УВАЖАЕМЫЕ СТУДЕНТЫ!

ВАМ НЕОБХОДИМО ВЫПОЛНИТЬ СЛЕДУЮЩЕЕ:

1. Ознакомиться с теорией и законспектировать лекцию не меньше трех листов, составить и ответить на вопросы.

2. Предоставит отчет конспекта лекции прислать в виде скриншото в течении трех дней. тел. 072-17-44-9-22.

3. Отправить преподавателю на почту **v.vika2014@mail.ru** и указать свою Ф.И.О, группу, и название дисциплины

Тема: Создание и администрирование пользователем совместно используемых ресурсов: общие папки; установка разрешений; контроль над пользователями. (продолжение)

Управление разрешениями

Разрешения обшего доступа применяются, когда пользователь обращается к файлу или папке через сеть, но они не принимаются во внимание, если пользователь получает доступ к данным ресурсам локально, как это было бы при его нахождении непосредственно за компьютером либо при использовании ресурсов на терминальном сервере.

В противоположность этому, разрешения NTFS применяются независимо от того, каким образом пользователь обращается к тем же ресурсам, то ли он подключается к ним дистанционно, то ли входит в них из консоли. Итак, когда доступ к файлам осуществляется локально, применяются только разрешения NTFS.

При дистанционном обрашении к тем же самым файлам применяется объединение
разрешений общего доступа и NTFS с вычислением наиболее ограничивающего
разрешения из этих двух типов.

Создание разрешений общего доступа

Разрешения общего доступа являются, пожалуй, простейшей формой управления
доступом, с которой вы будете иметь дело в Windows Server. Вспомните, что разреше
ния общего доступа оказывают воздействие, только когда вы пытаетесь обратиться
к ресурсу через сеть. Считайте разрешения общего доступа разновидностью пропус
ка в охраняемое здание. Когда вы подходите к входной двери и предъявляете свое
удостоверение, охранник просматривает вашу фамилию и выдает пропуск, который
указывает уровень доступа к внутренним помешениям. Если на пропуске написа
но «доступ уровня 1 » , он позволит зайти в любую комнату с уровнем 1 , но нику
да больше.
Если вы попытаетесь, оказавшись внутри, зайти в комнату с требуемым уровнем доступа 2, пропуск не сработает.
Определяя разрешения общего доступа, вы безопасно упраnляете уровнем доступа для каждого лиua у входной днери.
Однако имейте в виду, что упомянутая входная дверь — или разрешение уровня
общего ресурса — это не полная картина.

Разрешение уровня общего ресурса представляет только максимальный уровень доступа, который вы получите внутри.
Если вы располагаете разрешением Read на общем ресурсе, то самое большее, что вы сможете делать после дистанционного подЮіючения к нему — это чтение. Подобным образом, разрешение Change позволит в лучшем случает вносить изменения.
Если вы хотите иметь полный контроль над всем внутри общего ресурса, вам понадобится разрешение Full Control на общем ресурсе.
Но поймите, что когда мы говорим о том, что разрешение общего доступа — это максимальный уровень доступа, который вы получите внутри общего ресурса, то имеем в виду возможность наличия дополнительного ограничения внутри за счет применения разрешений уровня файлов(или NTFS).
Вы можете располагать полным доступом на общем ресурсе, но объект внутри нero может иметь разрешения NTFS, которые позволяют только читать его.

Определение разрешений общего доступа

Чтобы определить разрешения общего доступа, выполните следующие действия в кон
соли Computer Management.
! . Щелкните правой кнопкой мыши на имени общего ресурса, который вы хотите защитить, и выберите в контекстном меню пункт Properties (Свойства).
В открывшемся диалоговом окне свойств перейдите на ВЮiадку Share Permissions
(Разрешения общего доступа).
Вы можете попасть в это место из проводника Windows, щелкнув правой кнопкой мыши на локальной общей папке, выбрав в контекстном меню пункт Shar

ing and Security (Общий доступ и безопасность) и затем в открывшемся диалоговом окне шелкнув на кнопке Permissions (Разрешения).

ОтсутствиЕ полного ДОСТУПА У ГРУППЫ Everyone

Обратите внимание на то, что группа Everyone по умолчанию имеет разрешение

Read, что является великолепным шагом вперед в мире Windows в плане безопаснос

ти. Вплоть до версии Wmdows Server 2003 группа Everyone по умолчанию получала

доступ Full Control. Еще одно удобное свойство в Windows Server 2012 связано с тем, что группа Everyone больше не добавляется к папке при открытии к ней общего доступа.

В этом диалоговом окне вы видите область Group or user names (Имена групп или пользователей) со списком пользователей и групп, назначенных обшему ресурсу; для выбранного пользователя или группы в области, расположенной ниже, отображаются разрешения на этом открытом ресурсе. Разным пользователям и группам можно назначать разные уровни разрешений.

На уровне общего доступа имеются три типа разрешений, описанные в табл. 14.1.

Таблица 14.1. типы разрешений

Разрешение

Full Control

(Полный доступ)

Change (Изменение)

Read (Чтение)

Уровень доступа

Группа, которой назначено это разрешение, может выполнять любые функции над всеми файлами и папками внутри общего ресурса

Группа, которой назначено это разрешение, может читать и запускать, а также изменять и удалять файлы и папки внутри общего ресурса Группа, которой назначено это разрешение, может читать и запускать файлы и папки, но не модифицировать или удалять что-либо внутри общего ресурса Пример на рис. 14.8 демонстрирует доступ Read для группы Everyone. Хотя вы не видите здесь учетную запись Administrator с какими-то специальны ми правами, учтите, что локальные администраторы всегда имеют доступ Full
Control на общих ресурсах компьютера. Если вы хотите изменить разрешения,
предоставив доступ Full Control всем сетевым администраторам, то должны добавить их группу и назначить ей эти права.
2. Щелкните на кнопке Add (Добавить), чтобы открыть диалоговое окно Select
Users, Computers, Service Accounts, or Groups (Выбор пользователей, компью теров, учетных записей служб или групп), представленное на рис. 14.9.

3. Либо введите имя пользователя или группы, подлежащей добавлению, либо
щелкните на кнопке Advanced (Дополнительно), что приведет к отображению другого диалогового окна Select Users, Computers, Service Accounts, or Groups (рис. 14. 10), которое позволяет производить поиск в каталоге. Можете либо воспользоваться функциями поиска в Active Directory на вклад- ке Common Queries (Общие запросы), чтобы сузить выбор, либо щелкнуть накнопке Find N o w (Найти сейчас), что обеспечит перечисление всех пользователей и групп в каталоге.
4. Найдите желаемую группу (Domain Administrators (Администраторы доме- на) в настоящем примере) и щелкните на кнопке ОК и затем еще раз на кноп- ке ОК. Произойдет возврат обратно на вкладку Share Permissions с отображе- нием и вьщелением добавленной группы Domain Administrators.
5. Отметьте флажок Allow (Разрешить) для разрешения Full Control.

Опять-таки, имейте в виду, что разрешения уровня общего ресурса — это как раз
то, что вы сначала фильтруете для пользователей, обращающихся к файлам через
сеть. Независимо от разрешений, получаемых на уровне общего ресурса, это будет
наивысший уровень разрешений, который вы можете получить для файлов и папок
(как вы помните, применяется наиболее ограничивающий из них). Если вы имеете
права Read на общем ресурсе, но права Ful\ Control на файле, то общий ресурс не
позволит вам делать что-то кроме чтения.

Действия Allow и Deny

Отмечая флажок Allow (Разрешить) для разрешения Full Control, назначенного
группе Domain Administrators в предыдущем примере, вы наверняка замети ли, что для каждого перечисленного разрешения предусмотрен также флажок Deny
(Запретить). Разрешения общего доступа являются, наверное, простейшим набором
разрешений, с которыми вы будете иметь дело, поэтому они хорошо подходят для
объяснения действий Allow и Deny. Вот как они работают.

• Администратор общего ресурса, файла, учетной записи пользователя или че го-то еще может изменить разрешения на своем объекте. (На самом деле, это почти полное определение администратора.)

Существует несколько видов разрешений — Full Control, Change или Read в случае общих ресурсов. Для любого из них администратор может отметить флажок Allow или Deny либо же решить снять отметку с обоих флажков, оста

вив пользователя без Allow или Deny на этом разрешении.
• Если пользователь не имеет разрешения (другими словами, флажки Allow и Deny не отмечены), то он не получит доступ к объекту.

• Если для разрешения отмечен флажок Allow, пользователь может применить

разрешение, а если флажок Deny, то нет. Мы знаем, что это очевидно, но давайте посмотрим, как это проявляется в более сложных ситуациях.