МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

Университет ИТМО

Факультет информационных технологий и программирования
Кафедра информационных систем

Практическая работа № **6**
Основы работы с Active Directory в Windows Server

Выполнили студенты группы **M32101**:
Рожновский Иван
Юрченко Владислав

САНКТ-ПЕТЕРБУРГ

2021

Вопросы:

1. В службах каталогов присутствуют объекты двух типов - контейнеры и листья (по ассоциации с деревом).
Основной единицей хранения в AD является домен. Домен – контейнерный объект, представляющий собой фрагмент AD хранящийся на специальном компьютере с Windows Server. Домен может содержать объекты-контейнеры (Organization Unit) и конечные объекты (User, Group, Computer и т.п.). Домены AD могут объединяться в деревья, деревья в конгломераты более высокого уровня – леса. В AD относительно домена может строиться распределенная система в которых копии домена хранятся на нескольких Windows Server, работающих в режиме контроллера домена.
2. База данных Active Directory хранится на контроллере домена в файле NTFS.DIT, который находится в папке %SYSTEMROOT%\NTDS.

EDD.CHK — проверочный (checkpoint) файл

EDB.LOG — журнал транзакций (событий). Все изменения, происходящие с каталогом Active Directory, содержатся в этом файле. Размер файла ограничивается 10 Мб.

EDBxxxx.LOG — вспомогательные журналы событий, которые создаются, когда файл EBD.LOG уже достиг 10 Мб, а данные еще не выгружены в файл NTDS.DIT. Соответственно каждый файл занимает не более 10 Мб дискового пространства

RES1.LOG — резервный файл журнала событий

RES2.LOG — резервный файл журнала событий

TEMP.EDB — временный журнал, который содержит информацию о событиях, происходящих в настоящий момент

SHEMA.INI — необязательный файл, используемый для инициализации файла NTDS.DIT во время загрузки контроллера домена

3. Файлы, которые содержат параметры политики («Шаблон групповой политики») расположены по пути C:\Windows\SYSVOL\[domain]\Policies\ на контроллере домена.

4. Group Policy Management, .NET

5. DSRM используется для восстановления Active Directory из резервных копий, исправления различных ситуаций и проблем с AD, а также для сброса забытых паролей пользователей и администраторов. В этом плане DSRM чем то похож на безопасный режим с поддержкой сети, но с отключенной Active Directory.
6.
Нажмите > кнопку "Запустить", введите ntdsutil и нажмите кнопку "ОК".

В командной области Ntdsutil введите задайте пароль dsrm.

В командной строке DSRM введите одну из следующих строк:

---Чтобы сбросить пароль на сервере, на котором вы работаете, введите сброс пароля на сервере null. Переменная null предполагает, что пароль DSRM сбрасывается на локальном компьютере. При запросе введите новый пароль. Обратите внимание, что при введите пароль не отображаются символы.

-или-

---Чтобы сбросить пароль для другого сервера, введите имя_сервера_, где _servername**— это DNS-имя сервера, на котором сбрасывается пароль DSRM. При запросе введите новый пароль. Обратите внимание, что при введите пароль не отображаются символы.

В командной области DSRM введите q.

В командной области Ntdsutil введите q для выхода.

7.NetBIOS — сетевой протокол. Нужен для обнаружения компьютеров в сети, построенной на базе TCP/IP.

8. Группы по умолчанию находятся в контейнерах «Встроенные» и «Пользователи». Для групп по умолчанию в контейнере «Встроенные» используется область действия «Встроенная локальная». Для этих групп область действия и тип изменить невозможно. В контейнере «Пользователи» содержатся группы, для которых определена глобальная область действия, и группы, для которых определена область действия в локальном домене. Находящиеся в этих контейнерах группы можно перемещать в другие группы или подразделения внутри домена, но не в другие домены.

9. Network Configuration Operators — Members of this group can make changes to TCP/IP settings and renew and release TCP/IP addresses on domain controllers in the domain. This group has no default members.

Performance Monitor Users — Members of this group can monitor performance counters on domain controllers in the domain, locally and from remote clients without being a member of the Administrators or Performance Log Users groups.

Performance Log Users — Members of this group can manage performance counters, logs and alerts on domain controllers in the domain, locally and from remote clients without being a member of the Administrators group.

Pre-Windows 2000 Compatible Access — Members of this group have read access on all users and groups in the domain. This group is provided for backward compatibility for computers running Windows NT 4.0 and earlier. By default, the special identity Everyone is a member of this group. For more information about special identities, see Special identities. Add users to this group only if they are running Windows NT 4.0 or earlier.

Print Operators — Members of this group can manage, create, share, and delete printers connected to domain controllers in the domain. They can also manage Active Directory printer objects in the domain. Members of this group can log on locally to domain controllers in the domain and shut them down. This group has no default members. Because members of this group can load and

unload device drivers on all domain controllers in the domain, add users with caution.

Remote Desktop Users — Members of this group can remotely log on to domain controllers in the domain.

Replicator — This group supports directory replication functions and is used by the File Replication service on domain controllers in the domain. This group has no default members. Do not add users to this group.

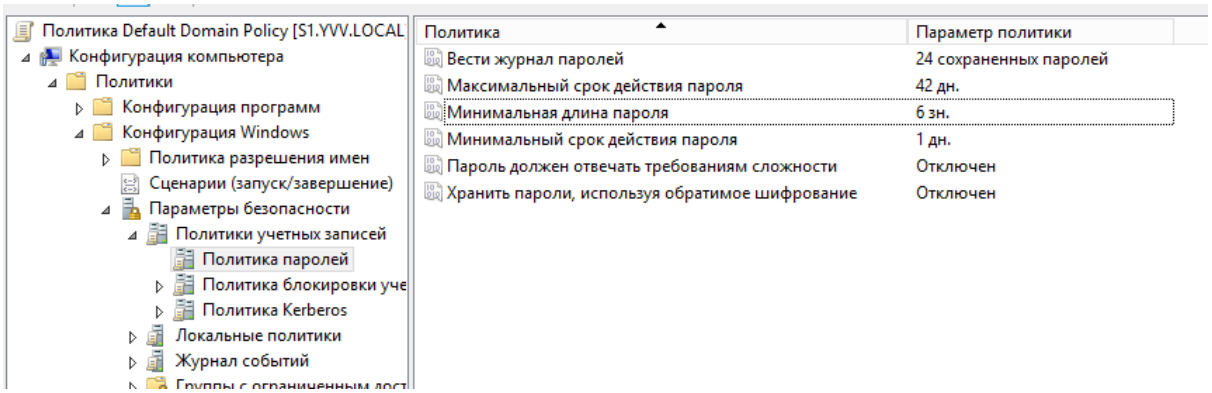
Server Operators — On domain controllers, members of this group can log on interactively, create and delete shared resources, start and stop some services, back up and restore files, format the hard disk, and shut down the computer. This group has no default members. Because this group has significant power on domain controllers, add users with caution.

Users — Members of this group can perform most common tasks, such as running applications, using local and network printers, and locking the server. By default, the Domain Users group, Authenticated Users, and Interactive are members of this group. Therefore, any user account created in the domain becomes a member of this group.

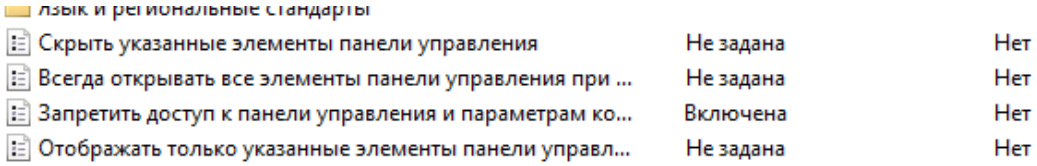
Артефакты:

1.

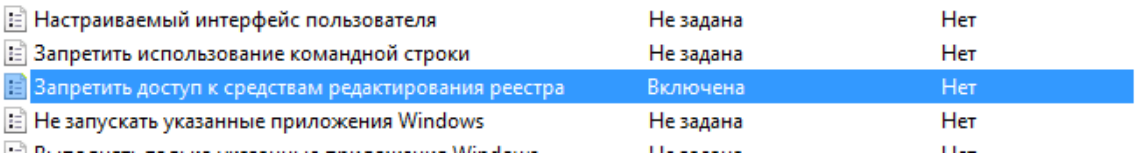
1.

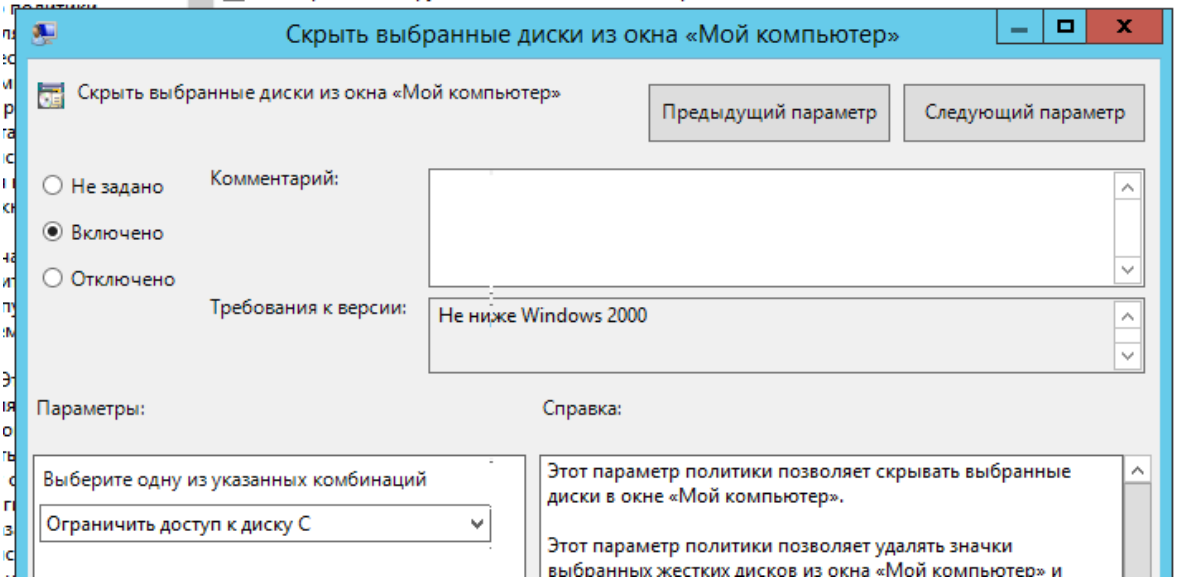


2.

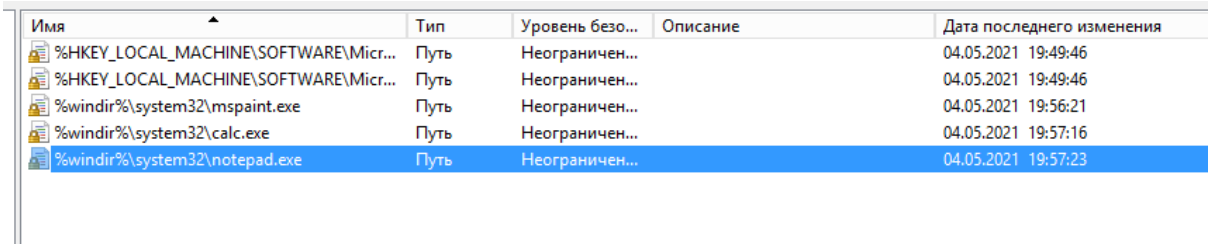

Скрыть указанные элементы панели управления Не задана Нет
Всегда открывать все элементы панели управления при ... Не задана Нет
Запретить доступ к панели управления и параметрам ко... Включена Нет
Отображать только указанные элементы панели управл... Не задана Нет


Запрет изменения звуков Не задана Нет
Защита заставки с помощью пароля Не задана Нет
Тайм-аут экранной заставки Включена Да
Применение указанной заставки Не задана Нет

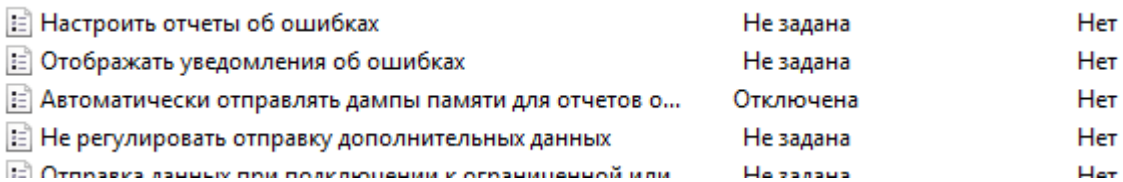

Настраиваемый интерфейс пользователя Не задана Нет
Запретить использование командной строки Не задана Нет
Запретить доступ к средствам редактирования реестра Включена Нет
Не запускать указанные приложения Windows Не задана Нет

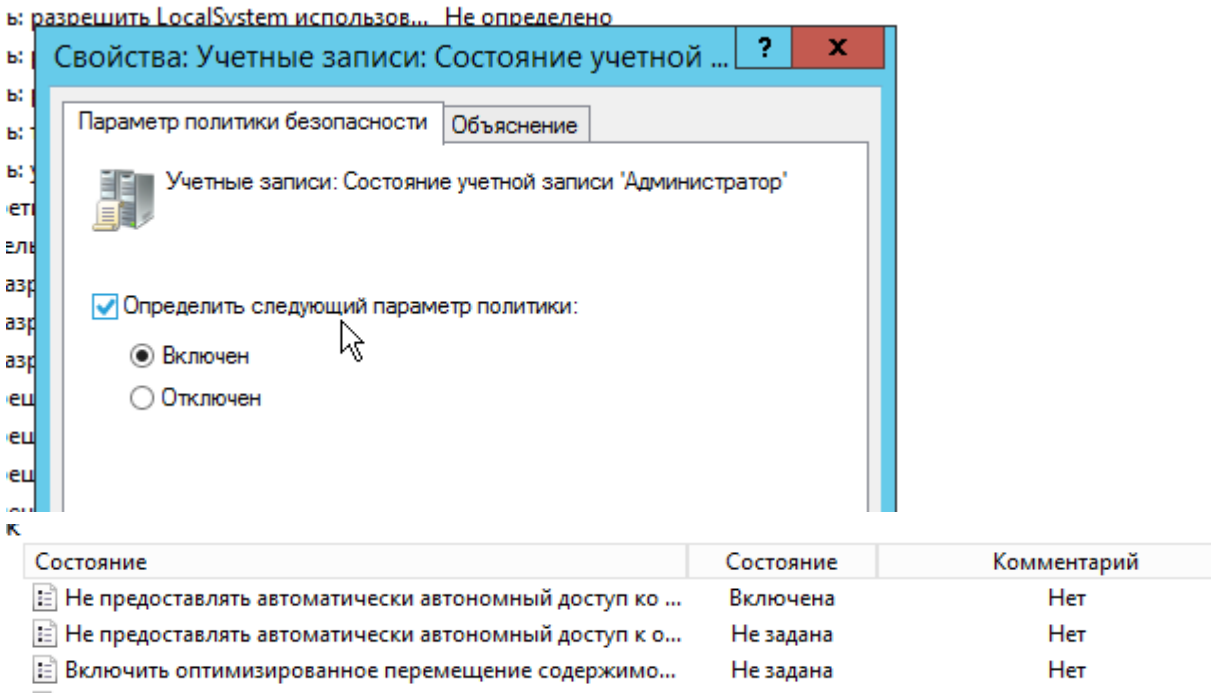

Скрыть выбранные диски из окна «Мой компьютер»
Скрыть выбранные диски из окна «Мой компьютер»
Предыдущий параметр
Следующий параметр
Не задано
Включено
Отключено
Комментарий:
Требования к версии:
Не ниже Windows 2000
Параметры:
Справка:
Выберите одну из указанных комбинаций
Ограничить доступ к диску C
Этот параметр политики позволяет скрывать выбранные диски в окне «Мой компьютер».
Этот параметр политики позволяет удалять значки выбранных жестких дисков из окна «Мой компьютер» и

3.


Имя Тип Уровень безо... Описание Дата последнего изменения
%HKEY_LOCAL_MACHINE\SOFTWARE\Micr... Путь Неограничен... 04.05.2021 19:49:46
%HKEY_LOCAL_MACHINE\SOFTWARE\Micr... Путь Неограничен... 04.05.2021 19:49:46
%windir%\system32\mspaint.exe Путь Неограничен... 04.05.2021 19:56:21
%windir%\system32\calc.exe Путь Неограничен... 04.05.2021 19:57:16
%windir%\system32\notepad.exe Путь Неограничен... 04.05.2021 19:57:23

4.


Настроить отчеты об ошибках Не задана Нет
Отображать уведомления об ошибках Не задана Нет
Автоматически отправлять дампы памяти для отчетов о... Отключена Нет
Не регулировать отправку дополнительных данных Не задана Нет



2. Import-Module ActiveDirectory

```
Import-Csv "C:\abc.csv" | ForEach-Object {
    $_ | New-ADUser
    # New-ADUser -GivenName $_.GivenName -Title $_.Title
-Department $_.Department -EmailAddress $_.EmailAddress
-MobilePhone $_.MobilePhone -Name $_.Name
-AccountPassword $_.AccountPassword -Path $_.Path
-HomeDirectory $_.HomeDirectory
    if ((Get-ADGroup -Filter {Name -like $_.Group} | measure).Count
-lt 1) {
        New-ADGroup -Name $_.Group
    }
    Add-ADGroupMember -Identity $_.Group -Members $_.Name
}

Import-Csv "C:\abc.csv" | ConvertTo-Html
```

3.
Восстановить удаленную группу:

```
Get-ADObject -Filter { Deleted -eq $True -and ObjectClass -eq
'group' -and Name -like '*Allow*' } –IncludeDeletedObjects|
Restore-ADObject –verbose
```

Восстановить компьютер:

```
Get-ADObject -Filter { Deleted -eq $True -and ObjectClass -eq 'computer' -and Name -like '*spb-fs02*' } –IncludeDeletedObjects| Restore-ADObject –verbose
```

Восстановление удаленной OU
Сначала нужно восстановить корневой OU:

```
Get-ADObject -Filter { Deleted -eq $True -and ObjectClass -eq 'organizationalunit' -and Name -like '*SPB*' } –IncludeDeletedObjects| Restore-ADObject
```

Затем все вложенные OU:

```
Get-ADObject -Filter { Deleted -eq $True -and ObjectClass -eq 'organizationalunit' -and LastKnownParent -eq 'OU=SPB,DC=winitpro,DC=ru' } –IncludeDeletedObjects| Restore-ADObject
```

Теперь можно восстановить все удаленные объекты в этих OU по параметру LastKnownParent (пользователей, компьютеры, группы, контакты):

```
Get-ADObject -Filter { Deleted -eq $True} –IncludeDeletedObjects -Properties *| Where-Object LastKnownParent -like '*OU=SPB,DC=winitpro,DC=ru'| Restore-ADObject
```

4. dsquery ou -name unit-for-delete | dsget ou -members | dsrm
5. Get-ADObject -SearchBase "CN=Deleted Objects,DC=acme,DC=com" -Filter {lastKnownParent -eq "OU=unit-for-delete,DC=acme,DC=com"} -IncludeDeletedObjects | Restore-ADObject