Лабораторная работа № 8

Планирование клиентов и групп в ОС Windows NT Server

**Цель работы:** Изучить основы планирования клиентов и групп в ОС Windows NT Server

**Оборудование:** Персональный компьютер, Microsoft Windows NT Domain Controller

Основное назначение сети – совместное использование ресурсов. В Windows NT управление ресурсами организовано на интуитивно понятном уровне.

# Управление пользователями и учетными записями

В большинстве сетей управление на уровне отдельных пользователей связано с множеством затруднений. Для упрощения задач администрирования Windows NT 4 содержит специальную программу – User Manager For Domains (вызывается из меню Start – Start >• Programs >• Administrative Tools (Common) > User Manager For Domains). В User Manager For Domains администраторы создают учетные записи пользователей и групп, а также работают с ними.

Для упрощения работы (и экономии вашего времени) управление пользователями основано на концепции группового администрирования. Как только пользователь включается в группу, он наследует все права и ограничения доступа, присвоенные данной группе.

Чтобы и далее упростить процесс управления пользователями, Microsoft предусмотрительно создает встроенные группы (как локальные, так и глобальные). Обратите внимание – встроенные группы нельзя удалить или переименовать. Обычно эти группы оказываются удобными для администрирования прав и ограничений пользователей. Кроме того, некоторые пользователи включаются в эти встроенные группы по умолчанию. Пользователей можно включать или удалять из этих групп по своему усмотрению.

## Работа с User Manager For Domains

User Manager For Domains – основной инструмент для управления правами пользователей. Ниже перечислены основные функции и задачи User Manager For Domains:

1. Создание, изменение, дублирование и удаление групповых учетных записей.
2. Создание, изменение, дублирование и удаление учетных записей пользователей.
3. Установка политики учетных записей (выбор стандартных требований к паролям, параметров блокировки учетных записей, статуса отключения и т. д.).
4. Создание прав и определение политики аудита для пользователей.
5. Установление доверительных отношений.

## Создание новых пользователей и групп

Чтобы создать в User Manager For Domains новую учетную запись пользователя или группы, выполните следующие действия:

1. Запустите User Manager For Domains и откройте меню User.
2. Выберите команду New User для создания пользователя (или команду New Group для создания группы).
3. Заполните диалоговое окно New User: введите имя пользователя (User Name), полное имя (Full Name) (необязательно), описание (Description) (необязательно), пароль (Password) и подтверждение пароля (Confirm Password).
4. Установите соответствующие флажки в нижней части окна New User, если:

• Пользователь должен изменить пароль при первом входе в систему.

• Пользователю не разрешается менять свой пароль.

• Для пароля не существует ограничений срока действия.

• Учетная запись отключается.

Кроме четырех флажков в нижней части диалогового окна находятся шесть кнопок. Они управляют многими возможностями, доступными для данного пользователя:

1. Groups (Группы). Кнопка позволяет добавить пользователей в группу (или группы) или удалить их.
2. Profiles (Профиль). Кнопка позволяет определить путь к профилям конкретного пользователя, к сценариям входа и основному каталогу пользователя.
3. Hours (Время). Кнопка позволяет задать интервал времени, в течение которого пользователю разрешается вход в сеть. Если к концу разрешенного времени пользователь уже зарегистрирован, то по умолчанию он остается в сети, однако повторный вход станет возможным лишь с наступлением разрешенного интервала.
4. Logon To (Вход с). Кнопка разрешает вход пользователя в систему только с определенных компьютеров. Тем не менее, пользователи редко остаются на одном месте, поэтому желательно оставить значение по умолчанию (вход с любой рабочей станции).
5. Account (Учетная запись). Здесь задается срок окончания действия учетной записи (полезно для временных или контрактных работников). По умолчанию используется значение Never (Никогда), однако вы можете ввести определенную дату.
6. Dialin (Связь). Здесь пользователю предоставляется возможность модемного подключения к сети, а при необходимости задается такой элемент защиты, как ответный звонок сервера.

## Модификация существующих учетных записей

Создание учетных записей пользователей является одной из самых распространенных задач сетевых администраторов. Новые пользователи часто занимают место уже существующих – переименовать учетную запись работника, переведенного на другое место, проще, чем создавать новую. Для этого достаточно выполнить команду User > Rename в User Manager For Domains. He забудьте предупредить нового работника о том, чтобы он сменил пароль при первом входе, потому что среди прочих параметров будет сохранен и старый пароль.

К сожалению, учетные записи пользователей довольно часто удаляются случайно. Единственный выход из положения – заново создать учетную запись с тем же именем, правами и ограничениями. Сделать это проще, чем кажется потому что вы можете создать шаблоны прав пользователей для отделов и групп. Затем из меню User вы копируете шаблон, переименовываете его для нового пользователя и продолжаете действовать с этой точки, если вам потребуется задать дополнительные права или ограничения.

Если для пользователя были изменены права доступа, этот пользователь должен завершить работу и войти заново – лишь тогда новые права вступят в силу.

# Домены и контроллеры

Домен представляет собой совокупность сетевых рабочих станций и серверов, которая управляется как единая группа. В Windows NT для каждого домена должен существовать контроллер, занимающийся администрированием прав пользователей этого домена. Первый сервер NT, установленный в домене, назначается основным контроллером домена (PDC, Primary Domain Controller). Данный сервер отвечает за проверку пользователей домена во время входа в систему, потому что на PDC находится информация об учетных записях пользователей и безопасности, касающаяся всего домена. Следующий устанавливаемый сервер принимает на себя роль резервного контроллера домена (BDC, Backup Domain Controller). На BDC хранится копия информации об учетных записях пользователей и безопасности домена (через заданные интервалы времени эта копия синхронизируется с PDC). Если PDC по какой-либо причине перестает работать, BDC автоматически не начинает выполнять функции PDC, но пользователи по-прежнему могут входить в сеть. Хотя наличие BDC необязательно, оно в высшей степени желательно.

Если вам по техническим причинам потребуется отключить PDC, BDC можно повысить до PDC вручную. Однако это необходимо сделать до отключения PDC, иначе могут быть потеряны данные учетных записей, которые еще не были скопированы между контроллерами. Изменение роли BDC выполняется с помощью программы Server Manager (Start > Programs > Administrative Tools (Common) > Server Manager):

1. Запустите Server Manager.
2. Откройте меню Computer.
3. Выберите команду Promote To Primary Domain Controller.
4. Подтвердите свое решение.

# Управление локальными и глобальными группами

Без группового администрирования управление пользователями было бы довольно сложной задачей. Основная идея – присваивать права доступа только группам, а затем управлять правами отдельных пользователей, включая или удаляя их из различных групп по мере необходимости. Если следовать этому принципу, вам почти не придется задавать права доступа к ресурсам для отдельных пользователей. Учетным записям пользователей практически не назначаются никакие права – все они наследуются от групп, к которым принадлежат пользователи.

Хороший подход к реализации безопасности пользователей в NT заключается в том, чтобы создать группу для каждого ресурса в сети. Для каждого ресурса будет существовать группа, управляющая доступом к нему. После создания таких групп вам придется в основном управлять группами и их членами, а не конкретными ресурсами.

В Windows NT существует два вида групп: локальные и глобальные. Локальные группы доступны лишь в локальном домене; глобальные группы распространяются за пределы доменов. Другое важное отличие заключается в том, что локальные группы могут содержать и пользователей, и другие группы, тогда как глобальные группы содержат только пользователей. Никакие локальные или глобальные группы не могут входить в другую глобальную группу.

Итак, если вы хотите предоставить домену Engineering доступ к цветному принтеру в домене Marketing, следует создать глобальную группу (например, EngnrPrint) и разрешить ей доступ к принтеру. Снова обратите внимание: тот факт, что домен Marketing доверяет глобальной группе EngnrPrint доступ к цветному принтеру, вовсе не означает, что один домен обладает какими-либо дополнительными правами для ресурсов другого домена, если такие права не были специально заданы.

Как упоминалось выше, в NT существует несколько встроенных локальных и глобальных групп, которым по умолчанию назначаются определенные привилегии. В табл. 1 перечислены эти группы (локальные и глобальные) вместе со стандартными членами и описаниями.

**Таблица 1.** Встроенные группы в Windows.

|  |  |  |  |
| --- | --- | --- | --- |
| Название группы | Стандартные члены | Локальная/ глобальная | Описание |
| Account Operators (операторы учетных записей) | Нет | Локальная | Члены группы могут администрировать учетные записи пользователей и групп |
| Administrators (администраторы) | Администраторы домена, Администратор | Локальная | Члены группы обладают неограниченными возможностями администрирования компьютер/домен |
| Backup Operators (операторы архива) | Нет | Локальная | Члены группы имеют доступ с целью архивации файлов |
| Domain Admins (администраторы домена) | Администратор | Глобальная | Назначенные администраторы домена |
| Domain Guests (гости домена) | Гость | Глобальная | Все гости домена |
| Domain Users (пользователи домена) | Администратор | Глобальная | Все пользователи домена |
| Guests  (гости) | Гость | Локальная | Пользователи, которым был предоставлен доступ к компьютеру/домену |
| Everyone  (Все) | Все | Глобальная/ локальная | Все пользователи |
| Print Operators (операторы печати) | Нет | Локальная | Члены группы могут администрировать принтеры домена |
| Replicators (репликаторы) | Нет | Локальная | Поддержка репликации файлов в домене |
| Server Operators (операторы сервера) | Администратор | Локальная | Члены группы могут администрировать серверы домена |
| Users  (пользователи) | Пользователи домена | Локальная | Обычные пользователи |

Кроме того, каждая группа обладает определенным типом доступа на уровне каталогов:

1. Full Control (Полный доступ) – пользователи могут добавлять, читать и изменять файлы, изменять разрешения для каталогов и становиться владельцами каталогов и файлов.
2. List (Право просмотра) – пользователи могут получать списки файлов и подкаталогов данного каталога.
3. Read (Право чтения) – пользователи могут читать файлы и запускать приложения из каталога.
4. Add (Право добавления) – пользователи могут добавить в каталог новые файлы, но не могут изменить их.
5. Add & Read (Право добавления и чтения) – пользователи могут добавлять и читать файлы в каталоге, но не могут их изменять.
6. Change (Право изменения) – пользователи могут добавлять, читать и изменять содержимое файлов каталога.
7. No Access (Нет доступа) – пользователи не могут обратиться к каталогу (даже если они являются членами других групп, которым такой доступ разрешен).

Когда пользователь принадлежит нескольким группам домена, приоритетным является право с минимальными ограничениями. Например, если пользователь имеет полный доступ для одной группы и право чтения – для другой, то в результате он будет иметь привилегии полного доступа.

# О политиках, профилях и сценариях входа

Существует несколько способов определения параметров сетевых пользователей. Настройка такого рода в Windows NT осуществляется с помощью различных политик, профилей и сценариев входа, описанных в следующих разделах.

## Системные политики

Системная политика определяет состояние окружения и возможные действия пользователя. Для создания и администрирования системных политик используется программа System Policy Editor (Start > Programs > Administrative Tools (Common) > System Policy Editor).

С помощью System Policy Editor можно выбрать программы, отображаемые в панели управления пользователя, настроить вид его рабочего стола, указать сетевые параметры, определить параметры входа в сеть и права доступа, а также настроить содержимое меню Start для данного пользователя.

Вы можете определить стандартную системную политику для всех пользователей домена или же назначить разные политики для отдельных пользователей, компьютеров и групп. При создании системных политик изменяется содержимое системного реестра для компьютеров или пользователей – точнее, реестр изменяется для текущего пользователя и локального компьютера.

Чтобы определить системную политику в качестве стандартной, сохраните ее в каталоге \WinNT\System32\Repl\Export\Scripts под именем NTCONFIG.POL. Файлы этого каталога дублируются на другие NT-серверы и рабочие станции, участвующие в репликации. Скопированные файлы хранятся в каталоге \WinNT\System32\Repl\Import\ Scripts. При определении системной политики в System Policy Editor выбирается один из двух режимов: режим реестра (Registry mode) или файловый режим (Policy File mode). Для этого сделайте следующее:

1. Откройте меню File в System Policy Editor.
2. Выберите одну из двух команд: Open Policy или Open Registry. Команда Open Policy позволяет изменить существующую политику. Команда Open Registry приводит вас к разделам системного реестра для локального компьютера и локального пользователя. Внесите необходимые изменения прямо в реестр и сохраните их.

Непосредственная модификация реестра грозит нарушить целостность системы. При повреждении некоторых областей реестра NT перестает загружаться. Перед тем как вносить изменения в реестр, всегда создавайте его резервную копию и действуйте очень осторожно.

## Профили

Профили пользователей применяются для создания и управления нестандартными конфигурациями рабочего стола отдельных пользователей. В профиль пользователя входят такие параметры, как тип заставки, сетевые соединения, оформление рабочего стола, настройки мыши и программные группы. Профили могут создаваться как для пользователей, так и для групп. Профили пользователей находятся в каталогах WINNT\Profiles\<ИМЯ-ПОЛЬЗОВАТЕЛЯ>.

Профили защищают ваши сетевые ресурсы от пользователей, а пользователей – от самих себя. Профили пригодятся в тех случаях, когда сетевые пользователи удаляют или перемещают команды меню и группы. Заставляя пользователей держаться в рамках профиля, вы создаете неизменяемый, последовательный пользовательский интерфейс; это сокращает затраты на сопровождение и бережет нервы пользователей.

Вы можете заставить пользователя использовать конкретный профиль – для этого следует создать обязательный профиль пользователя (Mandatory User Profile), который не может быть изменен или сохранен пользователем. Чтобы создать обязательный профиль, создайте перемещаемый профиль, скопируйте его в общий каталог, предоставьте доступ к нему соответствующим пользователям, переименуйте файл NTUSER.DAT в NTUSER.MAN и введите UNC-путь к профилю в диалоговом окне User Profile Path, которое вызывается из окна User Environment Profile для каждого пользователя.

Иногда при сбоях PDC пользователь при входе в систему не получает обязательного профиля. Когда это происходит, Windows NT находит последний локальный кэшированный профиль данного пользователя или стандартный профиль, присвоенный его рабочей станции. Локальный кэшированный профиль используется в том случае, если пользователь в прошлом успешно регистрировался в домене. Если же пользователь никогда не регистрировался в домене, используется стандартный профиль.

Перемещаемый профиль создается так:

1. Скопируйте профиль пользователя с рабочей станции в общий сетевой каталог.
2. Откройте панель управления и дважды щелкните на значке System.
3. Выберите профиль пользователя, выполните команду Сору То и введите полный UNC-путь к серверу, на котором будет находиться профиль.
4. В диалоговом окне User Profile введите полный UNC-путь к профилю в поле User Profile Path.

В профиль пользователя также можно включить выбор основного каталога пользователя. Чтобы сделать это для существующей учетной записи, которая в данный момент имеет локальный основной каталог, необходимо выполнить следующие действия:

1. Выполнить команду Connect в диалоговом окне User Environment Profile из программы User Manager.
2. Выбрать общий диск и ввести полный UNC-путь к новому основному каталогу пользователя. Полный UNC-путь включает имя сервера, на котором находится основной каталог (имя домена указывать не нужно). Переменная %НОМЕРАТН% содержит UNC-путь к основному каталогу пользователя лишь после того, как новый каталог будет задан.

Если ваши пользователи часто и/или неразумно меняют свою конфигурацию, создайте профили и заставьте пользователей придерживаться заданных параметров. Хотя такие ограничения могут раздражать пользователей, это лучший способ оградить всех от неприятностей.

## Сценарии входа

Если задуматься над тем, сколько разнообразных средств и возможностей пользовательской конфигурации существует в Windows NT, существование сценариев входа выглядит довольно странно. Тем не менее по нескольким причинам сценарии входа необходимы для обеспечения обратной совместимости. Во-первых, профили пользователей работают только на компьютерах с NT, а для DOS-клиентов используют сценарии входа для обеспечения последовательных сетевых соединений. Кроме того, если в вашей сети все еще остались старые серверы LAN Manager, сценарии входа обеспечивают совместимость с этими серверами для всех клиентов.

Кроме того, параметры подключения пользователя к сети или сетевому принтеру можно задать и без тщательно спланированной системы профилей. Если вы определили личные профили пользователей и хотите добавить к ним единые параметры сетевых соединений, сценарии входа справятся и с этой задачей. Наконец, если вы не хотите тратить время на разработку сложной последовательной системы профилей, сценарии входа являются простой и удобной альтернативой.

Сценарии входа помогают настроить окружение пользователя, не управляя всеми его аспектами. Для сохранности вы должны экспортировать сценарии входа с PDC на все BDC сети. В этом случае при выходе из строя PDC копия сценариев останется на BDC и будет доступна пользователям при входе. Сценарии входа не требуется экспортировать на каждую рабочую станцию. Экспортируемые файлы всегда следует помещать в подкаталоги каталога Winnt\System32\Repl\Export. По умолчанию для экспортирования сценариев входа на PDC используется каталог Winnt\System32\Repl\Export\Scripts.

# Задания для выполнения

1. По полученному у преподавателя заданию спланировать клиентов и группы.
2. Объяснить спланированную структуру.
3. Для созданных пользователей изменить с помощью System Policy Editor политики.

# Контрольные вопросы

1. Для чего предназначена программа User Manager for Domains?
2. В чем отличие между конкретным пользователем и группой?
3. Можно ли удалить встроенную группу?
4. В чем разница между локальными группами и глобальными?
5. Какие ограничения можно наложить на профиль пользователя?
6. Зачем нужны сценарии входа?
7. Где хранятся профили пользователей?
8. Для чего нужна программа System Policy Editor?
9. Что означает тип доступа NO ACCESS?