Лабораторная работа № 1

Управление правами доступа к файлам и папкам в ОС (Windows, Linux)

Теоретические Примечания

Учетная запись пользователя определяет, как вы взаимодействуете с вашим компьютером и как вы его настраиваете. Например, ваша учетная запись определяет, какие приложения, файлы и папки вы можете использовать, какие изменения вы можете внести в свой ПК и каковы ваши личные предпочтения, такие как внешний вид главного экрана, фон рабочего стола или заставка. Если вы создаете отдельные учетные записи для других, им не нужно совместно использовать одни и те же настройки, что означает, что вы можете ограничить доступ к своей электронной почте, работать в социальных сетях и других файлах и использовать разные изображения учетных записей , цвета или фоновые рисунки рабочего стола для каждой учетной записи.

Есть три типа учетных записей. Каждый тип дает вам другой уровень контроля над вашим ПК:

• Учетные записи администратора обеспечивают максимальный контроль над ПК и должны использоваться реже. Вы, вероятно, создали этот тип учетной записи, когда вы впервые использовали свой компьютер.

• Стандартные аккаунты предназначены для повседневной работы. Если вы настраиваете учетные записи для других на своем ПК, рекомендуется предоставить им стандартные учетные записи.

• Учетные записи детей полезны для родителей, которые хотят отслеживать или устанавливать ограничения на использование ПК своим ребенком с настройками в Windows Security. Для получения дополнительной информации о семейной безопасности см. Настройка семейной безопасности.

Помимо выбора одного из этих типов учетных записей, вы также можете выбрать метод входа для каждого типа: люди могут входить в Windows с учетной записью Microsoft или локальной учетной записью.
Пользователи (как доменные, так и локальные), группы пользователей и компьютеры (назовем их всех) имеют уникальные идентификаторы безопасности - SID. С этим идентификатором система и сущность «знают». SID имеет уникальное значение в домене и формируется при создании пользователя или группы или при регистрации компьютера в домене.

Когда входящий в систему пользователь вводит имя пользователя и пароль, операционная система проверяет, верен ли пароль, и, если пароль правильный, создает маркер доступа пользователя. Маркер включает в себя SID и все SID групп пользователей, к которым принадлежит пользователь.

Для защищаемых объектов (таких как файлы, папки, реестр Windows) создается дескриптор безопасности. Он связан со списком контроля доступа (ACL), который содержит информацию о том, как субъектам предоставляются определенные права доступа к объекту. Чтобы определить, следует ли предоставить запрошенный тип доступа к объекту, операционная система сравнивает SID в маркере доступа субъекта с SID, содержащимся в ACL.

Разрешения суммируются, и запрет является более высоким приоритетом, чем разрешение. Например, если пользователю разрешено читать файл, а в группе, к которой он принадлежит, - писать, то пользователь может читать и писать. Если у пользователя есть разрешение на чтение и группа, к которой он / она принадлежит, чтение запрещено, пользователь не может прочитать файл.

Если говорить о файлах и папках, механизмы безопасности в файловых системах поддерживаются только на дисках файловой системы NTFS. Файловая система FAT (и ее вариант - FAT32) не подразумевает возможность сохранения ACL, связанного с файлом.

Политики безопасности Windows очень эффективны для защиты компьютеров Windows, предоставляя пользователям ограниченный доступ. Если политики безопасности Windows не настроены правильно, пользователи могут легко манипулировать реестром, апплетами панели управления и другими критическими параметрами системы, что может привести к сбоям системы. Поэтому правильная настройка политик безопасности Windows на каждом компьютере с Windows в сети очень важна.

Локальная политика безопасности системы - это набор информации о безопасности локального компьютера. Информация о локальной политике безопасности включает следующее:

1. Доверенные домены для аутентификации попыток входа в систему.

2. Какие учетные записи пользователей могут получить доступ к системе и как. Например, в интерактивном режиме, по сети или как услуга.

3. Права и привилегии, приписываемые учетным записям.

4. Политика аудита безопасности.

Условия для работы

Для выполнения задачи вам понадобятся две учетные записи - учетная запись_ администратора и учетная запись_пользователя, которая не входит в группу администраторов. Нам также понадобится группа (group_ account). Все группы и учетные записи являются доменами, поэтому управление будет осуществляться с помощью пользователей и компьютеров Active Directory.

Работая под учетной записью администратора, мы создадим новую папку (Test). В его свойствах выберите вкладку «Безопасность» (рисунок 1). Вы можете только просматривать существующую авторизацию. Чтобы отредактировать их, вы должны нажать Edit, что позволит вам изменить список контроля доступа на папку (рисунок 2).

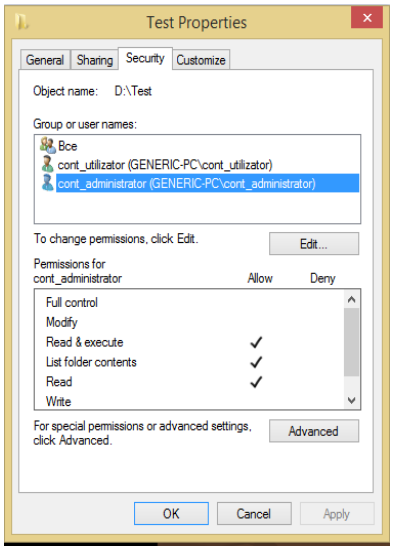

Рисунок 1

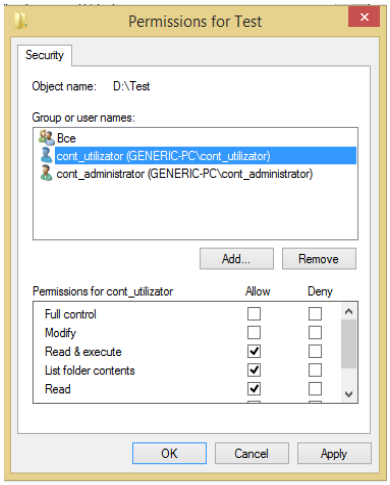

Рисунок 2

Условия для работы

Выполните шаги, аналогичные описанным выше. Убедитесь, что user account_user не находится в списке доступа к папкам, но входит в группу Users. Переключите пользователей, войдите в учетную запись пользователя, попробуйте открыть папку и создать в ней новую папку. Какое из этих действий было успешным? Почему?

Снова переключайте пользователей. Под учетной записью администратора добавьте доступ к файлу учетной записи пользователя в список пользователей и разрешите ему вносить изменения (Modify). Попробуйте снова создать папку.

Как оказалось, вы можете добавлять пользователей в список доступа. Под учетной записью администратора удалите группу Пользователи. Вы не сможете сделать это, появится предупреждение (рисунок 3), что эти разрешения унаследованы от родительского объекта. Чтобы отменить наследие, вы должны на вкладке «Безопасность» / Security (рисунок 1) нажать «Дополнительно» / Advanced. В появившемся окне (рисунок 4) отмечается, что включены наследуемые разрешения «Включить» из родительского свойства этого объекта (Include inheritable permissions from this object's parent). Это означает, что объект наследует ACL родителя, но его можно добавить только в родительский ACL для разрешений или запретов. Если вы нажмете кнопку «Редактировать» / Edit и сбросите этот флажок, появится вопрос, что делать со списком наследования - его можно скопировать (в ACL объекта) или удалить («Удалить»). Чаще всего, чтобы не потерять настройки, делаются копии, а затем список корректируется.

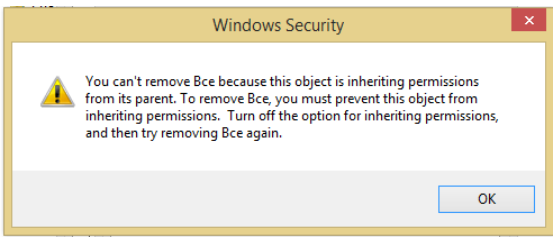

Рисунок 3

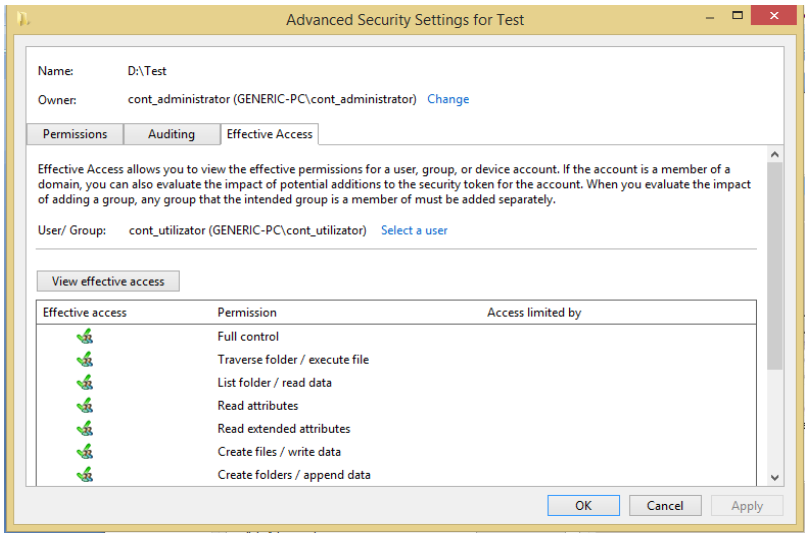

Рисунок 4

Условия для работы

Удалите группу пользователей из ACL для папки.

Если вы отредактируете права доступа в окне «Дополнительные параметры безопасности», вы увидите список разрешений, которые отличаются от того, что было ранее (рис. 5).

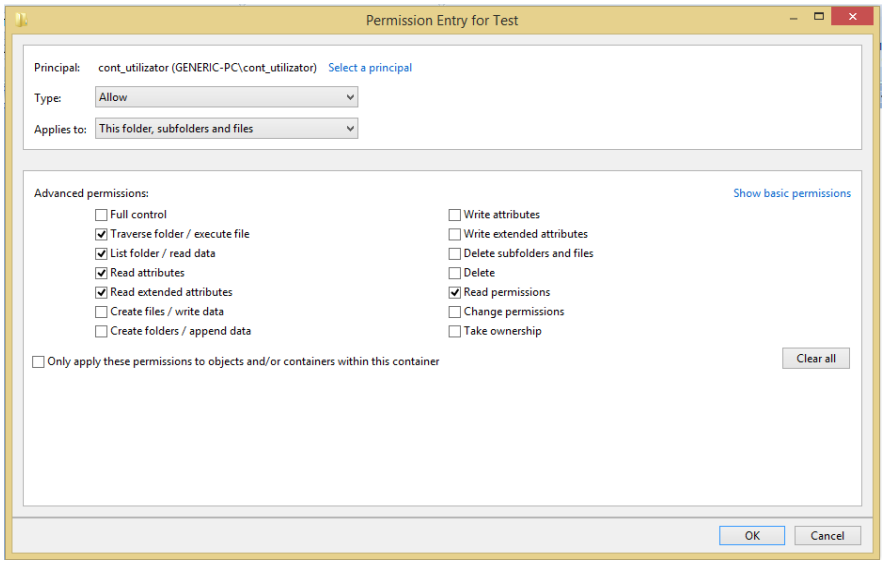

Рисунок 5

Это так называемые специальные разрешения. Ранее замеченные разрешения по умолчанию (чтение / read, запись / write и т. Д.) состоят из специальных разрешений. Взаимодействия между ними изображены на рис. 6. Более подробную информацию по этой теме можно найти, например, с помощью справки Windows.

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents (folders only)	Read	Write
Traverse Folder/Execute File	x	x	x	x		
List Folder/Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files/Write Data	x	x				x
Create Folders/Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x				x
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					
Synchronize	x	x	x	x	x	x

Рисунок 6

Как упоминалось ранее, при определении прав доступа предполагается активировать или дезактивировать права, как для пользователя, так и для всех групп, членом которых он является. Чтобы узнать действующее (efective) разрешение, вы можете воспользоваться вкладкой «Действующие разрешения» (Effective Permissions) (рис. 4). Нажав клавишу выбора, вы можете выбрать пользователя или группу, для которой будет отображаться подсказка.

Условия для работы

Убедитесь, что пользователю TestUser в папке, в которой выполняется действие, разрешено изменять. Проверьте текущее эффективное разрешение.

Не завершая сеанс пользователя, перейдите к сеансу администратора. Добавьте в папку разрешений список, чтобы запретить группе TestGroup любой доступ (выберите «Запретить полный контроль»). Введите пользователя TestUser в группу TestGroup. Посмотрите на эффективное решение для пользователя TestUser.

Переключитесь на сеанс пользователя TestUser. Попробуйте открыть папку и создать документ. Выйдите из сеанса TestUser и войдите снова. Затем попробуйте открыть папку и создать документ. Как мы можем объяснить этот результат (подсказка находится в начале описания лабораторной работы)?

Теперь рассмотрим вопросы владения папкой или файлом. Пользователь, создавший файл или папку, становится его владельцем. Текущий владелец объекта, вы можете увидеть, если в дополнительных настройках безопасности (рисунок 4), выберите вкладку Владелец.

Владелец файла может изменить разрешения для этого файла, даже если ему / ей отказано в доступе.

Процедура смены владельца файла в Windows Server 2008 отличается от той, что была в предыдущих версиях операционной системы. Ранее администратор или пользователь, которому принадлежит папка (папка), могли даже стать владельцами файлов. Более того,

владельцем может быть либо конкретный пользователь, либо группа администраторов (администраторов) - другой владелец группы не назначен.

В Windows Server 2008 администратор (или член группы администраторов) может стать не только владельцем, но и передать право собственности произвольному или групповому пользователю. Но это считается привилегированным и недоступным для любого пользователя, имеющего право на эту папку. На рисунке 7 показано, что администратор стал владельцем папки Test в группе TestGroup.

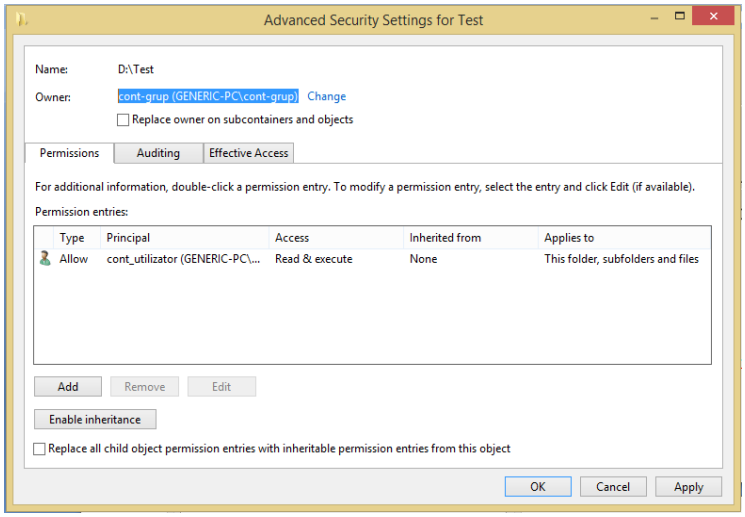

Рисунок 7

Условия для работы

Передайте право собственности на группу TestGroup, в которую входит пользователь TestUser. Получив доступ к этой учетной записи, измените разрешения, чтобы TestUser мог работать с этой папкой.

При использовании компьютера под управлением Windows Server 2008 в качестве файлового сервера важно учитывать, что в общей папке он разделяет разрешения, регулирующие доступ к сети. Это можно сделать на вкладке «Общий доступ» (рис. 9.8). В этом случае доступ к сети и разрешение на работу с общей папкой разрешают и NTFS. Результат является самым ограничительным. Например, если для общего каталога установлено «только чтение», а в разрешениях NTFS - «изменить», то, наконец, пользователь, подключающийся к сети, может только читать файлы. И тот же пользователь локального доступа получает право на изменение (разрешение на общую папку не будет затронуто).

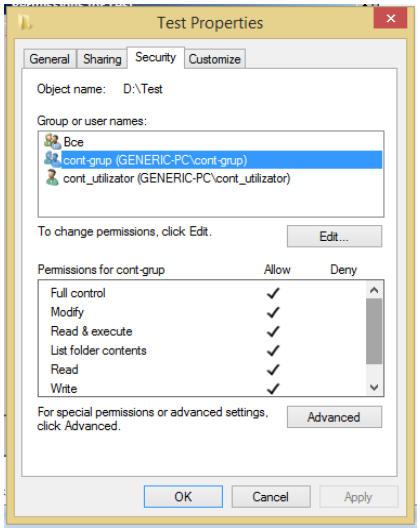

Рисунок 8