Министерство образования и науки Российской Федерации

УНИВЕРСИТЕТ ИТМО

УТВЕРЖДАЮ

Старший преподаватель
_____ А. Д. Береснев
«_____» _____ 2014 г.

ОТЧЕТ
О ВЫПОЛНЕНИИ ЛАБОРАТОРНОЙ РАБОТЫ
по курсу «Администрирование в информационных системах»

по теме:
Основы работы с Active Directory

Санкт-Петербург
2014

СПИСОК ИСПОЛНИТЕЛЕЙ

Студент гр. 3512 _____ В. А. Петухов
(подпись, дата)

Студент гр. 3512 _____ В. А. Кукин
(подпись, дата)

Студент гр. 3512 _____ А. А. Чехомов
(подпись, дата)

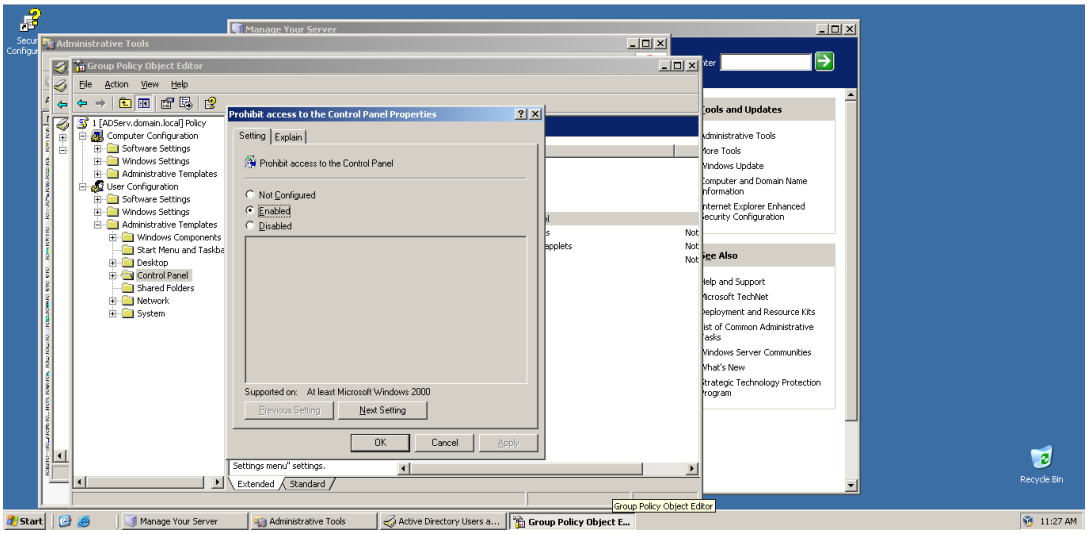
Скрипт из задания 20

```
set name=%1
set passwd=%2
set unit=%3
if %unit%== "M" set unit= ouManagers else set unit= ouSellers
if %unit%== "M" set group= gManagers else set group= gSellers
cd /d C:\UsersHome\
mkdir %name%
dsadd user CN=%group%,DC=domain,DC=local -memberof
CN=%group%,OU=%unit%,DC=domain,DC=local -pwd %passwd% -hmdrv W: -hmdir
\\ADServ\%name% -profile \\ADServ\%name%\_profile -mustchpwd yes
net share %name%=C:\UsersHome\%name%$ /grant:%name%,full
xcacls C:\UserHome\%name% /T /G %name%:f
```

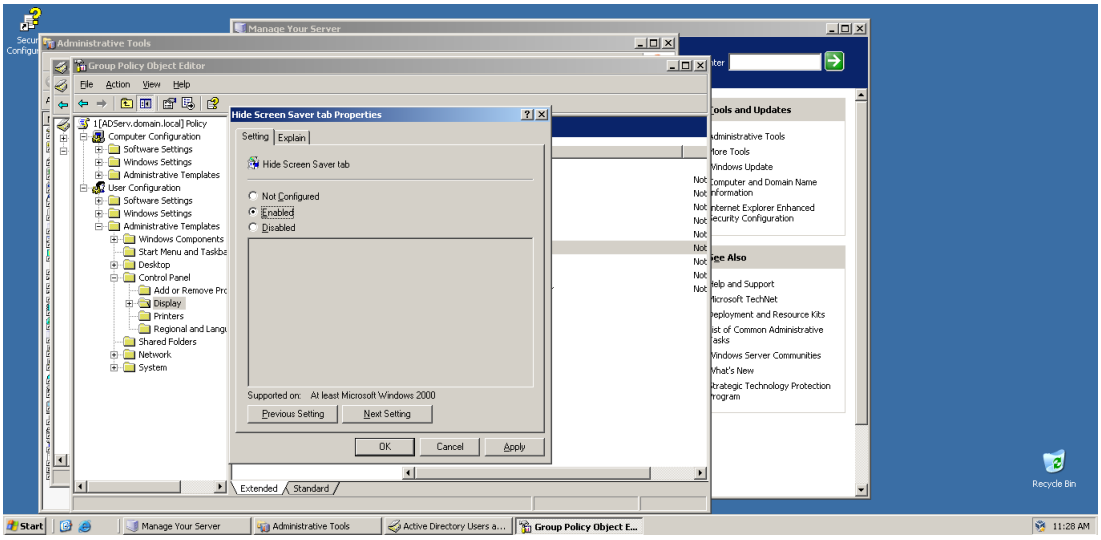
Перечень установленных групповых политик

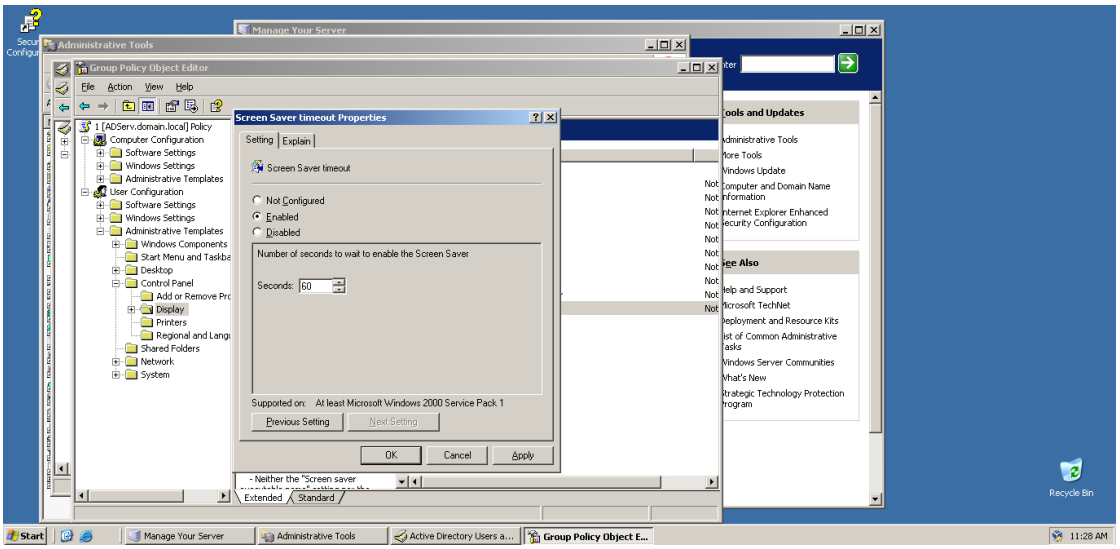
Создать групповую политику для контейнера Sellers, с помощью которой будет:

- Запрещен доступ к Панели управления

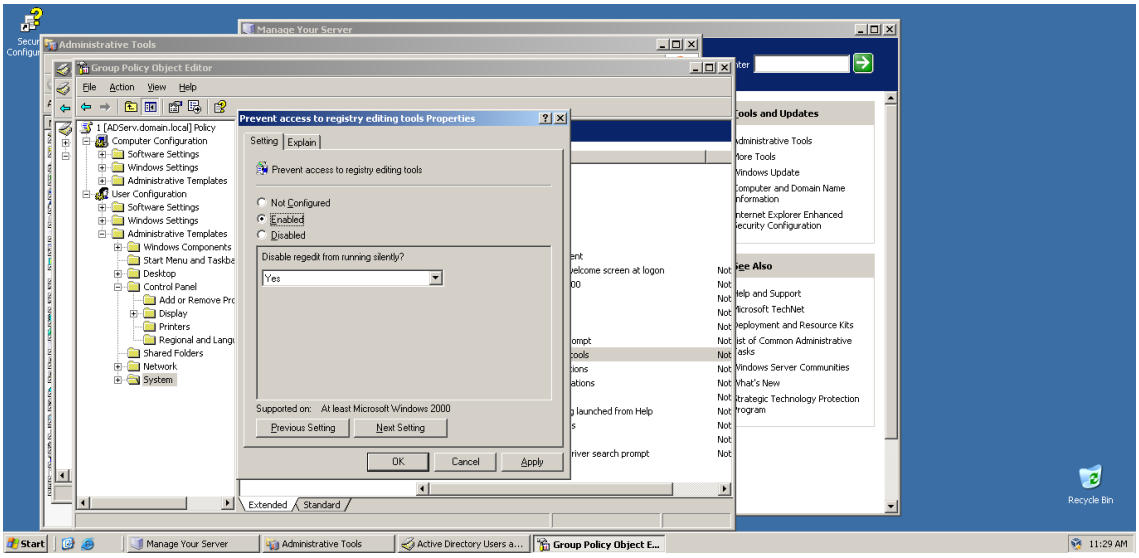


- Установлена блокировка экрана при периоде неактивности 1 минута, с отключением возможности менять этот параметр

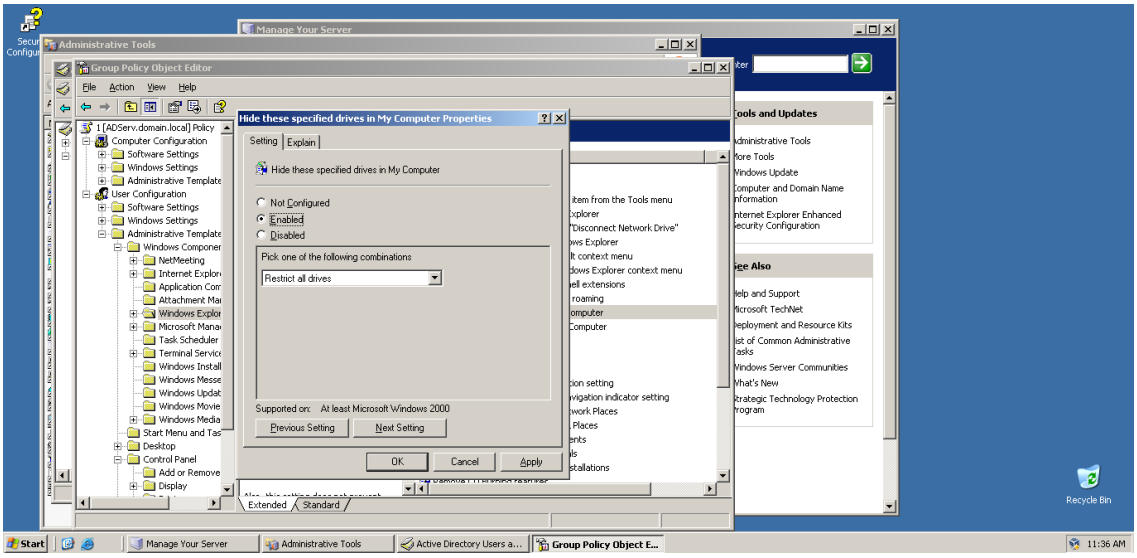




- Запретить пользователю редактировать реестр

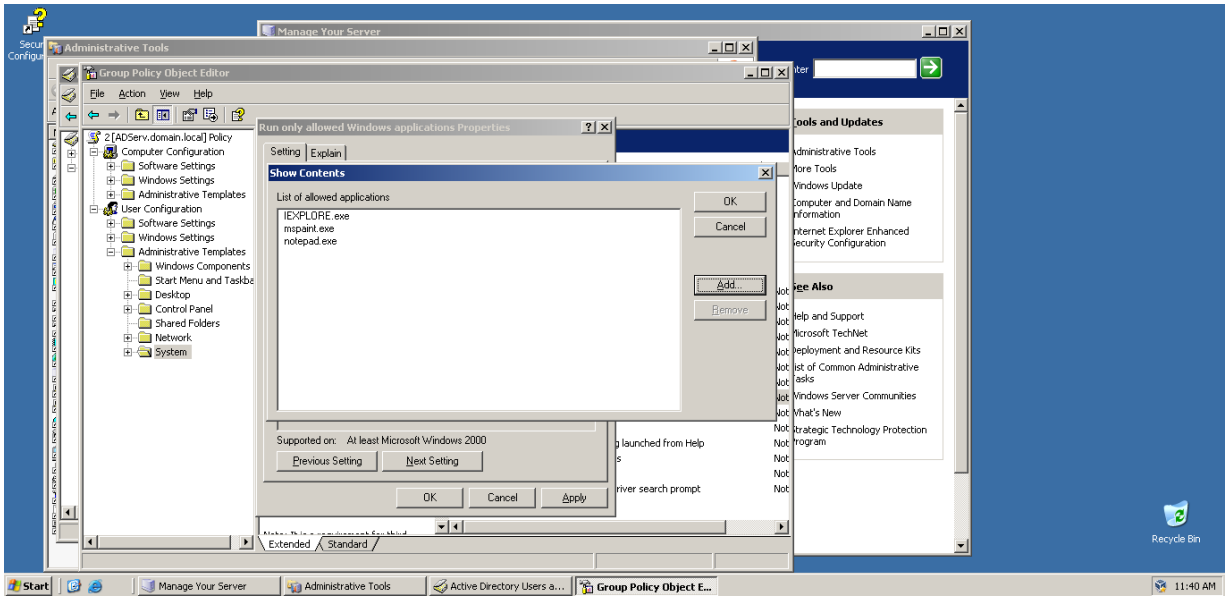


- Скрыть в проводнике диск C:



Создать групповую политику в контейнере Managers, которая будет определять приложения, которые может запускать пользователь:

- Paint;
- IE;
- Notepad.



Создать контейнер для объектов – компьютеров и создать в нем групповую политику, которая:

- отключает сбор и передачу в Microsoft сообщений об ошибках

Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> System Services -> Error reporting service = Disabled

- отключит локальные учетные записи Администратор (Administrator)

Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> Accounts: Administrator account status = Disabled

- запретит пользователю пользоваться механизмом Offline Files

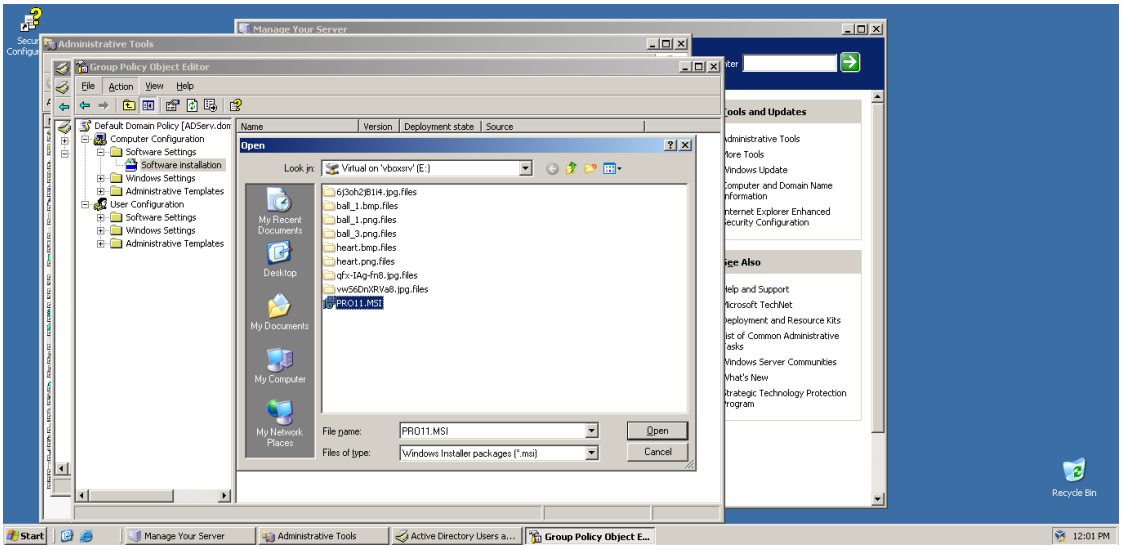
Computer Configuration -> Administrative Templates -> Network -> Offline Files -> Allow or Disallow use of the Offline Files feature = Disabled

- установит на клиентских компьютерах для всех файловых объектов на диске C:\ следующий ACL (Администраторы, Система – полный доступ, Пользователи домена – чтение, просмотр каталогов, выполнение файлов)

Computer Configuration -> Windows Settings -> File System -> Add file... -> C:\

Создайте отдельную групповую политику с помощью которой разверните на клиентском компьютере программу 7-zip (инсталлятор MSI).

Computer configuration -> Software settings -> Software installation -> New... -> Package



Путь к файлу: \\ADServ\windows\sysvol

Ответы на вопросы

1. Раскройте смысл терминов: дерево доменов, лес и схема Active Directory?

   Домен — минимальная структурная единица организации Active Directory

   Дерево доменов — иерархическая система доменов, имеющая единый корень (корневой домен)

   Лес доменов — множество деревьев доменов, находящихся в различных формах доверительных отношений

   Схема Active Directory — это оснастка консоли управления (MMC), которая используется для просмотра схемы доменных служб Active Directory (AD DS) и управления ею.

   Схема содержит формальные определения каждого класса объектов, которые могут быть созданы в лесу Active Directory. Кроме того, схема содержит формальные определения каждого атрибута, который может или должен существовать в объекте Active Directory.

2. Перечислите роли контроллера домена и их назначение.

   Контроллер домена — сервер, хранящий *каталог* и обслуживающий запросы пользователей к каталогу. Помимо хранения данных контроллер домена может выступать в качестве одной из FSMO-ролей.

FSMO — типы выполняемых контроллерами домена Active Directory операций, требующие обязательной уникальности сервера, выполняющего данные операции.

В зависимости от типа операции уникальность FSMO подразумевается в пределах или леса доменов, или домена.

Различные типы FSMO выполняются одним или несколькими контроллерами домена. Выполнение FSMO сервером называют ролью сервера.

Название	Оригинальное название	Пределы уникальности	Описание
Владелец схемы	Schema Master	Лес доменов	Отвечает за внесение изменений в схему Active Directory. Эта роль необходима для предотвращения противоречивых изменений с двух серверов.
Владелец доменных имён	Domain Naming Master	Лес доменов	Отвечает за состав леса, принимает и удаляет домены.
Владелец относительных идентификаторов	Relative ID Master	Домен	Выдает и удаляет относительные идентификаторы любых объектов (пользователей, компьютеров, принтеров) в домене.
Эмулятор основного контроллера домена	Primary Domain Controller Emulator (PDC Emulator)	Домен	Эмулирует основной контроллер домена для приложений, работающих с возможностями домена Windows NT.
Владелец инфраструктуры домена	Infrastructure Master	Домен	Поддерживает идентификаторы удаляемых или перемещаемых объектов на время репликации изменений (с удалением или перемещением) между контроллерами домена.

3. Как с помощью команды DSMOD изменить пароль пользователю?

   dsadd user имя_пользователя -pwd *пароль*
4. Где на контроллере домена хранятся файлы, содержащие групповые политики домена?

«Оболочка» для GPO представляет собой папку, хранящуюся в папке Политик (Policies). По умолчанию она располагается по следующему пути c:\Windows\Sysvol\sysvol\Policies. В папке Policies список папок представлен длинным буквенно-цифровым значением. Это буквенно-цифровое значение представляет собой GUID (Global Unique Identifier) для GPO.

5. Где на контроллере домена хранится Active Directory в виде файлов?

Все данные базы данных службы Active Directory хранятся в отдельном файле ***Ntds.dit*** на контроллере домена. Этот файл данных по умолчанию находится в папке ***%SystemRoot%\NTDS***, расположенной на контроллере домена. В нем хранится вся информация каталога, предназначенная для данного домена, а также данные, являющиеся общими для всех контроллеров домена в данной организации.

Вторая копия файла Ntds.dit находится в папке %SystemRoot%\ System32. Эта версия файла - поставляемая копия (копия, заданная по умолчанию) базы данных каталога, она используется для установки службы Active Directory. Этот файл копируется на сервер во время установки Microsoft Windows Server 2003, чтобы сервер можно было назначать контроллером домена без необходимости обращаться к инсталляционной среде. Во время выполнения мастера инсталляции Active Directory (Dcpromo.exe) файл Ntds.dit копируется из папки System32 в папку NTDS. Затем копия, сохраненная в папке NTDS, становится действующей копией хранилища данных каталога. Если это не первый контроллер домена в домене, то файл будет обновлен из других контроллеров домена через процесс репликации.

6. Какие виды групп в Active Directory существуют?

В Active Directory существуют два типа групп: группы распространения и группы безопасности. Группы распространения могут быть использованы для создания списков рассылки электронной почты, а группы безопасности — для задания разрешений на использование общих ресурсов.

7. В чем отличие групп от контейнеров?

Контейнер аналогичен объекту в том смысле, что он также имеет атрибуты и принадлежит пространству имён, но, в отличие от объекта, контейнер не обозначает ничего конкретного: он может содержать **группу** объектов или другие контейнеры.

8. Что такое авторизация DHCP сервера? Для чего она выполняется?

Авторизация DHCP-сервера является обязательным условием его нормального функционирования. В каталоге Active Directory должен быть создан объект, соответствующий установленному DHCP-серверу. Только после этого клиенты смогут работать с данным сервером. Все обязанности по осуществлению контроля над авторизацией DHCP-серверов возложены непосредственно на сами DHCP-серверы

Авторизация DHCP-сервера добавляет и использует классы объектов, являющиеся частью базовой схемы каталога, что обеспечивает следующие усовершенствования:

доступность списка IP-адресов компьютеров, авторизуемых для работы в сети в качестве DHCP-серверов;

обнаружение неавторизованных DHCP-серверов и предотвращение их запуска или работы в сети.