Администратор может управлять доступом пользователей к каталогам и файлам в разделах диска, отформатированных под файловую систему NTFS. Разделы, отформатированные под FAT и HPFS, не поддерживаются средствами защиты Windows NT. Однако можно защитить разделяемые по сети каталоги независимо от того, какая используется файловая система.

Для зашиты файла или каталога необходимо установить для него разрешения (permissions). Каждое установленное разрешение определяет вид доступа, который пользователь или группа пользователей имеют по отношению к данному каталогу или файлу. Например, когда вы устанавливаете разрешение Read к файлу MY IDEAS.DOC для группы COWORKERS, пользователи из этой группы могут просматривать данные этого файла и его атрибуты, но не могут изменять файл или удалять его.

Windows NT позволяет использовать набор стандартных разрешений, которые можно устанавливать для каталогов и файлов. Стандартными разрешениями для каталогов являются: No Access, Read, Add, Add&Read, Change и Full Control.

Стандартными разрешениями для файлов являются:

No Access, Read, Change и Full Control.

Стандартные разрешения представляют собой группы индивидуальных разрешений. Каждому стандартному разрешению соответствует определенная установка фиксированного набора индивидуальных разрешений. Индивидуальные разрешения могут быть:

Read (R), Write (W), Execute (X), Delete (D),

Change Permission (P), Take Ownership (O).

При установке стандартного разрешения рядом с ним в скобках отображаются заглавные буквы установленных индивидуальных разрешений. Например, при установке для файла стандартного разрешения Read рядом со словом Read появляется аббревиатура RX, которая означает, что стандартному разрешению Read соответствует установка двух индивидуальных разрешений - Read и Execute.

Администратор может с помощью утилиты File Manager устанавливать как стандартные, так и индивидуальные разрешения.

Для того, чтобы эффективно пользоваться возможностями механизмов безопасности NTFS, нужно помнить следующее:

* Пользователи не могут пользоваться каталогом или файлом, если они не имеют разрешения на это, или же они не относятся к группе, которая имеет соответствующее разрешение.
* Разрешения имеют накопительный эффект за исключением разрешения No Access, которое отменяет все остальные имеющиеся разрешения. Например, если группа CO-WORKERS имеет разрешение Change для какого-то файла, а группа Finance имеет для этого файла только разрешение Read, и Петров является членом обеих групп, то у Петрова будет разрешение Change. Однако, если разрешение для группы Finance изменится на No Access, то Петров не сможет использовать этот файл, несмотря на то, что он член группы, которая имеет доступ к файлу.
* Когда вы создаете в каталоге файлы и подкаталоги, то они наследуют разрешения, которые имеет каталог.
* Пользователь, который создает файл или каталог, является владельцем (owner) этого файла или каталога. Владелец всегда имеет полный доступ к файлу или каталогу, так как может изменять разрешения для него. Пользователи - члены группы Administrators - могут всегда стать владельцами любого файла или каталога.
* Самым удобным путем управления защитой файлов и каталогов является установка разрешений для групп пользователей, а не для отдельных пользователей. Обычно пользователю требуется доступ ко многим файлам. Если пользователь является членом какой-либо группы, которая имеет доступ к этим файлам, то администратору проще лишить пользователя этих прав, удалив его из состава группы, а не изменять разрешения для каждого файла. Заметим, что установка разрешения для индивидуального пользователя не отменяет разрешений, данных пользователю как члену некоторой группы.

*Для каталога индивидуальные разрешения имеют следующий смысл:*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | R | W | X | D | P | O | FC |
| Просматривать имена файлов в каталоге | **\*** | **O** | **\*** | **O** | **\*** | **O** | **\*** |
| Просматривать атрибуты каталога | **\*** | **O** | **\*** | **O** | **\*** | **O** | **\*** |
| Добавлять файлы и подкаталоги | **O** | **\*** | **O** | **\*** | **O** | **\*** | **\*** |
| Изменять атрибуты каталога | **O** | **\*** | **O** | **\*** | **O** | **\*** | **\*** |
| Переходить в подкаталоги каталога | **O** | **\*** | **\*** | **O** | **\*** | **O** | **\*** |
| Просматривать владельца каталога и разрешения | **\*** | l | **\*** | **O** | **\*** | **O** | **\*** |
| Удалять каталог | **O** | **\*** | **O** | **\*** | **O** | **\*** | **\*** |
| Изменять разрешения каталога | **O** | **\*** | **O** | **\*** | **\*** | **O** | **\*** |
| Становиться владельцем каталога | **O** | **\*** | **O** | **\*** | **O** | **\*** | **O** |

*Для файла индивидуальные разрешения имеют следующий смысл:*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | R | W | X | D | P | O | FC |
| Просматривать данные файла | **\*** | **O** | **O** | **O** | **O** | **O** | **\*** |
| Просматривать атрибуты файла | **\*** | **O** | **\*** | **O** | **O** | **O** | **\*** |
| Изменять атрибуты файла | **O** | **\*** | **O** | **O** | **O** | **O** | **\*** |
| Изменять и добавлять данные в файл | **O** | **\*** | **O** | **O** | **O** | **O** | **\*** |
| Выполнять файл, если это программа | **O** | **O** | **\*** | **O** | **O** | **O** | **\*** |
| Просматривать владельца файла и разрешения | **\*** | **\*** | **\*** | **O** | **O** | **O** | **\*** |
| Удалять файл | **O** | **O** | **O** | **\*** | **O** | **O** | **\*** |
| Изменять разрешения файла | **O** | **O** | **O** | **O** | **\*** | **O** | **\*** |
| Становиться владельцем файла | **O** | **O** | **O** | **O** | **O** | **\*** | **\*** |

Для файлов имеется следующее соответствие индивидуальных и стандартных разрешений файла:

No Access - Ни одного

Read - RX

Change - RWXD

Full Control - Все разрешения

Стандартные разрешения для каталога представляют собой объединения индивидуальных разрешений для каталога и для файлов, входящих в этот каталог:

No Access (Ни одного) (Ни одного)

List (RX) (Не определены)

Read (RX) (RX)

Add (WX) (Не определены)

Add&Read (RWX) (RX)

Change (RWXD) (RWXD)

Full Control (Все разрешения) (Все разрешения)

**5.6. Управление профилями пользователей**

Когда пользователь локально входит первый раз в какой-либо компьютер, то для него по умолчанию создается профиль. Все настройки среды (цвет фона, обои, шрифты и т.п.) автоматически сохраняются в подкаталоге Profiles системного каталога данного компьютера, например, C:\NT40w\Profiles\*username*, где *username* - имя пользователя. Профиль хранится в файле с именем ntuser.dat

Администратор также может настраивать профиль пользователя, входя в какой-либо компьютер под именем этого пользователя.

В отличие от профиля пользователя, который устанавливается по умолчанию, существует также Roaming - перемещаемый профиль пользователя, который формирует одну и ту же среду для данного пользователя, независимо от того, с какого компьютера он вошел в сеть.

Перемещаемые пользовательские профили хранятся централизовано на сервере, а не на локальных компьютерах пользователей.

Администратор может определить для пользователя один из двух типов перемещаемых профилей.

* Индивидуальный перемещаемый профиль, который пользователь может изменять. Любые изменения, которые пользователь внес в свою среду, вносятся в индивидуальный перемещаемый профиль тогда, когда пользователь логически выходит из сети. Когда тот же пользователь входит снова, с сервера загружается последний вариант профиля. Таким образом, если используются перемещаемые индивидуальные профили, то у каждого пользователя имеется свой собственный перемещаемый профиль. Этот профиль хранится в файле ntuser.dat в одном из разделяемых каталогов сервера.
* Обязательный (mandatory) перемещаемый профиль - это заранее сконфигурированный администратором профиль, который пользователь не может изменить. Один обязательный профиль может быть назначен нескольким пользователям. Этот вид профиля целесообразно назначать тем пользователям, которым требуется одинаковая среда, например, операционистам банка. Обязательный профиль должен иметь расширение .man. Индивидуальный профиль можно сделать обязательным, переименовав его из Ntuser.dat в Ntuser.man.

Начиная с версии 4.0, администратору предлагается более мощное средство управления профилями пользователей - System Policy Editor. С его помощью администратор может изменять профиль пользователя, не входя под его именем. При этом он может устанавливать ограничения, которые невозможно было бы установить, входя под именем пользователя, например, запрет на использование команды Run. System Policy Editor может может использоваться для формирования как локальных, так и перемещаемых профилей. Перемещаемый профиль хранится в файле Ntconfig.pol в разделяемом каталоге Netlogon на PDC.

**5.7. Аудит**

**5.7.1. Назначение аудита**

Аудит - это функция Windows NT, позволяющая отслеживать деятельность пользователей, а также все системные события в сети. С помощью аудита администратор получает информацию

* + о выполненном действии,
  + о пользователе, который выполнил это действие,
  + о дате и времени выполнения действия.

Администратор использует политику аудита (Audit Policy) для выбора типов событий, которые нужно отслеживать. Когда событие происходит, в журнал безопасности того компьютера, на котором оно произошло, добавляется новая запись. Журнал безопасности является тем средством, с помощью которого администратор отслеживает наступление тех типов событий, которые он задал.

Политика аудита контроллера домена определяет количество и тип фиксируемых событий, происходящих на всех контроллерах домена. На компьютерах Windows NT Workstation или Windows NT Server, входящих в домен, политика аудита определяет количество и тип фиксируемых событий, происходящих только на данном компьютере.

Администатор может установить политику аудита для домена для того, чтобы:

* отслеживать успешные и неуспешные события, такие как логические входы пользователей, чтение файлов, изменения в разрешениях пользователей и групп, выполнение сетевых соединений и т.п.;
* исключить или минимизировать риск неавторизованного использования ресурсов;
* анализировать временные тенденции, используя архив журнала безопасности.

Аудит является частью системы безопасности. Когда все средства безопасности отказывают, записи в журнале оказываются единственным источником информации, на основании которой администратор может сделать выводы о том, что произошло или готовится произойти в системе.

Установление политики аудита является привилегированным действием: пользователь должен либо быть членом группы Administrators на том компьютере, для которого устанавливается политика, либо иметь права Manage auditing and security log.

**5.7.2. Реализация политики аудита**

Политика аудита устанавливается отдельно для каждого компьютера. Например, для аудита логического входа пользователей в домен необходимо установить политику аудита на PDC (эта же политика определена и для всех BDC домена). Для наблюдения за доступом к файлам на сервере домена - member server- необходимо установить политику аудита на этом сервере.

События записываются в журнал определенного компьютера, но могут просматриваться из любого компьютера сети пользователем, который имеет права администратора на тот компьютер, где произошло событие.

Установка политики аудита включает два этапа:

* определение политики аудита с помощью панели Audit Policy утилиты User Manager for Domains или User Manager;
* определение каталогов, файлов и принтеров, доступ к которым необходимо отслеживать. Для этого используется Windows NT Explorer или панель Printers. Наблюдение за файлами и каталогами возможно только для файловой системы NTFS.

Просмотр журнала событий осуществляется с помощью утилиты Event Viewer (журнал Security).

**5.8. Репликация каталогов в сети Windows NT**

Иногда в сети полезно иметь несколько копий одного и того же файла на разных компьютерах. Примерами таких файлов может быть файл с номерами телефонов сотрудников предприятия, другие справочные данные, которые нужны одновременно многим клиентам сети. Поэтому для снижения нагрузки на сервер, хранящий такой файл, целесообразно разместить копии (реплики) этого файла на нескольких серверах сети и распределить нагрузку между этими серверами между клиентами сети.

Для поддержания синхронизма между данными разных копий файла применяется схема мастер-копии файла. Одна копия файла является мастер-копией, то есть оригиналом, в котором разрешается делать изменения. Другие версии этого файла создаются путем копировании по сети мастер-копии. Процесс копирования мастер-копии на серверы сети называется репликацией. Обычно репликация выполняется либо периодически, либо при возникновении изменений в мастер-копии.

Сервис репликации Windows NT позволяет автоматически реплицировать файлы, находящиеся в определенном каталоге любого компьютера, в каталоги других компьютеров сети.

Другим примером необходимости репликации файлов, харакетрным для сети Windows NT, является необходимость репликации файлов входных сценариев (Logon Scripts) пользователей и файлов системной политики (System Policy Files) в том случае, когда в сети есть кроме основного и резервные контроллеры домена.

Это связано с тем. что когда пользователь аутентифицируется на контроллере домена (неважно, на основном или резервном), то контроллер по умолчанию ищет файл входного сценария или файл системной политики в своем определенном локальном каталоге. Например, файл системной политики должен по умолчанию находиться в каталоге system-root\system32\Repl\Import\Scripts (имеющем разделяемое имя NETLOGON). Поэтому для того, чтобы пользователь имел один и тот же профиль, заданный в файле системной политики, независимо от того, какой контроллер домена его аутентифицирует, нужно поместить копии этого файла на все контроллеры домена

*Модель репликации* Windows NT включает следующие элементы:

* *Экспортирующий сервер*. Этот сервер реплицирует обновляемые файлы из определенного назначенного для репликации каталога на импортирующий компьютер. Экспортирующим сервером может быть только компьютер под управлением Windows NT Server.
* Импортирующий компьютер. Этот компьютер принимает обновленные реплицируемые файлы от экспортирующего компьютера. Импортирующий компьютер может принимать обновленные файла от определенного экспортирующего компьютера или же от всех экспортирующих компьютеров домена. В качестве импортирующих компьютеров могут выступать компьютеры под управлением Windows NT Server, Windows NT Workstation, LAN Manager for OS/2 Server.
* Каталоги экспорта и импорта. Сервер экспортирует файлы из подкаталогов главного каталога экспорта. По умолчанию, этим каталогом является каталог systemroot\System32\Repl\Export. Для экспортирования файлов администратор должен создать в этом каталоге подкаталоги для каждой группы файлов, которая должна экспортироваться. Необходимо отметить, что файлы, помещенные непосредственно в каталог systemroot\System32\Repl\Export, экспортироваться не будут. Например, для экспорта файлов Logon Scripts, необходимо поместить их в подкаталог system-root\System32\Repl\Export\Scripts.

Каждый импортирующий компьютер должен иметь главный каталог импорта, который соответствует главному каталогу экспорта. По умолчанию это каталог system-root\System32\Repl\Import.

* Сервис репликации каталогов Directory Replicator service. Этот сервис управляет репликацией файлов. Он работает на каждом экспортирующем сервере и импортирующем компьютере. Сервис репликации копирует из главного каталога экспортирующего компьютера все подкаталоги вместе с файлами в главный каталог импорта каждого импортирующего компьютера. При изменении какого-либо файла в подкаталогах главного каталога экспорта сервис репликации копирует его в соответствующий подкаталог импорта.

Сервис репликации на каждом компьютере, участвующем в процессе репликации, должен работать под именем некоторого вымышленного пользователя, например, repl, специально созданного для этих целей. Конфигурирование сервиса для входа под именем пользователя выполняется из панели Services. Данный пользователь должен быть членом групп Backup Operator и Replicator для копирования файлом репликации в обход возможных запретов по правам доступа.

Сервис репликации периодически проверяет состоянии экспортируемых файлов для обнаружения изменений. Когда изменение обнаружено, то происходит следующие действия:

* + Экспортирующий сервер посылает уведомление о изменении импортирующим компьютерам или по домену.
  + Когда импортирующий компьютер получает уведомление, то он обращается к серверу экспорта и читает структуру каталога экспорта.
  + Импортирующий компьютер копирует все новые или измененные файлы в свои подкаталоги импорта, а также удаляет из своих подкаталогов импорта те файлы, которые отсутствуют в подкаталогах экспорта.

Параметры сервиса репликации находятся в Registry:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Serveces\Replicator\Parameters

**5.9. Практические занятия**

**5.9.1. Создание и удаление пользователей**

Упражнение по созданию пользователей на компьютере с русскоязычной версией Windows NT Workstation.

* Создайте новых локальных пользователей (**Внимание! Во избежание проблем с запоминанием паролей назначайте новым пользователям пароли, совпадающие с их именами.**)
* Для создания учетных записей новых пользователей нужно использовать утилиту *Диспетчер пользователей.*
* Переименуйте пользователя *Администратор* в adm\_ws1 (или adm\_ws2, adm\_ws3, ... - в соответствии с именем компьютера), для того, чтобы можно было в дальнейших экспериментах не путать администраторов разных доменов и рабочих станций друг с другом.
* Создайте для групп *Администраторы, Пользователи и Опытные пользователи* новых пользователей, дайте им имена с приставками типа \_ws1, например, Nik\_ws2.
* Для пользователей групп Пользователи и Опытные пользователи проверить их возможности по использованию ресурсов домена.

Упражнение по созданию пользователей на компьютере с англоязычной версией Windows NT Server.

* Пользователи, работающие за серверами Windows NT Server входят в них, как в домен, то есть, например, в DOM1 и т.п., и создают новых пользователей домена. (**Внимание! Во избежание проблем с запоминанием паролей назначайте новым пользователям пароли, совпадающие с их именами.**)
* Для создания учетных записей новых пользователей нужно использовать утилиту User Manager for Domains.
* Пользователь Administrator переименовывается в adm\_dom1 (adm\_dom2, ...) - в соответствии с именем домена, для того, чтобы можно было в дальнейших экспериментах не путать администраторов разных доменов и рабочих станций друг с другом.
* Создайте для групп Domain Admins, Domain Users и Server Operators новых пользователей с именами с приставками \_dom1 и т.п.

Для новых пользователей домена (кроме администраторов) выполните следующие действия:

* Задайте интервал времени, когда пользователю разрешен вход в систему - пункт Hours в меню New User.
* Запретите вход с некоторых компьютеров в пределах домена. Для этого в панели New User нужно выбрать Log on To, и в окне диалога выбрать May Log On To These Workstation. В появившемся новом окне диалога задайте имена тех компьютеров, с которых будет разрешен вход.
* Установите дату истечения срока действия учетной информации данного пользователя - пункт Account в меню New User.
* Проверьте действие введенных установок, выполняя логические входы в домен.
* Убедитесь в возможности транзитной аутентификации - входе в домен с любого компьютера домена.

**5.9.2. Исследование разрешений (permissions), предоставляемых пользователям и группам пользователей по доступу к файлам и каталогам**

1. Создайте новый каталог в разделе С: локального диска, поместите в него несколько файлов из имеющихся каталогов путем копирования.
2. Проверьте, какие индивидуальные разрешения по отношению к этому каталогу установлены операционной системой по умолчанию. Для этого используйте пункт Properties меню File папки, в которую входит новый каталог. В закладке Security нажмите кнопку Permissions.
3. Задайте каталогу стандартное разрешение CHANGE для одного из новых пользователей, например, user\_dom1. Для этого в закладке Security нажмите кнопку Permissions, а затем кнопку Add (перед этим полезно удалить разрешение Full Control для группы Everyone).
4. Отметьте в следующем списке, какие действия вы можете выполнить по отношению к этому каталогу:
   * Просматривать имена файлов в каталоге
   * Просматривать атрибуты каталога
   * Добавлять файлы и подкаталоги
   * Изменять атрибуты каталога
   * Переходить в подкаталоги каталога
   * Просматривать владельца каталога и разрешения
   * Удалять каталог
   * Изменять разрешения каталога
   * Становиться владельцем каталога
5. Выберите один из файлов данного каталога. Проверьте, какие действия вы можете выполнить по отношению к этому файлу. Заполните таблицу:
   * Просматривать данные файла
   * Просматривать атрибуты файла
   * Изменять атрибуты файла
   * Изменять и добавлять данные в файл
   * Выполнять файл, если это программа
   * Просматривать владельца файла и разрешения
   * Удалять файл
   * Изменять разрешения файла
   * Становиться владельцем файла
6. После проверки прав доступа к локальным файлам:
   * сделайте новый каталог разделяемым (share) и задайте для него право Read,
   * войдите по сети в рабочую станцию домена под тем же именем, что и в упражнении 3 (то есть, user\_dom1),
   * проверьте, какие права есть по отношению к этому каталогу при доступе по сети.

**5.9.3. Исследование прав различных пользователей и групп пользователей (User Rights)**

Цель работы: Выяснить разницу между правами пользователей компьютера (Windows NT Workstation и Windows NT Server), правами пользователей домена, правами пользователей локальной группы компьютера, локальной группы домена, и глобальной группы.

**Локальный пользователь** компьютера может:

* Интерактивно войти в свой компьютер, если он имеет право Log on locally, и если компьютер не заблокирован другим пользователем (блокировка преодолевается только администратором данного компьютера);
* Войти в компьютер по сети, если он является локальным пользователем этого компьютера и наделен правом Access this computer from network;
* Пользоваться ресурсами своего компьютера в соответствии в правами и разрешениями, данными ему по умолчанию или администратором;
* Доступ к ресурсам других серверов домена (учитывая, что он не является пользователем домена) ему разрешен только тогда, когда он является и локальным пользователем каждого сервера.

**Пользователь домена** (не являющийся локальным пользователем компьютера, с которого он входит) может:

* Если он включен во встроенную глобальную группу Domain Users, то он может пользоваться ресурсами всех серверов домена с правами встроенного пользователя User, так как по умолчанию глобальная группа Domain Users включается в локальную группу Users всех серверов домена.

**Администратор домена** (входит в глобальную группу Domain Admins) может:

* + Заводить пользователей и группы (локальные и глобальные) домена на PDC;
  + Присоединять компьютеры к домену;
  + Просматривать разделяемые ресурсы (share) на серверах домена (кроме Windows for Workgroups), создавать и менять разрешения на доступ к ним;
  + Создавать локальных пользователей на компьютерах Windows NT Workstation.

**5.9.4. Управление профилями пользователей**

Для создания перемещаемых профилей пользователя:

1. Откройте апплет "Система" панели управления.
2. Выберите закладку User Profiles, скопируйте профиль администратора в какую-либо ПУСТУЮ папку. В диалоге копирования измените права использования профиля.
3. Сделайте папку, содержащую скопированный профиль, разделяемой.
4. В диспетчере пользователей укажите путь к папке профиля в графе профиля пользователя.
5. Если профиль должен быть принудительным, переименуйте в папке профиля ntuser.dat в ntuser.man.

Для установки обязательных профилей (системных политик) в домене с помощью System Policy Editor необходимо:

1. Создать новую политику с помощью System Policy Editor. Установить в ней необходимые параметры и ограничения среды пользователя с помощью иконки Default User.
2. Сохранить файл политики под именем ntconfig.pol в разделяемом каталоге NETLOGON на контроллере вашего домена (разделяемый каталог NETLOGON соответвует каталогу NT40s\System32\Repl\Import\Scripts).
3. Войти в рабочую станцию домена под любым именем и проверить, действуют ли установки, сделанные в файле политики, на среду пользователя.