УВАЖАЕМЫЕ СТУДЕНТЫ!

ВАМ НЕОБХОДИМО ВЫПОЛНИТЬ СЛЕДУЮЩЕЕ:

1. Ознакомиться с теорией и законспектировать лекцию не меньше трех листов.

2. Предоставит отчет конспекта лекции прислать в виде скриншото в течении трех дней .

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.

Пользователи, ресурсы и операции доступа

Администрирование пользователей состоит в создании учетной информации пользователей (определяющей имя пользователя, принадлежность пользователя к различным группам пользователей, пароль пользователя), а также в определении прав доступа пользователя к ресурсам сети - компьютерам, каталогам, файлам, принтерам и т.п.

Создание учетной информации пользователей осуществляется в сети Windows NT утилитой User Manager для локального компьютера и User Manager for Domains для всех компьеров домена. Права доступа к ресурсам задаются в сети Windows NT различными средствами, в зависимости от типа ресурса. Возможность использования копьютеров Windows NT Workstation в качестве рабочих станций - с помощью User Manager for Domains, доступ к локальным каталогам и файлам (только для файловой системы NTFS, поддерживающей права доступа) - с помощью средств Windows NT Explorer, к удаленным разделяемым каталогам - с помощью Server Manager, доступ к принтерам - из панели Printers.

Типы пользователей и групп пользователей

В сети Windows NT могут быть определены следующие типы пользователей и групп пользователей:

- *локальный интерактивный пользователь компьютера* (пользователь, который заведен в локальной учетной базе данных компьютера, и который работает с ресурсами компьютера интерактивно);
- *локальный сетевой пользователь компьютера* (пользователь, который заведен в локальной учетной базе данных компьютера, и который работает с ресурсами компьютера через сеть);
- *пользователь домена* (пользователь, который заведен в глобальной учетной базе данных домена на PDC);

- *локальная группа компьютера* (может создаваться на всех компьютерах домена, кроме PDC и BDC, в которых она вырождается в локальную группу домена);
- *локальная группа домена* - состоит из пользователей домена (заводится только на PDC);
- *глобальная группа домена* - состоит из пользователей домена (может входить в локальную группу домена).

Для каждого типа групп имеется некоторый набор встроенных групп: Administrators, Server Operators, Users, Everyone, DomainUsers и др.

Для однозначной идентификации глобальной группы в многодоменной сети, используется составное ее имя, например Marketing\Managers, где Marketing - имя домена, Managers - имя глобальной группы.

Типы объектов

- *Каталоги и файлы*. Процедуры задания правил доступа различаются для локальных и разделяемых (share) каталогов и файлов. Операции: read, full control, change, add, ...;
- *Принтеры;*
- *Операционная система*. По отношению к этому типу объектов определяются права по выполнению различных сервисов и утилит: вход, архивирование файлов, изменение конфигурации панелей Program Manager, ...

Типы операций доступа

Операции доступа - это действия объектов над субъектами. Операции могут быть либо разрешены, либо запрещены, либо вообще не иметь смысла для данной пары объекта и субъекта.

Все множество операций разделяется на подмножества, имеющие особые названия:

- разрешения (permissions) - это множество операций, которые могут быть определены для субъектов всех типов по отношению к объектам типа файл, каталог или принтер;
- права (user rights) - определяются для объектов типа группа на выполнение некоторых системных операций: создание резервных копий, выключение компьютера (shutdown) и т.п. Права назначаются с помощью User Manager for Domains;
- возможности пользователей (user abilities) - определяются для отдельных пользователей на выполнение действий, связанных с формированием их операционной среды, например, изменение состава программных групп, показываемых на экране дисплея, включение новых иконок в Desktop, возможность использования команды Run и т.п.

Права и разрешения данные группе автоматически предоставляются ее членам, позволяя администратору рассматривать большое количество пользователей как единицу учетной информации.

Возможности пользователей определяются профилем пользователя.

Локальные, глобальные и специальные группы

Windows NT Server использует три типа групп: локальные, глобальные и специальные. Каждый тип имеет свое назначение, возможности и ограничения.

Локальная группа может определяться для домена или для компьютера. Локальные группы дают пользователям права и разрешения на ресурсы того компьютера (или домена), где хранится учетная информация локальной группы. Доступ к ресурсам компьютера - Windows NT Workstation или Windows NT Server могут быть определены только для членов локальной группы этого компьютера, даже если эти компьютеры являются членами домена. Например, доступ к ресурсам сервера Windows NT Server 2 на рисунке 5.1 может быть определен только для пользователей, учетные данные которых хранятся в SAM 2 этого компьютера.

Так как база SAM PDC копируется на все BDC домена, то пользователи, определенные в PDC, могут иметь права на ресурсы как PDC, так и всех BDC домена.

Доступ к ресурсам компьютера для пользователей домена обеспечивается за счет механизма включения в локальную группу отдельных пользователей домена и глобальных групп домена. Включенные пользователи и группы получают те же права доступа, что и другие члены данной группы. Механизм включения глобальных групп в локальные является основным средством централизованного администрирования прав доступа в домене Windows NT.

Локальная группа не может содержать другие локальные группы. Поэтому в сети, использующей модель рабочей группы нет возможности определить на одном компьютере всех пользовавтелей сети и предоставлять им доступ к ресурсам других компьютеров.

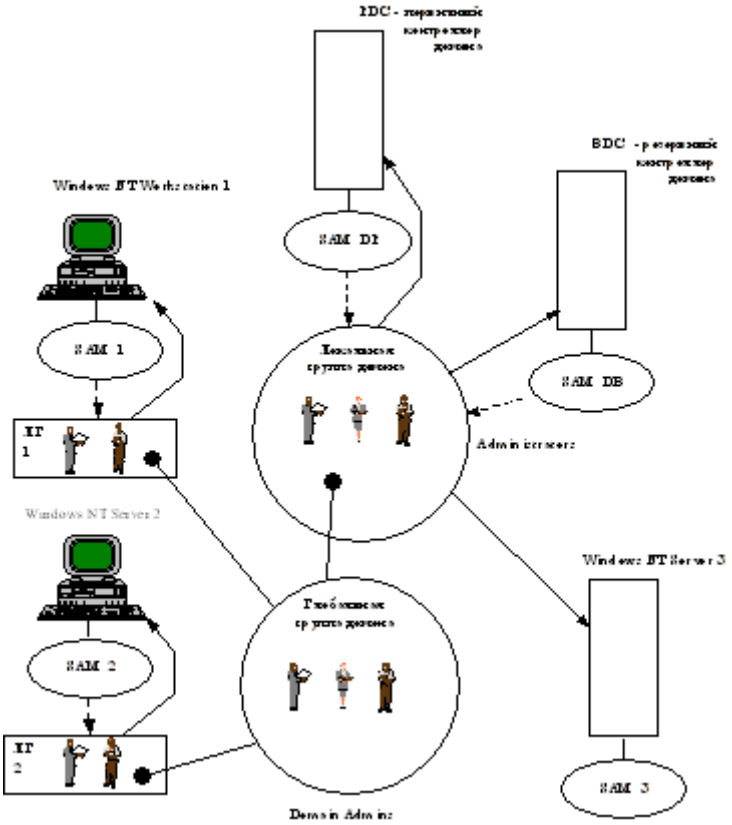

Рис. 5.1. Пример глобальной группы

В любом случае локальная группа объединяет некоторое число пользователей и глобальных групп, которым присваивается общее имя - имя локальной группы. Локальные группы могут включать пользователей и глобальные группы не только данного домена, но и любых доверяемых доменов.

Windows NT Workstation и Server поддерживают несколько встроенных локальных групп для выполнения системных задач. Администратор может создавать дополнительные локальные группы для управления доступом к ресурсам. Встроенные локальные группы делятся на две категории - администраторы (Administrators), которые имеют все права и разрешения на данный компьютер, и операторы, которые имеют ограниченные права на выполнение специфических задач. Для Windows NT Server имеются следующие группы-операторы: операторы архивирования (Backup Operator), репликаторы (Replicator), операторы сервера (Serevr Operator), принт-операторы (Print Operator) и операторы учетной информации (Account Operator). Для Windows NT Workstation имеется только две группы операторов - Backup Operators и Power Users.

Кроме того, как на Windows NT Server, так и на Windows NT Workstation имеются втроенные локальные группы Users - для обычных пользователей, и Guests - для временных пользователей, которые не могут иметь профиля и должны обладать минимальными правами.

Для упрощения организации предоставления доступа пользователям из другого домена в Windows NT введено понятие глобальной группы.

Глобальная группа пользователей - это группа, которая имеет имя и права, глобальные для всей сети, в отличие от локальных групп пользователей, которые имеют имена и права, действительные только в пределах одного домена. Администратор доверяющего домена может предоставлять доступ к ресурсам своего домена пользователям из глобальных групп тех доменов, которым данный домен доверяет. Глобальные группы можно включать в состав локальных групп пользователей ресурсного домена.

Глобальная группа - это некоторое число пользователей одного домена, которые группируются под одним именем. Глобальным группам могут даваться права и разрешения путем включения их в локальные группы, которые уже имеют требуемые права и разрешения. Глобальная группа может содержать только учетную информацию пользователей из локальных учетных баз данных, она не может содержать локальные группы или другие глобальные группы.

Существует три типа встроенных глобальных групп: администратор домена (Domain Admins), пользователи домена (Domain Users) и гости домена (Domain Guests). Эти группы изначально являются членами локальных групп администраторов, пользователей и гостей соответственно.

Необходимо использовать встроенные группы там, где только это возможно. Рекомендуется формировать группы в следующей последовательности:

1. В учетном домене необходимо создать пользователей и добавить их к глобальным группам.
2. Включить глобальные группы в состав локальных групп ресурсных доменов.
3. Предоставить локальным группам необходимые права и разрешения.

Специальная группа - используется исключительно Windows NT Server для системного доступа. Специальные группы не содержат учетной информации пользователей и групп. Администраторы не могут приписать пользователей к этим группам. Пользователи либо являются членами этих групп по умолчанию (например, каждый пользователь является членом специальной группы Everyone), либо они становятся ими в зависимости от своей сетевой активности.

Существует 4 типа специальных групп:

- Network (Сетевая)
- Interactive (Интерактивная)
- Everyone (Каждый)
- Creator Owner (Создатель-Владелец).

Любой пользователь, который хочет получить доступ к разделяемому ресурсу по сети, автоматически становится членом группы Network. Пользователь, локально вошедший в компьютер, автоматически включается в группу Interactive. Один и тот же пользователь в зависимости от того, как он работает с компьютером, будет иметь разные права. Любой пользователь

сети является членом группы Everyone. Администратор может назначить группе Everyone любые права. При этом администратор может предоставить любые права пользователю, не заводя на него учетной информации на своем компьютере. Группа Creator Owner содержит учетную информацию пользователя, который создал ресурс или владеет им.

В файловой системе NTFS разрешения группе Creator Owner даются на уровне каталога. Владелец любого каталога или файла, созданного в данном каталоге, получает разрешения, данные группе Creator Owner. Например, можно назначить какому-либо каталогу для членов группы Everyone разрешения Read (Чтение), а группе Creator Owner предоставить доступ Full Control (Полное управление). Любой пользователь, который создает файлы или подкаталоги в этом каталоге, будет иметь к ним доступ Full Control.

Встроенные группы пользователей и их права

Права определяются для объектов типа группа на выполнение некоторых системных операций: создание резервных копий, выключение компьютера (shutdown) и т.п. Права назначаются с помощью User Manager for Domains.

Операторы учетной информации (Accounts operators) не могут изменять учетную информацию администраторов, или же изменять глобальную группу Domain Admins или локальные группы Administrators, Server Operators, Account Operators, Print Operators или Backup Operators.
[2]Хотя члены группы Users имеют право создавать локальные группы домена, но они не смогут им воспользоваться, если им не разрешено входить локально в сервер или не разрешено пользоваться утилитой User Manager for Domains.
[3]Хотя Everyone имеет право блокировать сервер, только пользователи, которые могут также входить локально в этот сервер могут в действительности его заблокировать.

Похожие права можно задать и по отношению к Windows NT Server, не выполняющему роль PDC или BDC - с помощью утилиты User Manager for Domains, а также к Windows NT Workstation с помощью утилиты User Manager.

Возможности пользователей

Возможности пользователей - определяются для отдельных пользователей на выполнение немногочисленных действий, касающихся реорганизации их операционной среды:

1. Включение новых программных единиц (иконок) в группу программ панели Program Manager;
2. Создание программных групп Program Manager;
3. Изменение состава программных групп;
4. Изменение свойств программных единиц (например, включение в стартовую группу);
5. Запуск программ из меню FILE в Program Manager;
6. Установление соединений с сетевым принтером, кроме тех (которые уже предусмотрены в профиле пользователя).

Возможности пользователя являются частью так называемого профиля пользователя (User Profile), который можно изменять с помощью утилиты User Profile Editor. Профиль наряду с описанными возможностями включает и установки среды пользователя на его рабочем компьютере, такие как цвета, шрифты, набор программных групп и их состав.

Разрешения на доступ к каталогам и файлам

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 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)

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.