ISBN 978-5-901795-13-2 ПРОГРАММНЫЕ СИСТЕМЫ: ТЕОРИЯ И ПРИЛОЖЕНИЯ. Переславль-Залесский, 2008

С. Г. О. Гюлалиев

Организация и настройка терминального доступа в компьютерных классах Университета города Переславля им. А.К. Айламазяна[*)]

Научные руководители: ст. препод. Л. В. Парменова
доц. В. Н. Юмагужина

Аннотация. Данная работа посвящена организации и настройке терминального доступа в Университете города Переславля им. А. К. Айламазяна. Применение терминального доступа позволяет снизить затраты на приобретение оборудования и обслуживание информационных систем, обеспечить высокую степень защищенности данных, надежности системы, удобства пользователей. Терминалы хорошо справляются с большинством задач, выполнямых пользователями на компьютере. При использовании терминального комплекса значительно облегчается работа системного администратора. Нет необходимости в регулярном обходе рабочих мест с целью исправления конфигураций, проверки правильности настроек и работы программ, все это можно делать удаленно, с рабочего места администратора. В статье описаны методы, средства и инструменты для организации терминального доступа.

1. Введение

В настоящее время в федеральных и муниципальных учреждениях, предприятиях различных отраслей, учебных заведениях, где для работы используется более 20 компьютеров, объединенных в локальную сеть, требуется организация и обеспечение максимального уровня безопасности, защиты и централизованного хранения конфиденциальной информации. В частности, требуется:

- подготовить большое количество рабочих мест для работы;
- установить программное обеспечение на каждый из компьютеров в отдельности;
- настроить установленное программное обеспечение;
- постоянно обновлять программное обеспечение на каждом из компьютеров;

[*)] Представлено по тематике: *Компьютерные сети и телекоммуникации, Технологии регистрации и мониторинга.*

- организовать резервное копирование важной информации пользователей с каждого компьютера;
- осуществлять техническую поддержку большого количества рабочих мест.

Решение этих задач традиционным методом не дает нам обеспечения максимального уровня безопасности, защиты конфиденциальной информации, централизованного хранения пользовательских данных. Для того чтобы решить задачи подобного уровня, имеет смысл организовать систему удаленной работы большого числа пользователей на одном центральном компьютере — сервере, а именно, нужно организовать и настроить систему терминального доступа. Применение подобной системы позволяет снизить затраты на приобретение оборудования и обслуживание информационных систем, обеспечить высокую степень защищенности данных, надежности системы, удобства пользователей. Терминалы хорошо справляются с большинством задач, выполняемых пользователями на компьютере (создание и редактирование документов в стандартных офисных программах, электронные таблицы, работа с базами данных и системами автоматизации, работа с Интернетом и электронной почтой, обучающие программы, бухгалтерские приложения и пр.). При использовании терминального комплекса значительно облегчается работа системного администратора. Не нужно регулярно обходить рабочие места с целью исправления конфигураций, проверки правильности настроек и работы программ. Все это можно делать удаленно, с рабочего места администратора. При работе пользователя с сервером терминалов, приложение выполняется на сервере, а по сети передаются только события клавиатуры, мыши и отображаемая информация. Пользователи видят только свои индивидуальные сеансы, которые управляются операционной системой независимо от других сеансов. Настройки пользователя (права, профили и пр.) осуществляются стандартными средствами операционной системы. Администратор имеет возможность удаленно подключиться к терминалу пользователя — это означает, что ему не нужно подходить к пользователю, чтобы помочь в работе с программами. Это удобно, если пользователи находятся далеко от службы поддержки (на другом этаже здания, в другом корпусе университета, в другом городе).

Университет города Переславля состоит из 2 корпусов. В главном корпусе университета имеются 2 компьютерных класса: в одном

компьютерном классе имеется 6 компьютеров, во втором 10 компьютеров, также есть настроенный доменный сервер. Все компьютеры объединены в локальную сеть и зарегистрированы в общем домене TRUBEZH. Во втором корпусе университета имеется один компьютерный класс, состоящий из 6-ти компьютеров и доменный сервер, компьютеры также объединены в локальную сеть и зарегистрированы в домене. В каждом из корпусов функционирует своя подсеть, настроена система персонализированного входа: студенты входят в систему под своим входным именем и паролем. На каждом компьютере в классах установлено программное обеспечение, необходимое для проведения учебных занятий.

2. Постановка задачи

Целью данной дипломной работы является настройка системы терминального доступа в Университете города Переславля, объединение двух корпусов УГП в одну систему, что повлечет за собой:

- снижение времени на настройку компьютеров в компьютерных классах, установку ПО, устранение возникающих проблем на компьютерах, т.е., вся настройка, установка и обновление ПО будет производиться только на одном компьютере — сервере;
- организацию централизованного развертывания программного обеспечения, т.е. все программное обеспечение, используемое в компьютерных классах университета, будет устанавливаться на одном компьютере — сервере;
- контроль за используемым в университете ПО, т.е. установка нового ПО без ведома администраторов невозможна; обеспечение единого централизованного входа пользователей в систему, т.е. студенты Университета будут выполнять работу на одном удаленном сервере, используя терминальную оболочку;
- обеспечение централизованного хранения данных для упрощения резервного копирования;
- объединение двух подсетей в один общий домен, в результате чего пропадет необходимость использования второй базы данных Active Directory, находящейся на сервере во втором корпусе Университета.

Реализация этой цели подразумевает решение следующих задач:

- выбор рабочей станции: анализ системных требований к оперативной памяти, к процессору и к конфигурации дисковой подсистемы;
- сборка серверной рабочей станции;
- подключение необходимых периферийных устройств, проверка работоспособности аппаратной части сервера;
- выбор конфигурации жесткого диска;
- выбор терминальных средств: установка и настройка;
- защита терминального сервера: ограничение прав доменным пользователям при помощи политик безопасности и реестра;
- защита компьютеров в компьютерных классах: создание единого профиля с ограниченными правами, ограничение прав при помощи политик безопасности и реестра;
- объединение подсетей первого и второго корпуса Университета в один общий домен.

3. Организация терминального доступа

3.1. Серверная рабочая станция: требования к аппаратной части терминального сервера

(1) Оперативная память

Для того чтобы определить, какой объем оперативной памяти нужен, был проведен эксперимент с программными продуктами, используемыми студентами в компьютерных классах Университета. Были выбраны приложения, которые требуют наибольшего объёма оперативной памяти. Одна терминальная сессия требует 128 Mb оперативной памяти. Приложения Visual Studio 2005 и MSDN Library 2005 были выбраны для эксперимента, потому что остальные программные приложения, используемые в компьютерных классах, не требуют большого объёма памяти. В Университете имеется три компьютерных класса, всего 25 рабочих мест. Для одной терминальной сессии требуется около 296 Mb оперативной памяти, а для 25 активных пользовательских сессий требуется 7400 Mb оперативной памяти. Еще 512 Mb оперативной памяти нужно для ОС Windows Server 2003, следовательно, общее количество требуемой оперативной памяти 7912 Mb.

Ниже в таблице 1 представлены результаты проведенного эксперимента.

Таблица 1. Результаты проведенного эксперимента

Приложения	**Использование ОЗУ в Мб**
Терминальная сессия	128
Visual Studio 2005	128
MSDN Library 2005	40
Windows Server 2003	512
Сумма при одновременном использовании данных приложений	
Кол-во сессий	
1	296
25	7912

Вывод: в ходе проведения описанного эксперимента было выяснено, что для 25 одновременно работающих сессий, при условии, что будут использоваться приложения указанные в таблице, достаточно 8 Гигабайт оперативной памяти.

(2) Процессор

Терминальные серверы поддерживают несколько одновременно подключенных пользовательских сессий, что означает параллельное выполнение нескольких процессов в системе [1]. Поэтому системные требования к процессору для терминального сервера высоки. Возможность одновременной обработки множества задач значительно увеличивает производительность терминального сервера. Поэтому большинство терминальных серверов являются многопроцессорными. Выбирая процессор, нужно опираться на его производительность при работе с прораммными приложениями.

На сегодняшний день большинство программных приложений являются многопоточным, а для работы с многопоточными приложениями предподчтительно использовать четырехъядерные процессоры. Был выбран четырехъядерный процессор Intel Core 2 Quad Q6600 2.4 Ггц. Этот процессор является младшей моделью четырехъядерных процессоров семейства Core, а его производительность практически равна производительности процессора Intel Core 2 Duo

E6850 3.00 Ггц, который является старшей моделью двухъядерных процессоров семейства Core. Каждый из этих процессоров имеет свои плюсы и минусы.

Преимущества двухъядерного процессора Intel Core 2 Duo E6850 над четырехъядерным Core 2 Quad Q6600:

- на 25% более высокая тактовая частота, позволяющая показывать лучшую производительность в приложениях, не оптимизированных под многопоточность;
- на 46% более низкое тепловыделение, позволяющее применение сравнительно несложных и недорогих систем охлаждения, в том числе и при разгоне.

Преимущества четырехъядерного процессора Intel Core 2 Quad Q6600 над двухъядерным Intel Core 2 Duo E6850:

- вдвое большее число вычислительных ядер, позволяющее добиваться высокого быстродействия при работе с многопоточными приложениями;
- вдвое больший суммарный объём кэш-памяти второго уровня, который также увеличивает быстродействие при работе с многопоточными приложениями.

В связи с тем, что большинство ожидаемых приложений проектируются с учетом оптимизации под многопоточные среды, то процессор Intel Core 2 Quad Q6600 2.4 Ггц является более перспективным процессором с этой точки зрения. Использование данной модели процессора в Университете также предподчтительнее, потому что большинство программных приложений, используемых в компьютерных классах для проведения занятий, являются многопоточными, например программный продукт Visual Studio 2005.

(3) Конфигурация жесткого диска

Кроме использования ресурсов процессора и оперативной памяти, программные приложения используют ресурсы жесткого диска. Для того, чтобы обеспечить высокую скорость чтения данных с диска, было решено использовать технологию RAID. Самым распространенным и оптимальным решением для терминальных серверов является RAID 5-го уровня.

RAID 5-го уровня — это отказоустойчивый массив независимых дисков с распределением контрольных сумм (массив с вращающейся четностью). Массив с вращающейся четностью — это массив, в котором хранение кодов четности осуществляется не на специально выделенном диске,а блоками, располагающимися поочередно на всех дисках. Блоки данных и контрольные суммы циклически записываются на все диски массива, т.е. отсутствует выделенный диск для хранения информации о четности. Также эти контрольные блоки позволяют вычислить пропущенный блок в случае выхода одного из дисков из строя, поэтому RAID 5-го уровня является отказоустойчивым при выходе из строя одного диска [1]. В случае RAID 5 все диски массива имеют одинаковый размер, но один из них невидим для операционной системы. Например, если 3 диска имеют размер 1 Гб, то фактически размер массива составляет 2 Гб, 1 Гб отводится на контрольную информацию. Самый большой недостаток уровней RAID от 2-го до 4-го — это наличие отдельного (физического) диска, хранящего информацию о четности. Операции считывания не требуют обращения к этому диску, и, как следствие, скорость их выполнения достаточно высока, но при каждой операции записи на нем изменяется информация, поэтому схемы RAID 2–4 не позволяют проводить параллельные операции записи. RAID 5 не имеет этого недостатка, так как контрольные суммы записываются на все диски массива, что делает возможным выполнение нескольких операций считывания или записи одновременно. RAID 5 имеет достаточно высокую скорость записи-считывания и малую избыточность, т.е. он экономичен.

3.2. Технология Terminal Services в Windows Server 2003

Windows спроектирована как однопользовательская операционная система, т.е. в один и тот же момент времени в ней может интерактивно работать только один пользователь [1]. Служба Windows Server 2003 Terminal Services ломает эту модель, внедряя между слоями системы и пользователя слой сеанса. Помимо Windows Server 2003 Terminal Services в качестве терминального сервера можно использовать известный на сегодняшний день Citrix Metaframe Server.

Но Citrix Metaframe Server является надстройкой над Microsoft Terminal Services, а не самостоятельным программным продуктом. Для его функционирования нужен сервер с установленной службой Microsoft Terminal Services и всеми необходимыми лицензиями компании Microsoft. Лицензии для Citrix Metaframe Presentation Server преобретаются дополнительно на количество одновременно работающих пользовательских соединений. В связи с тем, что в университете на сервере установлена лицензионная версия ОС Windows Server 2003 и сервер лицензий для терминальных служб активирован, то устанавливать Citrix Metaframe Server и использовать его в качестве терминального сервера нецелесообразно. К тому же Windows Server 2003 Terminal Services обладает всеми необходимыми возможностями и инструментами для того чтобы выполнять роль терминального сервера.

В таблице 2 представлены сравнительные характеристики терминальных серверов Citrix Metaframe Server и Terminal Services.

Таблица 2. Сравнение Citrix Metaframe и Terminal Services

Возможности	**Citrix Metaframe**	**Terminal Services**
Протокол передачи	TCP/IP, IPX/SPX	TCP/IP
Переназначение локальных портов	Есть	Есть
Переназначение локальных дисков	Есть	Есть
Переназначение устройств USB	Есть	Есть
Печать на локальный принтер	Есть	Есть
Печать на сетевой принтер	Есть	Есть
Звук	Есть	Есть
Сжатие	Автоматически	Автоматически
Шифрование	До 128 бит	До 128 Бит
Восстановление разъединенных сеансов	Автоматически	Автоматически
Поддерживаемые ОС клиента	Win32, Unix, Linux, Macintosh	Win32, Linux, Macintosh
Собственный сервер лицензирования	Есть	Есть

3.3. Настройка терминального сервера

После установки операционной системы, на сервере была установлена служба Terminal Services. В настройках службы Terminal Server Licensing активирован сервер лицензий для того, чтобы пользователи могли подключиться к серверу. В настройках Terminal Services Configuration выставлено ограничение до 25 одновременно подключенных сессий, т.е. одновременно к серверу может подключиться максимум 25 пользователей [1].

Для предоставления доступа к серверу доменным пользователям терминальный сервер был зарегистрирован в домене TRUBEZH. После чего на сервере для его защиты были активированы следующие групповые политики безопасности [2]:

- Delete cached copies of roaming profiles — удаляет копию перемещаемого профиля после его выхода из системы;
- Hides the Manage item on the Windows Explorer context menu — скрывает вкладку «Управление в контекстном меню проводника»;
- Remove Task Manager — удаляет «Диспетчер задач»;
- Remove and prevent access to Shutdown command — запрещает доступ к команде «Завершить работу компьютеры»;
- Remove Run menu from Start menu — удаляет меню «Выполнить» из меню «Пуск»;
- Prohibit access to the Control Panel — запрещает доступ к панели управления;

Так же на сервере активирован скрипт, который записывает в журнал событий следующую инмормацию:

- имя пользователя, который за день осуществлял вход в операционную систему и выход из нее;
- имя клиентской рабочей станции, с которой осуществлялся вход и выход;
- дату входа и выхода (число, месяц, год);
- время входа и выхода пользователей.

3.4. Настройка компьютеров в компьютерных классах Университета

(1) Первый корпус Университета

Компьютеры в аудиториях уже зарегистрированы в домене TRUBEZH, все сетевые настройки выдаются DHCP-сервером, следовательно возможно подключиться с локальных компьютеров к терминальному серверу. Для того, чтобы приблизить компьютеры в аудиториях к тонким терминальным клиентам, был создан единый профиль с ограниченными правами доступа. При помощи ключей реестра запрещен доступ локальным ресурсам компьютеров, удалены все ярлыки с рабочего стола [3]. При помощи политики Logon locally запрещен доступ доменным пользователям к компьютерам. На рабочий стол скопирован настроенный клиент Remote Desktop при помощи которого можно подключиться к терминальному серверу.

(2) Второй корпус Университета

Компьютеры в аудитории №6 не были зарегистрированые в домене TRUBEZH. Для того, чтобы компьютеры получили все необходимые доменные настройки, было сделано следующее:

- на доменном контроллере в настройках DHCP-сервера была создана специальная зона для подсети второго корпуса со всеми необходимыми настройками [4];
- серверу, находящийся в втором корпусе и выполняющий роль второго контроллера домена, была дана роль сетевого агента DHCP (DHCP Relay Agent), в настройках DHCP Relay Agent выставлено перенаправление запросов на DHCP-сервер, находящийся в первом корпусе Университета [4];
- помимо настроек DHCP Relay Agent, в сетевых настройках сервера выставлен DNS сервер доменного котроллера, находящегося в первом корпусе Университета;

После выполенных настроек, компьютеры в аудитории №6 были зарегистрированы в домене TRUBEZH, сетевые настройки также были выданы DHCP-сервером.

4. Результаты

В рамках данной работы было сделано следующее:

- проведен анализ системных требований к оперативной памяти, к процессору и конфигурации дисковой подсистемы, по результатам анализа выбрана серверная рабочая станция;

- произведена сборка серверной рабочей станции;
- подключены необходимые периферийные устройства;
- произведена проверка работоспособности аппаратной части сервера;
- выбрана, установлена и настроена операционная система на сервере;
- для непосредственной работы терминального сервера установлены и настроены терминальные службы;
- для безопасности сервера настроены необходимые групповые политики безопасности для доменных пользователей;
- на сервере установленно необходимое програмнное обеспечение для проведения практических занятий;
- компьютеры в компьютерных классах приближены к тонким терминальным клиентам, а именно, создан специальный пользователь с ограниченными правами доступа, права ограничены при помощи локальных политик безопасности и реестра;
- подсети первого и второго корпусов объединены в один общий домен;
- для ведения журнала событий на терминальном сервере были созданы два скрипта: первый скрипт записывает информацию в момент входа в операционную систему, а второй в момент выхода из операционной системы соотвественно.

Список литературы

[1] Грейсон М. Полное руководство по терминальным службам Windows Server 2003: Компьютерная литераруа, 2004. — 122 с.

[2] Зубанов Ф. Active Directory: подход профессионала. — 2-е изд., испр. — М.: Издательско-торговый дом «Русская редакция», 2006. — 544 с.

[3] Климов А., Чеботырев И. Реестр Windows, 2004. — 800 с.

[4] Реймер С., Малкер М. Active Directory для Windows Server 2003. — М.: Справочник администратора, 2004. — 512 с.

S. G. O. Gyulaliev. *Organizing and tuning of terminal access at the University of Pereslavl named after A. K. Aylamazyan* // Proceedings of Progranm Systems institute scientific-practical conference "Program systems: Theory and applications", devoted to the 15^{th} anniversary of Pereslavl University named A. K. Ailamazyan. — Pereslavl-Zalesskij, 2008. — p. 99 — 110. — ISBN 978-5-901795-13-2 *(in Russian).*

Abstract. The paper considers organizing and tuning terminal access at the University of Pereslavl named after A. K. Aylamazyan. Terminal access reduces expenses for purchasing hardware and provides high level of data security, sytem reliability and users comfort. Resources and tools of the terminal access are described.

Перевод проверен: Н. А. Прохорова