**Лабораторная работа 8. Управление доступом к файловым ресурсам с помощью FSRM**

**Подготовительная часть**

1. Для выполнения заданий этой работы нужен физический или виртуальный компьютер с адресом из подсети 172.18.192.0/22 (класс 131-4) и физически подключенный к сети университета или факультета ФИТ (172.18.196.0/22, классы ???-1).

2. Требуется установленное подключение с помощью удалённого рабочего стола к компьютеру DC90 под личной учётной записью, созданной в одной из первых работ.

**Часть 1. Назначение квот на папки**

**Задача 1.** Создание квоты

1. На компьютере DC90 откройте консоль **File Server Resource Manager**. Раскройте узел **Quota Management**. Перейдите в узел **Quota Templates**.

2. Создайте шаблон квоты со следующими параметрами:

Template name: **QTxx 2 MB**

Limit: **2 MB**

Hard quota**: Do not allow users to exceed limits**

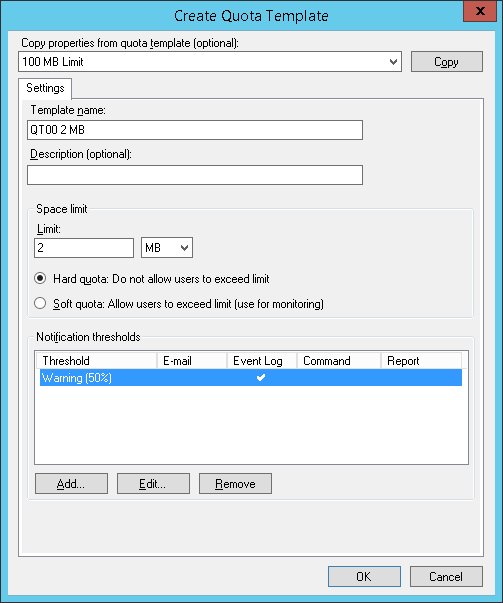
Notification threshold: Добавить новый (**Add…**)

Generate notifications when usage reaches (%): **50**

Перейдите на закладку **Event Log**

Включите параметр **Send warning to event log**.

Нажмите **OK**.

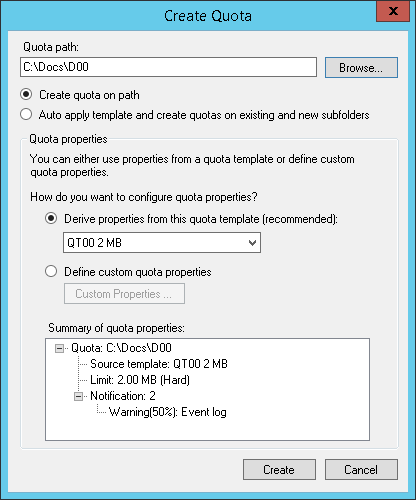


Нажмите **OK**.

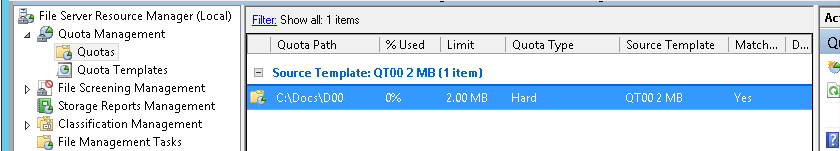
2. Создайте квоту для своей папки C:\Docs\Dxx на основе созданного шаблона:

Quota path: **C:\Docs\Dxx**

Derive properties from this quota template (recommended): **QTxx 2 MB**



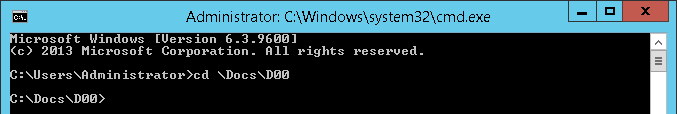
Нажмите **Create**.



**Задача 2.** Проверка квоты

1. На компьютере DC90 запустите командную консоль **cmd**.

2. Сделайте свою папку текущей:



3. Создайте файл размером 800 килобайт:

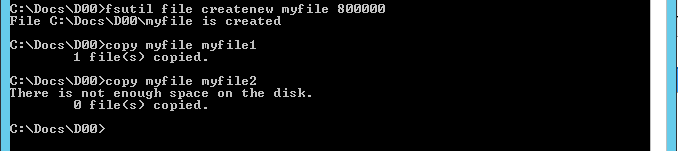
**fsutil file createnew myfile 800000**

4. Попытайтесь сделать две копии нового файла с именами myfile1 и myfile2

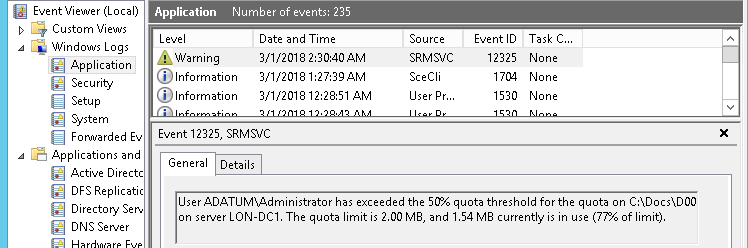
**copy myfile myfile1**

**copy myfile myfile2**

Удалось ли превысить квоту? \_\_\_\_\_\_\_\_\_\_\_\_



5. Откройте консоль **Event Viewer** и в контейнере **Windows Logs** откройте журнал **Application**. Найдите событие с кодом 12325.



6. Увеличьте ограничение в своем шаблоне до 3 MB. В окне **Update Quotes Derived from** **Template** выберите вариант **Apply template to derived quotas**.

7. Повторите попытку сделать вторую копию файла с именем myfile2. Она должна быть успешной.

**copy myfile myfile2**

**Часть 2. Использование фильтрования**

**Задача 1.** Создание фильтра (screen)

1. На компьютере DC90 откройте консоль **File Server Resource Manager**. Раскройте узел **File Screening Management**. Перейдите в узел **File Screens**.

2. Создайте новый фильтр с параметрами:

File Screen path: **C:\Docs\Dxx**

How do you want to configure file screen properties?

**Derive properties from this file screen template (recommended):**

**Block Audio and Video Files**

**Задача 2.** Проверка действия фильтра

1. На компьютере DC90 запустите командную консоль **cmd**.

2. Сделайте свою папку **C:\Docs\Dxx** текущей.

3. Создайте файл с расширением .doc.

**fsutil file createnew mydoc.doc 1000**

3. Попробуйте создайте файл с расширением .avi.

**fsutil file createnew film.avi 1000**

Успешно ли создался файл с расширением .avi? \_\_\_\_

4. Попробуйте создать файлы с другими расширениями, свойственными для медиа-файлов по вашему мнению.

Затем откройте узел **File Groups** в консоли **File Server Resource Manager** и просмотрите список расширений, включенных в группу **Audio and Video Files**.

**Задача 3.** Получение отчета о фильтрации файлов на сервере.

1. Перейдите в узел **Storage Reports Management** в консоли **File Server Resource Manager**.

2. Выберите команду **Generate Report Now…**.

На вкладке **Settings** в панели **Report data** выберите **File Screening Audit**.

Нажмите кнопку **Edit Parameters…**.

В поле **Selected users** укажите имя своего пользователя.

На вкладке **Scope** в панели **The following folders are included in this scope** укажите **C:\Docs\Dxx**.

Нажмите **OK**.

В окне **Generate Storage Reports** выберите вариант **Wait for reports to be generated and then display them**.

3. Откройте сгенерированный отчет с расширением .html.

**Часть 3. Использование шифрующей файловой системы EFS**

*Внимание. Возможна ситуация, что после выполнения лабораторной работы №5 у многих сгенерировалось много разнообразных сертификатов на основе шаблона UserXX других студентов. В таком случае, для всеобщего удобства каждому следует в консоли* **Certificate Templates Console** *изменить свойства своего шаблона UserXX, сняв разрешение* **Autoenroll** *для группы Authenticated users и удалить лишние сертификаты в оснастке* **Certificates***. Это необязательное действие, но в противном случае пролисты­вать список из сотен сертификатов может показаться утомительным.*

**Задача 1.** Создание зашифрованного файла

1. На компьютере DC90 в папке **C:\EFS** создайте текстовый файл с именем **textXX.txt** (в зависимости от настроек проводника расширение файла может не отображаться) и запишите в него строку осмысленного текста. Сохраните и закройте файл.

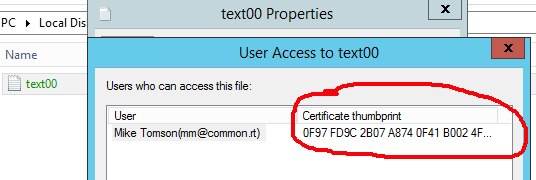
2. В проводнике Windows откройте свойства файла textXX.txt, на вкладке **General** нажмите кнопку **Advanced…**.

3. В окне **Advanced Attributes** отметьте опцию **Encrypt contents to secure data**, нажмите **OK**.

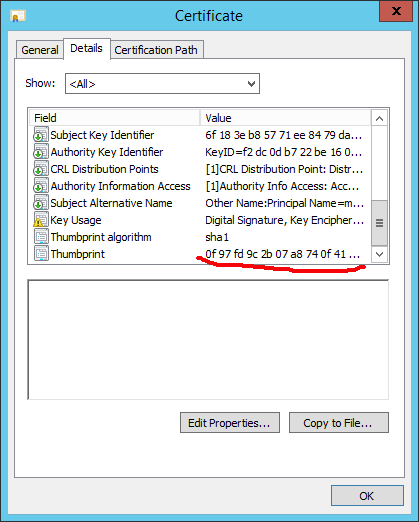
4. В окне **textXX Properties** нажмите **Apply**. В окне **Encryption Warning** выберите **Encrypt** **the file only**, отметьте опцию **Always encrypt only the file** и нажмите кнопку **OK**.

5. В окне **textXX Properties** снова нажмите кнопку **Advanced…**, в окне **Advanced Attributes** нажмите кнопку **Details**. В верхней части окна User Access to textXX найдите **Certificate thumbprint** и запомните его несколько первых символов.

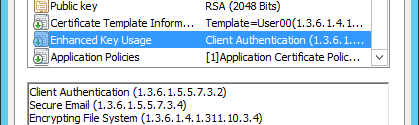
6. Закройте все диалоговые окна и убедитесь, что название файла отображается зеленым цветом в проводнике Windows.



7. В консоли **Certificates** найдите и откройте свой сертификат на основе шаблона UserXX, убедитесь, что **Thumbprint** такой же, что и в предыдущем пункте.



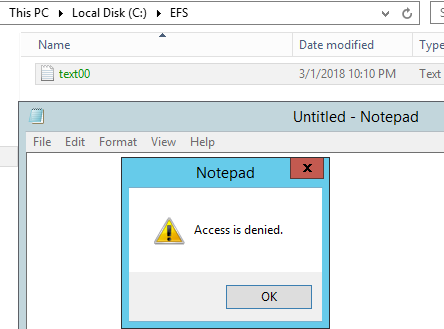
Убедитесь, что в полях **Enhanced Key Usage** и **Application Policies** присутствует **Encrypting File System**.



**Задача 2.** Предоставление совместного доступа к зашифрованному файлу

*Примечание. Это задание нужно выполнять совместно с кем-либо из студентов или преподавателем (использующим XX=00).*

1. На компьютере DC90 попробуйте открыть чужой файл в папке **C:\EFS**. Должно отобразиться сообщение об ошибке. Аналогичный результат должен быть у вашего напарника.



2. Откройте свойства своего файла, нажмите **Advanced…**, затем **Details**.

3. Нажмите кнопку **Add…** и добавьте сертификат напарника. Если их несколько, исполь­зуйте кнопку **View Certificate**, чтобы найти сертификат с правильным отпечатком (thumbprint).

4. Дождитесь появления сертификата в списке и нажмите кнопку **OK**.

5. Проверьте возможность доступа к чужому файлу. Теперь попытка должна быть успешной.

**Контрольные вопросы**

1. Можно установить квоту на диск /\* точнее, на том (volume) \*/ и без использования компонента **File Server Resource Manager – в свойствах тома, закладка Quota**. В чем принципиальные различия этих двух способов (назовите хотя бы два различия)?

2. Сохранится ли доступ к зашифрованным файлам после переустановки операционной системы на компьютере? А после принудительной смены пароля?

3. Если, работая на клиентском компьютере CL1, зашифровать файл, находящийся в общей папке на сервере SRV, как получить к нему доступ c клиентского компьютера CL2?