Санкт-Петербургский национальный исследовательский университет
Информационных технологий механики и оптики

Факультет информационных технологий и программирования

Лабораторная работа №7
По предмету Администрирование в информационных системах
«Active Directory»

Исполнитель: Трофимов В.А.
Руководитель: Береснев А.Д.
Группа: 3511

Санкт-Петербург
2014

Цель работы

Получить базовые навыки развертывания службы каталогов Active Directory на основе Windows, управления объектами AD, их правами и групповыми политиками.

Ответы на вопросы

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

Домен – область, объединяющая группу компьютеров (и других объектов), которые при работе в сети, при поиске доступных ресурсов, ориентируется на единый справочник (Active Directory). Данный справочник (Active Directory) распространяет на эти компьютеры свои политики безопасности.

Несколько доменов, которые используют общее пространство имен Active Directory, создают дерево доменов Active Directory.

Несколько деревьев доменов, которые принадлежат одному предприятию, создают лес.

Схема определяет, какие типы объектов могут существовать в AD. Сама схема состоит из двух типов объектов: объекты классов схемы и объекты атрибутов схемы. Один объект класса схемы определяет один тип объекта Active Directory (например, объект «Пользователь»), а один объект атрибута схемы определяет атрибут, который объект может иметь.

Перечислите роли контроллера домена и их назначение

- Владелец схемы (Schema Master). Контроллер домена, осуществляющий изменения в схеме каталога. Существование только одного владельца (хозяина) схемы в пределах леса доменов исключает возможность конфликтов, связанных с ее изменением. Отказ владельца схемы приводит к тому, что выполнение операции расширения схемы станет невозможным.
- Владелец доменных имен (Domain Naming Master). Контроллер домена, отслеживающий изменения в структуре леса доменов. Любое изменение пространства имен доменов Active Directory (добавление, удаление, а также переименование доменов) осуществляется исполнителем данной роли. Тем самым гарантируется целостность пространства имен и уникальность его компонентов. Отказ исполнителя этой роли приводит к тому, что любое изменение пространства имен каталога станет невозможным.

- Владелец идентификаторов (Relative ID Master). Контроллер домена, осуществляющий генерацию идентификаторов (глобальные идентификаторы, идентификаторы безопасности и т. п.). От идентификатора в первую очередь требуется уникальность. Самый простой способ гарантировать уникальность генерируемых идентификаторов — возложить обязанность исполнителя данной роли на один контроллер в домене. Отказ исполнителя данной роли приводит к тому, что создание объектов в домене станет невозможным.
- Эмулятор основного контроллера домена (PDC Emulator). Если домен находится на функциональном уровне Windows 2000 mixed, эмулятор основного контроллера домена (PDC) используется для обеспечения репликации изменений между контроллерами домена Windows NT и Windows 2000/Server 2003. Исполнитель роли фактически эмулирует домен Windows NT. Поскольку в домене Windows NT допустимо наличие только одного основного контроллера, его эмулятор в домене Active Directory также может быть только один. На других функциональных уровнях эмулятор основного домена используется для изменения паролей учетных записей, а также играет ведущую роль в процессе синхронизации системных часов всех контроллеров домена. Эмулятор PDC по умолчанию выбирается оснасткой Group Policy Object Editor. Поэтому, если исполнитель данной роли недоступен, администратор может столкнуться с серьезными проблемами при редактировании объектов групповой политики.
- Владелец инфраструктуры (Infrastructure Master). Контроллер домена, отвечающий за структуру каталога. В процессе удаления или перемещения объектов один из контроллеров домена должен взять на себя обязанности по сохранению ссылки на данные объекты до тех пор, пока эти изменения не будут реплицированы на все остальные контроллеры домена. Если в домене имеются несколько контроллеров домена, желательно не совмещать функции исполнителя данной роли и сервера глобального каталога. Лучше разнести эти функции на разные контроллеры домена, которые обязательно должны быть соединены высокоскоростным каналом. Если в домене имеется только один контроллер, этим требованием можно пренебречь.

Как с помощью команды DSMOD изменить пароль пользователю?

```
dsadd user cn=USERNAME,ou= OURGANIZATIONUNIT,dc=username,dc=local
dsmod user cn= USERNAME,ou=OURGANIZATIONUNIT,dc=username,dc=local -pwd PASSWORD
```

Где на контроллере домена хранятся файлы, содержащие групповые политики домена?

```
C:\WINDOWS\sysvol\domain\Policies
```

Где на контроллере домена хранится данные об объектах Active Directory в виде файлов?

```
C:\WINDOWS\NTDS
```

Какие виды групп в Active Directory существуют?

Есть два типа групп: группы безопасности и группы распространения. Группы распространения используются в основном почтовыми приложениями, эти группы не имеют SID, поэтому им не могут быть даны права на ресурсы. При отправке сообщения группе распространения, сообщение рассылается всем членам этой группы.

Группы безопасности используются при разграничении прав доступа в ACL (списки контроля доступа) объектам. Также данные группы могут использоваться в качестве групп распространения. Так как группы безопасности могут быть использованы и для разграничения доступа, и для рассылки сообщений, многие организации используют только группы безопасности.

В чем отличие групп от контейнеров?

Объекты могут быть хранилищами для других объектов (группы безопасности и распространения). Объект уникально определяется своим именем и имеет набор атрибутов — характеристик и данных, которые он может содержать; последние, в свою очередь, зависят от типа объекта. Атрибуты являются составляющей базой структуры объекта и определяются в схеме. Схема определяет, какие типы объектов могут существовать.

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.

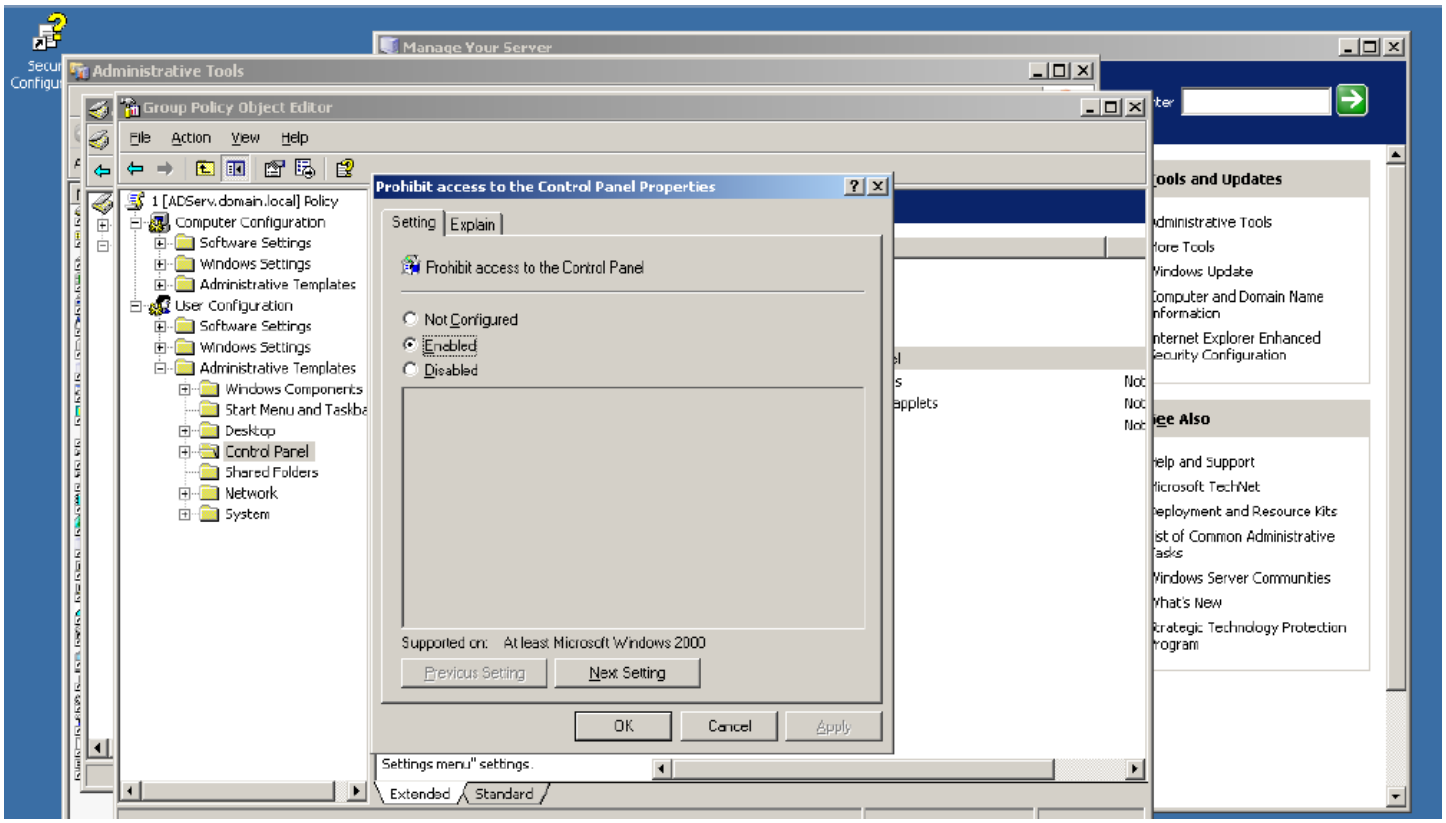
Что такое авторизация DHCP сервера? Для чего она выполняется?

Прежде чем DHCP-сервер сможет приступить к процессу выделения адресов DHCP-клиентам, он предварительно должен быть авторизован. Авторизация

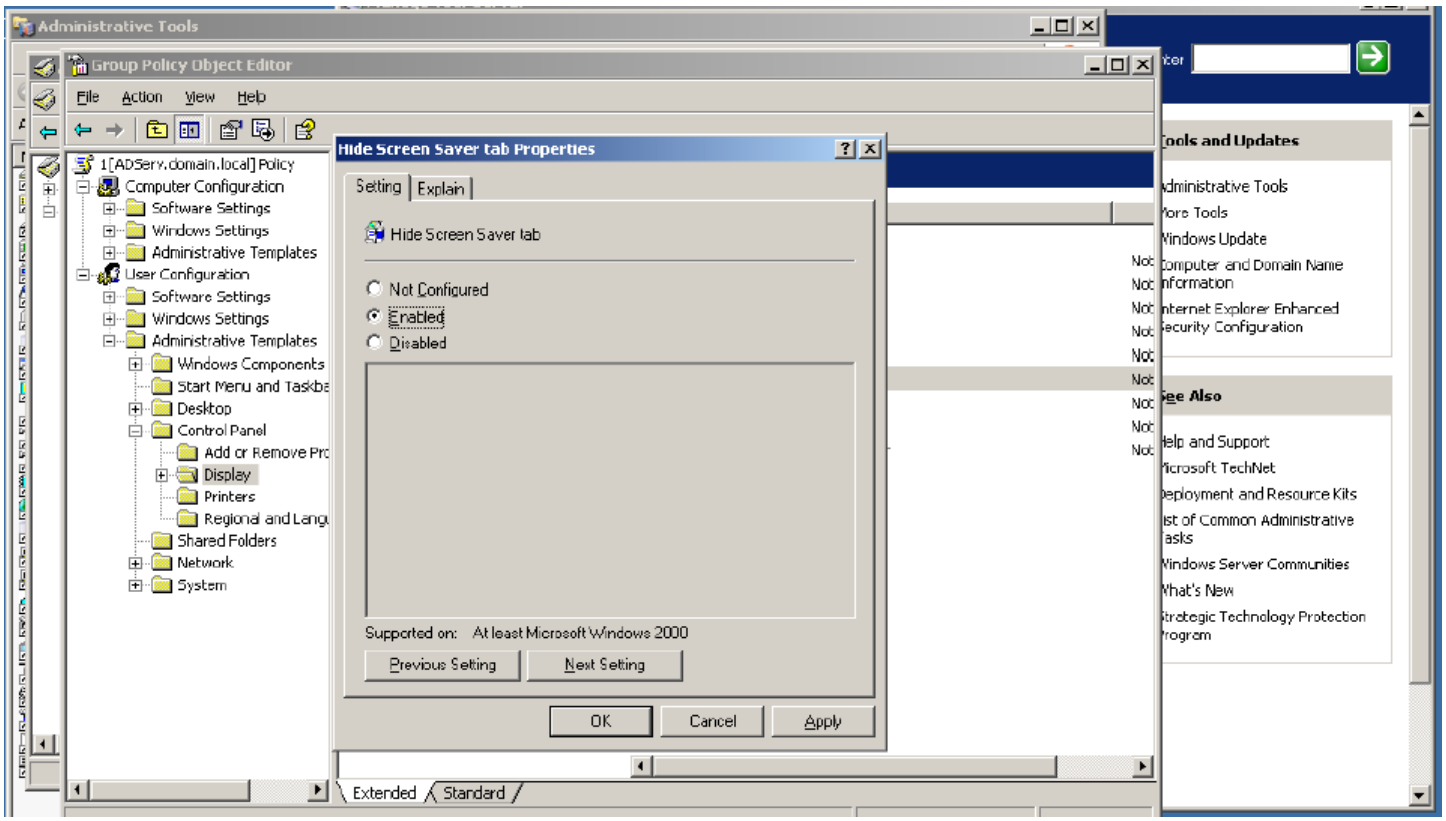
DHCP-сервера является обязательным условием его нормального функционирования. Иными словами, в каталоге Active Directory должен быть создан объект, соответствующий установленному DHCP-серверу.

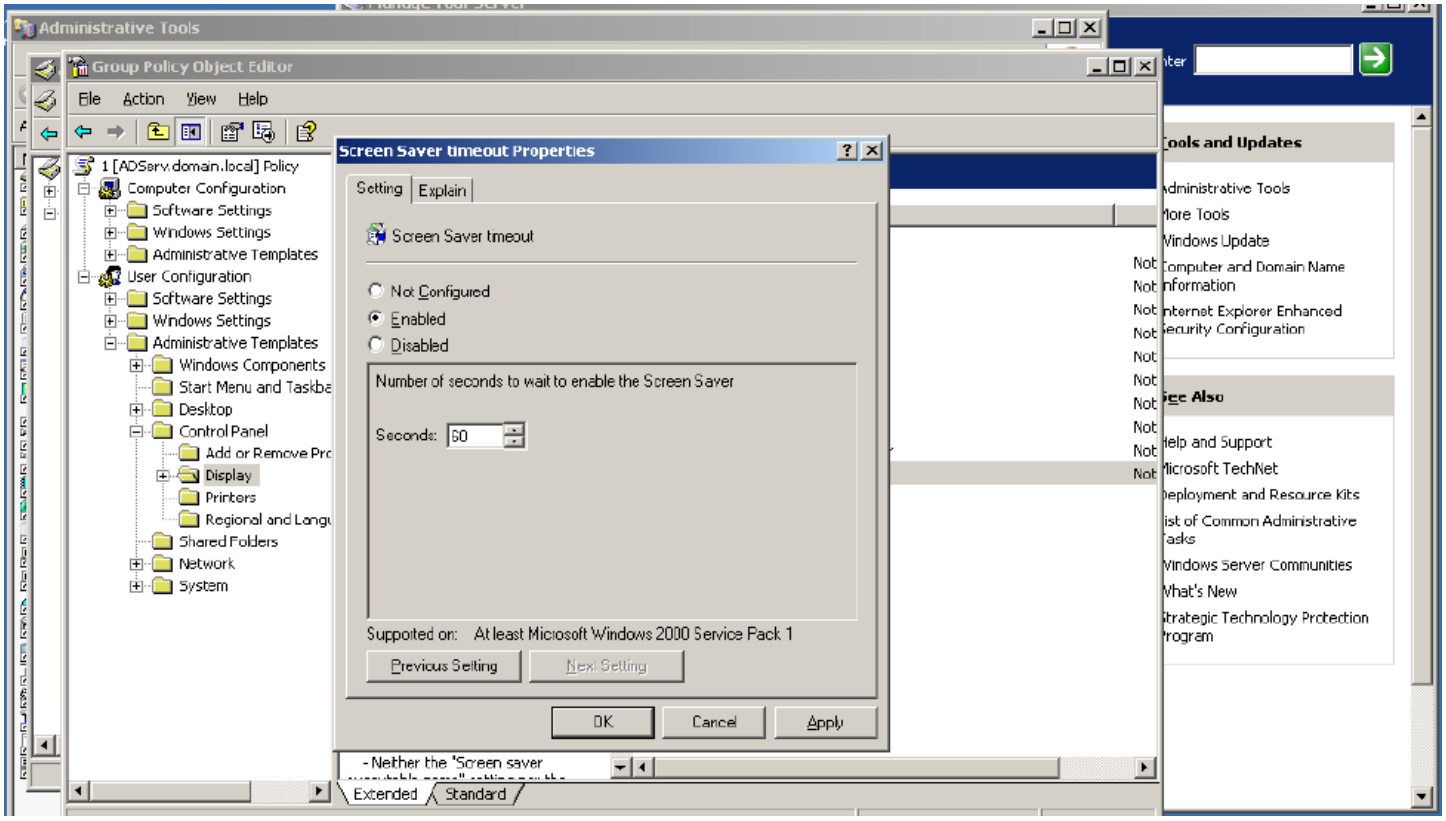
Групповые политики

Запрет доступа к панели управления

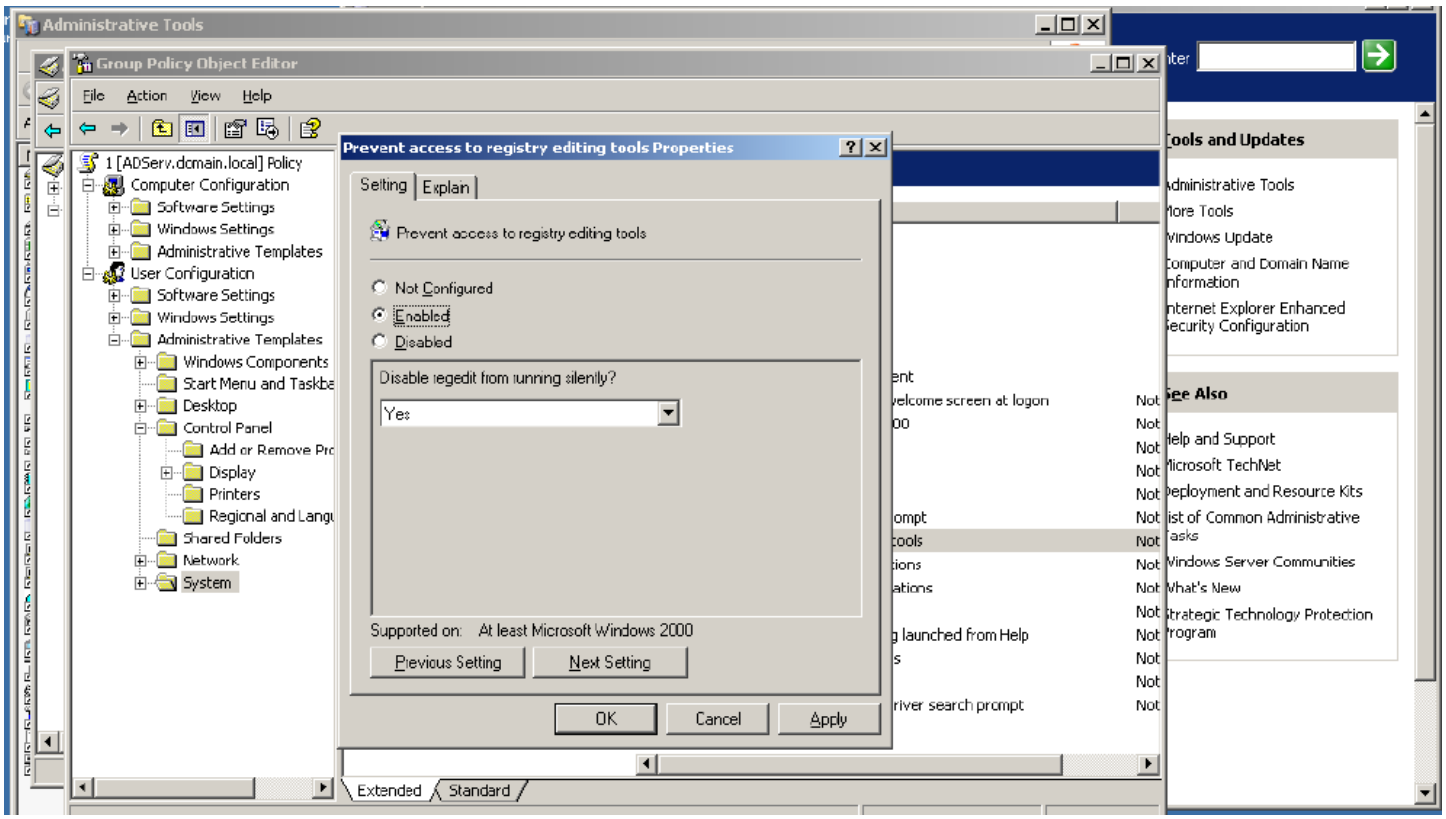


Блокировка экрана при неактивности 1 минута, с запретом на изменение

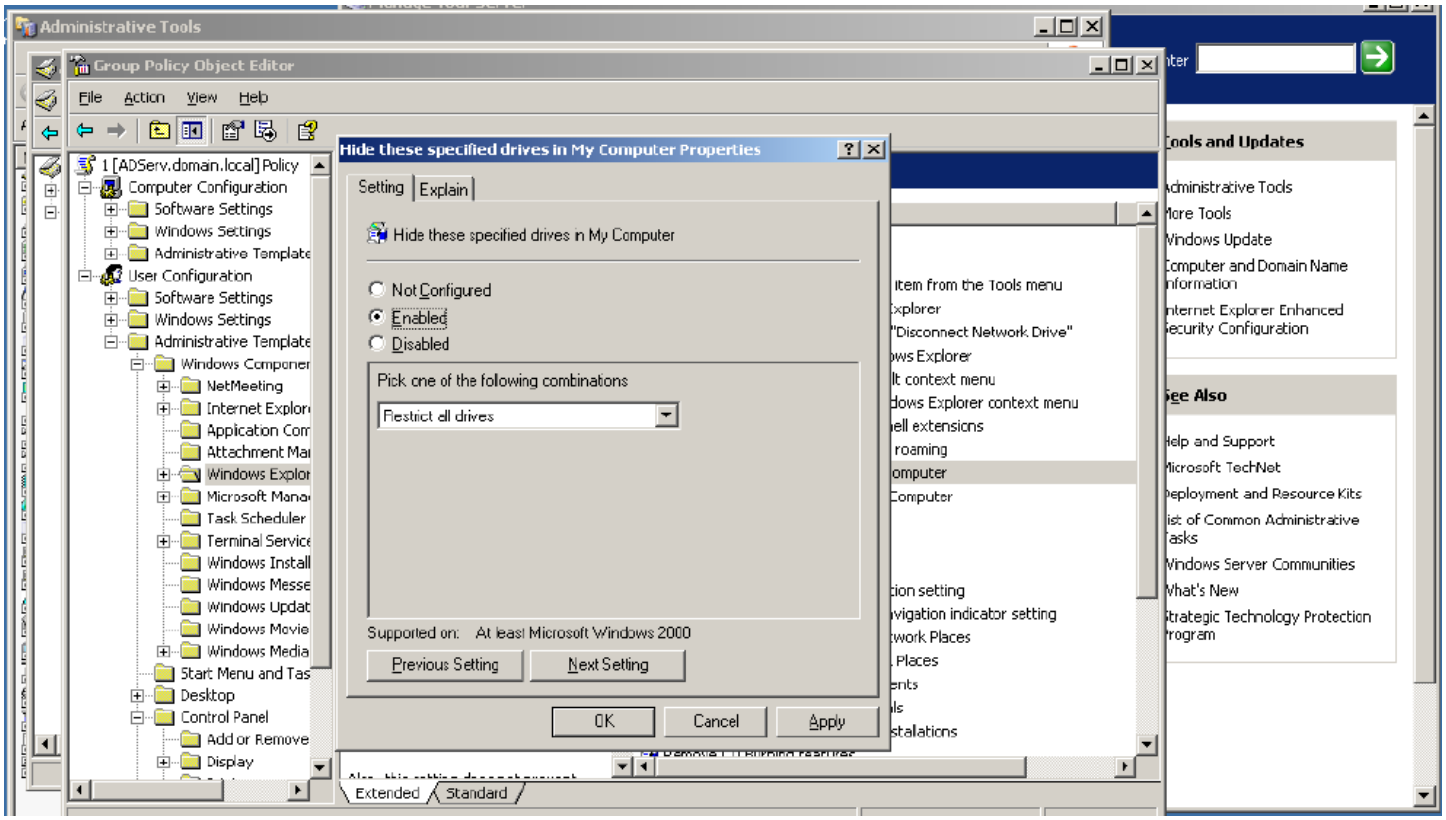




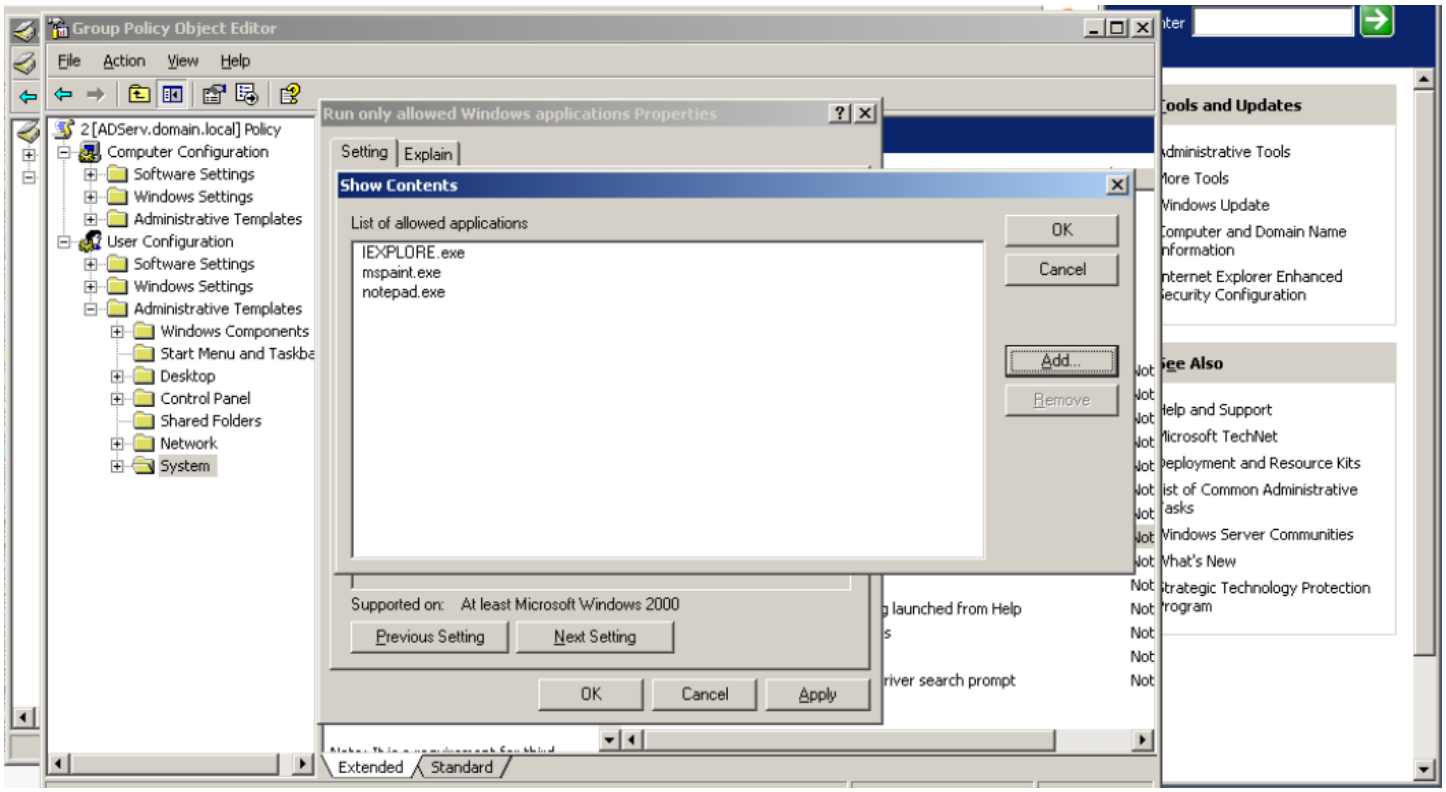
Запрет на редактирование реестра



Скрытие диска C в проводнике



Разрешенные для запуска приложения



Отключение сбора и передачи отчетов об ошибке

`Computer Configuration » Windows Settings » Security Settings » Local Policies » Security Options » System Services » Error reporting service = Disabled`

Отключение локальной учетной записи Администратор

`Computer Configuration » Windows Settings » Security Settings » Local Policies » Security Options » Accounts: Administrator account status = Disabled`

Запрет использования offline files

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

Установка прав на файлы диска C

```
Computer Configuration » Windows Settings » File System » Add file... » C:\
```

Скрипт

```
set name=%1
set password=%2
set unit=%3
if %unit=="M" set unit=ouManagers else set unit=ouSellers
if %unit=="M" set gr=gManagers else set gr=gSellers
dsadd user cn=%gr%,ou=%unit%,dc=TROFIV,dc=local -pwd %password% -mustchpwd yes -memberof %gr% -profile \\ADServ\UsersHome\%name%\_profile -hmdrv W: -hmdir \\ADServ\UsersHome\%name%
net share %name%=C:\UsersHome\%name% /grant:%name%,change
icacls %name% /grant %1:(OI)(CI)F
```

Вывод команды XCACLS

```
XCACLS %DIRECTORY_NAME% > C:\output.txt

SELLERS

C:\AllUsers\Sellers BUILTIN\Administrators:F
 TROFIV\gSellers:(OI)(CI)(special access:)
 READ_CONTROL
 SYNCHRONIZE
 FILE_GENERIC_READ
 FILE_GENERIC_WRITE
 FILE_GENERIC_EXECUTE
 FILE_READ_DATA
 FILE_WRITE_DATA
 FILE_APPEND_DATA
 FILE_READ_EA
 FILE_WRITE_EA
 FILE_EXECUTE
 FILE_DELETE_CHILD
 FILE_READ_ATTRIBUTES
 FILE_WRITE_ATTRIBUTES
TROFIV\uSeller1:(OI)(CI)(special access:)
 READ_CONTROL
 SYNCHRONIZE
 FILE_GENERIC_READ
 FILE_GENERIC_WRITE
 FILE_GENERIC_EXECUTE
 FILE_READ_DATA FILE_WRITE_DATA
 FILE_APPEND_DATA
 FILE_READ_EA
 FILE_WRITE_EA
 FILE_EXECUTE
 FILE_DELETE_CHILD
 FILE_READ_ATTRIBUTES
 FILE_WRITE_ATTRIBUTES
BUILTIN\Administrators:(OI)(CI)F
 NT AUTHORITY\SYSTEM:(OI)(CI)F
 CREATOR OWNER:(OI)(CI)(IO)F
 BUILTIN\Users:(OI)(CI)R
 BUILTIN\Users:(CI)(special access:)
 FILE_APPEND_DATA
 BUILTIN\Users:(CI)(special access:)
 FILE_WRITE_DATA
```

```
MANAGERS

C:\AllUsers\Managers BUILTIN\Administrators:F
 TROFIV\gManagers:(OI)(CI)(special access:)
 READ_CONTROL
 WRITE_OWNER
 SYNCHRONIZE
 FILE_GENERIC_READ
 FILE_GENERIC_WRITE
 FILE_GENERIC_EXECUTE
 FILE_READ_DATA
 FILE_WRITE_DATA
 FILE_APPEND_DATA
 FILE_READ_EA
 FILE_WRITE_EA
 FILE_EXECUTE
 FILE_DELETE_CHILD
 FILE_READ_ATTRIBUTES
 FILE_WRITE_ATTRIBUTES
 TROFIV\uManager1:(OI)(CI)(special access:)
 READ_CONTROL
 SYNCHRONIZE FILE_GENERIC_READ
 FILE_GENERIC_WRITE
 FILE_GENERIC_EXECUTE
 FILE_READ_DATA
 FILE_WRITE_DATA
 FILE_APPEND_DATA
 FILE_READ_EA
 FILE_WRITE_EA
 FILE_EXECUTE
 FILE_DELETE_CHILD
 FILE_READ_ATTRIBUTES
 FILE_WRITE_ATTRIBUTES
 BUILTIN\Administrators:(OI)(CI)F
 NT AUTHORITY\SYSTEM:(OI)(CI)F
 CREATOR OWNER:(OI)(CI)(IO)F
 BUILTIN\Users:(OI)(CI)R
 BUILTIN\Users:(CI)(special access:)
 FILE_APPEND_DATA
 BUILTIN\Users:(CI)(special access:)
 FILE_WRITE_DATA

COMMON

C:\AllUsers\Common BUILTIN\Administrators:F
 Everyone:(OI)(CI)(NP)(IO)R
 BUILTIN\Administrators:(OI)(CI)F
 NT AUTHORITY\SYSTEM:(OI)(CI)F
 CREATOR OWNER:(OI)(CI)(IO)F
 BUILTIN\Users:(OI)(CI)R
 BUILTIN\Users:(CI)(special access:)
 FILE_APPEND_DATA
 BUILTIN\Users:(CI)(special access:)
 FILE_WRITE_DATA

BLACKHOLE

C:\AllUsers\BlackHole BUILTIN\Administrators:F
 TROFIV\gManagers:(OI)(CI)(special access:)
 SYNCHRONIZE
 FILE_WRITE_DATA
 FILE_APPEND_DATA FILE_WRITE_EA
 FILE_WRITE_ATTRIBUTES
 TROFIV\gSellers:(OI)(CI)(special access:)
```

```
SYNCHRONIZE
FILE_WRITE_DATA
FILE_APPEND_DATA
FILE_WRITE_EA
FILE_WRITE_ATTRIBUTES
BUILTIN\Administrators:(OI)(CI)F
NT AUTHORITY\SYSTEM:(OI)(CI)F
CREATOR OWNER:(OI)(CI)(IO)F
BUILTIN\Users:(OI)(CI)R
BUILTIN\Users:(CI)(special access:)
FILE_APPEND_DATA
BUILTIN\Users:(CI)(special access:)
FILE_WRITE_DATA
```