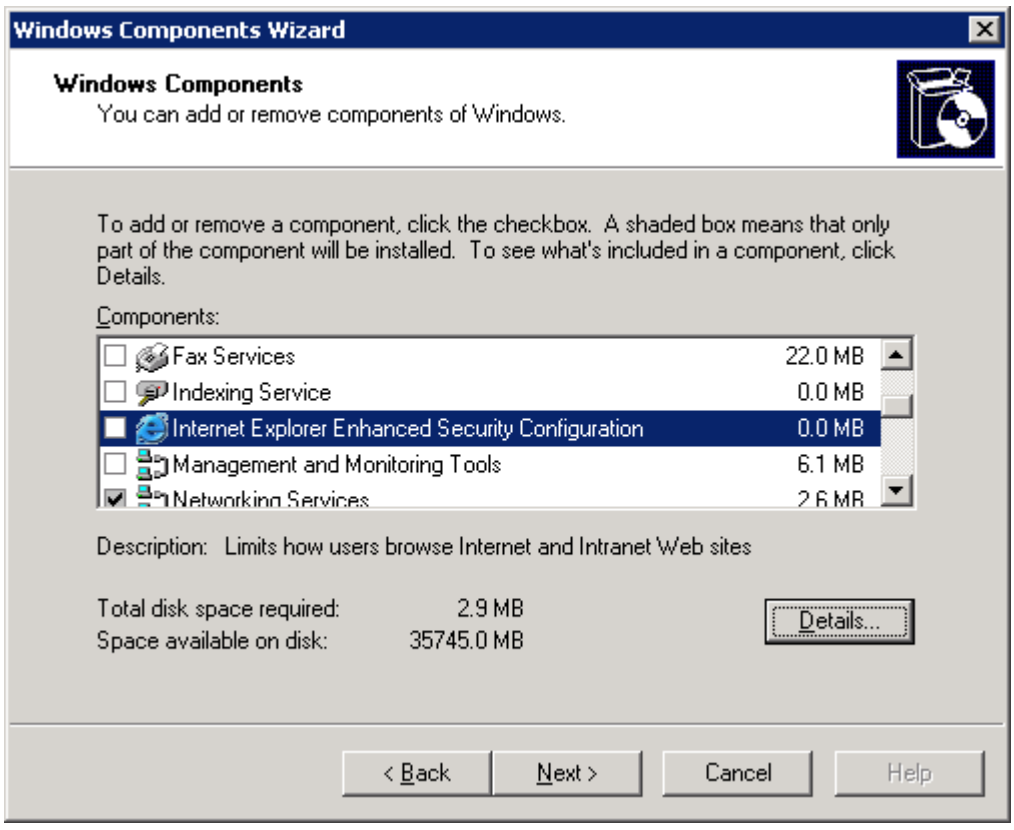
Internet Explorer Enhanced Security Configuration по умолчанию устанавливается для всех групп пользователей WS2K3, если вы не добавили роль терминального сервера - конфигурация Internet Explorer Enhanced Security Configuration на терминальном сервере зависит от метода установки операционной системы:

Тип установки	Enhanced Security Configuration			
	Administrators	Power Users	Limited Users	Restricted Users
Обновление ОС	Yes	Yes	No	No
Тихая инсталляция ОС	Yes	Yes	No	No
Ручная инсталляция Terminal Services	Yes	Yes	Prompt	Prompt

При ручной установке роли Terminal Services, мастер Configure Your Server Wizard предлагает запретить Internet Explorer Enhanced Security Configuration для групп Limited Users и Restricted Users. Это улучшает браузинг в интернет для этих пользователей и защита полагается на разрешения файловой системы, а ОС предотвращает таким пользователям выполнять или инсталлировать вредный код.

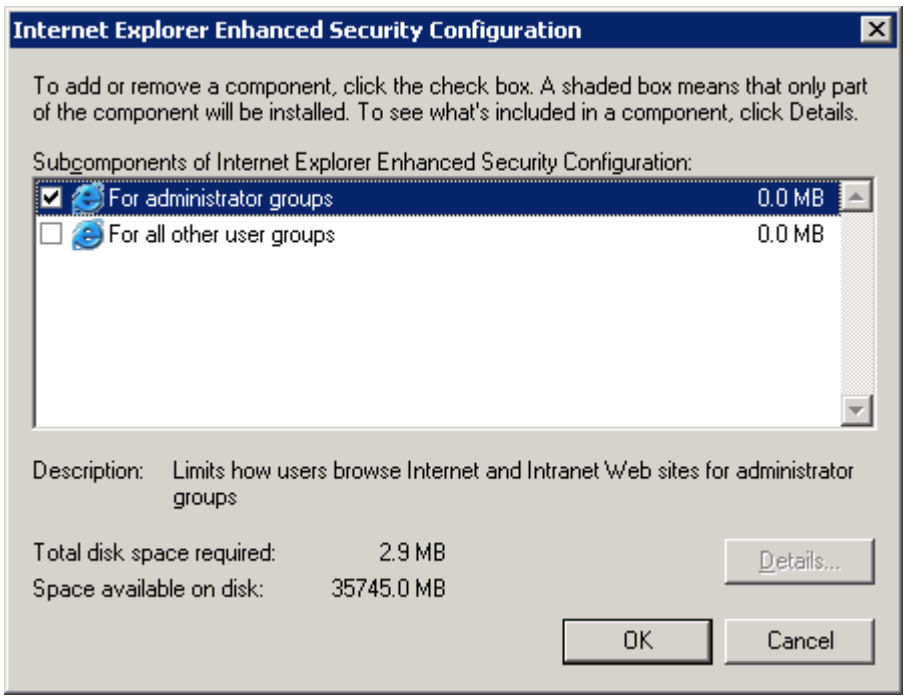
Независимо от разрешения или запрещения Internet Explorer Enhanced Security Configuration, группам Limited Users и Restricted Users запрещается инсталлировать на терминальный сервер элементы ActiveX. Администратор должен вручную инсталлировать необходимые компоненты на сервере.

Чтобы вручную разрешить или запретить Internet Explorer Enhanced Security Configuration, используйте Add/Remove Programs в панели управления:



Если вы хотите разрешить Internet Explorer Enhanced Security Configuration для всех пользователей, отметьте соответствующую опцию. Чтобы указать группы, к которым будет

применяться Internet Explorer Enhanced Security Configuration, щелкните Details. В появившемся окне вы можете применить расширенную безопасность к администраторам и прочим группам. На терминальном сервере лучше всего разрешить для администраторов и запретить для остальных групп.



Изменения, вносимые Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration меняет настройки зоны для IE, повышая безопасность:

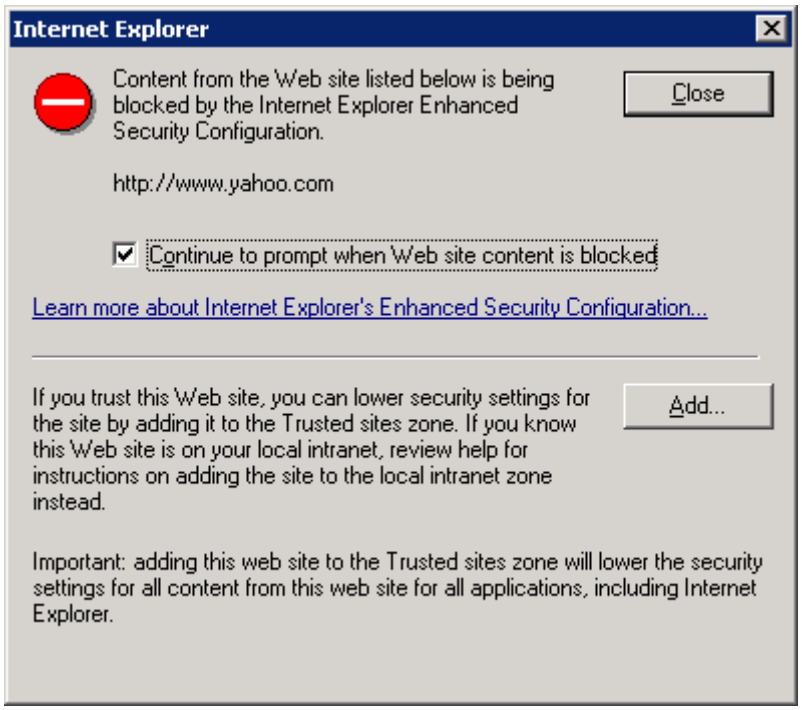
Зона	Уровень по умолчанию	Уровень, устанавливаемый Internet Explorer Enhanced Security Configuration
Internet Zone	Medium	High
Local Intranet Zone	Medium Low	Medium Low
Trusted Sites Zone	Low	Medium
Restricted Sites Zone	High	High

Помимо изменения уровня безопасности зон, Internet Explorer Enhanced Security Configuration меняет зону для всех веб-сайтов интранет. По умолчнию все сайты интранет (определяемые вашим суффиксом DNS), находятся в локальной зоне интранет (Local Intranet Zone). При включенном Internet Explorer Enhanced Security Configuration, сайты интранет помещаются в зону Интернет (Internet Zone) и обрабатываются с уровнем безопасности High, если вы вручную не добавили их в зону Local Intranet Zone. Единственные сайты в локальной зоне Local Intranet Zone при использовании Internet Explorer Enhanced Security Configuration - это локальные сайты (http://localhost, https://localhost, hcp://system). Локальные сайты должны находиться в локальной зоне интранет для правильной работы различных утилит. Internet Explorer Enhanced Security Configuration также меняет расширенные свойства:

Свойство	Параметр	Новое значение	Результат
Browsing	Вывод диалога конфигурации расширенной безопасности	On	Выводит окно с предупреждением, что сайт интернет пытается использовать скрипт или ActiveX.

Browsing	Enable Browser Extensions	Off	Запрет всех особенностей, которые вы инсталлировали для использования с IE и которые созданы компаниями, отличными от Microsoft.
Browsing	Enable Install On Demand (Internet Explorer)	Off	Запрет установки компонентов IE, если это запрашивается веб-страницей.
Browsing	Enable Install On Demand (Other)	Off	Запрет установки компонентов, если это запрашивается веб-страницей.
Microsoft VM	JIT compiler for virtual machine enabled (requires restart)	Off	Запрет компилятора Microsoft VM.
Multimedia	Don't display online content in the media bar	On	Запрет воспроизведения содержимого в полосе IE.
Multimedia	Play sounds in Web pages	Off	Запрет музыки и прочих звуков
Multimedia	Play animations in Web pages	Off	Запрет анимации
Multimedia	Play videos in Web pages	Off	Запрет видеоклипов
Security	Check for server certificate revocation (requires restart)	On	Автоматически проверяет - не аннулирован ли сертификат веб-сайта перед тем, как принять сертификат.
Security	Check for signatures on downloaded programs	On	Автоматически проверяет и отображает идентичность загружаемых программ.
Security	Do not save encrypted pages to disk	On	Запрет сохранения ащищенной информации в папке Temporary Internet Files.
Security	Empty Temporary Internet Files folder when browser is closed	On	Автоматическая очистка папки Temporary Internet Files при закрытии браузера.

Браузинг может быть чрезмерно ограничен, если вы примените Internet Explorer Enhanced Security Configuration. Если вы используете инструменты на основе Web, или Web-станицы с активным содержимым для системного администрирования, вам следует добавить эти сайты либо в зону Local Intranet Zone, либо в зону Trusted Sites Zone. Для облегчения изменения зон, Microsoft добавила в IE в меню File элемент *Add this site to…* (если разрешен Internet Explorer Enhanced Security Configuration). Тогда если вам попадется веб-страница с активным содержимым, то появится окно с предупреждением и кнопкой, позволяющей добавить сайт в список доверенных сайтов.



Управление разрешенными элементами ActiveX

Независимо от Internet Explorer Enhanced Security Configuration, группам Limited Users и Restricted Users запрещена установка любых элементов ActiveX и другого активного кода на терминальном сервере - члены этих групп просто не имеют прав записи в каталоги, где хранятся активные элементы.

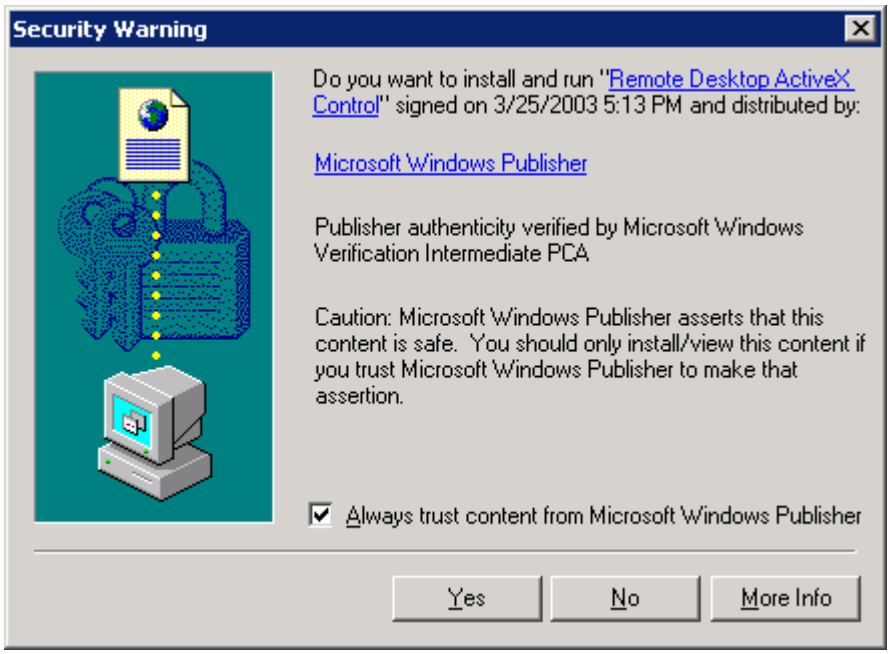
Однако, иногда необходимо разрешить пользователям доступ к веб-страницам, использующих активный код. Вам, как администратору, необходимо управлять такими элементами. Вы можете делать это разными способами. Для ручной инсталляции элементов для пользователей:

1. Зарегистрируйтесь на терминальном сервере под администратором и откройте в IE веб-страницу с активным содержимым.

2. Если разрешен Internet Explorer Enhanced Security Configuration, вы получите предупреждение. Щелкните *Add…* для добавления сайта в список доверенных сайтов, либо выберите из меню File пункт *Add this site to…* для добавления сайта в локальную зону интранет

3. Появится еще одно окно, предлагающее установить активный элемент; выберите опцию *Always trust…* и щелкните OK.

4. Элемент теперь установлен для пользователей терминального сервера.



При администрировании большого числа терминальных серверов вам вряд ли захочется инсталлировать элементы на каждом сервере. Для автоматизации этого процесса вы можете либо включить элементы в основной образ (если используете клонирование и Sysprep), или можете перехватить файлы и упаковать их в пакеты MSI, а затем использовать групповые политики для инсталлции их на терминальных серверах.

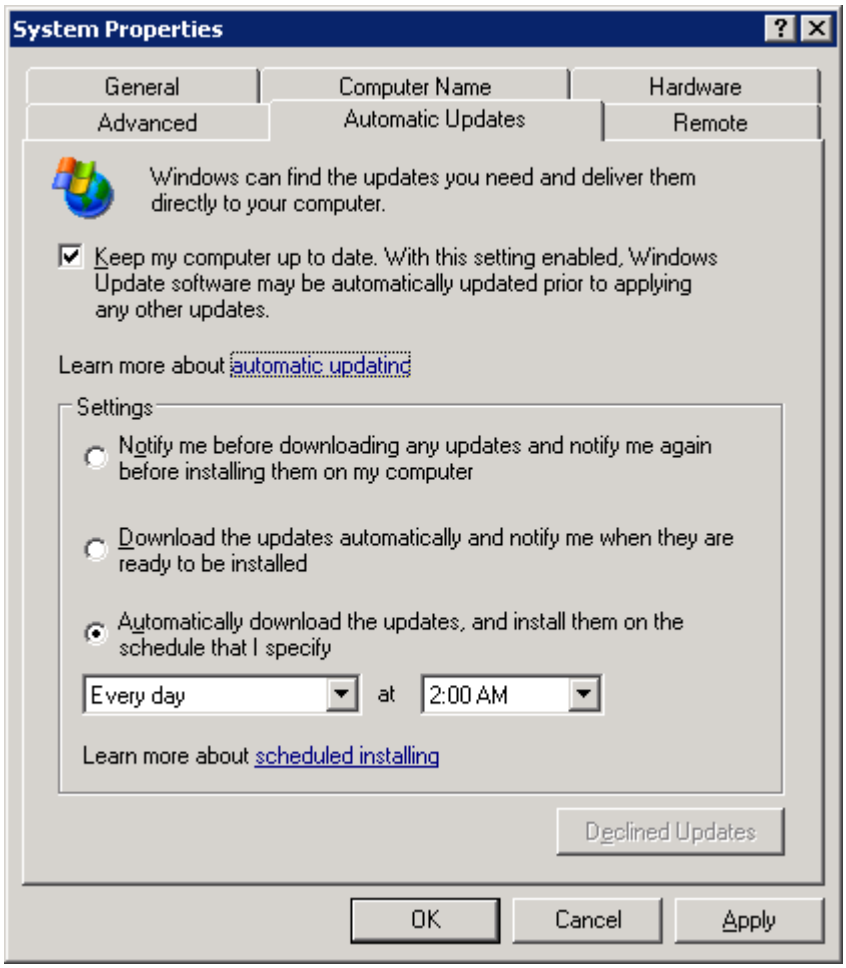
Internet Explorer Enhanced Security Configuration применяется только к IE. Если вы используете другие браузеры интернет, вам необходимо применять другую модель безопасности.

Реализация Windows Automatic Updates

Internet Explorer Enhanced Security Configuration может защитить вас от вредного кода, который может быть найден на веб-страницах. Microsoft периодически выпускает заплаты и обновления, предназначенные для закрытия брешей в безопасности, но за инсталляцию этих обновлений отвечаете вы.

С выходом W2K3 и Windows XP, Microsoft включил клиента автоматического обновления (Windows Automatic Updates). WS2K3 также включает в себя эту службу. С помощью Windows Automatic Updates вы можете настроить серверы и рабочие станции так, чтобы они загружали и инсталлировали любые критические обновления. Automatic Updates Client весьма разносторонний и может быть настроен для любых ситуаций.

Вы можете настроить автоматическое обновление вручную или при помощи групповых политик. Для ручной настройки откройте в панели управления апплет System и выберите вкладку *Automatic Updates*:



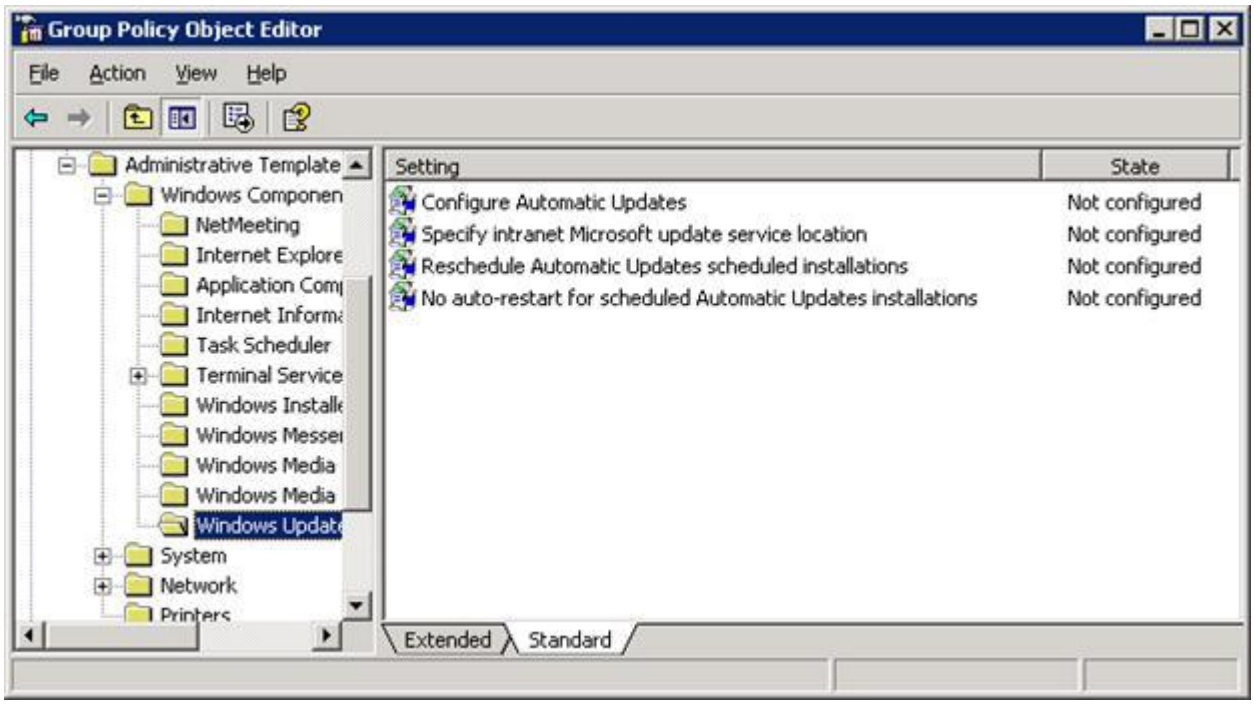
На этой вкладке вы можете разрешить или запретить автоматическое обновление, а также настроить режим работы клиента. Доступные режимы:

- *Notify before downloading* (Уведомить перед загрузкой) —Клиент регулярно проверяет наличие новых обновлений. Если таковое найдено, клиент помещает иконку в панель задач при регистрации на сервере администратора. Администратор щелкает на этой иконке, загружает и инсталлирует обновление.

- *Automatically download but notify before installing* (Автоматически загружать и предупреждать перед установкой) —Клиент регулярно проверяет наличие новых критических обновлений. Если есть обновление, клиент автоматически загружает его, а затем помещает иконку в панель задач при регистрации на сервере администратора. Администратор щелкает на этой иконке и инсталлирует обновление.

- *Automatically download and install at a specific time* (Автоматически загружать и устанавливать в указанное время) —Клиент регулярно проверяет наличие новых обновлений. Если есть обновление, клиент автоматически загружает его, но инсталлирует в укаазнное время.

Вы также можете настроить автоматическое обновление при помощи групповых политик:



Настройка *Configure Automatic Updates* определяет режим и расписание. Она предлагает те же опции, что и апплет панели управления.

Следующая настройка, *Specify intranet Microsoft update service location*, перенаправляет клиента на внутренний сервер Software Update Services (SUS)

Reschedule Automatic Updates scheduled installations определяет, как долго после загрузки нужно ждать до запуска инсталлции обновлений, если компьютер в назначенное время был выключен. Это полезно для рабочих станций, но не обязательно для серверов.

Наконец, *No auto-restart for scheduled Automatic Updates installations* позавляет перезагрузку. Эта настройка полезна, если у вас работает скрипт автоматической перезагрузки и вы не хотите перезагржать сервер дважды.

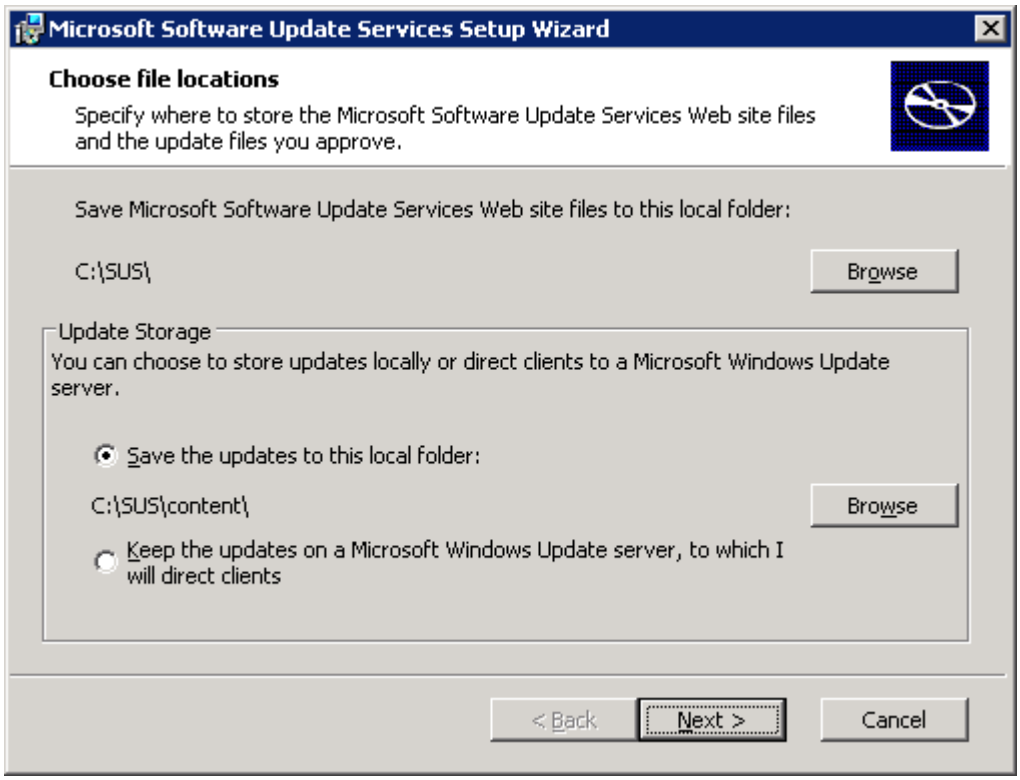
При настройке Automatic Updates вы должны учитывать некоторые факторы. Если ваши серверы используются только в рабочие часы, расписание инсталляции обновлений настроить несложно. Однако, если серверы используются круглосуточно, составьте график обновлений так, чтобы все серверы не перезагружались одновременно.

Использование SUS

В больших или критических средах вы можете захотеть выбирать, какие обновления необходимы вы вашей среде, или иметь возможность проверить обновления на тестовом сервере до установки его на рабочий сервер. Для этого Microsoft предлагает SUS.

SUS устанавливается на Win2K IIS или WS2K3 Application Server и заменяет собой сайт Microsoft Automatic Updates. Затем вы используете GPO, чтобы перенаправить клиента Automatic Updates на внутренний сервер SUS. Клиент тогда загружает обновления с сервера SUS, а не с сайта Microsoft.

Для установки SUS загрузите инсталлятор с сайта Microsoft (http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp). Инсталляция по умолчанию размещает исходные файлы в каталоге `C:\sus\content` и требует от вас вручную санкционировать новые версии ранее санкционированных обновлений до того, как клиенты смогут их загрузить и инсталлировать. Вы можете изменить эти опции либо после инсталляции, либо выбрав заказную инсталляцию в мастере Windows Installer:

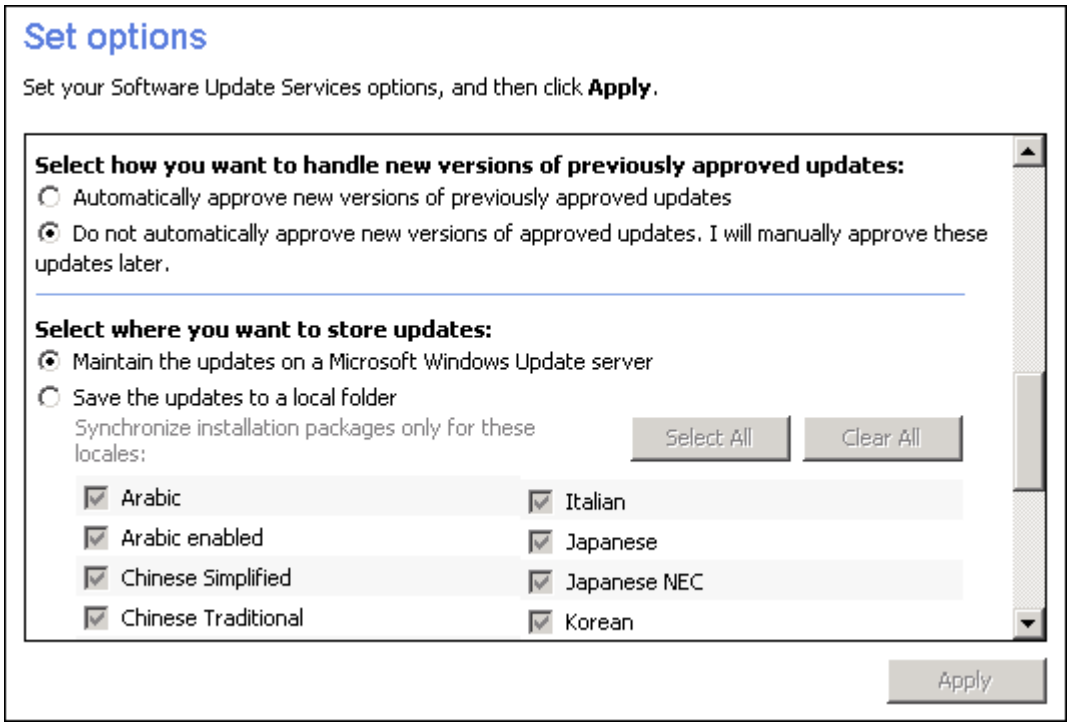


Если на сервере приложений мало свободного места на диске и терминальный сервер имеет выход в Интернет, вы можете оставить опцию хранить исходные файлы обновлений на сервере Microsoft. Вы оставляете за собой возможность выборочно потверждать и проверять обновления, но не будете иметь локальные копии исходных файлов.

Иногда Microsoft выпускает обновленные версии ранее выпущенных заплат. SUS позволяет вам считать обновленные версии новыми версиями (это полезно, если вы тестируете обновления перед установкой их в рабочей среде) или автоматически санкционировать новую версию, если уже установили оригинальную.

После установки SUS, вы можете настроить и управлять службой посредством веб-интерфейса http://localhost/susadmin или удаленно через http://<servername>/susadmin. В нем вы можете настроить прокси-сервер (если он нужен для доступа к серверу Microsoft), указать имя, которое клиенты будут использовать для доступа к SUS, выбрать синхронизацию обновлений с сервером Microsoft или с другим сервером SUS (полезно, если у вас есть несколько серверов SUS), а также изменить две опции, установленные во время установки.

Если для обновления исходных файлов вы используете локальное хранилище, вы можете выбрать, какие локализованные версии следует загружать. Выберите только те языки, которые поддерживают клиенты, поскольку дополнительные файлы могут потреблять много места на диске и увеличить время синхронизации.



В интерфейсе администрирования SUS вы также можете указать, где инициировать синхронизацию. Во время синхронизации сервер загружает последний каталог обновлений с Microsoft, а также исходные файлы обновлений (если вы выбрали локальное хранение). После выполнения ручной синхронизации и убедившись, что прокси настроен правильно, вы должны создать расписание синхронизации, чтобы ваш сервер SUS всегда содержал последние обновления.

После синхронизации вашего сервера SUS, используйте административный интерфейс для санкционирования новых обновлений.

SUS содержит описание каждого обновления, ссылку на подробности инсталляции, список операционных систем, к которым применяется данное обновление. На экране подробностей имеется гиперссылка на бюллетень Microsoft, в котором содержится дополнительная информация.

Если вы планируете проверить обновления до применения их в рабочей среде, вы можете вручную загрузить их с сайта Windows Update или создать два сервера SUS — один для тестов, а второй для рабочей среды. Санкционируйте обновления сначала на тестовом сервере, а затем, после проверки, санкционируйте их на рабочем сервере.

Чтобы настроить терминальные серверы для вытягивания обновлений с сервера SUS, настройте GPO тем же способом, как для Microsoft Automatic Updates, но используйте *Specify Intranet Microsoft update service location* и укажите там URL вашего сервера SUS.

SUS позволяет вам управлять, какие обновления будут установлены на терминальных серверах. Хотя этот метод дает возможность проверить обновления перед установкой, он также требует ручного санкционирования. Вы должны бдительно следить за появлением бюллетеней безопасности Microsoft или часто проверять свой сервер SUS - не появились ли там новые обновления.

На момент написания этой статьи, клиент Automatic Updates имел один существенный недостаток. Если обновление или пакет обновлений загружены и готовы к инсталляции, клиент не сможет загрузить новые обновления до тех пор, пока не будут инсталлирован первый набор. Поэтому вам следует либо настроить ежедневный график инсталляции, либо еженедельно санкционировать обновления на сервере SUS. Тогда клиент при запросе SUS загружает и инсталлирует все ожидающие обновления.

Развертывание сервис-паков и заплат

Microsoft также выпускает сервис-паки (service packs) и заплаты (hotfixes). Их необходимо тщательно проверять перед установкой в рабочей среде, поскольку сервис-паки содержат очень большое число изменений, и кроме того, есть тестовые заплаты, поддержка которых со стороны Microsoft ограничена.

Использование групповых политик для развертывания пакетов обновлений

Выяснив, что сервис-пак вам подходит, вам необходимо установить его на терминальных серверах. Начиная с Win2K, Microsoft стала выпускать сервис-паки в виде пакетов MSI, чтобы вы могли назначать их с помощью групповых политик. Это экономит время по сравнению с ручной установкой на каждом сервере.

Файл UPDATE.MSI должен использоваться только для развертывания сервис-паков с помощью групповых политик. Никогда не устанавливайте сервис-пак вручную, используя файл MSI — вместо этого используйте файл UPDATE.EXE.

Вы назначаете сервис-пак компьютеру таким же способом, как любой другой компонент программного обеспечения компьютера. Начните с распаковки файлов сервис-пака в сетевую папку, доступную для всех терминальных серверов. Для распаковки запустите исполняемый файл с ключом -X (например, WS2K3SP1.EXE –X). Затем укажите папку, в которую будут распакованы файлы.

Затем, используя Group Policy Management Console измените GPO и назначьте сервис-пак компьютерам. Раскройте Computer Configuration, Software Settings, Software installation. Щелкните правой кнопкой на этом узле, выберите New, Package. Вам предложат указать пакет MSI. Введите путь UNC к файлу UPDATE.MSI в папке, в которой вы распаковали файлы, и щелкните Open.

Вам будет предложено назначить пакет с опциями по умолчанию или открыть окно расширенных настроек. Вы можете выбрать Assigned и щелкнуть OK — для сервис-паков расширеных настроек нет.

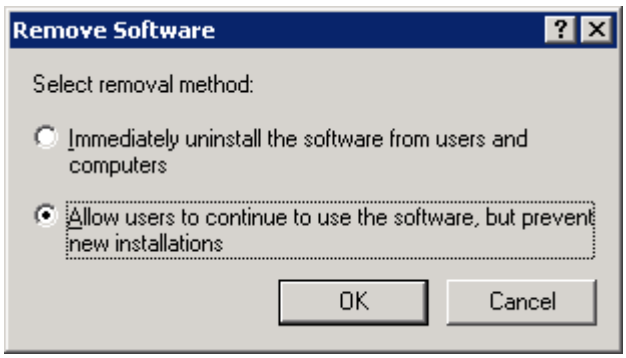
При следующей перезагрузке сервера, получившего GPO, сервис-пак будет установлен.

Microsoft всегда выпускает сервис-паки, включающие в себя обновления, содержавшиеся в предыдущих сервис-паках. Поэтому при установке нового сервера вам нужно установить только

один сервис-пак. Когда вы готовы установить новый сервис-пак, вам необходимо удалить назначения GPO для предыдущих сервис-паков, чтобы оба сервис-пака не устанавливались на новую машину.

Вам не следует деинсталлировать предыдущие сервис-паки перед установкой нового. Просто удалите назначение.

Для удаления назначения предыдущих сервис-паков, используйте Group Policy Management Console для редактирования GPO, испльзованной для назначения. Щелкните правой кнопкой на пакете и выберите All Tasks, Remove. В появившемся диалоге выберите вторую опцию, предотвращение новых инсталляций.



После того, как вы удалили назначение старого сервис-пака, вы можете создать назначение нового. При следующей перезагрузке серверы получат последний сервис-пак.

Развертывание заплат

Windows Automatic Updates и SUS заботятся только о критических обновлениях и обновлениях безопасности. Если вы решили, что вам необходимы другие, некритические обновления, вам необходим способ установить их на ваши серверы.

Для новых серверов наилучшим способом будет интеграция заплат в процесс создания сервера. Если вы используете клонирование или образы RIS, эта задача может быть решена либо ручной установкой фиксов до запуска Sysprep или Ripprep. Если вы создаете серверы с автоматической (unattended) инсталляцией, вы можете добавить их с помощью файла CMDLINES.TXT.

Подробнее об интеграции заплат в автоматическую инсталляцию Windows, см. статью Hotfix Installation and Deployment Guide

Однако, Microsoft не предоставляет ясного способа развернуть заплаты на нескольких существующих серверах. Руководство предлагает единственный способ - инсталляция с сетевого ресурса. Этот процесс подходит для небольших сред, но для крупных ферм вам наверняка захочется его автоматизировать. Следующие предлагаемые способы будут работать не во всех случаях и не являются исчерпывающим списком. Выберите тот способ, который лучше всего подходит для вас.

Использование файла ZAP

Если вам одновременно нужно установить только одну заплату, хорошим выбором будет использование файла ZAP. Файлы ZAP используются для установки программ, оличных от пакетов MSI, с помощью групповых политик. Файлы ZAP - это обычные текстовые файлы, содержащие информацию, необходимую для инсталляции приложения. Пример такого файла:

```
[Application]
; Only FriendlyName and SetupCommand are required,
; everything else is optional.
; FriendlyName is the name of the program that
; will appear in the software installation snap-in
```

```
; and the Add/Remove Programs tool.
; REQUIRED

FriendlyName = "Hotfix Q911001"
; SetupCommand is the command line used to
; Run the program's Setup. If it is a relative
; path, it is assumed to be relative to the
; location of the .zap file.
; Long file name paths need to be quoted. For example:

; SetupCommand = "long folder\setup.exe" /unattend
; or
; SetupCommand = "\\server\share\long _
; folder\setup.exe" /unattend
; REQUIRED
SetupCommand = "Q######_WS2K3_SP1_x86_en.exe" /M
; Version of the program that will appear
; in the software installation snap-in and the
; Add/Remove Programs tool.
; OPTIONAL
DisplayVersion = 1.0
; Version of the program that will appear
; in the software installation snap-in and the
; Add/Remove Programs tool.
; OPTIONAL
Publisher = Microsoft
```

Основной недостаток при использовании файлов ZAP для установки заплат состоит в том, что после установки требуется перезагрузка сервера. Поэтому этот метод не подходит для установки нескольких заплат.

Аргументы командной строки для всех инсталляторов заплат от Microsoft следующие:

/F Принудительное закрытие всех открытых приложений при перезагрузке компьютера заплатой

/N Не делать резервные копии для последующего удаления заплаты

/Z Не перезагружать компьютер по завершении инсталляции

/Q Тихий режим - вмешательства пользователя не требуется

/M Использовать режим автоматической инсталляции

/L Выдать список установленных заплат

Использование скрипта остановки

Поскольку большинство заплат требуют перезагрузки, для их инстлляции можно использовать скрипт остановки (shutdown). Вы не хотите инсталлировать заплату при каждой остановке сервера, поэтому в него необходимо добавить проверу перед вызовом инсталляционной программы. Простейший способ проверки, установлена ли заплата, состоит в запросе реестра. Все заплаты Microsoft регистрируют сами себя в реестре:

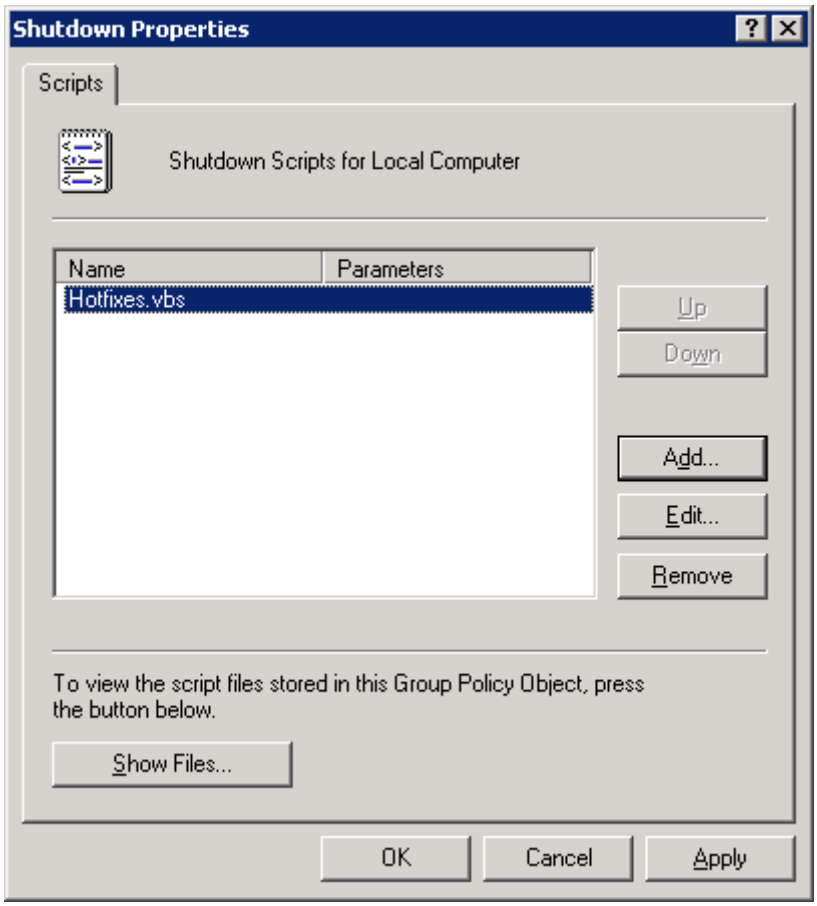
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\WS2K3\<*SPx*>\<*HotfixName*>
  <*SPx*> - сервис-пак, содержащий заплату, а <*HotfixName*> - это статья Microsoft Knowledge Base, в которой описана заплата

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix\<*HotfixName*>
  <*HotfixName*> - это статья Microsoft Knowledge Base, в которой описана заплата

Пример скрипта на Visual Basic:

```
On Error Resume Next
Set WshShell = WScript.CreateObject("WScript.Shell")
WshShell.RegRead("HKLM\SOFTWARE\Microsoft\Updates\WS2K3\SP1\Q819639\Descripti
on")
If Err then
      Hotfix1="Q819639_WS2K3_SP1_x86_en.exe /Z /M"
      WshShell.Exec(Hotfix1)
End If
WshShell.RegRead("HKLM\SOFTWARE\Microsoft\Updates\WS2K3\SP1\KB818529\Descript
ion")
If Err then
      Hotfix2="KB818529_WS2K3_SP1_x86_en.exe /Z /M"
      WshShell.Exec(Hotfix2)
End If
```

Чтобы указать этот скрипт как скрипт останова, используйте Group Policy Management Console для редактирования GPO, применяемого к терминальным серверам. Раскройте Computer Configuration, Windows Settings, Scripts (Startup/Shutdown), в правой панели дважды щелкните Shutdown. Откроется окно совйств скрипта:



Щелкните Show Files и скопируйте ваш файл скрипта и все инсталляционные файлы заплаты в эту папку. Затем используйте кнопку *Add* для настройки скрипта на запуск при остановке системы (shutdown). При каждом выключении или перезагрузке сервером скрипт проинсталлирует необходимые заплаты, отсутствующие в системе.

Хотя заплаты содержат встроенную логику, которая предотвращает их установку на систему с более новым сервис-паком, запретите или измените ваш скрипт после установки нового сервис-пака для уменьшения нагрузки - не нужно тратить время на попытки установки ненужных заплат.

Практика защиты от вирусов

Защита от вирусов - это последняя линия обороны от вредоносного кода. Вы можете создать фильтры в корпоративной почтовой системе, использовать почтового клиента типа Microsoft Outlook 2002, который блокирует все исполняемые прикрепления, установить строгие правила брэндмауэров и прокси-серверов на соединениях с Интернет. Тем не менее, вирусы всегда находят способ проникнуть в вашу систему.

Программы защиты от вирусов работают сканируя индивидуальные файлы и активные процессы в памяти и сравнивают их с базой данных известных сигнатур. Большинство антивирусов защищают от всех трех типов вредоносного кода; однако, защита зависит от антивирусной базы данных. Вы должны постоянно ее обновлять, поэтому выбирайте продукт, предоставляющий метод обновления своей базы данных.

В следующем списке содержатся практические рекомендации по применению и настройке антивирусного ПО:

- Выбирайте продукт, предлагающий обновление своей базы данных вирусов без перезагрузки сервера

- Если ваш терминальный сервер критически важен, выбирайте продукт, который позволяет вытягивать свои обновления с внутреннего источника, давая возможность проверить обновления до установки их на рабочих серверах.

- Многие антивирусы размещают свою иконку на панели задач. Проконсультировавшись с продавцом, уберите иконку из системного трея (обычно удалением из ключа HKEY_LOCAL_MACHINE\Software\Micrrosoft\Windows\CurrentVersion\Run). Это уменьшит нагрузку на сервер, вызванную программой, выполняемой в каждом пользовательском сеансе.

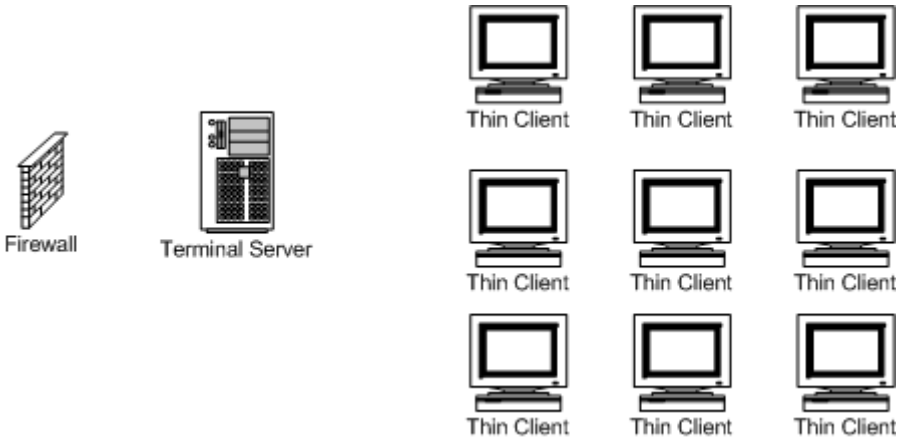
- Помимо сканирования в реальном веремени (сканирование каждого файла при обращении к нему пользователя и процессов в памяти) многие продукты позволяют сканирование по расписанию всех файлов в системе. Настройте расписание так, чтобы сканирование производилось в нерабочие часы.

Все вместе

Как вы видели, есть несколько способов обеспечения безопасности терминальных серверов и защиты их от вирусов. В этом разделе мы рассмотрим два примера того, как реализуются эти способы.

Пример 1: Небольшая среда (театр)

Давид работает администратором терминального сервера в небольшой компании. По вечерам и по выходным он добровольно администрирует и оказывает техническую поддержку местному общественному театру. Чтобы снизить издержки и поддерживать стабильность сети, он потратил деньги из своего гранта для создания терминальной инфраструктуры для театра:



Инфраструктура состоит из 9 тонких клиентов, используемых сотрудниками театра, терминального сервера и персонального брэндмауэра, подключенного к линии DSL. Пользователи подключаются к терминальному серверу и получают в свое распоряжение полный рабочий стол со всеми необходимыми установленными приложениями. Они сохраняют документы в своих папках My Documents на терминальном сервере и имеют доступ к общей папке для общих документов. Эта папка также находится на терминальном сервере. Профили пользователей, общая папка и система резервируются по ночам, в 1 час, на внешний жесткий диск, подключенный к серверу.

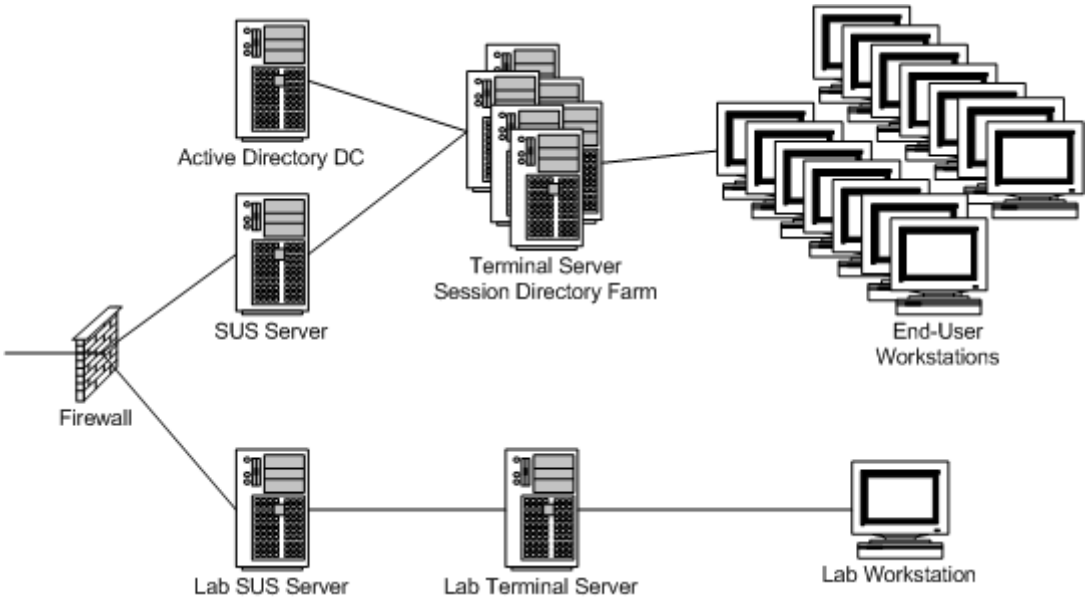
Давид хочет иметь надежную и безопасную сеть, поэтому он применил следующие меры защиты:

- Брэндмауэр настроен на использование NAT и блокирует входящие запросы. Это позволяет персоналу ходить по Web, но предотвращает проникновение червей из Интернет.
- Весь персонал театра на терминальном сервере находится в группе Limited Users. Это предотвращает установку нежелательных компонентов ActiveX, но не применяет к ним Internet Explorer Enhanced Security Configuration, поэтому они могут ходить по Интернет и не получать предупреждающих сообщений.
- Клиент Automatic Updates настроен на автоматическую загрузку и установку критических обновлений от Microsoft по ночам, в 4 часа. Разрешена автоматическая перезагрузка.
- На сервере установлено антивирусное ПО и настроено на загрузку обновлений с сервера производителя каждую ночь в 3 часа.
- Есть только один сервер, поэтому Давид устанавливает сервис-паки и заплаты вручную.

Пример 2: BigBusiness, Inc.

BigBusiness, Inc - средняя компания с числом служащих около 2000. Из-за разнообразия задач каждый пользователь имеет рабочую станцию Windows XP с локально установленными приложениями. Есть два критических приложения, требующих частого обновления и доступа к большим базам пользовательских данных.

Для оптимизации производительности и упрощения развертывания обновлений приложения, персонал службы автоматизации BigBusiness создал ферму каталога сеансов и разместил два при приложения на терминальных серверах. Пользователи обращаются к приложению посредством веб-страницы Remote Desktop Web Connection, которая подключает пользователей к отпределенному приложению, а не к рабочему столу сервера.



Персонал службы автоматизации BigBusiness настроили следующую конфигурацию:

- Корпоративный брэндмауэр блокирует весь входящий траффик на терминальные серверы
- Все пользователи находятся в группе Limited Users, для всех пользователей разрешено Internet Explorer Enhanced Security Configuration. Поскольку пользователи на терминальном сервере не имеют доступа к IE, эту конфигурацию можно разрешить, не влияя на работу пользователей.
- На всех терминальных серверах установлено антивирусное ПО и настроено на загрузку обновлений с локального сайта FTP. Обновления антивируса сначала проверяются в лабораторной среде, а затем выгружаются на FTP.
- Установлены два сервера SUS - один рабочий, а второй - тестовый. Новые критические обновления сначала проверяются на тестовом сервере SUS. Тестовый терминальный сервер настроен на загрузку обновлений с тестового SUS ежедневно в 1 час дня. На следующий день после санкционирования нового обновления производится проверка тестового терминального сервера и приложений. Если обновление не повлияло на сервер или приложения, оно санкционируется на рабочем сервере SUS.
- Рабочие серверы разбиты на группы. Каждый день вечером для каждой группы серверов запускается скрипт, запрещающий новые логины. Ночью клиент Automatic Updates для каждой группы загружает обновления с рабочего сервера SUS и выполняет перезагрузку. В течении недели все серверы получают новые обновления.
- В случае угрозы можно изменить групповые политики так, чтобы клиент Automatic Updates на всех серверах вытянул обновления этой ночью. Поэтому критические обновления могут быть развернуты на серверах в течении одного дня.
- При выходе нового пакета обновлений он тщательно проверяется в тестовой среде. Если проблем не выявлено, он назначается рабочим серверам через GPO. Для каждой группы серверов сервис-пак устанавливается во время автоматической перезагрузки. В течении недели все серверы получают новый сервис-пак.

Прложение A: Клиенты Terminal Services

Remote Desktop Connection for Windows Server 2003

http://www.microsoft.com/downloads/details.aspx?FamilyID=a8255ffc-4b4a-40e7-a706-cde7e9b57e79&DisplayLang=en

Если вам необходим клиент в формате MSI (для распространения через GPO), запустите с комадной строки:

```
msrdpcli.exe /c
```

Remote Desktop Connection Client for Mac

http://www.microsoft.com/downloads/details.aspx?FamilyID=c669fcf7-c868-4d45-95f3-f75ddd969232&DisplayLang=en

Remote Desktop Web Connection

http://www.microsoft.com/downloads/details.aspx?FamilyID=e2ff8fb5-97ff-47bc-bacc-92283b52b310&DisplayLang=en

Terminal Services Client for PocketPC (2000 and 2002)

http://www.microsoft.com/windowsmobile/resources/downloads/pocketpc/tsc.mspx

---

Приложение B: Важные ссылки

Windows Server 2003 Terminal Services Technology Center

http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.mspx

Microsoft TechNet: Terminal Services

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/technologies/terminal/default.asp

Terminal Server Sizing Sample Scripts

http://www.microsoft.com/windows2000/techinfo/administration/terminal/loadscripts.asp

Windows Server 2003 Terminal Server Licensing

http://www.microsoft.com/windowsserver2003/techinfo/overview/termservlic.mspx

Terminal Services Client Access License Activation Web site

https://activate.microsoft.com

Software Update Services (SUS)

http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp

---

Приложение C: Изменения в реестре

Список изменений в реестре из главы 2.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\Explorer]
"LinkResolveIgnoreLinkInfo"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
"IdleWinStationPoolCount"=dword:00000005

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp\UserOverride\Control Panel\Desktop]
"AutoEndTasks"="1"
"CursorBlinkRate"="-1"
"DragFullWindows"="0"
"MenuShowDelay"="10"
"WaitToKillAppTimeout"="20000"
"SmoothScroll"=dword:00000000
"Wallpaper"="(none)"

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp\UserOverride\Control Panel\Desktop\WindowMetrics]
"MinAnimate"="0"
```

Приложение D: Скрипты

USRLOGON.CMD

Ниже приведен измененный USRLOGON.CMD, использующий возможности Win2K отображать домашний каталог в папку пользователя. Удаления выделены ~~ЗАЧЕРКИВАНИЕМ~~, а добавления - **ЖИРНЫМ** шрифтом. Для использования скрипта вы должны установить значение ROOTDRIVE на букву, используемую для домашних каталогов пользователей.

```
@Echo Off
Call "%SystemRoot%\Application Compatibility Scripts\SetPaths.Cmd"
If "%_SETPATHS%" == "FAIL" Goto Done

Rem
Rem This is for those scripts that don't need the RootDrive.
Rem

If Not Exist "%SystemRoot%\System32\Usrlogn1.cmd" Goto cont0
Cd /d "%SystemRoot%\Application Compatibility Scripts\Logon"
Call "%SystemRoot%\System32\Usrlogn1.cmd"
:cont0
Rem
Rem Determine the user's home directory drive letter.  If this isn't
Rem set, exit.
Rem
Cd /d %SystemRoot%\"Application Compatibility Scripts"
Call RootDrv.Cmd
If "A%RootDrive%A" == "AA" End.Cmd
~~Rem~~
~~Rem Map the User's Home Directory to a Drive Letter~~
~~Rem~~
Rem
Rem Subst the user’s profile directory onto the ROOTDRIVE
```

```
Rem if it is not already mapped as the Home Directory
Rem
if /I "%rootdrive%" == "%homedrive%" goto NoSubst

:DoSubst
Net Use %RootDrive% /D >NUL: 2>&1
Subst %RootDrive% "%HomeDrive%%HomePath%"
if ERRORLEVEL 1 goto SubstErr
goto AfterSubst
:SubstErr
Subst %RootDrive% /d >NUL: 2>&1
Subst %RootDrive% "%HomeDrive%%HomePath%"
:AfterSubst

:NoSubst
Rem
Rem Invoke each Application Script.  Application Scripts are automatically
Rem added to UsrLogn2.Cmd when the Installation script is run.
Rem

If Not Exist %SystemRoot%\System32\UsrLogn2.Cmd Goto Cont1
Cd Logon
Call %SystemRoot%\System32\UsrLogn2.Cmd

:Cont1

:Done
```

TSSHUTDN Wrapper

TSSHUTDN.EXE - это утилита, используемая для выключения или перезагрузки терминального сервера. Эта утилита предупреждает пользователей о выключении сервера, двавая им возможность сохранить работу. Затем она запускает для каждого сеанса команду logoff и выключает сервер. К сожалению, эта утилита выключает, а не перезагружает сервер.

Я написал обертку для предотвращения случаных выключений. Скопируйте этот код и сохраните в формате VBS в каталоге SYSTEM32. Для запуска скрипта введите с командной строки имя файла VBS (например, я назвал этот файл TSSHUTDOWN.VBS):

```
' AUTHOR: Greyson Mitchem, The Definitive Guide to WS2K3 TS
' This VBS file is a safety wrapper for the native
' TSSHUTDN.EXE that shuts down or reboots a TS.
' This script will collect the parameters for
' the tsshutdn command.

set oShell=CreateObject("Wscript.Shell")
set oNet=CreateObject("Wscript.Network")
returnkey=msgbox("This script collects the parameters needed
to"&VBCRLF&"correctly shutdown or reboot a Terminal Server."&VBCRLF&"You may
abort the process at any time by hitting CANCEL."&VBCRLF&VBCRLF&"Do you wish
to continue?", VBOKCancel + VBInforamtion, "TS Shutdown")

IF returnkey=VBCancel THEN Wscript.Quit(1)

Server=InputBox("Enter the name of the server you wish to Reboot/Shudown:",
"Server Name", oNet.ComputerName)

if trim(Server)="" then Wscript.Quit(1)
```

```
bRestart=MSGBox("Do you wish to have the server
reboot?"&VBCRLF&VBCRLF&"Clicking NO will PowerDown the system without
rebooting.", VBYesNoCancel + vbQuestion, "Reboot or PowerDown")

Select Case bRestart
     Case vbYes
           sOption="/REBOOT"
     Case vbNo
           sOption="/POWERDOWN"
     Case vbCancel
           Wscript.Quit(1)
End Select

Wait=InputBox("Please enter the number of seconds to give users to finish
working before forcibly logging them off:", "Wait Time", "60")

if trim(Wait)="" then Wscript.Quit(1)

Delay=InputBox("Please enter the number of seconds to wait after all users
have logged off before shutting down the system:", "Wait Time", "30")

if trim(Delay)="" then Wscript.Quit(1)

' All Parameters have been collected.  Now we build the comand line.

ShutdnCMD="tsshutdn.exe "&wait&" /server:"&Server&" "&sOption&"
/Delay:"&Delay&" /v"

oShell.RUN(ShutdnCMD)

Wscript.Quit(0)
```

Если вы хотите создать ссылку, то используйте команду
`wscript %systemroot%\system32\<scriptname.vbs>`

Скрипт перезагрузки

Далее приведен скрипт регулярной перезагрузки сервера. Частота перезагрузки сервера зависит от ваших особенностей - числа пользователей, среды перемещаемых профилей, установленных приложений и т.п. Для правильного запуска скрипта вам нуобходимы два дополнительных файла - Sleep.EXE и текстовый файл yes.txt, содержащий букву Y.

```
REM
REM Sending a message to any currently logged-on users
REM warning them that a maintenance reboot will occur
REM in 10 minutes.
REM
change logon /disable
msg * Please save your work and log off. Maintenance reboot in 10 minutes.

REM Pausing for 5 minutes
sleep 300
REM 5 minute warning
msg * Save your work now and log off. Maintenance reboot in 5 minutes
REM Pausing for 5 minutes
sleep 300
REM 30 second warning
msg * Maintenance reboot in progress. You will be logged off in 30 seconds
REM Pausing for 30 seconds
sleep 30

REM Logging all users off
logoff rdp-tcp < yes.txt

REM Stopping the Print Spooler service and deleting any
REM orphaned files.
net stop spooler
del %systemroot%\system32\spool\printers\*.* /q

REM Rebooting the TS
tsshutdn /REBOOT
```

Приложние E: Командные утилиты Terminal Services

Change User

Для переключения системы между режимами инсталляции и исполнения, используйте следующие команды.
Для переключения терминального сервера в режим инсталляции:

```
CHANGE USER /install
```

Для переключения сервера в режим исполнения:

```
CHANGE USER /execute
```

Change Logon

Разрешает или запрещает новые регистрации на терминальном сервере. Не затрагивает существующих зарегистрированных пользователей.
Для разрешения регистрации:

```
CHANGE LOGON /enable
```

Для запрещения новых регистраций:

```
CHANGE LOGON /disable
```

При перезагрузке сервера регистрация на нем разрешается автоматически, даже если перед выключением она была запрещена.

Query

Выводит список всех терминальных серверов в текущем или указанном домене:

```
QUERY TERMSERVER [servername] [/domain:domain] [/address] [/continue]
```

где:

- *servername* - имя запрашиваемого сервера
- /domain:*domain* - имя домена (по умолчанию текущий домен)
- /address - включить в вывод адреса IP каждого сервера
- /continue - не делать пауз между экранами

Query Session

Выводит список всех текущих сеансов на указанном терминалном сервере

```
QUERY SESSION [sessionname | username | sessionid] [/server:servername]
[/mode] [/flow] [/connect] [/counter]
```

где:

- *sessionname* - имя запрашиваемого сеанса
- *username* - имя пользователя
- *sessionid* - идентификатор сеанса
- /server:*servername* - имя сервера. По умолчанию - сервер, на котором вы зарегистрировались.
- /mode - вывод текущих настроек
- /flow - вывод текщих настроек управления потоком
- /connect - вывод текущих настроек соединения
- /counter - вывод информации о счетчиках для сервера

Query User

Выводит список всех текущих пользователей на терминальном сервере

```
QUERY USER [username | sessionname | sessionid] [/server:servername]
```

где:

- *sessionname* - имя запрашиваемого сеанса
- *username* - имя пользователя
- *sessionid* - идентификатор сеанса

- /server:*servername* - имя сервера. По умолчанию - сервер, на котором вы зарегистрировались.

Вы можете сократить команду QUERY USER до QUSER

Query Process

Выводит список процессов, выполняющихся на терминальном сервере (можно отфильтровать для сеанса).

```
QUERY PROCESS [* | processid | username | sessionname | /id:nn |
 programname] [/server:servername] [/system]
```

где:

- * - все процессы
- *processed* - информаци только о процессе с указаным ID
- *username* - все процессы, выполняемые в контексте указанного пользователя
- *sessionname* - процессы, выполняемые в контексте указанного сеанса
- */ID:nn* - процессы, выполняемые в сеансе с указанным номером ID
- *programname* - процессы, порожденные указанной исполяемой программой
- /server:*servername* - имя запрашиваемого сервера
- /system - список системных процессов

Logoff

Выход пользователя и удаление его сеанса. Без аргументов команда закроет сеанс текущего пользователя.

```
LOGOFF [sessionid | sessionname] [/server:servername] [/v]
```

где:

- *sessionid* - идентификатор закрываемого сеанса
- *sessionname* - имя закрываемого сеанса
- /server:*servername* - севрер, на котором надо завершить сеанс. По умолчанию сервер, к которому вы подключены.
- /v - вывод подробной информации о выполняемых действиях

MSG

Посылает сообщение полюзователю или пользователям на терминальном сервере

```
MSG [username | sessionname | sessionid | @filename | *] [/server:servername]
[/time:seconds] [/v] [/w] message
```

где:

- *username* - имя пользователя, которому надо отправить сообщение
- *sessionname* - имя сеанса, которому надо отправить сообщение
- *sessionid* - ID сеанса
- *@filename* имя текстового файла, содержащего имена пользователей, сеансов или идентификаторов сеансов, которым надо послать сообщение.
- * - отправка сообщения всем пользователям текущего или укаазнного сервера
- /server:*servername* - указывает сервер, к которому подключены получатели сообщения
- /time:*seconds* - число секунд отображения сообщения во всплывающем окне перед тем, как оно закроет само себя
- /v - вывод информации во время отправки сообщения

- /w - окно с сообщением должно ждать, пока пользователь не щелкнет OK
- *message* - текст самого сообщения

Reset Session

Завершение сеанса без предупреждения пользователя и без аккуратного выхода. Может использоваться для завершения зависших сеансов.

```
RESET SESSION [sessionname | sessionid] [/server:servername] [/v]
```

где:

- *sessionname* - имя сеанса
- *sessionid* - ID сеанса
- /server:*servername* - имя сервера, на котором выполняется сеанс
- /v - выводить информацию об осуществляемых действиях

Shadow

Созает теневой сеанс для удаленного упарвления:

```
SHADOW [sessionname | sessionid] [/server:servername] [/v]
```

где:

- *sessionname* - имя сеанса
- *sessionid* - ID сеанса
- /server:*servername* - имя сервера

Terminal Services Profile

Заполняет профиль Terminal Services указанного пользователя. Может использоваться для копирования содержимого профиля Terminal Services от одного пользователя к другому. Эта команда требует привилегий администратра.

```
TSPROF /update [/domian:domainname | /local] /profile:path username

TSPROF /copy [/domian:domainname | /local] [/profile:path] src_user dest_user

TSPROF /q [/domian:domainname | /local] username
```

где:

- /update - заполняет профиль пользователя *domainname**username* с маршрутом *path*
- /copy копирует профиль Terminal Services из *src_user* в *dest_user* и, если указано, обновляет путь к профилю для пользователя *dest_user* маршрутом *path*
- /q вывод маршрута Terminal Services Profile для указанного пользователя

Terminal Server Shutdown

Выключает или перезагружает сервер, давая пользователям возможность сохранить работу и выйти.

```
TSSHUTDN [wait_time] [/server:servername] [/reboot] [/powerdown]
[/delay:logoffdelay] [/v]
```

где:

- *wait_time* - число секунд ожидания после предупреждения пользователя до принудительного закрытия из сеансов (по умолчанию 30 секунд).
- /server:*servername* - имя выключаемого/перезагружаемого сервера
- /reboot - перезагрузить сервер
- /powerdown - выключить сервер после остановки Windows; эту функцию должен поддерживать BIOS
- /delay:*logoffdelay* - число секунд ожидания после выхода всех пользователей до отключения (по умолчанию 30 секунд)
- /v - вывод подробной информации об осуществляемых дейтсвиях

Параметры командной строки клиента Remote Desktop Client

```
MSTSC [<Connection File>][/v:<server[:port]>] [/console]
[[/f[ullscreen]|[/w:<width> /h:<height>]]|[/Edit"connection file"][/Migrate]
```

где:

- *<Connection File>* - файл RDP для соединения
- */v:<server[:port]>* - имя сервера или его адрес IP, а также номер порта
- */console* - подключение к консольному сеансу WS2K3
- */f[ullscreen]* - запуск клиента в полноэкранном режиме
- */w:<width> /h:<height>* - задает высоту и ширину окна соединения
- */edit* - открывает файл RDP для редактирования
- */Migrate* - миграция старых соединений Client Connection Manager из реестра в файлы RDP