MCSE

Training Kit

Exam 70-217

Microsoft®

Windows 2000 Active Directory® Services

Microsoft Press

Учебный
курс
MCSE

Сертификационный экзамен 70-217

Microsoft®

Windows 2000 Active Directory® Services

Официальное пособие Microsoft для самостоятельной подготовки

3-е издание, исправленное

Москва 2004

РУССКАЯ РЕДАКЦИЯ

УДК 004
ББК 32.973.26-018.2
М59

Microsoft Corporation

М59 Microsoft Windows 2000 Active Directory Services. Учебный курс MCSE: Пер. с англ. - 3-е изд., испр. — М.: Издательско-торговый дом «Русская Редакция», 2004. — 608 стр.: ил.

ISBN 5-7502-0247-X

Эта книга посвящена работе службы каталогов Active Directory. Вы научитесь планировать, настраивать и администрировать инфраструктуру Active Directory и систему доменных имен (Domain Name System, DNS). Вы узнаете об использовании Active Directory для централизованного управления пользователями, группами, общими папками и сетевыми ресурсами, об администрировании среды пользователя и программного обеспечения средствами групповой политики, о порядке внедрения, об устранении проблем с безопасностью, а также о мониторинге и оптимизации производительности Active Directory.

Учебный курс адресован профессионалам в области информационных систем, которые занимаются установкой, настройкой, контролем и сопровождением Microsoft Windows 2000, а также тем, кто хочет подготовиться к сертификационному экзамену по программе MCSE 70-217: *Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure*.

Издание состоит из 15 глав, двух приложений и предметного указателя.

УДК 004
ББК 32.973.26—018.2

Подготовлено к изданию по лицензионному договору с Microsoft Corporation, Редмонд, Вашингтон, США.

ISBN 0-7356-0999-3 (англ.)
ISBN 5-7502-0247-X

Содержание

06 этой книге

Мы рады представить вам учебный курс MCSE — «Microsoft Windows 2000 Active Directory Services». Он посвящен установке, настройке, администрированию, мониторингу, поиску и устранению неполадок в Microsoft Windows 2000 Active Directory.

Вы познакомитесь со службой каталогов Active Directory и научитесь планировать, настраивать и администрировать ее инфраструктуру, настраивать *систему доменных имен* (Domain Name System, DNS) для управления разрешением имен, а также схему и репликацию. Вы узнаете об использовании Active Directory для централизованного управления пользователями, группами, общими папками и сетевыми ресурсами, об администрировании пользовательского окружения и программного обеспечения средствами групповой политики, о порядке внедрения и устранении неполадок защиты службы каталогов, а также о способах наблюдения и оптимизации производительности Active Directory. Вы изучите удаленную установку Windows 2000 при помощи *служб удаленной установки* (Remote Installation Services, RIS).

Данный курс входит в программу сертификации системных инженеров Microsoft.

Примечание О программе сертификации MCSE см. далее раздел «Программа сертификации специалистов Microsoft».

Главы учебника подразделяются на занятия, большинство которых содержат упражнения, предназначенные для демонстрации излагаемых методов и приобретения практических навыков. Каждое занятие заканчивается кратким обобщением материала — «Резюме», а глава — вопросами, которые помогут вам определить, насколько вы усвоили материал.

В разделе «Начало работы» вводной главы книги перечислены конкретные требования к аппаратуре, программному обеспечению и параметрам сетевой конфигурации, необходимые для освоения материала и выполнения практических заданий курса. Внимательно прочитайте его, прежде чем приступать к материалам учебного курса.

Кому адресована эта книга

Данный курс адресован тем, кто занимается установкой, настройкой, контролем и сопровождением Microsoft Windows 2000 Active Directory, а также тем, кто желает сдать сертификационный экаамен MCSE 70-217: *Implementing and Administering Microsoft a Windows 2000 Directory Services Infrastructure*.

Для изучения данного курса необходимо:

- знать основы современных сетевых технологий;
- знать Microsoft Windows 2000 Server в объеме соответствующего курса MSCE.

Справочные материалы

К ним относятся:

- официальные документы по Windows 2000, доступные в сети Интернет по адресуhttp://www.microsoft.com/windows/server/;
- справочная система Windows 2000 Server;
- справочная система средств поддержки (доступна после их установки);
- документация Windows 2000 Server Resource Kit.

Соглашения, принятые в учебном курсе

В этом разделе мы расскажем о терминологии и обозначениях, принятых в учебнике.

Структура книги

- Каждая глава начинается с раздела «В этой главе», содержащего краткий обзор обсуждаемых тем.
- Главы состоят из занятий, большинство из которых содержат упражнения. Выполнив их, вы закрепите изученный материал и приобретете практические навыки. Упражнения отмечены значком на полях.

Внимание! Большинство упражнений курса являются продолжением упражнений из предыдущих глав. Поскольку состояние системы на тестовом компьютере в ходе выполнения практических занятий изменяется, вероятно, вам не удастся выполнить упражнение из середины курса, если вы не выполнили предыдущих.

- Каждую главу завершает раздел «Закрепление материала», вопросы которого помогут вам проверить, насколько твердо вы усвоили материал.
- Приложение А «Вопросы и ответы» содержит вопросы всех глав книги и ответы на них.

О примечаниях

Практически во всех главах встречаются примечания разных видов.

- Совет — поясняет возможный результат или описывает альтернативный метод решения задачи.
- Внимание! — предупреждает о возможной потере данных или содержит сведения, необходимые для выполнения поставленной задачи.
- **Примечание** — содержит дополнительную информацию.

Обозначения

- **Вводимые вами символы или команды набраны строчными буквами полужирного начертания.**
- *Курсив* в операторах указывает, что в этом месте вы должны подставить собственные значения. Кроме того, курсивом выделены новые термины и понятия, а также рекомендуемые дополнительно источники информации.
- Имена файлов, папок и каталогов начинаются с Прописных Букв (за исключением имен, которые вы задаете сами). Кроме особо оговоренных случаев, для ввода имен файлов и каталогов в диалоговом окне или в командной строке вы можете использовать строчные буквы.
- Названия элементов интерфейса для русифицированной версии даются в скобках после английских названий.
- Расширения имен файлов набраны строчными буквами.
- Аббревиатуры напечатаны ПРОПИСНЫМИ БУКВАМИ.

- Примеры кола, текста, выводимого на экран, и текста, вводимого в командной строке, выделены моноширинным шрифтом (все его символы имеют одинаковую ширину).
- Необязательные элементы операторов заключены в квадратные скобки []. Например [*имя_файла*] *в* синтаксисе команды означает, что после команды можно указать имя файла. Сами скобки вводить НЕ надо.
- Обязательные элементы операторов заключены в фигурные скобки {}. Сами скобки вводить НЕ надо.
- Некоторые разделы помечены значками.

Значок	Описание
	Упражнение для закрепления навыков, приобретенных при изучении материала
	Этим значком отмечены разделы «Закрепление материала» в конце каждой главы. Ответы см. в приложении А «Вопросы и ответы»

Комбинации клавиш клавиатуры

- Знак «+» между названиями клавиш означает, что их следует нажать одновременно. Например, выражение «Нажмите Alt+Tab» обозначает, что, удерживая нажатой клавишу Alt, нужно нажать клавишу Tab.
- Запятая между названиями клавиш означает их последовательное нажатие. Например, выражение «Нажмите Alt, F, X» означает, что надо последовательно нажать и отпустить указанные клавиши. Если же указано «Нажмите Alt+W, L», то сначала следует нажать клавиши Alt и W вместе, потом отпустить их и нажать клавишу L.
- Команды меню можно подавать с клавиатуры. Для этого нажмите клавишу Alt (чтобы активизировать меню), а затем последовательно — выделенные или подчеркнутые буквы в названиях нужных разделов меню или команд. Кроме того, некоторым командам сопоставлены комбинации клавиш клавиатуры (они указаны в меню).
- Флажки и переключатели также можно включать и снимать с клавиатуры. Для этого достаточно нажать Alt, а затем клавишу, соответствующую подчеркнутой букве в названии флажка или переключателя. Кроме того, нажимая клавишу Tab, вы можете сделать зону нужного параметра активной, а затем включить или снять выбранный флажок или переключатель, нажав клавишу «пробел».
- Работу с диалоговым окном всегда можно прервать, нажав клавишу ESC.

Обзор глав и приложений

Задача курса — помочь вам научиться устанавливать, настраивать, администрировать, контролировать и обслуживать Active Directory Windows 2000. Курс предполагает самостоятельную работу, включает занятия, упражнения и проверочные вопросы. Он рассчитан на последовательное изучение, но это не значит, что вы не можете работать с интересующими вас главами в произвольном порядке (дополнительная информация содержится в следующем разделе «С чего начать»). В этом случае советуем обращать внимание на раздел «Прежде всего» в начале каждой главы, где указаны предварительные требования для выполнения упражнений.

Итак, краткое содержание глав и приложений учебного курса.

- В разделе «Об этой книге» собраны сведения о содержании учебника и данные о структурных единицах и условных обозначениях, принятых в нем. Внимательно прочитайте его: это поможет вам эффективно работать с материалами курса, а также выбрать интересующие вас темы. Здесь также описана установка Microsoft Windows 2000 Server — эта ОС понадобится вам для выполнения упражнений данного курса.

- Глава 1 «Знакомство с Microsoft Windows 2000» содержит обзор возможностей Windows 2000. Вы узнаете о ее архитектуре и службах каталогов Windows 2000.
- Глава 2 «Введение в Active Directory» познакомит вас с компонентами Active Directory, — объектами, доменами, организационными подразделениями (ОП), деревьями и лесами. Также мы расскажем о концепциях Active Directory, в том числе о глобальном каталоге, репликации, доверительных отношениях, пространстве имен DNS и правилах именования.
- Глава 3 «Задачи и средства администрирования Active Directory» посвящена основным задачам администрирования Active Directory — настройке, администрированию пользователей и групп, защите сетевых ресурсов, администрированию рабочей среды пользователя, аудиту и наблюдению ресурсов и событий. Также в главе рассказывается о средствах администрирования Active Directory, включая консоль управления (Microsoft Management Console, MMC) и Task Scheduler (Диспетчер задач).
- В главе 4 «Внедрение Active Directory» описано поэтапное сопровождение Active Directory, состоящее из планирования, установки, определения ролей хозяина операций и внедрения структуры ОП.
- В главе 5 «Взаимодействие DNS и Active Directory» обсуждается разрешение имен и зоны DNS, а также устранение неполадок в конфигурации DNS и Active Directory. В практической части описана настройка зон, их репликация и передача.
- Глава 6 «Настройка сайтов» посвящена настройке параметров сайта, межсайтовой репликации, а также устранению неполадок межсайтовой репликации.
- Глава 7 «Управление учетными записями пользователей» посвящена учетным записям пользователей и их планированию. Описываются способы создания и настройки параметров домена, локальных учетных записей пользователей, создание профилей пользователей и домашних каталогов. Также обсуждается порядок обслуживания ученых записей пользователей, их отключение, включение, переименование, удаление, разблокирование и смена паролей.
- В главе 8 «Управление учетными записями групп» рассказывается о стратегии планирования групп и порядке их создания, а также о встроенных в Windows 2000 группах и группах, включающих администраторов.
- Глава 9 «Безопасность сетевых ресурсов» посвящена папкам и разрешениям доступа к файлам в файловой системе NTFS. Вы научитесь назначать разрешения NTFS папкам и файлам для учетных записей пользователей и групп, а также узнаете, как перемещение или копирование файлов и папок влияет на эти разрешения. В конце главы описано решение типичных проблем доступа к ресурсам.
- В главе 10 «Администрирование общих папок» рассказывается об общих папках и их планировании. Обсуждается процесс предоставления обшего доступа к папкам и их зашита с помощью разрешений, а также установка распределенной файловой системы (DFS) Mcrosoft для предоставления пользователям удобного доступа к общим папкам, размещенным в сети.
- В главе 11 «Администрирование Active Directory» описаны задачи администрирования Active Directory, включая поиск объектов, назначение им разрешений, публикацию ресурсов, перенос объектов в пределах и между доменами, делегирование административного управления в ОП, резервное копирование, восстановление и устранение неполадок Active Directory.
- В главе 12 «Администрирование групповой политики» рассказывается о концепциях групповой политики и ее планировании. Описывается процесс внедрения групповой политики, управление с ее помощью программным обеспечением и специальными папками, а также последовательность устранения неполадок, связанных с групповой политикой.
- В главе 13 «Администрирование конфигурации безопасности» обсуждается использование параметров безопасности для определения конфигурации безопасности системы, включая аудит, журналы безопасности, права пользователей, шаблоны безопасно-

сти и утилиту Security Configuration and Analysis. В конце главы рассказывается об устранении неполадок конфигурации безопасности.

- Глава 14 «Управление производительностью Active Directory» посвящена средствам мониторинга производительности, поддержки и мониторинга общих папок.
- В главе \5 «Установка Windows 2000 с использованием RIS» рассказывается о службах удаленной установки (RIS). Поэтапно описано сопровождение и администрирование RIS. В конце главы приведены ответы на часто задаваемые вопросы и информация об устранении неполадок, связанных с RIS.
- В приложении А «Вопросы и ответы» приведены ответы на вопросы из упражнений и разделов «Закрепление материала» всех глав учебного курса.
- Приложение Б «Установка и настройка службы DHCP» содержит основные инструкции по установке и настройке службы **DHCP** для подготовки к использованию **RIS.**

С чего начать

Данный курс предназначен для самостоятельного изучения, поэтому вы можете пропускать некоторые занятия, чтобы вернуться к ним потом. Помните, что для выполнения упражнений курса необходимо выполнить процедуру установки, описанную в этой главе. Чтобы определить, с чего начать изучение курса, обратитесь к следующей таблице.

Если Вы	Что делать
готовитесь к сдаче сертификационного экзамена 70-217: *Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure*	см. раздел «Начало работы», а также описание процедур установки далее в этой главе. Затем изучите все материалы этого курса
хотите изучить информацию по определенной теме экзамена	см. раздел «Материалы для подготовки к экзаменам».

Материалы для подготовки к экзаменам

В следующих таблицах перечислены темы сертификационного экзамена 70-217: *Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure* и главы настоящего учебного курса, где обсуждаются соответствующие вопросы.

Примечание Конкретная программа любого экзамена определяется компанией Microsoft и может быть изменена без предварительного уведомления.

Установка, настройка и устранение неполадок Active Directory

Тема	Где обсуждается	
	Глава	Занятие
Установка, настройка и устранение неполадок Active Directory		
Установка Active Directory	4	2
Создание сайтов	6	1
Создание подсетей	6	1
Создание связей между сайтами	6	1
Создание мостов связей сайтов	6	2
Создание объектов подключений	6	2

(продолжение)

Тема	Где обсуждается Глава	Занятие
Установка, настройка и устранение неполадок компонентов Active Directory		
Создание серверов глобального каталога	6	4
Перенос объектов сервера между сайтами	6	4
Перенос ролей хозяина операций	4	3
Проверка установки Active Directory	4	1
Внедрение структуры ОП	4	4
Резервное копирование и восстановление Active Directory		
Принудительное восстановление Active Directory	11	6
Восстановление системы после сбоя	11	7

Установка, настройка, управление, мониторинг и устранение неполадок DNS

Тема	Где обсуждается Глава	Занятие
Установка, настройка, управление, **мониторинг и устранение неполадок DNS**		
Объединение Active Directory DNS с альтернативными DNS	5	2, 4
Настройка зон для динамического обновления	5	2, 4
Управление, **мониторинг и устранение неполадок DNS**		
Управление репликацией данных DNS	5	3, 4

Установка, настройка, управление, мониторинг, оптимизация и устранение неполадок при управлении конфигурацией

Тема	Где обсуждается Глава	Занятие
Внедрение и устранение неполадок групповой политики		
Создание объектов групповой политики (ОГП)	12	3, 6
Привязка существующего ОГП	12	3, 6
Делегирование административного управления групповой политикой	12	3, 6
Изменение наследования групповой политики	12	3, 6
Фильтрование параметров групповой политики путем сопоставления ОГП группам безопасности	12	3, 6
Настройка групповой политики	12	3, 6
Управление и устранение неполадок среды пользователя средствами групповой политики		
Управление средой пользователя средствами административных шаблонов	12	3, 6
Назначение пользователям и компьютерам политики сценариев	12	3, 6

(продолжение)

Тема •	Где обсуждается Глава	Занятие
Управление и устранение неполадок программного обеспечения средствами групповой политики		
Развертывание ПО средствами групповой политики	12	4
Обслуживание ПО средствами групповой политики	12	4
Настройка параметров развертывания	12	4
Решение типичных проблем развертывания ПО	12	6
Управление конфигурацией сети средствами групповой политики	12	5
Развертывание Windows 2000 средствами RIS		
Установка образа на компьютер-клиент RIS	15	2
Создание загрузочного диска RIS	15	2
Настройка параметров удаленной установки	15	2
Устранение неполадок RIS	15	4
Управление образами для выполнения удаленных установок	15	3
Настройка безопасности RIS		
Авторизация сервера RIS	15	3
Предоставление прав на создание учетной записи компьютера	15	3
Предварительная подготовка компьютеров-клиентов RIS для дополнительной безопасности и балансировки нагрузки	15	3

Управление, мониторинг и оптимизация компонентов Active Directory

Тема	Где обсуждается Глава	Занятие
Управление объектами Active Directory		
Перенос объектов Active Directory	11	4
Публикация ресурсов в Active Directory	11	3
Поиск объектов в Active Directory	11	1
Создание и управление учетными записями вручную или при помощи сценариев	8	3, 4, 5 3, 4, 5
Управление доступом к объектам Active Directory	11	2
Делегирование административного управления объектами в Active Directory	11	5
Управление производительностью Active Directory		
Мониторинг, поддержка и устранение неполадок производительности контроллера домена	14	1, 2, 3
Мониторинг, поддержка и устранение неполадок компонентов Active Directory	14	1, 2, 3
Управление и устранение неполадок репликации Active Directory		
Управление межсайтовой репликацией	6	K 2, 3
Управление внутрисайтовой репликацией	6	1, 3

(окончание)

Настройка, управление, мониторинг и устранение неполадок безопасности Active Directory

Тема	Где обсуждается	
	Глава	Занятие
Настройка и устранение неполадок безопасности в инфраструктуре службы каталогов		
Применение политик безопасности средствами групповой политики	13	1, 3, 4, 7
Создание, анализ и модификация конфигураций безопасности при помощи оснастки Security Configuration and Analysis и шаблонов безопасности	13	5, 6, 7
Внедрение политики аудита	13	2, 7
Мониторинг и анализ событий безопасности	13	3

Начало работы

Данный курс предназначен для самостоятельного изучения и содержит упражнения и практические рекомендации, которые помогут вам освоить Windows 2000 Active Directory.

Для выполнения большинства упражнений вам потребуется один компьютер с Windows 2000 Server. Однако некоторые упражнения требуют наличия двух компьютеров; для лучшего понимания материала курса постарайтесь их не пропустить. Если у вас нет возможности раздобыть второй компьютер, прочитайте пункты упражнения и попытайтесь понять логику действий.

Для изучения этого курса рекомендуется выделить отдельную сеть, чтобы не нарушать работу сети вашего предприятия и пользователей вашего домена. Тем не менее вы можете выполнять упражнения и в существующей сети.

Внимание! Для выполнения некоторых упражнений потребуется изменить конфигурацию серверов. Если вы подключены к большой сети, это может привести к нежелательным результатам. Перед выполнением таких упражнений предварительно проконсультируйтесь с сетевым администратором.

Аппаратное обеспечение

Компьютер должен соответствовать приведенной далее минимальной конфигурации, а установленное на нем оборудование необходимо выбрать из списка совместимых с Windows 2000 устройств (Hardware Compatibility List, HCL):

- 32-разрядный процессор Pentium с частотой не менее 166 МГц;
- не менее 64 Мб оперативной памяти для сети с числом клиентских компьютеров от одного до пяти (для большинства сетей рекомендуется 128 Мб);
- жесткий диск с 2 Гб свободного пространства;
- 12-скоростной привод CD-ROM (для установки Windows 2000 по сети привод CD-ROM не требуется);
- монитор SVGA с разрешением 800 x 600 (рекомендуется 1024 x 768);
- дисковод для дискет 3,5-дюйма (если ваш привод CD-ROM не поддерживает загрузку и вы не можете запустить с него программу установки);
- мышь Microsoft или другое совместимое устройство.

Программное обеспечение

Для выполнения практических заданий вам потребуется установочный компакт-диск Microsoft Windows 2000 Server. Пробную версию Windows 2000 Server и инструкции по загрузке можно найти на Web-узле Microsoft по адресу: http://www.microsoft.com/windows 2000/downloads/default.asp (материалы по Windows 2000 на русском языке: http://www microsoft.com/rus/windows2000).

Подготовка компьютера к выполнению практических заданий

Ниже описаны основные этапы подготовки вашего компьютера к выполнению заданий этого курса. Если ранее вы не устанавливали Windows 2000 или другую сетевую ОС, обратитесь к опытному сетевому администратору. После выполнения каждого этапа отметьте галочкой соответствующую строку. Подробные инструкции для выполнения каждого этапа описаны ниже. Итак, кратко:

- создайте установочные дискеты Windows 2000 Server;
- запустите программу установки Windows 2000 Server;
- установите сетевые компоненты;
- установите аппаратное обеспечение.

Примечание Далее рассказано, как установить Windows 2000. Это поможет вам подготовить компьютер для выполнения заданий этой книги. Однако обучение установке не входит в цели данного курса. Подробнее об установке Windows 2000 Server рассказано в учебном курсе MSCE, посвященном Microsoft Windows 2000 Server.

Установка Windows 2000 Server

Для выполнения упражнений этого курса необходимо установить Windows 2000 Server. Компьютер, предназначенный для этого, не должен содержать форматированных разделов. Раздел на жестком диске для установки Windows 2000 Server в качестве изолированного сервера рабочей группы можно создать непосредственно в процессе установки Windows 2000 Server.

Для выполнения приведенных ниже инструкций на вашем компьютере должна быть установлена MS-DOS или любая версия Windows, причем умеющая обращаться к каталогу Bootdisk установочного компакт-диска с Windows 2000 Server. Если ваш компьютер настроен для загрузки с CD-ROM, вы можете установить Windows 2000, не используя установочные дискеты. В этом случае в BIOS надо отключить поддержку загрузки с CD- ROM.

Внимание! Для выполнения этой процедуры потребуются четыре дискеты емкостью 1,44 Мб каждая. Запись на дискеты выполняется поверх уже имеющихся данных; при этом соответствующего предупреждения вы не получите.

► Создание установочных дискет Windows 2000 Server

1. Наклейте на четыре пустые отформатированные дискеты емкостью 1,44 Мб наклейки со следующими надписями:
   - «Установочный диск Windows 2000 Server №1»;
   - «Установочный диск Windows 2000 Server №2»;
   - «Установочный диск Windows 2000 Server №3»;
   - «Установочный диск Windows 2000 Server №4».
2. Вставьте установочный компакт-диск для Microsoft Windows 2000 Server в привод CD- ROM.

3. Если появится сообщение Windows 2000 CD-ROM с запросом на установку или обновление операционной системы до Windows 2000, щелкните кнопку No.
4. Откройте окно командной строки.
5. Введите букву привода CD-ROM в командную строку и нажмите Enter.
6. Сделайте активным каталог Bootdisk, введя в командную строку **cd bootdisk**, и нажмите Enter.
7. Если на компьютере, на котором вы создаете загрузочные дискеты, установлена MS-DOS, 16-разрядная версия Windows, Windows 95 или Windows 98, введите в командной строке **makeboot** a: (где a: — имя вашего дисковода) и нажмите Enter. Если на компьютере установлена Windows NT или Windows 2000, введите makebt32 a: (где a: — имя вашего дисковода) и нажмите Enter. Появится сообщение, что будут созданы четыре установочные дискеты для Windows 2000, для чего вам необходимо приготовить четыре пустых отформатированных гибких дискеты высокой плотности.
8. Нажмите любую клавишу для продолжения. Появится сообщение, что нужно вставить в дисковод дискету, на которую будет записана установочная информация.
9. Вставив в дисковод пустую отформатированную дискету, надписанную «Установочный диск Windows 2000 Server № 1» и нажмите любую клавишу. После создания образа диска Windows 2000 попросит вас поочередно вставить вторую, третью и четвертую дискеты.
10. В командной строке введите exit и нажмите Enter.

Выньте дискету из дисковода и компакт-диск из привода CD-ROM.

► Запуск программы установки Windows 2000 Server

Примечание При описании этой процедуры предполагается, что на вашем компьютере не установлена ОС, жесткий диск не разбит на разделы, а поддержка загрузки с CD-ROM отключена.

---

1. Вставьте дискету, надписанную «Установочный диск Windows 2000 Server № 1» и загрузочный диск Windows 2000 Server и перезагрузите компьютер.

   После перезапуска компьютера появится сообщение, что выполняется проверка вашей системной конфигурации. Вскоре после этого откроется окно Windows 2000 Setup.

   Обратите внимание на серую строку внизу экрана. В ней сообщается, что выполняется проверка компьютера и загрузка Windows 2000 Executive — минимальной версии ядра Windows 2000.
2. Вставьте в дисковод дискету №2 (когда увидите соответствующее сообщение) и нажмите Enter.

   Setup произведет загрузку HAL, шрифтов, драйверов шины и других программ, обеспечивающих работу материнской платы, шины и других аппаратных средств вашего компьютера. Кроме того, будут загружены исполнимые файлы Windows 2000 Setup.
3. Вставьте в дисковод дискету №3 (когда увидите соответствующее сообщение) и нажмите Enter.

   Setup произведет загрузку драйверов контроллера дисковода и инициализацию драйверов, обеспечивающих поддержку доступа к дисководу. Во время этого процесса Setup может несколько раз останавливаться.
4. Вставьте в дисковод дискету №4 (когда увидите соответствующее сообщение) и нажмите Enter.

   Будут загружены драйверы периферийных устройств, например драйвер дисковода и файловых систем, после чего произойдет инициализация Windows 2000 Executive и загрузка оставшихся установочных файлов.

   Если вы устанавливаете пробную версию Windows 2000, программа установки предупредит вас об этом.

5. Прочитав сообщение Setup, нажмите Enter.
   Заметьте, что программа установки позволяет вам произвести не только первоначальную установку, но и восстановить поврежденную версию Windows 2000.
6. Прочитайте сообщение, содержащееся в окне Welcome To Setup, и нажмите Enter для продолжения установки. Откроется окно License Agreement (Лицензионное соглашение),
7. Прочитайте лицензионное соглашение. Для прокрутки текста пользуйтесь клавишей Page Down.
8. Выберите I Accept The Agreement (Я принимаю соглашение), нажав клавишу F8.
   Откроется окно Windows 2000 Server Setup (Установка Windows 2000 Server), где вам предлагается выбрать область диска (или уже существующий раздел) для установки Windows 2000, На этом этапе вы можете создавать и удалять разделы на вашем жестком диске.
   Если ваш жесткий диск ранее не содержал разделов (как предполагается в этом упражнении), то вы увидите на диске неразмеченное пространство.
9. Убедившись, что выбрано Unpartitioned space (Неразмеченное пространство), введите с.
   Появится сообщение, что сейчас будет создан новый раздел, а также указаны минимальный и максимальный возможные размеры этого раздела.
10. Выбрав размер раздела (минимум 2 Гб), нажмите Enter.
    Новый раздел будет назван C: New (Unformatted).

Примечание На этом этапе вы можете создавать и дополнительные разделы на свободном дисковом пространстве. Тем не менее созданием разделов рекомендуется заниматься после установки Windows 2000, используя оснастку Disk Management.

11. Убедившись, что выбран новый раздел, нажмите Enter.
    Появится предложение выбрать файловую систему для нового раздела.
12. Воспользовавшись клавишами управления курсором, выберите Format The Partition Using The NTFS File System (Отформатировать раздел под файловую систему NTFS) и нажмите Enter.
    Setup отформатирует раздел под NTFS, выполнит проверку жесткого диска на наличие ошибок, которые могут повлечь сбои в установке, после чего скопирует файлы на диск. Это займет несколько минут.
    По завершении копирования компьютер будет перезагружен.
13. Выньте установочную дискету из дисковода.

Внимание! Если ваш компьютер настроен для загрузки с CD-ROM и поддержка загрузки с CD-ROM не была отключена в BIOS, то при перезапуске произойдет загрузка именно с него. Это приведет к тому, что программа установки будет запушена с самого начала. В этом случае выньте компакт-диск из привода CD-ROM и перезагрузите компьютер.

14. Программа установки скопирует дополнительные файлы, после чего перезагрузит ваш компьютер и запустит мастер установки Windows 2000.

► Графический режим установки

Примечание С этого момента Setup начинает работать в графическом режиме.

1. В окне мастера установки Windows 2000 щелкните кнопку Next (Далее) для сбора информации о компьютере.

Setup произведет конфигурирование папки и разрешений NTFS для файлов ОС. После этого будет выполнен поиск устройств, подключенных к компьютеру, а также установка и конфигурирование драйверов этих устройств. Это займет несколько минут.

2. Убедившись, что системные и пользовательские параметры и раскладка клавиатуры, указанные в окне Regional Settings (Региональные настройки), соответствуют нужному вам языку и региону, щелкните Next.

Примечание Чтобы изменить региональные параметры после того, как Windows 2000 уже установлена, дважды щелкните значок Regional Options на панели управления.

---

3. Введите ваше имя в поле Name (Имя) и имя вашей организации в поле Organization (Организация), затем щелкните Next.

Примечание Если откроется окно Your Product Key (Ключ продукта), введите в него номер, указанный на желтой наклейке на задней стороне коробки установочного компакт-диска Windows 2000 Server.

Откроется окно Licensing Modes (Режимы лицензирования) с предложением выбрать режим лицензирования. По умолчанию устанавливается режим лицензирования Per Server (На сервер). Setup попросит вас ввести количество приобретенных для этого сервера лицензий.

4. Щелкните переключатель Per Server Number Of Concurrent Connections (Число одновременных соединений для одного сервера) и установите число одновременных соединений равным 5 (для этого введите 5 в соответствующее поле). Далее щелкните Next.

Внимание! Для выполнения упражнений курса рекомендуется выбрать параметр Per Server Number Of Concurrent Connections и задать число одновременных подключений равным 5. Тем не менее число одновременных соединений не должно превышать количества имеющихся у вас лицензий. Вы можете также использовать режим лицензирования Per Seat вместо Per Server.

Откроется окно Computer Name And Administrator Password (Имя компьютера и административный пароль). Обратите внимание, что имя компьютера сгенерировано на основе имени вашей организации.

5. В поле Computer Name (Имя компьютера) введите **server**1.

Вы увидите имя компьютера. Оно состоит из прописных букв вне зависимости от того, использовали ли вы при вводе строчные или прописные буквы.

Внимание! Если ваш компьютер подключен к сети, для задания имени компьютера обратитесь к администратору.

На протяжении всего курса учебный компьютер в вопросах и упражнениях будет обозначаться именем Server1. Если вы назвали свой сервер по-другому, вместо имени Server1 подставляйте имя вашего сервера.

6. В поля Administrator Password (Пароль администратора) и Confirm Password (Подтверждение пароля) введите строчными буквами password и щелкните кнопку Next. Пароль чувствителен к регистру, поэтому убедитесь, что слово password набрано именно строчными буквами.

Для изучения этого курса пароль администратора password вполне подходит. В реальных ситуациях для пароля администратора рекомендуется выбирать более сложное сочетание символов (чтоб затруднить угадывание). В частности, Microsoft рекомендует

составлять пароль из прописных и строчных букв, а также чисел и других символов (например, Lp6*g9).

Откроется окно Windows 2000 Components (Компоненты Windows 2000), в котором перечислены доступные компоненты Windows 2000.

7. Щелкните Next.

Вы можете установить дополнительные компоненты после установки Windows 2000. Для этого дважды щелкните значок Add/Remove Programs (Установка и удаление программ) на панели управления. Пока же вам нужно установить только компоненты, выбранные по умолчанию. Дополнительные компоненты вы зададите позже, в ходе изучения курса.

Если во время установки на вашем компьютере был обнаружен модем, откроется окно Modem Dialing Information (Информация о модеме).

8. Если открылось окно Modem Dialing Information, введите в него код региона или города и щелкните Next.

Откроется окно Date And Time Settings (Настройки даты и времени).

Внимание! Работа многочисленных служб Windows 2000 основана на данных о дате и времени. Поэтому, чтобы избежать проблем в будущем, укажите правильный часовой пояс и регион.

---

9. Введя правильные параметры даты, времени и часового пояса, щелкните Next.

Откроется окно Network Settings (Сетевые настройки), и будут установлены сетевые компоненты.

► Завершение установки сетевых компонентов

Сетевые компоненты — неотъемлемая часть Windows 2000 Server. При их настройке существуют возможности выбора. Пока вам нужно установить только основные сетевые компоненты, а дополнительные вы установите во время выполнения упражнений курса.

1. Убедившись, что на странице Networking Settings (Сетевые параметры) выбран параметр Typical Settings, щелкните Next. Начнется установка сетевых компонентов.

Выбор параметра Typical Settings означает, что будут установлены компоненты, используемые для реализации и предоставления доступа к сетевым ресурсам. Кроме того, протокол TCP/IP будет автоматически запрашивать IP-адрес у сервера DHCP.

Откроется окно Workgroup Or Computer Domain (Рабочая группа или домен) с запросом, хотите ли вы включить ваш компьютер в рабочую группу или домен.

2. Убедившись, что в окне Workgroup Or Computer Domain выбран переключатель No, This Computer Is Not On A Network or Is On A Network Without A Domain (Компьютер не подключен к сети или входит в сеть без доменов) и в качестве имени рабочей группы указано WORKGROUP, щелкните Next.

Откроется окно Installing Components (Установка компонентов), в котором изображается статус выполняемых операций по установке и настройке остальных компонентов ОС. Это займет несколько минут.

Затем откроется окно Performing Final Tasks (Выполнение завершающих задач), в котором отображается ход операций по завершению копирования файлов, внесению и сохранению изменений в конфигурации и удалению временных файлов. Если аппаратное обеспечение вашего компьютера ненамного превосходит минимальные требования, для завершения этой фазы установки может понадобиться более 30 минут.

По завершении установки откроется окно Completing The Windows 2000 Setup Wizard (Завершение работы мастера установки Windows 2000)

3. Выньте установочный компакт-диск с Windows 2000 Server из привода CD-ROM и щелкните кнопку Finish (Готово).

Внимание! Если ваш компьютер поддерживает загрузку с CD-ROM и вы не вынули установочный компакт-диск, то после перезагрузки компьютера программа установки запустится снова, В этом случае выньте CD-ROM и перезагрузите компьютер еще раз.

После перезагрузки будет запущена только что установленная версия Windows 2000 Server.

► Завершение установки аппаратных средств

Сейчас вы выполните поиск устройств Plug and Play, не обнаруженных на предыдущих стадиях установки,

1. Войдите в систему, нажав Ctrl+Alt+Delete.
2. В диалоговом окне Enter Password (Ввод пароля) введите **administrator** в поле User Name (Имя пользователя) и password — в поле Password (Пароль).
3. Щелкните OK.
4. Если Windows 2000 найдет устройства, которые не были обнаружены при установке, откроется окно мастера Found New Hardware (Обнаруженные устройства), сообщая вам, что Windows 2000 устанавливает соответствующие драйверы.

   Если откроется окно мастера Found New Hardware, убедитесь, что флажок Restart The Computer When I Click Finish (Перезагрузить компьютер после окончания установки) не выбран, и щелкните кнопку Finish для завершения работы мастера Found New Hardware,

   Откроется окно Configure Your Server (Настройка вашего сервера), позволяющее вам конфигурировать множество различных параметров и служб.
5. Выберите I Will Configure This Server Later (Настроить сервер позднее) и щелкните кнопку Next (Далее).
6. В следующем окне сбросьте флажок Show This Screen At Startup (Показывать это окно при запуске).
7. Закройте окно Configure Your Server.

   Установка Windows 2000 Server завершена, и вы зарегистрированы с учетной записью Administrator.

Примечание Для правильного завершения работы Windows NT Server в меню Start выберите команду Shut Down и следуйте инструкциям на экране.

Чтобы вы могли выполнять упражнения, связанные с работой в сети, компьютеры должны иметь возможность связываться друг с другом. Назначьте первый компьютер с именем Server1 *основным контроллером домена* (primary domain controller, PDC) Domain1. В большинстве процедур этого курса второй компьютер будет выполнять функции клиента или дополнительного сервера.

Внимание! Если ваши компьютеры являются частью большой сети, обратитесь к сетевому администратору и проверьте, не входят ли имена компьютеров, доменов и другая введенная при установке информация в конфликт с текущими сетевыми параметрами. В случае конфликта попросите администратора присвоить вашим компьютерам другие значения и используйте их на протяжении всего курса.

Программа сертификации специалистов Microsoft

Программа сертификации специалистов Microsoft (Microsoft Certified Professional, MCP) — отличная возможность подтвердить ваши знания современных технологий и программных продуктов этой фирмы. Лидер отрасли в области сертификации — компания Microsoft разработала современные методы тестирования. Экзамены и программы сертификации подтвердят вашу квалификацию разработчика или специалиста по реализации решений на основе технологий и программных продуктов Microsoft. Сертифицированные Microsoft профессионалы квалифицируются как эксперты и высоко ценятся на рынке труда.

Программа сертификации специалистов предлагает восемь типов сертификации по разным специальностям.

- **Сертифицированный специалист Microsoft (Microsoft Certified Professional, MCP)** — предполагается глубокое и доскональное знание по крайней мере одной операционной системы Microsoft. Сдав дополнительные экзамены, кандидаты подтвердят право на работу с продуктами Microsoft BackOffice, инструментальными средствами или прикладными программами.
- **Сертифицированный специалист Microsoft + Интернет (MCP + Internet)** — должен разбираться в планировании систем защиты, установке и конфигурировании серверных продуктов, управлении ресурсами сервера, расширении возможностей сервера средствами сценариев *интерфейса общего шлюза* (Common Gateway Interface, CGI) и *интерфейса прикладного программирования сервера Интернета* (Internet Server Application Programming Interface, ISAPI), мониторинге работы сервера, анализе его производительности и устранении неисправностей.
- **Сертифицированный специалист Microsoft + Site Bulding (MCP + Site Bulding)** — планирование, создание, поддержка и управление Web-узлами с применением технологий и продуктов Microsoft.
- **Сертифицированный системный инженер Microsoft (Microsoft Certified Systems Engineer)** — умение эффективно планировать, развертывать, сопровождать и поддерживать информационные системы на базе Microsoft Windows 95, Microsoft Windows NT и интегрированного семейства серверных продуктов Microsoft BackOffice.
- **Сертифицированный системный инженер Microsoft + Интернет (MCSE + Internet)** – развертывание и сопровождение многофункциональных решений для интрасети и Интернета, включая программы просмотра, представительские серверы, базы данных, системы сообщений и коммерческие компоненты. Кроме того, сертифицированные по этой специальности инженеры должны уметь управлять Web-узлом и выполнять его анализ.
- **Сертифицированный администратор баз данных Microsoft (Microsoft Certified Database Administrator, MCDBA)** — разработка физической структуры, логических моделей данных, создание физических БД, создание служб доступа к данным с использованием T-SQL, управление и поддержка БД, настройка и управление системой защиты, мониторинг и оптимизация БД, а также установка и настройка Microsoft SQL Server.
- **Сертифицированный разработчик программных решений на основе продуктов Microsoft (Microsoft Certified Solution Developer, MCSD)** — разработка и создание прикладных приложений с применением инструментальных средств, технологий и платформ Microsoft, включая Microsoft Office и Microsoft BackOffice.
- **Сертифицированный преподаватель Microsoft (Microsoft Certified Trainer, MCT)** — теоретическая и практическая подготовка для ведения соответствующих курсов в авторизованных учебных центрах Microsoft.

Преимущества программы сертификации Microsoft

Программа сертификации Microsoft — один из самых строгих и полных тестов оценки знаний и навыков в области проектирования, разработки и сопровождения программного обеспечения. Сертифицированными специалистами Microsoft становятся лишь те, кто демонстрирует умение решать конкретные задачи, применяя продукты компании. Программа тестирования позволяет не только оценить квалификацию специалиста, но и служит ориентиром для всех, кто стремится достичь современного уровня знаний в этой области. Как и любой другой тест или экзамен, сертификация Microsoft является показателем определенного уровня знаний специалиста, что важно при трудоустройстве.

Для специалистов. Звание Microsoft Certified Professional даст вам следующие преимущества:

- официальное признание знаний и опыта работы с продуктами и технологиями Microsoft;
- доступ к технической информации о продуктах Microsoft через защищенную область Web-узла MCP;
- членство MSDN Online Certified Membership, обеспечивающее доступ к лучшим техническим ресурсам, сообществу MCP и другим полезным ресурсам и службам (некоторые из элементов узла MSDN Online доступны лишь на английском языке, а в некоторых странах — недоступны вообще); для получения растущего списка услуг, доступных сертифицированным членам, обратитесь на Web-узел MSDN;
- эмблемы, свидетельствующие, что вы имеете квалификацию сертифицированного специалиста Microsoft;
- приглашения на конференции, семинары и специальные мероприятия для специалистов Microsoft;
- сертификат «Microsoft Certified Professional»;
- подписку на различные издания Microsoft, содержащие ценную техническую информацию о продуктах и технологиях Microsoft.

Кроме того, в зависимости от типа сертификации и страны, сертифицированные специалисты получают:

- годовую подписку на ежемесячно распространяемые компакт-диски Microsoft TechNet Technical Information Network;
- годовую подписку на программу бета-тестирования продуктов Microsoft (вы бесплатно получите до 12 компакт-дисков с бета-версиями новейших программных продуктов компании Microsoft),

Для работодателей и организаций. Сертификация позволяет быстро окупить затраты на технологии Microsoft и извлечь максимум прибыли из этих технологий. Исследования показывают, что сертификация сотрудников по программам Microsoft:

- быстро окупается за счет стандартизации требований к обучению специалистов и методов оценки их квалификации;
- позволяет увеличить эффективность обслуживания клиентов, повысить производительность труда и снизить расходы на сопровождение ОС;
- обеспечивает надежные критерии найма специалистов и их продвижения по службе;
- предоставляет методы оценки эффективности труда персонала;
- обеспечивает гибкие методы переподготовки сотрудников для обучения новым технологиям;
- позволяет оценить партнеров — сторонние фирмы.

Дополнительную информацию о том, какую пользу ваша компания извлечет из сертификации, вы найдете на странице http://www.microsoft.com/mcp/mktg/bus_bene.htm (русскоязычная страница — http://www.microsoft.com/rus/mcp/org_benefits.html).

Требования к соискателям

Требования к соискателям определяются специализацией, а также служебными функциями и задачами.

Соискатель сертификата Microsoft должен сдать экзамен, подтверждающий его глубокие знания в области программных продуктов Microsoft. Экзаменационные вопросы, подготовленные с участием ведущих специалистов компьютерной отрасли, отражают **реалии** применения программных продуктов компании Microsoft.

- **«Сертифицированный специалист Microsoft»** — кандидаты на это звание сдают экзамен по работе с одной из операционных систем. Кандидат может сдать дополнительные экзамены, которые подтвердят его право на работу с продуктами Microsoft BackOffice, инструментальными средствами или прикладными программами.
- **«Сертифицированный специалист Microsoft + Интернет»** — кандидаты на это звание **сдают** экзамен по ОС Microsoft Windows NT Server 4.0, поддержке TCP/IP и экзамены по Microsoft Internet Information Server.
- **«Сертифицированный специалист Microsoft + Site Building»** — кандидаты на это звание сдают два экзамена по основам технологий Microsoft Front Page, Microsoft Site Server и Microsoft Visual InterDev.
- **«Сертифицированный системный инженер Microsoft»** — кандидаты на это звание сдают экзамены по технологии ОС Microsoft Windows, сетевым технологиям и технологиям интегрированного семейства серверных продуктов Microsoft BackOffice,
- **«Сертифицированный системный инженер Microsoft + Интернет»** — кандидаты на это звание сдают семь экзаменов по операционным системам и два — по выбору.
- **«Сертифицированный администратор баз данных Microsoft»** — кандидаты на это звание сдают три ключевых экзамена и один — по выбору.
- **«Сертифицированный разработчик программных решений на основе продуктов Microsoft»** — кандидаты сдают два экзамена по основам технологии ОС Microsoft Windows и два — по технологиям интегрированного семейства серверных продуктов Microsoft BackOffice.
- **«Сертифицированный преподаватель Microsoft»** — надо подтвердить свою теоретическую и практическую подготовку для ведения соответствующих курсов в авторизованных учебных центрах Microsoft. Более подробные сведения о сертификации по этой программе вы получите в компании Microsoft по телефону (800) 636-7544 (в США и Канаде) или по адресу http://www.microsoft.com/train_cert/mct/. За пределами США и Канады обращайтесь в местные отделения компании Microsoft.

Подготовка к экзаменам

Рекомендуются три режима подготовки: самостоятельная работа, интерактивный режим, а также занятия с инструктором в авторизованных центрах подготовки.

Самостоятельная подготовка

Самостоятельная подготовка — наиболее эффективный метод подготовки для инициативных соискателей. Издательства «Microsoft Press» и «Microsoft Developer Division» предлагают весь спектр учебных пособий для подготовки к экзаменам по программе сертификации специалистов Microsoft. Учебные курсы для самостоятельного изучения, адресованные специалистам компьютерной отрасли, содержат теоретические и практические материалы, мультимедийные презентации, упражнения и необходимое ПО. Все эти пособия позволяют наилучшим образом подготовиться к сдаче сертификационных экзаменов.

Интерактивная подготовка

Интерактивная подготовка средствами Интернета — альтернатива занятиям в учебных центрах. Вы можете выбрать наиболее удобный распорядок занятий в виртуальном классе, где научитесь работать с продуктами и технологиями компании Microsoft и подготовитесь к сдаче экзаменов. В интерактивном режиме доступно множество курсов Microsoft — от обычных официальных до специальных, доступных лишь в интерактивном режиме. Интерактивные ресурсы доступны круглосуточно в сертифицированных центрах подготовки.

Сертифицированные центры технического обучения Microsoft

Сертифицированные центры технического обучения Microsoft (Certified Technical Education Center, CTEC) — самый простой способ пройти курс обучения под руководством опытного инструктора и стать сертифицированным специалистом. Microsoft CTEC — всемирная сеть учебных центров, которые позволяют специалистам повысить свой технический потенциал под руководством сертифицированных инструкторов Microsoft.

Список центров CTEC в США и Канаде можно получить, обратившись на Web-узел компании Microsoft по адресу http://www.microsoft.com/CTEC/default.htm (на русском языке: http://www.microsoft.com/rus/CTEC/default.htm).

Техническая поддержка

Мы постарались сделать все от нас зависящее, чтобы и сам учебный курс, и прилагаемый к нему компакт-диск не содержали ошибок. Если все же у вас возникнут вопросы или вы захотите поделиться своими предложениями или комментариями, обращайтесь в издательство Microsoft Press по одному из этих адресов.

Электронная почта tkinput@microsoft.com

Почтовый адрес: Microsoft Press
Attn:MCSE Training Kit-Microsoft Windows 2000 Professional Editor
One Microsoft Way
Redmond,WA 98052-6399

Издательство «Microsoft Press» публикует постоянно обновляемый список исправлений и дополнений к своим книгам по адресу http://mspress.microsoft.com/support/.

Учтите, что по указанным почтовым адресам техническая поддержка не предоставляется. Для получения подробной информации о технической поддержке программных продуктов Microsoft обращайтесь на Web-узел компании Microsoft по адресу http://www.microsoft.com/support/ или звоните в службу Microsoft Support Network Sales по телефону (800) 936-3500 - в США.

Подробнее о получении полных версий программных продуктов Microsoft вы можете узнать, позвонив в службу Microsoft Sales по телефону (800) 426-9400 или по адресу www.microsoft.com.

ГЛАВА 1

Знакомство с Microsoft Windows 2000

В этой главе

В этой главе вы познакомитесь с операционной системой Microsoft Windows 2000 и набором функций, входящих в эту ОС. Вы узнаете о роли, которую они играют, и о различиях в администрировании рабочей группы и домена. Мы расскажем об архитектуре Windows 2000 и о службах каталога Windows 2000. Кроме того, вы освоите на практике основные процедуры входа в систему и выполнение ключевых задач в диалоговом окне Windows Security (Безопасность Windows).

Прежде всего

Для изучения материалов этой главы необходимо выполнить процедуру установки, описанную во вводной главе.

Занятие 1. Краткий обзор возможностей Windows 2000

Вы познакомитесь с семейством продуктов Windows 2000, с их возможностями и преимуществами. Мы расскажем об основных различиях между этими продуктами и о среде, для использования в которой они предназначены.

Изучив материал этого занятия, вы сможете:

- ✓ рассказать о Windows 2000;
- ✓ объяснить ключевые различия между Windows 2000 Professional и Windows 2000 Server;
- ✓ описать возможности и преимущества Windows 2000;
- ✓ описать различия между моделями рабочей группы и домена в сетевой среде.

Продолжительность занятия — около 15 минут.

Семейство Windows 2000

Windows 2000 представляет собой многоцелевую ОС с встроенной поддержкой клиент-серверных и одноранговых сетей. Она сконструирована на основе технологий, уменьшающих совокупную стоимость владения и обеспечивающих масштабируемость от небольшой до крупной корпоративной сети. *Совокупная стоимость владения* (Total cost of ownership, TCO) — общая сумма, необходимая на приобретение компьютеров и развертывание программного обеспечения, их дальнейшее сопровождение и техническую поддержку. Другой главный фактор, влияющий на TCO, — снижение производительности из-за ошибок пользователей, аппаратных проблем или из-за обновлений программ и их настройки.

В этом учебном курсе мы рассмотрим две версии ОС Windows 2000.

- Windows 2000 Professional. Этот продукт представляет собой высокопроизводительную безопасную сетевую корпоративную ОС, сочетающую лучшие возможности Microsoft Windows 98 и управляемость, надежность, безопасность и быстродействие Microsoft Windows NT Workstation 4.0. Windows 2000 Professional используется в качестве настольной ОС в одноранговой сети в составе рабочей группы или в качестве рабочей станции в составе домена Windows 2000 Server или Windows NT. Данный продукт можно считать основной настольной ОС Microsoft для предприятий любого масштаба.
- Windows 2000 Server. Это сервер файлов, печати, терминалов и приложений, а также платформа Web-сервера, содержащая все возможности Windows 2000 Professional, и множество новых серверных функций. Оптимальный выбор для поддержки корпоративных приложений среднего размера, Web-серверов, рабочих групп и филиалов.

Семейство Windows 2000 также включает еще два продукта: Windows 2000 Advanced Server и Windows 2000 Datacenter Server.

- Windows 2000 Advanced Server. Этомощный промышленный сервер приложений, обеспечивающий поддержку *сетевой операционной системы* (network operations system, NOS) и служб Интернета. Advanced Server поддерживает физическую память большого объема, кластеризацию и балансировку нагрузки. Подробное знакомство с данным продуктом и его возможностями выходит за рамки нашего курса.
- Windows 2000 Datacenter Server. Это самая мощная и функциональная ОС в семействе Windows 2000. Оптимизирована для хранения больших объемов данных, эконометрического анализа, моделирования крупных научных и инженерных проектов и много-

серверных систем. Подробное знакомство с данным продуктом и его возможностями также выходит за рамки нашего курса.

В табл. 1-1 перечислены новые возможности Windows 2000.

Табл. 1-1. Новые возможности Windows 2000

Возможность	Описание
Служба каталогов Active Directory	Каталог Active Directory является масштабируемой, основанной на стандартах Интернета и полностью интегрированной на уровне операционной системы службой каталогов корпоративного уровни. Эта служба упрощает администрирование и облегчает поиск нужных ресурсов. Служба каталога Active Directory предоставляет широкий набор средств и возможностей, включая групповую политику, несложное масштабирование, поддержку нескольких протоколов проверки подлинности и использование стандартов Интернета
Интерфейсы службы Active Directory (Active Directory Service Interfaces, ADSI)	Интерфейсы службы Active Directory являются моделью службы каталогов и набором COM-интерфейсов. Они позволяют приложениям Windows 95, Windows 98, Windows NT и Windows 2000 получать доступ к данным в некоторых сетевых службах каталогов, в том числе и Active Directory. Данные средства включены в пакет для разработчиков Software Development Kit (SDK)
Асинхронный режим передачи (Asynchronous Transfer Mode, ATM)	Является высокоскоростным протоколом с установкой соединения, разработанным для передачи по сети потоков данных различных типов. Он применим как к локальным, так и к глобальным сетям. Режим ATM позволяет осуществлять одновременную передачу по сети звука, информации, графики и видео
Службы сертификации	Службы сертификации и средства управления сертификатами в Windows 2000 позволяют внедрить собственную инфраструктуру открытого ключа. Инфраструктура открытого ключа позволяет применить такие стандартные технологии, как подключение по смарт-картам, проверка подлинности клиентов по протоколам SSL и TLS, зашита электронной почты, электронные подписи и защита подключений с помощью средств безопасности протокола IP. С помощью служб сертификации можно установить центры сертификации, предоставляющие и отзывающие сертификаты X.509 V3, и управлять ими. Это позволяет обеспечить независимость от коммерческих служб сертификации клиентов, хотя при необходимости возможно объединение коммерческой службы проверки подлинности клиентов с созданной инфраструктурой открытого ключа
Службы компонентов	Службы компонентов являются набором служб на основе расширений COM (модели компонентных объектов) и Microsoft Transaction Server (более раннем выпуске системы обработки транзакций на основе компонентов). Эти службы обеспечивают повышение производительности и безопасности при обработке транзакций, предоставляют возможность управления транзакциями и группировки объектов в пулы, выстраивания компонентов в очереди, а также позволяют осуществлять администрирование и создание пакетов приложений
Дисковые квоты	Применяются на томах с файловой системой NTFS для просмотра и ограничения количества дискового пространства конкретных пользователей. Вы можете задать способ реакции системы на превышение порогового значения

Табл. 1-1. Новые возможности Windows 2000 ***(продолжение)***

Возможность	Описание
Протокол Dynamic Host Configuration Protocol (DHCP) со службами Domain Name System (DNS) и Active Directory	Совместная работа протокола DHCP со службами DNS и Active Directory в сетях IP помогает избежать назначения и отслеживания IP-адресов вручную. Протокол DHCP автоматически назначает IP-адреса компьютерам и другим ресурсам, подключенным к сети IP
Шифрованная файловая система (Encrypting File System, EFS)	Шифрованная файловая система Windows 2000 дополняет имеющиеся средства управления доступом и обеспечивает дополнительный уровень зашиты данных. Шифрованная файловая система интегрирована с системными службами, что позволяет легко управлять ею. а также повышает ее надежность и прозрачность для пользователя
Графическое средство управления дисками	Оснастка Disk Management (Управление дисками) позволяет управлять дисковым пространством и включает множество новых возможностей, например поддержку томов и точек их монтирования
Групповая политика (часть Active Directory)	Политики могут быть использованы для определения действий и параметров для пользователей и компьютеров. В отличие от локальной политики, групповая политика позволяет установить политики для всего узла, домена или организационной единицы в каталоге Active Directory. Управление на основе политики упрощает выполнение таких задач, как обновление операционной системы, установка приложений, настройка профилей пользователей и блокировка настольных систем
Службы индексирования	Служба индексирования предоставляет быстрый, простой и безопасный способ поиска пользователями локальных или сетевых данных. Для поиска в файлах различного формата и на различных языках пользователи могут применять великолепные средства запросов, как с помощью команды Search (Поиск) из меню Start (Пуск), так и на страницах в формате HTML, отображаемых обозревателем
IntelliMirror	Средства IntelliMirror позволяют осуществить такой контроль для клиентов с системой Windows 2000 Professional. Набор средств IntelliMirror позволяет определить политики на основе должностных обязанностей пользователей, участия их в группах и расположении. С помощью таких политик рабочие станции с Windows 2000 Professional автоматически настраиваются в соответствии с конкретными потребностями пользователей при каждом входе в сеть независимо от места подключения к сети
Служба проверки подлинности в Интернете (Internet Authentication Service, IAS)	Предоставляет пользователям централизованное управление проверкой подлинности, авторизацией, обработкой учетных записей и аудитом удаленных пользователей и пользователей виртуальных частных сетей. Служба IAS использует протокол RADIUS (Remote Authentication Dial-In User Service), разработанный группой IETF (Internet Engineering Task Force)
Общий доступ к подключению Интернета (Internet Connection Sharing, ICS)	Позволяет подключить к Интернету домашнюю или небольшую офисную сеть. Например, ваша домашняя сеть подключена к Интернету при помощи модема. Для предоставления доступа к Интернету с компьютера, на котором установлен модем, необходимо на всех остальных компьютерах сети настроить преобразование сетевых адресов (network address translation, NAT), адресацию и службу разрешения имен

Табл. **1-1.** Новые возможности Windows 2000 *(продолжение)*

Возможность	Описание
Internet Information Services (IIS) 5.0	Мощные средства IIS, включенные в Microsoft Windows 2000 Server, упрощают совместное использование документов и данных в локальной сети организации и Интернете. Службы IIS позволяют внедрить масштабируемые и надежные Web-приложения, а также включать имеющиеся данные и приложения в Интернет. Службы IIS включают поддержку страниц ASP и других возможностей
Internet Security Protocol (IPSec)	Безопасность протокола Интернета (IPSec) может быть использована для защиты подключений в локальной сети и создания безопасных структур виртуальных частных сетей в Интернете. Это средство было разработано группой IETF (Internet Engineering Task Force) и считается промышленным стандартом для шифрования данных при передаче по протоколу TCP/IP
Kerberos V5	Kerberos V5 является хорошо зарекомендовавшим себя стандартным протоколом для проверки подлинности в сети. Этот протокол позволяет организовать быстрый единый процесс подключения пользователей к необходимым ресурсам серверов с системой Windows 2000 на уровне организации, а также к другим ресурсам, доступ к которым осуществляется с поддержкой данного протокола. Поддержка протокола Kerberos V5 предоставляет дополнительные преимущества, такие, как взаимная проверка подлинности, при которой проверка должна выполняться как клиентом, так и сервером, и делегирование проверки подлинности, при которой данные пользователя отслеживаются от узла к узлу
Поддержка протокола Layer 2 Tunneling Protocol (L2TP)	Протокол туннелирования канального уровня L2TP является версией протокола PPTP (Pointto-Point Tunneling Protocol) с повышенной степенью зашиты и используется для туннелирования, назначения адресов и проверки подлинности
Поддержка протокола LDAP	Общепринятый стандарт LDAP (Lightweight Directory Access Protocol) является основным протоколом, используемым для доступа к Active Directory. Протокол LDAP версии 3 был определен группой IETF (Internet Engineering Task Force)
Очереди сообщений	Интегрированные средства очередей сообщений в Windows 2000 помогают разработчикам создавать и внедрять приложения, отличающиеся надежностью сетевой работы, в том числе и в Интернете. Эти приложения могут взаимодействовать с приложениями, работающими на различных платформах, таких, как большие ЭВМ и системы на основе UNIX
Консоль управления Microsoft (Microsoft Management Console, MMC)	Консоль управления Microsoft (MMC) позволяет упорядочить нужные административные средства и действия в едином интерфейсе. Также имеется возможность делегирования задач определенным пользователям путем создания для них заранее сконфигурированных консолей MMC. Такие консоли будут содержать выбранные вами для этих пользователей средства

Табл. 1-1. Новые возможности Windows 2000 (*продолжение*)

Возможность	Описание
Трансляция сетевых адресов (Network Address Translation, NAT)	NAT скрывает управляемые изнутри IP-адреса от внешних сетей, транслируя закрытые внутренние адреса в открытые внешние адреса. Это уменьшает стоимость регистрации IP-адресов, позволяя внутри сети использовать незарегистрированные IP-адреса с их последующей трансляцией в небольшое количество зарегистрированных внешних адресов. При этом скрывается структура внутренней сети, что уменьшает риск ее атаки извне
Перенос, поддержка и интеграция операционных систем	Windows 2000 тесно интегрирована с имеющимися операционными системами и содержит как средства поддержки операционных систем Windows предыдущих версий, так и новые средства для поддержки других распространенных операционных систем. Windows 2000 предоставляет следующие возможности: • взаимодействие с Windows NT Server 3.51 и 4.0; • поддержку клиентов с различными операционными системами, включая Windows 3.x, Windows 95, Windows 98 и Windows NT Workstation 4.0; • взаимодействие с большими и средними ЭВМ с помощью шлюзов транзакций и очередей S/390 и AS/400 через SNA-сервер; • файловый сервер для Macintosh, позволяющий клиентам Macintosh организовывать общий доступ к файлам и использовать общие ресурсы Windows 2000 Server с помощью протокола TCP/IP (протокол AFP через IP)
Plug and Play (PnP)	Поддержка Plug and Play на аппаратном и программном уровне позволяет серверу автоматически обнаружить изменения конфигурации и настроить новую конфигурацию без вмешательства пользователя и перезагрузки
Качество обслуживания (Quality of Servict, QoS)	Используя QoS, управляют распределением сетевых ресурсов между приложениями. Важным приложениям можно дать больше ресурсов, а менее значимым — меньше. Протоколы и службы QoS обеспечивают гарантированную, быструю систему доставки информации по сети
Служба удаленной установки (Remote Installation Services, RIS)	С помощью служб удаленной установки можно произвести удаленную установку Windows 2000 Professional, не посещая каждого клиента. Конечные компьютеры-клиенты должны либо поддерживать удаленную загрузку с PXE boot ROM (Pre-Boot execution Environment), либо должны быть загружены с гибкого диска удаленной загрузки. Установка системы на несколько клиентов значительно упрощается
Съемные запоминающие устройства и внешнее хранилище	Служба Removable Storage (съемные ЗУ) упрощает отслеживание съемных носителей (таких, как ленты или оптические диски) и управление аппаратными библиотеками, например устройствами смены дисков. Служба внешнего хранилища автоматически копирует редко используемые файлы на съемный носитель, руководствуясь заданными пользователем критериями. Если объем свободного места на диске снижается до указанного уровня, служба внешнего хранилища удаляет с диска содержимое кэша файлов. Если файл понадобится в дальней шем, содержимое автоматически вызывается из хранилища. Remote Storage (Удаленное хранилище) позволяет сократить расходы, так как съемные оптические диски и магнитные ленты имеют более низкую стоимость в пересчете на один мегабайт

Табл. 1-1. Новые возможности Windows 2000 (*продолжение*)

Возможность	Описание
Служба маршрутизации и удаленного доступа	Служба Routing and Remote Access (Маршрутизация и удаленный доступ) является интегрированной службой, обеспечивающей как конечные подключения для удаленных клиентов и клиентов виртуальных частных сетей, так и маршрутизацию для протоколов IP, IPX и AppleTalk. Служба маршрутизации и удаленного доступа позволяет серверу с системой Windows 2000 Server выполнять функции сервера удаленного доступа, сервера виртуальной частной сети, шлюза или маршрутизатора подразделения организации
Загрузка в защищенном режиме	При запуске Windows 2000 в безопасном режиме используется минимальный набор драйверов и служб, после чего просматривается журнал с последовательностью событий, произошедших после запуска. При этом диагностируются проблемы с драйверами и другими компонентами, затрудняющими нормальную загрузку системы
Инфраструктура смарт-карт	Службы сертификации и средства управления сертификатами в Windows 2000 позволяют внедрить собственную инфраструктуру открытого ключа. Инфраструктура открытого ключа позволяет применить такие стандартные технологии, как подключение по смарт-картам, проверка подлинности клиентов по протоколам SSL и TLS, защита электронной почты, электронные подписи и защита подключений средствами безопасности протокола IP
Интерфейс TAPI 3.0	Объединяет возможности IP-связи и обычной телефонной связи, что позволяет разработчикам создавать мощные приложения компьютерной телефонии нового поколения, работающие с Интернетом или локальными сетями так же эффективно, как и с обычной телефонной линией
Службы терминалов	Только семейство Windows 2000 Server предлагает ОС для серверов, имеющих интегрированные службы эмуляции терминалов. Службы терминалов позволяют пользователям получить доступ с помощью различных средств предыдущих версий к приложениям, работающим на сервере. Например, пользователи могут работать с виртуальным рабочим столом Windows 2000 Professional и 32-разрядными приложениями на компьютерах, не позволяющих работать с этими средствами локально. Службы терминалов предоставляют такую возможность как клиентам с системами Windows, так и клиентам с другими системами. (Для клиентов с системами, отличными от Windows, требуется наличие программного обеспечения компании Citrix Systems.)
Виртуальная частная сеть (Virtual Private Network, VPN)	Виртуальная частная сеть предоставляет пользователям доступ к сети, даже если они находятся за пределами организации, и сократить затраты на такое подключение. С помощью виртуальных частных сетей пользователи могут легко создать безопасное подключение к сети организации- Подключение осуществляется через местного поставщика услуг Интернета, что сокращает затраты. Для создания подключений к виртуальным частным сетям система Windows 2000 Server предоставляет перечисленные ниже новые протоколы с повышенной степенью защиты.

Табл. 1-1. Новые возможности Windows 2000 *(окончание)*

Возможность	Описание
	• Протокол L2TP (Layer 2 TunnelingProtocol), версия протокола PPTP (Point-to-Point Tunneling Protocol) с повышенной степенью защиты. Протокол L2TP используется для туннелирования, назначения адресов и проверки подлинности. • Протокол IPSec (Internet Protocol Security), стандартный протокол, обеспечивающий наивысший уровень безопасности в виртуальных частных сетях. Протокол IPSec позволяет применить шифрование практически для всех объектов сетевого уровня
Службы мультимедиа Windows	Позволяют отправлять пользователям потоки высококачественных данных мультимедиа по Интернету и локальным сетям
Сервер сценариев Windows (Windows Scripting Host, WSH)	Позволяет автоматизировать такие действия, как создание ярлыка, а также подключение и отключение от сервера сети; не зависит от языка программирования. Сценарий может быть написан на любом стандартном языке сценариев, таком, как Visual Basic Scripting Edition или JScript

Сетевая среда Windows 2000

Основана на модели рабочей группы или домена. Как Windows 2000 Professional, так и Windows 2000 Server могут использоваться Б обеих моделях. Различия в администрировании этих двух продуктов зависят от модели сетевой среды.

Модель **рабочей группы**

Рабочая группа (workgroup) — логическая группировка сетевых компьютеров, предоставляющих доступ к ресурсам, например к файлам и принтерам. Рабочая группа используется в *одноранговых* (peer-to-peer) сетях, в которых все компьютеры рабочей группы обеспечивают равноправный доступ к ресурсам без выделенного сервера. Каждый компьютер рабочей группы под управлением Windows 2000 Server или Windows 2000 Professional ведет *локальную БД безопасности* (рис. 1-1), которая представляет собой список учетных записей пользователей и информацию о защите ресурсов компьютера, на котором она находится. Поэтому администрирование учетных записей пользователей и зашита ресурсов в рабочей группе децентрализовано.

Недостатки модели рабочей группы:

- пользователю приходится иметь учетные записи на всех компьютерах, к которым ему необходим доступ;
- любые изменения учетных записей пользователей, например смена пароля или добавление новой учетной записи, необходимо выполнить на каждом компьютере рабочей группы. Если вы забудете добавить новую учетную запись пользователя на один из компьютеров рабочей группы, новый пользователь не сможет войти в систему этого компьютера и получить доступ к его ресурсам;
- предоставление доступа к файлам и устройствам выполняется конкретными компьютерами только для пользователей, имеющих учетные записи на каждом конкретном компьютере.

Преимущества рабочей группы Windows 2000:

- рабочей группе не нужен компьютер с Windows 2000 Server для хранения централизованной информации безопасности;
- рабочая группа обеспечивает простоту в проектировании и сопровождении: по сравнению с доменом не требуется трудоемкое планирование и администрирование;
- рабочая группа удобна для небольшого количества расположенных рядом компьютеров. (Использование рабочей группы непрактично в сетях, состоящих более чем из 10 компьютеров.)

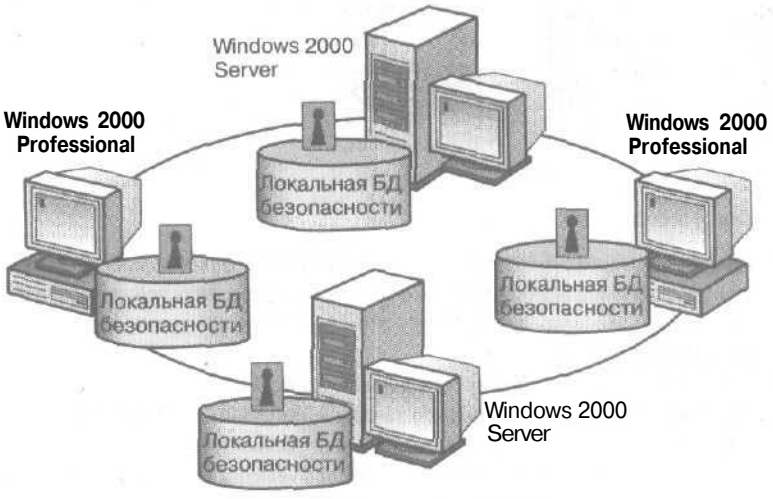


Рис. 1-1. Пример рабочей группы Windows 2000

Примечание В рабочей группе компьютер с Windows 2000 Server, не являющийся членом домена Windows 2000, называется *изолированным сервером* (stand-alone server).

Модель домена

Домен (domain) Windows 2000 — логическая группа сетевых компьютеров, предоставляющих доступ к центральной БД каталогов (рис. 1-2). *База данных каталога* (directory database) содержит учетные записи пользователей и параметры безопасности для домена. БД каталога, или просто каталог, является частью БД службы каталогов. Служба Active Directory пришла на смену контейнерам с «доменной» информацией из предыдущих версий Windows. Active Directory также содержит информацию о службах и других ресурсах, организациях и т. п.

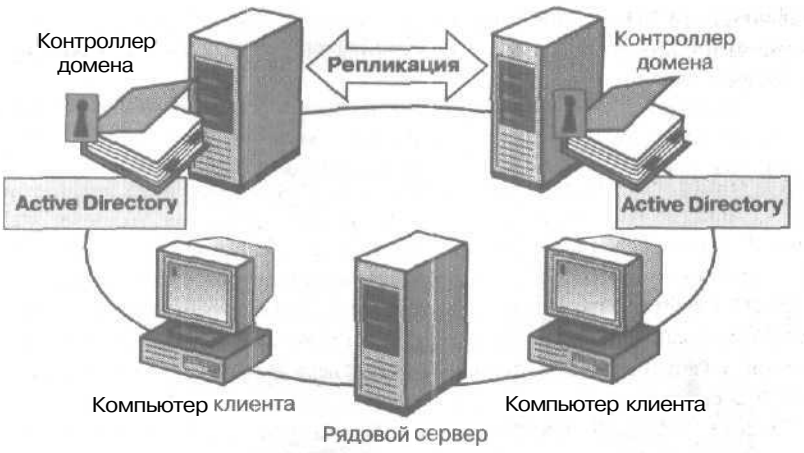


Рис. 1-2. Пример домена Windows 2000

В домене каталоги находятся на компьютерах, сконфигурированных как контроллеры домена, где задаются параметры безопасности взаимодействия пользователей с доменом. Защита и администрирование централизованы. В роли контроллеров домена могут выступать только компьютеры с Windows 2000 Server.

Домен не связан с определенным местоположением или конкретным типом конфигурации сети. Компьютеры в домене могут находиться рядом в небольшой локальной сети или в разных странах, связываясь друг с другом при помощи различных физических соединений: модемов, линий ISDN (Integrated Services Digital Network), оптоволоконных линий, линий Ethernet, соединений типа «эстафетное кольцо», соединений с ретрансляцией кадров, спутниковых и арендованных каналов. Дополнительная информация о доменах — в главе 2.

Преимущества использования домена Windows 2000 таковы:

- домен позволяет выполнять централизованное управление, так как вся информация о пользователях хранится централизованно. Измененный пользователем пароль автоматически реплицируется по всему домену;
- домен обеспечивает единый процесс входа в систему пользователей для получения доступа к разрешенным сетевым ресурсам, например к файлам, принтерам и приложениям. Другими словами, пользователь входит в систему на одном компьютере и обращается к ресурсам другого компьютера сети в течение времени действия соответствующих разрешений;
- домен обеспечивает масштабируемость, что позволяет администратору создавать очень большие сети.

Типичный домен Windows 2000 включает следующие компьютеры.

- Контроллеры домена Windows 2000 Server. Каждый контроллер домена хранит и ведет копию каталога. В домене необходимо однократно создавать учетную запись пользователя, которую Windows 2000 записывает в каталог. Когда пользователь входит в домен, контроллер проверяет по каталогу его имя, пароль и полномочия. При наличии нескольких контроллеров домена они периодически реплицируют информацию своих каталогов.
- Рядовые серверы Windows 2000 Server. *Рядовой сервер* (member server) — сервер не сконфигурированный как контроллер домена. Он не хранит информацию каталога и не выполняет проверку подлинности пользователей домена; обеспечивает доступ к ресурсам, таким, как папки или принтеры.

- Клиентские **компьютеры** с Windows 2000 Professional. Это компьютеры клиентов с запущенным окружением пользовательского рабочего стола, позволяющие получать доступ к ресурсам домена.

Резюме

Windows 2000 является многоцелевой ОС со встроенной поддержкой клиент-серверных и одноранговых сетей. Семейство Windows 2000 состоит из четырех продуктов: Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server и Windows 2000 Datacenter Server. Windows 2000 Professional оптимизирован для самостоятельного использования в качестве настольной ОС, на сетевом компьютере в составе рабочей группы одноранговой сети или рабочей станции домена Windows 2000 Server. Windows 2000 Server оптимизирован для использования в качестве файлового сервера, сервера печати и приложений, а также платформы Web-сервера.

Рабочая группа Windows 2000 представляет собой логическую группу сетевых компьютеров, предоставляющих доступ к ресурсам, например к файлам и принтерам. Рабочая группа не имеет контроллера домена Windows 2000 Server. Защита и администрирование в Windows 2000 Professional и на рядовых серверах Windows 2000 Server в рабочих группах децентрализованы, так как каждый компьютер ведет свой список учетных записей пользователей и параметров безопасности своих ресурсов.

Домен Windows 2000 представляет собой логическую группировку сетевых компьютеров, предоставляющих доступ к центральной БД каталогов, содержащих информацию о безопасности и учетные записи пользователей. В домене защита и администрирование централизованы, так как каталог находится на контроллере домена, который управляет всеми параметрами безопасности взаимодействий пользователей с доменом.

Занятие 2. Краткий обзор архитектуры Windows 2000

Windows 2000 является модульной **ОС,** представляющей собой коллекцию небольших, самодостаточных программных компонентов, совместно работающих для выполнения задач ОС. Каждый компонент выполняет набор функций, представляющих собой интерфейс к остальной части системы.

Изучив материал этого занятия, вы сможете:

- ✓ определять слои и их компоненты в архитектуре ОС Windows 2000.

Продолжительность занятия — около 15 минут.

Уровни, подсистемы и диспетчеры Windows 2000

Архитектура Windows 2000 поддерживает два основных режима; пользовательский (непривилегированный) и режим ядра (привилегированный) (рис.1-3). На этом занятии вы познакомитесь с архитектурой Windows 2000 и ее компонентами.

Рис. 1-3. Архитектура **Windows 2000**

Пользовательский режим

Windows 2000 имеет два различных типа компонентов пользовательского режима: полсистемы среды и встроенные подсистемы.

Подсистемы среды

Одна из возможностей Windows 2000 — способность выполнять приложения, написанные для разных ОС. Это достигается использованием *подсистем среды* (environment subsystems), которые эмулируют разные ОС, предоставляя необходимые приложениям API-интерфейсы. Подсистемы среды принимают от приложений вызовы API, преобразуют их в формат, понятный Windows 2000, и затем передают для обработки исполняемым службам.

В табл. 1-2 перечислены подсистемы среды из состава Windows 2000.

Табл.1-2. Подсистемы среды в Windows 2000

Подсистема среды	Назначение
32-разрядная подсистема Windows 2000 на основе Windows (Win32)	Отвечает как за управление приложений Win32, так и за предоставление среды для приложений Win16 и MS-DOS. Управляет всеми операциями ввода-вывода на экран между подсистемами, Это гарантирует непротиворечивый пользовательский интерфейс независимо от выполняемого пользователем приложения
Подсистема OS/2	Предоставляет набор API для 16-разрядных приложений текстового режима OS/2
Интерфейс переносимых ОС для подсистем UNIX (POSIX)	Предоставляет API для POSIX-приложений

На подсистемы среды и приложения, работающие в них, налагаются некоторые ограничения:

- они не имеют прямого доступа к оборудованию;
- они не имеют прямого доступа к драйверам устройств;
- они не имеют доступа к некоторым операциям API буфера обмена;
- они не имеют доступа к некоторым функциям расширений Microsoft CD-ROM (MSCDEX);
- они не имеют доступа к API переключения задач;
- они ограничены в назначении адресного пространства;
- они вынуждены использовать пространство жесткого диска под виртуальную память при нехватке памяти для ОС;
- они работают на более низком приоритетном уровне, чем процессы режима ядра;
- поскольку они работают на более низком приоритетном уровне, чем процессы режима ядра, им менее доступны ресурсы *центрального процессора* (central processing unit, CPU) чем процессы, которые работают в режиме ядра.

Встроенные подсистемы

Множество разных встроенных подсистем выполняет важные функции ОС. В правой части рис.1-3 показана универсальная подсистема. Эта встроенная подсистема может быть любой, примеры некоторых встроенных подсистем перечислены в табл. 1-3.

Табл. 1-3. Встроенные подсистемы Windows 2000

Встроенная подсистема	Назначение
Подсистема безопасности	Контролирует права и разрешения, связанные с учетными записями пользователей. Отслеживает, каким системным ресурсам назначен аудит. Принимает запросы на вход пользователей в систему. Инициирует аутентификацию входа в систему
Служба рабочей станции	Сетевая встроенная подсистема, предоставляющая API для доступа к сетевой системе переадресации. Дает пользователям Windows 2000 доступ к сети
Служба сервера	Сетевая встроенная подсистема, предоставляющая API для доступа к сетевому серверу. Предоставляет пользователям Windows 2000 доступ к сетевым ресурсам

Режим ядра

Уровень режима ядра имеет доступ к системным данным и оборудованию. Режим **ядра** предоставляет прямой доступ к памяти, программы этого режима выполняются в защищенной области памяти. Он состоит из четырех компонентов: исполняемой части ОС Windows 2000, драйверов устройств, микроядра и *уровня абстрагирования от оборудования* (Hardware Abstraction Layer, HAL).

Исполняемая часть ОС Windows 2000

Выполняет большую часть операций ввода-вывода и управления объектами, включая обеспечение безопасности. Он не занимается вводом с клавиатуры и выводом на экран — за это отвечает подсистема Microsoft Win32. Исполняемая часть ОС Windows 2000 содержит компоненты режима ядра Windows 2000. Каждый из них предоставляет два отличающихся набора служб и подпрограмм:

- **системные службы** — доступны как подсистемам пользовательского режима, так и другим исполняемым компонентам ОС;
- **встроенные подпрограммы** — доступны только другим компонентам в пределах ОС.

Исполняемая часть ОС состоит из компонентов режима ядра (табл. 1-4).

Табл. 1-4. Компоненты исполняемой части Windows 2000

Компонент	Назначение
Диспетчер ввода-вывода	Управляет процессами ввода-вывода устройств. Компоненты, входящие в диспетчер ввода-вывода, включают *файловые системы* (file systems), принимающие запросы ввода-вывода и транслирующие их в вызовы конкретных устройств. Сетевая переадресация и сервер сети реализованы в виде драйверов файловой системы. *Драйверы устройств* (device drivers) — низкоуровневые драйверы, напрямую взаимодействующие с оборудованием, они принимают ввод и записывают вывод. *Диспетчер кэша* (cache manager) ускоряет операции ввода-вывода, сохраняя считанные данные в системной памяти. Диспетчер кэша также ускоряет запись путем кэширования запросов на запись и выполнения записи на диск в фоновом режиме
Монитор безопасности	Устанавливает политики безопасности на локальном компьютере

Табл. 1-4. Компоненты исполняемой части Windows 2000 *(продолжение)*

Компонент	Назначение
Диспетчер виртуальной памяти (Virtual Memory Manager, VMM)	Система управления памятью, которая устанавливает виртуальную память и управляет ею, а также предоставляет защищенное адресное пространство для каждого процесса. VMM также контролирует *подкачку по запросу* (demand paging) и позволяет использовать дисковое пространство для перемещения программ и данных из физической памяти и в нее
Диспетчер межпроцессного взаимодействия (Interprocess Communication Manager, IPC)	Управляет связями между клиентами и серверами, например между подсистемой среды (которая может работать в роли клиента запрашивающего информацию) и компонентом службы ОС (работает в роли сервера, который отвечает на запрос информации). Диспетчер IPC состоит из двух компонентов: *средства локального вызова процедур* (local procedure call, LPC), обслуживающего соединения, когда клиенты и серверы существуют на одном и том же компьютере, и *средства удаленного вызова процедур* (remote procedure call, RPC), обслуживающего соединения, когда клиенты и серверы находятся на разных компьютерах
Диспетчер процессов	Создает и завершает процессы и потоки. *Процесс* (process) — это программа или ее часть. *Поток* (thread) — определенный набор команд в программе
Plug and Play	Обеспечивает центральное управление процессами PnP. Взаимодействует с драйверами устройств, управляя добавлением и запуском устройств
Диспетчер питания	Управляет API-интерфейсами питания, координирует события, связанные с питанием, и генерирует запросы управления питанием
Диспетчер окон и *интерфейс графических устройств* (Graphical Device Interface, GDI)	Два данных компонента, выполненные в виде одного драйвера устройства с именем Win32k.sys, управляют системой дисплея. Диспетчер окон управляет окнами и выводом на экран, а также отвечает за ввод информации с клавиатуры и мыши и передает введенные сообщения приложениям. GDI содержит функции, требуемые для рисования и обработки графики
Диспетчер объектов	Создает, управляет и уничтожает объекты, занимающие ресурсы ОС, например процессы, потоки и структуры данных

Драйверы устройств

Транслируют вызовы драйверов в команды управления конкретными устройствами.

Микроядро

Управляет только микропроцессором. Ядро координирует все функции ввода-вывода и синхронизирует действия исполнимых служб.

Уровень абстрагирования от оборудования

Скрывает детали аппаратного интерфейса, делая Windows 2000 переносимой на различные аппаратные архитектуры. Содержит аппаратно-зависимый код, ответственный за интерфейсы ввода-вывода, контроллеры прерываний и механизм многопроцессорного взаи-

модействия. Позволяет Windows 2000 работать в системах на базе Intel и Alpha одновременно, то есть разработчикам не пришлось создавать две отдельные версии для каждой платформы.

Резюме

В этом занятии вы познакомились с архитектурой Windows 2000, которая состоит из двух основных режимов: пользовательского и режима ядра. В режиме ядра имеется два типа компонентов: подсистемы среды, позволяющие Windows 2000 выполнять приложения написанные для разных ОС, и встроенная подсистема, выполняющая жизненно важные функции ОС. На уровне режима ядра выполняется прямой доступ к системным данным и оборудованию, прямой доступ к памяти и программам в ее защищенной области.

Занятие 3. Краткое знакомство со службой каталогов Windows 2000

Служба каталогов используется для уникальной идентификации пользователей и ресурсов в сети. Для работы службы каталогов Windows 2000 применяет Active Directory. Важно понимать основную цель Active Directory и ее ключевые возможности. Знание взаимодействия компонентов архитектуры Active Directory позволит вам разобраться в том, как Active Directory сохраняет и восстанавливает данные. На занятии вы познакомитесь с функциями, возможностями и архитектурой Active Directory.

Изучив материал этого занятия, вы сможете:

- ✓ объяснить работу службы каталога;
- ✓ объяснить назначение Active Directory;
- ✓ перечислить возможности и уровни архитектуры Active Directory.

Продолжительность занятия — около 20 минут.

Что такое служба каталогов

Каталог (Directory) — сохраненный набор информации об объектах, связанных друг с другом некоторым способом. Например, в телефонном справочнике хранятся имена объектов и соответствующие им телефонные номера. Телефонный справочник также может содержать адрес или другую информацию об объекте.

В распределенных компьютерных системах или глобальных сетях типа Интернета существует множество объектов, например файловые серверы, принтеры, службы факсов, приложения, базы данных и пользователи, которые находят и используют эти объекты. Необходимо, чтобы администраторы имели возможность управлять этими объектами. Служба каталогов централизованно хранит всю информацию, требуемую для использования и управления этими объектами, упрощая процесс поиска и управления данными ресурсами.

В данном курсе термины *каталог* и *служба каталогов* относятся к каталогам, расположенным в глобальных и частных сетях. *Каталог* предоставляет средство хранения информации, относящейся к сетевым ресурсам, облегчая их поиск и управление ими. *Служба каталогов* — сетевая служба, которая идентифицирует все ресурсы сети и делает их доступными пользователям. Служба каталогов отличается от каталога тем, что хотя они оба являются источниками информации, служба делает ее доступной для пользователей.

Служба каталогов работает как главный коммутатор сетевой ОС. Она управляет идентификацией и отношениями между распределенными ресурсами и позволяет им работать вместе. Ввиду поддержки службой каталогов этих фундаментальных функций ОС, они должны быть тесно связаны с механизмами управления и безопасности ОС для обеспечения целостности и защищенности сети. Они также необходимы для определения и поддержания инфраструктуры сети организации, администрирования системы и контроля активности пользователей информационной службы компании.

Назначение службы каталогов

Служба каталога предоставляет средства организации и упрощения доступа к ресурсам сетевой компьютерной системы. Пользователи и администраторы могут не знать точное название необходимых им объектов. Им достаточно знать один или несколько атрибутов

рассматриваемых объектов. Пользователи обращаются к службе каталогов для запроса списка объектов, отвечающих известным атрибутам (рис. 1-4.). Например, в ответ на запрос «Найти все цветные принтеры на третьем этаже» каталог выдаст сведения обо всех объектах цветных принтеров с атрибутами «цветной» и «третий этаж» (или у которых атрибут местоположения равен «третий этаж»). Служба каталогов позволяет искать объект по одному или нескольким его атрибутам.

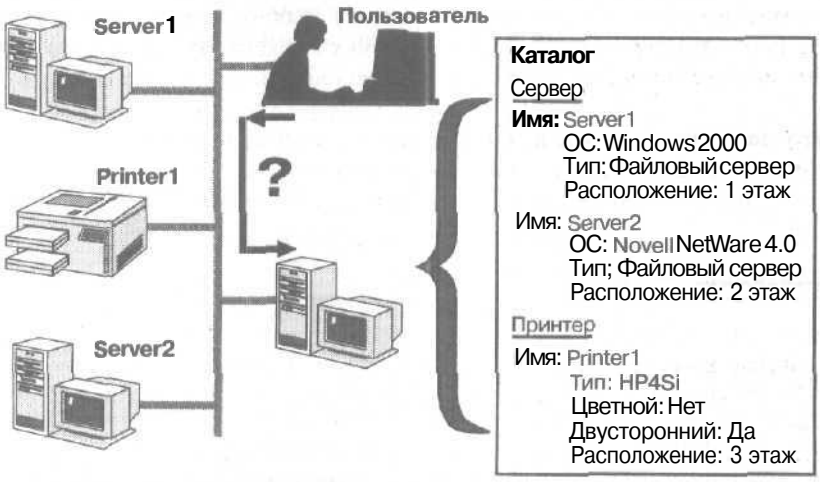


Рис. 1-4. Работа службы каталогов

Служба каталогов выполняет и другие функции:

- назначение безопасности для зашиты объектов БД от внешних вторжений или внутренних пользователей, не имеющих доступа к данным объектам;
- распространение каталога на множество компьютеров сети;
- дублирование каталога для предоставления доступа большему количеству пользователей и отказоустойчивости;
- деление каталога на несколькохранилищ, расположенных на разных компьютерах сети. Это увеличивает доступное для каталога пространство в целом и позволяет хранить больше объектов.

Служба каталогов является как инструментом администрирования, так и инструментом пользователя. При расширении сети приходится управлять все большим количеством объектов ресурсов, и наличие службы каталога становится насущной необходимостью.

Возможности службы каталогов Windows 2000

Active Directory — это служба каталогов в Windows 2000 Server. Active Directory содержит каталог, в котором хранится информация о сетевых ресурсах и службы, предоставляющие доступ к этой информации. Ресурсы, хранящиеся в каталоге, такие, как данные, сведения о принтерах, серверах, базах данных, группах, службах, компьютерах, политике безопасности, — называются *объектами* (object).

Active Directory встроена в Windows 2000 Server и обеспечивает:

- упрощенное администрирование;
- масштабируемость;
- поддержку открытых стандартов;
- поддержку стандартных форматов имен.

Упрощенное администрирование

Active Directory иерархически упорядочивает ресурсы в *домене* (domain) — логическом объединении серверов и других сетевых ресурсов в единое имя домена. Домен является основной единицей репликации и безопасности в сети Windows 2000.

Каждый домен включает один или несколько контроллеров домена. *Контроллер домена* (domain controller) — компьютер под управлением Windows 2000 Server, обеспечивающий доступ пользователей в сеть: вход в систему, проверку подлинности и доступ к каталогу и общим ресурсам. Для простоты администрирования все контроллеры домена равнозначны. Изменения, сделанные на любом из них, реплицируются на остальные контроллеры в домене.

Active Directory дополнительно упрощает администрирование, предоставляя единую точку администрирования всех объектов сети. Благодаря этому администратор может, войдя в систему на одном компьютере, управлять объектами, расположенными на любом компьютере в сети.

Масштабируемость

В Active Directory каталог помещает информацию в разделы, позволяющие хранить множество объектов. В результате каталог расширяется с ростом организации. Это позволяет переходить от небольших установок с несколькими сотнями объектов к большим с миллионами объектов.

Примечание Вы можете распределить информацию каталога по нескольким компьютерам в сети.

Поддержка открытых стандартов

Active Directory соответствует концепции пространства имен Интернета в части службы каталогов Windows 2000. Это позволяет унифицировать и управлять множеством пространств имен, существующих в настоящее время в разнородном программном и аппаратном окружении корпоративных сетей. В качестве системы именования Active Directory использует DNS и способен обмениваться информацией с любым приложением или каталогом, использующим LDAP или протокол передачи гипертекста (HTTP).

Внимание! Active Directory совместно использует информацию с другими службами каталога, поддерживающими LDAP версий 2 и 3, например *службой каталогов Novell* (Novell Directory Services, NDS).

DNS

Поскольку Active Directory для доменного именования и службы поиска использует DNS, имена доменов Windows 2000 также являются именами DNS. Windows 2000 Server применяет динамическую DNS (DDNS), позволяющую клиентам с динамически назначенными адресами напрямую регистрироваться на сервере с работающей службой DNS и динамически обновлять таблицу DNS. В однородной среде DDNS устраняет потребность в других службах именования Интернета, например в *службе имен Интернета для Windows* (Windows Internet Name Service, WINS).

Внимание! Для правильной работы Active Directory и связанного с ней клиентского программного обеспечения необходимо установить и настроить службу **DNS.**

Поддержка LDAP и HTTP

Active Directory отвечает стандартам Интернета и напрямую поддерживает LDAP и HTTP. LDAP — версия протокола доступа к каталогу X.500, разработан в качестве упрощенной альтернативы протокола доступа к каталогам (Directory Access Protocol, DAP). Active Directory поддерживает обе версии LDAP: 2 и 3. HTTP является стандартным протоколом для отображения страниц во всемирной сети Интернет. Пользователи могут просматривать каждый объект в Active Directory, как HTML-страницу в обозревателе Web, пользуясь при запросах и просмотре объектов Active Directory всеми преимуществами знакомой модели обозревателя Web.

Примечание Для обмена информацией между каталогами и приложениями Active Directory использует LDAP. Для получения дополнительной информации о LDAP выполните поиск по ключевому слову «RFC 1777», используя обозреватель Web.

Поддержка стандартных форматов имен

Active Directory поддерживает несколько общих форматов имен, следовательно, для обращения к Active Directory пользователи могут выбрать наиболее привычный формат. В табл. 1-5 описаны некоторые стандартные форматы, поддерживаемые Active Directory.

Табл. 1-5. Стандартные форматы имен, поддерживаемые Active Directory

Формат	Описание
RFC 822	**Применяется** в форме *пользователь@домен*, **знаком** большинству пользователей по адресам электронной почты **Интернета**
HTTP универсальный указатель на ресурсы (URL)	Применяется в форме http://*домен/путь_к_странице*, знаком пользователям обозревателей Web
Универсальные правила именования LDAP URL	Применяется в форме *\\microsoft.com\xl\BUDGET.XLS* в сетях на основе Windows 2000 Server для обращения к общим томам, принтерам и файлам Active Directory поддерживает проект RFC 1779 и использует атрибуты, как показано в следующих примерах: LDAP://someserver.microsoft.com/ CN=FirstnameLastname, OU=sys, OU=product, OU=division, DC=devel где CN — имя; OU — имя организационного подразделения; DC — имя компонента домена; LDAP URL — сервер, на котором расположены службы Active Directory и атрибутное имя объекта

Место Active Directory в архитектуре Windows 2000

На предыдущем занятии вы узнали, что для предоставления приложениям доступа к службам в Windows 2000 применяется сочетание модулей и режимов. Два режима доступа к процессору — *режим ядра* и *пользовательский режим* — отделяют от процессов верхнего уровня низкоуровневые, платформозависимые процессы, защищая приложения от различий платформ и предотвращая прямой доступ приложений к системному коду и данным. Каждое приложение, в том числе и служебные, выполняется в отдельном *модуле* (module) в пользовательском режиме, из которого оно запрашивает системные службы посредством API, получающего ограниченный доступ к системным данным. Процесс приложения начинается в пользовательском режиме и переносится в режим ядра, где происходит его фактическая обработка в защищенной среде. Затем процесс переносится обратно в пользовательский режим. Active Directory работает в безопасной подсистеме в пользовательском режиме. *Эталонный монитор безопасности* (security reference monitor), работающий в режиме ядра, является основным средством установления правил безопасности одноименной подсистемы. На рис. 1-5 показано расположение Active Directory в Windows 2000.

Тесная взаимосвязь службы каталога и подсистемы безопасности является основой для работы распределенных систем Windows 2000. Доступ к любому объекту каталога требует сначала удостоверения личности (проверки подлинности), а затем и проверки разрешений доступа (авторизации), которая выполняется компонентами подсистемы безопасности вместе с эталонным монитором безопасности.

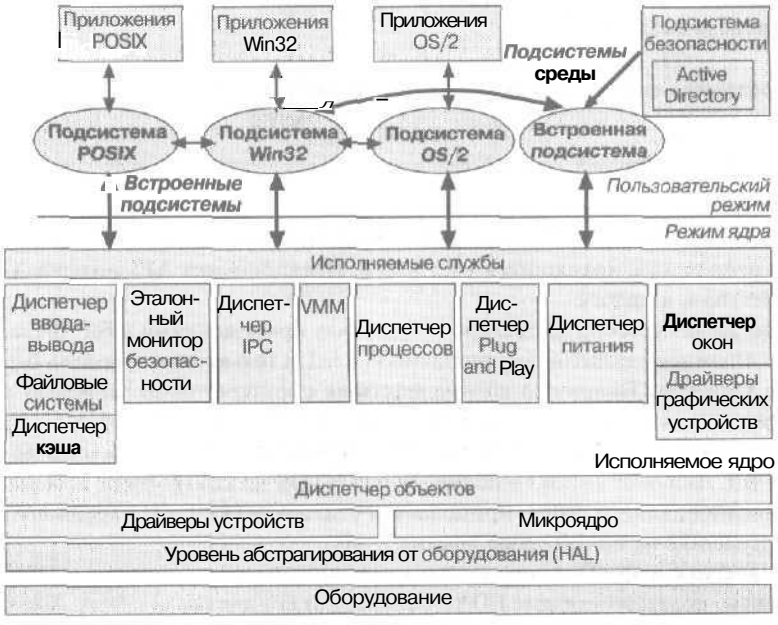


Рис. 1-5. Место Active Directory в архитектуре Windows 2000

Последний управляет доступом применительно к объектам Active Directory.

Архитектура Active Directory

Функциональную структуру Active Directory можно представить в виде многоуровневой архитектуры, в которой уровни являются процессами, предоставляющими клиентским приложениям доступ к службе каталога. Active Directory состоит из трех уровней служб и не-

скольких интерфейсов и протоколов, совместно работающих для предоставления доступа к службе каталога. Три уровня служб охватывают различные типы информации, необходимой для поиска записей в БД каталога. Выше уровней служб в этой архитектуре находятся протоколы и API-интерфейсы, осуществляющие связь между клиентами и службой каталога.

На рис. 1-6 изображены уровни службы Active Directory и соответствующие им интерфейсы и протоколы. Стрелки показывают, как различные клиенты получают при помощи интерфейсов доступ к Active Directory.

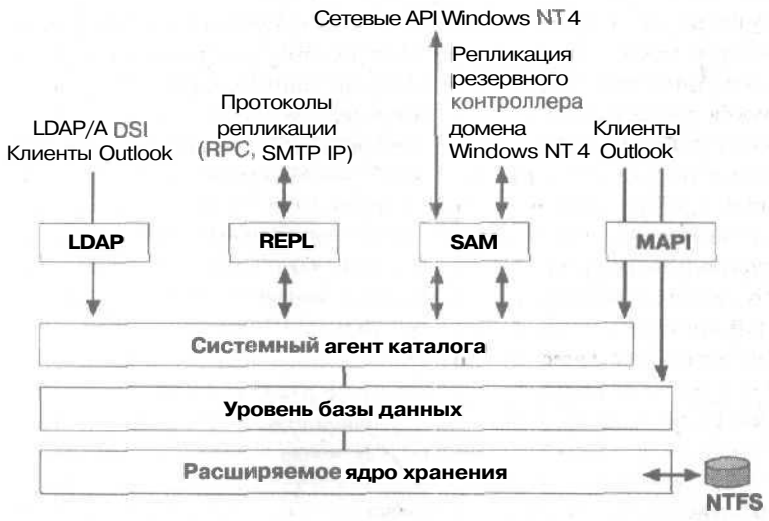


Рис. 1-6. Архитектура **Active Directory**

Ниже перечислены основные компоненты служб.

- Системный агент **каталога** (Directory System Agent, DSA). Выстраивает иерархию родительско-дочерних отношений, хранящихся в каталоге. Предоставляет API-интерфейсы для вызовов доступа к каталогу.
- Уровень БД. Предоставляет уровень абстрагирования между приложениями и БД. Вызовы из приложений никогда не выполняются напрямую к БД, а только через уровень БД.
- **Расширяемое** ядро хранения. Напрямую взаимодействует с конкретными записями в хранилище каталога на основе атрибута относительного составного имени объекта.
- Хранилище данных (файл БД **NTDS.DIT**). Управляется при помощи расширяемого механизма хранения БД, расположенного в папке \Winnt\NTDS на контроллере домена. Для администрирования данного файла применяется утилита NTDSUTIL, хранящаяся в папке \Winnt\system32 на контроллере домена.

Клиенты получают доступ к Active Directory, используя механизмы, поддерживаемые DSA.

- LDAP/ADSI. Клиенты, поддерживающие LDAP, используют его для связи с DSA. Active Directory поддерживает LDAP версии 2 (описан в RFC 1777). Клиенты Windows 2000, Windows 98 и Windows 95 с установленными клиентскими компонентами Active Directory для связи с DSA используют LDAP версии 3. Хотя ADSI является средством абстрагирования API LDAP, Active Directory использует только LDAP.
- API-интерфейс **обмена сообщениями** (Messaging API, MAPI). Традиционные клиенты MAPI, например Microsoft Outlook, подключаются к DSA, используя интерфейс поставщика адресной книги MAPI RPC.

- Диспетчер учетных записей безопасности (Security более Accounts Manager, SAM). Клиенты Windows NT версии 4.0 или более ранней используют интерфейс SAM для связи с DSA. Репликация с резервных контроллеров в домене смешанного режима также выполняется через интерфейс SAM.
- **Репликация (REPL).** При репликации каталога, агенты DSA взаимодействуют друг с другом, используя патентованный интерфейс RPC.

Резюме

На этом занятии вы узнали, что служба каталога является сетевой службой, которая идентифицирует все ресурсы в сети и предоставляет доступ к ним пользователям и приложениям. Служба каталога отличается от каталога тем, что хотя они оба являются источниками информации, служба предоставляет ее пользователям.

Вы также узнали, что служба каталога Active Directory включена в состав Windows 2000 Server. Active Directory состоит из каталога, в котором хранится информация о таких сетевых ресурсах, как данные, принтеры, серверы, базы данных, группы, компьютеры, политики безопасности. Каталог способен расширяться в зависимости от размера установки — он может содержать как несколько сотен объектов для небольших систем, так и миллионы объектов для больших. Active Directory предоставляет упрошенное администрирование, масштабируемость, поддержку открытых стандартов и стандартных форматов имен.

Наконец, вы узнали, что Active Directory выполняется в подсистеме безопасности в пользовательском режиме. Эталонный монитор безопасности, работающий в режиме ядра, является основным средством контроля правил безопасности одноименной подсистемы. Функциональную структуру Active Directory можно представить в виде многоуровневой архитектуры, в которой уровни являются процессами, предоставляющими клиентским приложениям доступ к службе каталога. Active Directory состоит из трех уровней служб и нескольких интерфейсов и протоколов, совместно работающих для предоставления доступа к службе каталога.

Занятие 4. Вход в систему Windows 2000

На этом занятии мы расскажем о процессе входа в систему домена или локального компьютера с использованием диалогового окна Log On To Windows (Вход в Windows), А также объясним процесс проверки подлинности пользователя при входе в систему. Этот обязательный процесс гарантирует, что доступ к ресурсам и данным компьютера сети получат только легальные пользователи.

Изучив материал этого занятия, вы сможете:

- ✓ использовать возможности диалогового окна Log On To Windows;
- ✓ понять, как Windows 2000 выполняет аутентификацию пользователя при его входе в систему домена или локального компьютера;
- ✓ войти в систему изолированного сервера.

Продолжительность занятия — около 10 минут.

Вход в систему домена

Для входа в систему Windows 2000 необходимо предоставить имя пользователя и пароль, Windows 2000 выполняет аутентификацию пользователя для проверки его подлинности во время процесса входа в систему. Доступ к ресурсам и данным компьютера сети смогут получить только легальные пользователи. Windows 2000 выполняет аутентификацию пользователей как при входе в домен, так и при входе в систему локального компьютера.

При загрузке компьютера с Windows 2000 в окне Welcome To Windows (Добро пожаловать в Windows) появится приглашение для входа в систему с предложением нажать одновременно клавиши Ctrl+Alt+Delete (рис. 1-7). Этот способ гарантирует, что вы предоставляете имя и пароль только ОС Windows 2000. Затем Windows 2000 откроет диалоговое окно Log On To Windows (рис. 1-7).

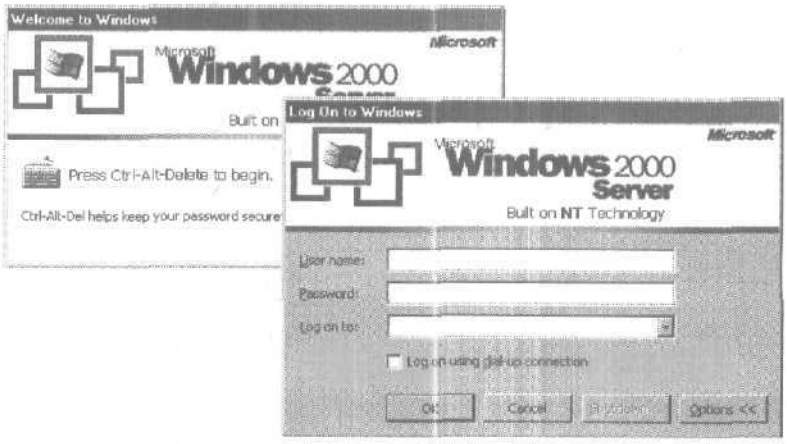


Рис. 1-7. Окно Welcome To Windows (Добро пожаловать в Windows) и диалоговое окно Log On To Windows (Вход в Windows)

В табл. 1-6 описаны элементы по умолчанию диалогового окна Log On To Windows.

Табл. 1-6. Элементы диалогового окна Log On To Windows

Элемент	Описание
Поле User Name (Пользователь)	Уникальное имя пользователя для входа в систему, назначаемое администратором. Для входа в домен по имени пользователя учетная запись пользователя должна находится в каталоге
Поле Password (Пароль)	Пароль необходимо набирать с учетом регистра. На экран вместо символов пароля выводятся звездочки (*). Для предотвращения несанкционированного доступа к ресурсам и данным необходимо держать пароль в секрете
Список Log On To (Вход в)	Выберите домен, содержащий вашу учетную запись. Список содержит все домены доменного дерева
Флажок Log On Using Dial-Up Connection (С использованием удаленного доступа)	Позволяет удаленному пользователю подключаться к серверу домена по модему
Кнопка Shutdown (Завершить работу)	Щелкнув ее, вы закроете все файлы, сохраните данные ОС и подготовите компьютер к безопасному отключению. На компьютерах под управлением Windows 2000 Server кнопка Shutdown по умолчанию недоступна. Так предотвращается возможность использования данного диалогового окна несанкционированными пользователями для завершения работы сервера. Чтобы завершить работу сервера, пользователь должен обладать правом входа в систему на этом сервере
Кнопка Options (Параметры)	Включает и отключает наличие поля списка Log On To и флажка Log On Using Dial-Up Connection

Внимание! Для входа в систему домена или локального компьютера с любого компьютера под управлением Windows 2000 Server пользователь должен обладать разрешением Log On Locally (Локальный вход в систему) или иметь административные привилегии для данного сервера. Это позволяет обезопасить сервер.

Регистрация на локальном компьютере

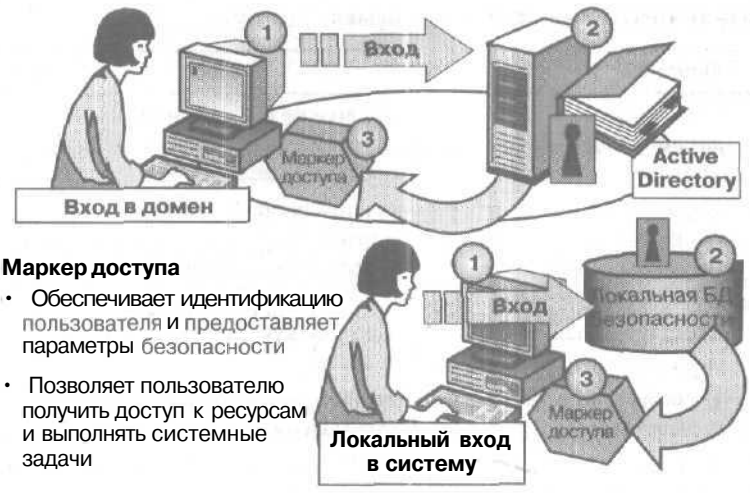
Пользователь сможет войти в систему локально в одном из следующих случаях:

- компьютер включен в рабочую группу;
- компьютер является членом домена, но не его контроллером. Пользователю необходимо выбрать имя компьютера в списке Log On To диалогового окна Log On To Windows.

Примечание Контроллеры домена не поддерживают локальную БД безопасности. Поэтому локальные учетные записи недоступны на контроллерах домена, и пользователям запрещен локальный вход в их систему.

Процесс проверки подлинности Windows 2000

Для доступа к компьютеру с Windows 2000 или к его любому ресурсу пользователю необходимо предоставить имя пользователя и пароль. Способ аутентификации пользователя Windows 2000 зависит от того, входит ли пользователь в домен или локально (рис. 1-8).



■ **Маркер доступа**

- Обеспечивает идентификацию пользователя и предоставляет параметры безопасности
- Позволяет пользователю получить доступ к ресурсам и выполнять системные задачи

Рис. 1-8. Процесс проверки подлинности при входе в Windows 2000

Процесс проверки подлинности состоит из нескольких этапов.

1. Пользователь входит в систему, предоставляя необходимую информацию, включающую имя пользователя и пароль.
   - Если пользователь входит в систему домена, Windows 2000 переадресует эту информацию контроллеру домена.
   - Если пользователь входит в систему локально, Windows 2000 переадресует эту информацию подсистеме безопасности локального компьютера.
2. Windows 2000 сравнивает информацию, введенную при входе в систему с пользовательской информацией, которая хранится в соответствующей БД.
   - При входе пользователя в домен введенная информация сравнивается с данными в копии каталога на контроллере домена.
   - При локальном входе пользователя введенная информация сравнивается с данными в локальной БД безопасности, которую содержит подсистема безопасности локального компьютера.
3. Если информация совпала и учетная запись включена, Windows 2000 создает для пользователя *маркер доступа* (access token) — удостоверение пользователя для компьютеров в домене или для локального компьютера. Маркер доступа содержит параметры безопасности пользователя, включая его *идентификатор безопасности* (security **ID,** SID). Эти параметры безопасности позволяют пользователю получить доступ к соответствующим ресурсам и выполнять определенные системные задачи. SID является уникальным номером, идентифицирующим учетные записи пользователя, группы и компьютера.
4. Если информация не совпадает или учетная запись отключена, доступ в домен или на локальный компьютер для пользователя запрещается.

Примечание Всякий раз при подключении пользователя к компьютеру или к другому ресурсу этот компьютер или ресурс проверяет подлинность пользователя и возвращает маркер доступа. Этот процесс проверки подлинности прозрачен для пользователя.

Практикум: вход в систему изолированного сервера

Вы научитесь входить в систему изолированного сервера в составе рабочей группы из диалогового окна Log On To Windows.

► **Задание: войдите в систему изолированного сервера**

1. Нажмите Ctrl + Alt+Delete.

   Откроется диалоговое окно Log On To Windows (Вход в Windows).

2. В поле User Name (Пользователь) наберите administrator (учетную запись администратора вы настроили во время процедуры установки, описанной в разделе «Об этой книге»). По умолчанию в данном поле отображается имя учетной записи, которая последний раз использовалась на данном компьютере. Если вы входите в систему в первый раз, в поле отобразится имя учетной записи по умолчанию.
3. В поле Password (Пароль) наберите password (тот пароль, который вы назначили учетной записи администратора во время установки). Запомните, что символы пароля следует набирать с учетом регистра. Заметьте, что в целях безопасности вместо символов в строке пароля выводятся звездочки.
4. Щелкните OK.

Резюме

В этом занятии вы узнали, что при загрузке Windows 2000 пользователю для входа в систему предлагается нажать клавиши Ctrl+Alt+Delete. В результате открывается диалоговое окно Log On To Windows, где пользователю предлагается ввести имя и пароль. Кроме того, мы рассказали о различных элементах диалогового окна Log On To Windows, Выполнив практическое задание, вы научились входить в систему изолированного сервера в составе рабочей группы.

Пользователь может войти в систему локального компьютера или в домен, если компьютер является его членом. Если пользователь вводит доменную учетную запись, его имя и пароль проверяет контроллера домена. Если пользователь вводит локальную учетную запись, имя и пароль проверяются в БД безопасности локального компьютера.

Занятие 5. Диалоговое окно Windows Security

Это занятие посвящено функциям и элементам диалогового окна Windows Security (Безопасность Windows).

Изучив материал этого занятия, вы сможете:

- ✓ использовать функции диалогового окна Windows Security.

Продолжительность занятия — около 20 минут.

Использование диалогового окна Windows Security

Диалоговое окно Windows Security предоставляет легкий доступ к важным функциям безопасности. Необходимо, чтобы ваши пользователи их изучили,

Диалоговое окно Windows Security отображает учетную запись текущего рабочего сеанса, имя домена или компьютера, к которому пользователь подключен, дату и время входа пользователя. Эти сведения важны для пользователей, имеющих несколько учетных записей, например обычную учетную запись и запись с административными привилегиями. Для входа в диалоговое окно Windows Security необходимо нажать клавиши Ctrl+Alt+Delete (рис. 1-9).

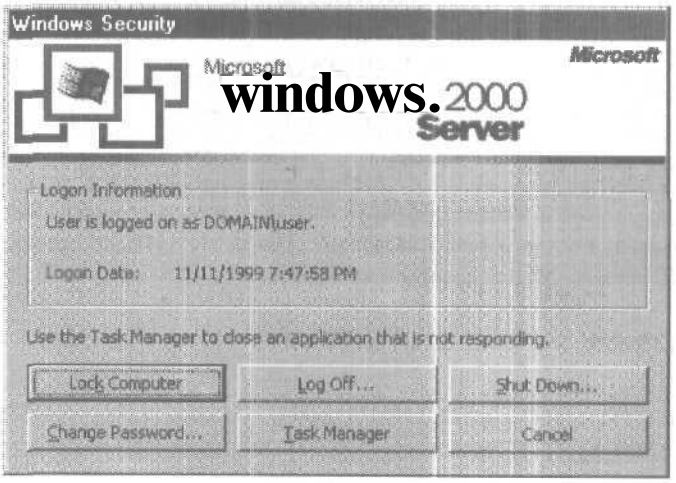


Рис. 1-9. Диалоговое окно Windows Security

В табл. 1-7 описаны кнопки диалогового окна Windows Security.

Табл. 1-7. Кнопки **диалогового окна Windows Security**

Кнопка	Описание
Lock Computer (Блокировка)	Позволяет обезопасить компьютер без выхода из системы. Выполнение программ не прерывается. Применяется, если пользователю надо ненадолго отлучиться. Чтобы разблокировать компьютер, достаточно нажать клавиши Ctrl+Alt+Delete и ввести правильный пароль. Администратор также может разблокировать компьютер, завершив сеанс текущего пользователя системы. Данный выход из системы является принудительным, поэтому существует опасность потери информации
Log Off (Выход из системы)	Позволяет завершить сеанс текущего пользователя и закрыть все работающие программы. При этом Windows 2000 продолжает свою работу .
Shut Down (Завершение работы)	Позволяет закрыть все файлы, сохранить все данные ОС и подготовить компьютер к безопасному отключению
Change Password (Смена пароля)	Позволяет изменить пароль вашей учетной записи. Для создания нового пароля необходимо знать старый. Это единственный способ изменить ваш собственный пароль. Администраторы могут потребовать от пользователей регулярной смены пароля и установить ограничения на используемые пароли в рамках политики учетных записей
Task Manager (Диспетчер задач)	Предоставляет текущий список выполняющихся задач, суммарный объем задействованной памяти и ресурсов процессора и быстрый просмотр их использования каждой программой, программным компонентом или системным процессом. Task Manager также применяется для переключения программ и остановки «зависших» программ
Cancel (Отмена)	Закрывает диалоговое окно Windows Security

Практикум: использование диалогового окна Windows Security

Вы научитесь:

- блокировать компьютер;
- изменять ваш пароль;
- закрывать программу, используя Task Manager;
- выходить из системы Windows 2000;
- завершать работу компьютера.

Для выполнения этих действий вы воспользуетесь диалоговым окном Windows Security.

▶ **Задание 1: заблокируйте компьютер**

1. Нажмите клавиши Ctrl+Alt+Delete.
   Откроется диалоговое окно Windows Security.
2. Щелкните кнопку Lock Computer (Блокировка).
   Откроется окно Computer Locked (Блокировка компьютера) с напоминанием, что компьютер используется, но заблокирован и что его может открыть только администратор или заблокировавший компьютер пользователь.

3. Нажмите клавиши Ctrl+Alt+Delete.

   Откроется диалоговое окно Unlock Computer (Снятие блокировки компьютера).

4. Для разблокирования компьютера в поле Password (Пароль) введите ваш пароль, затем щелкните OK.

► **Задание 2: смените пароль**

1. Нажмите клавиши Ctrl+Alt+Delete.

   Откроется диалоговое окно Windows Security.

2. Щелкните кнопку Change Password (Смена пароля).

   Откроется одноименное диалоговое окно. Заметьте, что в поле User Name (Пользователь) и в списке Log On To (Вход в) отображается имя текущей учетной записи пользователя и имена домена или компьютера.

3. В поле Old Password (Старый пароль) наберите текущий пароль.
4. В полях New Password (Новый пароль) и Confirm New Password (Подтверждение) наберите новый пароль и щелкните OK.

   Смена вашего пароля подтверждена.

5. Щелкните OK для возврата в диалоговое окно Windows Security.
6. Щелкните кнопку Cancel.

► **Задание 3: закройте программу из Task Manager**

Вы откроете программу Wordpad, а затем закроете ее, используя Task Manager. Такой порядок действий применяется, если необходимо закрыть программы, не отвечающие на запросы.

1. Раскройте меню Start\Programs\Accessories (Пуск\Программы\Администрирование) и щелкните WordPad.

   Откроется окно программы WordPad.

2. Напечатайте в нем несколько любых символов или слов.
3. Нажмите клавиши Ctrl+Alt+Delete.

   Откроется диалоговое окно Windows Security.

4. Щелкните кнопку Task Manager (Диспетчер задач).

   Откроется диалоговое окно Windows Task Manager (Диспетчер задач Windows).

5. Щелкните вкладку Applications (Приложения), если она не открылась по умолчанию.

   Откроется список выполняющихся программ.

6. В списке задач щелкните WordPad, затем щелкните кнопку End Task (Снять задачу).

   При прекращении ответов на запросы программой WordPad, откроется окно с показанным на рис. 1-10 сообщением.

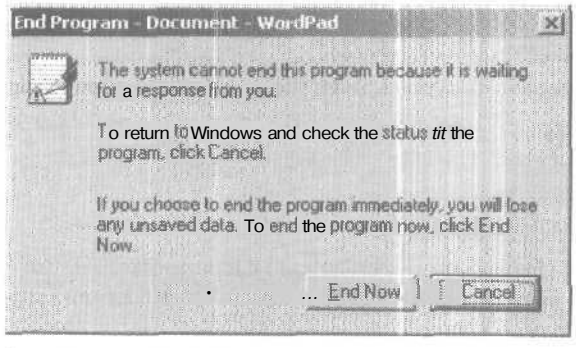


Рис. 1-Ю. Сообщение о снятии программы

Примечание Если программа сама перестала отвечать на запросы (без вызова End Task), в окне станет активной кнопка Wait (Ожидать), позволяющая дождаться ответа приложения.

Если необходимо вернуться в WordPad для сохранения сделанных в документе изменений до того, как WordPad перестал отвечать, щелкните кнопку Cancel. Если необходимо закончить работу WordPad без сохранения изменений, щелкните кнопку End Now (Завершить сейчас) для завершения сеанса WordPad.

Примечание При закрытии программ с использованием Task Manager все не сохраненные данные в этих программах будут утеряны.

7. Выйдите из Task Manager.

▶ Задание 4: выйдите из системы

1. Нажмите клавиши Ctrl + Alt+Delete.
   Откроется диалоговое окно Windows Security.
2. Щелкните кнопку Log Off (Выход из системы).
   Откроется окно с просьбой подтвердить выход из системы.
3. Щелкните кнопку Yes.

Примечание Существует альтернативный способ выхода из системы: в меню Start (Пуск) выберите команду Shut Down (Завершение работы), в открывшемся окне выберите в списке Log Off Administrator (Завершение сеанса Администратор) и щелкните OK.

▶ Задание 5: завершите работу компьютера

1. Нажмите клавиши Ctrl+Alt+Delete.
   Откроется диалоговое окно Windows Security.
2. Щелкните кнопку Shut Down (Завершение работы).
   Откроется окно Shut Down Windows (Завершение работы Windows). По умолчанию в списке выбрано Shut Down (Завершение работы).
3. Щелкните OK для завершения работы или Cancel для возврата в диалоговое окно Windows Security.

Резюме

В этом занятии вы узнали, что для вызова диалогового окна Windows Security (Безопасность Windows) необходимо нажать клавиши Ctrl+Alt+Delete и что в данном окне содержится информация об используемой учетной записи и домене или компьютере, который ее авторизовал. Выполняя практикум, вы из диалогового окна Windows Security заблокировали компьютер, изменили ваш пароль, запустили Task Manager, завершили рабочий сеанс, а затем и работу компьютера.

Закрепление материала

7 J Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении А «Вопросы и ответы» в конце книги.

1. Каково основное различие между Windows 2000 Professional и Windows 2000 Server?

2. В чем состоит главное различие между рабочей группой и доменом?

3. Какие из встроенных подсистем отвечают за работу Active Directory?

4. Каково назначение Active Directory?

5. Что происходит при входе пользователя в домен?

6. Как пользоваться диалоговым окном Windows Security (Безопасность Windows)?

ГЛАВА 2

Введение в Active Directory

В этой главе

Для идентификации пользователей и ресурсов в сети используется служба каталогов. По сравнению с предыдущими версиями Windows в Microsoft Windows 2000 возможности Active Directory значительно расширены. Active Directory представляет собой единое средство управления сетью: позволяет легко добавлять, удалять и перемещать пользователей и ресурсы. Эта глава полностью посвящена Active Directory.

Прежде всего

Для изучения материалов этой главы выполнять никакие предварительные действия не надо.

Занятие 1. Знакомство с Active Directory

Средства Active Directory позволят вам спроектировать структуру каталога так, как это нужно вашей организации. На этом занятии вы познакомитесь с использованием объектов Active Directory и назначением ее компонентов,

Изучив материал этого занятия, вы сможете:

- ✓ объяснить назначение атрибутов объекта и схемы Active Directory;
- ✓ дать определение и описать функции компонентов Active Directory.

Продолжительность занятия — около 30 минут.

Объекты Active Directory

Из главы 1 вы узнали, что, подобно всем службам, которые делают информацию доступной и полезной, Active Directory хранит информацию о сетевых ресурсах. Эти ресурсы, например данные пользователей, описания принтеров, серверов, баз данных, групп, компьютеров и политик безопасности, и называются *объектами* (object).

Объект — это отдельный именованный набор атрибутов, которыми представлен сетевой ресурс. *Атрибуты* (attribute) объекта являются его характеристиками в каталоге. Например, атрибуты *учетной записи пользователя* (user account) могут включать в себя его имя и фамилию, отдел, а также адрес электронной почты (рис. 2-1)

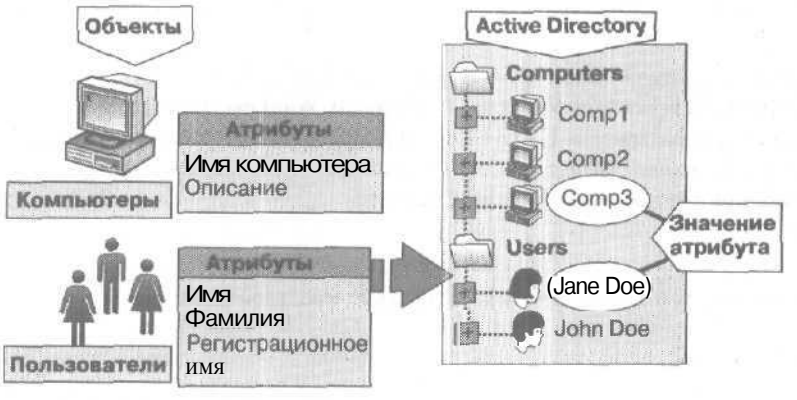


Рис. 2-1. Объекты Active Directory и их атрибуты

В Active Directory объекты могут быть организованы в классы, то есть в логические группы. Примером класса является объединение объектов, представляющих учетные записи пользователей, группы, компьютеры, домены или организационные подразделения (ОП).

Примечание Объекты, которые способны содержать другие объекты, называются *контейнерами* (container). Например, домен — это контейнерный объект, который может содержать пользователей, компьютеры и другие объекты.

Какие именно объекты могут храниться в Active Directory, определяется ее схемой,

Схема Active Directory

Схема Active Directory — это список *определений* (definitions), задающих виды объектов, которые могут храниться в Active Directory, и типы сведений о них. Сами эти определения также хранятся в виде объектов, так что Active Directory управляем ими посредством тех же операций, которые используются и для остальных объектов в Active Directory.

В схеме существуют два типа определений: *атрибуты* и *классы*. Также они называются *объектами схемы* (schema objects) или *метаданными* (metadata).

Атрибуты определяются отдельно от классов. Каждый атрибут определяется только один раз, при этом его разрешается применять в нескольких классах. Например, атрибут Description используется во многих классах, однако определен он в схеме только однажды, что обеспечивает ее целостность.

Классы, также называемые *классами объектов* (object classes), описывают, какие объекты Active Directory можно создавать. Каждый класс является совокупностью атрибутов. При создании объекта атрибуты сохраняют описывающую его информацию. Например, в число атрибутов класса User входят Netwok Address, Home Directory и пр. Каждый объект в Active Directory — это экземпляр класса объектов.

В Windows 2000 Server встроен набор базовых классов и атрибутов. Определяя новые классы и новые атрибуты для уже существующих классов, опытные разработчики и сетевые администраторы могут динамически расширить схему. Например, если Вам нужно хранить информацию о пользователях, не определенную в схеме, можно расширить схему для класса Users. Однако такое расширение схемы — достаточно сложная операция с возможными серьезными последствиями. Поскольку схему нельзя удалить, а лишь деактивировать, и она автоматически реплицируется, вы должны подготовиться и спланировать ее расширение.

Компоненты Active Directory

Active Directory использует компоненты для построения структуры каталога, отвечающей требованиям вашей организации. Логическую структуру организации представляют следующие компоненты Active Directory: домены, организационные подразделения, деревья, леса. Физическая структура организации представлена узлами (физическими подсетями) и контроллерами доменов. В Active Directory логическая структура полностью отделена от физической.

Логическая структура

В Active Directory ресурсы организованы в логическую структуру, отражающую структуру вашей организации. Это позволяет находить ресурс по его имени, а не физическому расположению. Благодаря логическому объединению ресурсов в Active Directory физическая структура сети не важна для пользователей. На рис. 2-2 показаны взаимоотношения компонентов Active Directory.

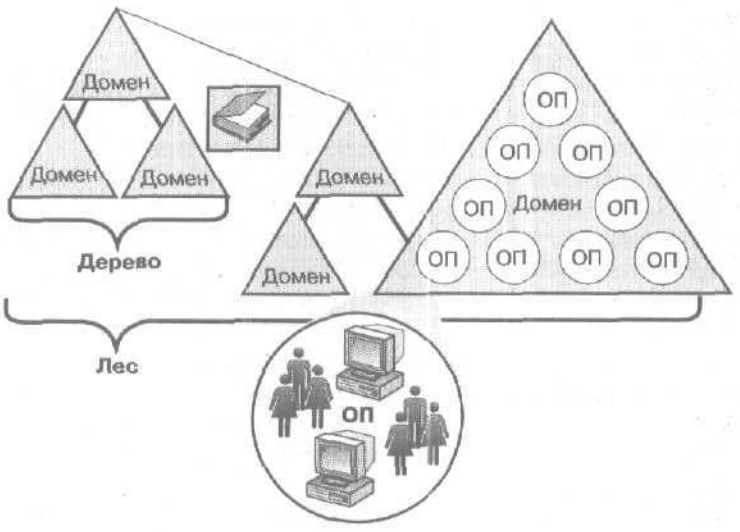


Рис. 2-2. Ресурсы, организованные в логическую иерархическую структуру

Домен

Основным элементом логической структуры в Active Directory является домен, способный содержать миллионы объектов. В домене хранятся объекты, которые считаются «интересными» для сети, «Интересные» объекты — это то, в чем члены сетевого сообщества нуждаются для своей работы: принтеры, документы, адреса электронной почты, базы данных, пользователи, распределенные компоненты и прочие ресурсы. Active Directory может состоять из одного или более доменов.

Объединение объектов в один или более доменов позволяет отразить в сети организационную структуру компании. Общие характеристики доменов таковы:

- все сетевые объекты существуют в пределах домена, а каждый домен хранит информацию только о тех объектах, которые содержит. Теоретически каталог домена может содержать до 10 миллионов объектов, но фактически — это около 1 миллиона объектов на домен;
- домен обеспечивает безопасность. В *списках управления доступом* (access control lists, ACL) определяется доступ к объектам домена. В них заданы разрешения для пользователей, которые могут получить доступ к объекту, и указан тип этого доступа. В Windows 2000 объекты включают файлы, папки, общие ресурсы, принтеры и другие объекты Active Directory. В разных доменах никакие параметры безопасности, например административные права, политики безопасности, списки управления доступом, не пересекаются между собой. Администратор домена имеет абсолютное право устанавливать политики только внутри данного домена.

Организационное подразделение

Организационное подразделение (ОП) — это контейнер, используемый для объединения объектов домена в логические административные группы, отражающие деятельность или бизнес-структуру организации. Организационное подразделение (ОП) может содержать объекты, например учетные записи пользователей, группы, компьютеры, принтеры, приложения, совместно используемые файловые ресурсы, а также другие ОП из того же домена.

Иерархия ОП одного домена не зависит от иерархической структуры другого домена, а каждый домен может иметь свою собственную структуру ОП.

ОП представляют собой средства выполнения административных задач, поскольку являются объектами наименьшего масштаба, которым разрешается делегировать административные полномочия, то есть администрирование пользователей и ресурсов.

На рис. 2-3 видно, что домен domain.com содержит три ОП: US, Orders и Disp. Летом количество заказов на отгрузку увеличивается, поэтому руководство решило нанять дополнительного администратора для отдела заказов. Он должен иметь права только для создания учетных записей пользователей, а также для предоставления пользователям доступа к файлам отдела и сетевым принтерам. Вместо создания другого домена этот запрос можно удовлетворить, передав новому администратору соответствующие права доступа в ОП Orders.

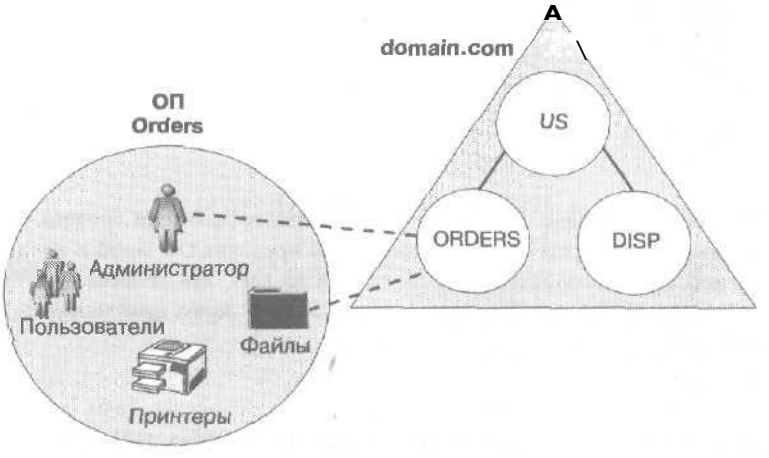


Рис. 2-3. Использование ОП для выполнения административных задач

Если в дальнейшем от нового администратора потребуют создавать учетные записи пользователей в ОП US, Orders и Disp, ему можно предоставить соответствующие права отдельно в каждом ОП. Однако лучше всего предоставить ему полномочия в ОП US, чтобы они были унаследованы в ОП Orders и Disp. По определению, в Active Directory все дочерние объекты (Orders и Disp) наследуют разрешения от своих объектов-родителей (US). Предоставление полномочий на высшем уровне с использованием возможностей их наследования облегчают жизнь администратору,

Дерево

Дерево (tree) — это группа, или иерархически упорядоченная совокупность из одного или более доменов Windows 2000, созданная путем добавления одного или более дочерних доменов к уже существующему родительскому домену. Все домены в дереве используют связанное пространство имен и иерархическую структуру именования. Подробнее пространства имен описаны в следующем занятии. Характеристики деревьев таковы:

- согласно стандартам *доменной системы имен* (Domain Name System, DNS), доменным именем дочернего домена будет объединение его относительного имени и имени родительского домена. На рис. 2-4 microsoft.com является родительским доменом, а us.microsofl.com и uk.microsoft.com — его дочерними доменами. У uk.microsoft.com имеется дочерний домен sls.uk.microsoft.com;
- все домены в пределах одного дерева совместно используют общую схему, которая служит формальным определением всех типов объектов, находящихся в Вашем распоряжении при развертывании Active Directory;

- все домены в пределах одного дерева совместно используют общий глобальный каталог, который служит центральным хранилищем информации об объектах в дереве. Подробнее глобальный каталог рассматривается в следующем занятии.

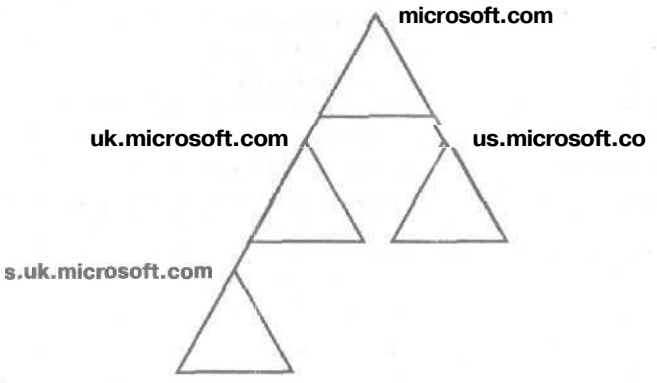


Рис. 2-4. Дерево доменов

Создавая иерархию доменов в дереве, Вы можете поддерживать должный уровень безопасности и регулировать административные полномочия в пределах ОП либо в пределах целого домена. Предоставив пользователю полномочия на ОП, эти разрешения вы сможете распространить вниз по дереву. Такую структуру дерева легко адаптировать к организационным изменениям в компании.

Лес

Лес (forest) — это группа, или иерархически упорядоченная совокупность, из одного или более отдельных и полностью независимых доменных деревьев. Деревья обладают следующими характеристиками:

- у всех деревьев в лесе общая схема;
- у всех деревьев в лесе разные структуры именования, соответствующие своим доменам;
- все домены в лесе используют общий глобальный каталог;
- домены в лесе функционируют независимо друг от друга, однако лес допускает обмен данными в масштабе всей организации;
- между доменами и деревьями доменов существуют двусторонние доверительные отношения.

На рис. 2-5 лес образован из деревьев microsoft.com и msn.com. Пространство имен связано только в пределах каждого дерева.

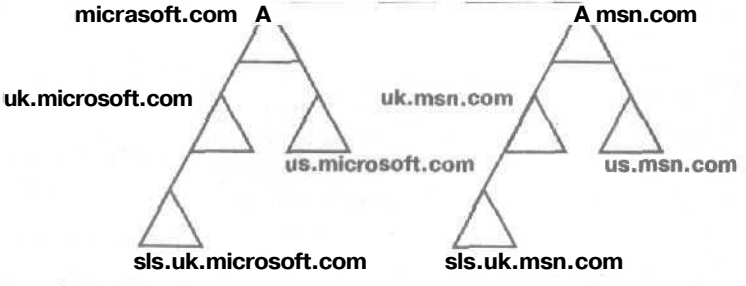


Рис. 2-5. Лес деревьев

Физическая структура

Физические компоненты Active Directory — это узлы и контроллеры домена. Эти компоненты применяются для разработки структуры каталога, отражающей физическую структуру вашей организации.

Сайт

Сайт (site) — это объединение одной или более подсетей IP для создания максимально возможного ограничения сетевого трафика, высоконадежным каналом связи с высокой пропускной способностью. Как правило, границы узла совпадают с границами ЛВС. Когда Вы группируете подсети, следует объединять только те из них, которые между собой связаны быстрыми, дешевыми и надежными сетевыми соединениями. Быстрым считается соединение, обеспечивающее пропускную способность не менее 512 кбит/с, впрочем зачастую достаточно и 128 кбит/с.

В Active Directory сайты не являются частью пространства имен. Просматривая логическое пространство имен, вы увидите, что компьютеры и пользователи сгруппированы в домены и ОП, а не в сайты. Сайты содержат лишь объекты компьютеров и соединений, нужные для настройки межсайтовой репликации.

Примечание Один домен может охватывать несколько географических сайтов, а один сайт может содержать учетные записи пользователей и компьютеры из многих доменов.

Контроллеры домена

Контроллер домена — это компьютер с Windows 2000 Server, хранящий реплику каталога домена (локальную БД домена). Поскольку в домене может быть несколько контроллеров домена, все они хранят полную копию той части каталога, которая относится к их домену.

Ниже перечислены функции контроллеров домена:

- каждый контроллер домена хранит полную копию всей информации Active Directory, относящейся к его домену, а также управляет изменениями этой информации и реплицирует их на остальные контроллеры того же домена;
- все контроллеры в домене автоматически реплицируют между собой все объекты в домене. При внесении в Active Directory каких-либо изменений они на самом деле производятся на одном из контроллеров домена. Затем этот контроллер домена реплицирует изменения на остальные контроллеры в пределах своего домена. Задавая частоту репликаций и количество данных, которое Windows 2000 будет передавать при каждой репликации, можно регулировать сетевой трафик между контроллерами домена;
- важные обновления, например отключение учетной записи пользователя, контроллеры домена реплицируют немедленно;
- Active Directory использует репликацию с несколькими *хозяевами* (multimaster replicaton), в котором ни один из контроллеров домена не является главным. Все контроллеры равноправны, и каждый из них содержит копию базы данных каталога, в которую разрешается вносить изменения. В короткие периоды времени информация в этих копиях может отличаться до тех пор, пока все контроллеры не синхронизируются друг с другом;
- наличие в домене нескольких контроллеров обеспечивает отказоустойчивость. Если один из контроллеров домена недоступен, другой будет выполнять все необходимые операции, например записывать изменения в Active Directory;

- контроллеры домена управляют взаимодействием пользователей и домена, например находят объекты Active Directory и распознают попытки входа в сеть.

Резюме

На этом занятии вы узнали, что объект — это отдельный именованный набор атрибутов, которым представлен сетевой ресурс Active Directory. Атрибуты объекта описывают характеристики определенного ресурса в каталоге. В Active Directory объекты можно организовать в классы, которые служат логическими определениями объектов. Схема Active Directory содержит формальное определение содержания и структуры каталога, в том числе все атрибуты и классы объектов.

Также Active Directory предлагает метод проектирования структуры каталога, отвечающей потребностям и структуре конкретной организации. Логическая структура иерархии домена в Active Directory полностью отделена от физической структуры.

Логическое объединение ресурсов в Active Directory позволяет искать ресурс по его имени, а не по физическому расположению. Ключевым элементом логической структуры в Active Directory является домен, который хранит информацию только о тех объектах, которые он содержит. Организационное подразделение (ОП) — это контейнер, используемый для организации объектов в логические административные группы. Деревом называется иерархически упорядоченное объединение одного или более доменов Windows 2000, которые используют связанное пространство имен, а лесом — иерархически упорядоченное объединение одного или более деревьев, которые образуют раздельное пространство имен.

Физическая структура Active Directory основана на сайтах и контроллерах домена. Сайт — это группировка одной или более подсетей IP, объединенных высокоскоростными каналами связи. Контроллером домена называется компьютер с Windows 2000 Server, хранящий реплику каталога домена.

Занятие 2. Концепции работы Active Directory

Вместе с Active Directory введено несколько новых понятий, например глобальный каталог, репликация, доверительные отношения, пространство имен DNS и правила наименования. Важно понимать их значение применительно к Active Directory.

Изучив материал этого занятия, вы сможете:

- ✓ объяснить назначение глобального каталога в Active Directory;
- ✓ объяснить репликацию Active Directory;
- ✓ объяснить отношения защиты между доменами в дереве (доверительные отношения);
- ✓ описать пространство имен DNS, используемое в Active Directory;
- ✓ описать используемые в Active Directory правила наименования.

Продолжительность занятия — около 20 минут.

Глобальный каталог

Глобальный каталог (global catalog) — это центральное хранилище информации об объектах в дереве или лесе (рис, 2-6). По умолчанию глобальный каталог автоматически создается на первом контроллере домена в лесе, и этот контроллер становится *сервером глобального каталога* (global catalog server). Он хранит полную реплику атрибутов всех объектов в своем домене, а также частичную реплику атрибутов всех объектов для каждого домена в лесе. Эта частичная реплика хранит те атрибуты, которые чаще других нужны при поиске (например, по имени или фамилии пользователя, по регистрационному имени пользователя и т. д.). Атрибуты объекта в глобальном каталоге наследуют исходные разрешения доступа из тех доменов, откуда они были реплицированы, и таким образом, в глобальном каталоге обеспечивается безопасность данных.

Глобальный каталог выполняет две важные функции;

- обеспечивает регистрацию в сети, предоставляя контроллеру домена информацию о членстве в группах;
- обеспечивает поиск информации в каталоге независимо от расположения данных.

Когда пользователь регистрируется в сети, глобальный каталог предоставляет контроллеру домена, который обрабатывает информацию о процессе регистрации в сети, полные данные о членстве учетной записи в группах. Если в домене только один контроллер, сервер глобального каталога и контроллер домена — это один и тот же сервер. Если же в сети несколько контроллеров домена, то глобальный каталог располагается на том из них, который сконфигурирован для этой роли. Если при попытке регистрации в сети глобальный каталог недоступен, то пользователю разрешается зарегистрироваться лишь на локальном компьютере.

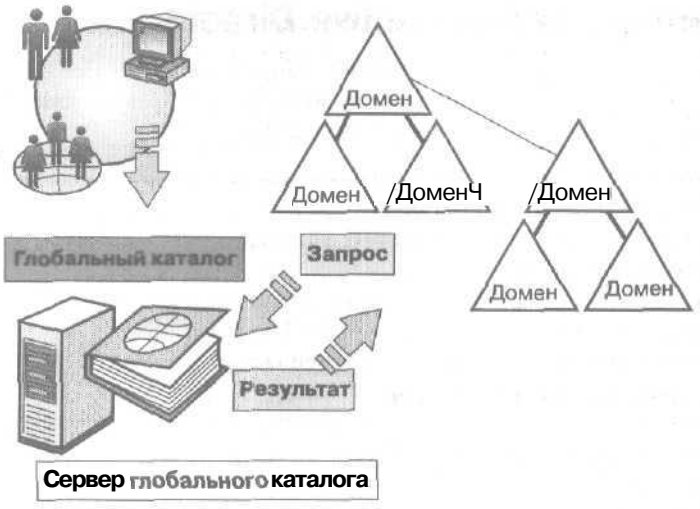


Рис. 2-6. Глобальный каталог — центральное хранилище информации

Внимание! Если пользователь является членом группы Domain Admins (Администраторы домена), то он сможет зарегистрироваться в сети, даже когда глобальный каталог недоступен,

Глобальный каталог позволяет максимально быстро и с минимальным сетевым трафиком отвечать на запросы программ и пользователей об объектах, расположенных в любом месте леса или дерева доменов. Глобальный каталог может разрешить запрос в том же домене, в котором этот запрос был инициирован, так как информация обо всех объектах всех доменов в лесе содержится в едином глобальном каталоге. Поэтому поиск информации в каталоге не вызывает лишнего трафика между доменами.

В качестве сервера глобального каталога вы можете по своему выбору настроить любой контроллер домена либо дополнигельно назначить на эту роль другие контроллеры домена. Выбирая сервер глобального каталога, надо учесть, справится ли сеть с трафиком репликации и запросов. Впрочем, дополнительные серверы позволят ускорить время отклика на запросы пользователей. Рекомендуется, чтобы каждый крупный сайт предприятия имел собственный сервер глобального каталога.

Репликация

Необходимо, чтобы с любого компьютера в дереве доменов или лесе пользователи и службы могли все время получать доступ к информации в каталоге. Репликация позволяет отражать изменения в одном контроллере домена на остальных контроллерах в домене. Информация каталога реплицируется на контроллеры домена как в пределах узлов, так и между ними.

Виды реплицируемой информации

Хранимая в каталоге информация делится на три категории, которые называются *разделами каталога* (directory partition). Раздел каталога служит объектом репликации. В каждом каталоге содержится следующая информация:

- **информация о схеме** — определяет, какие объекты разрешается создавать в каталоге и какие у них могут быть атрибуты;

- **информация о конфигурации** — описывает логическую структуру развернутой сети, например структуру домена или топологию репликации. Эта информация является общей для всех доменов в дереве или лесе;
- **данные домена** — описывают все объекты в домене. Эти данные относятся только к одному определенному домену, Подмножество свойств всех объектов во всех доменах хранится в глобальном каталоге для поиска информации в дереве доменов или лесе,

Схема и конфигурация реплицируются на все контроллеры домена в дереве или лесе. Все данные определенного домена реплицируются на каждый контроллер именно этого домена. Все объекты каждого домена, а также часть свойств всех объектов в лесе реплицируются в глобальный каталог.

Контроллер домена хранит и реплицирует:

- информацию о схеме дерева доменов или леса;
- информацию о конфигурации всех доменов в дереве или лесе;
- все объекты и их свойства для своего домена. Эти данные реплицируются на все дополнительные контроллеры в домене, Часть всех свойств объектов домена реплицируется в глобальный каталог для организации поиска информации.

Глобальный каталог хранит и реплицирует:

- информацию о схеме в лесе;
- информацию о конфигурации всех доменов в лесе;
- часть свойств всех объектов каталога в лесе (реплицируется только между серверами глобального каталога);
- все объекты каталога и все их свойства для того домена, в котором расположен глобальный каталог.

Внимание! Из-за полной синхронизации всех данных в домене расширение схемы может пагубно влиять на большие сети.

Как работает репликация

Active Directory реплицирует информацию в пределах сайта чаще, чем между сайтами, сопоставляя необходимость в обновленной информации каталога с ограничениями по пропускной способности сети.

Репликация внутри сайта

В пределах сайта Active Directory автоматически создает топологию репликации между контроллерами одного домена с использованием кольцевой структуры. Топология определяет путь передачи обновлений каталога между контроллерами домена до тех пор, пока обновления не будут переданы на все контроллеры домена (рис. 2-7).

Кольцевая структура обеспечивает существование минимум двух путей репликации от одного контроллера домена до другого, и если один контроллер домена временно становится недоступен, то репликация на остальные контроллеры домена все равно продолжится.

Дабы убедиться, что топология репликации все еще эффективна, Active Directory периодически ее анализирует. Если вы добавите или уберете контроллер домена из сети или узла, то Active Directory соответственно изменит топологию.

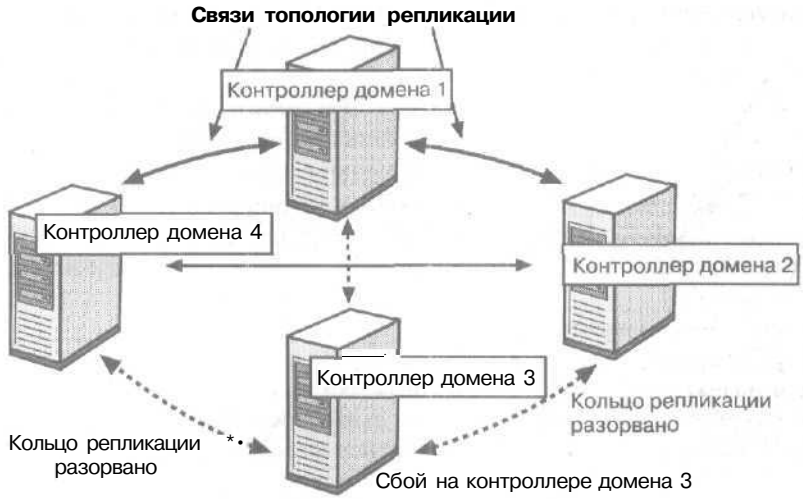


Рис. 2-7. **Топология репликации**

Репликация между сайтами

Для обеспечения репликации между узлами нужно представить сетевые соединения в виде *связей сайтов* (site link). Active Directory использует информацию о сетевых соединениях для создания объектов-соединений, что обеспечивает эффективную репликацию и отказоустойчивость.

Вы должны предоставить информацию о применяемом для репликации протоколе, стоимости связи сайтов, о времени доступности связи и о том, как часто она будет использоваться. Исходя из этого, Active Directory определит, как связать сайты для репликации. Лучше выполнять репликацию в то время, когда сетевой трафик минимален,

Доверительные отношения

Доверительное отношение (trust realtionship) — это такая связь между двумя доменами, при которой доверяющий домен признает регистрацию в сети в доверяемом домене. Active Directory поддерживает две формы доверительных отношений.

- **Неявные двусторонние транзитивные доверительные отношения (implicit two-way transitive** trust). Это отношения между родительским и дочерним доменами в дереве и между доменами верхнего уровня в лесе. Они определены по умолчанию, то есть доверительные отношения между доменами в дереве устанавливаются и поддерживаются неявно (автоматически). Транзитивные доверительные отношения — это функция протокола идентификации Kerberos, по которому в Windows 2000 проводится авторизация и регистрация в сети.

  Как показано на рис. 2-8, транзитивные доверительные отношения означают следующее: если Домен А доверяет Домену В, а Домен В доверяет Домену С, то Домен А доверяет Домену С. В результате присоединенный к дереву домен устанавливает доверительные отношения с каждым доменом в дереве. Эти доверительные отношения делают все объекты в доменах дерева доступными для всех других доменов в дереве.

  Транзитивные доверительные отношения между доменами устраняют необходимость в междоменных доверительных учетных записях. Домены одного дерева автоматически устанавливают с родительским доменом двусторонние транзитивные доверительные отношения. Благодаря этому пользователи из одного домена могут получить доступ к

ресурсам любого другого домена в дереве (при условии, что им разрешен доступ к этим ресурсам).

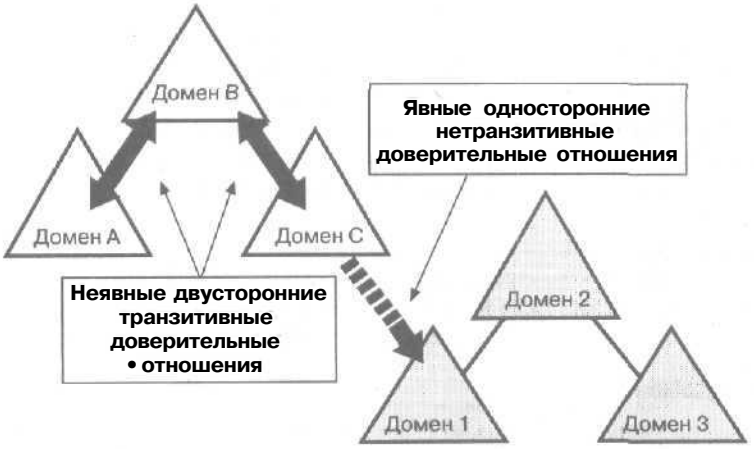


Рис. 2-8. Два вида доверительных отношений в Active Directory

- **Явные односторонние нетранзитивные доверительные отношения (explicit one-way nontransitive trust).** Это отношения между доменами, которые не являются частью одного дерева. Нетранзитивные доверительные отношения ограничены отношениями двух доменов и не распространяются ни на какие другие домены в лесе. В большинстве случаев вы сами можете явно (вручную) создать нетранзитивные доверительные отношения. Так, на рис. 2-8 показаны односторонние транзитивные доверительные отношения, в которых Домен С доверяет Домену 1, так что пользователи в Домене 1 могут получить доступ к ресурсам в Домене С. Явные односторонние нетранзитивные доверительные отношения — это единственно возможные отношения между:
  - доменом Windows 2000 и доменом Windows NT;
  - доменом Windows 2000 в одном лесе и доменом Windows 2000 в другом лесе;
  - доменом Windows 2000 и *сферой* (realm) MIT Kerberos V5, что позволяет клиентам из сферы Kerberos регистрироваться в домене Active Directory для получения доступа к сетевым ресурсам.

Пространство имен DNS

Подобно всем службам каталогов, изначально Active Directory считается пространством имен. *Пространство имен* (namespace) — это любая ограниченная область, в которой можно разрешить имя. *Разрешение имени* (name resolution) — процесс перевода имени в некий объект или информацию, которую это имя представляет. Пространство имен Active Directory основано на системе имен DNS, и это позволяет взаимодействовать с сетью Интернет. Частные сети широко используют DNS для разрешения имен компьютеров, а также для поиска компьютеров в локальной сети и Интернете. Применение DNS дает следующие преимущества:

- имена DNS легче запомнить, чем IP-адреса;
- имена DNS реже меняются, чем IP-адреса. IP-адрес сервера может измениться, а имя сервера останется прежним;
- DNS позволяет пользователям подключаться к локальным серверам, применяя те же правила именования, что и в Интернете.

Примечание Подробности см. в RFC 1034 и 1035. Для ознакомления с этими документами на поисковом узле Интернета введите ключевое слово **RFC 1034** или **RFC 1035.**

Поскольку Active Directory использует DNS в качестве службы именования и поиска своих доменов, то имена доменов Windows 2000 также являются именами DNS. Windows 2000 Server применяет *динамическую доменную систему именования* (Dynamic DNS, DDNS), что позволяет клиентам, которым адреса выделяются динамически, регистрироваться прямо на DNS-сервере и динамически обновлять таблицу DNS. Наличие DDNS в однородных сетях позволяет отказаться от других служб именования Интернета, например Windows Internet Name Service (WINS).

Внимание! Для правильной работы Active Directory и взаимодействующего с ней клиентского программного обеспечения надо установить и сконфигурировать службу DNS.

Пространство имен домена

Пространство имен домена (domain namespace) — это схема именования, которая обеспечивает иерархическую структуру для базы данных DNS. Каждый *узел* (node) этой иерархии представляет собой раздел базы данных DNS. Такие узлы называются *доменами.*

База данных DNS индексирована по имени, поэтому каждый домен должен иметь имя. При добавлении домена к иерархии имя родительского домена добавляется к имени дочернего домена, который называется *поддоменом* (subdomain). Следовательно, имя домена определяет его место в иерархии. Например, на рис. 2-9 имя sales.microsoft.com определяет домен sales в качестве поддомена для microsoft.com, а microsoft в качестве поддомена для домена com.

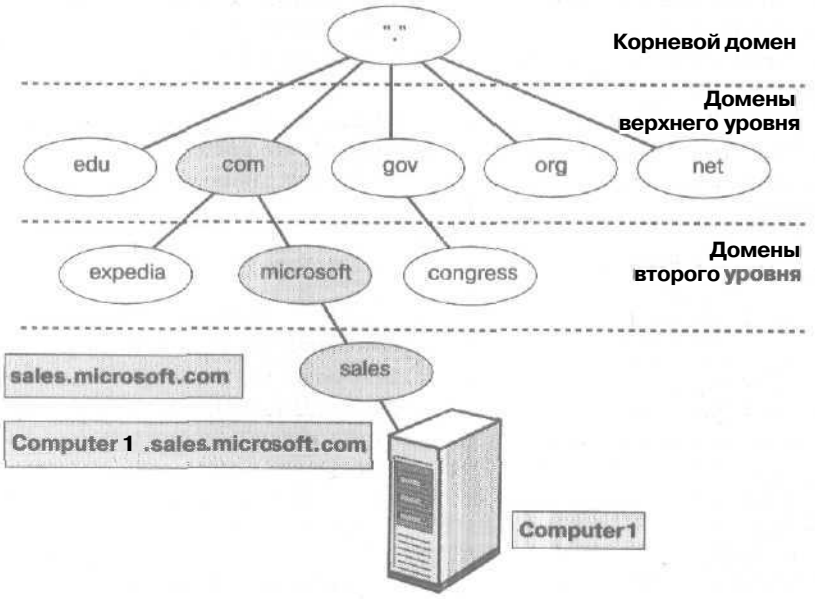


Рис. 2-9. Иерархическая структура пространства имен домена

Иерархическая структура пространства имен домена обычно состоит из корневого домена, доменов верхнего уровня, доменов второго уровня и имен узлов.

Существуют два типа пространств имен:

- **связанное пространство имен** (contiguous namespace) — имя дочернего объекта в иерархии всегда содержит имя родительского домена. Дерево — это связанное пространство имен;
- **раздельное пространство имен** (disjointed namespace) — имена родительского объекта и его потомка напрямую не связаны одно с другим, Лес — это раздельное пространство имен. Например, рассмотрим следующие имена доменов:
  - www.microsoft.com;
  - msdn.microsoft.com;
  - www.msn.com.

Первые два имени доменов составляют связанное пространство имен в пределах microsoft.com, а третье — является частью раздельного пространства имен.

Примечание Термин *домен в* контексте DNS не относится к понятию домена, которое используется в службе каталогов Windows 2000. Домен Windows 2000 — это группа компьютеров и устройств, которую администрируют, как единое целое.

Корневой домен

Это вершина иерархии; он обозначается точкой (.). Корневой домен Интернета управляется несколькими организациями, в частности Network Solutions, Inc.

Домены верхнего уровня

Домены верхнего уровня построены по организационному признаку либо по географическому положению. В табл. 2-1 приведены примеры имен доменов верхнего уровня.

Табл. 2-1. Примеры доменов верхнего уровня

Домен верхнего уровня	Описание
gov	Правительственные организации
com	Коммерческие организации
edu	Образовательные организации
org	Некоммерческие организации
net	Коммерческие сети или узлы Интернета

Примечание Частью доменов верхнего уровня могут быть также двухбуквенные коды стран, например ru для России или аи для Австралии.

Домены верхнего уровня могут содержать домены второго уровня и имена узлов,

Домены второго уровня

Такие организации, как Network Solutions, Inc., регистрируют уже существующие в Интернете домены второго уровня для частных лиц и организаций. Имя второго уровня состоит из двух частей: имени верхнего уровня и уникального имени второго уровня. В табл, 2-2 приведены примеры доменов второго уровня.

Табл. 2-2. **Примеры доменов второго уровня**

Домен второго уровня	*Описание*
ed.gov	Департамент образования Соединенных Штатов
microsoft.com	Корпорация Microsoft
stanford.edu	Стэндфордекий Университет
w3.org	Консорциум World Wide Web
pm.gov.au	Премьер-министр Австралии

Примечание В случае использования кодов стран gov.au, edu.au и com.au являются доменами верхнего уровня. Если же имя построено как *имя_организации*.au, аи является доменом верхнего уровня.

Имя узла

Указывает на определенный компьютер иди ресурс в Интернете или в частной сети. Например, на рис. 2-9 Computer1 — это имя узла. Это самая левая часть *полного доменного имени* (Fully Qualified Domain Name, **FQDN),** которое описывает положение компьютера в доменной иерархии. На рис. 2-9 имя computer1.sales.microsoft.com. (в том числе и завершающая точка, которая обозначает корневой домен) является полным доменным именем.

Примечание Имя узла — это не то же самое, что имя компьютера, имя NetBIOS или другого протокола именования.

Зона

Это отдельная часть пространства имен домена, которая служит для разделения пространства имен на управляемые секции.

Для распределения административных задач между несколькими группами домен разделяется на несколько зон. Так, на рис. 2-10 пространство имен домена microsoft.com разделено на две зоны. Это позволяет одному администратору управлять доменами microsoft и sales, а другому — доменом development.

Зона должна содержать связанное пространство имен. Например, в структуре, показанной на рис. 2-10, невозможно создать зону, которая состояла бы только из доменов sales.microsoft.com и development.microsoft.com, потому что домены sales и development — не целостные.

Привязки имен к IP-адресам для зоны хранятся в *файле зоны.* Каждая зона привязана к определенному домену, который называется *корневым доменом зоны* (zone's root domain). Файл зоны содержит информацию только о поддоменах в пределах своей зоны.

На рис. 2-10 microsoft.com является корневым доменом для Zone1, а его файл зоны содержит привязки имен к IP-адресам для доменов microsoft и sales. Корневым доменом для Zone2 является development, а его файл зоны содержит соответствия привязки имен к IP-адресам только для домена development. База данных Zone1 не содержит привязок для домена development, хотя он и является поддоменом для microsoft.

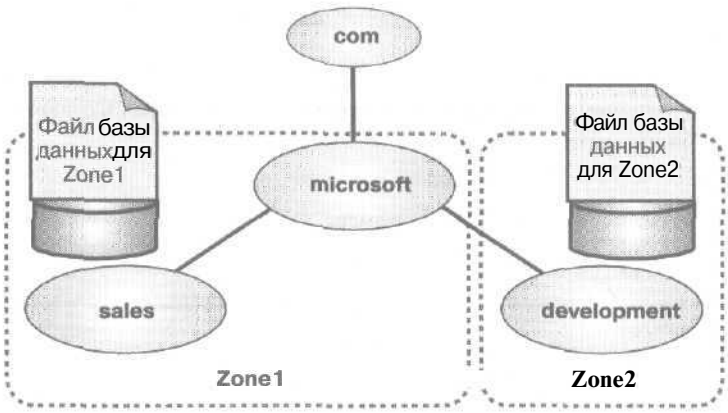


Рис. 2-10. Деление доменного пространства имен на зоны

Сервер имен

Хранит файл зоны, содержащий сведения для одной или нескольких зон и, как часто говорят, полномочный в пространстве имен соответствующей зоны.

На одном из *серверов имен* (name server) содержится главный файл базы данных зоны, который называется *основным файлом зоны* (primary zone database file). То есть в каждой зоне должен быть хотя бы один сервер имен. Такие изменения в зоне, как добавление доменов или компьютеров, выполняются на том сервере, который хранит основной файл базы данных зоны.

Остальные серверы имен в зоне страхуют сервер, содержащий основной файл БД юны. Использование нескольких серверов имен дает следующие преимущества:

- выполнение зонных передач. Добавочные серверы имен получают копию БД зоны с того сервера, который хранит основной файл зоны, и периодически запрашивают с него обновления данных зоны. Это и называется *зонной передачей* (zone transfer);
- избыточность. Если происходит сбой на сервере, хранящем основной файл зоны, то дополнительные серверы продолжают обслуживать клиентов;
- увеличение скорости доступа для удаленных клиентов. Если таких клиентовмного, то стоит применить дополнительные серверы имен, чтобы уменьшить трафик запросов через ГВС-соединения;
- уменьшение нагрузки на сервер, который хранит основной файл зоны.

Примечание Подробности о настройке DNS для Active Directory см. в главе 5.

Правила именования

Каждый объект в Active Directory идентифицируется по имени. В Active Directory применяются разные правила именования: *составные имена* (distinguished name, DN), *относительные составные имена* (relative distinguished name, RDN), *глобально уникальные идентификаторы* (globally unique identifier, GU1D) и *основные имена пользователей* (user principal name, UPN).

Составное имя

Каждый объект в Active Directory имеет *составное имя* (distinguished name, DN). Оно уникально идентифицирует объект и содержит информацию для клиента, достаточную для

извлечения объекта из каталога. DN включает имя домена, содержащего объект, и полный путь к объекту по иерархии контейнеров.

Например, вот какое DN идентифицирует объект-пользователя Firstname Lastname в домене microsoft.com (где Firstname и Lastname представляют собой реальные имя и фамилию в учетной записи пользователя):

```
DC=COM/DC=Microsoft/OU=dev/CN=Users/CN=Firstname Lastname
```

В таблице описаны атрибуты, использованные в примере.

Табл. 2-3. Атрибуты составного имени

Атрибут	Описание
DC	Имя компонента домена
OU	Имя ОП
CN	Общее имя

Составные имена должны быть уникальными. Active Directory не допускает их дублирования.

Примечание Дополнительная информация о составных именах содержится в RFC 1779. Для ознакомления с этими документами на поисковом узле Интернета введите ключевое слово **RFC 1779.**

Относительное составное имя

Active Directory поддерживает поиск по атрибутам, то есть вы сможете найти объект, даже не зная его точного DN или если это имя было изменено. *Относительное составное имя* (relative distinguished name, RDN) объекта — это часть имени, которое является атрибутом самого объекта. В предыдущем примере RDN для объекта-пользователя Firstname Lastname — Firstname Lastname, а RDN родительского объекта — Users.

Active Directory позволяет копировать RDN объектов, однако в рамках одного организационного подразделения **(ОП)** такие имена должны быть уникальны. Например, если в ОП есть учетная запись пользователя Jane Doe, добавить в то же ОП запись пользователя с таким же именем нельзя. Однако в разных ОП разрешено создать одинаковые учетные записи Jane Doe, поскольку каждая будет иметь уникальное DN (рис. 2-11).

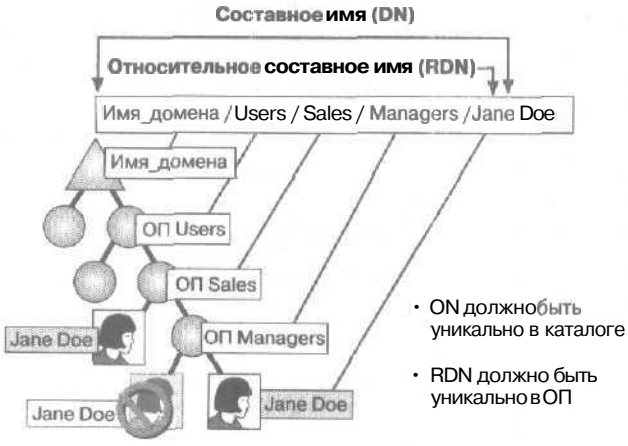


Рис. 2-11. Составные имена и относительные составные имена

Глобально уникальный идентификатор

Глобально уникальный идентификатор (globally unique identifier, GUID) — это гарантированно уникальный 128-разрядный номер, назначенный при создании объекта. Он не изменяется даже после перемещения или переименования объекта. Приложения могут хранить GUID объекта и гарантированно находить объект независимо от его текущего DN.

В ранних версиях Windows NT ресурсы домена были связаны с *идентификатором безопасности* (security identifier, SID), формируемом внутри домена, то есть SID оставался уникальным только в рамках домена. GUID уникален во всех доменах, причем это его качество сохраняется при перемещении объектов из одного домена в другой.

Основное имя пользователя

Основное имя пользователя (user principal name, UPN) — это дружественное имя, которое короче DN и легче для запоминания. Основное имя пользователя состоит из сокращенного имени, представляющего пользователя и, как правило, DNS-имени домена, в котором находится объект USER. Формат основного имени таков: имя пользователя, символ @, суффикс основного имени пользователя. Например, пользователь James Smith в microsoft.-com мог бы иметь основное имя вида username@microsoft.com. UPN не зависит от DN объекта-пользователя, поэтому объект User разрешается перемешать или переименовывать, не изменяя регистрационного имени пользователя.

Резюме

На этом занятии вы узнали несколько новых понятий, используемых в Active Directory, например глобальный каталог, репликация, доверительные отношения, пространство имен DNS и правила именования.

Глобальный каталог — это служба и место физического хранения, которое содержит реплику определенных атрибутов каждого объекта в Active Directory. Глобальный каталог применяется для поиска объектов в сети без репликации всей информации домена между контроллерами доменов.

Репликация в Active Directory обеспечивает отражение изменений в одном из контроллеров домена на остальные контроллеры. Active Directory автоматически формирует в сайте кольцевую топологию для репликации между контроллерами одного домена. Вы можете повлиять на топологию репликации, настраивая связи сайтов.

Доверительные отношения — это связь между двумя доменами, при которой доверяющий домен признает регистрацию в сети, произведенную в доверяемом домене. Active Directory поддерживает два вида доверительных отношений: неявные двусторонние транзитивные доверительные отношения и явные односторонние нетранзитивные отношения.

Active Directory использует DNS в качестве службы именования и поиска компьютеров в домене, поэтому имена доменов Windows 2000 являются также и DNS-именами. Windows 2000 Server применяет DDNS, так что клиенты с динамически выделяемыми адресами получают право регистрироваться прямо на DNS-сервере и динамически обновлять таблицу DNS. Пространства имен бывают связанные и раздельные.

И, наконец, вы узнали о правилах именования в Active Directory: о составных именах (DN), относительных составных именах (RDN), глобально уникальных идентификаторах (GU1D), основных именах пользователей (UPN).

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении А «Вопросы и ответы» в конце книги.

1. Что такое схема Active Directory?

2. Каково назначение организационного подразделения (ОП)?

3. Что такое сайты и домены и чем они отличаются?

4. Чем отличаются неявные двусторонние транзитивные доверительные отношения и явные односторонние нетранзитивные отношения?

ГЛАВА 3

Задачи и средства администрирования Active Directory

В этой главе

Мы познакомим вас с задачами и средствами администрирования службы каталогов Active Directory. К задачам относятся: настройка и администрирование Active Directory, администрирование объектов пользователей и групп, защита сетевых ресурсов, администрирование рабочих столов компьютеров, безопасность Active Directory, управление работой Active Directory и удаленная установка Windows 2000. К основным средствам управления относятся: средства администрирования, оснастки (расположены в меню Start\Administrative Tools) и Task Scheduler (Планировщик задач).

Прежде всего

Для изучения материалов этой главы необходимо:

- выполнить процедуру установки, описанную во вводной главе;
- уметь регистрироваться в Windows 2000;

Занятие 1. Задачи администрирования Active Directory

На этом занятии мы расскажем о задачах администрирования Active Directory.

Изучив материал **этого занятия, вы** сможете:

- ✓ описать задачи администрирования Active Directory Windows 2000.

Продолжительность занятия — около 5 минут.

Задачи администрирования Active Directory Windows 2000

Администрирование Active Directory Windows 2000 включает как конфигурирование, так и повседневное обслуживание. Административные задачи можно разделить на восемь категорий (табл. 3-1).

Табл. 3-1. Задачи администрирования Active Directory

Категория	Перечень задач
Конфигурирование Active Directory	Планирование, развертывание, управление, наблюдение, оптимизация и устранение неполадок Active Directory, включая структуру домена, структуру *организационных подразделений* (ОП) и структуру узла. Определение эффективной топологии узла
Администрирование объектов пользователей и групп	Планирование, создание и поддержание учетных записей пользователей и групп для обеспечения входа пользователей в сеть и получения ими доступа к необходимым ресурсам
Зашита сетевых ресурсов	Администрирование, наблюдение, устранение неполадок в работе служб проверки подлинности. Планирование, внедрение и назначение политики безопасности для защиты данных и общих ресурсов, включая папки, файлы и принтеры
Администрирование Active Directory	Контроль расположения и управление объектами Active Directory. Планирование и реализация резервного копирования и восстановления Active Directory
Администрирование рабочих столов компьютеров	Распространение, установка и настройка рабочих столов компьютеров средствами групповой политики
Зашита Active Directory	Администрирование, наблюдение и устранение неполадок конфигурации безопасности. Планирование и реализация политики аудита сетевых событий для выявления брешей в защите
Управлениефункционированием Active Directory	Выявление и устранение неполадок контроллера домена и компонентов Active Directory средствами наблюдения за производительностью и диагностики
Удаленная установка Windows 2000	Использование службы Remote Installation Services (RIS) для удаленного развертывания Windows 2000

Заметим, что в настоящем учебном курсе, предназначенном для самостоятельной подготовки, описаны все эти категории — в соответствующих главах настоящей книги.

Резюме

Из материала этого занятия вы узнали о задачах администрирования Active Directory, которые включают конфигурирование Active Directory, администрирование объектов пользователей и групп, организацию зашиты сетевых ресурсов и Active Directory, администрирование Active Directory, администрирование рабочих столов компьютеров, управление производительностью Active Directory и удаленную установку Windows 2000.

Занятие 2, Средства администрирования Active Directory

Мощные и гибкие утилиты из состава Windows 2000 Server упрощают администрирование службы каталогов. Для администрирования Active Directory применяют стандартные консоли управления или создают пользовательские консоли, ориентированные на выполнение конкретных задач. На этом занятии вы познакомитесь со средствами администрирования Active Directory и консолью управления MMC.

Изучив материал этого **занятия,** вы сможете:

- ✓ описать функции оснасток Active Directory Users and Computers, Active Directory Sites and Services, Active Directory Domains and Trusts;
- ✓ описать функции и компоненты консоли управления MMC, включая дерево консоли, панели, оснастки, расширения и режимы консоли.

Продолжительность **занятия** - около 20 минут.

Средства администрирования Active Directory

Автоматически устанавливаются на компьютеры, сконфигурированные как контроллеры домена Windows 2000. Кроме того, они доступны из дополнительного пакета программ Administrative Tools. Этот пакет программ можно установить и на другие ОС семейства Windows 2000, чтобы администрировать Active Directory с компьютера, не являющегося контроллером домена. В меню Administrative Tools контроллера домена Windows 2000 доступны следующие стандартные консоли администрирования Active Directory:

- Active Directory Domains and Trusts (Active Directory — домены и доверие);
- Active Directory Sites and Services (Active Directory — сайты и службы);
- Active Directory Users and Computers (Active Directory — пользователи и компьютеры);

Консоль Active Directory Domains and Trusts

Предназначена для управления доверительными отношениями между доменами, принадлежащими к одному или разным лесам, к доменам Windows NT или даже сферам Kerberos V5. Консоль Active Directory Domains and Trusts позволяет:

- наладить взаимодействие с другими доменами (домены под управлением более старых версий, чем Windows 2000, или домены в других лесах Windows 2000) путем управления явными доверительными отношениями между доменами;
- менять режим работы домена Windows 2000 со смешанного на естественный;
- добавлять или удалять различные суффиксы *основного имени пользователя* (user principal name, UPN), применяемые для создания регистрационных имен пользователей;
- передавать от одного контроллера домена к другому роль хозяина именования домена;
- предоставлять информацию об управлении доменами.

Консоль Active Directory Sites and Services

Позволяет предоставлять информацию о физической структуре вашей сети путем публикации сайтов в Active Directory. Эти сведения используются Active Directory, чтобы определить, как реплицировать каталог и обрабатывать запросы к службам.

Консоль Active Directory Users and Computers

Позволяет добавлять, модифицировать, удалять и упорядочивать учетные записи пользователей Windows 2000, компьютеров, групп безопасности и распространения, организационные подразделения, а также ресурсы, опубликованные в каталоге вашей организации.

Прочие средства администрирования Active Directory

Помимо консолей Active Directory из меню Administrative Tools, для администрирования Active Directory предусмотрены дополнительные средства.

Оснастка Active Directory Schema

Предназначена для просмотра и модификации схемы Active Directory. По умолчанию эта оснастка не установлена в меню Administrative Tools. Ее необходимо установить вручную вместе с пакетом Administration Tools для Windows 2000, щелкнув кнопку Add/Remove Programs на панели управления. Для выполнения этих операций не используйте файл ADMINPAK.MSI с компакт-диска Windows 2000 Server.

▶ **Установка оснастки Active Directory Schema**

1. Зарегистрируйтесь как администратор.
2. Раскройте меню Start\Settings (Пуск\Настройка) и щелкните Control Panel (Панель управления).
3. Дважды щелкните Add/Remove Programs (Установка и удаление программ).
4. В диалоговом окне Add/Remove Programs щелкните кнопку Change Or Remove Programs (Замена или удаление программ), щелкните Windows 2000 Administration Tools и затем — Change (добавить).
5. В окне мастера установки средств администрирования щелкните Next.
6. В окне Setup Options (Параметры установки) щелкните переключатель Install All Of The Administrative Tools (Установка всех средств администрирования), а затем — Next.
7. Мастер установит средства администрирования Windows 2000. По завершении работы мастера щелкните кнопку Finish (Готово).
8. Закройте диалоговое окно Add/Remove Programs, а затем — и Control Panel.
9. В меню Start выберите команду Run (Выполнить).
10. В поле Open (Открыть) введите **mmc** и щелкните OK.
11. В меню Console (Консоль) щелкните Add/Remove Snap-In (Добавить/удалить оснастку).
12. В одноименном окне щелкните кнопку Add (Добавить).
13. В окне Add Standalone Snap-In (Добавить изолированную оснастку) в колонке Snap-In (Оснастка) дважды щелкните Active Directory Schema (Схема Active Directory), затем щелкните кнопки Close (Закрыть) и OK.
14. Для сохранения этой консоли в меню Console выберите команду Save (Сохранить).

Внимание! Модификация схемы Active Directory представляет собой сложную операцию, которую рекомендуется выполнять программными методами опытным программистам или операторам системы. Более подробно о модификации схемы Active Directory написано в руководстве для программистов *Microsoft Active Directory Programmer's Guide*.

Средства поддержки Active Directory

В составе Windows 2000 Support Tools предусмотрено несколько дополнительных средств, полезных для конфигурирования, управления и отладки Active Directory. Они находятся в

паке \Support\Tools на установочном компакт-диске Windows 2000. Эти средства предназначены для специалистов службы поддержки Microsoft, а также опытных пользователей.

Для использования средств поддержки Active Directory их надо установить на ваш компьютер.

▶ **Установка Windows 2000 Support Tools**

1. Запустите Windows 2000. Для установки средств поддержки нужны полномочия администратора.
2. Вставьте в привод CD-ROM установочный компакт-диск Windows 2000.
3. Из окна Microsoft Windows 2000 CD (Компакт-диск Microsoft Windows 2000) просмотрите содержимое компакт-диска.
4. Откройте каталог \SUPPORT\TOOLS.
5. Щелкните Setup.exe.
6. Выполняйте инструкции, которые будут появляться на экране.

Программа установки копирует файлы Windows 2000 Support Tools на жесткий диск, что потребует 18,2 Мб свободного места. Она также создаст папку Windows 2000 Support Tools в папке Programs меню Start.

Программа установки добавит также каталог \Program Files\Resource Kit (или папку с тем именем, которое вы выберете для установки средств поддержки) к переменной среды PATH вашего компьютера.

В табл. 3-2 описаны средства поддержки Active Directory.

Табл. 3-2. Средства поддержки Active Directory

Средство	Назначение
ACLDIAG.EXE: ACL Diagnostics [1]	Определяет, разрешен или запрещен доступ пользователю к данному объекту каталога. Может также использоваться для восстановления значений по умолчанию для таблиц управления доступом. Подробнее — в главе 14
ADSI Edit[3]	Оснастка консоли управления Microsoft, используемая для просмотра всех объектов в каталоге (включая схему и сведения о конфигурации), изменения объектов и установки таблиц управления доступом для объектов
DFSUTIL.EXE: Distributed File System Utility[1]	Управляет всеми возможностями распределенной файловой системы (DFS), проверяет совместимость конфигураций серверов DFS, отображает топологию DFS
DNSCMD.EXE: DNS Server Troubleshooting Tool[1]	Выполняет проверку динамической регистрации записей ресурсов DNS, включая безопасное обновление DNS, а также отмены регистрации записей ресурсов
DSACLS.EXE[1]	Отображает и модифицирует списки управления доступом для объектов в Active Directory. Подробнее — в главе 14
DSASTAT.EXE: Active Directory Diagnostic Tool[1]	Сравнивает контексты именования на контроллерах домена и выявляет различия. Подробнее — в главе 14
LDP.EXE: Active Directory Administration Tool[2]	Позволяет выполнять LDAP-операции в отношении Active Directory. Подробнее — в главе 14
MOVETREE.EXE: Active Directory Object Manager[1]	Перемещает объекты Active Directory, например объекты организационных подразделений (ОП) и пользователей, между доменами в одном лесу. Подробнее — в главе 11

Табл. 3-2. Средства поддержки Active Directory *(окончание)*

Средство	Назначение
NETDOM.EXE: Windows 2000 Domain Manager[1]	Управляет доменами Windows 2000 и доверительными отношениями между ними
NLTEST.EXE[1]	Предоставляет список главных контроллеров домена, сведения о доверительных отношениях и репликации, а также обеспечивает принудительное завершение работы системы. Подробнее — в главе 14
REPADMIN.EXE: Replication Diagnostics Tool[1]	Позволяет проверять согласованность репликации между партнерами репликации, наблюдать состояние репликации, показывать мета-данные репликации, принудительно вызывать события репликации и пересчет проверки согласованности знаний. Подробнее — в главе 14
REPLMON.EXE: Active Directory Replication Monitor[2]	Позволяет показывать топологию репликации, наблюдать за состоянием репликации (включая групповые политики), принудительно вызывать события репликации и пересчет проверки согласованности знаний. Программа имеет графический интерфейс пользователя. Подробнее — в главе 14
SDCHECK.EXE: Security Descriptor Check Utility[1]	Проверяет распространение и репликацию таблицы управления доступом для определенных объектов каталога. Эта служебная программа позволяет администратору определять правильность наследования таблиц управления доступом, а также проверять, была ли произведена репликация изменений таблицы управления доступом с одного контроллера домена на другой. Подробнее — в главе 14
SIDwalker:Security Administration Tools	Управляет политиками управления доступом в системах Windows 2000 и Windows NT. Состоит из трех отдельных программ: Showaccs.exe[1] и Sidwalk.exe[1] для изучения и изменения записей управления доступом, а также Security Migration Editor[3] — для редактирования соответствий между старыми и новыми идентификаторами безопасности (SID)

[1] Утилита командной строки.
[2] Утилита с графическим интерфейсом.
[3] Оснастка MMC (Microsoft Management Console).

Подробности о средствах поддержки Active Directory см. в комплекте «Microsoft Windows Server 2000 Resource Kit» (Microsoft Press, 2000)*.

Интерфейсы службы Active Directory

Набор интерфейсов службы Active Directory (Active Directory Service Interfaces, ADSI) предоставляет простой, мощный, объектно-ориентированный интерфейс для работы с Active Directory. ADSI облегчает программистам и администраторам создание программ, обращающихся к службам каталога при помощи высокоуровневых инструментальных средств, например Microsoft Visual Basic, Java, C, или Visual C++, а также таких языков сценариев, как VBScript, JScript, или PerlScript, независимо от базовых различий между разными про-

* Книги из комплекта «Ресурсы Windows 2000» переводятся издательством «Русская Редакция». Они появятся в продаже в середине 2001 года. — *Прим. ред.*

странствами имен. ADSI представляет собой полностью программируемый объект автоматизации, предназначенный для использования администраторами.

ADSI позволяет создавать или покупать программы, обеспечивающие единую точку доступа к многочисленным каталогам в вашей сетевой среде независимо от того, основаны ли те каталоги на LDAP или другом протоколе.

Консоль управления MMC

MMC (Microsoft Management Console) — средство создания, сохранения и работы с наборами административных инструментов, называемых *консолями* (console). Открывая средства администрирования Active Directory, вы на самом деле открываете соответствующую консоль. Такие средства, как Active Directory Domains and Trusts (Active Directory — домены и доверие), Active Directory Sites and Services (Active Directory — сайты и службы) и Active Directory Users and Computers (Active Directory — пользователи и компьютеры) являются консолями. Сама по себе консоль не предоставляет функций управления. Это программа, выполняющая роль несущего узла для управляющих приложений, называемых *оснастками* (snap-in), Оснастки служат для выполнения одной или более административных задач.

Существует два типа консолей: предварительно сконфигурированные (стандартные) и пользовательские. Первые содержат наиболее часто используемые оснастки и обычно располагаются в программной группе Administrative Toots (Администрирование). Пользовательские консоли создаются для выполнения уникального набора административных задач. Для удаленного администрирования годятся как предварительно сконфигурированные, так и пользовательские консоли MMC.

Стандартные консоли MMC

Содержат оснастки для выполнения типичных административных задач. Одновременно с Windows 2000 устанавливается ряд таких консолей, которые:

- содержат одну или более оснасток, обеспечивающих выполнение набора связанных административных задач;
- работают в пользовательском режиме, поэтому их невозможно модифицировать, сохранить или добавить в них дополнительные оснастки. Напротив, при создании пользовательских консолей, вы можете добавлять сколько угодно стандартных консолей в качестве оснасток в собственную консоль;
- отличаются друг от друга в зависимости от ОС компьютера и от установленных компонентов Windows 2000. Стандартные консоли для Windows 2000 Server и Windows 2000 Professional — различаются;
- могут быть добавлены при установке дополнительных компонентов Windows 2000. Необязательные для установки компоненты Windows 2000 могут включать дополнительные консоли, которые добавляются при установке какого-либо компонента. Например, вместе со службой DNS будет установлена консоль DNS.

В табл. 3-3 перечислены некоторые стандартные консоли MMC в Windows 2000 и их функции.

Табл. 3-3. Стандартные консоли MMC

Консоль	Функции
Active Directory Domains and Trusts	Управление доверительными отношениями между доменами

Табл. 3-3. Стандартные консоли MMC *(продолжение)*

Консоль	Функции
Active Directory Sites and Services [1, 2]	Создание сайтов для управления репликацией данных Active Directory
Active Directory Users and Computers [1, 2]	Управление пользователями, компьютерами, группами безопасности и другими объектами Active Directory
Component Services (Службы компонентов)	Конфигурирование и управление приложениями COM+
Computer Management (Управление компьютером)	Управление дисками и предоставление доступа к другим средствам администрирования локальных и удаленных компьютеров
Configure Your Server (Настройка сервера)[1]	Установка и настройка служб Windows для вашей сети
Data Sources (ODBC) [Источникиданных (ODBC)]	Добавление, удаление и конфигурирование драйверов и источников данных ODBC (Open Database Connectivity) — открытого интерфейса доступа к базам данных, встроенного в Windows
DHCP [1, 2]	Конфигурирование и управления службами DHCP (Dynamic Host Configuration Protocol)
Distributed File System (DFS) [Распределенная файловая система (DFS)][1]	Создание и управление распределенными файловыми системами, связывающими воедино сетевые папки разных компьютеров
DNS [1,2]	Управление службой DNS, преобразующей DNS-имена компьютеров в IP-адреса
Domain Controller Security Policy (Политика безопасности контроллера домена)[1, 2]	Просмотр и модификация политики безопасности контроллера домена подразделения
Domain Security Policy (Политика безопасности домена) [1, 2]	Просмотр и модификации политики безопасности домена, прав пользователей и политики аудита
Event Viewer (Просмотр событий)	Просмотр системных журналов Windows и других программ
Internet Services Manager (Диспетчер служб Интернета)[1]	Управление IIS (Internet Information Services) — информационными службами Интернета, Web-сервером для узлов Интернета и интрасетей
Licensing (Лицензирование)[1]	Управление клиентскими лицензиями для серверных продуктов
Local Security Policy (Локальная политика безопасности) [3]	Просмотр и модификация локальной политики безопасности, прав пользователей и политики аудита
Performance (Системный монитор)	Вывод графиков производительности системы и настройка системных журналов и оповещений
Routing and Remote Access (Маршрутизация и удаленный доступ)[1]	Настройка и администрирование служб маршрутизации и удаленного доступа

Табл. 3-3. Стандартные консоли MMC *(продолжение)*

Консоль	Функции
Server Extensions Administrator (Администратор серверных расширений)[1]	Администрирование Microsoft FrontPage Server Extensions и Web-серверов с расширениями FrontPage
Services (Службы)	Запуск и остановка служб
Telnet Server Administration (Управление сервером Telnet)[1]	Просмотр и модификация параметров и подключений сервера Telnet

[1] Не включена в состав Windows 2000 Professional.
[2] Не предусмотрена на изолированном сервере Windows 2000 Server.
[3] Не предусмотрена на контроллере домена Windows 2000 Server.

Пользовательские консоли MMC

Готовые консоли управления MMC помогут вам выполнять многие административные задачи. Однако вам в любом случае в какой-то момент понадобится создать собственную консоль управления. Хотя предварительно сконфигурированные консоли модифицировать нельзя, допустимо комбинировать стандартные оснастки с оснастками производства сторонних фирм, выполняющими сходные задачи, для создания пользовательских консолей MMC. Затем вы можете сделать следующее:

- сохранить пользовательскую консоль для дальнейшего использования;
- предоставить пользовательскую консоль для работы другим администраторам;
- запустить пользовательскую консоль MMC с любого компьютера для централизации и унификации выполнения административных задач.

Метод комбинирования оснасток позволит вам решить любые административные задачи. Создайте пользовательскую консоль управления — и вам больше не придется переключаться с одной программы на другую или же работать по очереди с разными стандартными консолями, так как все необходимые оснастки, будут у вас «под рукой».

Консоли сохраняются как файлы с расширением .msc. Все параметры оснасток, включенных в консоль, сохраняются и восстанавливаются при открытии файла, даже если файл консоли открывается на другом компьютере или в другой сети.

Дерево консоли и панель подробных сведений

В каждой MMC есть *дерево консоли* (console tree), где отражается иерархическая организация оснасток в составе консоли MMC. Как показано на рис. 3-1, данная консоль содержит оснастки Device Manager (Диспетчер устройств) для локального компьютера и Disk Defragmenter (Дефрагментация диска).

Дерево консоли организует оснастки из состава консоли, что позволяет быстро найти необходимую оснастку. Элементы, которые вы добавляете к дереву консоли, появляются под корнем консоли. *Панель подробных сведении* (details panel) отображает в виде списка содержимое активной оснастки.

Каждая консоль управления MMC содержит меню Action (Действие) и View (Вид). Состав команд этих зависит от текущего (выбранного) элемента в дереве консоли.

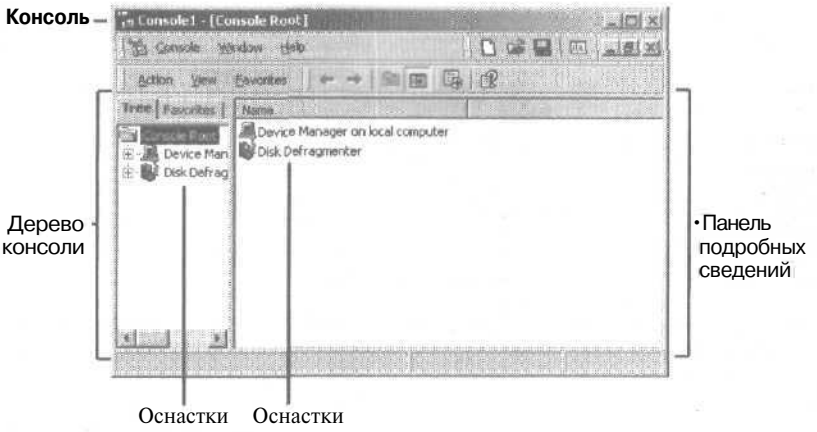


Рис. 3-1. Пример MMC

Оснастки

Оснастками называют приложения, созданные для работы в MMC. С их помощью выполняют административные задачи. Оснастки делятся на изолированные и расширения.

Изолированные оснастки

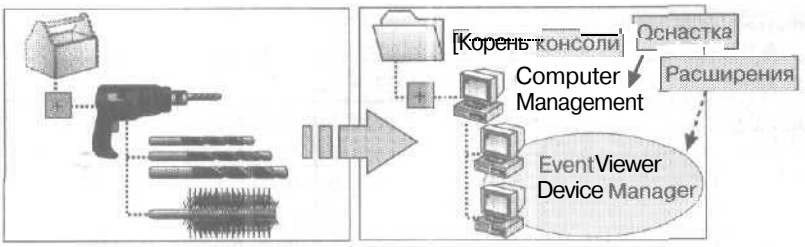
Обычно называют просто *оснастками* (snap-in). Каждая изолированная оснастка обеспечивает выполнение одной функции или нескольких связанных функций. Windows 2000 Server укомплектован стандартным набором оснасток. Windows 2000 Professional содержит сокращенный набор стандартных оснасток.

Расширения

Оснастки-расширения обычно называют просто *расширениями* (extension). Они обеспечивают дополнительную административную функциональность другим оснасткам.

- Расширения созданы для работы с одной или несколькими изолированными оснастками. Они подключаются к изолированным оснасткам. Например, расширение Software Installation (Установка программ) доступно в изолированной оснастке Group Policy, но не содержится в изолированной оснастке Disk Defragmenter, поскольку установка программ не имеет отношения к дефрагментации диска.
- При добавлении расширений Windows 2000 выводит на экран только расширения, совместимые с изолированной оснасткой. Windows 2000 помещает оснастки-расширения в соответствующее место в изолированной оснастке.
- При добавлении оснастки к консоли управления по умолчанию добавляются все предусмотренные для нее расширения. Вы можете также удалить любое расширение из оснастки.

На рис. 3-2 иллюстрируются понятия «оснастка» и «расширение». Ящик с инструментами (консоль управления MMC) содержит дрель (оснастку). Дрелью сверлят, используя стандартное сверло, а для выполнения дополнительных функций применяют насадки или другие сверла (аналогично расширениям).



- **Оснастки — средства администрирования.**
- **Расширения дополняют функциональность других оснасток.**
  - Расширения предварительно **назначаются оснасткам.**
  - Одни и те же расширения **можно** применять одновременно в **нескольких оснастках.**

Рис. 3-2. Оснастки и расширения

Настройка параметров консоли

Параметры консоли используются для настройки работы MMC. Для этого необходимо выбрать режим работы консоли, который определяет функциональность MMC для человека, работающего с сохраненной консолью. Консоль предусматривает два режима работы: режим Author (авторский) и режим User (пользовательский).

Примечание Дополнительные параметры консоли можно задать при помоши групповой политики. Подробнее об установке групповой политики — в главе 12.

Авторский режим

Сохранив консоль в авторском режиме, вы предоставляете полный доступ к ее функциям, включая модификацию консоли. Вы позволите пользователям выполнять следующие действия:

- добавлять или удалять оснастки;
- создавать новые окна;
- просматривать все части дерева консоли;
- сохранять консоль MMC.

Примечание По умолчанию все новые консоли MMC сохраняются в авторском режиме.

Пользовательский режим

Консоль MMC обычно рекомендуется сохранять в пользовательском режиме, если вы планируете предоставить ее другим администраторам. В таком режиме пользователи не смогут добавить или удалить из нее оснастки или сохранить консоль.

Предусмотрено три типа пользовательских режимов с различными уровнями доступа и функциональности (табл. 3-4).

Табл. 3-4. Пользовательские режимы консоли MMC

Пользовательский режим	Когда стоит использовать
Full Access (Полный доступ)	Предоставляется вся функциональность консоли MMC, включая возможность добавлять и удалять оснастки, создавать новые окна, а также доступ ко всем узлам дерева консоли
Limited Access, Multiple Windows (Ограниченный доступ с возможностью создавать новые окна)	Могут просматривать в консоли несколько окон, а также открывать новые окна и обращаться к дереву консоли
Limited Access, Single Window (Ограниченный доступ без возможности создавать новые окна)	Могут просматривать в консоли одно окно, но не вправе открывать новые окна и обращаться к дереву консоли

Резюме

На этом занятии вы познакомились со средствами администрирования Active Directory, Консоль Active Directory Domains and Trusts управляет доверительными отношениями между доменами. Консоль Active Directory Sites and Services создает сайты для управления репликацией данных Active Directory. Консоль Active Directory Users and Computers управляет пользователями, компьютерами, группами безопасности и другими объектами Active Directory.

MMC — инструмент для создания и сохранения средств администрирования, называемых консолями, а также работы с ними. Консоли MMC содержат одно или более управляющих приложений, называемых оснастками и позволяющих выполнять административные задачи. Предварительно сконфигурированные (стандартные) консоли MMC содержат заданный набор оснасток; ссылки на них содержатся в программной группе Administrative Tools. Пользовательские консоли MMC создаются для выполнения набора уникальных административных задач. Для удаленного администрирования годятся как стандартные, так и пользовательские консоли MMC.

Вы также узнали, что в каждой консоли MMC есть дерево консоли. Оно отражает иерархическую организацию оснасток консоли. Это позволяет быстро и легко находить нужную оснастку. Панель подробных сведений отображает в виде списка содержание активной оснастки. Оснастки делятся на изолированные и расширения.

Параметры консоли позволяют настраивать работу консоли MMC. Прежде всего необходимо выбрать один из двух режимов работы консоли: Author (авторский) и User (пользовательский). Сохраняя консоль MMC в авторском режиме, вы предоставляете полный доступ к ее функциям, включая модификацию консоли. Если же консоль сохранена в режиме User, пользователи не смогут добавить или удалить из нее оснастки или сохранить консоль.

Занятие 3, Консоли управления

На этом занятии вы научитесь применять стандартные консоли и создавать, использовать и модифицировать пользовательские.

Изучив материал этого занятия, вы сможете:

- ✓ применять стандартные консоли MMC;
- ✓ создавать пользовательские консоли MMC;
- ✓ создавать пользовательские консоли MMC для удаленного администрирования.

Продолжительность занятия — 30 минут.

Стандартные MMC

Для выбора стандартной консоли управления раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование). Открыть стандартную консоль Computer Management можно, щелкнув правой кнопкой мыши значок My Computer (Мой компьютер) на рабочем столе и выбрав в контекстном меню команду Manage (Управление).

Пользовательские консоли управления

Для создания пользовательской консоли необходимо открыть пустую консоль и затем добавить в нее оснастки для выполнения требуемых административных задач.

► **Запуск MMC и открытие пустой консоли**

1. В меню Start (Пуск) выберите команду Run (Выполнить).
2. В поле Open введите mmc и щелкните OK.

   Откроется окно консоли MMC, озаглавленное Console 1. Оно содержит окно Console Root. Это и есть пустая консоль MMC. Теперь вам необходимо решить, что делать дальше.

   В табл. 3-5 описаны варианты использования разных параметров в меню Console (Консоль).

Табл. 3-5. Использование параметров настройки в меню консоли Console

Параметр настройки	Когда следует использовать
New (Создать)	Когда вы хотите создать новую пользовательскую консоль MMC
Open (Открыть)	Когда вы собираетесь задействовать сохраненную консоль MMC
Save (Сохранить) или Save As (Сохранить как)	Когда вы хотите сохранить консоль MMC для дальнейшей работы
Add/Remove Snap-In (Добавить/удалить оснастку)	Когда вы хотите добавить (или удалить) одну или более оснасток и соответствующие им расширения в (из) консоль MMC
Options (Параметры)	Когда вы хотите настроить режим консоли и создать пользовательскую консоль MMC

3. Закройте консоль MMC.

Использование консоли управления для удаленного администрирования

При создании пользовательской консоли MMC можно настроить оснастку для удаленного администрирования. Это позволит вам выполнять административные задачи из любого места сети. Например, вы сможете использовать компьютер с Windows 2000 Professional для администрирования компьютера с Windows 2000 Server. Для удаленного администрирования годятся не все оснастки; это определяется ее конструктивными особенностями.

Для выполнения удаленного администрирования:

- разрешается использовать оснастки с других компьютеров, на которых установлены другие версии Windows 2000;
- необходимы специальные оснастки, разработанные для удаленного администрирования. Если оснастка обладает функциями удаленного управления, Windows 2000 предложит вам выбрать целевой компьютер для администрирования.

Предположим, что вам необходимо администрировать Windows 2000 Server на компьютере с Windows 2000 Professional. Поскольку Windows 2000 Professional не содержит всех средств администрирования, доступных в Windows 2000 Server, понадобится установить недостающие консоли на компьютер с Windows 2000 Professional. Получив доступ к серверу из окна My Network Places (Мое сетевое окружение) и запустив мастер установки средств администрирования Windows 2000 при помощи Add/Remove Programs на панели управления, вы сможете скопировать недостающие консоли на компьютер с Windows 2000 Professional- Затем сконфигурируйте каждую консоль для работы с севером. Имейте в виду, что некоторые из них могут и не запуститься на вашем компьютере, ведь мастер — лишь средство для их загрузки на удаленную машину.

Практикум: работа с консолью MMC

Выполнив это упражнение, вы научитесь:

- работать со стандартными консолями;
- настраивать консоль;
- упорядочивать и добавлять оснастки.

Упражнение 1: работа со стандартной консолью MMC

▶ **Задание: задействуйте стандартную консоль MMC**

1. Зарегистрируйтесь как Administrator (Администратор).
2. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Event Viewer (Просмотр событий).

   Откроется консоль управления Event Viewer, отображающая содержимое журналов событий. Event Viewer применяется для контроля работы различного программного обеспечения и аппаратных средств.

   Какие три журнала перечислены в дереве консоли?

   Можете ли вы добавить оснастки в консоль?
3. Закройте Event Viewer.

Упражнение 2: создание пользовательской консоли MMC

Вы научитесь создавать и настраивать консоль управления. Вы расположите консоль так, чтобы к ней было легко получить доступ. Вы научитесь средствами консоли выяснять, когда последний раз запускался компьютер. Вы также научитесь добавлять оснастку с расширениями.

► Задание 1: создайте пользовательскую консоль MMC

1. В меню Start (Пуск) выберите команду Run.
2. В поле Open введите mmc и щелкните OK.

   Откроется окно MMC, озаглавленное Console1 и содержащее окно Console Root (Корень консоли). Это — пустая консоль управления MMC. Для создания адаптированной пользовательской консоли определите, какая оснастка вам понадобится.
3. Разверните окно Console1.
4. Разверните окно Console Root.
5. Для просмотра текущей конфигурации консоли в меню Console (Консоль) выберите команду Options (Параметры).

   Откроется окно Options (Параметры) с вкладкой Console (Консоль), где можно задать режим консоли.

   Чем отличается консоль, сохраненная в пользовательском режиме, от консоли, сохраненной в авторском режиме?
6. Удостоверьтесь, что в списке Console Mode (Режим консоли) выбрано Author Mode (Авторский режим) и щелкните OK.
7. В меню Console выберите команду Save As (Сохранить как).

   Откроется одноименное окно.
8. В поле File Name (Имя файла) введите All Events и щелкните кнопку Save.

   Имя вашей консоли появится в заголовке окна MMC.
9. В меню Console выберите команду Exit (Выход).

   Создание и сохранение пользовательской консоли All Events завершено.

► Задание 2: откройте созданную вами консоль

1. Раскройте меню Start\Programs\Administrative Tools и щелкните All Events.

   Откроется консоль АЛ Events, которую вы только что сохранили.

► Задание 3: добавьте оснастку Event Viewer в консоль

1. В меню Console консоли управления All Events щелкните Add/Remove Snap-In (Добавить/удалить оснастку).

   Откроется одноименное окно с активной вкладкой Standalone (Изолированная оснастка). Заметьте, что в данный момент нет ни одной загруженной оснастки, Вы добавите оснастку в корень консоли.
2. Щелкните кнопку Add (Добавить).

   Откроется окно Add Standalone Snap-In (рис. 3-3).

   Обратите внимание на имеющиеся оснастки. MMC позволяет добавлять одну или более оснасток к консоли, а значит, — создавать собственные средства управления.
3. Выберите оснастку Event Viewer (Просмотр событий) и щелкните кнопку Add (Добавить).

   Откроется окно Select Computer (Выбор компьютера) с предложением указать, какой компьютер вы хотите администрировать.

   Имейте в виду, что вы можете добавить Event Viewer для компьютера, на котором вы работаете в данный момент; если же он входит в состав сети, вы можете добавить Event Viewer и для удаленного компьютера.

Примечание Чтобы добавить Event Viewer для удаленного компьютера, щелкните Another Computer (другим компьютером) и затем — кнопку Browse (Обзор). В диалоговом окне Select Computer (Выбор: Компьютер) щелкните удаленный компьютер, для которого вы бы хотели добавить Event Viewer, а затем — OK.

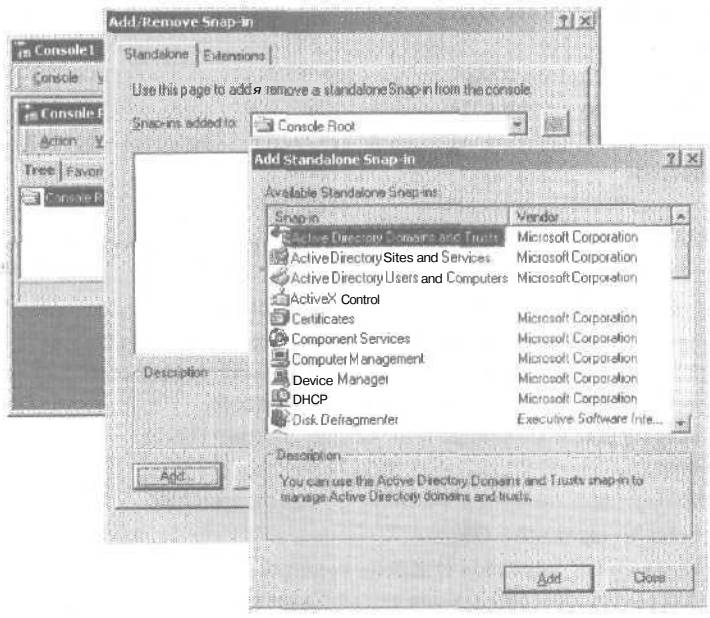


Рис. 3-3. **Диалоговое окно Add Standalone Snap-In (Добавить изолированную оснастку)**

4. Удостоверьтесь, что в диалоговом окне Select Computer выбран Local Computer (локальным компьютером) и щелкните кнопку Finish (Готово).
5. В окне Add Standalone Snap-In щелкните кнопку Close (Закрыть), а в окне Add/Remove Snap-In - OK.
   Оснастка Event Viewer (Local) появится в дереве консоли и в панели подробных сведений.

Совет Чтобы посмотреть полное имя папки, переместите границу между областями экрана консоли вправо.

► **Задание 4: выясните, когда последний раз запускался компьютер**

1. В дереве консоли All Events раскройте папку Event Viewer (Local) и щелкните System (Система).
   Справа будут перечислены последние события системы.
2. Дважды щелкните самое последнее информационное событие, для которого в колонке Source (Источник) значится eventlog.
   Откроется окно Event Properties (Свойства: событие). Служба журнала событий была запущена при запуске системы. Дата и время показывает приблизительное время запуска вашей системы.
3. Закройте диалоговое окно Event Properties, щелкнув OK.

4. В меню Console щелкните Exit, чтобы закрыть консоль All Events.

   Появится сообщение MMC с запросом, хотите ли вы сохранить параметры консоли All Events.

5. Щелкните кнопку No (Нет).

▶ **Задание 5: удалите расширения из оснастки**

1. В меню Start (Пуск) выберите команду Run.
2. В поле Open введите **mmc** и щелкните OK.

   Откроется пустая консоль.

3. Разверните окна Console1 и Console Root.
4. В меню Console выберите команду Add/Remove Snap-In.

   Откроется окно Add/Remove Snap-In с активной вкладкой Standalone. Вы добавите оснастку в корень консоли.

5. Щелкните Add.

   Откроется диалоговое окно Add Standalone Snap-In. Все перечисленные здесь оснастки — изолированные.

6. Выберите оснастку Computer Management и щелкните кнопку Add.

   Откроется окно Computer Management, предлагая вам указать, какой компьютер вы хотите администрировать. В данном упражнении вы добавите оснастку Computer Management (Управление компьютером) для своего компьютера.

7. Удостоверьтесь, что выбран Local Computer и щелкните кнопку Finish.
8. Щелкните кнопку Close.

   Оснастка Computer Management появится в списке оснасток консоли.

9. В окне Add/Remove Snap-In щелкните OK.

   Оснастка Computer Management появится в дереве консоли под корнем консоли. Корень консоли выполняет роль контейнера для нескольких категорий административных функций.

10. Раскройте узел Computer Management и изучите доступные функции, а затем раскройте узел System Tools (Служебные программы).

Примечание На данном этапе упражнения не используйте ни одну из этих программ.

   Заметьте, что предусмотрено несколько расширений, в том числе System Information (Сведения о системе) и Device Manager (Диспетчер устройств). Вы можете ограничить функциональность оснастки, удалив расширения.

11. В меню Console щелкните Add/Remove Snap-In.

    Откроется окно Add/Remove Snap-In с активной вкладкой Standalone.

12. Щелкните Computer Management (Local) и перейдите на вкладку Extensions (Расширения),

    Появится список расширений для оснастки Computer Management.

    Какой фактор определяет набор расширений, перечисленных в этом окне?

13. Сбросьте флажок Add All Extensions (Добавить все расширения), а затем в списке Available Extensions (Доступные расширения) сбросьте флажки напротив Device Manager Extension (Расширение диспетчера устройств) и System Information Extension (Расширение сведений о системе).
14. Щелкните OK.

    Снова откроется окно консоли.

15. Раскройте узлы Computer Management (Управление компьютером) и System Tools (Служебные программы), чтобы убедиться, что расширения System Information и Device Manager удалены.

Примечание На данном этапе упражнения не используйте ни одну из этих программ.

Когда нужно удалять расширения из консоли?

16. Закройте консоль.

Появится сообщение MMC с запросом, хотите ли вы сохранить параметры консоли.

17. Щелкните кнопку No.

Резюме

На этом занятии вы узнали, что стандартные консоли MMC содержат оснастки, которые используются чаще всего. Практическая часть занятия посвящена просмотру стандартных консолей MMC и запуску консоли Event Viewer.

Для выполнения набора уникальных административных задач можно создать пользовательскую консоль MMC. Ярлыки ваших консолей добавляются в меню Start. В практикуме вы создали две пользовательских консоли: первая содержала оснастку Event Viewer, с помощью которой вы узнали время последнего запуска компьютера, а вторая, созданная вами, — оснастку Computer Management. Мы рассказали, как ограничить функциональность консоли, удалив расширения из стандартного набора расширений оснастки. Наконец, вы узнали, как создаются пользовательские консоли для удаленного администрирования.

Занятие 4. Task Scheduler

Планировщик задач Task Scheduler (Планировщик задач) используется для планирования запуска программ и командных файлов единожды, по расписанию или при возникновении определенных событий в операционной системе. Task Scheduler применяется для выполнения многих административных задач.

Изучив материал этого занятия, вы сможете:

✓ использовать Task Scheduler для выполнения задач по расписанию.

Продолжительность занятия — 25 минут.

Знакомство с Task Scheduler

Windows 2000 сохраняет планируемые задачи в папке Scheduled Tasks (Назначенные задания), которая находится в папке Control Panel (Панель управления); ее также можно открыть из меню Start\Programs\Accessories\System Tools (Пуск\Программы\Стандартные\Служебные). Вы также можете получить доступ к папке Scheduled Tasks на другом компьютере, просматривая его ресурсы из окна My Network Places (Мое сетевое окружение). Допускается переносить задачи из папки Scheduled Tasks с одного компьютера на другой. Например, вы можете создать файлы задач обслуживания, а затем скопировать их на компьютер какого-то пользователя.

Task Scheduler (Планировщик задач) используется для:

- запуска обслуживающих утилит через определенные интервалы времени;
- запуска программ, когда снижается нагрузка на компьютер.

Параметры

Для планирования задач служит мастер Scheduled Task (Мастер планирования заданий). Для его запуска дважды щелкните значок Add Scheduled Task (Добавить задание) в папке Scheduled Tasks. В табл. 3-6 описаны параметры, которые вы можете настроить с помощью мастера.

Табл. 3-6. Параметры мастера Scheduled Task

Параметр	Описание
Frequency (Выполнять это задание)	Частота выполнения задания: ежедневно, еженедельно, ежемесячно, однократно, при запуске системы или при вашей регистрации в системе
Application (Приложение)	Приложения, расписание запуска которых требуется создать. Выберите приложения из списка зарегистрированных программ Windows 2000 или щелкните кнопку Browse (Обзор), чтобы указать любое другое приложение или командный файл
Task name (Имя задания)	Имя задания
Time and date (День и время запуска задания)	Время и дата начала выполнения задания. Вы можете указать дни, по которым следует выполнять задание
Name and password (Имя пользователя и пароль)	Имя пользователя и пароль. Вы можете указать свои имя пользователя и пароль или чужие имя и пароль, чтобы приложение выполнялось в соответствии с параметрами безопасности соответствующей учетной записи.

Табл. 3-6. Параметры мастера Scheduled Task *(окончание)*

Параметр	Описание
	Если учетная запись, использованная для регистрации в системе, не обладает разрешениями, необходимыми назначенному заданию, можно ввести другую — с требуемыми разрешениями. Например, запустить назначенное резервное копирование по учетной записи, которая обладает разрешением на архивирование данных и но имеет других административных прав
Advanced Properties (Установить дополнительные параметры)	Флажок, позволяющий по завершении работы с мастером вывести диалоговое окно с дополнительными параметрами задания

Дополнительные параметры заданий

Помимо параметров, доступных в Scheduled Task, можно настраивать и другие параметры заданий. В табл. 3-7 описаны вкладки диалогового окна дополнительных свойств задания.

Табл. 3-7. Вкладки диалогового окна Advanced Properties мастера Scheduled Task Wizard

Вкладка	Описание
Task (Задание)	Позволяет изменить назначенное задание или учетную запись, используемую для его выполнения, а также включить и выключить назначенное задание
Schedule **(Настройка)**	**Определяет расписания выполнения** текущего задания. **Вы** можете задать **дату, время и число запусков** задания (например, запускать задание в 22.00 по пятницам)
Settings (Параметры)	Задает условия запуска и удаления задания, например здесь можно указать, чтобы задание выполнялось, когда компьютер не используется, или работает от сети, а не от батарей. Также можно настроить включение компьютера для выполнения задания в определенное время
Security (Безопасность)	Определяет список пользователей и групп, обладающих разрешением на выполнение задания. Здесь же можно изменить разрешения на выполнение задания для пользователя или группы

Практикум: использование Task Scheduler

Выполнив практические задания, вы научитесь:

- планировать задачи для автоматического запуска;
- конфигурировать параметры Task Scheduler.

Сейчас вы попробуете спланировать запуск Disk Defragmenter (Дефрагментация диска) в заданное время. Вы также научитесь конфигурировать параметры планировщика задач Task Scheduler.

► **Задание 1: спланируйте автоматический запуск задания**

1. Дважды щелкните значок My Computer (Мой компьютер), откройте окно Control Panel и дважды щелкните значок Scheduled Tasks (Назначенные задания).

   Откроется окно Scheduled Tasks. Поскольку на данный момент назначенных заданий нет, отображается лишь значок Add Scheduled Task (Добавить задание).

2. Дважды щелкните значок Add Scheduled Task.

   Откроется окно мастера Scheduled Task.

3. Щелкните Next.

   Появится список установленных в системе приложений. Чтобы создать расписание запуска программы, не зарегистрированной в Windows 2000, щелкните кнопку Browse (Обзор) и укажите требуемое приложение.

4. Щелкните кнопку Browse (Обзор).

   Откроется диалоговое окно Select Program To Schedule (Выберите приложение, для которого следует составить расписание).

5. Дважды щелкните папку Program Files, а затем — папку WINNT.
6. Щелкните папку Accessories, а затем дважды — значок DFRG.MSC.
7. В качестве имени задания введите Launch Disk **Defragmenter** (рис. 3-4).

   Здесь можно ввести описание, которое будет более понятным, чем имя программы. По завершении работы мастера в папке Scheduled Tasks (Назначенные задания) появится задание с указанным именем.

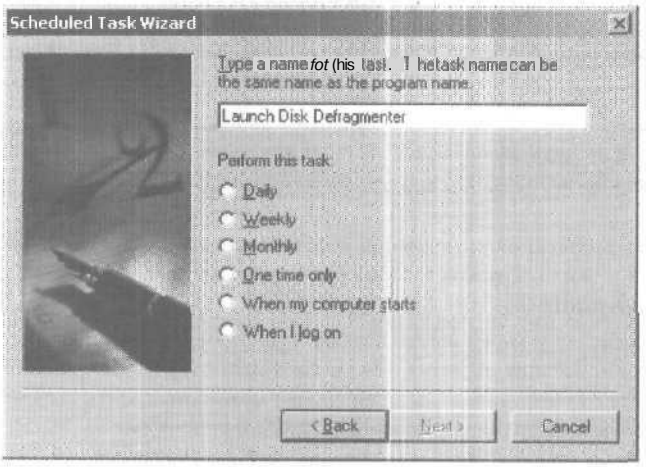


Рис. 3-4. Окно мастера Scheduled Task (Мастер планирования заданий)

8. Щелкните переключатель One Time Only (однократно), а затем — Next.
9. В поле Start Time (Время начала) укажите время на 4 минуты позднее текущего системного времени. Запомните указанное время.

   Чтобы узнать системное время, взгляните на панель задач. Не меняйте значение поля Start Date (Дата начала).

10. Щелкните Next.

    Мастер предложит ввести имя и пароль учетной записи пользователя. После запуска задание получает все права и разрешения, которыми обладает указанная в этом окне учетная запись. Кроме того, на программу накладываются все ограничения учетной записи пользователя. Заметьте, что ваше имя пользователя, SERVER1\Administrator, уже указано по умолчанию (если имя вашего компьютера отличается от SERVER1, будет указано соответствующее имя).

    Прежде чем продолжить, укажите в обоих полях ввода пароля правильный пароль данной учетной записи.

    Теперь настройте консоль для работы с использованием ваших административных разрешений.

11. В полях Enter The Password (Введите пароль) и Confirm Password (Подтверждение) введите **password**.
12. Щелкните Next.

    Не помечайте флажок Advanced Properties (Установить дополнительные параметры) — с этими параметрами вам предстоит работать на следующем этапе упражнения.
13. Щелкните кнопку Finish (Готово).

    Заметьте, что мастер добавил задание в список назначенных заданий.
14. Чтобы убедиться, что вы корректно настроили расписание запуска задания, дождитесь времени, указанного при выполнении пункта 9. Будет запущен Disk Defragmenter.
15. Закройте **Disk** Defragmenter.

► **Задание 2: настройте дополнительные параметры Task Scheduler**

1. В окне Scheduled Tasks (Назначенные задания) дважды щелкните значок Launch WordPad.

   Откроется диалоговое окно Launch WordPad. Просмотрите вкладки и изучите доступные параметры. Это те же параметры, которые можно настраивать после включения флажка Advanced Properties (Установить дополнительные параметры) в последнем окне мастера Scheduled Task. Не изменяйте каких-либо значений параметров.
2. Перейдите на вкладку Settings (Настройка).

   Просмотрите доступные параметры.
3. Включите флажок Delete The Task If It Is Not Scheduled To Run Again (Удалить задание, если нет его повторения по расписанию).
4. Перейдите на вкладку Schedule (Расписание) и укажите время на 2 минуты опережающие текущее.

   Запомните указанное время.
5. Щелкните OK.

   Чтобы убедиться, что вы корректно настроили расписание запуска задания, дождитесь времени, указанного при выполнении пункта 4. Будет запущен WordPad.
6. Закройте WordPad.

   Заметьте, что в папке Scheduled Tasks больше нет назначенного задания. Возможность удалять задания после завершения его выполнения позволяет автоматически удалять одноразовые задания.
7. Закройте окно Scheduled Tasks (Назначенные задания).
8. Завершите сеанс работы с Windows 2000.

Резюме

Планировщик задач Task Scheduler можно использовать для составления расписания запуска программ и командных файлов один раз, в равные промежутки времени, в указанное время или при определенных событиях в операционной системе. Windows 2000 сохраняет спланированные задачи в папке Scheduled Tasks (Назначенные задания), которая находится в папке Control Panel в My Computer. Спланировав запуск задачи, вы можете модифицировать любой из ее параметров или дополнительных функций, включая сам запуск программы.

Доступ к папке Scheduled Tasks на другом компьютере можно получить, просмотрев ресурсы компьютера из окна My Network Places (Мое сетевое окружение). Например, вы можете создать файлы задач обслуживания, а затем скопировать их на компьютер какого-то пользователя. Вы научились использовать мастер Scheduled Task для составления рас писания запуска Disk Defragmenter в указанное время.

Закрепление материала

? 1 Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении А «Вопросы и ответы» в конце книги.

1. Какие функции выполняют консоли управления Active Directory Domains and Trusts, Active Directory Sites and Services и Active Directory Users and Computers?

2. Для чего создаются пользовательские консоли управления MMC?

3. Когда и почему целесообразно использовать расширение?

4. Вам необходимо создать пользовательскую консоль для администратора, которому требуются лишь консоли Computer Management и Active Directory Users and Computers. Причем, администратор:
   - не должен иметь возможность добавлять какие-либо дополнительные консоли или оснастки;
   - должен иметь полный доступ к обеим консолям;
   - должен иметь возможность управлять обеими консолями.

   Какой режим консоли следует использовать для конфигурирования данной пользовательской консоли?

5. Что необходимо сделать для удаленного администрирования компьютера с Windows 2000 Server с компьютера, на котором установлена Windows 2000 Professional?

6. Вам необходимо автоматически запускать служебную программу на компьютере с Windows 2000 Server один раз в неделю. Как это сделать?

ГЛАВА 4

Внедрение Active Directory

В этой главе

Успех внедрения Windows 2000 зависит от планирования Active Directory. В этой главе рассказывается о планировании внедрения службы Active Directory и об этапах ее установки с использованием мастера, а также о внедрении структуры организационного подразделения (ОП) и настройке его параметров.

Прежде всего

Для изучения материалов этой главы необходимо:

- выполнить процедуры установки, описанные во вводной главе;
- уяснить различия между рабочей группой и доменом;
- знать различия между контроллером домена и рядовым сервером;
- уметь использовать консоль управления Microsoft (Microsoft Management Console, MMC).

Занятие 1. Планирование внедрения Active Directory

Active Directory позволяет проектировать структуру каталогов, отвечающую потребностям вашей организации. Прежде чем внедрять Active Directory, необходимо изучить структуру бизнеса вашей организации и спланировать структуру домена, пространства имен домена, ОП и сайта. Гибкость Active Directory позволяет создать структуру сети, оптимизированную для вашей организации. Здесь рассказывается о планировании внедрения Active Directory.

Изучив материал этого занятия, вы сможете:

- ✓ спланировать структуру домена;
- ✓ спланировать пространство имен домена;
- ✓ спланировать структуру ОП;
- ✓ спланировать структуру сайта.

Продолжительность **занятия** — около 35 минут.

Планирование структуры домена

Поскольку основным звеном логической структуры в Active Directory является домен, который может хранить миллионы объектов, важной задачей является тщательное планирование его структуры. При этом вы должны принять во внимание:

- структуру логической и физической среды вашей организации;
- требования администрирования;
- требования к структуре домена.

Оценка логической среды

Для определения логической структуры организации необходимо понимать, как организация работает. Например, на рис. 4-1 показано воображаемое деление фирмы Microsoft по функциональному и географическому признакам. Фирма состоит из функциональных подразделений Administration (Управление), Purchasing (Закупка), Sales (Продажа) и Distribution (Распространение). Фирма имеет офисы в городах Канзас-Сити, Сент-Паул, Чикаго и Коламбус.

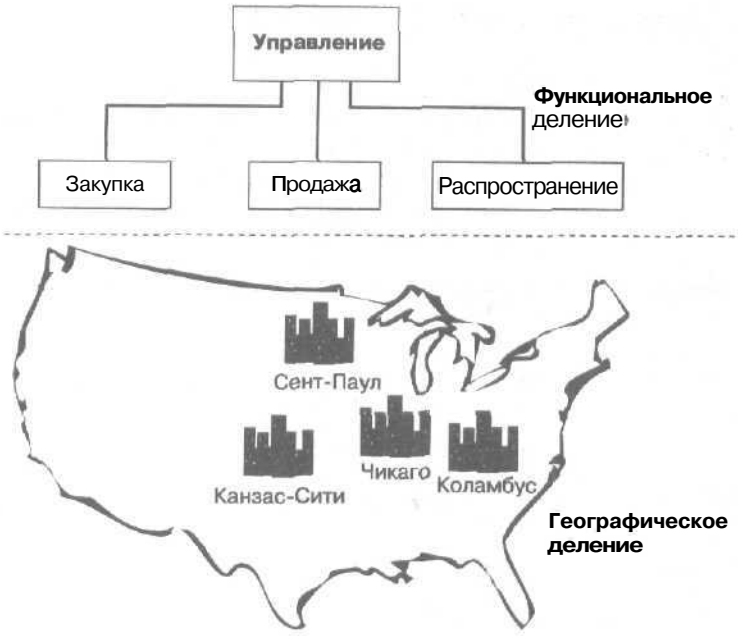


Рис. 4-1. Деление фирмы Microsoft по функциональному и географическому признакам

Требования пользователей и сети

Этот параметр позволит вам определить технические требования для внедрения Active Directory. Вы уже изучили географическое местоположение организации, а теперь вам надо выяснить требования пользователей и сети, чтобы определить логические требования для внедрения Active Directory. Для каждого функционального и географического подразделения выясните:

- количество сотрудников;
- темпы роста;
- планы расширения.

Для оценки сетевых требований для каждого географически изолированного подразделения определите:

- организацию сетевых соединений;
- скорость каждого сетевого соединения;
- использование сетевых соединений;
- подсети TCP/IP.

Например, на рис. 4-2 показаны требования для Microsoft. В четырех географически изолированных подразделениях организации работает примерно одинаковое количество служащих. Однако, если рассматривать функциональные подразделения, то больше сотрудников занято в группе Administrators. В ближайшие 5 лет планируется 3-процентный рост всех подразделений. Офис в Чикаго является концентратором ГВС. Сетевые соединения используются умеренно, но большая нагрузка приходится на соединение Канзас-Сити — Чикаго.

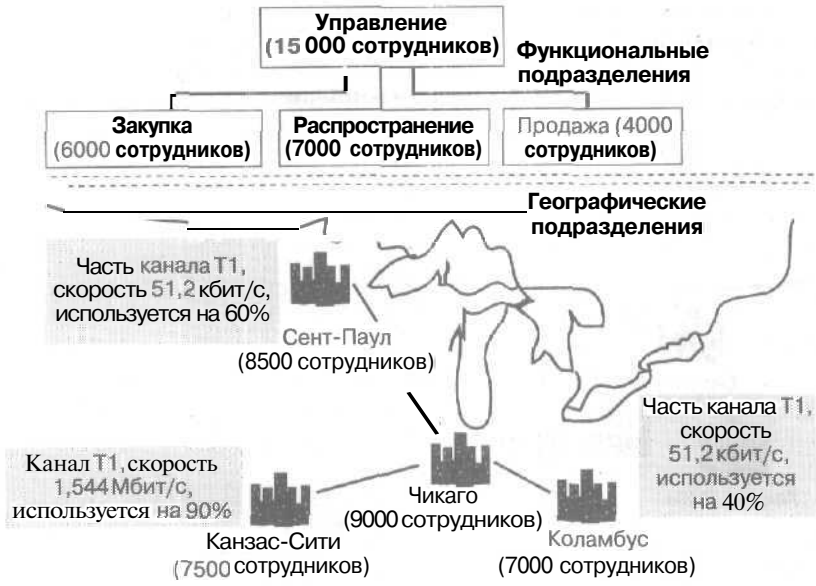


Рис. 4-2. Требования пользователей и сети для подразделений

Оценка требований управления

Оценка управления сетевыми ресурсами помогает планировать структуру домена. Определите способ сетевого администрирования вашей организации.

- **Централизованное администрирование.** Функционирование сети поддерживается одной группой администраторов. Этот метод часто используется в небольших компаниях с ограниченным количеством подразделений и функций.
- **Децентрализованное администрирование.** Сеть обслуживают несколько администраторов или групп администраторов. Группы могут делиться в зависимости от местоположения или функций, выполняемых подразделениями.
- **Выборочное администрирование.** Администрирование части ресурсов осуществляется централизованно, а части — децентрализовано.

В приведенном примере требуется децентрализованное администрирование. Каждому физическому подразделению нужна своя группа администраторов для обеспечения сетевых служб для всех четырех функциональных подразделений.

После определения логической и физической структуры и требований администрирования для вашей организации можно выяснить требования, предъявляемые домену.

Необходимость создания нескольких доменов

Простейшей доменной структурой считается отдельный домен. При планировании стоит начинать с одного домена и затем добавлять их по мере необходимости.

Один домен охватывает несколько сайтов и содержит миллионы объектов. Помните: структуры домена и сайта разделены и отличаются гибкостью. Отдельный домен может охватывать несколько физических сайтов, а отдельный сайт может включать пользователей и компьютеры из разных доменов. Планирование структуры сайта рассматривается далее на этом занятии.

Нет необходимости создавать отдельные домены специально для каждого имеющегося в организации подразделения. Внутри каждого домена можно моделировать иерархию

управления организацией для делегирования или администрирования с использованием ОП, которые будут выступать в роли логических контейнеров для других объектов. Затем можно назначать политику групп и помещать в ОП пользователей, группы и компьютеры. Планирование структуры ОП рассматривается далее на этом занятии.

Имеет смысл создавать более одного домена, если:

- сетевое администрирование — децентрализованное;
- выполняется контроль репликации;
- организации предъявляют различные требования к паролям;
- имеется множество объектов;
- в сети используются различные доменные имена Интернета;
- необходимо выполнять некие международные требования;
- внутренние требования политик различаются.

В приведенном примере фирме Microsoft требуются несколько доменов, так как:

- в чикагском офисе требования к паролям — более жесткие;
- необходимо контролировать репликацию активно используемого соединения Чикаго — Канзас-Сити;
- в течение ближайших двух лет планируется создание нового подразделения в Фарго (Северная Дакота).

Способы организации домена

Если вы решили, что вашей организации нужно несколько доменов, организуйте домены в иерархию в соответствии с потребностями организации. Можно организовать домены и виде дерева или леса. Помните: домены в деревьях и лесах имеют одну и ту же конфигурацию, схему и глобальный каталог. Совместно использовать ресурсы в таком случае позволяют двусторонние доверительные отношения.

Основное различие между деревьями и лесами доменов отражено в *структуре их доменных имен* (Domain Name Service, DNS). Все домены в дереве имеют связанное пространство имен DNS. Если вашу организацию можно представить как группу подразделений, в сети, вероятно, применяется непрерывное пространство имен DNS, и вам следует создавать несколько доменов в одном дереве доменов. Если вы собираетесь объединить организации с уникальными доменными именами, создавайте лес. Его можно также использовать для разделения зон DNS. Каждое дерево в лесе имеет свое уникальное пространство имен.

В нашем примере организационная структура фирмы Microsoft привязана к группе доменов в дереве домена. Microsoft не является подразделением другой организации, и в будущем не планируется создание подразделений.

Планирование доменного пространства имен

В Active Directory домены имеют DNS-имена. Прежде чем использовать DNS в сети, необходимо спланировать пространство имен DNS. Вы должны продумать, как будете применять именование DNS и чего хотите добиться с его помощью. Вот на какие вопросы вам надо предварительно ответить.

- Имеете ли вы опыт выбора и регистрации доменных имен DNS для использования в Интернете?
- Будет ли внутреннее пространство имен Active Directory совпадать с внешним пространством имен Интернета?
- Какие требования и концепции именования следует применить при выборе доменных имен DNS?

Выбор доменного имени DNS

При настройке DNS-серверов рекомендуется сначала выбрать и зарегистрировать уникальное родительское имя DNS, оно будет представлять вашу организацию в Интернете. Например, Microsoft использует имя microsoft.com. Это имя является доменом второго уровня внутри одного из доменов верхнего уровня, используемых в Интернете.

Прежде чем задавать родительское имя DNS для вашей организации, убедитесь, что это имя не присвоено другой организации. В настоящее время большей частью пространства имен DNS Интернета управляет фирма Network Solutions, Inc., хотя есть и другие фирмы.

Родительское имя DNS можно соединить с именем местоположения или подразделения внутри вашей организации для формирования других имен поддоменов. Например, добавим к домену второго уровня Microsoft поддомен Chicago, создав пространство имен chicago.microsoft.com.

Внутреннее и внешнее пространства имен

Для внедрения Active Directory существуют два вида пространств имен. Пространство имен Active Directory совпадает с заданным зарегистрированным пространством имен DNS или отличается от него.

Совпадающие внутреннее и внешнее пространства имен

Согласно этому сценарию, организация использует одно и то же имя для внутреннего и внешнего пространств имен (рис. 4-3). Имя mcrosoft.com применяется как внутри, так и вне организации. Для реализации этого сценария надо соблюдать следующие условия:

- пользователи внутренней частной сети компании должны иметь доступ как к внутренним, так и к внешним серверам (по обе стороны брандмауэра);
- для защиты конфиденциальной информации клиенты, осуществляющие доступ извне, не должны иметь доступ к внутренним ресурсам компании или иметь возможность разрешать их имена.

Кроме того, необходимы две раздельные зоны DNS, одна из которых, за пределами брандмауэра, обеспечивает разрешение имен для общедоступных ресурсов. Она не сконфигурирована для разрешения имен внутренних ресурсов, поэтому доступ к ним извне получить нельзя.

Недостаток этой конфигурации — предоставление доступа к внешним ресурсам внутренним клиентам, так как внешняя зона DNS не сконфигурирована для разрешения имен внутренних ресурсов. Один из способов преодоления этого недостатка — создать дубликат внешней зоны во внутренней зоне DNS для разрешения имен ресурсов внутренними клиентами. Если используется прокси-сервер, прокси-клиент надо настроить так, чтобы он обращался к microsoft.com как к внутреннему ресурсу.

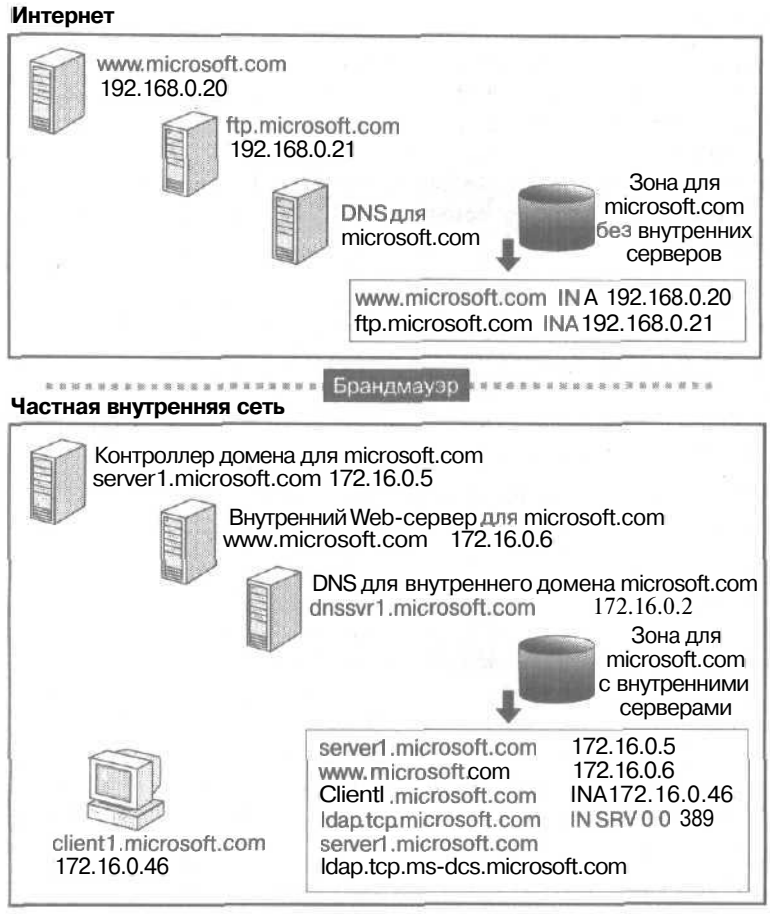


Рис. 4-3. Совпадающие внутреннее и внешнее пространства имен

Преимущества:

- имя дерева, microsoft.com, согласовано в частной сети и Интернете;
- появляется возможность унифицировать вход в систему — для этого пользователи локальной сети и Интернета смогут применять одно и то же имя; например, jsmith@microsoft.com будет служить и регистрационным именем и идентификатором электронной почты.

Недостатки:

- усложняется конфигурация — при настройке прокси-клиентов надо учесть, что внутренние и внешние ресурсы отличаются;
- придется следить, чтобы внутренние ресурсы случайно не стали общедоступными;
- вдвое усложняется управление ресурсами, потому что, например, придется дублировать записи зоны для внутреннего и внешнего разрешения имен;
- даже если пространство имен одно и то же, внутренние и внешние ресурсы будут представляться пользователям по-разному.

Отличающиеся внутреннее и внешнее пространства имен

В этом случае компания использует различные внутреннее и внешнее пространства имен (рис. 4-4). Изначально в зонах по разные стороны брандмауэра имена различаются. Имя microsoft.com используется вне брандмауэра, а msn.com — внутри.

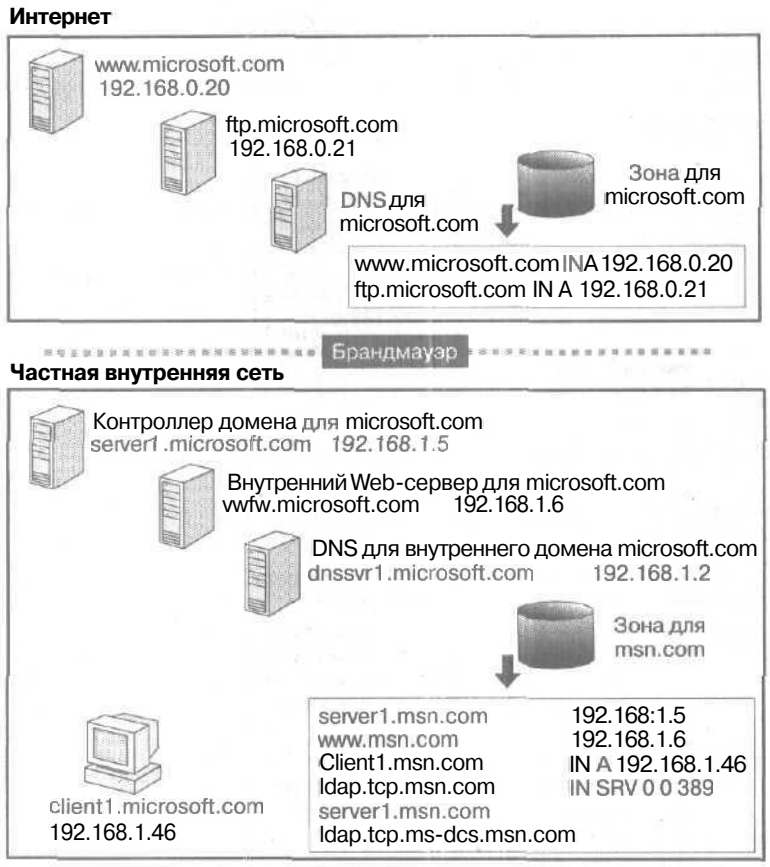


Рис. 4-4. Отличающиеся внутреннее и внешнее пространства имен

Для этого необходимо зарегистрировать два пространства имен в DNS Интернета. Цель регистрации — предотвратить дублирование внутреннего имени другой общедоступной сетью. Если имя не зарезервировано, внутренние клиенты не смогут отличить внутреннее имя от имени, зарегистрированного в общедоступной сети пространства имен DNS.

Таким образом, устанавливаются две зоны. Одна отвечает за разрешение имен в пространстве microsoft.corn, другая — в msn.com внутри брандмауэра. Пользователям не составит труда различать внутренние и внешние ресурсы.

Преимущества:

- очевидно различие между внутренними и внешними ресурсами;
- среда проще в управлении;
- упрощается настройка прокси-клиентов, так как при опознавании внешних ресурсов списки исключений содержат только microsoft.com.

Недостатки:

- регистрационные имена отличаются от имен электронной почты. Например, John Smith входит в систему с именем jsmith@msn.com, а адрес его электронной почты — jsmith@microsoft.com;
- в DNS Интернета придется зарегистрировать несколько имен.

Примечание В этом сценарии имена входа в систему различаются по умолчанию. Администратор может воспользоваться консолью управления для изменения суффикса *основного имени пользователя* (user principal name, UPN), в результате чего имя входа пользователя будет совпадать с его электронным адресом.

Требования и концепции доменного именования

При планировании пространства имен для корневых доменов и поддоменов необходимо учитывать следующие рекомендации:

- выбирайте имя корневого домена, которое не будет меняться. Его корректировка впоследствии может обойтись вам весьма дорого или вообще окажется невозможной;
- используйте простые имена: их легче запоминать и применять для поиска ресурсов;
- используйте стандартные символы DNS и Unicode. Windows 2000 поддерживает следующие стандартные символы DNS: A—Z, a—z, 0—9 и символ дефиса (-), как определено в документе **RFC** 1035. Набор символов Unicode включает дополнительные символы, отсутствующие в ASCII, которые требуются для других иностранных языков;

Примечание Используйте набор символов Unicode, только если его поддерживают все DNS-серверы. О наборе символов Unicode см. также в документе RFC 2044, для этого в поисковой машине Интернета введите ключевое слово «RFC 2044».

- ограничьте количество уровней доменов. Обычно количество уровней в имени, согласно иерархии **DNS,** не должно превышать трех-четырех. Большое число уровней усложняет администрирование;
- применяйте уникальные имена. Каждый поддомен должен иметь уникальное имя внутри родительского домена, чтобы имя не повторялось во всем пространстве имен **DNS;**
- избегайте длинных имен — не более 63 символов, включая разделители. Общая длина не должна превышать 255 символов. Строчные и заглавные буквы не различаются.

На рис. 4-5 изображена структура домена для Microsoft. Корневой домен компании, microsoft.com, содержит поддомены для ее четырех подразделений.

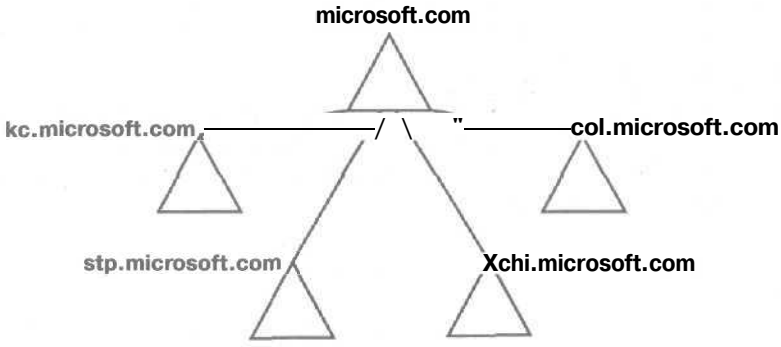


Рис. 4-5. Структура домена Microsoft

Планирование структуры ОП

После определения структуры домена организации и планировании доменного пространства имен необходимо разработать структуру организационных подразделений (ОП). Можно создать иерархию ОП в домене. В отдельном домене разместите пользователей и ресур-

сы, повторив структуру компании в конкретном ОП. Таким образом, вы сможете создать логичную и осмысленную модель организации и делегировать административные полномочия на любой уровень иерархии.

В каждом домене разрешается внедрять собственную иерархию ОП. Если ваша организация имеет несколько доменов, вы можете создать структуры ОП внутри каждого домена независимо от структуры в других доменах.

ОП позволяет:

- отразить структуру компании и организации внутри домена. Без ОП все пользователи поддерживаются и отображаются в одном списке независимо от подразделения, местоположения и роли пользователя;
- делегировать управление сетевыми ресурсами, но сохранить способность управлять ими. Вы можете присваивать административные полномочия пользователям или группам на уровне ОП;
- изменять организационную структуру компании;
- группировать объекты так, чтобы администраторы легко отыскивали сетевые ресурсы. Это облегчит обеспечение безопасности и выполнение любых административных задач. Например, вы можете сгруппировать все учетные записи пользователей для временных сотрудников в ОП, названном TempEmployees;
- ограничить видимость сетевых ресурсов в Active Directory. Например, разрешить пользователями просматривать только объекты, к которым они имеют доступ.

Планирование иерархии ОП

При планировании иерархии ОП важно соблюсти ряд правил.

1. Хотя глубина иерархии ОП не ограничена, производительность мелкой иерархии выше, чем глубокой.
2. ОП должны отражать неизменные структурные единицы организации.

Существует много способов структурирования ОП в организации. Важно определить, какая модель ляжет в основу иерархии ОП. Примите во внимание следующие модели классификации ОП в иерархии ОП: модель деления на ОП согласно выполняемым задачам; географическая модель деления на ОП; модель деления на ОП согласно выполняемым задачам и географическому местоположению.

Модель деления на ОП согласно выполняемым задачам

ОП можно создавать, учитывая функции, которые необходимо выполнять внутри организации (рис. 4-6.). Верхний уровень ОП - ADMIN, DEVELOPMENT fDEVEL) и SALES - соответствует бизнес-подразделениям компании. Второй уровень ОП — функциональные подразделения внутри бизнес-подразделений.

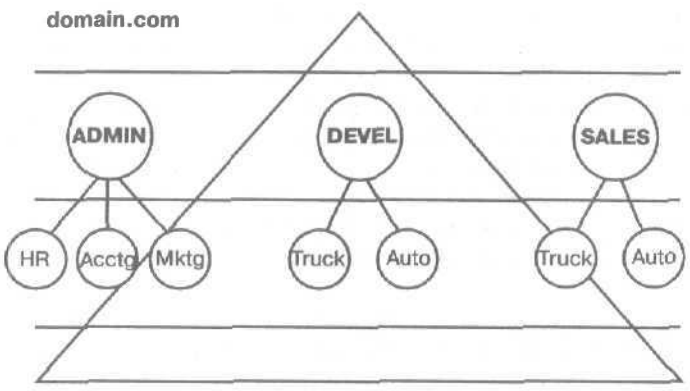


Рис. 4-6. Модель деления на ОП согласно выполняемым задачам

Географическая модель деления на ОП

Иногда при создании ОП учитывается местоположение филиалов компании (рис. 4-7). Верхний уровень ОП — WEST, CENTRAL и EAST — соответствует региональным подразделениям организации, а второй представляет физическое местоположение восьми офисов компании.

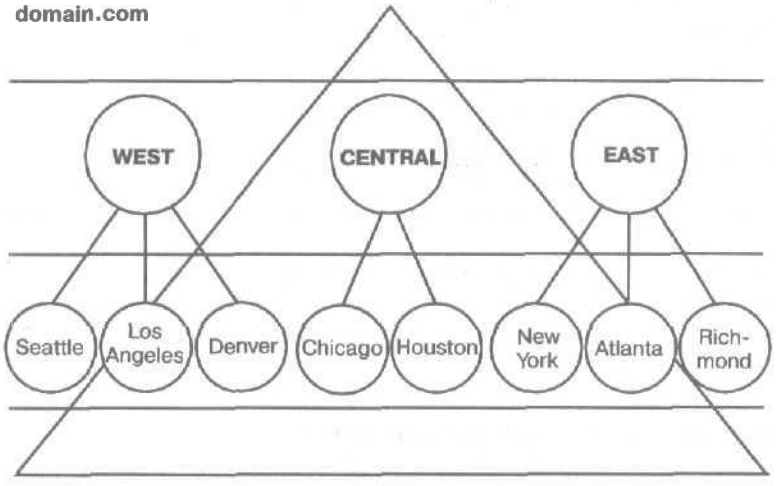


Рис. 4-7. Географическая модель деления на ОП

Модель деления на ОП согласно выполняемым задачам и географическому местоположению

В некоторых случаях две описанные выше модели создания ОП совмещают (рис. 4-8). Верхний уровень ОП — NORTH AMERICA и EUROPE — учитывает, на каких континентах расположены офисы компании. Второй уровень ОП построен на основе функциональных особенностей каждого подразделения внутри организации.

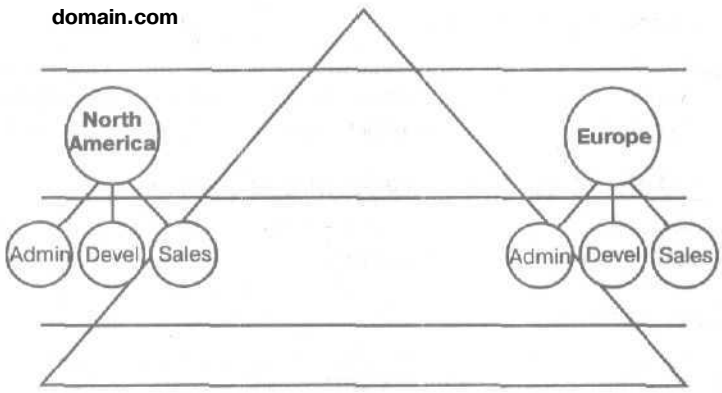


Рис. 4-8. Модель деления на ОП по выполняемым задачам и географическому местоположению

Планирование структуры сайта

Сайт — это часть физической структуры Active Directory, совокупность одной или нескольких IP-подсетей, соединенных высокоскоростными каналами связи. В Active Directory структура сайта связана с физической средой и поддерживается отдельно от логической среды и структуры домена. Отдельный домен может включать несколько сайтов, а отдельный сайт — несколько доменов или частей нескольких доменов. Основная задача сайта — обеспечивать хорошее сетевое соединение.

Настройка сайтов влияет на работу Windows 2000 следующим образом.

- **Регистрация рабочей станции и проверка подлинности.** При входе пользователя в систему Windows 2000 попытается найти контроллер домена на сайте компьютера пользователя, чтобы обслужить запрос регистрации в системе и последующие запросы сетевой информации.
- **Репликация каталога.** Расписание и маршрут репликации каталога домена могут быть сконфигурированы для внутри- и межсайтовой репликации по отдельности. Обычно система настраивается так, чтобы межсайтовая репликация осуществлялась реже, чем внутрисайтовая.

Оптимизация трафика регистрации рабочей станции

При планировании сайтов продумайте, какой контроллер (контроллеры) домена будут использовать рабочие станции подсети. Чтобы задать регистрацию рабочей станции только на определенных контроллерах доменов, спланируйте сайты так, чтобы только эти контроллеры доменов располагались в той же подсети, что и рабочая станция.

Оптимизация репликации каталогов

При планировании сайтов продумайте, где будут размещаться контроллеры доменов и сетевые соединения между ними. Поскольку каждый контроллер домена должен выполнять репликацию каталога с другими контроллерами своего домена, спланируйте сайты так, чтобы репликация выполнялась в периоды минимальной нагрузки на сеть. Подумайте о создании сервера-плацдарма, чтобы обеспечить выбор контроллера домена, используемого в качестве приемника для репликации между сайтами.

Проектирование структуры сайта

Проектирование структуры сайта для сети, состоящей из одной ЛВС, — простая задача. Поскольку локальные соединения — обычно быстрые, вся сеть может быть одним сайтом. Создайте отдельный сайт *с* собственными контроллерами доменов, если контроллеры доменов будут недостаточно быстро отвечать на запросы пользователей. Понятие «недостаточно быстро» зависит от быстродействия сети. Обычно оно не отвечает требованиям, если сеть расположена на большой территории или неудачно спроектирована.

При проектировании структуры сайта организации, имеющей несколько физических подразделений, следуйте правилам, перечисленным далее.

1. **Выясните особенности физической среды.** Изучите информацию, собранную при определении структуры домена, в том числе расположение сайтов, скорость обмена данными в сети, организацию и использования сетевых подключений и подсети TCP/IP.
2. **Определите физические сети, формирующие домены.** Выясните, какие из них включены в каждый домен.
3. **Определите, какие участки сети вы назначите сайтами.** Если участку сети требуется контроль регистрации рабочих станций или репликация каталога, этот участок необходимо сделать сайтом.
4. **Определите физические соединения сайтов.** Выясните типы соединений, скорости и назначение, так чтобы их удалось определить как объекты соединений сайтов. *Объект межсайтовой связи* (site link object) содержит план, где задано время выполнения репликации между сайтами, которые он соединяет.
5. **Для каждого объекта межсайтовой связи задайте стоимость и расписание.** Для репликации применяется самая дешевая межсайтовая связь. Задайте приоритет каждой связи, указав стоимость (по умолчанию — 100 единиц; чем меньше затраты, тем больше приоритет). По умолчанию репликация осуществляется каждые 3 часа. Задайте ее в соответствии с вашими потребностями.
6. **Обеспечьте избыточность конфигурированием моста связей сайтов.** *Мост связей сайтов* (site link bridge) обеспечивает отказоустойчивость репликации.

Примечание О конфигурировании сайтов и репликации между сайтами рассказано в главе 6.

Резюме

Перед внедрением Active Directory изучите структуру организации и спланируйте структуру домена, доменное пространство имен, структуру ОП и сайтов.

При планировании структуры домена оцените логическую и физическую структуру организации, административные требования, необходимость в нескольких доменах и организацию доменов.

Решите также, как будете использовать именование DNS, в том числе и выбранные ранее доменные имена DNS, и будет ли внутреннее пространство имен DNS совпадать или отличаться от внешнего. Существуют определенные требования к именованию и правила, которым нужно следовать при выборе имен DNS.

ОП позволяют создать логичную и осмысленную модель вашей организации и делегировать административные полномочия на любой уровень иерархии. Существует несколько способов структурирования ОП организации.

Структура сайтов влияет на трафик регистрации рабочих станций и репликацию каталогов Windows 2000. Необходимо соблюдать некоторые правила при проектировании структуры сайта организации, имеющей несколько физических подразделений.

Занятие 2. Установка Active Directory

На этом занятии мы расскажем об установке и удалении Active Directory и использовании мастера установки, а также о БД и общем системном томе, создаваемом Active Directory в процессе установки. Кроме того вы узнаете о настройке DNS для Active Directory и о режимах доменов.

Изучив материал этого занятия, вы сможете:

- ✓ установить Active Directory;
- ✓ удалить Active Directory из контроллера домена.

Продолжительность занятия — около 25 минут.

Мастер установки Active Directory

Мастер установки Active Directory выполняет следующие функции:

- добавляет контроллер домена к существующему домену;
- создает первый контроллер домена в новом домене;
- создает новый дочерний домен;
- создает новое дерево домена;
- устанавливает DNS-сервер;
- создает БД и журналы БД;
- создает общий системный том;
- удаляет службы Active Directory с контроллера домена.

Для запуска мастера установки Active Directory в программной группе Administrative Toots (Администрирование) щелкните Configure Your Server (Настройка сервера) или выполните команду DCPROMO из командной строки. Любым из этих способов вы запустите на изолированном сервере мастер, который поможет вам установить Active Directory и создать новый контроллер домена.

При установке Active Directory можно добавить новый контроллер домена к существующему домену или создать первый контроллер нового домена.

Добавление контроллера к существующему домену

В этом случае вы создаете равноправный контроллер домена. Он обеспечит отказоустойчивость и уменьшит нагрузку на имеющиеся контроллеры доменов.

Создание первого контроллера для нового домена

В этом случае вы создаете новый домен. Он нужен для распределения информации, что позволит вам настроить Active Directory в соответствии с потребностями организации. При создании нового домена разрешается создать новый дочерний домен или новое дерево (табл. 4-1).

Табл. 4-1. Создание новых доменов

Что создается	Описание
Новый дочерний домен	Является дочерним по отношению к имеющемуся
Новое дерево домена	**При** создании нового дерева новый домен не является частью существующего. Можно создать новое дерево в существующем лесе или новый лес

Конфигурирование DNS для Active Directory

Active Directory использует DNS в качестве службы поиска, позволяя компьютерам находить контроллеры доменов. Для поиска контроллера в определенном домене клиент запрашивает DNS о записях ресурсов, содержащих имена и IP-адреса LDAP-серверов домена. LDAP — это протокол, используемый для осуществления запросов и обновления Active Directory и выполняющийся на всех контроллерах домена. Нельзя установить Active Directory, не имея на компьютере службы DNS, потому что Active Directory использует DNS в качестве службы поиска. Однако можно установить DNS без установки Active Directory.

Для конфигурирования DNS-сервера автоматически надо воспользоваться мастером установки Active Directory. Вам не придется вручную настраивать DNS для поддержки Active Directory; это не касается тех случаев, когда вы хотите использовать DNS-сервер без Windows 2000 или создаете особую конфигурацию. Впрочем, чтобы задать конфигурацию, отличную от задаваемой мастером установки по умолчанию, вы можете вручную сконфигурировать DNS, воспользовавшись консолью DNS. Конфигурирование DNS вручную мы в этой книге рассматривать не будем, обратитесь к учебному курсу MCSE издательства «Русская Редакция» «Администрирования сети на основе Windows 2000», 2001.

Примечание О конфигурировании DNS для Active Directory — в главе 5.

База данных и общий системный том

Установка Active Directory создает БД и ее журнал, а также общий системный том (табл. 4-2).

Табл. 4-2. Типы файлов, создаваемых установкой Active Directory

Тип создаваемого файла	Описание
БД и ее журнал	БД — это каталог для нового домена. По умолчанию БД и ее журнал располагаются в каталоге *systemroot*\NTDS, где *systemroot* — это каталог Windows 2000. Для повышения производительности размещайте БД и журнал на разных жестких дисках
Общий системный том	Это структура папки, существующая на всех контроллерах доменов Windows 2000. Он хранит сценарии и некоторые объекты групповой политики для текущего домена и предприятия. По умолчанию общий системный том располагается в каталоге *systemroot*\SYSVOL. Общий системный том должен располагаться в разделе или томе, отформатированном под NTFS 5.0

Репликация общего системного тома идет по тому же расписанию, что и репликация Active Directory, поэтому вы можете не заметить репликацию файлов вновь созданного общего системного тома, пока не пройдет два цикла репликации (обычно это занимает минут 10). Дело в том, что первый цикл репликации файла обновляет конфигурацию других системных томов, уведомляя их о добавлении нового системного тома.

Режимы домена

Существуют два режима домена: смешанный и основной.

Смешанный режим

При первой установке или обновлении контроллера домена до Windows 2000 Server контроллер запускается в *смешанном режиме* (mixed mode), что позволяет ему взаимодействовать с любыми контроллерами доменов под управлением предыдущих версий Windows NT.

Основной режим

Если на всех контроллерах домена установлен Windows 2000 Server и вы не собираетесь больше добавлять в этот домен контроллеры нижнего уровня, переведите домен в *основной режим* (native mode).

При изменении режима со смешанного на основной происходит следующее:

- прекращается поддержка репликации нижнего уровня, после чего в этом домене запрещается иметь контроллеры, не работающие под управлением Windows 2000 Server;
- запрещается добавление новых контроллеров нижнего уровня в данный домен;
- сервер, выполнявший роль основного контроллера домена, перестает быть таковым; все контроллеры становятся равноправными.

Примечание Изменение режима домена возможно лишь в одном направлении. Вам не удастся перейти из основного режима в смешанный.

▶ **Перевод домена в основной режим**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Active Directory Users And Computers (Active Directory — пользователи и компьютеры).
2. Щелкните название домена правой кнопкой мыши и выберите в контекстном меню команду Properties (Свойства).
3. На вкладке General (Общие) щелкните Change Mode (Изменить режим).
4. В окне сообщения Active Directory щелкните кнопку Yes (Да), затем — OK.
5. Перезагрузите компьютер.

Удаление служб Active Directory с контроллера домена

Выполнение команды DCPROMO из диалогового окна Run на контроллере домена позволяет удалить Active Directory с этого контроллера, превратив его в рядовой сервер. Если контроллер является последним в домене, он станет изолированным сервером. Если вы удаляете Active Directory со всех контроллеров в домене, вы также удаляете БД каталога для этого домена, и домен перестает существовать. Компьютерам, соединенным с этим доменом, с этого момента запрещается входить в него и пользоваться его службами.

▶ **Удаление Active Directory с контроллера домена**

1. Зарегистрируйтесь в системе как администратор.
2. Раскройте меню Start\Run (Пуск\Выполнить), наберите в поле Open (Открыть) команду **dcpromo** и щелкните OK.

   Откроется окно мастера установки Active Directory.
3. В окне мастера щелкните Next.
4. Если сервер является последним контроллером в домене, пометьте соответствующий флажок и щелкните Next.
5. Введите имя пользователя и пароль с правами Enterprise Administrator (Администратор предприятия) для этого домена и щелкните Next.

6. Введите и подтвердите пароль учетной записи Administrator (Администратор) сервера и щелкните Next.
7. В окне сводной информации щелкните Next.
8. Щелкните кнопку Finish (Готово), чтобы завершить удаление Active Directory с компьютера.

Практикум: установка Active Directory

Установите Active Directory на изолированный сервер, превратив его таким образом в контроллер домена для нового домена. Для этого воспользуйтесь программой DCPROMO и мастером установки Active Directory. Просмотрите созданный домен и поработайте с консолью Active Directory Users And Computers. Убедитесь, что служба DNS работает.

▶ Задание 1: установите службу Active Directory на изолированный сервер

1. Перезагрузите компьютер и зарегистрируйтесь как администратор.

   Если откроется окно Configure Your Server (Настройка сервера), закройте его, потому что для выполнения этого упражнения вам понадобится программа DCPROMO.
2. Раскройте меню Start\Run (Пуск\Выполнить).

   Откроется диалоговое окно Run (Выполнить).
3. В поле Open (Открыть) наберите **dcpromo** и щелкните OK.

   Откроется окно мастера установки Active Directory.
4. Щелкните Next.

   Откроется окно Domain Controller Type (Тип контроллера домена).
5. Выберите Domain Controller For A New Domain (Контроллер домена в новом домене) и щелкните Next.

   Откроется окно Create Tree Or Child Domain (Создание дерева или дочернего домена).
6. Убедитесь, что выбран переключатель Create A New Domain Tree (Создать новое дерево домена) и щелкните Next.

   Откроется окно Create Or Join Forest (Создание леса или присоединение к лесу).
7. Щелкните переключатель Create A New Forest Of Domain Trees (Создать новый лес доменных деревьев) и затем — Next.

   Откроется окно New Domain Name (Имя DNS-домена).
8. В окне Full DNS Name For New Domain (Полное DNS-имя нового домена) наберите **microsoft.com** и щелкните Next.

   (Если вы используете отличное от microsoft.com имя домена, введите его).

   Через несколько секунд откроется окно NetBIOS Domain Name (NetBIOS-имя домена).
9. Убедитесь, что MICROSOFT (или сокращение DNS-имени, которое вы выбрали) появилось в окне NetBIOS Domain Name и щелкните Next.

   Откроется окно Database and Log Locations (Местоположение базы данных и журнала).
10. Убедитесь, что для размещения базы данных и протокола выбран путь *systemroot*\NTDS и щелкните Next. (Если ОС Windows 2000 установлена не в папке WINNT, оба пути будут указывать на папку NTDS в папке, где установлена Windows 2000.)

    Откроется окно Shared System Volume (Общий доступ к системному тому).
11. Убедитесь, что для размещения SYSVOL указан путь *systemroot*\SYSVOL (Если Windows 2000 установлена не в каталоге WINNT, общий системный том будет находиться в подпапке SYSVOL папки, где установлена Windows 2000).

Каково требование к размещению SYSVOL?

Каково назначение SYSVOL?

12. Щелкните Next, чтобы подтвердить путь *systemroot*\SYSVOL (или путь к каталогу, в котором установлена Windows 2000) в качестве пути к SYSVOL.

    Появится сообщение, напоминающее о необходимости установки и конфигурирования DNS-сервера. Щелкните OK. Откроется окно Configure DNS (Настойка DNS).

13. Выберите Yes, Install And Configure DNS On This Computer (Да, автоматически установить и настроить DNS) и щелкните Next.

    Откроется окно Permissions (Разрешения).

14. Если администратор не советует иначе, выберите Permissions Compatible Only With Windows 2000 Server (Разрешения, совместимые только с серверами Windows 2000) и щелкните Next.

    Откроется окно Directory Services Restore Mode Administrator Password (Пароль администратора для режима восстановления).

15. Введите пароль, который хотите присвоить этой учетной записи сервера Administrator в случае, если компьютер загрузится в режиме Directory Services Restore (Режим восстановления), затем щелкните Next.

    Откроется окно Summary (Сводка), представляющее список выбранных вами параметров установки.

16. Изучите содержание этого окна и щелкните Next.

    Появится индикатор хода установки Configuring Active Directory (Идет настройка Active Directory). Этот процесс займет несколько минут. Вам потребуется вставить в дисковод установочный компакт-диск Windows 2000 Server.

17. Когда откроется окно Completing The Active Directory Installation Wizard (Завершение работы мастера установки Active Directory), щелкните кнопку Finish (Готово) и затем — кнопку Restart Now (Перезагрузить компьютер сейчас).

► Задание 2: просмотрите домен из окна My Network Places

1. Зарегистрируйтесь как администратор.
2. Если откроется окно Configure Your Server (Настройка сервера), закройте его.
3. Дважды щелкните значок My Network Places (Мое сетевое окружение).

   Откроется одноименное окно.

   Какие параметры отображаются?

4. Дважды щелкните значок Entire Network (Вся сеть), затем дважды щелкните значок Microsoft Windows Network (сеть Microsoft Windows).

   Что вы видите?

5. Закройте окно Microsoft Windows Network.

► Задание 3: просмотрите домен с помощью Active Directory Users And Computers

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Active Directory Users And Computers.

   Откроется одноименная консоль.

2. В дереве консоли дважды щелкните microsoft.com (или имя вашего домена).

   Что содержит узел microsoft?

3. В дереве консоли щелкните Domain Controllers.

Обратите внимание: на правой панели появится название SERVER1. Если вы не использовали SERVER1 в качестве имени вашего сервера, то вместо него появится DNS-имя сервера,

4. Закройте консоль Active Directory Users And Computers.

► **Задание 4: протестируйте службу DNS с помощью консоли DNS**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните DNS.
2. Откроется консоль DNS. В дереве консоли DNS щелкните правой кнопкой SERVER1 (или имя вашего сервера) и выберите команду Properties (Свойства).

   Откроется окно свойств SERVER1 (Если вы задали своему серверу другое имя, в заголовке окна будет значиться оно).
3. Перейдите на вкладку Monitoring.
4. В списке Select A Test Type (Выберите тип теста) пометьте флажки A Simple Query Against This DNS Server (Простой запрос к этому DNS-серверу) и A Recursive Query To Other DNS Servers (Рекурсивный запрос к другим DNS-серверам) и щелкните Test Now (Протестировать).

   В окне свойств Server1 в списке результатов тестирования должна появиться надпись PASS (Пройден успешно) — в столбцах Simple Query (Простой запрос) и Recursive Query (Рекурсивный запрос).
5. Щелкните OK.
6. Закройте консоль DNS.

Резюме

Мастер установки Active Directory можно запустить либо выполнив команду Configure Your Server, либо введя команду DCPROMO в командной строке. Мастер установки Active Directory используется для добавления контроллера к существующему домену, для создания первого контроллера нового домена, для создания нового дочернего домена и нового дерева доменов, а также для удаления Active Directory из контроллера домена.

БД Active Directory — это каталог для нового домена. По умолчанию БД и журналы располагаются в папке *systemroot*\NTDS. Во время установки Active Directory создается общий системный том — структура папок, существующая на всех контроллерах доменов Windows 2000. В нем хранятся сценарии и некоторые объекты групповых политик для текущего домена и предприятия. По умолчанию он располагается в папке *systemroot*\SYSVOL.

Active Directory использует DNS в качестве службы поиска, позволяя компьютерам находить контроллеры доменов, поэтому нельзя установить Active Directory, не имея в сети службы DNS. Можно сконфигурировать DNS-сервер автоматически, средствами мастера установки Active Directory. Если вы не используете отличный от Windows 2000 DNS-сервер и не собираетесь выполнять особую конфигурацию, нет необходимости конфигурировать DNS для поддержки Active Directory вручную.

Существуют смешанный и основной режимы работы домена. Смешанный режим допускает совместимость с предыдущими версиями Windows NT, а основной используется, только если все контроллеры в домене работают под управлением Windows 2000 Server.

Занятие 3. Роли хозяина операций

Это специальные роли, назначаемые одному или нескольким контроллерам в домене Active Directory. Контроллеры доменоа, которым назначены эти роли, выполняют репликацию с одним хозяином. Здесь рассказывается о ролях хозяина операций и задачах, связанных с их назначениями.

Изучив материал этого занятия, вы сможете:

- ✓ описать роли мастера операций в лесе и домене;
- ✓ спланировать расположение хозяина операций;
- ✓ просмотреть назначения роли хозяина операций;
- ✓ передать назначения роли хозяина операций.

Продолжительность занятия — около 15 минут.

Роли хозяина операций

Active Directory поддерживает репликацию БД с несколькими хозяевами между всеми контроллерами домена. Однако некоторые изменения не следует выполнять в этом режиме, поэтому один или более контроллеров доменов разрешается привлекать к выполнению операций, которые должны выполняться с одним хозяином (они не могут выполняться одновременно в разных местах сети). *Роли хозяина операций* (operations master roles) назначаются контроллерам доменов для выполнения операций с одним хозяином.

В любом лесе Active Directory одному или нескольким контроллерам доменов разрешается назначать пять ролей хозяина операций. Необходимо, чтобы одни роли содержались в каждом лесе, другие — в каждом домене леса. Можно изменить назначение ролей хозяина операций после установки, но в большинстве случаев это не требуется. Вы должны знать, какие роли хозяина операций назначены контроллеру домена; это пригодится, если с контроллером возникнут проблемы или вы захотите исключить его из работы.

Роли хозяина операций на уровне леса

Каждый лес Active Directory должен содержать следующие роли:

- хозяин схемы;
- хозяин именования домена.

Это роли должны быть уникальны в лесе, то есть во всем лесе может быть только один хозяин схемы и один хозяин именования домена.

Хозяин схемы

Хозяин схемы управляет всеми обновлениями и изменениями схемы. Для обновления схемы леса необходимо иметь доступ к хозяину схемы. В любой момент времени может быть только один хозяин схемы в составе всего леса.

Хозяин именования домена

Контроллер домена, выполняющий роль хозяина именования домена, управляет операциями добавления или удаления доменов в составе леса. В любой момент времени может быть только один хозяин именования домена в составе всего леса.

Роли хозяина операций на уровне домена

Каждый домен в лесе должен иметь следующие роли:

- хозяин относительных идентификаторов;
- эмулятор *основного контроллера домена* (primary domain controller, PDC);
- хозяин инфраструктуры.

Эти роли должны быть уникальны в каждом домене: каждому домену в лесе разрешается иметь только одного хозяина относительных идентификаторов, эмулятор PDC и хозяина инфраструктуры.

Хозяин относительных идентификаторов

Хозяин относительных идентификаторов назначает ряд относительных идентификаторов каждому контроллеру в своем домене. В любой момент времени в каждом домене леса может быть только один контроллер домена, выполняющий роль хозяина относительных идентификаторов.

Каждый раз при создании объекта пользователя, группы или компьютера контроллер домена назначает данному объекту уникальный код безопасности. Он состоит из кода безопасности домена (который одинаков для всех кодов безопасности, созданных в этом домене) и относительного кода безопасности, уникального для каждого кода безопасности, созданного в домене.

Для перемещения объекта между доменами (с помощью служебной программы Movetree.exe) необходимо произвести перемещение на контроллере, который выполняет роль хозяина относительных идентификаторов домена, содержащего в данный момент этот объект.

Эмулятор основного контроллера домена

Если в домене есть компьютеры без установленного клиентского программного обеспечения Windows 2000 или резервные контроллеры домена Windows **NT,** эмулятор основного контроллера домена работает как основной контроллер домена Windows **NT.** Он обрабатывает изменения паролей от клиентов и реплицирует обновления на резервные контроллеры домена. В любой момент времени в каждом домене леса может быть только один контроллер домена, выполняющий роль эмулятора основного контроллера домена.

При работе домена Windows 2000 в основном режиме эмулятор основного контроллера получает преимущественную репликацию изменений пароля, выполненных другими контроллерами в данном домене. При изменении пароля репликация этих изменений на каждый контроллер домена занимает некоторое время. Если проверка подлинности при входе в сеть заканчивается неудачно из-за неверного пароля на одном контроллере домена, он пересылает запрос на проверку подлинности на эмулятор основного контроллера домена, прежде чем отказать в доступе.

Хозяин инфраструктуры

Хозяин инфраструктуры отвечает за обновление ссылок «группа — пользователь» при переименовании или изменении членов группы. В любой момент времени в каждом домене может быть только один контроллер домена, выполняющий роль хозяина инфраструктуры.

При переименовании или перемещении члена группы (и размещении данного члена в другом домене, отличном от домена этой группы) он может временно не отображаться в группе. Хозяин инфраструктуры домена, содержащего данную группу, отвечает за обновление группы и обладает сведениями об имени и расположении данного члена. Хозяин

инфраструктуры распространяет обновленные сведения с помощью репликации с несколькими хозяевами.

Зашита не подвергается опасности в период времени между переименованием члена группы и обновлением этой группы. Только администратор, просматривающий участие в отдельной группе, может заметить временное несоответствие.

Планирование расположения хозяина операций

При использовании небольшого леса Active Directory с одним доменом и одним контроллером домена данный контроллер выполняет роли всех хозяев операций. При создании первого домена в составе нового леса все роли одиночного хозяина операций автоматически назначаются первому контроллеру в этом домене.

При создании нового дочернего домена или корневого домена нового дерева в составе существующего леса первому контроллеру в новом домене автоматически назначаются следующие роли:

- хозяин относительных идентификаторов;
- эмулятор основного контроллера домена;
- хозяин инфраструктуры.

Так как возможен только один хозяин схемы и один хозяин именования доменов в составе леса, данные роли остаются в домене, который был создан первым в данном лесе.

На рис. 4-9 показано принятое по умолчанию распределение ролей хозяина операций в лесе.

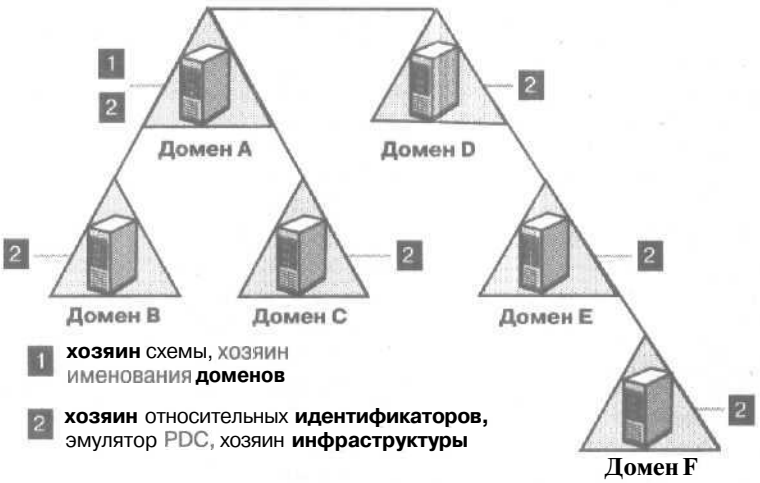


Рис. 4-9. Принятое по умолчанию распределение ролей хозяина операций в лесе

На рисунке Домен А был первым, созданным в составе леса (он также называется корневым доменом леса). Содержит обе роли хозяина операций на уровне всего леса. Первому контроллеру в остальных доменах назначаются три роли, которые относятся только к определенному домену.

Расположение по умолчанию хозяев операций подходит для леса, развернутого на несколько контроллеров домена в одном сайте. В лесе, который содержит множество контроллеров или несколько сайтов, иногда возникает необходимость переместить назначенные по умолчанию роли хозяев операций на другие контроллеры в составе домена или леса.

Планирование назначения ролей хозяев операций в домене

Если в домене только один контроллер, то ему принадлежат все роли в домене. В ином случае следует выбрать два контроллера, которые являются прямыми партнерами репликации и входят в состав хорошо организованной сети. Один из контроллеров домена следует сделать хозяином операций. Другой контроллер необходимо сделать запасным хозяином операций. Контроллер домена в роли *запасного* (standby) *хозяина операций* используется в случае отказа контроллера домена, выполняющего роль хозяина операций.

В типичных доменах следует назначать роли хозяина относительных идентификаторов и эмулятора основного контроллера домена контроллеру домена, выполняющему роль хозяина операций. В домене очень большого размера вы уменьшите пиковую загрузку эмулятора основного контроллера, разместив данные роли на разные контроллеры, каждый из которых является прямым партнером репликации контроллера домена в роли запасного хозяина операций. Следует сохранять эти роли на одном контроллере до тех пор, пока загрузка хозяина операций не потребует разделения этих ролей.

Роль хозяина инфраструктуры следует назначить любому контроллеру домена, который не является глобальным каталогом, но имеет с ним хорошую связь. Глобальный каталог может находиться в любом домене того же сайта, что и контроллер домена. Если контроллер домена в роли хозяина операций отвечает данным требованиям, его следует использовать до тех пор, пока загрузка контроллера не потребует разделения ролей.

Планирование ролей хозяев операций для леса

После планирования всех ролей для каждого домена, следует рассмотреть роли для леса. Роли хозяина схемы и хозяина именования доменов всегда назначаются одному контроллеру домена. Для повышения производительности эти роли следует назначать контроллеру домена, который имеет хорошую связь с компьютерами, используемыми администратором или группой, ответственными за обновления схемы и создание новых доменов. Загрузка данных ролей хозяев операций очень мала, поэтому для облегчения управления следует помешать эти роли на контроллер одного из доменов леса.

Планирование развития

В общем случае при развитии леса не требуется изменять расположение ролей хозяина операций. Но если планируется удаление контроллера домена, изменение статуса глобального каталога контроллера домена либо изменение порядка взаимодействия частей сети, следует пересмотреть план и соответственно скорректировать назначения ролей хозяина операций.

Определение назначений ролей хозяина операций

Прежде чем изменять назначения ролей хозяина операций, необходимо ознакомиться с текущими назначениями,

► **Определение хозяина относительных идентификаторов, эмулятора PDC и хозяина инфраструктуры**

1. Откройте консоль Active Directory Users and Computers (Active Directory — пользователи и компьютеры).
2. В дереве консоли щелкните правой кнопкой папку Active Directory Users and Computers, затем — Operations Masters (Хозяева операций).
3. В открывшемся окне выберите один из следующих вариантов:
   - щелкните вкладку R1D, и в поле Operations Master (Хозяин операций) появится имя хозяина относительных идентификаторов;

- щелкните вкладку PDC, и в окне Operations Master появится имя эмулятора PDC;
- щелкните вкладку Infrastructure (Инфраструктура), и в поле Operations Master появится имя хозяина инфраструктуры.

4. Щелкните кнопку Cancel (Отмена), чтобы закрыть окно Operations Master.

▶ **Определение хозяина именования доменов**

1. Откройте консоль Active Directory Domains and Trusts (Active Directory — домены и доверие).
2. В дереве консоли щелкните правой кнопкой папку Active Directory Domains and Trusts и выберите команду Operations Master.

   В окне Change Operations Master (Изменение хозяина операций) имя текущего хозяина именования домена появится в поле Domain Naming Operations Master (Хозяин именования доменов).
3. Щелкните кнопку Close (Закрыть), чтобы закрыть окно Change Operations Master.

▶ **Определение хозяина схемы**

1. Откройте оснастку Active Directory Schema (Схема Active Directory).

Примечание Эта оснастка устанавливается в составе пакета Windows 2000 Administration Tools (Администрирование Windows 2000). Об установке консоли Active Directory Schema см. главу 3.

---

2. В дереве консоли щелкните правой кнопкой Active Directory Schema, затем левой — Operations Master.
3. В окне Change Schema Master (Смена хозяина схемы) имя текущего хозяина схемы появится в поле Current Operations Master (Текущий хозяин операций).

Передача ролей хозяина операций

Подразумевает перемещение их с одного контроллера домена на другой при содействии исходного владельца ролей. В зависимости от передаваемых ролей хозяина операций перемещение осуществляется с помощью одной из трех оснасток Active Directory.

▶ **Передача роли хозяина относительных идентификаторов, эмулятора PDC или хозяина инфраструктуры**

1. Откройте консоль Active Directory Users and Computers.
2. В дереве консоли щелкните правой кнопкой узел домена, который станет новым хозяином относительного идентификатора, эмулятором PDC или хозяином инфраструктуры, затем щелкните Connect To Domain (Подключение к домену).
3. В окне Connect To Domain введите имя домена или щелкните кнопку Browse (Обзор), чтобы выбрать домен из списка, затем щелкните OK.
4. В дереве консоли щелкните правой кнопкой узел Active Directory Users And Computers и выберите команду Operations Masters (Хозяин операций).
5. В открывшемся окне выберите один из следующих вариантов:
   - щелкните вкладку RID, затем — кнопку Change (Изменить);
   - щелкните вкладку PDC, затем — кнопку Change;
   - щелкните вкладку Infrastructure, затем — кнопку Change.
6. Щелкните OK, чтобы закрыть окно Operations Masters.

▶ **Передача роли хозяина именования доменов**

1. Откройте консоль Active Directory Domains And Trusts .
2. В дереве консоли щелкните правой кнопкой узел контроллера домена, который станет новым хозяином именования домена, затем щелкните Connect To Domain.
3. В окне Connect To Domain введите имя домена или щелкните кнопку Browse, чтобы выбрать домен из списка, затем щелкните OK.
4. В дереве консоли щелкните правой кнопкой папку Active Directory Domains And Trusts и выберите команду Operations Master.
5. В окне Change Operations Master щелкните кнопку Change.
6. Щелкните OK, чтобы закрыть окно Change Operations Master.

▶ **Передача роли хозяина схемы**

1. Откройте оснастку Active Directory Schema.
2. В дереве консоли щелкните правой кнопкой Active Directory Schema и выберите команду Change Domain Controller (Изменение контроллера домена).
3. В окне Change Domain Controller выберите один из следующих вариантов:
   - любой DC, чтобы Active Directory выбрала новый хозяин операции схемы;
   - задать Name (Имя) и ввести имя нового хозяина схемы, чтобы определить новый хозяин операции схемы.
4. Щелкните OK.
5. В дереве консоли щелкните правой кнопкой Active Directory Schema и выберите команду Operations Master.
6. В окне Change Schema Master (Смена хозяина схемы) щелкните кнопку Change.
7. Щелкните OK, чтобы закрыть окно Change Schema Master.

Действия в случае отказов хозяина операций

Некоторые роли хозяина операций имеют решающее значение для работы сети. Другие же могут не выполняться некоторое время, прежде чем из-за этого возникают проблемы. Обычно недоступность компьютера, играющего роль хозяина операций, выясняется при попытке выполнить какую-либо операцию, за которую отвечает этот хозяин.

Если хозяин операций недоступен по причине сбоя компьютера или сети, можно назначить роль хозяина операций другому контроллеру домена. Это также называется принудительным перемещением роли хозяина операций.

Перед принудительным перемещением сначала следует определить причину и ожидаемую продолжительность неисправности компьютера или сети. Если причина неполадки сети или компьютера скоро будет устранена, подождите, пока исполняющий роль хозяина операций компьютер снова станет доступен. Если неисправен контроллер домена, в данный момент выполняющий эту роль, необходимо определить, можно ли его восстановить и снова подключить.

В целом, назначение роли хозяина операций является радикальным методом, который стоит применять, только если невозможно восстановить текущий хозяин операций. Принятие решения зависит от роли и времени, в течение которого обладатель роли будет недоступен. Проблемы, возникающие при различных неполадках обладателей роли, обсуждаются в следующих главах.

Внимание! Контроллер домена, роль хозяина схемы, именования или относительного идентификатора которого была передана, *никогда* не возвращайте в работу без предварительного форматирования дисков и переустановки Windows 2000.

Отказ хозяина схемы

Временная недоступность хозяина схемы незаметна для пользователей. Да и администратор не заметит этого, пока не попытается изменить схему либо установить приложение, изменяющее ее в процессе установки.

Если хозяин схемы долгое время недоступен, можно назначить его роль хозяину операций, находящемуся в режиме ожидания. Тем не менее присвоение этой роли — радикальное решение, и его следует предпринимать, только если неполадку хозяина схемы нельзя исправить.

Отказ хозяина именования домена

Временная недоступность хозяина именования доменов незаметна для пользователей. Администратор сети это также вряд ли обнаружит, пока не попытается добавить или удалить домен из леса.

Если хозяин именования доменов долгое время недоступен, можно назначить его роль хозяину операций, находящемуся в режиме ожидания. Тем не менее присвоение этой роли - радикальное решение, и его следует предпринимать, только если неполадку хозяина доменов нельзя исправить.

Отказ хозяина относительных идентификаторов

Временная недоступность хозяина относительных идентификаторов незаметна для пользователей. Администратор сети это также вряд ли обнаружит, пока не закончатся относительные идентификаторы в домене, где создаются объекты.

Если хозяин относительных идентификаторов долгое время недоступен, можно назначить его роль хозяину операций, находящемуся в режиме ожидания. Тем не менее присвоение этой роли — радикальное решение, и его следует предпринимать, только если неполадку хозяина относительных идентификаторов нельзя исправить.

Отказ эмулятора PDC

Отказ эмулятора основного контроллера домена заметно отражается на работе пользователей сети. Поэтому, когда эмулятор PDC недоступен, надо немедленно назначить его роль другому контроллеру домена.

Если эмулятор PDC долгое время недоступен и в его домене есть клиенты, не имеющие программного обеспечения Windows 2000 либо резервные контроллеры домена Windows NT, следует присвоить роль эмулятора PDC хозяину операций, находящемуся в режиме ожидания. Когда исходный эмулятор основного контроллера домена исправят, можно вернуть его роль исходному контроллеру домена.

Отказ хозяина инфраструктуры

Временная недоступность хозяина инфраструктуры незаметна для пользователей. Администратор сети это также вряд ли обнаружит, если он не переименовал или не переместил большое количество учетных записей незадолго до этого.

Если хозяин инфраструктуры недоступен длительное времени, можно назначить его роль контроллеру домена, который не является глобальным каталогом, но имеет с ним надежное соединение (из любого домена). Желательно, чтобы данный контроллер находился в том же сайте, что и текущий глобальный каталог. Когда хозяин инфраструктуры будет исправлен, можно возвратить его роль исходному контроллеру домена.

Резюме

В лесе существуют две роли хозяина операций: хозяин схемы и хозяин именования домена, а в домене — три: хозяин относительных идентификаторов, эмулятор PDC и хозяин инфраструктуры. В маленьком лесе Active Directory с одним доменом и контроллером последнему назначаются все роли хозяина операций. Когда в новом лесе создается первый домен, ему автоматически назначаются все роли хозяина операций. Передача ролей хозяина операций означает перемещение их с одного контроллера домена на другой, осуществляемое с помощью одной из трех консолей Active Directory.

Занятие 4. Внедрение структуры ОП

Организационные подразделения (ОП) должны отражать подробности структуры организации. Каждый домен может иметь собственную иерархию ОП. Если ваша организация содержит несколько доменов, вы вправе создать ОП внутри каждого домена независимо от структур ОП в других доменах. Сейчас мы расскажем об этапах создания структуры ОП.

Изучив материал этого занятия, вы сможете:

- ✓ **создать ОП.**

Продолжительность занятия — около 10 минут.

Создание ОП

Для создания ОП служит оснастка Active Directory Users and Computers (Active Directory — пользователи и компьютеры). ОП всегда создается на первом доступном контроллере домена, с которым контактирует оснастка, и затем ОП реплицируется на все остальные контроллеры.

▶ **Создание ОП**

1. Зарегистрируйтесь в качестве администратора.
2. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Active Directory Users And Computers (Active Directory — пользователи и компьютеры).
3. Щелкните контейнер, где вы хотите создать ОП, — домен (например, microsoft.com) или другое ОП.
4. В меню Action (Действие) выберите New (Создать), а затем — Organizational Unit (Подразделение).
5. В окне New Object — Organizational Unit (Новый объект — Подразделение) в поле Name (Имя) введите имя нового ОП и щелкните OK.

Задание свойств ОП

По умолчанию с каждым создаваемым ОП ассоциируется набор свойств, аналогичных атрибутам объектов.

Свойства, присвоенные ОП, можно использовать для поиска ОП в каталоге. По этой причине для каждого ОП надо детально описать свойства. Например, можно осуществлять поиск по описанию или адресу ОП,

Вкладки окна свойств ОП — General (Общие), Managed By (Управляется) и Group Policy (Групповая политика) — содержат информацию о каждом ОП. Например, если заполнены все поля вкладки General (рис. 4-10), вы можете найти ОП, используя его описание или другое поле.

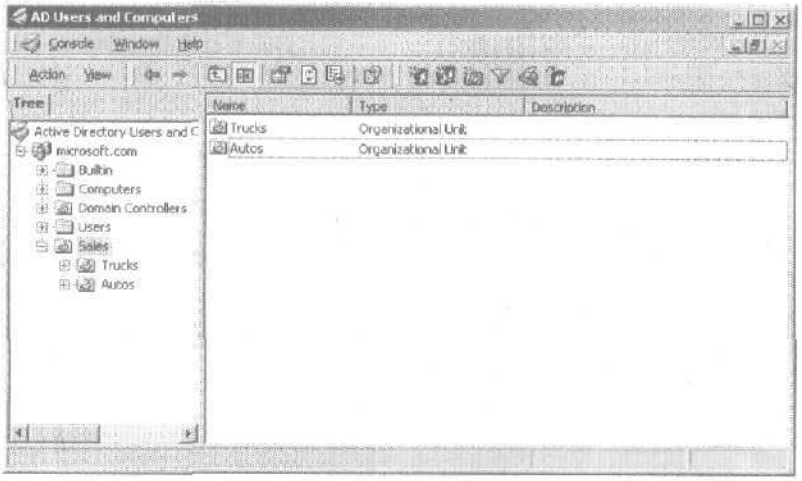


Рис. 4-10. Вкладка General (Общие) окна свойств ОП

В табл. 4-3 описаны вкладки окна свойств ОП.

Табл. 4-3. Вкладки окна свойств ОП

Вкладка	Описание
General (Общие)	Содержит описание ОП, адрес, город, штат или провинцию, почтовый индекс и страну или район
Managed By (Управляется)	Содержит имя владельца ОП, местонахождение офиса, адрес, город, штат или провинцию, страну или район, номер телефона и номер факса
Group Policy (Групповая политика)	Содержит связи политики групп ОП

▶ **Настройка свойств ОП**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers,
2. Раскройте домен,
3. Щелкните правой кнопкой ОП и выберите команду Properties.
4. Щелкните соответствующую вкладку свойств ОП, которые хотите задать или поменять, и введите значения в каждое поле.

Практикум: создание ОП

Создайте часть организационной структуры домена с помощью создания трех ОП.

▶ **Задание: создайте ОП**

1. Зарегистрируйтесь как администратор.
2. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Active Directory Users And Computers (Active Directory — пользователи и компьютеры).

   Отобразится одноименная консоль.

3. Раскройте домен microsoft.com (или заданный вами домен).

   ОП отображаются в списке домена в виде папок со значком книги каталога. Папки без значков — это специализированные контейнеры.

   Какие ОП заданы в вашем домене по умолчанию?

   Чтобы убедиться, что вы создаете новое ОП там, где нужно, сначала выберите соответствующее местоположение.
4. В дереве консоли щелкните ваш домен (например, microsoft.com).
5. В меню Action (Действие) выберите пункт New (Создать) и щелкните Organizational Unit (Подразделение).

   Откроется окно New Object — Organizational Unit (Новый объект — Подразделение). Заметьте: требуется задать только имя ОП. Окно указывает местоположение, где будет создан объект. Это должен быть ваш домен.
6. В поле Name (Имя) введите **Sales** и щелкните OK.
7. В дереве консоли щелкните ОП Sales.
8. В меню Action выберите команду New и щелкните Organizational Unit.
9. В поле Name введите Trucks и щелкните OK.

   Оснастка отобразит вновь созданное ОП Trucks (ниже Sales).
10. Ниже ОП Sales создайте еще одно ОП с именем Autos.

    Active Directory Users and Computers отобразит вновь созданное ОП Autos (отображается ниже ОП Sales) в добавление к ОП Trucks и стандартным ОП в домене (рис. 4-11).

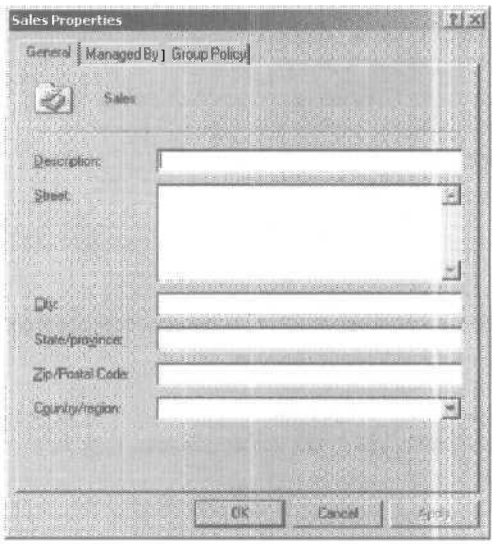


Рис. 4-11. Структура ОП

Резюме

Для создания нового ОП используется консоль Active Directory Users and Computers. ОП всегда создается на первом доступном контроллере домена, с которым может связаться консоль MMC, и затем реплицируется на все остальные контроллеры.

С каждым создаваемым ОП по умолчанию ассоциируется набор свойств, аналогичных атрибутам объектов, которые могут использоваться для поиска ОП в каталоге.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении А «Вопросы и ответы» в конце книги.

1. Каковы причины создания нескольких доменов?

2. Для вашей организации внешнее пространство имен Интернета зарезервировано регистрационной организацией DNS. При планировании внедрения Active Directory вы рекомендуете расширить это пространство имен для внутренней сети. Какие это дает преимущества?

3. Каким образом настройка сайтов отражается на работе Windows 2000?

4. Что такое обший системный том, каково его назначение, где он расположен и как называется?

5. Каково назначение ролей хозяина операций?

6. Какое средство применяется для создания ОП?

ГЛАВА 5

Взаимодействие DNS и Active Directory

В этой главе

При разработке Microsoft Windows 2000 Server особое внимание уделялось интегрированию службы DNS с Active Directory. При совместном использовании Active Directory и Windows 2000 Server это означает:

- для обнаружения контроллеров домена Windows 2000 используется процедура разрешения имен DNS. Служба Netlogon обращается к серверу DNS при регистрации контроллеров домена в DNS;
- службу Active Directory можно использовать для хранения, интегрирования и репликации зон.

В этой главе мы познакомим вас с процессом разрешения имен в DNS, с понятием «зона», а также объясним преимущества зон, интегрированных в Active Directory. В упражнениях этой главы вы займетесь конфигурированием зоны. Кроме того, мы расскажем о репликации и передаче зон и опишем устранение неполадок при конфигурации Active Directory и DNS.

Прежде всего

Для изучения материалов этой главы необходимо:

- выполнить процедуры установки, описанные во вводной главе;
- установить Active Directory, как описано в главе 4;
- уметь работать с MMC.

Занятие 1. Основы разрешения имен в DNS

Служба DNS обеспечивает разрешение имен для клиентов под Windows 2000. Разрешение имен позволяет пользователю обращаться к серверам по имени, а не по IP-адресу, который трудно запомнить. Сейчас мы расскажем о процессе разрешения имен.

Изучив материал этого занятия, вы сможете:

- описать процесс разрешения имен;

Продолжительность занятия — около 10 минут

Разрешение имен

Это процесс определения IP-адреса по имени DNS; он похож на поиск в телефонном справочнике, где имени и фамилии сопоставлен номер телефона. Например, для подключения к Web-узлу Microsoft вы используете имя www.microsoft.com. DNS разрешает это имя в связанный с ним IP-адрес 207.46.130.149. Таблица соответствия имен IP-адресам хранится в распределенной базе данных DNS.

IP-адресация

Каждый компьютер, поддерживающий протокол TCP/IP, идентифицируется своим IP-адресом; 32-битный IP-адрес состоит их двух частей — идентификаторов сети и узла.

- Идентификатор сети, называемый также адресом сети, определяет конкретную подсеть в большой TCP/IP-сети. Все системы, которые получают и разделяют доступ к одной подсети, имеют общий идентификатор сети внутри своего полного IP-адреса. Этот идентификатор также используется для уникального определения каждой подсети внутри общей сети.
- Идентификатор узла, называемый также адресом узла, определяет узел TCP/IP (рабочую станцию, сервер, маршрутизатор или другое устройство, поддерживающее TCP/IP) внутри каждой сети. Адрес узла такого устройства однозначно определяет конкретную систему внутри ее сети.

Вот пример 32-битного IP-адреса:
10000011 01101011 00010000 11001000

Для удобства IP-адреса записываются в десятично-точечной нотации. 32-битный адрес разделяется на четыре 8-битных октета. Октеты записываются в десятичной системе и разделяются точками. Так, показанный нами IP-адрес записывается в десятичной нотации как 131.107.16.200, где сетевую часть составляют два первых числа (131.107), а идентификатор узла — два последних (16.200).

Запрос поиска

Серверы DNS разрешают прямые и обратные запросы. Прямой запрос определяет IP-адрес по имени, а обратный — имя по адресу. Сервер DNS способен разрешать запрос только в пределах своей зоны полномочий. Если же он не может разрешить запрос, он передает его другому серверу DNS, который, вероятно, сумеет это сделать. Серверы DNS кэшируют результаты, чтобы снизить нагрузку на сеть.

Прямой запрос

Служба DNS использует для разрешения имен модель «клиент-сервер». Чтобы разрешить запрос прямого поиска, клиент посылает запрос локальному серверу **DNS.** Этот сервер либо сам разрешает запрос, либо передает его другому серверу **DNS.** На рис. 5-1 показано, как клиент, находящийся вне зоны microsoft.com запрашивает у сервера DNS IP-адрес сайта www.microsoft.com.

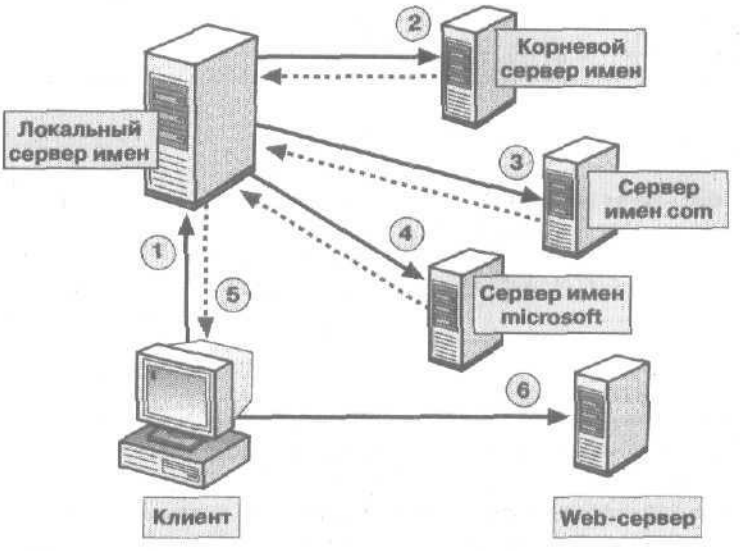


Рис. 5-1. Разрешение запроса прямого поиска

Ниже объясняется нумерация стадий на рис. 5-1.

1. Клиент передает запрос прямого поиска локальному серверу DNS.
2. Локальный сервер проверяет базу данных своей зоны, определяя, есть ли в ней данные для разрешения запроса. Локальный сервер не имеет полномочий в домене microsoft.com, поэтому он передает запрос одному из корневых серверов DNS, требуя разрешения имени узла. Корневой сервер возвращает ссылку на серверы DNS домена com.
3. Локальный сервер посылает запрос серверу DNS домена com, который возвращает ссылку на серверы домена microsoft.
4. Локальный сервер отправляет запрос серверу DNS домена microsoft. Так как этот сервер имеет полномочия в этой части пространства имен домена, он возвращает IP-адрес для www.microsoft.com локальному серверу DNS.
5. Локальный сервер посылает адрес www.microsoft.com клиенту.
6. Процесс разрешения имени завершен, и клиент получает доступ к сайту www.microsoft.com.

Кэширование на серверах DNS

При разрешении имени иногда приходится посылать несколько запросов, прежде чем ответ будет найден. При каждом запросе сервер находит другие серверы DNS, которые имеют полномочия в различных пространствах имен. Сервер кэширует результаты запросов, чтобы снизить нагрузку на сеть (рис. 5-2).

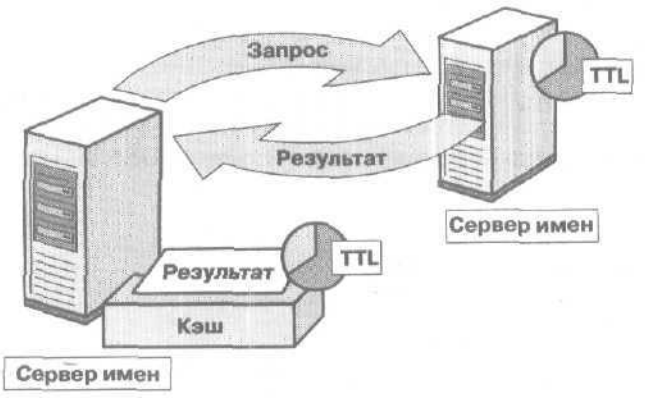


Рис. 5-2. Кэширование результатов запросов

Вот какие операции выполняет сервер DNS, когда получает результат запроса.

1. Сервер кэширует результат на определенное время, называемое *временем жизни* (Time to Live, TTL).

Примечание TTL задается в той зоне, из которой возвращается результат запроса. Значение по умолчанию — 60 минут.

---

2. Сразу после кэширования результата запроса начинается обратный отсчет TTL с его начального значения.
3. Когда время жизни истекает, сервер удаляет результат запроса из кэша.

Кэширование результатов запросов позволяет быстро разрешать запросы, адресованные в одну область пространства имен.

Примечание Малые значения TTL обеспечивают большую достоверность данных. При этом, однако, увеличивается нагрузка на сервер DNS. Большие значения TTL сокращают время, необходимое для разрешения запроса. Однако при изменениях в сети клиент не получит обновленную информацию до истечения TTL.

Обратный запрос

Запрос обратного поиска находит имя по IP-адресу. Такие утилиты, как NSLOOKUP, используют запросы обратного поиска для определения имен узлов. Кроме того, в некоторых приложениях обеспечение безопасности основано на проверке имен, а не IP-адресов.

Так как распределенная база данных DNS индексирована по имени, а не по IP-адресу, обратный поиск может потребовать длительного просмотра имен во всем домене. Для решения этой проблемы создан специальный домен второго уровня in-addr.arpa.

Домен in-addr.arps основан на той же иерархической системе имен, что и остальные области DNS; однако он базируется на IP-адресах, а не именах:

- имена поддоменов соответствуют IP-адресам в десятично-точечной нотации;
- октеты IP-адреса записываются в обратном порядке;
- владельцы доменов администрируют поддомены in-addr.arpa в соответствии с их IP-адресами и масками подсетей.

Например, на рис. 5-3 показано представление адреса 169.254.16.200 в домене in-addr.arpa. Компания, которой назначены IP-адреса в диапазоне от 169.254.16.0 до 169.254.16.255 с маской 255.255.255.0, получит полномочия в домене 16.254.169.in-addr.arpa.

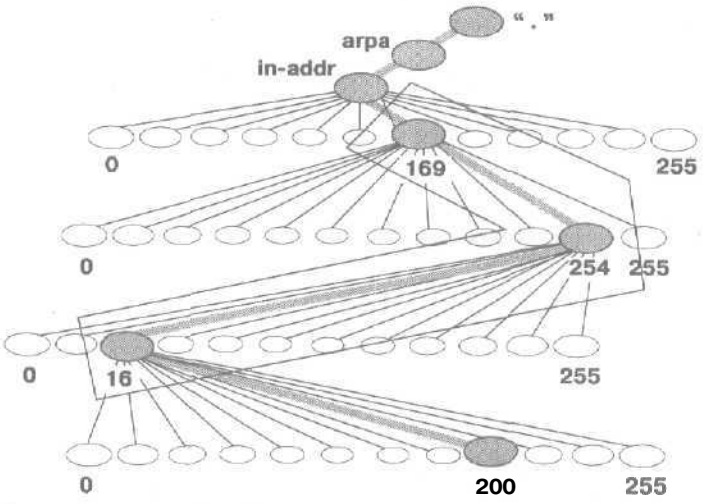


Рис. 5-3. Домен in-addr.arpa

Резюме

Разрешением имен называется процесс определения IP-адреса по имени, связь имен и адресов хранится в распределенной базе данных DNS. Мы рассказали, что серверы DNS разрешают запросы прямого поиска и что происходит, когда клиент запрашивает у сервера DNS IP-адрес. Вы также узнали, что серверы DNS кэшируют результаты запросов для снижения нагрузки на сеть.

Кроме запросов прямого поиска, серверы DNS разрешают также запросы обратного поиска. Такие запросы находят имя узла по IP-адресу. Так как распределенная база данных DNS индексирована по именам, а не по адресам, создан специальный домен второго уровня in-addr.arpa. Домен построен по тому же принципу, что и вся система DNS; однако, он базируется на IP-адресах, а не на именах.

Занятие 2, Зоны

Пространство имен DNS разделено на зоны, каждая из которых хранит информацию об одном или нескольких доменах. Зона является полномочным источником информации об имени каждого включенного в нее домена. На этом занятии вы познакомитесь с зонами DNS и с их конфигурацией.

Изучив материал этого занятия, вы сможете:

- определять тип зоны;
- перечислить преимущества зон, интегрированных с Active Directory;
- пояснить процесс делегирования зоны;
- конфигурировать зоны;
- конфигурировать динамическое обновление для зоны.

Продолжительность занятия — около 30 минут.

Служба DNS предусматривает возможность разделения пространства имен на одну или более зон, которые могут храниться, распределяться и реплицироваться на разных серверах DNS. Пространство имен домена представляет логическую структуру ресурсов сети, в то время как зона является физическим хранилищем этих ресурсов.

Планирование зоны

Принимая решение, надо ли разделять пространство имен домена на несколько зон, учитывайте следующие соображения:

- нужно ли передавать управление частью пространства имен в другое место или в другой отдел организации;
- есть ли необходимость разделять одну большую зону на несколько малых для распределения нагрузки между серверами, увеличения скорости разрешения имен или создания отказоустойчивой среды;
- потребуется ли создавать поддомены в будущем, например в случае открытия нового отделения.

Если ответ на один из этих вопросов положительный, возможно, имеет смысл разделить пространство имен домена на несколько зон. Решая вопрос о структуре зон, ориентируйтесь на нужды своей организации. Существует два типа зон: прямого и обратного просмотра.

Зона прямого просмотра

Позволяет выполнять запросы прямого поиска. Для работы службы DNS надо сконфигурировать минимум одну зону прямого просмотра на сервере DNS. Если вы устанавливаете Active Directory с помощью мастера и позволяете мастеру самому установить и настроить сервер DNS, он автоматически создаст зону прямого поиска, используя имя, которое вы указали для сервера.

▶ **Создание новой зоны прямого просмотра**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните DNS.
2. Раскройте узел сервера DNS.

3. Щелкните правой кнопкой папку Forward Lookup Zone (Зоны прямого просмотра) и выберите команду New Zone (Создать новую зону). Мастер проведет вас через процесс создания зоны прямого просмотра и поможет настроить следующие параметры: Zone Type (Тип зоны), Zone Name (Имя зоны), Zone File (Файл зоны) и Master DNS Servers (Главные серверы DNS).

Тип зоны

Вы можете выбрать один из трех типов зоны.

- **Интегрированная в Active Directory.** Зона, интегрированная в Active Directory, является главной копией новой зоны. Для хранения и репликации файлов зоны используется механизм Active Directory.
- **Основная.** Это также главная копия файла зоны, но хранится она в стандартном текстовом файле. Основную зону администрируют на том компьютере, где она была создана.
- **Дополнительная.** Является копией существующей зоны. Дополнительные зоны доступны только для чтения и хранятся в обычных текстовых файлах. Перед созданием дополнительной зоны нужно сначала сконфигурировать основную. При создании дополнительной зоны следует указать сервер DNS, выполняющий роль главного сервера, который будет передавать информацию о зоне на сервер, содержащий вспомогательную зону. Дополнительная зона создается для обеспечения избыточности и для снижения нагрузки на основной сервер.

Преимущества **зоны, встроенной в Active Directory**

Для сетей, где DNS используется совместно с Active Directory, встроенные основные зоны настоятельно рекомендуются по нескольким причинам.

- Обновление данных с нескольких серверов и обеспечение безопасности основаны на механизмах Active Directory.

  Для стандартной зоны процесс обновления информации DNS основан на модели одного главного сервера. В этой модели единственный полномочный сервер DNS представляет собой основной источник информации для зоны. Сервер поддерживает главную копию зоны в своем локальном файле. В этой модели уязвимым местом является основной сервер. Если он недоступен, запросы от клиентов на получение обновленной информации не выполняются.

  Если же хранение файлов интегрировано в Active Directory, изменения в DNS обрабатываются на основе модели с несколькими главными серверами. В этой модели любой полномочный сервер DNS (например, контроллер домена с поддержкой DNS) является основным источником информации для зоны. Так как главная копия зоны поддерживается в базе данных Active Directory, которая целиком реплицируется на все контроллеры домена, служба DNS способна обновлять зону на любом контроллере. В модели обновления с несколькими хозяевами любой основной сервер для интегрированной зоны способен обрабатывать запросы клиентов DNS по обновлению зоны, пока контроллер домена доступен в сети.

  При использовании интегрированной зоны вы можете также редактировать *список управления доступом* (access control list, ACL) для более тонкой настройки доступа к зоне или к отдельной записи ресурса в зоне. Например, на ACL для какого-либо домена в зоне могут быть наложены ограничения, разрешающие выполнять динамические изменения только указанным клиентам или позволяющие изменять зону или ее отдельные записи лишь отдельной группе, например администраторам домена. Эти возможности обеспечения безопасности недоступны для стандартных основных зон.

- Зоны автоматически копируются и синхронизируются, когда новая зона добавляется в домен Active Directory.

  Хотя службу DNS разрешается выборочно удалить из контроллера домена, интегрированные с Active Directory зоны всегда хранятся на каждом контроллере, так что хранение и администрирование зон не требуют дополнительных ресурсов. Кроме того, методы синхронизации информации, применяемые в Active Directory, работают быстрее, чем обычные методы обновления зоны, для которых иногда требуется копировать зону целиком.
- Храня данные DNS в Active Directory, вы упрощаете планирование и администрирование как DNS, так и Active Directory.

  Когда пространства имен хранятся и копируются раздельно, возникают дополнительные сложности при планировании и проектировании сети, которые могут привести к ее росту. Интегрируя данные DNS и Active Directory, вы совмещаете управление хранением и копированием информации.
- Репликация данных в Active Directory быстрее и эффективнее, чем стандартная репликация DNS.

  Поскольку репликация Active Directory выполняется «по свойствам», передаются только существенные изменения. Это позволяет копировать меньшие объемы данных.

Имя зоны

Как правило, зона именуется по имени верхнего домена в иерархии — корневого домена зоны. Например, зона, в которую входят microsoft.com и sales.microsoft.com, имеет имя microsoft.com. Подробнее о наименовании зон — в главе 2.

Файл зоны

Для стандартной зоны прямого просмотра вы должны указать файл, где будет храниться база данных зоны. По умолчанию имя файла состоит из имени зоны с расширением .dns. Например, для зоны microsoft.com файл зоны называется MICROSOFT.COM.DNS.

При переносе зоны с другого сервера вы можете импортировать существующий файл зоны. В этом случае до создания новой зоны необходимо поместить существующий файл зоны в каталог *systemroot*\System\DNS на новом сервере, где *systemroot* — каталог установки Windows 2000, обычно C:\Winnt.

Главные серверы DNS

Для дополнительной зоны прямого просмотра необходимо указать сервер DNS, с которого будет копироваться зона. Вы должны указать IP-адреса одного или нескольких серверов DNS.

Зона обратного просмотра

Обеспечивает выполнение запросов обратного поиска. Создавать зону обратного просмотра не обязательно. Однако эти зоны требуются для работы некоторых утилит, например NSLOOKUP, а также для записи имени вместо адреса в файлы журнала.

► **Создание зоны обратного просмотра**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните DNS.
2. В дереве консоли раскройте узел сервера DNS.

3. Щелкните правой кнопкой Reverse Lookup Zone (Зона обратного просмотра) и выберите команду New Zone (Создать новую зону). Мастер проведет вас через процесс создания зоны обратного просмотра и поможет настроить следующие параметры: Zone Type (Тип зоны), Zone Name (Имя зоны), Zone File (Файл зоны) и Master DNS Servers (Главные серверы DNS).

Тип зоны

Выберите один из трех типов (интегрированная в Active Directory, основная или дополнительная), как описано выше.

Наименование зоны обратного просмотра

Для идентификации зоны обратного просмотра укажите адрес сети или имя зоны. Например, для IP-адреса 169.254.16.200 сетевой адрес будет 169.254. Все запросы обратного поиска о сети 169.254 разрешаются именно в этой зоне.

Файл зоны обратного просмотра

Для стандартной зоны обратного просмотра необходимо указать файл зоны. Сетевой адрес и маска подсети задают имя файла зоны по умолчанию. При этом октеты записываются в обратном порядке, и добавляется суффикс in-addr.arpa. Например, файл зоны обратного поиска для сети 169.254 называется 254.169.in-addr.arpa.dns.

При переносе зоны с другого сервера вы можете импортировать существующий файл зоны. Перед созданием зоны не забудьте поместить этот файл в папку systemroot\System32\DNS на новом сервере.

Главные серверы DNS

Для дополнительной зоны обратного просмотра необходимо указать сервер DNS, с которого вы собираетесь копировать зону. Вы должны указать IP-адреса одного или нескольких серверов DNS.

Записи ресурсов

Записями ресурсов называются записи в базе данных зоны, которые связывают имена с данными о ресурсах сети, например IP-адресом. Существует много типов записей ресурсов. При создании зоны служба DNS автоматически добавляет две записи: *начальную запись зоны* (Start of Authority, SOA) и *запись ресурса имени сервера* (Name Server, NS). В табл. 5-1 описаны эти, а также другие наиболее часто встречающиеся типы записей.

Табл. 5-1. Наиболее популярные типы записей ресурсов

Тип записи ресурса	Описание
Запись ресурса адреса узла (A)	Связывает имя узла с IP-адресом для зоны прямого просмотра
Запись ресурса указателя (PTR)	Указатель на другую часть пространства имен. В частности в зоне обратного просмотра описывает соответствие имен адресам
Запись ресурса с каноническим именем (CNAME)	Создает альтернативное имя. или псевдоним, для указанного имени узла, Псевдоним позволяет использовать несколько имен для ссылки на один адрес. Например, вы можете разместить Web-сервер www.microsoft.com и FTP-сервер ftp.microsoft.com на одном и том же компьютере

Табл. 5-1. Наиболее популярные типы записей ресурсов *(окончание)*

Тип записи ресурса	Описание
Запись ресурса информации узла (HINFO)	Описывает тип процессора и операционную систему узла. Используется для быстрого анализа ресурсов
Запись ресурса почтового сервера (MX)	Описывает типы почтовых серверов и порядок их применения
Запись ресурса имени сервера (NS)	Перечисляет серверы DNS в домене
Запись ресурса размещения службы (SRV)	Определяет серверы, поддерживающие конкретную службу. Например, если клиент хочет найти сервер, проверяющий регистрацию в сети, он может послать запрос серверу DNS, чтобы получить список контроллеров домена и их адреса
Начальная запись зоны (SOA)	Определяет, какой сервер DNS является полномочным источником информации для этого домена. Первая запись в файле зоны должна быть записью SOA

Примечание Подробнее о записях ресурсов — в RFC 1035, RFC 1183, RFC 1886 и RFC 2052.

▶ **Просмотр записи ресурса**

1. В дереве консоли щелкните зону, для которой вы хотите посмотреть запись ресурса.
2. На правой панели щелкните запись, которую вы хотите посмотреть.
3. В меню Action (Действие) выберите команду Properties (Свойства).
4. В диалоговом окне свойств посмотрите свойства выбранной записи.
5. По завершении просмотра щелкните OK.

▶ **Добавление записи ресурса**

- Щелкните правой кнопкой зону, к которой вы хотите добавить запись, затем выберите тип записи, которую хотите добавить, например New Host (Создать узел) или New Mail Exchanger (Создать почтовый обменник).

Делегирование зоны

Формирование зоны начинается с единственной записи, содержащей имя корневого домена. Другие домены, добавляемые в базу данных, могут принадлежать к той же зоне или представлять собой часть другой зоны. После добавления поддомена разрешается:

- включить в оригинальную зону как ее часть;
- делегировать другой зоне, созданной для поддержки поддомена.

На рис. 5-4 показан домен microsoft.com, который содержит имена поддоменов домена microsoft. При создании на отдельном сервере домен microsoft был сконфигурирован как единая зона для всех имен microsoft. Если, однако, в домене microsoft.com вы собираетесь создавать поддомены, их надо включить в эту зону или делегировать в другую зону. На рис. 5-4 показано добавление поддомена example к домену microsoft.com. При этом создается зона example.microsoft.com для поддержки поддомена example.microsoft.com,

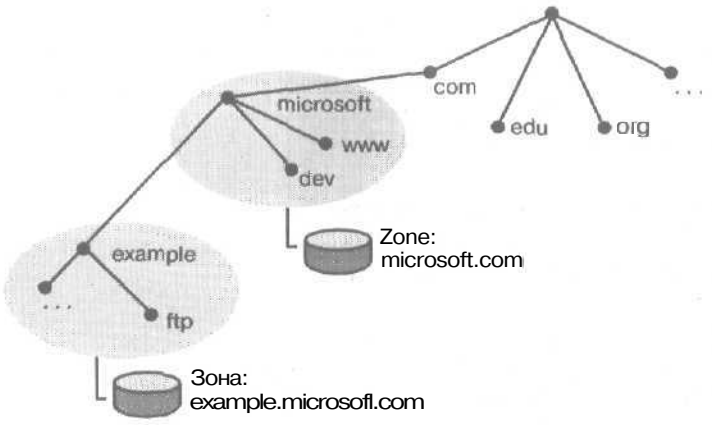


Рис. 5-4. Добавление поддомена в новую зону

При делегировании зоны вы должны также создать запись SOA, указывающую полномочный сервер DNS для новой зоны. Это необходимо для передачи полномочий и для обеспечения корректных ссылок на серверы DNS новой зоны. Делегировать зону вам поможет мастер.

▶ **Делегирование зоны**

1. В дереве консоли DNS щелкните поддомен, для которого вы хотите делегировать зону.
2. В меню Action выберите команду New Delegation (Создать делегирование).
3. В окне мастера щелкните Next.
4. В окне Delegated Domain Name (Имя делегируемого домена) укажите имя создаваемого домена и щелкните Next.
5. В окне Name Servers (Серверы имен) укажите серверы DNS, где будет находиться делегируемая зона, затем щелкните Next.
6. Проверьте параметры в окне сводной информации мастера, затем щелкните Finish (Готово).

Примечание **Все** домены и поддомены, возникающие в процессе делегирования зоны, надо создать в родительской зоне, причем до начала делегирования.

Конфигурирование Dynamic DNS

Служба DNS, поддерживающая динамическое обновление, называется Dynamic DNS (DDNS). В случае стандартной DNS после изменений в домене, где сервер имеет полномочия, необходимо вручную вносить изменения на основном сервере зоны. При наличии DDNS серверы и клиенты сети автоматически обновляют файлы зоны (рис. 5-5).

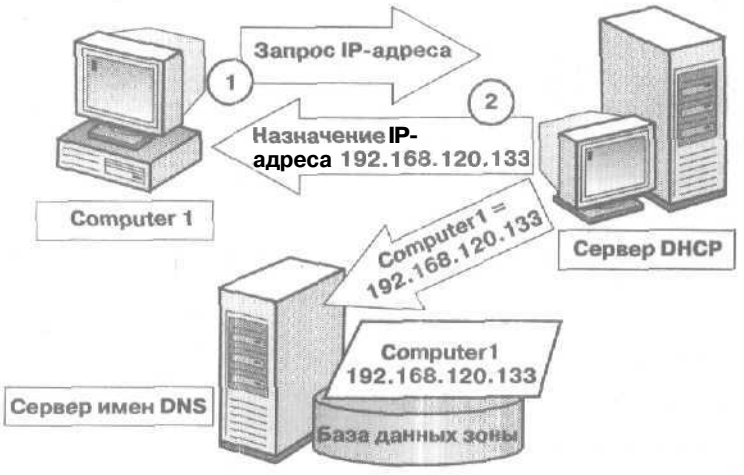


Рис. 5-5. DDNS обновляет базу данных зоны после изменения IP-адресов

Динамическое обновление

Чтобы инициировать динамическое обновление, надо задать список полномочных серверов. В нем необходимо указать дополнительные серверы, контроллеры доменов и прочие серверы, выполняющие регистрацию клиентов (например, серверы DHCP и серверы WINS).

Службы DDNS и DHCP взаимодействуют, дабы синхронизировать соответствие между именем и адресом для узлов сети. По умолчанию служба DHCP позволяет клиентам добавлять их собственные записи ресурса адреса узла (A) к зоне, после чего DHCP добавляет соответствующую запись ресурса указателя (PTR) к зоне. Служба DHCP очищает записи ресурсов A и PTR по истечении срока аренды адреса.

Внимание! Для поддержки динамического обновления, необходимо указать в конфигурации сервера DHCP соответствующий сервер DNS. Настройка DHCP не рассматривается в этом курсе; подробнее об этом — в руководстве, посвященном сетевой инфраструктуре Windows 2000.

▶ **Настройка зоны для динамического обновления**

1. В консоли DNS щелкните правой кнопкой в зоне прямого или обратного просмотра, которую вы хотите сконфигурировать, и выберите команду Properties.
2. На вкладке General (Общие) в списке Allow Dynamic Updates (Динамическое обновление) выберите один из следующих вариантов;
   - No (Нет) — динамическое обновление для этой зоны не разрешается.
   - Yes (Да) — все запросы динамического обновления для этой зоны разрешаются.
   - Only Secure Updates (Только безопасные обновления) — разрешаются лишь те обновления, которые используют DNS, безопасную для этой зоны. Это предпочтительный вариант.

Вариант Only Secure Updates появляется, только если зона интегрирована в Active Directory. Если вы выберете этот вариант, разрешение на обновление зоны проверяется по протоколу безопасного обновления DNS.

Примечание Подробнее о DNS - в RFC 2136 и RFC 2137.

Практикум: конфигурирование зоны

В этом практикуме вы попробуете сконфигурировать зоны. Сначала вы создадите зоны прямого и обратного просмотра, затем вы сконфигурируете эти зоны и, наконец, добавите запись ресурса PTR в зону обратного просмотра.

► Задание 1: создайте зону прямого просмотра

1. Раскройте меню Start\Programs\Administrative Tools, затем щелкните DNS.
   Откроется окно консоли DNS.
2. Дважды щелкните SERVER1 (или имя вашего компьютера).
   В окне отобразятся папки Forward Lookup Zones и Reverse Lookup Zones.
3. Щелкните правой кнопкой SERVER1 и выберите команду New Zone (Создать новую зону).
   Откроется окно мастера создания зоны.
4. Щелкните Next.
   Откроется окно выбора типа зоны.
5. Убедитесь, что выбран параметр Standard Primary (Основная), и щелкните Next.
   Откроется окно выбора типа просмотра.
6. Убедитесь, что выбрано Forward Lookup Zone (Зона прямого просмотра) и щелкните Next.
   Откроется окно задания имени зоны.
7. Наберите training.microsoft.com и щелкните Next. (Если вы в сети, спросите сетевого администратора, можно ли использовать такое имя домена.)
   Откроется окно создания файла зоны.
8. Убедитесь, что выбран параметр Create A New File With This File Name (Создать новый файл) и что имя создаваемого файла TRAINING.MICROSOFT.COM.DNS. (Если в пункте 7 вы указали другое имя домена, будет предложено это имя с расширением .dns.)
9. Щелкните Next.
   Откроется финальное окно мастера создания зоны.
10. Щелкните Finish (Готово).

► Задание 2: создайте зону обратного просмотра

1. Дважды щелкните на SERVER1, затем — New Zone.
   Откроется окно мастера создания зоны.
2. Щелкните Next.
   Откроется окно задания типа зоны.
3. Убедитесь, что выбран параметр Standard Primary, и щелкните Next.
   Откроется окно выбора типа поиска.
4. Убедитесь, что выбрано Reverse Lookup Zone (Зона обратного просмотра), и щелкните Next.
   Откроется окно задания имени зоны.
5. Убедитесь, что выбрано Network ID, и наберите **10.10.1** в поле Network ID (Код сети). (Если вы в сети и не используете статический IP-адрес 10.10.1.1, наберите октеты вашей подсети.)

Примечание Заметьте, что в поле имени в нижней части экрана автоматически добавляется in-addr.arpa, и имя зоны теперь — 1.10.10.in-addr.arpa. Если в предыдущем пункте вы указали другой сетевой адрес, имя зоны будет соответствовать ему.

---

6. Щелкните Next.
   Откроется окно создания файла зоны.
7. Убедитесь, что выбран вариант Create A New File With This File Name (Создать новый файл) и что имя создаваемого файла 10.10.1.in-addr.arpa.dns. (Если в п. 5 вы указали другой сетевой адрес, будет предложен этот адрес с расширением in-addr.arpa.dns.)
8. Щелкните Next.
   Откроется окно завершения создания зоны.
9. Проверьте информацию в окне и щелкните Finish (Готово).

▶ **Задание 3: настройте DDNS**

1. В консоли DNS дважды щелкните SERVER] (или имя вашего сервера).
2. Дважды щелкните Forward Lookup Zones (Зоны прямого поиска) и затем дважды – training.microsoft.com (или имя вашего тестового домена, созданного ранее),
3. Щелкните правой кнопкой training.microsoft.com (или имя тестового домена), затем щелкните Properties (Свойства).
   Откроется диалоговое окно свойств зоны.
4. На вкладке General (Общие) в списке Allow Dynamic Updates выберите Yes (Да) и щелкните OK.
   Это задает динамическое обновление для зоны прямого просмотра.
5. Дважды щелкните Reverse Lookup Zones, затем — папку 10.10.1.x Subnet или имя тестовой зоны, созданной ранее.
6. Щелкните правой кнопкой 10.10.1.x (или папку вашей зоны) и выберите команду Properties.
   Откроется диалоговое окно свойств зоны.
7. На вкладке General (Общие) в списке Allow Dynamic Updates выберите Yes (Да) и щелкните OK.

▶ **Задание 4: добавьте запись ресурса**

1. В консоли DNS щелкните Reverse Lookup Zones.
2. Щелкните имя ранее созданной тестовой зоны.
   Какие записи ресурсов уже существуют в зоне?
3. Щелкните правой кнопкой имя тестовой зоны, затем щелкните New Pointer (Создать указатель).
4. В поле Host IP Number (IP-номер узла) введите 1 в выделенном октете вашего IP-адреса.
   В поле Host Name (Имя узла) введите полное доменное имя вашего компьютера, заканчивающееся точкой. Вы можете просмотреть существующие записи, щелкнув кнопку Browse (Обзор). Например, если имя вашего компьютера SERVER1, надо ввести **server1.microsoft.com.** (не забудьте в конце поставить точку).
5. Щелкните OK.
   На правой панели добавится новая запись PTR.
6. Закройте консоль DNS.

Резюме

Служба DNS позволяет разделять пространства имен на зоны, которые могут храниться и копироваться на разных серверах. Пространство имен DNS представляет логическую структуру вашего домена, а зоны DNS обеспечивают физическое распределение ресурсов.

Мы рассказали, как конфигурировать зоны прямого и обратного просмотра, и описали преимущества зон, интегрированных в Active Directory; обновление из нескольких источников, повышение безопасности, автоматическая быстрая репликация при добавлении новых контроллеров или внесении иных изменений, упрощение администрирования.

Вы узнали, как добавлять записи ресурсов и делегировать зоны при добавлении поддоменов, а также что служба DNS поддерживает динамическое обновление, позволяя серверам и клиентам сети автоматически обновлять файлы зоны,

Выполняя практические задания, вы создали зоны прямого и обратного поиска, сконфигурировали зоны для динамического обновления и добавили запись ресурса PTR в зону обратного просмотра.

Занятие 3. Репликация и передача зон

В этом занятии объясняются понятия репликации и зонной передачи (взаимодействие серверов DNS для синхронизации данных).

Изучив материал этого занятия, вы сможете:

- пояснить цель зонной передачи;
- настроить зонную передачу.

Продолжительность занятия — около 10 минут.

Зоны играют важную роль в DNS, поэтому желательно, чтобы они были доступны более чем с одного сервера DNS. Это важно с точки зрения отказоустойчивости, так как, если сервер недоступен, запросы на разрешение имен выполняться не будут. При наличии в зоне нескольких серверов необходимо синхронизировать все копии зоны на каждом сервере DNS, что и выполняется в ходе зонной передачи.

Зоны с дополнительными серверами имеют следующие преимущества:

- дополнительные серверы обеспечивают избыточность данных, разрешая запросы даже в случае отказа основного сервера;
- дополнительные серверы могут снизить нагрузку на сеть; добавление сервера DNS на другом конце медленной сети упрощает администрирование и снижает трафик в сети;
- дополнительные серверы снизят нагрузку на основной сервер.

Сразу после добавления в зону нового дополнительного сервера выполняется *полная зонная передача* (Full Zone Transfer, AXFR) для создания на нем полной копии всех записей ресурсов. В ранних реализациях сервера DNS полная зонная передача выполнялась всегда, когда требовалось обновить зону после внесении изменений на основном сервере. Служба DNS для Windows 2000 Server поддерживает *добавочную зонную передачу* (Incremental Zone Transfer, **IXFR),** когда передаются только внесенные изменения.

Добавочная зонная передача

Дополнительный стандарт для передачи зоны IXFR описан в RFC 1995 и представляет собой наиболее эффективный метод синхронизации зоны.

В ранних реализациях DNS любой запрос на обновление данных зоны требовал полной зонной передачи. Для добавочной передачи требуется запрос IXFR. Он позволяет принимающим серверам выбирать только те записи, которые нужно синхронизировать с источником данных на другом сервере DNS.

При добавочной передаче в первую очередь определяются различия между источником и копией зоны. Если версии зон одинаковы, что определяется серийным номером в записи SOA каждой зоны, передача не выполняется.

Если серийный номер зоны источника больше, чем на дополнительном сервере, передаются только записи с большими серийными номерами. Для этого исходный сервер должен хранить историю последовательных изменений. Процесс добавочной передачи порождает гораздо меньший трафик в сети и выполняется быстрее.

Пример: зонная передача

Зонная передача инициируется вручную либо автоматически в следующих случаях:

- при запуске службы DNS на дополнительном сервере;
- по истечении периода обновления для зоны;

• после внесения изменений на основном сервере, если на нем задан список уведомлений.

Передача всегда инициируется сервером-получателем, который обращается к своему источнику данных. Это может быть основной или дополнительный сервер, сконфигурированный для него в качестве главного сервера. Когда сервер-источник получает загрос на обновление, он отвечает полной или добавочной передачей зоны.

На рис. 5-6 показан порядок передачи зоны между серверами. Он может варьироваться в зависимости от того, была ли зона скопирована ранее или же копируется впервые.

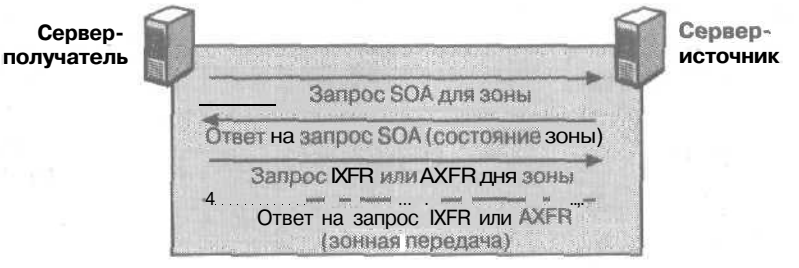


Рис. 5-6. Процесс зонной передачи

В этом примере запрос сервера-получателя к серверу-источнику выполняется в последовательности, описанной ниже.

1. По завершении новой конфигурации целевой сервер посылает запрос на полную передачу зоны серверу DNS, указанному в качестве источника данных.
2. Сервер-источник отвечает полной зонной передачей.

   Зона доставлена на запросивший сервер с серийным номером версии, установленной в записи SOA. Запись SOA содержит также интервал обновления (по умолчанию - 15 минут), показывающий, когда сервер должен обновить зону.
3. По истечении интервала обновления сервер требует обновления зоны, запрашивая информацию о записи SOA.
4. Сервер-источник отвечает на запрос.

   Ответ содержит текущий серийный номер на сервере-источнике.
5. Сервер-получатель сверяет полученный серийный номер и определяет, нужно ли обновлять зону.

   Если серийный номер в ответе равен локальному, значит, зоны совпадают и передача не требуется. В этом случае сервер-получатель обновляет зону, устанавливая новый интервал обновления, на основе указанного в ответе значения.

   Если серийный номер в ответе больше локального, значит, зона изменилась и необходимо выполнить передачу.
6. Если сервер-получатель обнаружил изменение зоны, он посылает запрос IXFR, содержащий серийный номер в своей записи SOA.
7. Сервер-источник отвечает полной или добавочной передачей зоны.

Если источник ведет историю изменений и поддерживает добавочную передачу для измененных записей, он отвечает добавочной передачей.

Если сервер не хранит историю изменений или не поддерживает добавочную передачу, он отвечает полной зонной передачей.

Примечание Windows 2000 Server поддерживает добавочную передачу зоны по стандарту IXFR. Ранние версии DNS в составе Windows NT Server 4.0, как и многие другие версии серверов DNS, не поддерживают добавочную зонную передачу и выполняют только полную передачу.

Безопасность при зонной передаче

В консоли DNS стоит указать серверы, которым разрешено участвовать в зонной передаче, Это поможет предотвратить запросы на обновление зоны от неавторизованных серверов.

► **Назначение серверов, способных участвовать в передачах зоны**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните DNS.
2. В дереве консоли DNS щелкните правой кнопкой зону, для которой нужно задать передачу зоны, затем щелкните Properties.
3. Выберите вкладку Zone Transfers (рис. 5-7).

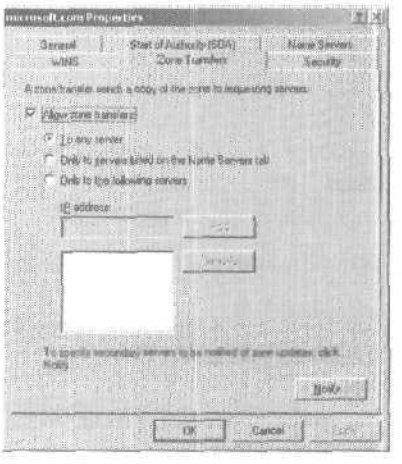


Рис. 5-7. Вкладка **Zone Transfers (Передачи зон)**

4. Укажите серверы, для которых нужно разрешить передачу зоны, и щелкните OK.

Уведомления DNS

Механизм извещения дополнительных серверов об изменениях зоны реализуется с помощью уведомлений DNS. Уведомляемые серверы могут затем инициировать процесс обновления зоны и получить изменения с уведомляющего сервера. Служба DNS поддерживает обновленный стандарт уведомлений DNS (RFC 1996).

Используйте уведомления DNS только для дополнительных серверов зоны. Для репликации зоны, интегрированной в Active Directory, они не требуются, так как серверы, встроенные в Active Directory, автоматически обновляют информацию о зоне примерно раз в 15 минут (в зависимости от значения в записи SOA). В таких случаях задание списка уведомлений может понизить скорость работы системы за счет ненужных запросов на зонную передачу.

► **Задание списка уведомляемых серверов**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните DNS.
2. В дереве консоли DNS щелкните правой кнопкой зону, для которой нужно установить передачу зоны, затем щелкните Properties.
3. На вкладке Zone Transfers щелкните кнопку Notify (Уведомить).
4. В диалоговом окне Notify (Уведомление) укажите дополнительные серверы, которые нужно уведомлять об изменениях зоны, затем щелкните OK.

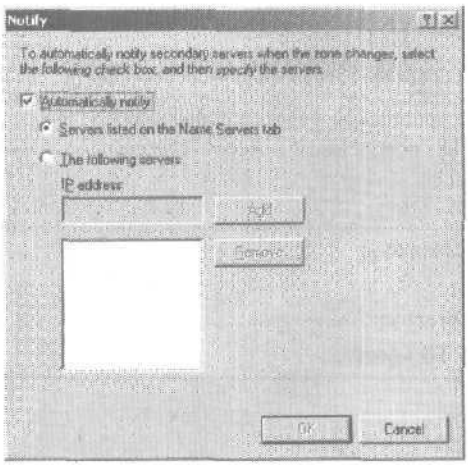


Рис. 5-8. Диалоговое окно Notify (Уведомление)

Процедура уведомления DNS

Уведомление выполняется в определенном порядке.

1. Зона на сервере DNS является источником данных для других серверов. При обновлении зоны обновляется серийный номер записи SOA.
2. Сервер-источник посылает уведомления всем серверам, перечисленным в перечне уведомлений.
3. Все дополнительные серверы, получившие уведомления, могут теперь инициировать передачу зоны с уведомляющего сервера. После этого происходит обычный процесс передачи зоны, описанный ранее.

Резюме

Для синхронизации данных на всех серверах зоны требуется зонная передача. В ранних версиях DNS, а также при добавлении нового дополнительного сервера DNS к сети выполняется полная передача зоны, при которой копируются все записи ресурсов зоны. Служба DNS для Windows 2000 Server поддерживает также более быструю добавочную зонную передачу, при которой передаются только последние изменения.

Разрешается задавать список серверов, авторизованных для передачи зоны, используя консоль DNS, а также о порядке уведомления дополнительных серверов об изменениях зоны. Это позволяет уведомляемым серверам инициировать процесс передачи зоны и лолучить изменения в данных зоны. В консоли DNS можно указывать вторичные серверы, которым нужно посылать уведомление; для репликации зон, встроенных в Active Directory, уведомления DNS не требуются.

Занятие 4. Мониторинг и устранение неполадок DNS для Active Directory

В этом занятии объясняются возможности наблюдения за работой сервера DNS. Здесь также описываются проблемы при настройке DNS, встроенной в Active Directory, и возможные решения этих проблем.

Изучив материал этого занятия, вы сможете:

- наблюдать работу сервера DNS;
- устранять неполадки DNS для Active Directory.

Продолжительность занятия — около 10 минут.

Наблюдение за сервером DNS

В Windows 2000 Server предусмотрены две способа контроля работы сервера DNS:

- запись событий по умолчанию в журнал сервера DNS;
- использование команд отладки для записи событий в текстовый файл.

Запись событий сервера DNS

При работе Windows 2000 Server сообщения о событиях сервера DNS хранятся в журнале (log-файле) сервера отдельно от файлов событий, связанных с другими приложениями. Этот журнал можно просмотреть из оснастки Event Viewer. В него записывается ограниченный набор событий, выявляемых службой DNS, таких, как запуск и остановка сервера.

Event Viewer также позволяет наблюдать за событиями DNS на компьютерах клиентов. Эти события заносятся в файл журнала на каждом компьютере с Windows 2000.

Примечание Подробнее об использовании Event Viewer — в главе 14.

Команды отладки

Консоль DNS позволяет задавать дополнительные параметры для создания временного текстового файла журнала. Этот файл — DNS.LOG — хранится в папке system_root\Systems32\Dns. Серверы DNS в Windows 2000 поддерживают отладочные команды, описанные ниже (табл. 5-2).

Табл. 5-2. Команды отладки серверов DNS

Команда	Назначение
Query	Записывать запросы, полученные от клиентов
Notify	Записывать уведомления, полученные от других серверов DNS
Update	Записывать изменения зоны, полученные от других компьютеров
Questions	**Записывать содержимое** раздела вопроса **для каждого запроса, обработанного сервером DNS**
Answers	Записывать содержимое раздела ответа для каждого запроса, обработанного сервером DNS
Send	Подсчитывать запросы, посланные сервером DNS

Табл. 5-2. Команды отладки серверов DNS (*окончание*)

Команда	Назначение
Received	Подсчитывать запросы, полученные сервером DNS
UDP	Подсчитывать запросы, полученные по протоколу UDP
TCP	Подсчитывать запросы, полученные по протоколу TCP
Full Packets	Подсчитывать полные пакеты, полученные и записанные сервером DNS
Write Through	Подсчитывать пакеты, прошедшие через сервер DNS туда и обратно

По умолчанию все эти дополнительные возможности отладки отключены. После активизации какой-либо из них служба DNS сможет контролировать дополнительные виды событий, что пригодится при отладке сервера.

Такой контроль требует много ресурсов (в некоторых случаях замедляется работа сервера и требуется дополнительное место на диске), поэтому его следует использовать к ратковременно, когда действительно нужна подробная информация о работе сервера.

► **Задание параметров отладки**

1. В консоли DNS щелкните правой кнопкой имя сервера, затем щелкните Properties.
2. На вкладке Logging задайте необходимые параметры отладки и щелкните OK.

Устранение неполадок DNS

В табл. 5-3 перечислены возможные неполадки DNS и способы их решения.

Табл. 5-3. Способы устранения неполадок DNS

Неполадки, связанные с зонной передачей

Причина	Решение
Приостановка службы DNS на сервере	Убедитесь, что все серверы, используемые в процессе передачи, доступны и службы DNS на них не приостановлены
Разрыв связи по сети между серверами DNS, используемыми в процессе зонной передачи	Используя команду PING, проверьте с двух сторон наличие сетевого канала между двумя серверами DNS. В случае неудачи одного из двух тестов ищите причину непосредственно в сети
Серийные номера зоны на *сервере-получателе* и сервере-источнике совпадают, что препятствует передаче	Используя консоль DNS, увеличьте серийный номер на вкладке SOA для *сервера-источника*, чтобы он превысил серийный номер сервера-получателя. После этого инициируйте передачу зоны на сервере-получателе
Возникают проблемы при взаимодействии сервера-источника и сервера-получателя	**Проверьте, не установлена** ли на **одном из** серверов старая **версия DNS,** например версия BIND
Зона содержит записи ресурсов и другие данные, которые сервер DNS не может правильно интерпретировать	Убедитесь, что зона не содержит несовместимых типов данных, например записей ресурсов неподдерживаемых типов, и ошибок. Также выясните, указана ли в конфигурации сервера приостановка загрузки некорректных данных, и определите метод проверки имен. Эти параметры задаются в консоли DNS

Табл. 5-3. Способы устранения неполадок DNS *(окончание)*

Неполадки, связанные с зонной передачей

Причина	Решение
Данные полномочной зоны некорректны	Если при передаче зоны постоянно происходят ошибки, убедитесь, что зона не содержит нестандартных данных. Чтобы определить вероятный источник ошибок, просмотрите сообщения в журнале сервера DNS

Прерывание делегирования зоны

Причина	**Решение**
Делегирование **зоны неправильно сконфигурировано**	Проверьте параметры делегирования зоны и исправьте конфигурацию, если это необходимо

Табл. 5-4. Способы устранения неполадок динамического обновления

Клиент не выполняет динамическое обновление

Причина	**Решение**
Клиент (или его сервер DHCP) не поддерживает протокол динамического обновления DNS	Убедитесь, что ваши клиенты поддерживают протокол динамического обновления и включены опции динамической поддержки в Windows 2000. Чтобы зарегистрировать компьютеры клиентов для динамического обновления, установите на них Windows 2000 либо установите в сети сервер DHCP для обслуживания клиентов
Клиент не смог зарегистрироваться на сервере DNS для динамического обновления из-за неполной конфигурации DNS	Убедитесь, что клиент правильно сконфигурирован, и при необходимости обновите конфигурацию. Для обновления конфигурации клиентов задайте первичный суффикс DNS на компьютере клиента с постоянным IP-адресом или задайте зависящий от соединения суффикс DNS на одном из сетевых подключений клиента
Клиент DNS не смог обновить информацию с сервера DNS из-за проблем на сервере	Если клиент может обращаться к своему основному и альтернативным серверам DNS, указанным в его конфигурации, значит, дело не в компьютере клиента. На клиентах под управлением Windows 2000 используйте Event Viewer для просмотра системного log-файла и определения причин неудач при обновлениях записей ресурсов узлов (A) и указателей (PTR)
Сервер DNS не поддерживает динамические **обновления**	Убедитесь, что сервер DNS, к которому обращается клиент, способен поддерживать протокол динамического обновления, описанный в RFC 2136. Так, серверы DNS на базе Windows NT 4.0, в отличие от серверов Windows 2000, не поддерживают динамическое обновление

Табл. 5-4. Способы устранения неполадок динамического обновления *(окончание)*

Клиент не выполняет динамическое обновление

Причина	Решение
Сервер DNS способен поддерживать динамическое обновление, но не делает этого	Убедитесь, что основная зона, откуда клиенты получают изменения, настроена на их поддержку. По умолчанию, сервер DNS с Windows 2000 для основной зоны не поддерживает динамические обновления. Отредактируйте свойства зоны на основном сервере DNS, если это необходимо
База данных зоны не доступна	Убедитесь, что зона существует и доступна для изменений. Для основных серверов DNS убедитесь, что файл зоны на сервере существует и зона не приостановлена. Дополнительные серверы не поддерживают динамическое обновление. Определите основной сервер зоны, способный их поддерживать, по данным записей ресурсов SOA и NS. Для зоны, интегрированной в Active Directory, убедитесь, что сервер DNS является контроллером домена и имеет доступ к базе данных Active Directory, где хранится файл зоны

Резюме

На этом занятии мы рассказали об управлении серверами DNS, а также о том, какие проблемы могут возникнуть при конфигурации зоны и о путях их решения.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении А «Вопросы и ответы» в конце книги.

1. С какой целью применяются запросы прямого поиска? Запросы обратного поиска?

2. Каковы преимущества использования зоны, встроенной в Active Directory?

3. Для чего нужна запись ресурса SOA?

4. Что нужно сделать для делегирования зоны?

5. Почему добавочная зонная передача эффективнее полной?

ГЛАВА 6

Настройка сайтов

В этой главе

Настройка сайтов влияет в Microsoft Windows 2000 на:

- регистрацию и аутентификацию рабочей станции;
- репликацию каталогов.

Примечание Конфигурация сайта также влияет на любые приложения, использующие возможности Active Directory, например Exchange 2000 или службы Personalization and Membership компонента Site Server.

Эта глава посвящена настройке параметров сайта и межсайтовой репликации. Кроме того, здесь рассказывается об устранении неполадок межсайтовой репликацией, а также обсуждается настройка параметров сервера.

Прежде всего

Для изучения материалов этой главы необходимо:

- настроить компьютеры в соответствии с инструкциями раздела «Об этой книге»;
- установить службу каталогов Active Directory, выполнив упражнения главы 4;
- иметь опыт работы с консолью управления (MMC).

Занятие 1. Настройка параметров сайта

Сейчас вы узнаете о настройке параметров сайта, в том числе о создании сайта, сопоставлении подсети сайту, подсоединении сайта с помощью связей и о выборе сервера лицензий сайта.

Изучив материал этого занятия, вы сможете:

- ✓ настроить параметры сайта,

Продолжительность занятия — около 20 минут.

Сайт

Сайт — это совокупность контроллеров домена, входящих в состав сети, объединенной высокоскоростными недорогими каналами связи. Контроллеры домена одного сайта выполняют репликацию на основе уведомлений: если на контроллере имеются какие-либо изменения, он уведомляет своих партнеров по репликации. Партнер, получивший уведомление, запрашивает изменения, после чего происходит репликация. Поскольку цена и скорость репликации внутри сайта особого значения не оказывают, репликация осуществляется по запросу, а не по расписанию. Репликация между сайтами происходит по расписанию; для выбора наиболее благоприятного времени репликации можно создать расписание, учтя объем сетевого трафика репликации и затраты на его передачу. Сайт — это эквивалент набору из одной или нескольких IP-подсетей.

При установке службы каталогов Active Directory на первом контроллере домена сайта в контейнере Sites создается объект с именем Default-First-Site-Name. В этом сайте необходимо установить первый контроллер домена. Дополнительные контроллеры устанавливаются в сайте первого контроллера домена (предполагается, что IP-адрес жестко связан с сайтом) или в другом существующем сайте. После установки первого контроллера домена имя Default-First-Site-Name можно изменить на любое другое.

Если вы устанавливаете Active Directory на дополнительные серверы, а в хранилище Active Directory определены дополнительные сайты и IP-адрес устанавливаемого компьютера соответствует имеющейся в существующем сайте подсети, контроллер добавляется в этот сайт. Иначе контроллер добавляется в сайт исходного контроллера домена.

▶ **Создание нового сайта**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Active Directory Sites And Services (Active Directory — сайты и службы).
2. Щелкните папку Sites правой кнопкой и выберите в контекстном меню команду New Site (Новый сайт).
3. В диалоговом окне New Object — Site (Новый объект — Сайт) введите в поле Name (Имя) имя нового сайта (рис. 6-1). Выберите объект связи сайтов и щелкните OK.

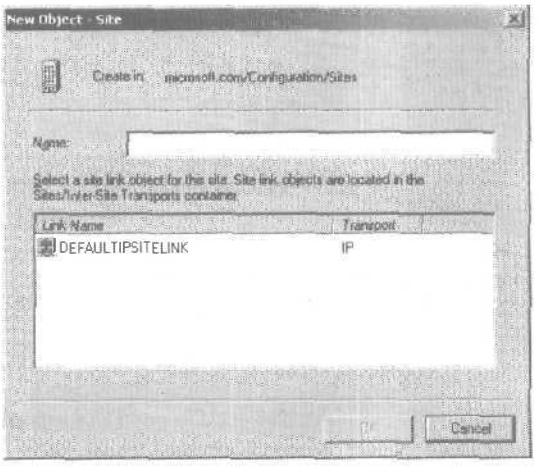


Рис. 6-1. Диалоговое окно New Object — Site

4. В окне сообщения щелкните OK.

► **Переименование сайта**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. Щелкните папку Sites.
3. Щелкните сайт правой кнопкой и выберите в контекстном меню команду Rename (Переименовать).
4. Введите новое имя сайта и щелкните в свободной части дерева консоли.

Подсети

Компьютеры сетей TCP/IP присоединяются к сайтам согласно их принадлежности к подсети или к набору подсетей. Подсеть объединяет компьютеры способом, который подчеркивает их географическую близость в сети. Сведения о подсети используются для поиска контроллера домена в том же сайте, к которому относится компьютер, аутентифицируемый в процессе регистрации. Кроме того, эти сведения позволяют определить оптимальный маршрут между контроллерами домена для репликации Active Directory,

► **Создание подсети**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. Дважды щелкните папку Sites.
3. Щелкните папку Subnets правой кнопкой и выберите в контекстном меню команду New Subnet (Создание подсети).
4. В диалоговом окне New Object — Subnet (Новый объект — Подсеть), введите в поле Address (Адрес) адрес подсети (рис. 6-2). В поле Mask (Маска) задайте маску подсети, описывающую диапазон адресов, относящихся к подсети данного сайта. Выберите сайт, которому будет сопоставлена подсеть, и щелкните OK.

Рис. 6-2. Диалоговое окно New Object — Subnet

► **Сопоставление существующей подсети сайту**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. Откройте папку Subnets, щелкните подсеть правой кнопкой и выберите команду Properties (Свойства).
3. В диалоговом окне свойств полсети (рис. 6-3) выберите в списке Site (Сайт) сайт, которому будет сопоставлена подсеть, и щелкните OK.

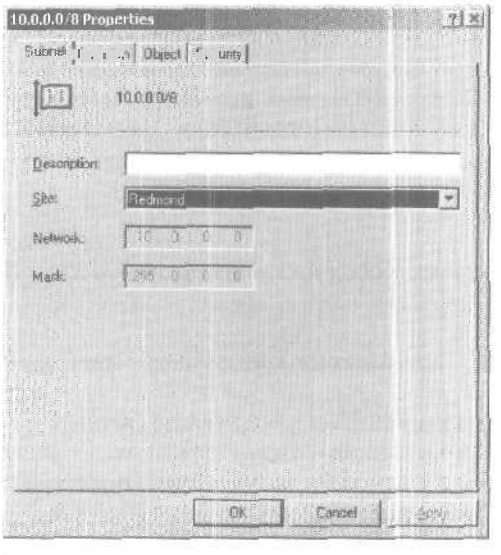


Рис. 6-3. Диалоговое окно свойств подсети

Связи сайтов

Для репликации между двумя сайтами необходимо создать между ними связь. Она не генерируется автоматически, и вам придется налаживать ее вручную, с помощью консоли Active Directory Sites and Services. При отсутствии линии связи между сайтами подключение двух компьютеров невозможно, а значит, и репликацию вам настроить не удастся. Каждая связь включает расписание, определяющее периодичность репликации между подключенными сайтами. Консоль Active Directory Sites and Services гарантирует, что каждый сайт добавлен как минимум в одну связь. Связать можно два и более сайтов; в этом случае все сайты должны принадлежать в одинаковой мере хорошо соединенным сетям.

При установке Active Directory на первый контроллер домена сайта мастер установки автоматически создает в контейнере IP объект с именем DEFAULTIPSITELINK. Для первого узла по умолчанию, создаваемого мастером, необходимо настроить данную связь. После установки первого контроллера домена имя DEFAULTIPSITELINK можно изменить на любое другое.

Протоколы репликации

Обмен данными из каталога производится с помощью разных сетевых протоколов, таких, как IP или SMTP:

- **IP-репликация.** Использует *удаленный вызов процедур* (remote procedure call, RPC) для репликации через связи сайтов (межсайтовой) и внутри сайта (внутрисайтовой). По умолчанию межсайтовая IP-репликация выполняется по соответствующему расписанию, впрочем можно настроить репликацию Active Directory, чтобы игнорировать расписания. Для IP-репликации не требуется центр сертификации.
- SMTP-репликация. Производится только через связи сайтов (межсайтовая), но не в пределах сайта. Так как протокол SMTP — асинхронный, обычно все расписания им игнорируются. Необходимо установить и настроить *центр сертификации* (certification authority, CA) предприятия для использования SMTP-связей сайтов. Центр сертификации (ЦС) подписывает сообщения SMTP, которыми обмениваются контроллеры домена для подтверждения подлинности обновлений каталога. Установка и настройка ЦС здесь не обсуждаются; подробнее об этом — в учебном курсе «Администрирование сети на основе Microsoft Windows 2000» (Русская Редакция, 2001).

▶ **Создание связи сайтов**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. Раскройте папку Inter-Site Transports и щелкните правой кнопкой папку IP или папку SMTP, в зависимости от того, какой протокол вы собираетесь использовать, затем выберите команду New Site Link (Новая связь сайтов).

Внимание! Для создания связи сайтов на основе протокола SMTP в сети должен быть доступен ЦС предприятия и протокол SMTP должен быть установлен на всех контроллерах домена, которые будут использовать данную связь сайтов.

---

3. В диалоговом окне New Object — Site Link (Новый объект — связь сайтов) в поле Name (Имя) введите имя связи сайтов (рис, 6-4).

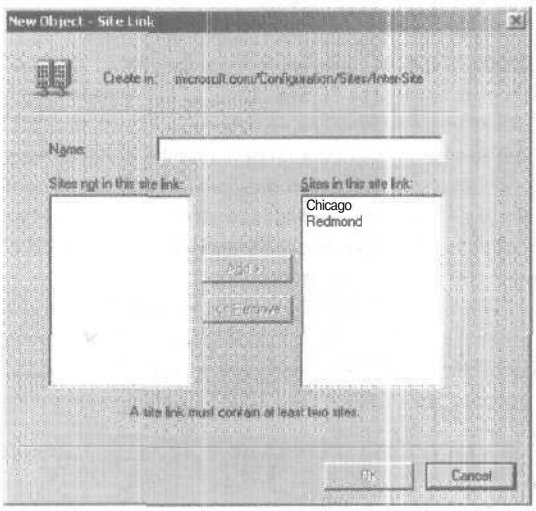


Рис. 6-4. Диалоговое окно New **Object — Site Link**

4. Выберите два или более соединяемых узлов и щелкните кнопку Add (Добавить).
5. Щелкните OK.

► **Добавление сайта к существующей связи сайтов**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. Раскройте папку Inter-Site Transports, затем папку IP или папку SMTP, щелкните правой кнопкой связь, к которой будет добавлен сайт, и выберите команду Properties.
3. В диалоговом окне свойств связи сайтов перейдите на вкладку General (Общие), выберите в списке Sites In This Site Link (Сайты в этой связи сайтов) сайт, добавляемый к данной связи, и щелкните кнопку Add (Добавить).
4. Щелкните OK.

Лицензирование сайтов

Чтобы обеспечить соответствие ПО организации лицензионным соглашениям Microsoft BackOffice, администратор может наблюдать приобретение, удаление и использование лицензий. Информация о лицензировании собирается на сервере с помощью службы License Logging (Служба учета лицензий), доступной в Windows 2000 Server.

Служба License Logging каждого сервера сайта реплицирует информацию о лицензировании в центральную БД, которая размещается на сервере, называемом сервером лицензий сайта. Администратор сайта или администратор сервера лицензий сайта может средствами консоли Licensing (Лицензирование) из папки Administrative Tools просмотреть полную историю лицензирования сайта, хранящуюся на сервере лицензий.

Первый созданный в сайте контроллер домена по умолчанию становится сервером лицензирования. Впрочем, сервер лицензий сайта может и не быть контроллером домена. Для оптимальной производительности сервер лицензий сайта и контроллер домена должны находиться в одном сайте. В большой организации с несколькими сайтами сбор сведений о лицензировании осуществляется отдельно для каждого сайта соответствующим сервером лицензий.

▶ **Выбор сервера лицензий сайта**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. Щелкните сайт, для которого требуется назначить сервер лицензий.
3. В правой панели щелкните правой кнопкой License Site Settings и выберите в контекстном меню команду Properties.
4. В диалоговом окне Licensing Site Settings Properties (Свойства: Licensing Site Settings) щелкните в области Licensing Computer (Компьютер лицензирования) кнопку Change (Изменить).
5. В диалоговом окне Select Computer (Выбор: Компьютер) выберите компьютер-сервер лицензий сайта и щелкните OK.
6. В диалоговом окне Licensing Site Settings Properties щелкните OK.

▶ **Просмотр лицензий сайта**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Licensing (Лицензирование).
2. В меню License (Лицензия) выберите команду Select Domain (Выбрать домен), чтобы подключиться к серверу лицензий сайта для домена.
3. В диалоговом окне Select Domain (Выбор домена) введите в поле Domain (Домен) имя сервера лицензий сайта и затем щелкните OK.

Практикум: настройка сайта

Сейчас вы настроите сайт — создадите его, сопоставите ему подсеть, подсоедините его с помощью связи сайтов, а также выберете сервер лицензий сайта.

▶ **Задание 1: переименуйте сайт**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.

   Откроется окно консоли Active Directory Sites and Services.
2. Щелкните папку Sites.

   Какие объекты отображаются в правой панели?
3. Щелкните сайт Default-First-Site-Name правой кнопкой и выберите в контекстном меню команду Rename (Переименовать).
4. Введите новое имя сайта, **Redmond,** и щелкните в свободном месте дерева консоли.

   Сайт Default-First-Site-Name переименован в Redmond.

▶ **Задание 2: создайте новый сайт**

1. Щелкните папку Sites правой кнопкой и выберите в контекстном меню команду New Site (Новый сайт).
2. В поле Name (Имя) введите **Chicago.** Выберите для связи сайта Chicago сайт DEFAULTIPSITELINK и щелкните OK.

   Откроется окно сообщения Active Directory, напоминающее, что для завершении настройки сайта Chicago необходимо:
   - убедиться, что сайт соответствующим образом подключен к другим сайтам посредством связей;
   - добавить подсети сайта в контейнер Subnets;
   - установить в сайте один или более контроллеров домена или переместить в сайт существующие контроллеры;
   - выбрать сервер лицензий сайта.

▶ **Задание 3:** создайте **подсеть**

1. Дважды **щелкните папку Sites.**
2. **Щелкните папку Subnets правой кнопкой и выберите в контекстном меню команду** New Subnet **(Создание** подсети).
3. **В поле** Address (Адрес) введите адрес подсети — **10.10.1.1. В поле** Mask (Маска) введите маску подсети — **255.0.0.0. Эта маска** описывает **диапазон адресов,** включенных в **подсеть данного** сайта. **Выберите** сайт Chicago, чтобы **сопоставить ему подсеть, и** щелкните **OK.**

   Подсеть 10.0.0.0/8 будет **создана и** сопоставлена сайту **Chicago.**

▶ **Задание 4: сопоставьте сайту существующую подсеть**

1. **Откройте папку** Subnet, щелкните подсеть 10.0.0.0/8 **правой кнопкой и выберите в контекстном меню команду Properties.**

   Откроется диалоговое окно свойств **подсети 10.0.0.0/8 с активной вкладкой Subnet (Подсеть).**
2. В списке Site (Сайт) **выберите** сайт **Redmond, которому** будет **сопоставлена данная подсеть, и** щелкните **OK.**

▶ **Задание 5: создайте связь сайтов**

1. **Откройте папку Inter-Site Transports и щелкните папку IP.**

   Какой объект отображается **в правой панели?**
2. **Щелкните папку IP правой кнопкой и выберите в контекстном меню** команду New Site **Link (Новая связь сайтов).**

   Откроется диалоговое окно New Object — Site **Link (Новый объект — Связь** сайтов).
3. В поле Name (Имя) введите **Redmond** to Chicago.
4. **Убедитесь, что сайты** Redmond **и Chicago отображаются в поле Sites In This Site Link** (Сайты в этой **связи сайтов), и щелкните OK.**

▶ **Задание 6: выберите сервер лицензий сайта**

1. **Щелкните** сайт **Chicago.**
2. **В правой панели** щелкните **License** Site Settings **правой кнопкой и выберите в контекстном меню команду Properties.**

   Откроется диалоговое окно License Site Settings Properties.
3. **В области** Licensing **Computer (Компьютер лицензирования) щелкните кнопку Change (Изменить).**

   Откроется диалоговое окно Select Computer **(Выбор: Компьютер).**
4. **Выберите SERVER1** (или имя вашего компьютера) **и щелкните OK.**

   Вы вернетесь в **диалоговое окно Licensing Site Settings Properties (Свойства: Licensing Site Settings). Теперь компьютером лицензирования** стал SERVER**1, а** доменом — **microsoft.com (или выбранные вами компьютер и домен;** см. область **Licensing Computer).**
5. Щелкните **OK.**
6. Закройте **консоль Active Directory Sites and Services.**

▶ **Задание 7: ознакомьтесь с лицензиями сайта**

1. **Раскройте меню** Start\Programs\Administrative **Tools и щелкните Licensing (Лицензирование).**

   Откроется окно утилиты MICROSOFT.COM — Licensing. Для просмотра сведений о лицензировании перейдите на вкладку Products View (Просмотр продуктов).

Резюме

Вы научились настраивать сайты. После создания сайта необходимо добавить его подсети в контейнер Subnets, убедиться, что сайт соединен соответствующим образом с другими сайтами посредством связей, а также выбрать сервер лицензий сайта. Объединение компьютеров в подсети подчеркивает их географическую близость в сети. Связи сайтов включают стоимость и расписание трафика репликации; при отсутствии связей репликация между двумя сайтами невозможна.

Служба License Logging каждого сервера сайта реплицирует информацию о лицензировании в центральную **БД,** которая размещается на сервере лицензий сайта. Администратор сайта или администратор сервера лицензий может из консоли Licensing изучить полную историю лицензирования сайта, хранящуюся на сервере лицензий.

Выполняя практическую часть занятия, вы создали сайт, сопоставили ему подсеть, соединили сайт с помощью связей и выбрали сервер лицензий сайта.

Занятие 2, Настройка репликации между сайтами

Сетевые подключения представлены связями сайтов. Путем создания связей сайтов и настройки их стоимости, а также частоты и доступности репликации вы информируете Active Directory о том, как использовать эти подключения для репликации данных каталога. Эффективность связей сайтов можно повысить, соединив перекрывающиеся существующие связи сайтов в мосты или создав мосты для всех связей сайтов. Кроме того, можно указать сервер-плацдарм, выступающий в качестве точки обмена информацией каталога между сайтами. На этом занятии рассказывается о настройке межсайтовой репликации.

Изучив материал этого занятия, вы сможете:

- ✓ настроить репликацию между сайтами.

Продолжительность занятия — около 25 минут.

Настройка межсайтовой репликации

Для настройки межсайтовой репликации необходимо выполнить действия, описанные ниже.

1. Создать связи сайтов (см. занятие 1).
2. Настроить атрибуты связи сайтов.
3. Создать мосты связей.
4. Настроить объекты подключения (не обязательно).
5. Выбрать основной сервер-плацдарм.

Атрибуты связей сайтов

В процессе настройки межсайтовой репликации необходимо задать стоимость связи, доступность и частоту репликации для всех связей сайтов.

Стоимость

Необходимо указать значение стоимости связи сайтов каждого доступного подключения, использующегося для межсайтовой репликации. Если имеется несколько избыточных сетевых подключений, следует установить связи сайтов для каждого подключения и затем назначить стоимости для данных связей сайтов, отражающие их относительную пропускную способность. Например, если вы пользуетесь высокоскоростной линией T-1 и если имеется подключение удаленного доступа к сети на случай недоступности линии T-1, следует указать более низкую стоимость для линии T-1 и более высокую — для подключения удаленного доступа к сети. Active Directory всегда выбирает подключение на основе сведений о его стоимости; таким образом, подключение с низкой стоимостью будет задействовано, пока оно доступно.

▶ **Задание стоимость связи сайтов**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Active Directory Sites And Services (Active Directory — сайты и службы).
2. Раскройте узел Inter-Site Transports , затем папку IP или SMTP. Щелкните требуемую связь сайтов правой кнопкой и выберите команду Properties (Свойства).

3. В окне свойств связи сайтов введите в поле Cost (Стоимость) стоимость репликации (рис. 6-5). Стоимость по умолчанию — 100; чем меньше значение, тем выше приоритет. Предположим, стоимость линии T1 равна 100 единицам, а стоимость подключения удаленного доступа — 120 единицам.

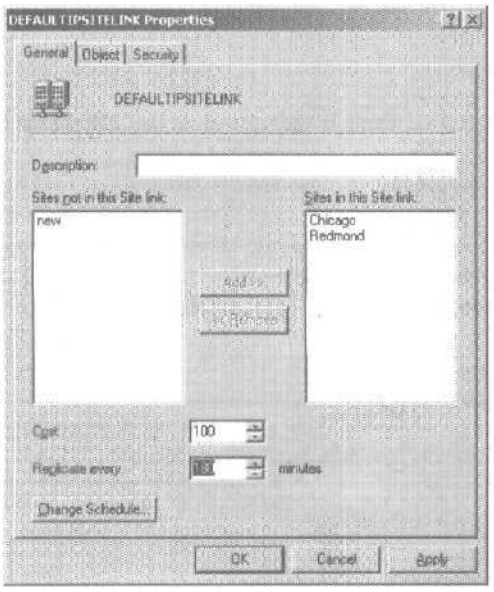


Рис. 6-5. Диалоговое окно свойств связи сайтов .

4. Щелкните OK.

Частота репликации

Для настройки частоты репликации задайте целое значение, определяющее время ожидания для Active Directory (в минутах) перед проверкой обновлений репликации. Интервал репликации должен быть как минимум 15 минут и не больше 10 080 минут (что соответствует неделе). Для успешной репликации необходимо, чтобы связь сайтов была всегда доступна. Если связь сайтов недоступна по расписанию в течение указанного срока между обновлениями репликации, то репликация не будет выполнена.

► **Настройка частоты репликации**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. Раскройте узел Inter-Site Transports, затем папку IP или SMTP. Щелкните требуемую связь сайтов правой кнопкой и выберите команду Properties.
3. В окне свойств связи укажите в поле Replicate Every (Реплицировать каждые) интервал времени в минутах между повторами репликации. Интервал по умолчанию — 180 минут; введенное значение округляется до числа, кратного 15, в диапазоне от 15 до 10 080.
4. Щелкните OK.

Доступность репликации

Следует настроить доступность репликации через связи сайтов чтобы указать, когда связь сайтов доступна для репликации. Так как протокол SMTP — асинхронный, обычно все

расписания им игнорируются. Поэтому доступность репликации через связи сайтов для SMTP-связи настраивается, только если:

- связи сайтов используют подключения по расписанию;
- очередь SMTP не включена в расписание;
- обмен данными производится серверами напрямую, без участия промежуточных устройств, например в основной сети Ethernet.

▶ **Настройка доступности репликации**

1. Раскройте меню Start\Programs\Administrative Tools и шелкните Active Directory Sites And Services.
2. Раскройте узел Inter-Site Transports, затем папку IP или SMTP. Щелкните требуемую связь сайтов правой кнопкой и команду Properties.
3. В диалоговом окне свойств связи щелкните Change Schedule (Изменить расписание).
4. В диалоговом окне Schedule For (Расписание для) укажите интервал времени, в течение которого данное подключение доступно или нет для репликации информации каталога (рис. 6-6). Затем щелкните OK,
5. В диалоговом окне свойств связи щелкните OK.

Примечание Ваши действия не возымеют эффекта, если в окне свойств межсайтового протокола помечен флажок Ignore Schedules (Игнорировать расписания).

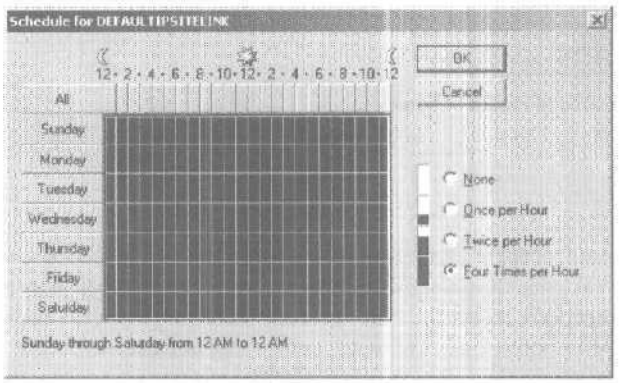


Рис. 6-6. Диалоговое окно Schedule For для связи сайтов

▶ **Игнорирование расписаний для межсайтового протокола**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. Раскройте узел Inter-Site Transports, щелкните папку IP или SMTP правой кнопкой мыши и выберите команду Properties.
3. В диалоговом окне свойств IP или SMTP на вкладке General (Общие) пометьте флажок Ignore Schedules (Игнорировать расписания).
4. Щелкните OK.

Мосты, объединяющие связи сайтов

Если для репликации подключено более двух сайтов, использующих одинаковый протокол, по умолчанию все связи сайтов «объединяются в мост» с точки зрения цены (предполагается. что связи соединяют одни и те же сайты). Связи сайтов, объединенные в мост,

являются *транзитивными,* то есть все связи сайтов для конкретного протокола неявно относятся к единому мосту связей сайтов для данного протокола. Таким образом, в полностью маршрутизируемой IP-сети (в сети, все сайты которой могут взаимодействовать друг с другом по протоколу IP) вам не надо настраивать какие либо мосты связей сайтов. В частично маршрутизируемой IP-сети функцию транзитивности связей сайтов для протокола IP можно отключить. В этом случае все IP-связи сайтов считаются нетранзитивными, и вам придется настраивать мосты связей сайтов. Мост связи сайтов — это эквивалент отдельной сети; все связи, составляюшие мост, способны транзитивно осуществлять маршрутизацию, однако вне моста маршрутизация не выполняется.

► **Создание моста связей сайтов**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. Раскройте узел Inter-Site Transports, затем щелкните папку IP или SMTP правой кнопкой и выберите в контекстном меню команду New Site Link Bridge (Новый мост связей сайтов).
3. В диалоговом окне New Object — Site Link Bridge (Новый объект — Мост связей сайтов) в поле Name (Имя) введите имя моста (рис. 6-7).

Рис. 6-7. Диалоговое окно New Object — Site Link Bridge

4. Выберите два или более соединяемых сайтов и щелкните кнопку Add (Добавить).
5. Щелкните OK.

Примечание Эта процедура избыточна и не возымеет эффекта, если в диалоговом окне свойств межсайтового протокола помечен флажок Bridge All Site Links (Установить мост для всех связей сайтов).

► **Объединение мостами всех связей сайтов для протокола межсайтовой репликации**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. Раскройте узел Inter-Site Transports, затем щелкните папку IP или SMTP правой кнопкой и выберите команду Properties.

3. В диалоговом окне свойств IP или SMTP на вкладке General (Общие) пометьте флажок Bridge All Site Link (Установить мост для всех связей сайтов).
4. Щелкните OK.

Настройка подключений вручную

В обычных условиях служба каталогов Active Directory автоматически создает и удаляет подключения. Хотя вы можете вручную добавлять и настраивать подключения, а также принудительно выполнять репликацию по конкретному подключению, в большинстве случаев вам следует разрешить автоматическую оптимизацию репликации на основе сведений, заданных в консоли Active Directory Sites and Services. Создавать подключение вручную следует, только если вы уверены в его необходимости и хотите, чтобы оно сохранялось, пока не будет удалено вручную.

▶ **Настройка подключения вручную**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. Дважды щелкните сайт, содержащий контроллер домена, для которого вы хотите вручную добавить или настроить подключение.
3. Раскройте папку Servers, затем папку контроллера домена и щелкните правой кнопкой мыши NTDS Settings и выберите команду New Active Directory Connection (Новое подключение Active Directory).
4. В диалоговом окне Find Domain Controllers (Поиск: контроллеры домена) щелкните контроллер домена для объекта-подключения и щелкните OK.
5. В диалоговом окне New Object — Connection (Новый объект — Подключение) в поле Name введите имя объекта и щелкните OK.

▶ **Принудительная репликация по подключению**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. Дважды щелкните сайт, содержащий подключение, по которому необходимо принудительно выполнить репликацию.
3. Откройте папку Servers, выберите контроллер домена, затем откройте NTDS Settings.
4. Щелкните правой кнопкой мыши требуемое подключение и выберите команду Replicate Now (Реплицировать сейчас) (рис. 6-8).

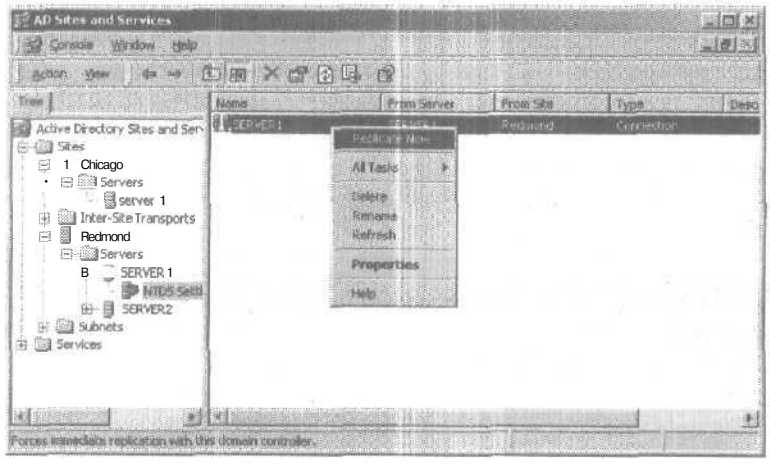


Рис. 6-8. Принудительная репликация по подключению

Назначение основного сервера-плацдарма

Обычно для обмена информацией между сайтами используются все контроллеры домена, однако, дабы более точно управлять репликацией, можно определить сервер-плацдарм, используемый для обмена данными каталога между сайтами. Наличие сервера-плацдарма позволяет выбрать основной контроллер домена для приема данных межсайтовой репликации. Затем сервер-плацдарм последовательно распространяет информацию каталога путем внутрисайтовойрепликации.

Сервер-плацдарм — это точка подключения для обмена данными каталога между сайтами. Можно определить основной сервер-плацдарм, если имеется компьютер, способный оперативно передавать и принимать данные в соответствующих объемах. Использование мощного компьютера и емкого канала связи гарантирует корректную обработку больших объемов трафика репликации. Если ресурсы контроллера домена удовлетворяют заданным вами параметрам Active Directory, он сможет самостоятельно эффективно обрабатывать данные каталога.

Можно задать несколько предпочитаемых серверов-плацдармов, но в любой момент времени только один из них будет активным. При отказе активного сервера-плацдарма Active Directory перекладывает его функции на другой сервер-плацдарм. Если невозможно использовать ни один из перечисленных пользователем серверов-плацдармов, Active Directory выберет в качестве основного сервера-плацдарма другой контроллер домена в сайте. На этот случай данный контроллер домена должен обладать достаточной пропускной способностью, удовлетворяющей повышенным требованиям, которые предъявляются к серверу-плацдарму.

Необходимо указать основной сервер-плацдарм, если для защиты сайта в вашей системе используется брандмауэр. В качестве основного сервера-плацдарма выберите прокси-сервер, выполняющий функции брандмауэра, при этом он станет точкой подключения для обмена данными с серверами, расположенными за пределами брандмауэра. Если этого не сделать, обмен данными каталога в ряде случаев выполняться не будет.

Выбранный основной сервер-плацдарм будет основным для обмена данными через протокол, соответствующий связи сайта. Другие контроллеры домена при необходимости также можно использовать для обмена данными каталога, но в нормальных условиях сервер-плацдарм выбирается первым для получения и отправки всех данных каталога.

▶ **Выбор основного сервера-плацдарма**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. В дереве консоли щелкните правой кнопкой мыши контроллер домена, который требуется сделать сервером-плацдармом, и выберите команду Properties.
3. В окне свойств контроллера домена в списке Transports Available For Inter-Site Data Transfer (Транспорты для передачи данных между сайтами) выделите один или несколько протоколов межсайтовой репликации, для которых данный компьютер будет основным сервером-плацдармом, и щелкните кнопку Add (Добавить).
4. Щелкните OK.

Практикум: настройка репликации между сайтами

Сейчас вы настроите стоимость связи сайтов, доступность и периодичность репликации, а также мост связи сайтов.

▶ Задание 1: залайте стоимость связи сайтов

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.

   Откроется окно консоли Active Directory Sites and Services.
2. Откройте папку Inter-Site Transports, затем папку IP и щелкните правой кнопкой мыши связь сайтов Redmond To Chicago, созданную на предыдущем занятии. В контекстном меню выберите команду Properties.

   Откроется диалоговое окно свойств связи Redmond To Chicago.
3. В поле Cost (Стоимость) введите стоимость репликации — 20.

▶ Задание 2: настройте периодичность связи сайтов

1. В поле Replicate Every (Реплицировать каждые) введите 120, чтобы задать промежуток времени в минутах между повторами репликации.

▶ Задание 3: настройте доступность репликации связи сайтов

1. Щелкните Change Schedule (Изменить расписание).

   Откроется диалоговое окно Schedule For Redmond To Chicago (Расписание для Redmond To Chicago).
2. Сделайте подключение доступным постоянно, кроме интервалов с 8:00 до 9:00 и с 16:00 до 17:00 с понедельника по пятницу.
3. В окне свойств связи Redmond To Chicago щелкните OK.

▶ Задание 4: создайте мост связей сайтов

1. Откройте папку Inter-Site Transports, щелкните папку IP правой кнопкой и выберите команду New Site Link Bridge (Создать мост связей сайтов).

   Откроется диалоговое окно New Object — Site Link Bridge (Новый объект — Мост связей сайтов).
2. В поле Name (Имя) введите **Redmond to Chicago Bridge.**
3. Убедитесь, что в поле Site Links In This Site Link Bridge (Связи сайтов, входящие в данный мост) отображаются связи DEFAULTIPSITELINK и Redmond to Chicago, и щелкните OK.

Резюме

Помните, что необходимо указать сведения о доступности, стоимости и частоте для всех связей сайтов — это часть процесса настройки межсайтовой репликации. Active Directory всегда выбирает подключение на основе сведений о его стоимости; таким образом, подключение с низкой стоимостью используется в первую очередь и до тех пор пока оно доступно. Создание мостов связей сайтов позволяет повысить эффективность репликации. Кроме того, установка основного сервера-плацдарма делает данный сервер основным для обмена данными через протокол, соответствующий связи сайтов.

Выполняя практикум, вы настроили стоимость связи сайтов, доступность и периодичность репликации, а также создали мост связи сайтов.

Занятие 3. Устранение неполадок репликации

Здесь обсуждаются проблемы, возникающие в процессе репликации. Как правило, проблемы, которые можно устранить средствами консоли Active Directory Sites and Services, таковы:

- новая информация каталога не распространяется своевременно;
- запросы на обслуживание не обрабатываются вовремя.

Здесь также рассказывается, как проверить топологию репликации.

Изучив материал этого занятия, вы сможете:

✓ устранять проблемы с репликацией.

Продолжительность занятия — около 5 минут.

Неэффективная репликация вызывает падение производительности службы Active Directory; например могут не распознаваться новые пользователи. В большинстве случаев в результате неэффективной обработки запросов и неэффективной репликации информация каталога устаревает, а контроллеры домена становятся недоступными. Каждую проблему можно решить одним или несколькими способами. В табл. 6-1 приведены рекомендации по устранению неполадок репликации.

Табл. 6-1. Устранение неполадок репликации

Репликация информации каталога прекратилась

Причина	Решение
Сайты, включающие клиентов и контроллеры домена, не имеют связей с контроллерами доменов другого сайта сети. Это вызывает сбои в обмене информацией каталога между сайтами	Создайте связь между текущим сайтом и сайтом, подключенным к остальным сайтам сети

Репликация информации каталога замедлилась, но не остановилась

Причина	Решение
Хотя все сайты соединены связями, существующая структура межсайтовой репликации недостаточно полна. Информация каталога реплицируется на все контроллеры домена, если они объединены связями, однако это не оптимальное решение. При наличии связей сайтов и отсутствии мостов распространение изменений с одних контроллеров доменов на другие, с которыми отсутствуют прямые связи, выполняется слишком долго	Убедитесь, что служба Active Directory настроена правильно. Для объединения нескольких связей сайтов, требующих более эффективной репликации, попробуйте создать мост или объединить в мост все связи сайтов

Табл. 6-1. Устранение неполадок репликации *(окончание)*

Репликация информации каталога замедлилась, но не остановилась

Причина	Решение
Текущих сетевых ресурсов недостаточно для обслуживания суммарного трафика репликации. Такая ситуация может повлиять на службы, не имеющие отношения к Active Directory, поскольку обмен информацией каталога требует значительных сетевых ресурсов	Увеличьте долю свободных сетевых ресурсов, выделяемых трафику каталога. Уменьшите частоту репликации в расписании. Настройте стоимость связей сайтов. Создайте связи сайтов или мосты связей сайтов, чтобы получить сетевые подключения с повышенной пропускной способностью
Информация каталога, изменившаяся на контроллерах домена в одном сайте, своевременно не обновилась на контроллерах домена в других сайтах, поскольку заданная в расписании частота межсайтовой репликации слишком низка	Увеличьте частоту репликации. Если репликация выполняется через мост, проверьте, какая связь сайтов сдерживает репликацию. Увеличьте интервал времени, отведенный для репликации, или частоту репликации в заданный интервал времени для проблемной связи сайтов
Клиенты пытаются запросить аутентификацию, информацию и службы у контроллера домена по подключению с низкой пропускной способностью. Это может замедлить отклик на запросы клиентов	Проверьте, имеется ли сайт, который способен лучше обслуживать подсеть клиента. Если медленно обслуживаемый клиент изолирован от контроллера домена, попробуйте создать другой сайт с собственным контроллером домена, к которому затем присоедините клиент. Создайте подключение с большей пропускной способностью

Проверка топологии репликации

Active Directory запускает процесс, который определяет стоимость межсайтовых подключений, проверяет доступность известных контроллеров домена и не были ли добавлены новые и затем на основе полученных сведений добавляет или удаляет объекты-подключения для формирования эффективной топологии репликации. Этот процесс не затрагивает объекты-подключения, созданные вручную.

▶ **Проверка топологии репликации**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. В дереве консоли щелкните правой кнопкой мыши сервер, который хотите использовать для проверки топологии репликации.
3. Щелкните NTDS Settings правой кнопкой и выберите в контекстном меню команду All Tasks\Check Replication Topology (Все задачи\Проверка топологии репликации).

Резюме

Мы рассказали о некоторых проблемах, возникающих в процессе репликации, а также о возможных способах их решения.

Занятие 4. Изменение параметров сервера

Чтобы сохранить конкурентноспособность в бизнесе, вам необходимо периодически конфигурировать параметры сервера для сайта. На этом занятии мы опишем некоторые особенности обслуживания сервера, в том числе создание объекта-сервера в сайте, перемещение этого объекта между сайтами, включение или отключение поддержки глобального каталога и удаление объекта бездействующего сервера из сайта.

Изучив материал этого занятия, вы сможете:

✓ настраивать объект сервера в сайте.

Продолжительность занятия — около 10 минут.

По мере роста и изменения сайта согласно потребностям бизнеса вам может потребоваться изменить параметры сервера для сайта:

- создать объект-сервер в сайте;
- переместить объект-сервер между сайтами;
- включить или отключить поддержку глобального каталога;
- удалить бездействующий объект-сервер из сайта.

Создание объекта-сервера в сайте

Данную процедуру можно использовать для создания в сайте рядовых серверов и контроллеров домена, Создание объекта-сервера — не то же самое, что установка контроллера домена с помощью мастера Active Directory Installation.

► **Создание объекта-сервера в сайте**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. В дереве консоли дважды шелкните сайт, в котором будет содержаться новый объект-сервер контроллера домена.
3. Щелкните папку Servers правой кнопкой и выберите команду New\Server (Создать\-Сервер).
4. В диалоговом окне New Object — Server (Новый объект — Сервер) в поле Name (Имя) введите имя нового объекта-сервера. Затем щелкните OK.

Перемещение объектов-серверов между сайтами

Описанную ниже процедуру можно использовать для перемещения рядовых серверов и контроллеров домена между сайтами.

► **Перемещение объекта-сервера между сайтами**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните пункт Active Directory Sites And Services.
2. В дереве консоли щелкните требуемый объект-сервер правой кнопкой и выберите команду All Tasks\Move (Все задачи\Переместить).
3. В диалоговом окне Move Server (Перемещение сервера) выберите сайт, куда собираетесь переместить объект-сервер, и щелкните OK.

Включение и отключение поддержки глобального каталога

Для регистрации в системе клиентам нужен доступ к глобальному каталогу, поэтому для использования преимуществ сайтов, в каждом из них должна быть минимум одна реплика глобального каталога.

► **Включение и отключение поддержки глобального каталога**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. В дереве консоли дважды щелкните контроллер домена, содержащий глобальный каталог.
3. Щелкните правой кнопкой мыши NTDS Settings и выберите команду Properties.
4. Для включения поддержки глобального каталога пометьте флажок Global Catalog (для отключения поддержки — сбросьте этот флажок) и щелкните OK.

Удаление бездействующего объекта-сервера из сайта

Используйте данную процедуру, если хотите навсегда удалить объект-сервер из сайта. Если в дальнейшем вы планируете заново активизировать сервер, вместо удаления сервера удалите его объект NTDS Settings. После повторной активизации сервера Active Directory автоматически создаст новый объект NTDS Settings, соответствующим образом включив сервер в топологию репликации.

► **Удаление бездействующего сервера**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services.
2. В дереве консоли щелкните правой кнопкой удаляемый объект-сервер и выберите команду Delete (Удалить).
3. В ответ на запрос подтвердить ваши намерения щелкните Yes.

Резюме

Вы научились настраивать параметры сервера, в том числе создавать объект сервера в сайте, перемещать этот объект между сайтами, включать или отключать поддержку глобального каталога, а также удалять бездействующий объект-сервера из сайта.

Закрепление материала

9 | Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении А «Вопросы и ответы» в конце книги.

1. Назовите четыре этапа настройки сайта.

2. Назовите два конфигурационных объекта сайта, которые мастер установки Active Directory создает автоматически.

3. Какой протокол использует удаленные вызовы процедур для межсаитовои и внутрисайтовой репликации?

4. Назовите три этапа настройки репликации между сайтами.

5. В чем отличие частоты и доступности репликации?

6. Для чего предназначен сервер-плацдарм?

ГЛАВА 7

Управление учетными записями пользователей

В этой главе

Здесь рассказывается, как использовать и планировать учетные записи, как создавать локальные и доменные учетные записи и задавать их свойства. Кроме того, вы узнаете, как настроить профили пользователей и их домашние папки, а также о том, как запретить, разрешить, переименовать, удалить, разблокировать учетные записи и как восстановить пароли пользователей.

Прежде всего

Для изучения материалов этой главы необходимо:

- понимать различия рабочей группы и домена;
- понимать различия контроллера домена и простого сервера;
- уметь входить и выходить из системы Windows 2000;
- знать правила именования в Active Directory.

Занятие 1. Учетные записи пользователей

Посредством учетной записи пользователь может подключиться к домену для доступа к ресурсам сети или зарегистрироваться на каком-либо компьютере, чтобы получить доступ к его ресурсам. Все, кто регулярно пользуется сетью, должны иметь уникальную учетную запись.

В Windows 2000 предусмотрено три типа учетных записей: локальные, доменные и встроенные. *Локальная учетная запись* (local user account) позволяет пользователю зарегистрироваться на конкретном компьютере, чтобы получить доступ к его ресурсам. Пользователь, обладающий *доменной учетной записью* (domain user account) может подключиться к домену, чтобы получить доступ к ресурсам сети. *Встроенная учетная запись* (built-in user account) позволяет выполнять функции администрирования или получать доступ к локальным или сетевым ресурсам. На этом занятии рассказано об учетных записях и различиях между ними.

Изучив материал этого занятия, вы сможете:

- ✓ рассказать о различиях между локальной и доменной учетными записями;
- ✓ рассказать о назначении встроенной учетной записи.

Продолжительность занятия — около 10 минут.

Локальная учетная запись

Позволяет войти в систему и получить доступ к ресурсам только того компьютера, на котором создана.

Windows 2000 создает локальную учетную запись только в локальной базе данных безопасности (рис. 7-1). Windows 2000 не реплицирует информацию о локальной учетной записи на какой-либо другой компьютер. Если существует локальная учетная запись, для проверки ее подлинности применяется локальная БД безопасности.

Не создавайте локальные учетные записи на компьютерах с Windows 2000, включенных в домен, так как домен не распознает такие записи. А значит, пользователь не получит доступ к ресурсам домена, а администратор домена не сможет управлять локальными учетными записями или назначать разрешения доступа к ресурсам домена, если только он не подсоединился к компьютеру с помощью меню Action (Действие) консоли Computer Management (Управление компьютером).

Локальные учетные записи

- Обеспечивает доступ к ресурсам на локальном компьютере
- Создаются в локальной БД безопасности

Рис. 7-1. Локальные учетные записи

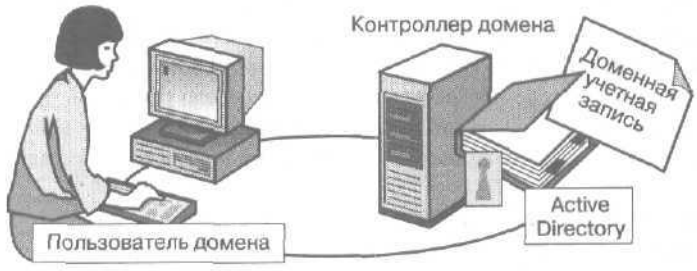
Учетные записи домена

Позволяют пользователям получить доступ к домену и его ресурсам из любого места сети. При входе в систему пользователь вводит свой пароль и регистрационное имя. На основе этих сведений Windows 2000 опознает пользователя и выделяет ему маркер доступа, который содержит информацию о пользователе и параметрах защиты. Маркер доступа идентифицирует пользователя для компьютеров с Windows 2000, к ресурсам которых он хочет получить доступ. Windows 2000 создает маркер доступа на время данной сессии.

Доменная учетная запись создается в контейнере или ОП в копии БД каталога Active Directory на контроллере домена (рис. 7-2). Этот контроллер реплицирует информацию о новой учетной записи на остальные контроллеры домена.

После этого все контроллеры в дереве домена могут опознать пользователя при входе в систему.

Примечание Репликация информации о доменной учетной записи на все контроллеры домена выполняется не сразу. Поэтому иногда пользователю не удается немедленно войти в систему по только что созданной учетной записи. По умолчанию репликация информации каталога выполняется каждые пять минут.



Доменные учетные записи
- Обеспечивают доступ к сетевым ресурсам
- Предоставляют маркер доступа для аутентификации
- Создаются в Active Directory на контроллере домена

Рис. 7-2. **Доменная учетная запись**

Встроенные учетные записи

Windows 2000 автоматически создает встроенные учетные записи. Наиболее часто применяются встроенные учетные записи Administrator (Администратор) и Guest (Гость).

Примечание Встроенные учетные записи IUSR_*имя_компьютера* и IWAM_*имя_компьютера* создаются автоматически, при установке на контроллер домена Internet Information Services (IIS). IUSR_*имя_компьютера* — это запись для анонимного доступа к IIS. IWAM_*имя_компьютера* — учетная запись для анонимного доступа к внепроцессным приложениям IIS.
Учетная запись TsInternetUser автоматически создается при установке Terminal Services на контроллере домена и используется службами терминалов.

Встроенная учетная запись Administrator

Применяется для управления компьютером в целом. Если ваш компьютер входит в домен, вы можете использовать эту запись для конфигурирования домена. Учетная запись

Administrator позволяет создавать и модифицировать учетные записи и труппы, управлять политикой безопасности, устанавливать принтеры, назначать разрешения учетным записям для доступа к ресурсам.

Учетную запись Administrator лучше использовать только для выполнения административных задач. О настройке учетных записей для выполнения задач, не связанных с администрированием, — в главе 8.

Примечание Удалить учетную запись Administrator нельзя. Обязательно переименуйте ее для повышения уровня зашиты. Причем используйте имя, никак не связанное с учетной записью Administrator. Это усложнит процесс ее взлома.

Встроенная учетная запись Guest

Применяется временными пользователями для входа в систему и по умолчанию отключена. Активизируйте ее только в сетях, не требующих высокой степени зашиты, и всегда назначайте пароль. Вы вправе переименовать эту учетную запись, но не можете ее удалить.

Резюме

В Microsoft Windows 2000 существуют разные типы учетных записей: локальные и доменные. Доменная учетная запись позволяет пользователю подключиться к домену, чтобы получить доступ к ресурсам сети. С помощью локальной учетной записи пользователь входит в систему на конкретном компьютере для получения доступа к его ресурсам. Также существуют встроенные учетные записи, которые бывают как доменными, так и локальными. Они предназначены для выполнения функции администрирования или получения доступа к ресурсам.

Доменная учетная запись создается в копии БД каталога Active Directory на контроллере домена. Этот контроллер реплицирует информацию о новой учетной записи на остальные контроллеры домена. Windows 2000 создает локальную учетную запись только в БД безопасности конкретного компьютера (локальной БД безопасности). Информация о локальной учетной записи не реплицируется на контроллеры домена. Встроенные учетные записи Windows 2000 создает автоматически.

Занятие 2. Планирование новых учетных записей

Вы можете ускорить процесс создания учетных записей, правильно планируя и организуя информацию. В этом занятии рассказывается о планировании:

- правил именования учетных записей;
- требований к паролям;
- параметров учетных записей (время, когда можно входить в систему, компьютеры, с которых это можно делать, а также срок действия пароля).

Изучив материал этого занятия, вы сможете:

- ✓ планировать создание новых учетных записей;
- ✓ рассказать, как требования для паролей влияют на уровни безопасности.

Продолжительность занятия — около 10 минут.

Правила именования учетных записей

Прежде всего, нужно знать, как пользователи идентифицируются в домене. Логичные правила и строгое их соблюдение помогут вам и вашим пользователям запомнить имена для входа в систему и найти их в списках.

В табл. 7-1 перечислены правила именования, которые необходимо учитывать при планировании учетных записей.

Табл. 7-1. Правила именования

Правило	Пояснение
Локальные учетные записи	Имена локальных учетных записей должны быть уникальны на компьютере, где вы их создаете
Доменные учетные записи	*Составное имя* (distinguished name, DN) для входа в систему должно быть уникальным в каталоге Active Directory. *Относительное составное имя пользователя* (relative distinguished name, RDN) должно быть уникально в пределах организационного подразделения (ОП), где вы создаете доменную учетную запись
Используйте максимум 20 символов	Имена пользователей могут содержать до 20 символов, как строчных, так и прописных. В поле разрешается ввести и большее число символов, но Windows распознает только первые 20
Избегайте недопустимых символов	Недопустимы следующие символы: « / \ [ ] : ; | = , + * ? < >
В именах пользователей регистр не различается	Вы можете использовать комбинацию специальных и алфавитно-цифровых символов для того, чтобы уникально идентифицировать пользователя. Регистр не имеет значения, но Windows 2000 сохраняет его
Согласуйте учетные записи для служащих с одинаковыми именами	Если есть два пользователя с именами Иванов Алексей Викторович, вы можете для первой записи взять фамилию пользователя и его инициалы, а для второй добавить еще несколько букв из имени или отчества для того, чтобы эти учетные записи различались. Например, ИвановАВ и ИвановАлексейВ. Другой вариант — пронумеровать имена пользователей: ИвановАВ1 и ИвановАВ2

Табл. 7-1. Правила именования *(продолжение)*

Правило	Пояснение
Отразите статус служащего	Укажите временный статус служащих в их учетной записи. Для этот можно использовать Т и дефис перед именем пользователя. Например, Т-ИвановАВ. Или применить скобки - ИвановАВ(Temp)
Совместимость с электронной почтой	Некоторые системы электронной почты не воспринимают такие символы, как пробел или круглые скобки

Требования к паролям

Чтобы упорядочить доступ к ресурсам системы, каждой учетной записи надо сопоставить пароль. Перечислим основные принципы назначения паролей.

- Всегда назначайте пароль для учетной записи Administrator (Администратор), чтобы предотвратить неавторизованный доступ.
- Определитесь, кто будет назначатьуникальные пароли для учетных записей: администратор или пользователи. Вы можете делать это сами и запретить пользователям их изменять. Другой вариант — разрешить пользователям ввести собственные пароли при первом входе в систему. В большинстве случаев лучше, когда пользователи сами управляют своими паролями.
- Придумайте пароли, которые трудно угадать. Избегайте паролей с очевидными ассоциациями (например, год рождения, имя родственника и т. п.).
- Длина пароля может достигать 128 символов. Рекомендуемая минимальная длина — 8 символов.
- Используйте как строчные, так и прописные буквы, числа, а также разрешенные символы.
- Между первой и седьмой позициямивставьте минимум один символьный знак.
- Пусть следующий пароль какможно больше отличается от предыдущего.
- Пароль не должен содержать имя пользователя или имя учетной записи.
- В качестве пароля не следует выбирать часто употребляемое слово или имя.

Примечание Групповые политики Windows 2000 также влияют на пароли. Подробнее об использовании групповых политик — в главе 12.

Параметры учетных записей

Необходимо определить часы, когда пользователю разрешено войти в сеть, а также компьютеры, с которых он может это сделать. Также надо установить, должен ли истекать срок действия учетных записей временных пользователей.

Часы входа в систему

Устанавливаются для пользователей, которым нужен доступ только в определенное время. Например, вы можете разрешить рабочим ночной смены доступ только в их рабочее время.

Компьютеры, с которых пользователю разрешено войти в систему

По умолчанию пользователям доступен домен с любого компьютера домена. По соображениям безопасности можно разрешить пользователям получать доступ к домену только с их компьютеров, Таким образом, пользователям не удастся получить важную информацию, хранящуюся на других компьютерах.

Внимание! Если использование NetBIOS поверх TCP/IP запрещено, Windows 2000 не сможет определить, с какого компьютера пользователи входят в систему, и, таким образом, вам не удастся указать компьютеры, с которых пользователи имеют право войти в систему.

Истечение срока действия учетной записи

Если срок действия учетной записи ограничен, то необходимо задать дату истечения срока действия учетной записи, чтобы гарантировать, что учетная запись будет запрещена по прошествии этого срока. Рекомендуется приурочить срок истечения учетных записей временных работников к моменту окончания их контракта.

Практикум: планирование новых учетных записей

Сейчас вы попробуете спланировать учетные записи для новых сотрудников.

Сценарий

Вам, администратору Windows 2000 в вашей корпоративной сети, нужно создать и настроить учетные записи для новых сотрудников. Предположим, недавно на работу принято девять сотрудников. Вам нужно определить:

- правила именования, позволяющие легко создать учетные записи для сотрудников с одинаковыми именами, а также для временных сотрудников;
- время, когда им разрешено входить в систему;
- компьютеры, с которых они могут входит в систему.

Условия

При назначении учетных записей следует выполнить следующие условия:

- каждому сотруднику нужна своя учетная запись;
- постоянные сотрудники должны сами отвечать за свои пароли;
- из соображений безопасности администратор будет сам контролировать пароли временных служащих;
- часы работы дневной смены — с 8:00 до 17:00, ночной смены — с 18:00 до 6:00,
- постоянным служащим необходим доступ к сети в любое время суток;
- временным служащим разрешается входить в систему только с их компьютеров и только во время их смены, они используют компьютеры с именами Tempi и Tетр2,

Список новых сотрудников

В табл. 7-2 приведены имена и другие сведения о новых сотрудниках.

Табл. 7-2. Сведения о новых сотрудниках

Имя пользователя	Должность	Отдел	Статус	Смена
Don Hall	Агент	Отдел продаж	Временный	День
Donna Hall	Менеджер	Отдел технической поддержки	Постоянный	Ночь
James Smith	Вице-президент	Обучение	Постоянный	День
James Smith	Агент	Отдел продаж	Постоянный	День
Jon Morris	Разработчик	Разработка продуктов	Временный	Ночь
Judy Lew	Разработчик	Разработка продуктов	Временный	День
Kim Yoshida	Президент	Обучение	Постоянный	День
Laurent Vernhes	Инженер	Отдел технической поддержки	Временный	Ночь
Sandra Martinez	Инженер	Отдел технической поддержки	Постоянный	День

Определение правил именования

Заполните табл. 7-3, используя информацию из разделов «Сценарий», «Условия» и «Список новых сотрудников», чтобы определить правила именования для новых служащих.

Табл. 7-3. План правил именования учетных записей новых сотрудников

Имя пользователя	Полное имя	Имя пользователя для входа в систему
Don Hall		
Donna Hall		
James Smith		
James Smith		
Jon Morris		
Judy Lew		
Kim Yoshida		
Laurent Vernhes		
Sandra Martinez		

Заполните табл. 7-4, используя информацию из разделов «Сценарий», «Условия» и «Список новых сотрудников», чтобы определить часы входа в систему для новых служащих и компьютеры, с которых они могут это сделать.

Табл. 7-4. План расписания входа в систему для новых сотрудников

Имя пользователя	Когда пользователю разрешено входить в систему	С каких компьютеров пользователю разрешен вход в систему
Don Hall		
Donna Hall		
James Smith		
James Smith		
Jon Morris		
Judy Lew		
Kim Yoshida		
Laurent Vernhes		
Sandra Martinez		

Выберите подходящие параметры смены паролей для каждого пользователя в табл. 7-5, чтобы определить, кто контролирует пароль пользователя.

Табл. 7-5. Планирование паролей для новых сотрудников

Имя пользователя	Пользователь должен сменить пароль при следующем входе в систему	Пользователь не может менять пароль
Don Hall		
Donna Hall		
James Smith		
James Smith		
Jon Morris		
Judy Lew		
Kim Yoshida		
Laurent Vernhes		
Sandra Martinez		

Резюме

При планировании учетных записей необходимо определить правила наименования учетных записей, требования к паролям, а также параметры учетных записей — время, когда вход в систему разрешен, компьютеры, с которых это можно делать, а также срок действия пароля. Учетные записи домена могут иметь длину до 20 символов и должны быть уникальны в ОП, в котором вы создаете доменную учетную запись. Составное имя для входа в систему (DN) должно быть уникально в каталоге. Относительное составное имя пользователя (RDN) должно быть уникально в пределах ОП, где вы создаете доменную учетную запись. Имена локальных учетных записей могут иметь длину до 20 символов и должны быть уникальны на компьютере, где вы их создаете. Если вы учтете все эти требования перед началом создания учетных записей, то сократите время, затраченное на создание учетных записей, и упростите управление этими учетными записями.

В практикуме вы попытались реализовать выдуманный сценарий. Вы создали правила именования, позволяющие легко создать учетные записи для сотрудников с одинаковыми именами, а также для временных сотрудников. Кроме того, основываясь на предоставленных сценарии и требованиях, вы создали расписание входа в систему для каждого пользователя, а также компьютеров, с которых они могут это сделать.

Занятие 3. Создание учетной записи

Локальные учетные записи создаются с помощью оснастки Local Users and Groups (Локальные пользователи и группы) консоли Computer Management (Управление компьютером). Доменные учетные записи создаются средствами консоли Active Directory Users and Computers (Active Directory — пользователи и компьютеры). Для использования этих инструментов необходимо иметь права администратора. На этом занятии мы расскажем о создании учетных записей и настройке их параметров.

Изучив материал этого занятия, вы сможете:

- ✓ создать локальную учетную запись;
- ✓ создать доменную учетную запись;
- ✓ настроить параметры учетной записи.

Продолжительность занятия — около 45 минут.

Создание локальной учетной записи

Оснастка Local Users and Groups (рис. 7-3) позволяет создавать, удалять или отключать локальные учетные записи на локальном компьютере или в рабочей группе, Нельзя создавать локальные учетные записи на контроллере домена.

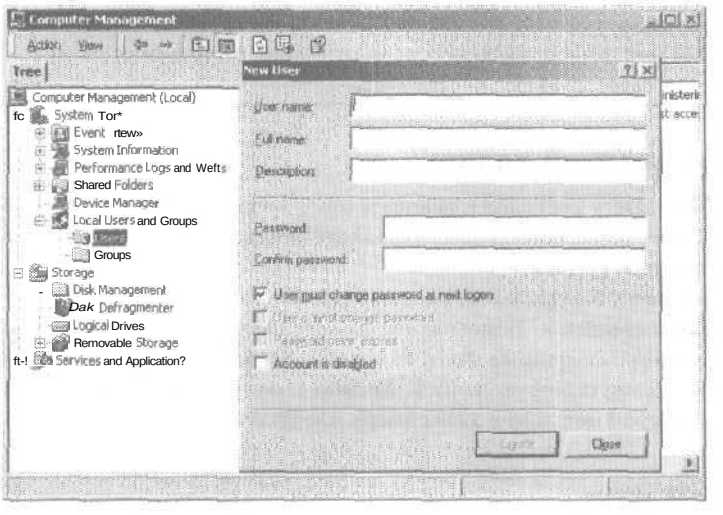


Рис. 7-3. **Оснастка Local Users and Groups и окно New User**

► Создание локальной учетной записи

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Computer Management (Управление компьютером).
2. Разверните окно Local Users And Groups (Локальные пользователи и группы), щелкните правой кнопкой папку Users (Пользователи) и выберите в контекстном меню команду New User (Новый пользователь).
3. В одноименном диалоговом окне (рис. 7-3) задайте параметры локальной учетной записи, как описано в табл. 7-6.

Табл. 7-6. Параметры локальной учетной записи

Параметр	Описание
User Name (Пользователь)	Имя пользователя для входа в систему (заполнить это поле необходимо)
Full Name (Полное имя)	Полное имя пользователя, в том числе имя и фамилия (также может включать отчество, инициалы и т. п.). Заполнять это поле не обязательно
Description (Описание)	Описание учетной записи или статуса пользователя (заполнять не обязательно)
User Must Change Password At Next Logon (Потребовать смену пароля при следующем входе в систему)	По умолчанию этот флажок отмечен, но при желании его можно снять. Он означает, что пользователь должен сменить пароль при следующем входе в систему
User Cannot Change Password (Запретить смену пароля пользователем)	Пароли разрешается изменять только администраторам
Password Never Expires (Срок действия пароля неограничен)	Пометьте этот флажок, если не хотите, чтобы пароль менялся. Если установлен флажок User Must Change Password At Next Logon, флажок User Cannot Change Password недоступен
Account Is Disabled (Отключить учетную запись)	Пометьте этот флажок, чтобы запретить использование учетной записи: например, если сотрудник отстранен от работы

Создание доменной учетной записи

Средствами консоли Active Directory Users and Computers (рис. 7-4) можно создавать, удалять или отключать доменные учетные записи на контроллере домена или локальные учетные записи на любом компьютере домена.

При создании доменной учетной записи имя входа пользователя по умолчанию относится к домену, в котором она создается. Впрочем, вы можете выбрать любой домен, на котором вы имеете право создавать доменные учетные записи. Кроме того, вам надо выбрать контейнер, где будете создавать новую запись. Можно создать доменную учетную запись в стандартном контейнере Users или в контейнере, где будут храниться доменные учетные записи.

▶ **Создание доменной учетной записи**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Active Directory Users and Computers (Active Directory — пользователи и компьютеры).
2. Раскройте домен, щелкните правой кнопкой контейнер Users (Пользователи) и выберите в контекстном меню команду New\User (Создать\Пользователь).

Примечание Users — просто контейнер по умолчанию. В производственной среде учетные записи пользователей следует добавлять в созданные вами ОП, а не в контейнер Users.

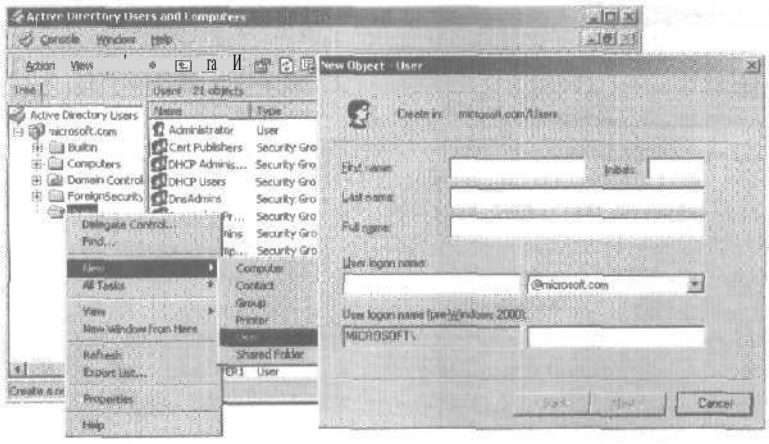


Рис. 7-4. **Консоль Active Directory Users and Computers и окно New Object** User

3. В окне New Object — User (Новый объект — пользователь) (рис. 7-4) задайте параметры доменного имени пользователя, описанные в табл. 7-7.

Табл. 7-7. **Параметры имени пользователя в окне New Object User**

Параметр	Описание
First Name (Имя)	Имя пользователя. Для добавления объекта пользователя необходимо заполнить одно из полей: First Name, Last Name, Full Name или Initials
Initials (Инициалы)	Инициалы пользователя
Last Name (Фамилия)	Фамилия пользователя
Full Name (Полное имя)	Полное имя пользователя. Должно быть уникально в контейнере, где создается учетная запись. Windows 2000 автоматически заполняет это поле, если вы ввели информацию в поля First Name, Initials или Last Name. Поле Create-In (Создать в) показывает, в каком контейнере будет расположена новая учетная запись
User Logon Name (Имя входа пользователя)	User Logon Name содержит поле и список, уникально определяющий пользователя в сети. Поле (слева) — это уникальное имя входа пользователя, основанное на правилах именования. Это поле необходимо заполнить, причем имя должно быть уникальным в домене. Список (справа) — это доменное имя
User Logon Name (Pre-Windows 2000) (Имя входа пользователя в предыдущих версиях Windows)	Уникальное имя, под которым пользователь входил в систему в предыдущих версиях Windows, например Windows NT 4.0 или Windows NT 3.51. Поле заполняется в обязательном порядке, имя должно быть уникальным в домене

Настройка пароля

В диалоговом окне New Object — User (Новый объект — пользователь) (рис. 7-4) щелкните Next, чтобы открыть второе диалоговое окно New Object — User (рис. 7-5), где задаются параметры пароля для доменной учетной записи.

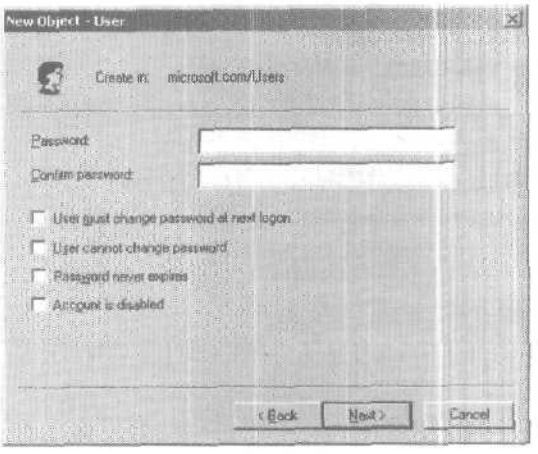


Рис. 7-5. **Окно** New **Object — User**

В табл. 7-8 описаны параметры пароля, перечисленные в окне New Object — User.

Табл. 7-8. Параметры пароля в окне New **Object — User**

Параметр	Описание
Password (Пароль)	Пароль, используемый для аутентификации пользователя. Для повышения уровня защиты всегда назначайте пароль
Confirm password (Подтверждение)	Подтвердите пароль, введя его вторично (это необходимо при назначении пароля)
User Must Change Password At Next Logon (Потребовать смену пароля при следующем входе в систему)	Пользователь должен сменить пароль при первом входе в систему. Таким образом, пользователь будет единственным человеком, знающим пароль
User Cannot Change Password (Запретить смену пароля пользователем)	Пароли вправе изменять только администраторы. Отметьте этот флажок, если одну и ту же доменную учетную запись (например, Guest) используют несколько человек или если вы хотите сохранить контроль над паролями учетных записей
Password Never Expires (Срок действия пароля не ограничен)	Отметьте этот флажок, если не хотите, чтобы пароль менялся. Если установлен флажок User Must Change Password At Next Logon, флажок User Cannot Change Password недоступен
Account Is Disabled (Отключить учетную запись)	Пометьте этот флажок, чтобы запретить использование учетной записи, например, если сотрудник отстранен от работы

Примечание Всегда требуйте, чтобы новые пользователи вводили собственный пароль при первом входе в систему. Это исключит существование учетной записи без пароля, а пароль будет знать только сам пользователь.

Совет Для большей безопасности в сетях создавайте случайные начальные пароли для всех новых учетных записей, используя произвольную комбинацию букв и цифр. Это обеспечит защиту учетных записей.

Практикум: создание доменной учетной записи

Создайте доменные учетные записи, перечисленные в табл. 7-9.

Табл. 7-9. Доменные учетные записи для практикума

First Name (Имя)	Last Name (Фамилия)	User Logon Name (Имя входа пользователя)	Password (Пароль)	Change Password (Изменить пароль)
User	One	User1	(пустой)	Must
User	Three	User3	(пустой)	Must
User	Five	User5	User5	Must
User	Seven	User7	User7	Must
User	Nine	User9	User9	Cannot

Выполнив следующее задание, вы создадите первую учетную запись с помощью консоли Active Directory Users and Computers. Далее повторите те же действия для создания остальных учетных записей.

▶ **Задание: создайте доменную учетную запись**

1. Зарегистрируйтесь как Administrator (Администратор).
2. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Active Directory Users and Computers (Active Directory — пользователи и компьютеры).

   Откроется одноименная консоль.
3. Раскройте узел microsoft.com (если вы используете другое имя домена, раскройте свой домен) и дважды щелкните папку Users.

   Какие учетные записи мастер установки Active Directory создал по умолчанию?
4. Щелкните правой кнопкой мыши папку Users и выберите в контекстном меню команду New\User (Создать\Пользователь).

   Откроется окно New object — User.

   Где в Active Directory будет создана новая учетная запись?
5. В поле First Name введите **User**.
6. В поле Last Name введите One.

   Заметьте: поле Full Name заполняется автоматически.
7. В поле User Logon введите **user1**.
8. В списке справа от окна User Logon выберите @microsoft.com (имя домена может отличаться, если вы не использовали microsoft.com в качестве доменного имени DNS).

   Имя входа пользователя в сочетании с доменным именем, появляющимся в окне справа от окна User Logon Name, — это полное имя входа пользователя в Интернете. Это имя уникально определяет пользователя в каталоге (например, user1@microsoft.com).

   Заметьте: поле имени входа для предыдущих версий Windows заполняется автоматически.

В каких случаях используется имя входа предыдущих версий Windows?

9. Щелкните Next, чтобы продолжить.
   Windows 2000 отобразит окно New Object — User, предлагая ввести параметры пароля и ограничения.
10. В полях Password и Confirm Password введите пароль или оставьте эти поля пустыми, если вы не присваиваете пароль.
    Если вы вводите пароль, обратите внимание, что на экране его символы заменяются звездочками (*), дабы посторонние не подсмотрели ваш пароль.
11. Определите, может ли пользователь изменять свой пароль.
    Каковы результаты одновременного применения флажков User Must Change Password At Next Logon и User Cannot Change Password? Поясните ответ.
    В каком случае следует выбрать флажок Account is Disabled при создании новой учетной записи?
12. После задания параметров пароля щелкните Next.
    Откроется окно New Object — User, содержащее параметры, сконфигурированные для этой учетной записи.
13. Проверьте правильность параметров и щелкните кнопку Finish (Готово).

Примечание Если настройки учетной записи оказались неверными, щелкните кнопку Back (Назад), чтобы изменить их.

Заметьте: на правой панели консоли Active Directory Users and Computers появилась вновь созданная учетная запись.

14. Повторите пункты 4—13 для остальных учетных записей.

Свойства учетной записи

С каждой создаваемой учетной записью ассоциируется набор свойств по умолчанию. После создания учетной записи можно настраивать персональные и учетные свойства, параметры входа и входящих звонков. Для пользователей домена эти учетные свойства равносильны свойствам объектов.

Вы можете использовать заданные для доменной учетной записи свойства для поиска пользователей в каталоге или для применения в других приложениях в качестве атрибутов объектов. Поэтому необходимо задать подробные определения для каждой создаваемой доменной учетной записи. ,

Вкладки окна свойств (рис. 7-6) содержат информацию об учетной записи. Описание этих вкладок приведено в табл. 7-10.

Табл. 7-10. Вкладки окна свойств учетной записи

Вкладка	Описание
General (Общие)	Имя и фамилия пользователя, отображаемое имя, местоположение офиса, номер(а) телефоиа(ов), электронный адрес, адрес домашней страницы и др.
Address (Адрес)	Все адресные данные
Account (Учетная запись)	Свойства учетной записи пользователя: имя входа пользователя, время входа, компьютеры, с которых пользователь может войти в систему, учетные параметры, срок действия

Табл. 7-10. Вкладки окна свойств учетной записи *(окончание)*

Вкладка	Описание
Profile (Профиль)	Путь профиля, сценарий входа, домашний каталог и совместно используемая папка с документами
Telephones (Телефоны)	Номера домашнего телефона, пейджера, мобильного телефона, факса, IP-телефона пользователя и комментарии
Organization (Организация)	Должность, отдел, компания, руководитель и прямые подчиненные
Remote Control (Удаленное управление)	Конфигурирует параметры служб Terminal Services
Terminal Services Profile (Профиль служб терминалов)	Конфигурирует профиль пользователя служб Terminal Services
Member Of (Член групп)	Группы, в которые входит пользователь
Dial-In (Входящие звонки)	Свойства входящих звонков пользователя
Environment (Среда)	Конфигурирует среду служб Terminal Services
Sessions (Сеансы)	Задает параметры ограничения длительности сеансов служб Terminal Services

Примечание Для локальной учетной записи окно свойств содержит только вкладки General, Member Of и Profile, поскольку локальные пользователи не считаются в Active Directory объектами пользователей.

Настройка личных свойств

Четыре вкладки окна свойств учетной записи таковы: General, Address, Telephones и Organization. Настройка атрибутов этих вкладок позволяет пользователям и администраторам искать пользователей в каталоге. Например, если заполнены все поля вкладки Address (рис. 7-6), можно найти человека по адресу или другому полю.

▶ **Настройка личных свойств**

1. В меню Administrative Tools (Администрирование) щелкните Active Directory Users and Computers, затем — имя домена.
2. Щелкните соответствующий контейнер, чтобы просмотреть имеющиеся доменные учетные записи.
3. Щелкните правой кнопкой соответствующую доменную учетную запись и в контекстном меню выберите команду Properties (Свойства).
4. Щелкните соответствующую вкладку личных свойств, которые хотите ввести или изменить, и введите значения всех свойств.
5. Щелкните OK.

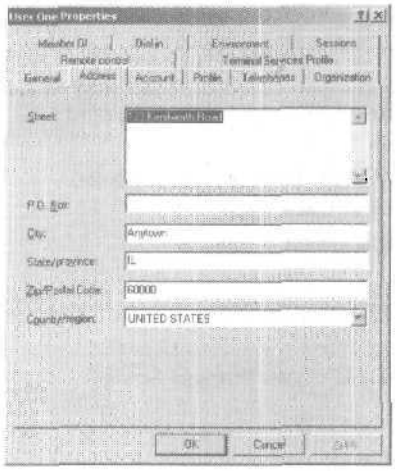


Рис. 7-6. Вкладка Address (Адрес) окна свойств учетной записи

Настройка свойств учетных записей

Для настройки свойств доменной учетной записи используется вкладка Account (Учетная запись) (рис. 7-7). Некоторые параметры доменных учетных записей совпадают для вкладок Account и New Object — User. В табл. 7-11 описаны дополнительные свойства учетных записей, недоступные при создании доменной учетной записи.

Табл. 7-11. Дополнительные параметры учетной записи

Параметр	Описание
Store Password Using Reversible Encryption (Хранить пароль, используя обратимое шифрование)	Позволяет войти в систему пользователям Macintosh. Компьютеры Macintosh только посылают этот тип команды
Smart Card is Required For Interactive logon (Для интерактивного входа в сеть нужна смарт-карта)	Позволяет пользователю войти в систему с использованием смарт-карты. Для этого требуется дополнительное аппаратное обеспечение — устройство считывания смарт-карт
Account is Trusted For Delegation (Учетная запись доверена для делегирования)	Позволяет пользователю присвоить права управления и администрирования части пространства имен другому пользователю, группе или организации
Account is Sensitive And Cannot Be Delegated (Учетная запись важна и не может быть делегирована)	Не допускает присвоения учетной записи для делегирования другой учетной записью
Use DES Encryption Types For This Account (Использовать для этой учетной записи типы шифрования DES)	Обеспечивается алгоритм шифрования DES

Табл. 7-11. Дополнительные параметры учетной записи *(окончание)*

Параметр	Описание
Do Not Require Kerberos Preauthentication (Без предварительной проверки подлинности Kerberos)	Отказ от предварительной аутентификации для учетных записей, использующих другую реализацию Kerberos. **Предварительную** аутентификацию используют не все реализации Kerberos
Account Expires (Срок действия учетной записи)	Устанавливается срок действия учетной записи. Щелкните переключатель Never (Не ограничен), если не хотите ограничивать срок действия учетной записи. Щелкните End Of (Истекает) и введите в поле дату окончания срока действия учетной записи, по истечении которого Windows 2000 автоматически отключит ее

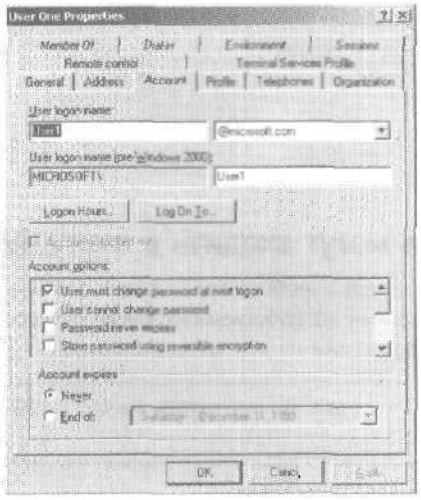


Рис. 7-7. Вкладка Account (Учетная запись) окна свойств учетной записи

Настройка времени входа

Для контроля за входом пользователя в домен задайте часы входа в систему — срок, в течение которого пользователям разрешается работать в сети. По умолчанию компьютер под управлением Windows 2000 доступен в любой день 24 часа в сутки. Можно разрешить вход только в рабочее время. Установка времени входа сокращает срок, в течение которого учетная запись открыта для несанкционированного доступа.

▶ **Настройка времени входа**

1. В окне свойств учетной записи на вкладке Account щелкните кнопку Logon Hours (Время входа),

   В одноименном окне голубым цветом отмечены часы, когда пользователю разрешено входить в систему. Белым отмечены часы, когда вход запрещен (рис. 7-8).
2. Чтобы разрешить или запретить доступ, проделайте следующие операции:
   - выберите прямоугольники, соответствующие дням и часам, для которых хотите разрешить доступ, щелкните время начала, перетащите на время окончания и щелкните переключатель Logon Permitted (Вход разрешен);

- выберите прямоугольники, соответствующие дням и часам, для которых хотите запретить доступ, щелкните время начала, перетащите на время окончания и щелкните переключатель Logon Denied (Вход запрещен);

3. Щелкните OK.

Важно помнить, что любые соединения с сетевыми ресурсами домена не прекращаются по окончании разрешенного времени пребывания пользователя в системе. Однако пользователь не сможет установить новые соединения.

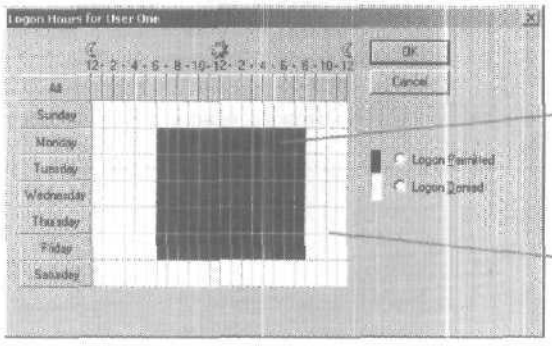


Рис. 7-8. Окно Logon Hours (Время входа)

Компьютеры, с которых пользователи могут входить в систему

По умолчанию пользователям разрешается входить в домен с любого компьютера домена. Потребуйте, чтобы пользователи входили на домен только с их собственных компьютеров. Это предотвратит их доступ к конфиденциальной информации на других компьютерах.

Примечание Чтобы контролировать компьютеры, с которых пользователь может войти на домен, необходимо включить NetBIOS поверх TCP/IP.

▶ **Определение рабочих станций для входа в систему**

1. В окне свойств на вкладке Account щелкните Log On To (Вход на).
2. В окне Logon Workstations (Рабочие станции для входа в систему) выберите параметр, определяющий, с какого компьютера пользователь может войти в систему (рис. 7-9).
3. Добавьте компьютеры, с которых пользователю разрешается войти в систему.

   Используйте заданное во время установки Windows 2000 имя компьютера, являющееся именем учетной записи компьютера в каталоге.
4. При необходимости удалите или отредактируйте имя компьютера, с которого пользователь может входить в систему.
5. Щелкните OK.

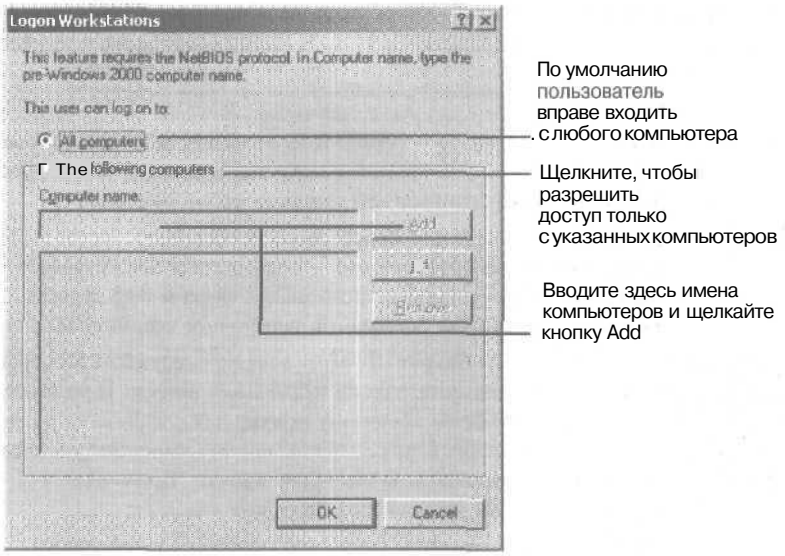


Рис. 7-9. **Окно Logon Workstations (Рабочие станции для входа в систему)**

Вкладка Dial-In

Вкладка Dial-In (Входящие звонки) позволяет контролировать, как пользователь выполняет телефонное подключение к сети. Для получения доступа к сети пользователь соединяется с компьютером, на котором работает служба Remote Access Service (RAS).

Примечание Помимо настройки параметров соединения и наличия службы RAS на сервере, к которому подсоединяется пользователь, надо настроить и коммутируемое соединение по телефону для сервера на компьютере клиента. Это поможет вам сделать мастер Network Connection (Мастер сетевого подключения), вызываемый из папки Network Connections (Сеть и удаленный доступ к сети) в окне My Computer (Мой компьютер).

В табл. 7-12 описаны параметры настройки безопасного коммутируемого соединения.

Табл. 7-12. **Параметры вкладки Dial-In окна свойств учетной записи**

Параметр	Описание
Allow Access (Разрешить доступ)	Включает доступ по телефонной линии или по виртуальной частной сети
Deny Access (Запретить доступ)	Отключает доступ по телефонной линии или по виртуальной частной сети
Control Access Through Remote Access Policy (Контролировать доступ с помощью политики удаленного доступа)	Определяет, что право удаленного доступа для этого пользователя контролируется посредством политики удаленного доступа
Verify Caller-ID (Проверять идентификатор)	Номер телефона, по которому пользователь подключается к сети по телефонной линии

Табл. 7-12. Параметры вкладки Dial-In окна свойств учетной записи *(окончание)*

Параметр	Описание
Callback Options (параметры ответного вызова)	Методы обратного вызова, в том числе: *No Callback (Ответный вызов не выполняется)* — сервер RAS не будет звонить пользователю, и пользователю придется оплачивать расходы на телефонное соединение. Этот параметр принят по умолчанию; *Set By Caller (Routing and Remote Access Service Only) (Устанавливается вызывающим)* — пользователь предоставляет телефонный номер для ответного звонка службы RAS сервера. Компания оплачивает расходы на телефонное соединение; *Always Callback To (Всегда по этому номеру)* — служба RAS сервера перезванивает пользователю по указанному номеру. Пользователь должен находиться по заданному номеру для соединения с сервером, что снижает риск того, что соединение выполнит уполномоченное лицо, поскольку номер задан заранее. Применяется в среде с высоким уровнем безопасности
Assign A Static IP Address (Присвоить статический IP-адрес)	Игнорируются параметры группового профиля телефонного соединения, и этому пользователю присваивается статический адрес TCP/IP
Apply Static Routes (Применять статические маршруты)	Конфигурируются заданные заранее маршруты для односторонних маршрутизируемых удаленных соединений по требованию
Static Routes (Статическиемаршруты)	Позволяет задать статические маршруты

Практикум: изменение свойств учетной записи

Измените свойства учетной записи. Настройте время входа и срок действия учетной записи для нескольких из созданных на предыдущем занятии учетных записей. Добавьте эти учетные записи в группу Print Operators (Операторы печати), чтобы эти учетные записи получили право входить на контроллер домена. Протестируйте ограничения времени входа, ограничения пароля, заданные при создании записей, и срок действия учетной записи.

Упражнение 1: настройка времени входа и срока действия учетной записи

Задайте время, в течение которого пользователи User3 и User5 могут входить на компьютер, и для пользователя User5 задайте срок действия учетной записи.

Сценарий

Измените параметры учетных записей согласно сведениям из табл. 7-13.

Табл. 7-13. Свойства учетной записи для упражнения 1

Учетная запись	Время входа	Срок действия учетной записи
User3	**18.00 – 6.00, с понедельника по пятницу**	
User5		Сегодня

Внимание! Чтобы выполнить следующее задание, зарегистрируйтесь как Administrator (Администратор), запустите консоль Active Directory Users and Computers и раскройте домен в дереве консоли.

▶ Задание 1: определите время входа

1. В дереве консоли Active Directory Users and Computers (Active Directory — пользователи и компьютеры) раскройте папку Users.
2. На правой панели щелкните правой кнопкой параметр User Three и выберите в контекстном меню команду Properties (Свойства),

   Откроется окно User Three Properties (Свойства: User Three), вкладка General (Общие).

   Какую информацию, кроме имени и фамилии, можно задать для учетной записи на вкладке General? Для чего нужна эта информация?
3. На вкладке Account (Учетная запись) щелкните кнопку Logon Hours (Время входа).

   Откроется окно Logon Hours For User Three (Время входа для User Three).

   В какое время пользователю User Three разрешается войти в систему?
4. Чтобы ограничить время входа пользователя, щелкните время начала первого интервала, в течение которого хотите запретить пользователю вход, и перетащите указатель на конечное время этого интервала.

   Все квадраты, соответствующие часам выбранного интервала будут обведены рамкой,

   Примечание Чтобы выбрать такой же интервал времени для всех дней недели выше строки Sunday (Воскресенье), щелкните серый квадрат, соответствующий началу периода, и перетащите указатель на время окончания. Чтобы выбрать день полностью, щелкните серый квадрат с названием дня.
5. Щелкните переключатель Logon Denied (Вход запрещен).

   Выделенный период изменит цвет на белый. Это означает, что пользователю запрещен вход в систему в течение этого срока.
6. Повторяйте пункты 4—5, пока не будут разрешены только нужные часы входа.
7. Щелкните OK, чтобы закрыть окно Logon Hours For User Three.
8. В окне User Three Properties щелкните OK, чтобы применить параметры и вернуться в консоль Active Directory Users and Computers.

▶ Задание 2: задайте срок действия учетной записи

1. В дереве консоли Active Directory Users and Computers (Active Directory — пользователи и компьютеры) щелкните папку Users (Пользователи).
2. На правой панели щелкните правой кнопкой User Five и выберите команду Properties (Свойства).

   Откроется окно User Five Properties (Свойства: User Five) на вкладке General (Общие).
3. Щелкните вкладку Account (Учетная запись).

   Когда окончится срок действия учетной записи?
6. Щелкните переключатель End Of (Истекает) и задайте текущую дату.
7. Щелкните OK, чтобы применить параметры и вернуться в консоль Active Directory Users and Computers.
8. Закройте окно консоли Active Directory Users and Computers и завершите сеанс Windows 2000.

Упражнение 2: тестирование учетных записей

Вы войдете под каждой из созданных на предыдущих занятиях учетных записей и протестируете результаты изменения параметров.

▶ Задание 1: протестируйте возможности входа в систему под каждой учетной записью

1. Попытайтесь войти как User1 без пароля.

   Отобразится информационное окно Logon Message (Сообщение о результатах входа) с требованием изменить пароль.
2. В окне Change Password (Смена пароля) не заполняйте поле Old Password (Старый пароль), а в поля New Password (Новый пароль) и Confirm New Password (Подтверждение) введите **student.**

   Появится сообщение, что пароль был изменен.
3. Щелкните OK, чтобы закрыть окно сообщения.

   Удалось ли вам войти в систему? Почему?

Существуют несколько способов разрешить пользователям входить на контроллер домена. В следующем задании добавьте пользователей в группу Print Operators (Операторы печати), поскольку этой группе разрешен вход на контроллер домена. Только пользователи, принадлежащие к определенным административным группам, имеют право интерактивно входить на контроллер домена. Группа — это набор учетных записей, группы упрощают администрирование, позволяя назначать разрешения нескольким пользователям одновременно, а не каждому индивидуально. О группах также рассказано в главе 8.

▶ Задание 2: добавьте пользователей в группу Print Operators

1. Зарегистрируйтесь как Administrator (Администратор).
2. В дереве консоли Active Directory Users and Computers (Active Directory — пользователи и компьютеры) щелкните папку Users.
3. На правой панели щелкните правой кнопкой User One и выберите команду Properties (Свойства).

   Откроется окно User One Properties (Свойства: User One), вкладка General (Общие).
4. Щелкните вкладку Member Of (Член группы).
5. Щелкните кнопку Add (Добавить).

   Откроется окно Select Groups (Выбор: Группа).
6. Щелкните Print Operators (Операторы печати), щелкните кнопку Add (Добавить), затем — OK.
7. Щелкните OK, чтобы закрыть окно User One Properties.
8. Повторите пункты 3—7 для пользователей User3, User5, User7 и User9.
9. Закройте окно консоли Active Directory Users and Computers и завершите рабочий сеанс.

▶ Задание 3: протестируйте параметры времени входа

1. Попытайтесь войти в систему как Userl с паролем student.

   Удалось ли вам войти в систему? Почему?
2. Завершите сеанс и попытайтесь войти как User3 без пароля.
3. В открывшемся окне измените пароль на **student.**

   Удалось ли вам войти в систему? Почему?

▶ Задание 4: протестируйте параметры пароля

1. Попытайтесь войти в систему как User7 без пароля.

   Удалось ли вам войти в систему? Почему?

2. Попытайтесь войти в систему как User7 с паролем User7.
3. В открывшемся окне измените пароль на **student.**
   Удалось ли вам войти в систему? Почему?
4. Завершите сеанс.
5. Попытайтесь войти в систему как User9 с паролем User9.
   Удалось ли вам войти в систему? Почему?

► Задание 5: протестируйте параметры пароля, попытавшись изменить его

1. Нажмите Ctrl+Alt+Delete.
   Откроется окно Windows Security (Безопасность Windows).
2. Щелкните кнопку Change Password (Смена пароля).
   Откроется одноименное окно.
3. В поле Old Password (Старый пароль) введите пароль для учетной записи User9, а в полях New Password (Новый пароль) и Confirm New Password (Подтверждение) введите **student** и щелкните OK.
   Удалось ли вам изменить пароль? Почему?
4. Щелкните OK, чтобы закрыть окно Change Password, затем щелкните кнопку Cancel (Отмена), чтобы вернуться в окно Windows Security.
5. Щелкните кнопку Log Off (Завершение работы).
   Откроется окно Log Off Windows (Завершение работы Windows), запрашивая подтверждение на выход из системы.
6. Щелкните OK, чтобы выйти из системы.

► Задание 6: протестируйте срок действия учетной записи

1. Попытайтесь войти в систему как User5.
2. В появившемся окне измените пароль на **student**.
   Удалось ли вам войти в систему? Почему?
3. Выйдите из Windows 2000.

► Задание 7: измените системное время

1. Войдите в домен как Administrator (Администратор), раскройте меню Start\Settings (Пуск\Настройка) и щелкните ярлык Control Panel (Панель управления).
2. На панели управления дважды щелкните значок Date/Time (Дата и время).
   Откроется окно Date/Time Properties (Свойства: дата и время).
3. В поле Date (Дата) введите завтрашнюю дату и щелкните OK, чтобы применить изменения и вернуться в панель управления.
4. Закройте окно панели управления и завершите сеанс.

► Задание 8: протестируйте срок действия учетной записи

1. Попытайтесь войти в систему как User5 с паролем student.
   Удалось ли вам успешно войти в систему? Почему?

► Задание 9: измените системное время

1. Войдите в домен как Administrator (Администратор), раскройте меню Start\Settings (Пуск\Настройка) и щелкните ярлык Control Panel (Панель управления).
2. На панели управления дважды щелкните значок Date/Time.
   Откроется окно Date/Time Properties.

3. В поле Date (Дата) введите сегодняшнюю дату и щелкните OK, чтобы применить изменения и вернуться в панель управления.
4. Закройте окно панели управления и выйдите из Windows 2000.

Резюме

Локальные учетные записи создаются с помощью оснастки Local Users and Groups (Локальные пользователи и группы), встроенной в консоль Computer Management (Управление компьютером), а доменные учетные записи — с помошью консоли Active Directory Users and Computers (Active Directory — пользователи и компьютеры). Доменная учетная запись всегда создается на первом доступном контроллере домена, к которому обращается консоль MMC, а затем реплицируется на остальные контроллеры.

С каждой создаваемой учетной записью ассоциируется набор свойств по умолчанию. Для доменных учетных записей эти свойства эквивалентны атрибутам объектов, их можно применять для поиска пользователей домена в каталоге.

Выполняя практикум, вы создали пять доменных учетных записей, настроили их свойства, в том числе изменили время входа, задали срок действия учетной записи и разрешение или запретили пользователю менять пароль. Заданные свойства вы протестировали.

Занятие 4. Создание профиля пользователя

Профиль пользователя (user profile) — набор папок и данных, где хранятся параметры состояния рабочего стола и приложений, а также личные данные. Там же хранится информация о сетевых подключениях, которые следует инициировать после входа в систему, & также сведения о содержимом меню Start (Пуск) и о дисках, подключенных к сетевым серверам. Профили пользователей обеспечивают тот вид рабочего стола для каждого пользователя, что и в предыдущий сеанс. На этом занятии мы расскажем о профилях пользователей и разнице между локальными, перемещаемыми и обязательными профилями.

Изучив материал этого занятия, вы сможете:

- ✓ объяснить разницу между локальными, перемещаемыми и обязательными профилями;
- ✓ настроить локальный, перемещаемый и обязательный профиль пользователя.

Продолжительность занятия — около 45 минут.

Возможности профиля пользователя

На компьютерах под управлением Windows 2000 профили пользователей автоматически создают и поддерживают параметры рабочего стола для каждого пользователя на локальном компьютере.

Преимущества профилей пользователей:

- на компьютере могут работать несколько пользователей, причем каждый из них настраивает рабочий стол «под себя»;
- параметры рабочего стола пользователя сохраняются с предыдущего сеанса;
- изменение среды рабочего стола одним пользователем не влияет на параметры других пользователей;
- профили пользователей можно хранить на сервере и передавать их на любой компьютер под управлением Windows NT 4.0 или Windows 2000 в сети. Такие профили называются *перемещаемыми* (roaming user profiles);
- сохраняются параметры работы приложений, сертифицированных для использования с Windows 2000.

В качестве средства управления профили пользователей предоставляют следующие возможности:

- позволяют создать профиль пользователя по умолчанию, предназначенный для решения задач конкретного пользователя;
- позволяют настроить *обязательный профиль пользователя* (mandatory user profile), который не сохраняет изменений рабочего стола, выполненных пользователем. Параметры обязательного профиля загружаются на локальный компьютер всякий раз, когда пользователь входит в систему;
- позволяют задать параметры профиля пользователя по умолчанию, которые будут включены во все индивидуальные профили пользователей.

Типы профилей

Существуют три типа профилей пользователей.

- **Локальный профиль пользователя.** Создается при первом входе в систему и хранится на локальном жестком диске компьютера. Все изменения, внесенные в локальный профиль, относятся только к тому компьютеру, на котором они сделаны.
- **Перемещаемый профиль пользователя.** Создается системным администратором и хранится на сервере. Он доступен при подключении к любому компьютеру сети. Изменения, внесенные в перемещаемый профиль, обновляются на сервере.
- **Обязательный профиль пользователя.** Это перемещаемый профиль, который можно применять для задания параметров для отдельных пользователей или групп пользователей. Только системные администраторы имеют право вносить в него изменения.

Параметры, хранящиеся в профиле пользователя

Профиль пользователя содержит параметры конфигурации и параметры для каждого пользователя — копию рабочего стола пользователя (табл. 7-14).

Табл. 7-14. Параметры, хранящиеся в профиле пользователя

Параметр	Источник
Все задаваемые пользователем параметры Windows Explorer	Windows Explorer (Проводник)
Документы пользователя	Папка My Documents (Мои документы)
Рисунки пользователей	Папка My Pictures (Мои рисунки)
Ярлыки избранных страниц Интернета	Папка Favorites (Избранное)
Подключенные пользователями сетевые диски	Подключенные сетевые диски
Связи с другими компьютерами сети	Папка My Network Places (Мое сетевое окружение)
Содержимое рабочего стола и ярлыки	Папка Desktop (Рабочий стол)
Заданные пользователем параметры цветов и текста экрана	Цвета и шрифты экрана
Данные приложений и заданные пользователем параметры конфигурации	Папка Application data и соответствующий куст реестра
Подключения к сетевым принтерам	Папка PrintHood
Все заданные пользователем параметры панели управления	Control Panel (Панель управления)
Все параметры программ, влияющих на среду Windows, включая Calculator, Clock, Notepad и Paint	Папка Accessories (Стандартные)

Табл. 7-14. Параметры, хранящиеся в профиле пользователя (*окончание*)

Параметр	Источник
Параметры программ, написанных специально для Windows 2000	Программы на базе Windows 2000
Любые закладки, помещенные в справочную систему Windows 2000	Интерактивные закладки пользователей

Содержимое профиля пользователя

Локальные профили хранятся в папке C:\Documents and Settings*регистрационное_имя_пользователя*, где C:\ — имя системного диска, а *регистрационное_имя_пользователя* — имя, которое пользователь вводит при входе в систему. Перемешаемые профили хранятся в общей папке на сервере. В табл. 7-15 показан пример содержимого папки профиля пользователя.

Табл. 7-15. Пример содержимого папки профиля пользователя

Папка	Описание
Application Data*	Специальные данные программ, например словарь. Разработчики программ решают, какие данные хранить в папке профиля пользователя
Cookies	Учетная информация, введенная пользователем при посещении разных узлов Интернета
Desktop (Рабочий стол)	Элементы рабочего стола, включая файлы, ярлыки и папки
Favorites (Избранное)	Ссылки на любимые страницы в Интернете
FrontPageTempDir	Временная папка, используемая Microsoft Front Page
Local Settings*	Данные приложений, файлы History и Temporary. Данные приложений можно перемешать на другой компьютер аналогично профилям
My Documents (Мои документы)	Документы пользователя
My Pictures (Мои рисунки)	Рисунки пользователя
NetHood*	Ярлыки элементов My Network Places
PrintHood*	Ярлыки элементов папки принтера
Recent*	Ярлыки к документам и папкам
SendTo*	Ярлыки к утилитам работы с документами
Start Menu (Главное меню)	Ярлыки к элементам программ
Templates (Шаблоны)	Элементы шаблонов пользователей
NTUSER.DAT*	Хранит параметры реестра пользователя

* Скрытый элемент.

В папке My Documents собраны вместе все параметры и личные документы пользователя; она является частью профиля пользователя. Windows 2000 автоматически создает папку My Documents, которая по умолчанию хранит данные пользователя для приложений Microsoft. Домашние папки могут также содержать файлы и программы для пользователей.

Локальные профили пользователей

Windows 2000 создает локальный профиль пользователя при первом входе пользователя на компьютер и хранит его на этом компьютере. Локальный профиль пользователя хранится в папке C:\Documents and Settings*регистрационное_имя_пользователя*, где C:\ — это имя системного диска, а *регистрационное_имя_пользователя* — имя, которое пользователь вводит при входе в систему. Когда пользователь входит на клиентский компьютер под управлением Windows 2000, он всегда получает собственную рабочую среду независимо от того, сколько пользователей помимо него работает на этом компьютере.

Пользователь изменяет локальный профиль, корректируя параметры рабочего стола. Например, он может создать новое сетевое соединение или добавить файл в папку My Documents. После выхода пользователя из системы Windows 2000 собирает все изменения в профиль пользователя, хранящийся на компьютере. При следующем входе пользователя генерируются новые сетевое соединение и файл.

Перемещаемые профили пользователей

Для поддержки пользователей, работающих на нескольких компьютерах, стоит создать перемещаемые профили пользователей. Этот профиль, создаваемый на сетевом сервере, доступен пользователю независимо от того, с какого компьютера тот входит в домен. В этом его отличие от локального профиля, действующего только на одном клиентском компьютере.

Когда пользователь входит в систему, Windows 2000 копирует перемещаемый профиль пользователя с сетевого сервера на клиентский компьютер и применяет его параметры к этому компьютеру. При первом входе пользователя на компьютер Windows 2000 копирует все документы на локальный компьютер. Далее, когда пользователь входит на компьютер, Windows 2000 сравнивает локально хранящиеся файлы профиля пользователя и файлы перемещаемого профиля. Он копирует только файлы, измененные с момента последнего входа пользователя на компьютер, что ускоряет процесс входа в систему.

Когда пользователь выходит из системы, Windows 2000 копирует изменения, внесенные в локальную копию перемещаемого профиля пользователя, обратно на сервер, где хранится профиль.

Стандартные перемещаемые профили пользователей

Можно создать стандартный перемещаемый профиль для группы пользователей, настроив рабочий стол и скопировав стандартный профиль на место перемещаемого профиля пользователя.

Стандартные перемещаемые профили:

- обеспечивают стандартную среду рабочего стола для нескольких пользователей, выполняющих сходные задачи, например применяющих одни и те же сетевые ресурсы;
- поддерживают рабочую среду пользователя, включающую только необходимые для работы соединения и приложения;
- облегчают устранение ошибок: зная параметры рабочих столов пользователей, специалисты службы технической поддержки быстро найдут отклонение или проблему.

Создание перемещаемых профилей пользователей

Храните перемещаемые профили на часто архивируемом сервере. Для ускорения входа в систему в сильно загруженной сети поместите папку перемещаемого профиля на рядовой сервер, а не на контроллер домена. Копирование перемещаемых профилей с сервера на компьютеры клиентов иногда занимает значительную часть полосы пропускания сети и увеличивает нагрузку на процессоры компьютеров. Хранение профилей на контроллере домена замедляет аутентификацию пользователей в домене.

Примечание Для успешного создания перемещаемых профилей и назначения домашних папок для учетных записей необходимо иметь право администрировать контейнерный объект, в котором находятся учетные записи.

► **Задание: настройте перемещаемый профиль пользователя**

1. На сервере создайте общую папку и используйте путь следующего формата: *\\имя_сервера\имя_общей_папки*.
2. На вкладке Profile (Профиль) окна свойств учетной записи (рис. 7-10) задайте путь к общей папке в поле Profile Path (Путь профиля) (например, *\\имя_сервера\имя_общей_папки\регистрационное_имя*).

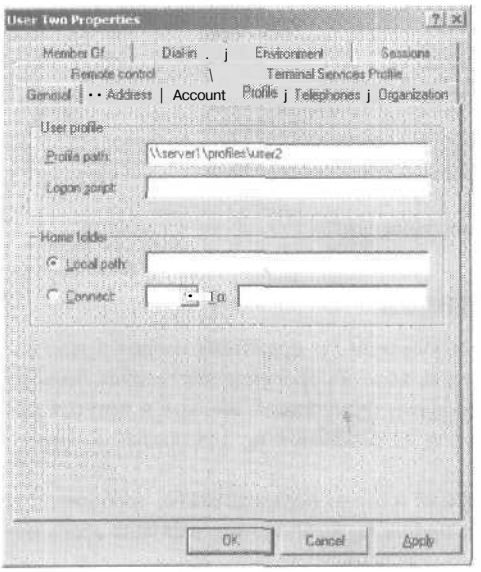


Рис. 7-10. Путь к профилю для перемещаемого профиля

Вместо регистрационного имени пользователя можно ввести переменную *%username%* — Windows 2000 автоматически заменит ее на имя учетной записи для перемещаемого профиля, что удобно при копировании учетных записей шаблонов.

Создание стандартного перемещаемого профиля пользователя

Вот как задают стандартный перемещаемый профиль для группы пользователей.

1. Создайте шаблон профиля пользователя соответствующей конфигурации. Для этого создайте учетную запись с помощью консоли Active Directory Users and Computers и настройте для нее рабочий стол.

2. Создайте на сервере общую папку, которая позволит пользователям получить доступ к шаблону профиля с удаленного компьютера.
3. Скопируйте шаблон профиля пользователя в общую папку на сервере и задайте пользователей, которые будут иметь право применять профиль, на вкладке User Profile (Профиль пользователя) окна System Properties (Свойства системы) в консоли управления (рис. 7-11).
4. Задайте путь к шаблону профиля на вкладке Profile окна свойства объекта пользователя (рис. 7-10).

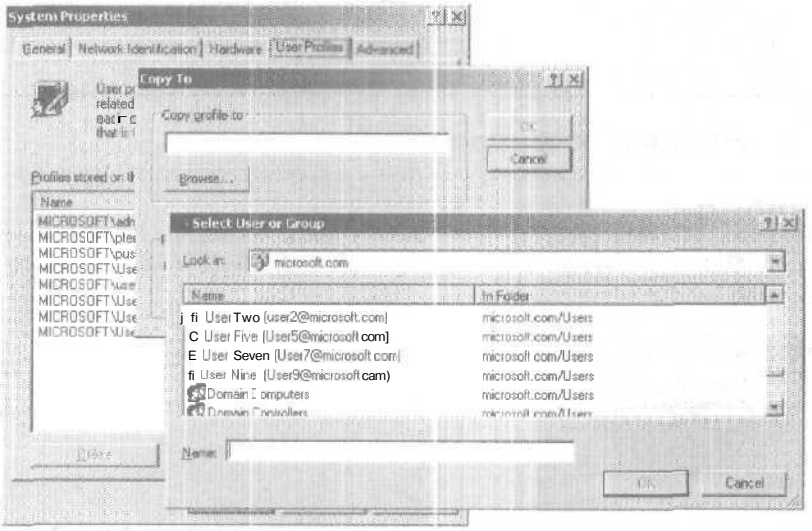


РИС. 7-11. Копирование шаблона профиля пользователя

Обязательные профили пользователей

Так называют профиль «только для чтения». Пользователи по-прежнему имеют право изменять параметры своего рабочего стола, но при выходе из системы эти коррективы не сохраняются. При следующем входе в систему профиль будет таким же, как и при предыдущей загрузке. Параметры обязательного профиля загружаются на локальный компьютер при каждом входе пользователя в систему.

Вы можете назначить один обязательный профиль многим пользователям, требования к рабочему столу которых совпадают. Изменив один профиль, вы измените рабочую среду нескольких пользователей.

Создание обязательного профиля пользователя

Скрытый файл в профиле (например, \SERVER1*общий_ресурс**регистрационное_имя_пользователя*), называемый NTUSER.DAT. содержит раздел системных параметров Windows 2000. применяемых к индивидуальной учетной записи и содержащих сведения о параметрах среды пользователя, например данные о внешнем виде рабочего стола. Этому файлу можно присвоить атрибут «только для чтения», изменив его название на NTUSER.MAN.

Практикум: работа с профилями пользователей

Настройте и протестируйте локальный профиль пользователя. Создайте и протестируйте стандартный перемещаемый профиль пользователя.

Упражнение 1: настройка локального профиля пользователя

Создайте локальную учетную запись и профиль, затем просмотрите, определите и протестируйте профиль.

► Задание 1: создайте учетную запись

1. Войдите в систему как Administrator (Администратор).
2. В консоли Active Directory Users and Computers создайте учетную запись puser (табл. 7-16). В списке справа от поля User Logon Name (Имя входа пользователя) выберите @microsoft.com.

Табл. 7-16. Параметры учетной записи puser для упражнения 1

First Name (Имя)	Last Name (Фамилия)	User Logon Name (Имя входа пользователя)	Password (Пароль)	Member Of (Член группы)
Profile	User	puser	Отсутствует	Print Operators (Операторы печати)

3. Выйдите из Windows 2000.

► Задание 2: создайте локальный профиль пользователя

1. Войдите в домен как puser.

   При первом входе в Windows 2000 локальный профиль пользователя создается с параметрами, заданными по умолчанию. Вход в систему в качестве puser создает локальный профиль пользователя.
2. Выйдите из Windows 2000.

► Задание 3: просмотрите существующие профили

1. Войдите в домен как Administrator (Администратор).
2. Раскройте меню Start\Settings (Пуск\Настройка), щелкните ярлык Control Panel (Панель управления) и в панели управления дважды щелкните значок System (Система).

   Откроется окно System Properties (Свойства системы).
3. Перейдите на вкладку User Profiles (Профили пользователей).

   Какие профили пользователей хранятся на вашем компьютере?
4. Щелкните OK, чтобы закрыть окно System Properties, затем закройте панель управления.
5. Выйдите из Windows 2000.

► Задание 4: определите и протестируйте локальный профиль

1. Войдите в домен как puser.
2. Щелкните правой кнопкой рабочий стол и выберите команду Properties (Свойства).

   Откроется окно Display Properties (Свойства: Экран).
3. Перейдите на вкладку Appearance (Оформление),

   Обратите внимание на текущую цветовую схему.
4. В списке Scheme (Схема) выберите другую схему и щелкните OK.

Рабочий стол немедленно изменится в соответствии с новой цветовой схемой.

5. Выйдите из системы и вновь войдите как puser.
   Сохранились ли цвета экрана? Почему?
6. Завершите сеанс.

Упражнение 2: определение стандартного перемещаемого профиля пользователя

Сейчас вы создадите общую папку, в которой может храниться стандартный перемещаемый профиль пользователя. Создайте учетную запись с именем Profile Template, которая будет служить моделью для стандартного перемещаемого профиля. Задайте параметры для профиля шаблона. Скопируйте профиль пользователя Profile Template в общую папку для User2. Задайте путь к профилю для User2. Вы можете протестировать стандартный профиль, если имеете доступ к двум компьютерам сети.

▶ Задание 1: создайте общую папку для хранения перемещаемых профилей пользователей

Примечание Общие папки подробно рассматриваются в главе 1. Сейчас вы создадите общую папку для совместного использования профилей пользователей.

1. Войдите в домен как Administrator (Администратор) на контроллере домена.
2. В папке C:\ (где C:\ — имя вашего системного диска) создайте папку с именем Profiles.
3. Щелкните правой кнопкой папку Profiles и выберите команду Properties (Свойства).
4. В окне Profiles Properties (Свойства: Profiles) перейдите на вкладку Sharing (Доступ).
5. Щелкните переключатель Share This Folder (Открыть общий доступ к этой папке), затем — кнопку Permissions (Разрешения).
6. В окне Permissions For Profiles (Разрешения для профилей) убедитесь, что выбрана группа Everyone (Все) и отмечен флажок Full Control (Полный контроль), и щелкните OK.
7. В окне Profiles Properties (Свойства: Profiles) щелкните OK.

▶ Задание 2; создайте шаблон профиля пользователя

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Active Directory Users and Computers (Active Directory — пользователи и компьютеры).
2. В консоли Active Directory Users and Computers создайте учетную запись ptemplate (табл. 7-17). В списке справа от поля User Logon Name (Имя входа пользователя) выберите @microsoft.com. Добавьте ptemplate к группе Print Operators (Операторы печати), чтобы пользователь мог войти в контроллер домена.
3. Выйдите из Windows 2000.
4. Войдите в систему как ptemplate.

   Локальный профиль пользователя автоматически создается для пользователей Profile Template на локальном компьютере в папке C:\Documents and Settings*регистрационное _имя_пользователя* (где C:\ — это имя вашего системного диска).

Табл. 7-17. Параметры учетной записи ptemplate для упражнения 2

First Name (Имя)	Last Name (Фамилия)	User Logon Name (Имя входа пользователя)	Password (Пароль)	Member Of (Член группы)
Profile	Template	ptemplate	Отсутствует	PrintOperators (Операторы печати)

5. Щелкните правой кнопкой рабочий стол и выберите команду Properties (Свойства). Откроется окно Display Properties (Свойства: Экран).
7. Перейдите на вкладку Appearance (Оформление).
   Обратите внимание на текущую цветовую схему.
8. В списке Scheme (Схема) выберите другую схему и шелкните OK.
   Рабочий стол немедленно изменится в соответствии с новой цветовой схемой.
9. Выйдите из системы и вновь войдите как ptemplate.
   Заметьте: цвета экрана сохранились в профиле пользователя.
10. Завершите сеанс Windows 2000.

▶ **Задание 3: скопируйте шаблон профиля в общую папку на сетевом сервере**

1. Войдите в систему как Administrator (Администратор).
2. Воспользуйтесь консолью Active Directory Users and Computers (Active Directory — пользователи и компьютеры) для создания учетной записи User2 (табл. 7-18). В списке справа от окна User Logon Name (Имя входа пользователя) выберите @microsoft.com. Добавьте User2 к группе Print Operators (Операторы печати), чтобы пользователь мог зарегистрироваться на контроллере домена.

Табл. 7-18. Параметры учетной записи User2 для упражнения 2

First Name (Имя)	Last Name (Фамилия)	User Logon Name (Имя входа пользователя)	Password (Пароль)	Member Of (Член группы)
User	Two	User2	Отсутствует	Print Operators (Операторы печати)

3. Раскройте меню Start\Settings (Пуск\Настройка) и шелкните ярлык Control Panel (Панельуправления).
4. На панели управления дважды шелкните значок System (Система).
   Откроется окно System Properties (Свойства системы).
5. Перейдите на вкладку User Profiles (Профили пользователей).
   Заметьте: были созданы профили для всех пользователей, ранее входивших на компьютер, в том числе и профиль пользователя MICROSOFT\ptemplate.
6. В списке Profiles Stored On This Computer (Профили, хранящиеся на этом компьютере) шелкните MICROSOFT\ptemplate, затем — Copy To (Копировать).
7. В открывшемся окне в поле Copy Profile To (Копировать профиль на) введите *имя_компьютера*\profiles\user2 (где *имя_компьютера* — это SERVER1 или имя вашею компьютера). Это местоположение общей папки, где будет храниться шаблон профиля.

▶ **Задание 4: определите пользователей, имеющих право применять профиль**

1. В окне Copy To (Копирование профиля) в области Permitted To Use (Разрешить использование) щелкните кнопку Change (Изменить).

   Откроется окно Select User Or Group (Выбор: Пользователь или группа).
2. В столбце Name (Имя) щелкните User Two, затем — OK.

   В столбце Permitted To Use окна Copy To появится строка MICROSOFT\user2.
3. Щелкните OK.

   В Windows Explorer (Проводник) просмотрите Profiles\user2. Обратите внимание на папки для параметров рабочего стола, хранящиеся в папке Profiles.

▶ **Задание 5: задайте путь к перемещаемому профилю пользователя**

1. В консоли Active Directory Users and Computers дважды щелкните User Two.

   Откроется окно User Two Properties (Свойства: User Two).
2. Перейдите на вкладку Profile (Профиль).
3. В поле Profile path (Путь к профилю) введите *имя_компьютера*\profiles\user2 (где *имя_компьютера* — это SERVER1 или имя вашего компьютера).
4. Щелкните OK.
5. Закройте консоль Active Directory Users and Computers.

Примечание Чтобы сделать профиль обязательным, введите действительное имя профиля, например, \\server1\profiles\user2\ntuser.man.

- Если пользователи будут входить на компьютер с Windows NT или Windows 2000, а не с Windows 3.1, то в пути к профилю не нужно указывать имя файла.
- Если пользователи будут входить на компьютер под управлением Windows NT 3.1, а также Windows NT 4.0 или Windows 2000, то путь к профилю должен содержать имя файла.
- Если пользователи будут входить только на компьютер под управлением Windows 2000, путь к профилю должен представлять собой имя папки и не должен включать расширение .man. Если заданная в пути папка не существует, то она автоматически создается при первом входе пользователя в систему.

▶ **Задание 6: протестируйте перемещаемый профиль**

1. Выйдите из системы и войдите как User2.

   Совпадают ли или отличаются цвета экрана и рабочий стол от заданных в Profile Template? Почему?

▶ **Задание 7: определите тип профиля, назначенного пользователю**

1. Выйдите из системы, войдите как Administrator (Администратор) и запустите панель управления.
2. Дважды щелкните строку System (Система) и перейдите на вкладку User Profiles (Профили пользователей).

   Какие типы профиля перечислены для учетной записи User2?
3. Выйдите из всех программ и из Windows 2000.

Примечание Если вы имеете доступ к двум компьютерам в сети, выполните эту процедуру на втором компьютере.

► Задание 8: протестируйте перемещаемый профиль с другого компьютера

1. Войдите на второй компьютер как User2.
2. Если откроется окно со списком параметров профиля, щелкните кнопку Download (Загрузить).

   Заметьте: цвета экрана те же, что и на первом компьютере, потому что перемещаемый профиль для шаблонной учетной записи загружается с сервера и применяется к компьютеру, где регистрируются под этой записью.
3. Выйдите со второго компьютера.

► Задание 9: удалите профиль пользователя Profile Template

1. На вкладке User Profiles (Профили пользователей) в списке Profiles Stored On This Computer (Профили, хранящиеся на этом компьютере) щелкните профиль MICROSOFT\ptemplate, затем — кнопку Delete (Удалить).

   Откроется окно сообщения Confirm Delete (Подтвердить удаление).
2. Щелкните кнопку Yes (Да), чтобы удалить локальный профиль.

   Профиль пользователя Profile Template будет удален с локального компьютера.

Резюме

Профиль пользователя — это набор папок и данных, хранящих данные о текущей среде рабочего стола пользователя и параметры приложений, а также личные данные. Профиль пользователя содержит также все сведения обо всех сетевых соединениях, которые возобновляются при входе пользователя на компьютер, например элементы меню Start (Пуск) и подключенные к сетевым серверам диски.

Существуют три типа профилей пользователей: локальный, перемещаемый и обязательный. Локальный профиль создается при первом входе в систему и хранится на локальном жестком диске компьютера. Все изменения, вносимые в локальный профиль, действительны только на том компьютере, где они сделаны. Перемещаемый профиль создается системным администратором и хранится на сервере. Этот профиль доступен при входе на любой компьютер сети. Вносимые в него коррективы обновляются на сервере. Обязательный профиль — это перемещаемый профиль, который применяется для задания определенных параметров индивидуальным пользователям или группам пользователей. Изменять его разрешено только системным администраторам.

Выполнив практикум, вы создали локальную учетную запись и профиль, который вы затем просмотрели, определили и протестировали. Также вы создали стандартный перемещаемый профиль пользователя, в том числе модель учетной записи пользователя в качестве шаблона профиля, скопировали шаблон профиля в общую папку на сервере и определили путь к профилю.

Занятие 5. Создание домашних папок

Хотя по умолчанию все документы пользователей хранятся в папке My Documents (Мои документы), Windows 2000 предоставляет еще одну возможность для их хранения — домашнюю папку.

Изучив материал этого занятия, вы сможете:

- ✓ работать с домашними папками.

Продолжительность занятия — около 5 минут.

Знакомство с домашними папками

Домашняя папка (home directory) — это дополнительная папка, позволяющая пользователям хранить личные документы, а старым приложениям — сохранять документы по умолчанию. Домашняя папка располагается на клиентском компьютере или в общей папке на файловом сервере. Поскольку домашняя папка не является частью перемещаемого профиля пользователя, ее размер не влияет на сетевой трафик при входе в систему. Вы можете разместить все домашние папки централизованно на сетевом сервере.

Хранение всех домашних папок на файловом сервере дает ряд преимуществ:

- пользователи получают доступ к своим домашним папкам с любого компьютера в сети;
- поддержка и администрирование документов пользователя выполняется централизованно;
- домашние папки доступны с компьютера клиента, на котором работает любая ОС Microsoft (в том числе MS-DOS, Windows 9x/2000).

Примечание Храните домашние папки на томе NTFS — это позволит вам задавать разрешения NTFS для зашиты документов пользователей. Если домашние папки хранятся на томе FAT, доступ к ним ограничивается только посредством разрешений доступа к общим папкам.

Создание домашних папок на сервере

Для успешного создания домашних папок необходимо иметь разрешение на администрирование контейнерного объекта, где расположена учетная запись пользователя. Для создания домашней папки на файловом сервере в сети выполните следующие действия:

- создайте и откройте совместный доступ к папке, в которой собираетесь хранить все домашние папки на сетевом сервере. Домашняя папка для всех пользователей будет вложена в эту общую папку;
- для общей папки отмените разрешение по умолчанию Full Control (Полный доступ) для группы Everyone (Все) и назначьте его группе Users (Пользователи). Это гарантирует, что доступ к общей папке получат только пользователи с доменными учетными записями;
- укажите путь на вкладке Profile (Профиль) диалогового окна свойств учетной записи в группе Home folder (Домашняя папка) (рис. 7-12). Поскольку домашняя папка находится на сетевом сервере, щелкните Connect (Подключить) и укажите букву подключаемого диска. В поле To (к) задайте имя UNC, например *\\имя_сервера\имя_общей_папки\регистрационное_имя_пользователя*. В качестве имени пользователя укажите переменную *%username%*, чтобы автоматически присвоить имя и создать домашнюю папку пользователя с тем же именем, под каким он входит в систему. Например, введите ***\\имя_сервера***\Users*%username%*.

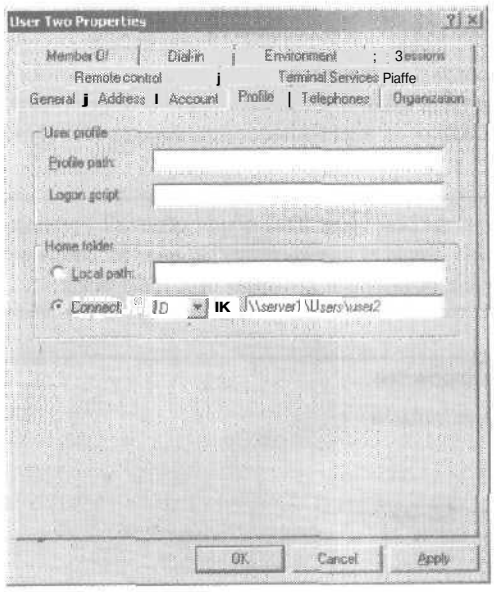


Рис. 7-12. Задание пути к домашней папке

Если вы задаете имя папки на томе NTFS с помощью переменной *%username%*, пользователь получит для нее разрешение Full Control. Все другие разрешения для этой папки удаляются, в том числе и права для учетной записи Administrator.

Резюме

Помимо папки My Documents (Мои документы), Windows 2000 позволяет создать домашнюю папку для хранения личных документов пользователей. Домашнюю папку можно создать на клиентском компьютере или в общей папке на файловом сервере. Поскольку домашняя папка не является частью перемещаемого профиля пользователя, ее размер не влияет на сетевой трафик при входе в систему.

Хранение всех домашних папок на файловом сервере дает ряд преимуществ. Во-первых, пользователи могут получить доступ к своим домашним папкам с любого компьютера в сети. Во-вторых, централизуются поддержка и администрирование документов пользователя. В-третьих, домашние папки доступны с компьютера клиента, на котором работает любая ОС Microsoft (включая MS-DOS, Windows 9x/2000).

Занятие 6, Изменение учетных записей

Иногда требуется изменить учетные записи согласно новым требованиям организации или при смене персональной информации, например фамилии или почтового адреса пользователя. Кроме того, в некоторых случаях приходится восстанавливать пароль или разблокировать учетную запись.

Примечание Учетная запись корректируется посредством изменения объекта учетной записи пользователя в хранилище Active Directory. Для успешного редактирования учетных записей надо иметь право на администрирование объекта, в котором они находятся.

Изучив материал этого занятия, вы сможете:

- ✓ отключать, включать и удалять учетные записи;
- ✓ менять пароли;
- ✓ разблокировать учетные записи.

Продолжительность занятия — около 30 минут.

Отключение, подключение, переименование и удаление учетной записи пользователей

- **Отключение/включение.** Учетную запись следует отключать, когда известно, что пользователю она в течение длительного времени не потребуется, но понадобится в будущем. Например, если сотрудник уходит в отпуск, отключите его учетную запись, а когда он вернется, включите ее.
- **Переименование.** Эта операция выполняется, когда надо сохранить все права, разрешения, членство в группе и большинство других свойств одной учетной записи и переназначить их другой записи. Например, если в организации появился новый бухгалтер, переименуйте учетную запись, изменив имя, фамилию и пароль пользователя для нового бухгалтера.
- Удаление. Удаляйте учетные записи уволенных сотрудников (если вы не собираетесь их переименовывать). Так вы исключите наличие неиспользуемых записей в Active Directory.

Процедуры отключения, подключения, переименования и удаления доменных и локальных учетных записей однотипны.

► Отключение, включение, переименование и удаление учетной записи пользователя

1. В консоли Active Directory Users and Computers (Active Directory — пользователи и компьютеры) раскройте дерево консоли так, чтобы была видна соответствующая учетная запись, и выберите ее.
2. В меню Action (Действие) выберите команду; которую хотите выполнить (рис. 7-13).

Примечание Если учетная запись включена, в меню Action появляется команда Disable Account (Отключить учетную запись). Если учетная запись отключена, в меню Action появляется команда Enable Account (Включить учетную запись).

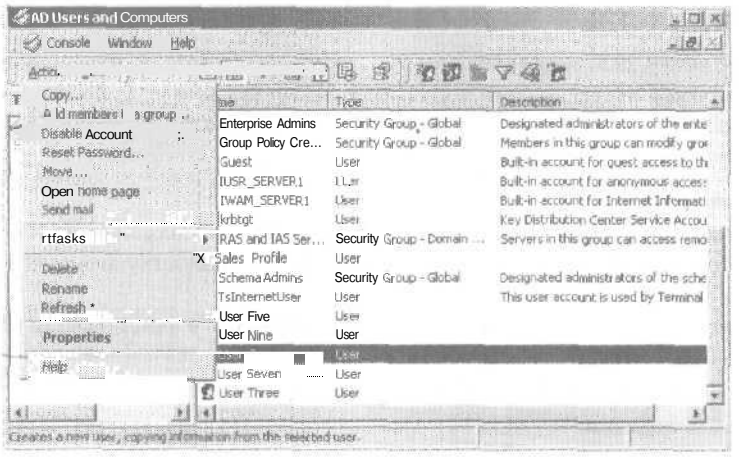


Рис. 7-13. Отключение, подключение, удаление или переименование учетных записей

Смена паролей и разблокирование учетных записей

Если пользователю не удается зарегистрироваться в домене или на локальном компьютере, возможно, необходима смена его пароля или разблокирование его учетной записи. Для этого вам надо иметь административные привилегии для объекта, в котором располагается данная учетная запись.

Смена пароля

Если срок действия пароля истечет до того, как его изменят, или пользователь забудет свой пароль, вам придется сменить пароль. Для этого старый пароль знать не обязательно.

После того как для учетной записи задан пароль (неважно кем — администратором или пользователем), этот пароль не виден ни пользователю, ни администратору. Это одна из мер безопасности: другим пользователям, включая администратора, чужой пароль недоступен. Иначе администратор мог бы воспользоваться им и войти в систему в качестве пользователя, которому этот пароль принадлежит, изменить его пароль, выполнить от лица этого пользователя какие-то действия, а затем задать прежний пароль пользователя.

▶ **Изменение пароля пользователя**

1. В консоли Active Directory Users and Computers раскройте дерево консоли, чтобы была видна соответствующая учетная запись, и выберите ее.
2. В меню Action (Действие) щелкните кнопку Reset Password (Смена пароля).

   Откроется одноименное окно.
3. Введите новый пароль, подтвердите его и щелкните OK.

В окне Reset Password всегда отмечайте флажок User Must Change Password A.t Next Logon (Потребовать смену пароля при следующем входе в систему), чтобы заставить пользователя изменить пароль при следующем входе в систему.

Примечание Если пользователь входит в систему только через Интернет, не отмечайте этот флажок.

Разблокирование учетных записей

Групповая политика Windows 2000 блокирует учетную запись пользователя, нарушившего заданные условия, например превысившего допустимое число неудачных попыток входа в систему. Если учетная запись заблокирована, Windows 2000 сообщает об ошибке. Подробнее о групповой политике — в главе 12.

► **Разблокировка учетной записи**

1. В консоли Active Directory Users and Computers (Active Directory — пользователи и компьютеры) раскройте дерево консоли так, чтобы была видна соответствующая учетная запись, и выберите запись, помеченную красным крестом.
2. В меню Action (Действие) щелкните пункт Properties (Свойства) и в одноименном окне перейдите на вкладку Account (Учетная запись).

   Заметьте: помечен флажок Account Lock Out (Заблокировать учетную запись).
3. Сбросьте этот флажок и щелкните OK.

Практикум: администрирование учетных записей

Подключите и отключите учетную запись и восстановите пароль для учетной записи.

Упражнение 1: подключение учетной записи

Отключите учетную запись, чтобы она больше не использовалась для входа в домен. Затем включите ту же запись.

► **Задание 1: отключите учетную запись**

1. Войдите в домен как Administrator (Администратор).
2. Откройте консоль Active Directory Users and Computers.
3. Раскройте домен microsoft.com и щелкните Users.
4. На правой панели щелкните правой кнопкой учетную запись Profile User, созданную на занятии 5, и в контекстном меню выберите команду Disable Account (Отключить учетную запись).

   Active Directory сообщит, что учетная запись была отключена. Учетная запись также помечена красным крестом.
5. Щелкните OK, чтобы вернуться в консоль Active Directory Users and Computers.
6. На правой панели консоли Active Directory Users and Computers щелкните правой кнопкой мыши учетную запись пользователя, которую только что отключили, чтобы появилось контекстное меню.

   Как определить, что учетная запись отключена?
7. Завершите сеанс Windows 2000.
8. Попытайтесь войти в систему как puser.

   Удалась ли эта попытка? Почему?

► **Задание 2: включите учетную запись**

1. Зарегистрируйтесь в домене как Administrator (Администратор).
2. Запустите консоль Active Directory Users and Computers.
3. Раскройте домен Microsoft.com и щелкните Users.
4. На правой панели щелкните правой кнопкой мыши созданную вами учетную запись Profile User и в контекстном меню выберите команду Enable Account (Включить учетную запись).

Active Directory сообщит, что учетная запись подключена.

5. Щелкните OK, чтобы вернуться в консоль Active Directory Users and Computers.
6. На правой панели консоли Active Directory Users and Computers щелкните правой кнопкой мыши учетную запись пользователя, которую только что включили, чтобы появилось контекстное меню.

   Как определить, что учетная запись включена?
7. Завершите сеанс Windows 2000.

▶ **Задание 3: протестируйте включение учетной записи и измените ее пароль**

1. Войдите в систему как puser.

   Удалось ли это? Почему?
2. Измените пароль на **student**.
3. Завершите сеанс Windows 2000.

Упражнение 2: восстановление пароля для учетной записи

▶ **Задание 1: смените пароль для учетной записи**

1. Войдите в домен как Administrator (Администратор).
2. Запустите консоль Active Directory Users and Computers.
3. Раскройте домен microsoft.com и щелкните Users.
4. На правой панели щелкните правой кнопкой учетную запись Profile User и в контекстном меню выберите команду Reset Password (Смена пароля).

   Откроется одноименное окно, содержащее поле для ввода нового пароля для этой учетной записи. Заметьте: Administrator не может узнать текущий пароль.
5. В полях New Password (Новый пароль) и Confirm Password (Подтверждение) введите **password** и пометьте флажок User Must Change Password At Next Logon (Потребовать смену пароля при следующем входе в систему). Щелкните OK.

   Active Directory сообщит, что пароль изменен.
6. Щелкните OK, чтобы вернуться в консоль Active Directory Users and Computers.
7. Завершите сеанс.

▶ **Задание 2: протестируйте смену пароля**

1. Войдите в систему как puser с паролем **password,**

   Удалось ли это? Почему?
2. Завершите сеанс.

Резюме

Учетную запись следует отключать, когда пользователю в течение длительного времени она не нужна, но может потребоваться в будущем.

Учетные записи переименовывают, когда надо сохранить все права, разрешения, членство в группе и большинство других свойств одной учетной записи и переназначить их другой. Например, если в организации появился новый бухгалтер, переименуйте учетную запись, изменив имя, фамилию и пароль пользователя для него.

Удаляйте учетные записи, если они более не требуются.

Если срок действия пароля истечет до того, как его изменят, или пользователь забудет свой пароль, смените пароль, чтобы пользователь мог войти на домен. Если пользователь забыл пароль или его учетная запись заблокирована, вы можете войти в систему как Administrator и разблокировать учетную запись.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении А «Вопросы и ответы» в конце книги.

1. Какие возможности предоставляют пользователям локальные и доменные учетные записи?

2. На что следует обратить внимание при планировании новых учетных записей?

3. Какая информация требуется для создания доменной учетной записи?

4. Пользователю нужен доступ к сетевым ресурсам из дома, но он не хочет оплачивать расходы на телефонную связь. Как следует настроить учетную запись?

5. В чем разница между локальным и перемещаемым профилями пользователя?

6. Как убедиться, что пользователь на клиентском компьютере с Windows 2000 имеет перемешаемый профиль?

7. Как убедиться, что пользователь имеет хранящуюся централизованно домашнюю папку?

8. Почему следует переименовывать учетную запись?

ГЛАВА 8

Управление учетными записями групп

В этой главе

Благодаря группам, администрирование учетных записей пользователей значительно упрощается, поскольку их можно объединять в управляемые единицы. На этом занятии мы расскажем о планировании и создании групп. Вы узнаете о группах по умолчанию имеющихся в Windows 2000. Кроме того, здесь обсуждаются группы, в которые следует объединить администраторов, а также преимущества применения утилиты Run As, которая позволяет пользователям запускать программу с правами администратора. Выполняя практическую часть занятия, вы спланируете и развернете в сети глобальные и локальные группы домена.

Прежде всего

Для выполнения заданий вам потребуется:

- настроить компьютер в соответствии с инструкциями вводной главы;
- внимательно изучить главу 7;
- знать отличия рабочей группы и домена, а также отличия контроллера домена и рядового сервера;
- создать учетные записи User1, User5 и User9 согласно инструкциям главы 7.

Занятие 1. Знакомство с группой

Здесь рассказывается о группах, а также о том, как они упрощают административные задачи. Вы также узнаете о типах и областях действия групп, которые можно создать в Windows 2000.

Изучив материал этого занятия, вы сможете:

- ✓ объяснить назначение групп;
- ✓ объяснить назначение групп безопасности и групп распространения;
- ✓ объяснить назначение локальных групп домена, а также глобальных и универсальных групп;
- ✓ объяснить назначение локальных групп.

Продолжительность занятия — около 15 минут.

Группа и разрешения

Группа (group) — это набор учетных записей пользователей. Группы упрощают администрирование, позволяя назначать разрешения и права группе пользователей, а не каждой отдельной учетной записи (рис. 8-1).

Назначая *разрешения* (permissions), Вы предоставляете пользователям доступ к определенным ресурсам и определяете права доступа. Если, например, нескольким пользователям требуется доступ к одному файлу, добавьте их учетные записи в группу, Затем дайте группе разрешение на считывание файла. *Права* (rights) дают возможность выполнять системные задачи, например изменять системное время, архивировать или восстанавливать файлы, а также локально регистрироваться в системе.

Рис. 8-1. Группы упрощают администрирование

Примечание Подробнее о разрешениях — в главе 9, о правах — в главе 13.

Кроме пользователей, в группу можно добавлять контакты, компьютеры и другие группы. Группы добавляют в другие группы для создания объединенных групп — таким образом упрощается назначение разрешений. Добавляя компьютеры в группу, Вы можете упростить предоставление доступа системной задаче одного компьютера к ресурсам другого.

Типы групп

Иногда группы создаются в целях защиты, например для назначения разрешений. В других случаях группы нужны, например, для отправки сообщений электронной почты. Таким образом, в Windows 2000 Server имеется два типа групп: *безопасности* и *распространения*. Тип группы определяет порядок ее использования. Группы обоих типов размещаются в хранилище Active Directory, что позволяет их применять в любом сегменте сети.

Группы безопасности

В ОС Windows 2000 доступны только группы безопасности, используемые для назначения разрешений и предоставления доступа к ресурсам. Программы поиска в хранилище Active Directory могут применять группы безопасности в целях, не связанных с безопасностью, например для запроса информации, требуемой Web-приложению. Поскольку в Windows 2000 используются лишь группы безопасности, о них мы и расскажем подробно в этой главе.

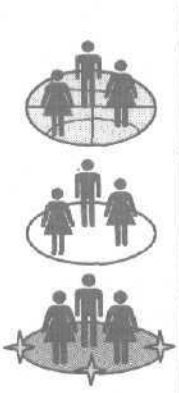
Группы распространения

Приложения обращаются к группам распространения, как к спискам пользователей, — для выполнения функций, не связанных с обеспечением защиты. Группы распространения следует применять, например, лишь для одновременной отправки сообщений электронной почты нескольким пользователям или других подобных операций. Назначать разрешения через группу распространения нельзя.

Примечание Группы распространения могут применять лишь приложения, предназначенные для работы со службой каталогов Active Directory. Например, предполагается, что будущие версии Microsoft Exchange Server будут обращаться к группам распространения, как к спискам распространения, для рассылки электронной почты.

Область действия группы

При создании группы надо определить ее тип и *область действия,* которая позволяет поразному использовать группы для назначения разрешений. Область действия также определяет, в каких сегментах сети группу можно применять. В соответствии с областями действия группы делятся на локальные группы домена, глобальные и универсальные (рис. 8-2).



Глобальная группа

Входят только пользователи из локального домена.
Участники могут обращаться к ресурсам в любом домене.

Локальная группа домена

Входят пользователи из любого домена.
Участники могут обращаться к ресурсам только в локальном домене.

Универсальная группа

Входят пользователи из *любого* домена.
Участники могут обращаться к ресурсам в любом домене.

Рис. 8-2. Деление групп согласно областям действия

Глобальная группа

Чаще всего применяется для организации пользователей *с* одинаковыми требованиями доступа к сети. Ее характеристики:

- **ограниченное членство** — можно добавлять членов лишь из того домена, где создана группа;
- **доступ к ресурсам любого домена** — глобальная группа позволяет назначать разрешения доступа к ресурсам любого домена.

Локальная группа домена

Чаще всего применяется для назначения разрешений доступа к ресурсам. Ее характеристики:

- **открытое членство** — можно добавлять членов из любого домена;
- **доступ к ресурсам одного домена** — позволяют назначать разрешения доступа к ресурсам того же домена, где была создана группа.

Универсальная группа

Чаще всего применяется для назначения разрешений доступа к связанным ресурсам, расположенных в нескольких доменах. Ее характеристики:

- **открытое членство** — можно добавлять участников из любого домена;
- **доступ к ресурсам любого домена** — универсальная группа позволяет назначать разрешения доступа к ресурсам в любом домене;
- **доступна лишь в доменах основного режима** — в доменах смешанного режима эти группы недоступны. Полный набор возможностей Windows 2000 доступен лишь в основном режиме.

Вложенность групп

Добавление одних групп в другие (вложенность групп) позволяет на порядок снизить число операций по назначению разрешений. Изучите потребности членов групп и создайте соответствующую иерархию групп. В основном режиме Windows 2000 допускает неограниченную вложенность групп. Так, можно создать группу для каждого региона, в котором имеются филиалы организации, затем добавить менеджеров в отдельные группы. Все региональные группы разрешено добавить в группу Worldwide Managers. Если региональным менеджерам потребуется доступ к некоторому ресурсу, задайте соответствующие права группе Worldwide Managers. Благодаря вложенности, эта группа включает всех членов региональных групп, поэтому менеджеры из всех регионов смогут обратиться к требуемому ресурсу. Это обеспечивает назначение разрешений по иерархии, а также децентрализованный контроль членства.

Придерживайтесь следующих рекомендаций:

- **при добавлении одних групп в другие попытайтесь снизить уровень вложенности.** Вложенность позволяет на порядок уменьшить число операций по назначению разрешений. Однако при многочисленных уровнях вложенности контроль за разрешениями усложняется. Наиболее эффективен первый уровень — он позволяет снизить число операций по назначению разрешений, одновременно упрощая контроль разрешений;
- **в целях контроля за назначением разрешений отдельно документируйте состав групп.** Допустим, администратор добавляет временных сотрудников в группу, созданную для разработчиков некоторого проекта. Другой администратор, не зная о временных сотрудниках, добавляет группу проекта в группу, обладающую доступом к конфиденциальной информации, и временные сотрудники получают к ней доступ, что неприемлемо.

Эффективная вложенность групп в многодоменной среде позволит снизить сетевой трафик между доменами и упростить администрирование дерева доменов. Для эффективного использования вложенности надо знать правила членства в группах.

Члены групп

Область действия группы определяет **круг** ее участников. Правила членства устанавливают, кого можно включить в группу. К членам групп относятся учетные записи пользователей и другие группы. Правила членства описаны в табл. 8-1.

Табл. 8-1. Правила членства в группах

Группа	Состав в основном режиме	Состав в смешанном режиме
Глобальная группа	Учетные записи пользователей и компьютеров, а также глобальные группы из того же домена	Учетные записи пользователей из того же домена и учетные записи компьютеров
Локальная группа домена	Учетные записи пользователей, компьютеров, глобальные и универсальные группы, входящие в любую локальную группу того же домена	Учетные записи пользователей и компьютеров, а также глобальные группы из любого домена
Универсальная группа	Учетные записи пользователей и компьютеров, глобальные и универсальные группы из любого домена	В смешанном режиме недоступна

Локальная группа

Локальная группа — это набор учетных записей пользователей компьютера. Применяйте локальные группы для назначения разрешений доступа к ресурсам компьютера, на котором она создана. Windows 2000 создает локальные группы в локальной БД защиты.

Внимание! Поскольку в Active Directory группы, согласно области действия являющиеся локальными группами домена, иногда называются просто локальными группами, важно различать обычные локальные группы и локальные группы домена.

Использование локальной группы

Помните, что локальные группы:

- действуют лишь на том компьютере, где они созданы. Разрешения локальных групп предоставляют доступ лишь к локальным ресурсам системы;
- можно использовать на компьютерах Windows 2000 Professional и рядовых серверах Windows 2000 Server. Создать локальные группы на контроллере домена нельзя, поскольку БД зашиты контроллера не зависит от БД Active Directory;
- позволяют ограничить доступ пользователей и групп к сетевым ресурсам без создания групп домена, как в среде Internet Information Server.

Ниже описаны правила членства в локальной группе:

- локальным группам разрешается содержать учетные записи пользователей компьютера, на котором создана группа;
- локальные группы нельзя включить в другие группы.

Резюме

Вы узнали, что группа — это набор учетных записей пользователей. Группы также могут включать другие группы, что упрощает администрирование, так как позволяет назначать разрешения и права группе пользователей, а не каждой отдельной учетной записи.

При создании группы надо определить ее тип и область действия. В Windows 2000 имеются группы распространения и безопасности, но используются лишь группы безопасности. Программы поиска в хранилище Active Directory также могут применять группы безопасности в целях, не связанных с безопасностью, например для работы с электронной почтой. По области действия группы делятся на локальные группы домена, глобальные и универсальные.

Существуют правила членства, определяющие, кто может состоять в глобальных и универсальных группах, а также в локальных группах домена.

Кроме того, мы рассказали, как использовать локальные группы для назначения разрешений доступа к локальным ресурсам компьютерам, на котором группа находится.

Занятие 2. Стратегия формирования группы

Для эффективной работы надо определить порядок использования групп, а также типы групп, которые предназначены для работы в особых ситуациях. Сейчас мы расскажем о стратегии внедрения глобальных и универсальных групп, а также локальных групп домена.

Изучив материал этого занятия, вы сможете:

- ✓ описать этапы стратегии внедрения;
- ✓ спланировать стратегию группирования.

Продолжительность занятия — около 30 минут.

Планирование глобальных и локальных групп домена

Прежде чем создавать группу, необходимо разработать соответствующую стратегию. Мы советуем вам использовать глобальные и локальные группы домена. Есть несколько общих правил, которых мы и советуем вам придерживаться.

1. Объедините пользователей со схожими обязанностями в одну группу; например, в бухгалтерии можно объединить учетные записи бухгалтеров в группу Accounting.
2. Определите, к каким ресурсам или труппам ресурсов обращаются сотрудники, и создайте для этого ресурса локальную труппу домена. Например, если в организации несколько цветных принтеров, создайте локальную группу домена Color Printers.
3. Выявите все глобальные группы, *обращающиеся* к одним и тем же ресурсам, и включите эти группы в соответствующую локальную группу домена; так, можно добавить глобальные группы Accounting, Sales и Management в локальную группу домена Color Printers.
4. Назначьте локальной группе домена соответствующие разрешения; например группе Color Printers надо назначить разрешения на доступ к цветным принтерам.

Распределение глобальных и локальных групп домена показано на рис. 8-3. Поместите учетные записи пользователей в глобальные группы, создайте для совместно используемых ресурсов локальную группу домена, включите глобальные группы в локальную и предоставьте локальной труппе домена нужные разрешения. Данная стратегия обеспечивает наибольшую гибкость при росте численности сотрудников и облегчает администратору назначение разрешений.

Некоторые возможные ограничения других стратегий перечислены ниже.

- **Добавление учетных записей пользователей в локальные группы домена и назначение последним разрешений.** Такая стратегия не позволяет предоставлять разрешения вне домена. Гибкость стратегии глобальных и локальных групп домена снижается с ростом сети.
- **Размещение учетных записей в глобальных группах и назначение им разрешений.** При наличии нескольких доменов данная стратегия может усложнить администрирование. Если глобальным группам нескольких доменов нужны одинаковые разрешения, придется назначать их каждой группе в отдельности.

Рис. 8-3. Планирование стратегии группирования

Использование универсальных групп

Есть несколько правил, о которых вам надо помнить.

- Универсальные группы можно использовать для предоставления доступа к ресурсам нескольких доменов. В отличие от локальных доменных универсальным группам можно назначать разрешения на доступ к ресурсам любого домена Вашей сети. Например, если ответственным лицам требуется доступ ко всем принтерам сети, создайте универсальную группу и назначьте ей разрешения на использование принтеров, подключенных к серверам печати всех доменов.
- Универсальные группы рекомендуется применять, только если их состав постоянен. При редактировании состава универсальной группы в дереве доменов иногда возникает ненужный трафик между контроллерами доменов, поскольку такие изменения реплицируются на многие контроллеры доменов.
- Рекомендуется, объединив глобальные группы нескольких доменов в универсальную группу, присвоить ей разрешения на доступ к ресурсу. Таким образом, универсальная группа используется аналогично локальным группам домена для назначения разрешений доступа к ресурсам. И все же в отличие от локальной группы, доменной универсальной группе можно назначать разрешения доступа к ресурсам других доменов.

Практикум: планирование новых учетных записей групп

Вы спланируете группы, необходимые для бизнес-сценария.

Ситуация

Предположим, вы — администратор отдела по обслуживанию клиентов производственной компании и управляете доменом, входящим в дерево доменов организации. Администрированием других доменов вы не занимаетесь, однако вам может потребоваться предоставить некоторым пользователям других доменов доступ к ресурсам вашего домена. Пользователи компании работают с несколькими разделяемыми сетевыми ресурсами. Компания также планирует развернуть программу электронной почты, использующую Active Directory.

Как администратору, вам требуется определить:

- необходимые группы;
- состав каждой группы. Это могут быть как учетные записи пользователей, так и другие группы;
- тип и область действия каждой группы.

Зафиксируйте разработанные вами стратегии в тетради «Планирование групп». При заполнении тетради укажите:

1. названия всех групп в колонке «Имя группы»;
2. тип и область действия группы;
3. состав группы.

Выполнив упражнение, посмотрите ответ в приложении А «Вопросы и ответы». Однако здесь дан лишь один из возможных вариантов ответов. Вполне вероятно, что вы спланировали учетные записи групп иначе.

В табл. 8-2 описаны обязанности сотрудников отдела по обслуживанию клиентов и их численность.

Табл. 8-2. Сведения о сотрудниках отдела по обслуживанию клиентов

Должность	Количество сотрудников
Контролер ОТК	20
Представитель отдела по обслуживанию клиентов	250
Техник	5
Менеджер	5
Торговый представитель	5
Администратор сети	2

В табл. 8-3 указано, к каким ресурсам обращаются различные категории сотрудников организации.

Табл. 8-3. Права доступа, необходимые сотрудникам

Категория сотрудников	Используемые ресурсы
Сотрудники отдела по обслуживанию клиентов и менеджеры	БД клиентов (необходим полный доступ)
Торговые представители	БД клиентов (необходим доступ только для чтения)
Все сотрудники	Политики компании (необходим доступ только для чтения)
Все сотрудники	Внутренние **объявления компании, получаемые** по электронной **почте**
Все заинтересованные сотрудники из любого домена	Периодические сообщения о событиях производства, рассылаемые по электронной почте
Все сотрудники, за исключением техников	Разделяемая установка Microsoft Office
Сетевые администраторы	Все ресурсы компании (необходим полный доступ)
Торговые представители (ваш и другие домены)	Отчеты о продажах

Заполнение тетради «Планирование групп»

Имя группы	Тип и область действия	Состав

Г. Необходимы ли в вашей сети локальные группы?

2. Необходимы ли в вашей сети универсальные группы?
3. Торговые представители вашей компании часто посещают штаб-квартиру и другие подразделения. Следовательно, придется создать для них учетные записи в других доменах с теми же правами доступа к ресурсам, какими обладают учетные записи торговых представителей в вашем домене. Вам также следует упростить процедуру предоставления администраторами других доменов доступа к ресурсам вашего домена. Как это осуществить?

Резюме

Вы изучили некоторые наиболее часто применяемые стратегии групп. Выбираемая стратегия зависит от среды Windows 2000. При наличии одного домена Microsoft рекомендует в большинстве сетей Windows 2000 использовать для предоставления доступа к ресурсам глобальные и локальные группы домена.

Стратегия использования глобальных и локальных групп домена заключается в объединении учетных записей пользователей в глобальные группы. Создается локальная группа домена с правами доступа ко всем необходимым ресурсам, и в нее добавляются глобальные группы. Такая стратегия обеспечивает наибольшую гибкость при росте числа сотрудников и облегчает администратору процедуру назначения разрешений.

Занятие 3. Формирование группы

Определив потребности пользователей и разработав план, вы можете заняться созданием группы. Для внедрения плана необходимо знать основные правила построения групп. На этом занятии рассказывается о создании, удалении и изменении состава групп, а также об изменении типа и области действия группы.

Изучив материал этого занятия, вы сможете:

- ✓ создавать и удалять группы;
- ✓ добавлять в группы новых членов;
- ✓ изменять тип и область действия группы.

Продолжительность занятия — около 25 минут.

Создание группы

Для создания и удаления групп служит оснастка Active Directory Users And Computers (Active Directory — пользователи и компьютеры). Группы следует создавать в контейнере Users или в ОП, созданных специально для групп. По мере роста и развития организации некоторые группы становятся ненужными. Такие группы следует удалять. Это одно из правил соблюдения безопасности.

► **Создание группы**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Active Directory Users And Computers (Active Directory — пользователи и компьютеры).
2. Раскройте узел домена, щелкните контейнер Users правой кнопкой мыши и выберите в контекстном меню команду New\Group (Создать\Группа).
3. В диалоговом окне New Object — Group (Новый объект — группа) (рис. 8-4) выберите необходимые параметры и щелкните OK.

   В табл. 8-4 описаны параметры диалогового окна New Object — Group консоли Active Directory Users and Computers.

Табл. 8-4. Параметры диалогового окна New Object — Group

Параметр	Описание
Group Name (Имя группы)	Имя новой группы. В пределах домена, где создается группа, имя должно быть уникальным
Group Name(preWindows 2000) [Имя группы (пред-Windows2000)]	Имя группы, созданной для обеспечения совместимости с предыдущими версиями Windows. Автоматически создается при вводе вами имени
Group Scope (Область действия группы)	Область действия группы. Возможные варианты: Domain Local (Локальная в домене), Global (Глобальная) и Universal (Универсальная). Переключатель Universal доступен, только если тип группы — Distribution или если сервер работает в смешанном режиме
Group Type (Тип группы)	Тип группы. Возможные варианты — Distribution (Группа распространения) и Security (Группа безопасности)

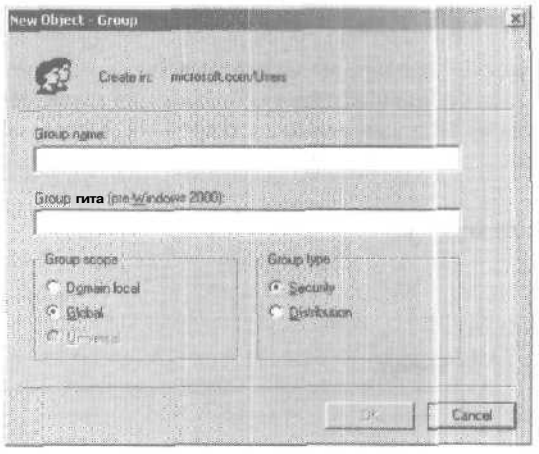


Рис. 8-4. Диалоговое окно New **Object — Group**

Удаление группы

Каждая группа обладает уникальным идентификатором защиты, SID, повторно применить который нельзя. SID в Windows 2000 служит для идентификации групп и присвоенных ей разрешений. Windows 2000 не использует повторно идентификаторы удаленных групп, даже если Вы создадите группу с именем, аналогичным имени удаленной группы. Следовательно, восстановить доступ к ресурсам, воссоздав группу, нельзя.

При удалении группы удаляется лишь сама группа и связанные с ней разрешения. Учетные записи пользователей — членов группы не затрагиваются.

Примечание Удалить группу, которая для одного из ее членов является основной, нельзя.

▶ **Удаление группы**

1. Щелкните название удаляемой группы правой кнопкой и выберите в контекстном меню команду Delete (Удалить).
2. В диалоговом окне Active Directory щелкните кнопку Yes.

Добавление членов в группу

В созданную группу можно добавлять членов — учетные записи пользователей, контакты, другие группы и компьютеры. Компьютеры добавляются в группу для предоставления им доступа к разделяемым ресурсам других систем, например для удаленного резервного копирования. Для добавления членов служит оснастка Active Directory Users And Computers.

▶ **Добавление членов в группу**

1. Откройте консоль Active Directory Users And Computers и раскройте контейнер Users.
2. Щелкните нужную группу правой кнопкой и выберите в контекстном меню команду Properties.
3. В диалоговом окне свойств перейдите на вкладку Members (Члены группы) и щелкните кнопку Add (Добавить).

   Откроется диалоговое окно Select Users, Contacts, Or Computers (Выбор: Пользователи, Контакты и Компьютеры) (рис. 8-5).

4. Чтобы добавить учетную запись пользователя, контакт, компьютер или группу из определенного домена, выберите нужный домен в списке Look **In** (Искать в). Кроме того, можно выбрать пункт Entire Directory (Вся папка) и просмотреть все учетные записи и группы хранилища Active Directory. Укажите нужную учетную запись или группу и щелкните кнопку Add (Добавить).

   Выбранные учетные записи отображаются в нижней части диалогового окна Select Users, Contacts, Or Computers.

Примечание Несколько учетных записей пользователей или групп разрешается добавлять по одной или все сразу, выделив их с помощью клавиш Shift или Ctrl. Удерживая Shift, можно выделить последовательный диапазон элементов списка; Ctrl позволяет выделять отдельные группы и учетные записи, Выбрав нужные элементы, щелкните кнопку Add (Добавить).

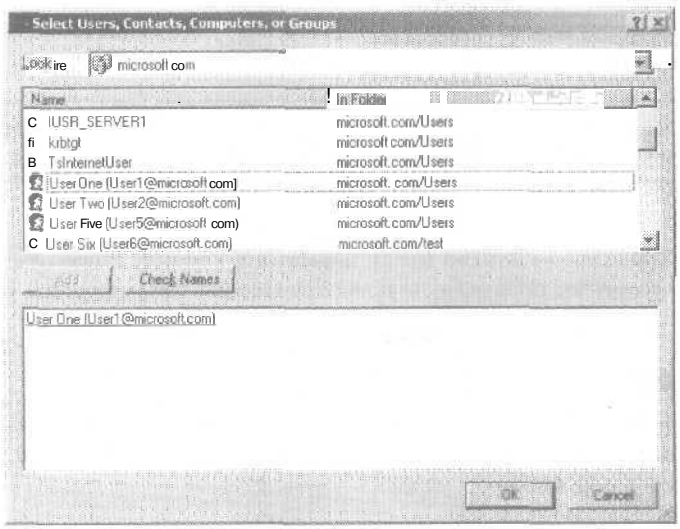


Рис. 8-5. Диалоговое окно Select Users, Contacts, Or Computers (Выбор: Пользователи, Контакты и Компьютеры)

5. Просмотрев выбранные элементы и убедившись, что все правильно, щелкните кнопку OK.
6. В диалоговом окне свойств щелкните OK.

Изменение типа группы

При изменении функций группы вам может потребоваться изменить ее тип. Например, у вас есть группа распространения, включающая сотрудников из нескольких доменов, работающих над одним проектом, и используемая для рассылки сообщений электронной почты. В ходе работы над проектом членам группы может потребоваться доступ к общей БД. Преобразовав группу распространения в группу безопасности и назначив ей соответствующие разрешения, вы обеспечите членам группы доступ к общей БД. Изменять тип группы можно лишь в доменах Windows 2000 естественного режима.

► **Изменение типа группы**

1. Щелкните нужную группу правой кнопкой мыши и выберите в контекстном меню команду Properties.
2. Для изменения типа группы воспользуйтесь вкладкой General открывшегося диалогового окна свойств.

Преобразование группы в универсальную

Со временем иногда требуется изменить область действия группы. Например, чтобы предоставить пользователям доступ к ресурсам других доменов, приходится преобразовать имеющуюся локальную доменную группу в глобальную. Изменять область действия группы разрешается лишь в доменах естественного режима.

Дабы изменить область действия группы следует:

- **преобразовать глобальную группу в универсальную** — это возможно, лишь когда глобальная группа не является членом другой глобальной группы;
- **преобразовать локальную группу домена в универсальную группу** — это возможно, только если локальная группа домена не содержит подобных групп.

Примечание Windows 2000 не поддерживает изменение области действия универсальной группы, поскольку ограничения на членство и область действия других групп более строгие.

► **Изменение типа группы**

1. Щелкните нужную группу правой кнопкой мыши и выберите команду Properties.
2. Для изменения типа группы воспользуйтесь вкладкой General открывшегося окна свойств.

Создание локальной группы

Для создания локальных групп применяется оснастка Local Users and Groups (Локальные пользователи и группы) консоли Computer Management (Управление компьютером). Локальные группы создаются в папке Groups.

► **Создание локальной группы**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Computer Management (Управление компьютером). В Windows 2000 Professional раскройте меню Start\Settings (Пуск\Настройка) и щелкните Control Panel (Панель управления).
2. Раскройте в дереве консоли папку Local Users And Groups (Локальные пользователи и группы) и щелкните подпапку Groups (Группы) правой кнопкой. Затем в контекстном меню выберите команду New Group (Создать группу).
3. В открывшемся диалоговом окне (рис. 8-6) введите имя и описание группы.

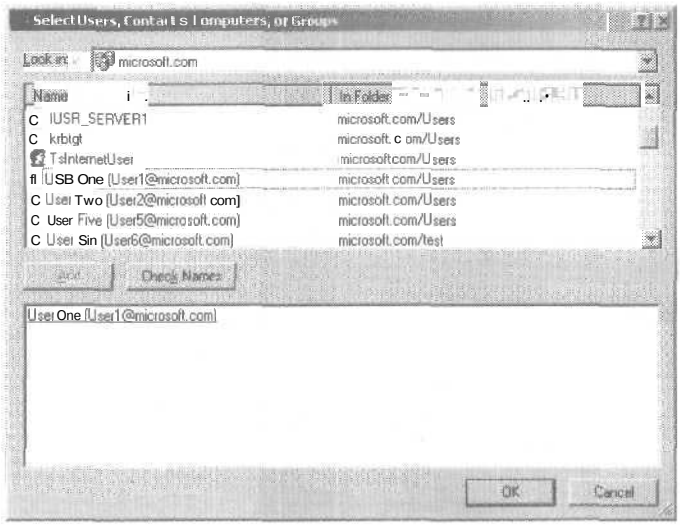


Рис. 8-6. Диалоговое окно New Group (Создание группы)

Параметры диалогового окна New Group (Создание группы) описаны в табл. 8- 5.

Табл. 8-5. Параметры диалогового окна New Group

Параметр	Описание
Group Name (Имя группы)	Уникальное имя локальной группы. Это единственный обязательный параметр. В имени разрешается использовать любые символы, кроме обратного слэша (\). Длина имени составляет до 256 символов; однако в некоторых окнах слишком длинные имена отображаться не будут
Description (Описание)	Описание группы
Members (Члены группы)	Состав группы
Add (Добавить)	Добавить пользователя в список членов группы
Delete (Удалить)	Удалить пользователя из списка членов группы
Create (Создать)	Создать группу

Членов в локальную группу можно добавить как при создании группы, так и после.

▶ **Удаление локальной группы**

1. Щелкните удаляемую группу правой кнопкой и выберите команду Delete (Удалить).
2. В диалоговом окне Active Directory щелкните кнопку Yes.

▶ **Добавление членов в локальную группу**

1. Откройте оснастку Local Users and Groups и раскройте папку Groups.
2. Щелкните нужную группу правой кнопкой и выберите команду Properties.
3. В открывшемся диалоговом окне свойств щелкните кнопку Add (Добавить).

Откроется диалоговое окно Select Users Or Groups (рис. 8-7).

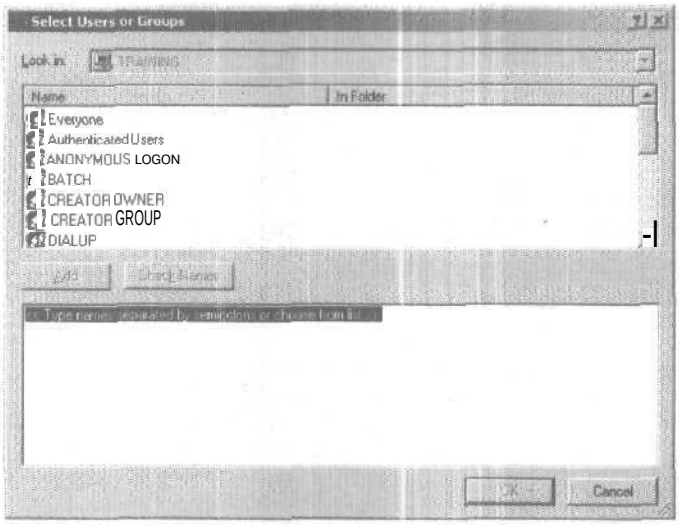


Рис. 8-7. **Диалоговое окно Select** Users **Or Groups (Выбор: Пользователи или Группы)**

4. В списке Look In (Искать в) отображается компьютер, для которого создается группа. Выберите требуемую учетную запись пользователя и щелкните кнопку Add (Добавить).
5. Просмотрев выбранные элементы и убедившись, что все правильно, щелкните кнопку OK.
6. В диалоговом окне свойств щелкните OK.

Практикум: создание группы

Вы создадите глобальную группу безопасности и добавите в нее ранее созданные учетные записи пользователей User1 и User5. Затем Вы создадите локальную группу безопасности домена, назначите ей разрешения на доступ к отчетам о продажах и добавите в нее глобальную группу.

Упражнение 1: создание глобальной группы и добавление в нее членов

Сейчас вы создадите глобальную группу безопасности и добавите в нее членов.

▶ **Задание: создайте глобальную группу в домене**

1. Зарегистрируйтесь в домене как Administrator (Администратор).
2. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers.
3. Раскройте узел домена и дважды щелкните контейнер Users.

   В правой панели консоли отобразится список имеющихся учетных записей и встроенных глобальных групп.
4. Щелкните контейнер Users правой кнопкой и выберите в контекстном меню команду New\Group.

   Откроется диалоговое окно New Object — Group. Обратите внимание на доступные области действия и типы групп. Для объединения учетных записей пользователей применяются глобальные группы безопасности.
5. В поле Group Name (Имя группы) введите **Sales.**

6. В области Group Scope (Область действия группы) щелкните переключатель Global (Глобальная), а в области Group Type (Тип группы) — переключатель Security (Группа безопасности).
7. Щелкните OK.

   Windows 2000 создаст группу и добавит ее в контейнер Users.

► **Задание 2: добавьте членов в глобальную группу**

1. В правой панели оснастки Active Directory Users and Computers дважды щелкните Sales.

   Откроется диалоговое окно свойств группы Sales.
2. Чтобы просмотреть состав группы, перейдите на вкладку Members (Члены группы).

   На текущий момент список членов группы пуст.
3. Чтобы добавить члена в группу, щелкните кнопку Add (Добавить).
4. Убедитесь, что в списке Look In (Искать в) диалогового окна Select Users, Contacts, Or Computers (Выбор: Пользователи, Компьютеры, Контакты или Группы) выбран ваш домен.
5. Выберите учетную запись User One и щелкните кнопку Add.
6. Выберите учетную запись User Five и щелкните кнопку Add.
7. Щелкните OK.

   Теперь пользователи User1 и User5 стали членами глобальной группы безопасности Sales.
8. Щелкните OK, чтобы закрыть диалоговое окно свойств группы Sales.

Упражнение 2: создание локальной группы домена и добавление в нее членов

Вы создадите локальную группу домена, предназначенную для предоставления разрешений на доступ к отчетам о продажах. Затем вы добавите в эту группу глобальную группу безопасности, созданную в упражнении 1.

> **Задание 1: создайте локальную группу домена**

1. Убедитесь, что оснастка Active Directory Users And Computers открыта и в дереве консоли выбран контейнер Users.
2. Щелкните контейнер Users правой кнопкой и выберите команду New\Group.

   Откроется диалоговое окно New Object — Group.
3. В поле Group Name введите **Reports**.
4. В группе Group Scope щелкните переключатель Domain Local (Локальная в домене), а в группе Group Type — переключатель Security (Группа безопасности).
5. Щелкните OK.

   Windows 2000 создаст локальную группу домена и добавит ее в контейнер Users.

► **Задание 2: добавьте членов в локальную группу домена**

1. В правой панели оснастки Active Directory Users and Computers дважды щелкните Reports.

   Откроется диалоговое окно свойств группы Reports.
2. Чтобы просмотреть состав группы, перейдите на вкладку Members.

   Пока список членов группы пуст.
3. Чтобы добавить члена в группу, щелкните кнопку Add.
4. В списке Look In диалогового окна Select Users, Contacts, Or Computers выберите Entire Directory.

В диалоговом окне Select Users, Contacts, Or Computers отобразится список объектов, которые можно добавить в группу. Размещение каждого объекта указано в формате *домен*\Users.

5. Щелкните заголовок столбца Name (Имя) списка учетных записей пользователей, групп и компьютеров.

   Список будет отсортирован в алфавитном порядке по имени.

6. Выберите группу Sales, щелкните кнопку Add и затем щелкните OK.

   Теперь группа Sales является членом локальной группы домена Reports.

7. Щелкните OK, чтобы закрыть диалоговое окно свойств группы Reports.

Резюме

Мы описали основные правила создания групп. Сначала необходимо выбрать область действия группы, учитывая ее назначение. Затем следует определить, имеются ли у вас необходимые разрешения для создания группы в данном домене. По умолчанию в домене группы могут создавать лишь члены группы Administrators (Администраторы) или Account Operators (Операторы учета). Администратор вправе предоставить пользователю разрешение на создание групп в домене, отдельном контейнере или ОП.

Консоль Active Directory Users and Computers (Active Directory — пользователи и компьютеры) позволяет создавать, удалять и изменять состав, тип и область действия универсальных, глобальных и локальных групп домена. Оснастка консоли применяется для создания, удаления и добавления членов Local Users and Groups (Локальные пользователи и группы) в локальные группы Computer Management (Управление компьютерами).

Выполняя практикум, вы создали глобальную группу безопасности и добавили в нее членов, а также создали локальную группу безопасности домена и добавили в нее ранее созданную глобальную группу.

Занятие 4. Группы по умолчанию

В Windows 2000 имеется четыре типа встроенных групп: глобальные, локальные группы домена, изолированные локальные и системные. Встроенные группы обладают предопределенным набором членов и прав. Права пользователей определяют круг задач, которые разрешается выполнять членам группы по умолчанию. На этом занятии рассказывается об использовании групп по умолчанию.

Изучив материал этого занятия, вы сможете:

- ✓ **рассказать о группах по умолчанию в Windows 2000.**

Продолжительность занятия — около 15 минут.

Встроенная глобальная группа

Позволяют объединять учетные записи общего типа. Windows 2000 по умолчанию добавляет членов в некоторые встроенные глобальные группы. Вы также можете добавлять в них новых членов, чтобы предоставить им права и разрешения группы.

При создании домена Windows 2000 создает встроенные глобальные группы в папке Users хранилища Active Directory. По умолчанию эти группы не наследуют каких-либо прав. Чтобы присвоить встроенной глобальной группе права, ее стоит добавить в локальную группу домена или явно назначить ей нужные права и разрешения.

Контейнер Users содержит все встроенные группы домена. В табл. 8-6 перечислены стандартные участники наиболее часто используемых встроенных глобальных групп.

Табл. 8-6. Стандартный состав наиболее часто используемых встроенных глобальных групп

Глобальная группа	Описание
Domain Admins (Администраторы домена)	Windows 2000 автоматически добавляет глобальную группу Domain Admins в локальную группу домена Administrators, чтобы члены группы Domain Admins могли выполнять административные задачи на любом компьютере домена. По умолчанию учетная запись Administrator включена в группу Domain Admins
Domain Users (Пользователи домена)	Windows 2000 автоматически добавляет глобальную группу Domain Users во встроенную локальную группу Users (Пользователи). Учетная запись Administrator (Администратор) по умолчанию включена в группу Domain Users, и Windows 2000 автоматически добавляет в эту группу все новые учетные записи пользователей домена
Domain Guests (Гости домена)	Windows 2000 автоматически добавляет глобальную группу Domain Guests во встроенную локальную группу Guests (Гости). Учетная запись Guest по умолчанию включена в группу Domain Guest; данная учетная запись по умолчанию отключена

Табл. 8-6. Стандартный состав наиболее часто используемых встроенных глобальных групп (*окончание*)

Глобальная группа	Описание
Enterprise Admins (Администраторы предприятия)	В эту группу можно добавить учетные записи (Администраторы предприятия) пользователей, которым нужны административные привилегии в масштабе всей сети. Встроенная локальная группа Administrators каждого домена по умолчанию включена в глобальную группу Enterprise Admins. По умолчанию учетная запись Administrator также является членом этой глобальной группы

Встроенная **локальная** группа **домена**

Windows 2000 создает встроенные локальные группы домена, что позволяет предоставить пользователям права и разрешения на выполнение задач в хранилище Active Directory, а также на контроллерах домена. Встроенные локальные группы домена предоставляют добавляемым в них учетным записям пользователей и глобальным группам набор предопределенных прав и разрешений.

Контейнер Builtin содержит все встроенные группы домена. В табл. 8-7 перечислены наиболее часто используемые встроенные локальные группы домена и права, которыми обладают их участники.

Табл. 8-7. Наиболее часто используемые встроенные локальные группы домена

Глобальная группа	Права
Account Operators (Операторы учета)	Члены группы вправе создавать, удалять и изменять права групп и учетных записей пользователей. Члены группы не имеют разрешений на изменение группы Administrators и любых групп операторов
Administrators (Администраторы)	Члены группы вправе выполнять все административные задачи на любых контроллерах домена, включая сам домен. По умолчанию членами данной локальной группы являются учетная запись Administrator, глобальные группы Domain Admins и Enterprise Admins
Backup Operators (операторы архива)	Членам группы позволено архивировать и восстанавливать все контроллеры домена при помощи утилиты Windows Backup (Архивация)
Guests (Гости)	Члены группы могут обращаться лишь к тем ресурсам и выполнять лишь те задачи, на которые у них имеются разрешения. Членам группы запрещено вносить постоянные изменения в конфигурацию рабочего стола. По умолчанию членами этой группы являются учетная запись Guest и глобальная группа Domain Guests. При установке некоторые службы автоматически добавляют пользователей в эту локальную группу. Например, службы Microsoft Internet Information Services (IIS) автоматически добавляют во встроенную группу Guests учетные записи анонимных пользователей

Табл. 8-7. Наиболее часто используемые встроенные локальные группы домена (*окончание*)

Глобальная группа	Права
Pre-Windows 2000 Compatible Access	Группа обратной совместимости, предоставляющая всем пользователям и группам домена разрешение «только для чтения». По умолчанию единственным членом данной группы является группа Everyone (Все) предшествующих ОС Windows
Print Operators (Операторы печати)	Члены группы вправе настраивать и управлять сетевыми принтерами на контроллерах домена
Replicator (Репликатор)	Члены группы могут реплицировать каталог. Единственным членом данной записи должна быть учетная запись пользователя домена, применяемая для регистрации в службе Repli cator контроллера домена. Не добавляйте в данную группу учетные записи реальных пользователей
Server Operators (Операторы сервера)	Члены группы вправе предоставлять в совместное использование дисковые ресурсы, архивировать и восстанавливать файлы на контроллере домена
Users (Пользователи)	Могут обращаться лишь к тем ресурсам и выполнять те задачи, на которые у них имеются разрешения. Членам труппы запрещено вносить постоянные изменения в конфигурацию рабочего стола. По умолчанию членами этой группы являются группа Domain Users , специальные группы Authenticated Users (Прошедшие проверку) и Interactive (Интерактивные). Поддержка системных групп осуществляется Windows 2000; удалить их нельзя. Группу Users рекомендуется применять для предоставления всем учетным записям домена прав и разрешений, которыми должен обладать каждый пользователь

Встроенная локальная группа

На всех изолированных и рядовых серверах, а так же на компьютерах с Windows 2000 Professional есть встроенные локальные группы. Они предоставляют разрешения на выполнение задач (восстановление и архивирование файлов, изменение системного времени, администрирование ресурсов системы и др.) на отдельном компьютере. Windows 2000 помещает встроенные локальные группы в папку Groups (Группы) оснастки Computer Management (Управление компьютером).

В табл. 8-8 описаны права, которыми обладают члены встроенных локальных групп. Кроме специально оговоренных случаев, в группах нет членов по умолчанию.

Табл. 8-8. Наиболее часто используемые встроенные локальные группы

Локальная группа	Права
Administrators (Администраторы)	Члены группы могут выполнять на компьютере любые административные задачи. Встроенная учетная запись Administrator компьютера по умолчанию является членом локальной группы Administrators. Если сервер-член или компьютер Windows 2000 Professional присоединяется к домену, Windows 2000 доба ляет в локальную группу Administrators глобальную группу Domain Admins

Табл. 8-8. Наиболее часто используемые встроенные локальные группы *(окончание)*

Локальная группа	Права
Backup Operators (Операторы архива)	Члены группы могут архивировать и восстанавливать систему с помощью утилиты Windows Backup
Guests (Гости)	Члены группы вправе обращаться лишь к тем ресурсам и выполнять лишь те задачи, на которые у них имеются разрешения. Членам группы запрещено вносить постоянные изменения в конфигурацию рабочего стола. Встроенная учетная запись Guest компьютера по умолчанию является членом локальной группы Guests; при установке эта учетная запись отключается. Если рядовой сервер или компьютер с Windows 2000 Professional присоединяется к домену, доменные группы в эту группу не добавляются
Power Users (Опытные пользователи)	Право создавать и изменять учетные записи пользователей компьютера, открывать доступ к ресурсам
Replicator (Репликатор)	Разрешение настраивать службы репликации файлов
Users (Пользователи)	Члены группы могут обращаться лишь к тем ресурсам и выполнять лишь те задачи, на которые у них есть соответствующие разрешения. Члены группы не могут вносить постоянные изменения в конфигурацию рабочего стола. По умолчанию Windows 2000 добавляет в группу Users все новые локальные учетные записи пользователей. Если рядовой сервер или компьютер с Windows 2000 Professional присоединяются к домену, Windows 2000 добавляет в локальную группу Users глобальную группу Domain Users и специальные группы Authenticated Users и INTERACTIVE

Встроенная **системная группа**

На всех Windows 2000-компьютерах есть встроенные системные группы. Системные группы не имеют определенного списка членов, который разрешалось бы изменять; состав членов таких групп различается в зависимости от метода доступа пользователя к ресурсу или компьютеру. При администрировании групп системные группы недоступны, однако они отображаются при назначении прав и разрешений доступа к ресурсам. Состав системных групп в Windows 2000 основан на способе доступа к компьютеру, а не на том, какие пользователи работают с компьютером. В табл. 8-9 перечислены наиболее часто используемые встроенные системные группы.

Табл. 8-9. Наиболее часто используемые встроенные системные группы

Системная группа	Описание
Anonymous Logon (Анонимный вход)	Включает все учетные записи, не аутентифицированные Windows 2000
Authenticated Users (Прошедшие проверку)	Включает всех пользователей компьютера и службы Active Directory, обладающих действительными учетными записями. Для предотвращения анонимного доступа к ресурсам вместо группы Everyone используйте эту группу

Табл. 8-9. **Наиболее часто используемые встроенные системные группы *(окончание)***

Системная группа	Описание
Creator Owner (Создатель-владелец)	Включает учетную запись пользователя, создавшего или вступившего во владение ресурсом. Если ресурс создан членом группы Administrators, владельцем ресурса считается группа Administrators
Dialup (Удаленный доступ)	Включает всех пользователей, подключенных в текущий момент по удаленному соединению
Everyone (Все)	Сюда входят все пользователи, работающие на компьютере. При назначении разрешений группе Everyone и включении учетной записи Guest будьте особенно осторожны. Windows 2000 аутентифицирует пользователя без действительной учетной записи как гостя (Guest). Такой пользователь автоматически получает все права и привилегии, которыми обладает группа Everyone
Interactive (Интерактивные)	Включает учетную запись пользователя, зарегистрировавшегося в системе. Члены группы Interactive могут подключаться к ресурсам компьютера, на котором они работают в данный момент. Пользователь регистрируется в системе и обращается к ресурсам, «взаимодействуя» с компьютером
Network (Сеть)	Все пользователи, работающие на других компьютерах сети и подключенные к общему ресурсу компьютера, на котором размещается группа

Резюме

Вы узнали, что в Windows 2000 имеется четыре типа встроенных групп: глобальные, локальные группы домена, изолированные локальные и системные. Встроенные группы обладают предопределенным набором членов и прав. Windows 2000 автоматически создает эти группы, и вам не надо вручную создавать группы и назначать разрешения для них.

Занятие 5. Группы для администраторов

Для оптимального уровня безопасности Microsoft рекомендует не включать администраторов в группу Administrators и не работать на компьютере, зарегистрировавшись в системе как администратор. На этом занятии рассказано, почему следует соблюдать эти правила, а также описаны меры безопасности, позволяющие защитить администраторов от различного рода атак.

Изучив материал этого занятия, вы сможете:

- ✓ объяснить, почему не следует работать на компьютере, зарегистрировавшись в системе в качестве администратора;
- ✓ перечислить группы, которые следует использовать администраторам для входа в систему;
- ✓ рассказать об использовании утилиты Run As для запуска программы с правами администратора.

Продолжительность занятия — около 15 минут.

Почему не следует работать на компьютере с полномочиями администратора

Работая на компьютере Windows 2000 в качестве администратора или члена одной из административных групп, вы подвергаете сеть риску различного рода атак. Простое посещение Web-узла может оказаться фатальным. Неизвестные узлы Интернета иногда содержат «троянские» программы, которые копируются и выполняются на вашем компьютере без вашего ведома. Если вы зарегистрировались как администратор, «троянский конь» может отформатировать жесткий диск, удалить все файлы, создать новую учетную запись пользователя с привилегиями администратора и т. п.

Таким образом, добавлять себя в группу Administrators и выполнять обычные задачи, зарегистрировавшись в системе с правами администратора, не рекомендуется. Для выполнения неадминистративной работы добавьте свою учетную запись в группу Users (Пользователи) или Power Users (Опытные пользователи). Если вам понадобится выполнить какую либо административную задачу, вы зарегистрируетесь в системе как администратор, выполните необходимые задачи и завершите сеанс работы.

Администраторы как члены групп Users и Power Users

Зарегистрировавшись в системе как член группы Users, вы можете выполнять обычные задачи, включая запуск приложений и просмотр узлов Интернета, не подвергая компьютер ненужному риску. В качестве члена группы Power Users вы можете выполнять обычные задачи и устанавливать программы, добавлять принтеры и работать с большинством программ из Control Panel. Если вам потребуется выполнить административную задачу, например обновить ОС или изменить параметры системы, завершите текущий сеанс работы и зарегистрируйтесь как администратор.

Если вам часто приходится регистрироваться в системе в качестве администратора для выполнения определенных задач управления, воспользуйтесь утилитой Run As для запуска приложений с правами администратора.

Запуск приложений с помощью утилиты Run As

Для запуска приложения, которому требуются права администратора, можно воспользоваться утилитой Run As. Она позволяет запускать административные программы с правами администратора локального компьютера или администратора домена, когда вы зарегистрированы в системе как обычный пользователь.

Средства утилиты Run As позволяют открыть любое приложение, ярлык программы, сохраненную консоль MMC или программу из Control Panel. При этом:

- необходимо указать соответствующую учетную запись пользователя и пароль;
- учетная запись пользователя должна обладать правами регистрации в данной системе;
- необходимо, чтобы приложение, консоль MMC или программа из Control Panel были доступны системе и учетной записи пользователя.

Некоторые приложения, например Windows Explorer, папка Printers и элементы рабочего стола, косвенно запускаются Windows 2000, их нельзя открыть с помощью утилиты Run As.

▶ **Запуск программы с правами администратора при помощи утилиты Run As**

1. В Windows Explorer щелкните требуемое приложение, ярлык программы, сохраненную консоль MMC или программу из Control Panel.
2. Удерживая клавишу Shift, щелкните приложение, консоль или элемент правой кнопкой мыши и выберите в контекстном меню команду Run As (Запустить как).
3. В диалоговом окне Run As (рис. 8-8) щелкните переключатель Run The Program As The Following User (Запустить программу от имени следующего пользователя).

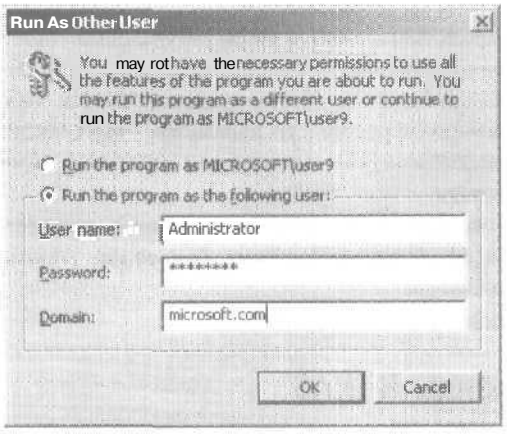


Рис. 8-8. Диалоговое окно Run As

4. Заполните поля User Name и Password, указав учетную запись и пароль администратора.
5. В поле Domain:
   - если вы собираетесь использовать учетную запись администратора локальной системы, наберите имя вашего компьютера;
   - если вы собираетесь использовать учетную запись администратора домена, наберите имя вашего домена.
6. Щелкните OK.

Если вы пытаетесь с помощью утилиты Run As открыть приложение, консоль MMC или элемент Control Panel из сетевого расположения, но при этом реквизиты для подключения к сетевому ресурсу отличаются от реквизитов для запуска приложения, возможно, произойдет сбой. Реквизиты для запуска приложения в некоторых случаях не имеют прав доступа к данному сетевому ресурсу.

При отказе утилиты Run As служба RunAs иногда прекращает свою работу. Из консоли Services (Службы) можно настроить автоматический запуск данной службы при загрузке ОС.

Примечание Утилиту Run As обычно применяют для запуска приложений с правами администратора, ее могут использовать не только администраторы. Любой пользователь, обладающий несколькими учетными записями, вправе открывать приложения, консоли MMC и элементы Control Panel, указывая один из своих реквизитов.

Кроме того, можно задать свойство ярлыков приложений и консолей MMC, при котором для открытия объекта запрашиваются альтернативные реквизиты. Щелкните ярлык правой кнопкой мыши, выберите в контекстном меню команду Properties и щелкните флажок Run As Different User (Запускать от имени другого пользователя). Когда вы щелкнете ярлык, откроется диалоговое окно, предлагающее указать дополнительные имя пользователя, пароль и домен.

Команда RUNAS

Работает аналогично утилите Run As. Синтаксис команды RUNAS таков:

runas [/profile] [/env] [/netonly] /user:*имя_учетной_записи* program

Описание параметров:

- **/profile** — имя профиля пользователя, который требуется загрузить;
- /env — вместо локальной среды пользователя будет использоваться текущее сетевое окружение;
- **/netonly** — указанные учетная запись и пароль применяются лишь для удаленного доступа;
- **/user:*имя_учетной_записи*** — учетная запись в формате *пользователь@домен* или *домен/пользователь,* применяемая для запуска приложения. Чтобы воспользоваться учетной записью администратора локального компьютера, вместо параметра **/user:** введите **/user:*имя_учетной_записи_администратора@имя_компьютера*** или **/user:*имя_компьютера/имя_учетной_записи_администратора***.

  Чтобы воспользоваться учетной записью администратора домена, вместо параметра **/user:** введите **/user:*имя_учетной_записи_администратора@имя_домена*** **или /user:*имя_домена/имя_учетной_записи_администратора***;
- **/program** — запускаемое приложение или выполняемая команда.

Примеры использования команды RUNAS

- Чтобы открыть экземпляр сеанса MS-DOS в Windows 2000 с правами администратора локального компьютера, выполните следующую команду:

  runas /user:*имя_локального_компьютера*\administrator cmd

  По запросу системы введите пароль администратора.
- Чтобы открыть экземпляр оснастки Computer Management с использованием учетной записи администратора домена companydomain\domainadmin, выполните следующую команду:

  runas /user:companydomain\domainadmin «mmc %windir%\system32\compmgmt.msc»

  По запросу системы введите пароль учетной записи.
- Чтобы открыть экземпляр Notepad оснастки Computer Management с использованием учетной записи администратора user в домене domam.microsoft.com, выполните следующую команду:

```
runas /user:user@domain.microsoft.com «notepad my_file.txt»
```

По запросу системы введите пароль учетной записи.

- Чтобы открыть экземпляр сеанса MS-DOS, сохраненной консоли MMC, элемента Control Panel или программы для администрирования сервера в другом лесу, выполните следующую команду;

```
runas /netonly /user:домен\имя_пользователя "команда»
```

домен и *имя_пользователя* должны указывать пользователя, обладающего правами администрирования сервера. По запросу системы введите пароль учетной записи. В этой же ситуации можно выполнить такую команду:

```
runas /user:имя_пользователя@domain.mycompany.com приложение.exe
```

Практикум: запуск программы с правами администратора при помощи утилиты Run As

Вы войдете в систему как User9 (данную учетную запись вы создали, выполняя упражнения предыдущей главы), затем при помощи утилиты Run As откроете консоль Active Directory Users and Computers с правами администратора домена.

▶ **Задание: запустите программу с правами администратора при помощи утилиты Run As**

1. Зарегистрируйтесь в системе, используя учетную запись User9.
2. Раскройте меню Start\Programs\Administrative Tools и выберите (не щелкайте) Active Directory Users And Computers.
3. Удерживая клавишу Shift, щелкните ярлык Active Directory Users And Computers правой кнопкой мыши и выберите в контекстном меню команду Run As (Запустить как).
4. В диалоговом окне Run As (Запуск от имени другого пользователя) щелкните переключатель Run The Program As The Following User (Запустить программу от имени следующего пользователя).
5. Убедитесь, что в поле User Name (Пользователь) значится Administrator.
6. В поле Password (Пароль) наберите пароль администратора.
7. В поле Domain (Домен) наберите **microsoft.com** (или имя своего домена).
8. Щелкните OK.

Теперь вы можете использовать консоль Active Directory Users And Computers с правами администратора.

Резюме

Работая с компьютером Windows 2000 в качестве администратора или члена одной из административных групп, вы подвергаете сеть риску различного рода атак. Для выполнения неадминистративных задач добавьте свою учетную запись в группу Users или Power Users. После этого, если вам потребуется выполнить какую либо административную задачу, вы зарегистрируетесь в системе как администратор, выполните необходимые задачи и завершите сеанс работы. Если вам часто приходится регистрироваться в системе в качестве администратора для выполнения определенных задач управления, воспользуйтесь утилитой Run As.

Утилита Run As позволяет запускать административные программы с правами администратора локального компьютера или администратора домена, когда вы зарегистрированы в системе как обычный пользователь.

Выполняя практикум, вы зарегистрировались в системе как обычный пользователь и при помощи утилиты Run As открыли консоль Active Directory Users and Computers с правами администратора домена.

Закрепление материала

Приведенные ниже вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении А «Вопросы и ответы» в конце книги.

1. Зачем нужны группы?

2. Какова цель добавления одних групп в другие?

3. Почему следует использовать не группы распространения, а группы безопасности?

4. Какую стратегию необходимо выбрать при использовании глобальных и локальных групп домена?

5. Почему не следует применять локальные группы на компьютере, который был присоединен к домену?

6. Опишите простейший способ предоставить пользователю права управления всеми компьютерами в домене?

7. Почему не следует работать на компьютере с полномочиями администратора? Что рекомендуется предпринять вместо этого?

8. Предположим, что штаб-квартира упоминавшейся здесь производственной компании имеет единственный домен в Париже. Менеджерам компании для выполнения своих задач требуется доступ к инвентаризационной БД. Как предоставить менеджерам доступ к этой БД?

9. Предположим, что в этой же компании используется среда с тремя доменами. Корневой домен находится в Париже, а другие домены — в Австралии и Северной Америке. Менеджерам из всех трех доменов для выполнения своих задач требуется доступ к расположенной в Париже инвентаризационной БД. Как предоставить менеджерам доступ к этой БД?

ГЛАВА 9

Безопасность сетевых ресурсов

В этой главе

Здесь рассказывается о разрешениях файлов и папок файловой системы NTFS, реализованной в Microsoft Windows 2000. Вы узнаете, как назначать разрешения файлов и папок NTFS учетным записям и группам и как перемещение и копирование файлов/папок влияет на разрешения файлов/папок NTFS. Кроме того, вы научитесь решать типичные проблемы доступа к ресурсам.

Прежде всего

Для изучения материалов этой главы вы должны:

- выполнить процедуру установки, описанную во вводной главе:
- выполнить упражнения из глав 7 и 8;
- сконфигурировать компьютер как контроллер домена.

Занятие 1. Общие сведения о разрешениях NTFS

Разрешения NTFS — это связанные с объектами правила, которые определяют, какие пользователи могут получить доступ к объекту и каким способом. На этом занятии вы узнаете о стандартных разрешениях NTFS доступа к файлам и папкам, а также о комбинировании разрешений для учетных записей и групп с разрешениями доступа к папкам и файлам.

Изучив материал этого занятия, вы сможете:

- ✓ определить стандартные разрешения NTFS для доступа к файлу и папке;
- ✓ описать результат применения множества разрешений NTFS для доступа к ресурсу;
- ✓ описать результат комбинирования разрешений доступа к ресурсу для учетной записи и для группы.

Продолжительность занятия — около 10 минут.

Разрешения NTFS

Разрешения NTFS позволяют определить круг пользователей и групп, обладающих доступом к файлам и папкам, а также права этих пользователей и групп в отношении данных файлов и папок. Разрешения NTFS доступны только на томах NTFS. На томах FAT или FAT32 использовать разрешения NTFS невозможно. Эффективность системы зашиты NTFS не зависит от способа доступа к файлу — пользователь может обращаться к требуемой папке или файлу как локально, так и по сети. Разрешения для папок отличаются от разрешений для файлов.

Разрешения NTFS для доступа к папкам

Разрешения для папок позволяют управлять доступом пользователей к папкам, а также к находящимся в них файлам/подпапкам и предоставляемым им правам. В табл. 9-1 перечислены стандартные разрешения NTFS для доступа к папке, которые вы можете назначить, и тип доступа, обеспечиваемый каждым разрешением.

Табл. 9-1. Разрешения NTFS для доступа к папке

Разрешение NTFS для доступа к лапке	**Круг полномочий**
Full Control (Полный доступ)	Позволяет менять разрешения, брать во владение и удалять подпапки и файлы, а также выполнять действия, не запрещенные всеми другими NTFS-разрешениями доступа к папке
Modify (Изменение)	Позволяет удалять папку и выполнять действия, допускаемые разрешениями Write и Read & Execute
Read & Execute (Чтение и выполнение)	Позволяет перемещаться через папку, чтобы достичь других файлов и папок, даже если пользователь не имеет разрешения для доступа к ним, и выполнять действия, допускаемые разрешениями Read и List Folder Contents
List Folder Contents (Список содержимого папки)	Позволяет просматривать имена файлов и подпапок в папке

Табл. 9-1. Разрешения NTFS для доступа к папке (*окончание*)

Разрешение NTFS для доступа к папке	Круг полномочий
Read (Чтение)	Позволяет просматривать файлы и подпапки в папке, узнать владельцев, разрешения и атрибуты палок типа Read-Only (Только чтение), Hidden (Скрытый), Archive (Архивный) и System (Системный)
Write (Запись)	Позволяет создавать новые файлы и подпапки в папке, менять атрибуты папки и узнавать владельцев и разрешения папки

Вы можете заблокировать разрешение для учетной записи пользователя или группы. Чтобы запретить доступ к папке, отмените разрешение Full Control.

Разрешения для файлов NTFS

Разрешения для файлов позволяют управлять доступом пользователей к файлам. В табл. 9-2 перечислены стандартные файловые разрешения NTFS, которые вы можете назначить, и обеспечиваемый ими тип доступа.

Табл. 9-2. Разрешения NTFS для доступа к файлу

Разрешение NTFS для доступа к файлу	Круг полномочий
Full Control (Полный доступ)	Позволяет менять разрешения и брать во владение, а также выполнять действия, разрешенные всеми другими NTFS-разрешениями на доступ к этому файлу
Modify (Изменение)	Позволяет изменять и удалять файл, а также выполнять действия, допускаемые разрешениями Write и Read & Execute
Read & Execute (Чтение и выполнение)	Позволяет запускать приложение, а также выполнять действия, допускаемые разрешением Read
Read (Чтение)	Позволяет читать файл, узнать владельца, разрешения и атрибуты файла
Write (Запись)	Позволяет перезаписывать файл, менять атрибуты, читать файл и узнать его владельца и разрешения

Список управления доступом

NTFS ведет *список управления доступом* (access control list, ACL), где перечислены все файлы и папки тома NTFS. В ACL указаны все учетные записи/группы, обладающие доступом к файлу или папке, а также тип предоставленного доступа. Чтобы пользователь получил доступ к ресурсу, в ACL должна присутствовать *запись управления доступом* (access control entry, ACE) для его учетной записи или группы, членом которой он является. Необходимо, чтобы запись обеспечивала требуемый тип доступа, например Read. При отсутствии в ACL соответствующей записи ACE пользователь не сумеет обратиться к ресурсу.

Правила назначения нескольких разрешений NTFS

Учетной записи пользователя и каждой группе, членом которой он является, можно назначить несколько разрешений. Для назначения разрешений необходимо знать правила и

приоритеты, касающиеся порядка назначения и совмещения разрешений NTFS, а кроме того, разбираться в наследовании разрешений NTFS.

Суммирование разрешений

Эффективные разрешения (effective permissions) доступа пользователя к ресурсу — это сумма разрешений NTFS, назначенных отдельной учетной записи пользователя и всем группам, в которых он состоит. Если у пользователя имеется разрешение Read для папки и он является членом группы, обладающей разрешением Write для той же самой папки, на него распространяются оба разрешения.

Разрешения для файлов перекрывают разрешения для папок

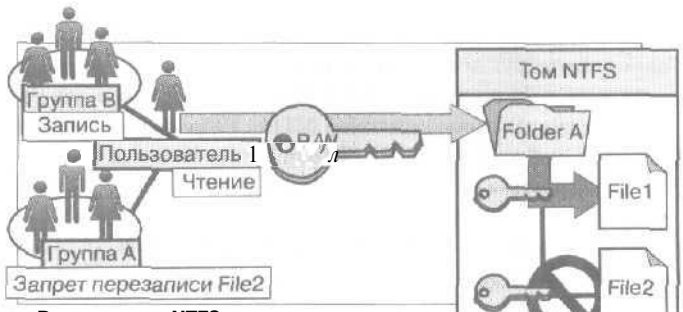
NTFS-разрешения для файлов приоритетнее разрешений для папок. Пользователь, обладающий разрешениями для файла, сможет обратиться к требуемому файлу даже при отсутствии разрешений на доступ к папке, содержащей этот файл. Пользователь вправе открывать файлы, если для этого у него имеются соответствующие разрешения, используя *универсальные правила именования* (universal naming convention, UNC) или локальный путь, даже при отсутствии разрешения на доступ к папке, в которой находится файл, и даже если папка от него скрыта. Иначе говоря, при отсутствии разрешения доступа к папке, содержащей нужный файл, достаточно знать полный путь к нему. Не имея разрешения доступа к папке, вы не сможете просмотреть ее, чтобы найти файл.

Примечание Специальное разрешение Traverse Folder/Execute File (Обзор папок/Выполнение файлов) позволяет или запрещает перемешаться через папку для доступа к другим файлам или папкам, даже если у пользователя нет к ней доступа. Это разрешение действует, только когда группе или пользователю не предоставлено право Bypass Traverse Checking (Обход перекрестной проверки) в оснастке Group Policy (Групповая политика). Подробнее о специальных разрешениях — в занятии 3. Подробнее о правах пользователя — в главе 13.

Приоритет отмены разрешений

Вы можете отменить разрешение на доступ к определенному файлу для учетной записи/группы. Но использовать такой способ контроля доступа к ресурсам не рекомендуется. Отмена разрешения перекрывает все остальные унаследованные разрешения, в том числе разрешения члена группы. Даже если пользователь имеет разрешение на доступ к файлу или папке как член группы, отмена разрешения для пользователя блокирует все другие разрешения, которое пользователь может иметь (рис. 9-1).

На рис. 9-1 иллюстрируется следующая ситуация. Пользователь обладает разрешением Read для папки А и является членом групп А и В. Группа В обладает разрешением Write для папки А. Для группы А аннулировано разрешение Write для доступа к File2. Теперь пользователь может считывать и записывать File1, а также считывать File2. Перезапись File2 невозможна, поскольку пользователь является членом группы А, для которой отменено разрешение записи этого файла.



- **Разрешения NTFS суммируются**
- Файловые разрешения перекрывают разрешения доступа к папкам
- Запрет перекрывает другие разрешения

Рис. 9-1. Несколько разрешений

Наследование разрешений NTFS

По умолчанию разрешения родительской папки наследуются и распространяются на содержащиеся в ней файлы и подпапки. Но наследование разрешений можно предотвратить (рис. 9-2).

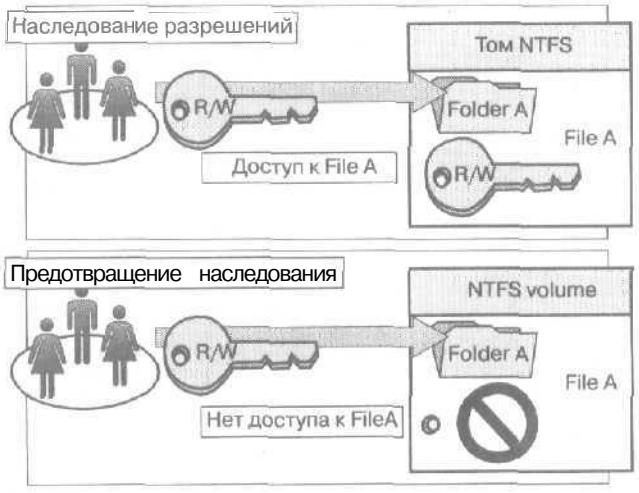


Рис. 9-2. Наследование разрешений

Все разрешения на доступ к родительской папке распространяются на содержащиеся в ней подпапки/файлы, а также на все вновь создаваемые в ней подпапки/файлы, в зависимости от параметров наследования данного объекта.

Предотвращение наследования разрешений

Можно предотвратить наследование разрешений родительской папки вложенными в нее подпапками/файлами, задав для них параметры наследования. Тогда они не будут наследовать разрешения родительской папки. Дочерняя папка, для которой заблокировано наследование разрешений, становится новой родительской папкой, и ее разрешения станут наследовать содержащиеся в ней файлы и подпапки.

Резюме

Разрешения NTFS позволяют определить круг пользователей и групп, обладающих доступом к файлам и папкам, а также права этих пользователей и групп в отношении данных файлов и папок. Разрешения NTFS доступны только на томах NTFS. Разрешения папок — Full Control, Modify, Read & Execute, List Folder Contents, Read и Write. Разрешения файлов подобны разрешениям папки. Разрешения для файлов — Full Control, Modify, Read & Execute, Read и Write.

NTFS ведет список ACL, где перечислены все файлы и папки тома NTFS. В ACL указаны все учетные записи и группы, обладающие доступом к файлу или папке, а также тип предоставленного доступа.

Учетной записи пользователя и каждой группе, членом которой он является, можно назначить несколько разрешений. Разрешения для файлов приоритетнее разрешений для папок.

Разрешения родительской папки наследуются и распространяются на все ее содержимое — файлы и подпапки. Можно предотвратить наследование разрешений родительской папки находящимися в ней подпапками и файлами. Дочерняя папка, для которой заблокировано наследование разрешений, становится новой родительской папкой, и ее разрешения наследуются содержащимися в ней файлами и подпапками. Наследование разрешений можно предотвратить и для файла.

Занятие 2, Назначение разрешений NTFS

При назначении разрешений NTFS необходимо следовать определенным правилам. Назначайте разрешения, допускайте или блокируйте их наследование согласно потребностям пользователя и группы. Из материалов этого занятия вы узнаете, как планировать разрешения NTFS.

Изучив материал этого занятия, вы сможете:

- ✓ спланировать, какие разрешения назначить пользователям или группам для приложений и папок данных;
- ✓ назначить учетным записям и группам разрешения доступа к папке и файлу

Продолжительность занятия - около 60 минут.

Планирование разрешений NTFS

Разрешениями NTFS легко управлять. Для этого вам надо усвоить несколько правил.

1. Группируйте файлы в папки приложений, папки данных и домашние папки. Сосредоточьте домашние и общие папки на отдельном томе, где нет приложений и файлов ОС. Благодаря этому:
   - вы сможете назначать разрешения только папкам, а не отдельным файлам;
   - упростится порядок резервного копирования — вам не придется архивировать файлы приложений; кроме того, все домашние и общие папки будут находиться на одном томе.
2. Предоставляйте пользователям лишь необходимый уровень доступа. Если пользователю достаточно лишь читать файл, назначьте его учетной записи разрешение Read. Так вы снизите вероятность случайного изменения или удаления важных документов и файлов приложений.
3. Создавайте группы в соответствии с типом доступа к ресурсам, который необходим членам группы, и затем назначайте соответствующие разрешения доступа. Назначать разрешения отдельным учетным записям следует лишь при необходимости.
4. Назначьте группам Users и Administrators разрешение Read & Execute для работы с данными и приложениями. Это предотвратит случайное удаление или повреждение приложений пользователями или вирусами,
5. Отключите наследование разрешений на уровне домашней папки. Это позволит пользователю определять разрешения для каждого файла или папки в домашней папке.
6. Помимо разрешения Read & Execute назначьте группе Users разрешение Write, а владельцам файлов и папок — Full Control. По умолчанию пользователь, создавший файл, является также его владельцем. Создав файл, вы можете предоставить другому пользователю разрешение стать его владельцем. При этом пользователи получают право считывать и изменять созданные другими пользователями документы, а также считывать, изменять и удалять собственные файлы и папки.
7. Отменяйте разрешения, только если необходимо заблокировать определенный тип доступа для некоторой учетной записи или группы.
8. Назначайте пользователями разрешения доступа к создаваемым ими файлам и папкам и научите их это делать.

Назначение разрешений NTFS

По умолчанию при форматировании тома NTFS группе Everyone (Все) назначается разрешение Full Control. В целях управления доступом пользователей к ресурсам это разрешение следует сменить и назначить другие разрешения NTFS. Будьте внимательны, назначая разрешения группе Everyone (Все) и активизируя учетную запись Guest (Гость). Windows 2000 аутентифицирует (проверяет подлинность) пользователя, не имеющего действительной учетной записи, как Guest. Этот пользователь автоматически получает все права и разрешения, назначенные группе Everyone (Все).

Назначение или смена разрешения

Администраторы, пользователи с разрешением Full Control и владельцы файлов/папок могут назначать разрешения учетным записям и группам.

▶ **Назначение или изменение разрешений NTFS для файла или папки**

1. Щелкните правой кнопкой мыши файл или папку, для которой вы хотите назначить разрешения, и выберите команду Properties (Свойства).
2. На вкладке Security (Безопасность) диалогового окна свойств (рис. 9-3) задайте параметры, описанные в табл. 9-3.

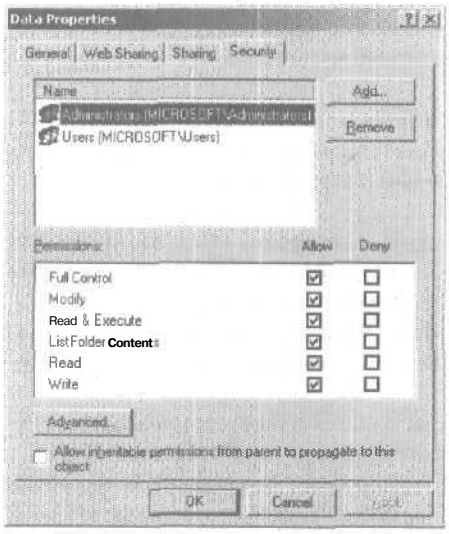


Рис. 9-3. Вкладка Security диалогового окна свойств для папки Data

Табл. 9-3. Параметры вкладки Security

Параметр	Описание
Name (Имя)	Позволяет выбрать учетную запись или группу, для которой вы хотите изменить разрешения или которую вы хотите удалить из списка
Permissions (Разрешения)	Пометив флажок Allow (Разрешить), вы включите разрешение, а пометив флажок Deny (Запретить), — отмените его

Табл. 9-3. Параметры вкладки Security *(окончание)*

Параметр	Описание
Add (Добавить)	Открывает диалоговое окно Select Users, Computers, Or Groups (Выбор Пользователи, Компьютеры или Группы), в котором можно указать учетные записи и группы для добавления в список Name
Delete (Удалить)	Удаляет выбранную учетную запись или группу и соответствующие разрешения доступа к данному файлу или папке
Advanced (Дополнительно)	Открывает для выбранной папки окно Access Control Settings (Параметры управления доступом), в котором вы можете предоставить или отменить специальные разрешения
Allow Inheritable Permissions From Parent To Propogate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект)	Определяет, будет ли этот объект наследовать разрешения от своего родительского объекта

Предотвращение **наследования разрешений**

По умолчанию подпапки и файлы наследуют разрешения родительской папки. Порядок наследования файлов регулируется в окне свойств папки на вкладке Security флажком Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект). Если флажки под разрешениями затенены, то файл или папка наследуют разрешения родительской папки.

Чтобы блокировать наследование разрешений родительской папки, сбросьте флажок Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект). Вам будет предложено выбрать один из параметров (табл. 9-4).

Табл. 9-4. Параметры, позволяющие предотвратить наследование разрешений

Параметр	Описание
Copy (Копировать)	Разрешения на доступ к родительской папке копируются для текущей папки, последующее наследование разрешений на доступ к родительской папке аннулируется
Delete (Удалить)	Унаследованные от родительской папки разрешения удаляются, сохраняются только разрешения, назначенные вами явно
Cancel (Отмена)	Диалоговое окно закрывается, состояние флажка Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект) не меняется

Практикум: планирование и назначение разрешений NTFS

Спланируйте разрешения доступа к папкам и файлам, исходя из бизнес-сценария. Затем реализуйте разрешения NTFS для файлов и папок вашего компьютера на основе второго сценария. Наконец, проверьте назначенные разрешения NTFS и убедитесь, что они работают должным образом.

Упражнение 1: планирование разрешений NTFS

Сейчас вы спланируете назначение разрешений NTFS для файлов и папок компьютера с Windows 2000 Professional на основе приведенного далее сценария.

Сценарий

По умолчанию группе Everyone (Все) назначено разрешение Full Control для всех файлов и папок (рис. 9-4). Изучите следующие критерии безопасности и запишите изменения, которые надо внести в разрешения файлов/папок NTFS , чтобы они соответствовали этим критериям.

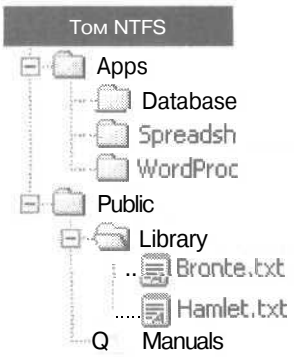


Рис. 9-4. Структура папок и файлов для упражнения

Для планирования разрешений NTFS определите:

- группы, которые требуется создать, и встроенные группы, которые вы собираетесь использовать;
- необходимые пользователям разрешения для доступа к папкам и файлам;
- необходимость отмены наследования разрешений для папок или файлов.

Помните:

- разрешения NTFS, назначенные папке, наследуются всеми ее подпапками/файлами. Чтобы назначить разрешения всем подпапкам/файлам папки Apps, назначьте этой папке разрешение NTFS;
- чтобы назначить папке или файлу более строгие разрешения, следует либо отменить нежелательные разрешения, либо блокировать наследование разрешений, сняв флажок Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект).

Задайте следующие критерии.

- Помимо встроенных групп, создайте группы Accounting, Managers, Executives.
- Назначьте группе Administrators (Администраторы) разрешение Full Control для доступа ко всем папкам и файлам.

- Пусть все пользователи запускают программы в папке WordProc, но не имеют возможности изменять файлы в этой папке.
- Право читать документы в папках приложений Spreadsheet и Database, запуская соответствующие программы для работы с БД и электронными таблицами, должны иметь лишь члены групп Accounting, Managers и Executives. Но лишите их возможности изменять файлы в этих папках.
- Всем пользователям надо предоставить право считывать и создавать файлы в папке Public.
- Никто не должен иметь прав изменять файлы в папке Public\Library.
- Возможность изменять и удалять файлы в папке Public\Manuals предоставляется лишь пользователю User81.

Какое разрешение NTFS по умолчанию следует удалить при назначении пользовательских разрешений файлу или папке?

Заполните табл. 9-5, чтобы спланировать и записать разрешения.

Табл. 9-5. Планирование разрешений для упражнения 1

Путь	Учетная запись пользователя или группы	Разрешения NTFS	Блокирование наследования (да\нет)
Apps			
Apps\WordProc			
Apps\Spreadsh			
Apps\Database			
Public			
Public\Library			
Public\Manuals			

Упражнение 2: назначение разрешений NTFS для папки Data

Сейчас вы назначите разрешения доступа к папке C:\Data (где C:\ — имя вашего системного диска), согласно приведенному ниже сценарию. Создайте сначала учетные записи пользователей и группы, перечисленные в табл. 9-6.

Табл. 9-6. Учетные записи пользователей и группы для упражнения 2

Группа	Учетная запись пользователя
Administrators (Администраторы)	User81, член группы Print Operators (Операторы печати)
Sales	User82, член групп Sales и Print Operators
Sales	UserS3, член групп Administrators и Print Operators

Создайте следующие папки (где C:\ — имя вашего системного диска):

- C:\Data
- C:\Data\Managers
- C:\Data\Managers\Reports
- C:\Data\Sales

Сценарий

Выполните следующие условия:

- все пользователи должны иметь возможность считывать документы и файлы в папке Data;
- всем пользователям разрешено создавать документы в папке Data;
- всем пользователям разрешено изменять содержание, свойства и разрешения документов, создаваемых ими в папке Data.

▶ Задание 1: удалите разрешения для группы Everyone (Все)

1. Зарегистрируйтесь как Administrator.
2. Щелкните значок My Computer (Мой компьютер) правой кнопкой мыши и выберите в контекстном меню команду Explore.
3. Откройте локальный диск C:\, щелкните правой кнопкой мыши папку Data и выберите в контекстном меню команду Properties (Свойства).

   Откроется диалоговое окно свойств папки Data на вкладке General (Общие).
4. Перейдите на вкладку Security (Безопасность), чтобы просмотреть разрешения доступа к папке Data.

   Перечислите имеющиеся разрешения на доступ к папке Data.

   Обратите внимание, что текущие разрешения изменить нельзя.
5. В списке Name (Имя) выберите группу Everyone (Все) и щелкните кнопку Remove (Удалить).

   Что вы видите?
6. Щелкните OK. чтобы закрыть окно сообщения.
7. Сбросьте флажок Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект), чтобы отменить наследование разрешений.

   В открывшемся диалоговом окне вам будет предложено скопировать для папки текущие унаследованные разрешения или удалить все разрешения, кроме назначенных явным образом.
8. Щелкните кнопку Remove (Удалить).

   Перечислите имеющиеся разрешения доступа к папке Data.

▶ Задание 2: назначьте группе Users (Пользователи) разрешение на доступ к папке Data

1. В диалоговом окне свойств папки Data щелкните кнопку Add (Добавить).

   Откроется диалоговое окно Select Users, Computers, Or Groups (Выбор: Пользователи, Компьютеры или Группы).
2. В списке Look In (Искать в) вверху окна выберите ваш домен.

   В этом списке можно указать компьютер или домен, откуда будут выбраны учетные записи для предоставления разрешений. Вам надо указать ваш домен, чтобы выбрать одну из учетных записей и групп, которые вы создали.
3. В списке Name (Имя) выберите Users (Пользователи) и щелкните кнопку Add (Добавить).

   Пользователи перечислены внизу диалогового окна Select Users, Computers, Or Groups Groups (Выбор: Пользователи, Компьютеры или Группы). В этом поле вы можете набрать несколько имен, разделяя их точкой с запятой. Если соответствующий объект хранится в доменном или глобальном каталоге Windows 2000, достаточно после набора первых символов имени щелкнуть кнопку Check Names. Windows 2000 завершит имя или предложит вам выбрать имя из списка.

4. Щелкните (Ж, чтобы вернуться в диалоговое окно свойств папки Data.
   Перечислите имеющиеся разрешения на доступ к папке.
5. Убедитесь, что выбрана группа Users (Пользователи), и пометьте флажок Allow (Разрешить) у разрешения Write.
6. Щелкните кнопку Apply (Применить), чтобы сохранить внесенные изменения.

► **Задание 3: назначьте группе CREATOR OWNER (Создатель-владелец) разрешения на доступ к папке Data**

1. В диалоговом окне свойств папки Data щелкните кнопку Add (Добавить).
   Откроется диалоговое окно Select Users, Computers, Or Groups (Выбор: Пользователи, Компьютеры или Группы).
2. Выберите в поле Look In (Искать в) вверху окна ваш домен.
3. В списке Name (Имя) выберите CREATOR OWNER (Создатель-владелец) и щелкните кнопку Add (Добавить).
   В поле под списком Name (Имя) внизу окна появится строка CREATOR OWNER (Создатель-владелец).
4. Щелкните OK, чтобы вернуться в окно свойств папки Data.
   Перечислите существующие разрешения папки.
5. Убедитесь, что выбрана группа CREATOR OWNER (Создатель-владелец), и пометьте флажок Allow (Разрешить) у разрешения Full Control. Затем щелкните кнопку Apply (Применить), чтобы сохранить внесенные изменения.
   Что вы видите?
6. Щелкните кнопку Advanced (Дополнительно), чтобы изучить дополнительные разрешения.
   Откроется диалоговое окно Access Control Settings For Data (Параметры управления доступом для Data).
7. Под полем Name (Имя) выберите CREATOR OWNER (Создатель-владелец).
   Какие разрешения назначены группе CREATOR OWNER (Создатель-владелец) и на какие файлы и папки они распространяются?
8. Щелкните OK.
9. В диалоговом окне свойств папки Data щелкните OK, затем выйдите из вашего домена.

► **Задание 4: проверьте разрешения, назначенные папке Data**

1. Зарегистрируйтесь в системе как User81 и запустите Windows Explorer (Проводник).
2. Откройте папку C:\Data.
3. В папке Data попробуйте создать текстовый файл с именем user81.
   Удалось ли это сделать? Почему?
4. Попробуйте выполнить с только что созданным файлом следующие операции: откройте файл; измените файл; удалите файл.
   Вы можете открывать, изменять и удалять файл, поскольку группа CREATOR OWNER (Создатель-владелец) обладает разрешением Full Control для папки Public.
5. Закройте все приложения и завершите сеанс работы с Windows 2000.

Упражнение 3: назначение разрешений NTFS

Сейчас вы назначите разрешения NTFS на доступ к папкам Data, Managers, Reperts и Sales согласно приведенному далее сценарию.

Сценарий

Назначьте папкам разрешения согласно табл. 9-7.

Табл. 9-7. *Разрешения* папок для упражнения 3

Имя папки	Учетная запись или группа	Разрешение
C:\Data	Группа Users (Пользователи)	Read & Execute
	Группа Administrators (Администраторы)	Full Control
C:\Data\Managers	Группа Users	Read & Execute
	Группа Administrators	Full Control
	Группа Managers	Modify
C:\Data\Managers\Reports	Группа Users	Read & Execute
	Группа Administrators	Full Control
	User82	Modify
C:\Data\Sales	Группа Users	Read & Execute
	Группа Administrators	Full Control
	Группа Accounting	Modify

► **Задание: назначьте разрешение на доступ к папке**

1. Зарегистрируйтесь в системе как Administrator и запустите Windows Explorer (Проводник).
2. Откройте локальный диск C;\.
3. Щелкните правой кнопкой мыши значок папки, для которой требуется изменить разрешения, и выберите в контекстном меню команду Properties (Свойства).

   Откроется окно свойств данной папки с выбранной вкладкой General (Обшие).
4. Перейдите на вкладку Security (Безопасность).
5. Если нужно изменить унаследованные разрешения для пользователя, учетной записи или группы, сбросьте флажок Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект) и, когда появится соответствующий запрос, щелкните кнопку Copy (Копировать).
6. Чтобы добавить учетным записям или группами разрешения для данной папки, щелкните кнопку Add (Добавить).

   Откроется диалоговое окно Select Users, Computers, Or Groups (Выбор: Пользователи, Компьютеры или Группы).
7. Убедитесь, что в списке Look In (Искать в) в верхней части окна выбран ваш домен.
8. В списке Name (Имя) выберите имя требуемой учетной записи или группы, сверившись со сценарием, и щелкните кнопку Add (Добавить).

   Учетная запись или группа появится в списке Name (Имя).
9. Повторите пункт 8 для каждой учетной записи или группы, перечисленной для данной папки в сценарии.
10. Щелкните OK, чтобы вернуться к диалоговому окну свойств.
11. Если окно Properties (Свойства) содержит учетные записи и группы, не перечисленные в сценарии, выделите их и щелкните кнопку Remove (Удалить).
12. Для всех учетных записей и групп, перечисленных для данной папки в предыдущем сценарии, выберите в списке Name учетную запись или группу, затем в списке разре-

шений пометьте флажок Allow (Разрешить) или Deny (Отменить) согласно требованиям сценария из упражнения 2.
13. Щелкните OK, чтобы сохранить изменения и закрыть диалоговое окно свойств,
14. Повторите эту процедуру для каждой папки, которой назначаете разрешения (см. сценарий).
15. Завершите рабочий сеанс.

Упражнение 4: проверка разрешений NTFS

Сейчас вы зарегистрируетесь в системе по разным учетным записям и проверите разрешения NTFS.

▶ **Задание 1: проверьте разрешения на доступ к папке Reports пользователя User81**

1. Зарегистрируйтесь в системе как User81 и запустите Windows Explorer (Проводник).
2. Откройте папку C:\Data\Managers\Reports.
3. Попробуйте создать файл в папке Reports.
   Удалось ли это? Почему?
4. Закройте Windows Explorer (Проводник) и завершите рабочий сеанс.

▶ **Задание 2: проверьте разрешение на доступ к папке Reports пользователя User82**

1. Зарегистрируйтесь в системе как User82 и запустите Windows Explorer (Проводник).
2. Откройте папку C:\Data\Managers\Reports.
3. Попробуйте создать файл в папке Reports.
   Удалось ли это? Почему?
4. Завершите рабочий сеанс.

▶ **Задание 3: проверьте разрешение на доступ к папке Sales пользователя Administrator**

1. Зарегистрируйтесь в системе как Administrator и запустите Windows Explorer (Проводник).
2. Откройте папку C:\Data\Sales.
3. Попробуйте создать файл в папке Sales.
   Удалось ли это? Почему?
4. Закройте Windows Explorer (Проводник) и завершите рабочий сеанс.

▶ **Задание 4: проверьте разрешение на доступ к папке Sales пользователя User81**

1. Зарегистрируйтесь в системе как User81 и запустите Windows Explorer (Проводник).
2. Откройте папку C:\Data\Sales,
3. Попробуйте создать файл в папке Sales.
   Удалось ли это? Почему?
4. Закройте Windows Explorer (Проводник) и завершите рабочий сеанс.

▶ **Задание 5: проверьте разрешения на доступ к папке Sales пользователя User82**

1. Зарегистрируйтесь в системе как User82 и запустите Windows Explorer (Проводник).
2. Откройте папку C:\Data\Sales.
3. Попробуйте создать файл в папке Sales.
   Удалось ли это? Почему?
4. Закройте все приложения и завершите рабочий сеанс.

Резюме

По умолчанию при форматировании тома NTFS группе Everyone (Все) назначается разрешение Full Control. Для управления доступом пользователей к ресурсам это разрешение следует сменить и назначить другие разрешения NTFS. Члены группы Administratots (Администраторы), владельцы файлов или папок и пользователи с разрешением Full Control могут назначать разрешения NTFS для пользователей и групп, чтобы управлять доступом к файлам и папкам. Назначение или смена разрешений NTFS на доступ к файлу или папке выполняется на вкладке Security (Безопасность) диалогового окна свойств этого файла или папки.

Подпапки и файлы по умолчанию наследуют разрешения родительской папки. Наследование разрешений можно отключить, после чего подпапки и файлы не будут наследовать разрешения, назначенные родительскому каталогу. При выполнении упражнений вы создали папки, назначили разрешения NTFS и проверили их, чтобы убедиться, что они настроены правильно.

Занятие 3. Специальные разрешения

Стандартные разрешения NTFS не всегда способны обеспечить особые права доступа. Для этого лучше назначить специальные разрешения NTFS, о которых мы и расскажем на этом занятии. Также мы опишем требования и процедуры, необходимые, чтобы стать владельцем папки или файла.

Изучив материал этого занятия, вы сможете:

- ✓ определить специальные разрешения;
- ✓ предоставить пользователям возможность изменять разрешения на доступ к файлам и папкам;
- ✓ предоставить пользователям возможность получать права владельцев файлом и папок;
- ✓ объяснить, как стать владельцем файла или папки;
- ✓ взять во владение файл или папку.

Продолжительность занятия — около 20 минут.

Специальные разрешения

Специальные разрешения, перечисленные в табл. 9-8. обеспечивают дополнительные возможности доступа для пользователей.

Табл. 9-8. Специальные разрешения на доступ к файлам **и папкам**

Специальное разрешение	Круг полномочий
List Folder/Read Data (Содержание папки/Чтение данных)	List Folder позволяет или запрещает просматривать имена файлов и названия папок внутри папки (применяется только к папкам). Read Data позволяет или запрещает просматривать данные в файлах (применимо только к файлам)
ReadAttributes(Чтение атрибутов)	**Позволяет или** запрещает **просматривать атрибуты** файла или папки, например **Read-Only** (Только **чтение) и** Hidden **(Скрытый).** Атрибуты определяются NTFS
Read Extended Attributes **(Чтение дополнительных** атрибутов)	Позволяет или запрещает просматривать дополнительные атрибуты файла или папки. Дополнительные атрибуты определяются программно и могут меняться
Read Permissions (Чтениеразрешений)	Позволяет или запрещает читать разрешения для файла или папки, например Full Control, Read и Write
Traverse Folder/Execute File (Обзор папок/Выполнение файлов)	Traverse Folder позволяет или запрещает перемещение через папки, к которым пользователь не имеет разрешения обращаться, чтобы добраться до файлов или папок, к которым пользователь имеет право обращаться (применяется только к папкам). Разрешение Traverse Folder вступает в силу, только когда группе или пользователю не предоставлено право пользователя Bypass Traverse Checking (Обход перекрестной проверки) в групповой политике. По умолчанию группе Everyone (Все) предоставляется право пользователя Bypass Traverse Checking. Разрешение Traverse Folder для папки не устанавливает разрешение Execute File для всех файлов в этой папке автоматически. Execute File позволяет или запрещает запускать программные файлы (применяется только к файлам)

Табл. 9-8. Специальные разрешения на доступ к файлам и папкам (*окончание*)

Специальное разрешение	Круг полномочий
Create Files/Write Data (Создание файлов/Запись данных)	Разрешение Create Files позволяет или запрещает создавать файлы в папке (применяется только к папкам). Разрешение Write Data позволяет или запрещает вносить изменения в файл и переписывать существующее содержание (применяется только к файлам)
Create Folders/Append Data (Создание файлов/Дозапись данных)	Разрешение Create Folders позволяет или запрещает создавать подпапки в папке (применяется только к папкам). Разрешение Append Data позволяет или запрещает добавлять данные в конец файла, но не изменением, удалением или перезаписью существующих данных (применяется только к файлам)
Write Attributes (Запись атрибутов)	Позволяет или запрещает менять атрибуты файла или папки, например Read-Only и Hidden. Атрибуты определяются NTFS
Write Extended Attributes (Запись дополнительных атрибутов)	Позволяет или запрещает менять расширенные атрибуты файла или папки. Расширенные атрибуты определяются программно и могут измениться
Delete Subfolders and Files (Удаление подпапок и файлов)	Позволяет или запрещает удалять подпапки и файлы, даже если им не назначено разрешение Delete
Delete (Удаление)	Позволяет или запрещает удалять файл или папку. Не имея разрешения Delete для файла или папки, вы сможете удалить его, если вам предоставлено разрешение Delete Subfolders and Files для родительской папки
Change Permissions (Смена разрешений/Смена владельца)	Позволяет или запрещает менять разрешения для файла или папки, например Full Control, Read и Write
Take Ownership (Смена владельца)	Позволяет или запрещает взять во владение файл или папку. Владелец всегда имеет право менять разрешения для файла или папки, независимо от любых разрешений, защищающих файл или папку
Synchronize (Синхронизация)	Позволяет или запрещает различным потокам ожидать дескриптора файла или папки и синхронизироваться с другим потоком, который может освободить его. Это разрешение имеет смысл только для многопоточных, многопроцессных программ

Специальные разрешения назначаются в диалоговом окне Permission Entry (Элементы разрешений) для соответствующего файла или папки. Чтобы его открыть, щелкните кнопку Advanced (Дополнительно) на вкладке Security (Безопасность) диалогового окна свойств файла или папки, а затем в окне Access Control Setting (Параметры управления доступом) для файла или папки щелкните кнопку View/Edit (Показать/Изменить).

Каждое из стандартных разрешений состоит из логической группы специальных разрешений. В табл. 9-9 перечислены стандартные разрешения и возможные для них специальные разрешения.

Табл. 9-9. Специальные разрешения, связанные со стандартными разрешениями на доступ к файлам и папкам

Специальное разрешение	lull Control	Modify	Read & Execute	List Folder Contents	Read
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	ч	x			x
Create Folders /Append Data	x	x			x
Write Attributes	x	x			x
Write Extended Attributes	x	x			x
Delete Subfol-ders and Files	x				
Delete	x	x			
Read Permissions	x	x	x	x	x
Change Permissions	x				
Take Ownership	x				
Synchronize	x	x	x	x	x

Примечание Хотя разрешения List Folder Contents и Read & Execute связаны, как показано, с одними и теми же специальными разрешениями, последние по-разному наследуются. Разрешение List Folder Contents наследуется папками, но не файлами и появляется, только когда вы просматриваете разрешения папки. Разрешение Read & Execute наследуется и файлами, и папками и всегда действует, когда вы просматриваете разрешения папки или файла.

Назначая специальные разрешения на доступ к папкам, вы можете выбрать, где применять разрешения для подпапок и файлов, расположенным ниже по иерархии.

Специальные разрешения Change Permissions и Take Ownership особенно полезны для управления доступом к ресурсам.

Смена разрешений

Пользователям и другим администраторам можно предоставить право изменять разрешения на доступ к файлу или папке, не предоставляя им разрешения Full Control для этого файла или папки. Таким образом, администратору или пользователю не удастся удалить или изменить файл или папку, но они смогут назначать для них разрешения.

Чтобы предоставить администраторам право изменять разрешения, назначьте группе Administrators разрешение Change Permissions для файла/папки.

Получение прав владельца

Принадлежащие пользователям и группам файлы и папки разрешается передавать во владение другим группам и пользователям. Вы можете предоставить какому-нибудь пользователю право стать владельцем объекта. Это же право доступно и вам, как администратору.

Помните правило: текущий владелец или любой пользователь с разрешением Full Control может назначить другой учетной записи или группе стандартное разрешение Full Control или специальное разрешение Take Ownership, предоставляя право на получение прав владельца объекта.

Администратор может стать владельцем папки или файла независимо от назначенных разрешений. Если администратор получает объект во владение, владельцем файла или папки становится группа Administrators (Администраторы), и любой ее член вправе изменять разрешения доступа к объекту и назначать разрешение Take Ownership другой учетной записи/группе. Например, если сотрудник увольняется, администратору разрешается взять во владение его файлы и назначать разрешение Take Ownership другому сотруднику. Затем последний сможет взять во владение файлы уволившегося сотрудника.

Внимание! Назначить кого-либо владельцем файла или папки нельзя. Владелец файла, администратор или пользователь с разрешением Full Control могут назначить разрешение Take Ownership учетной записи или группе, позволяя им стать владельцем объекта. Чтобы стать владельцем файла/папки, пользователь или член группы с разрешением Take Ownership должен явно получить его во владение.

Назначение специальных разрешений

Специальные разрешения позволяют пользователям изменять разрешения, а также становиться владельцами файлов и папок.

▶ **Задание разрешения Change Permissions или Take Ownership**

1. Щелкните правой кнопкой мыши файл или папку, для которых хотите установить специальные разрешения, в контекстном меню выберите пункт Properties (Свойства), затем перейдите на вкладку Security (Безопасность).
2. Щелкните кнопку Advanced (Дополнительно).
3. На вкладке Permissions (Разрешения) в диалоговом **окне** Access Control Settings (Параметры управления доступом) для файла или папки выберите учетную запись или группу, для которой вы хотите задать специальные разрешения (рис. 9-5).

   В диалоговом окне Access Control Settings вы можете просмотреть разрешения, которые применяются к файлу или папке, и где эти разрешения применяются, а также имя владельца.
4. Для флажка Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект):
   - пометьте флажок, чтобы разрешить для данного объекта наследование разрешений родительской папки,

     или
   - сбросьте, чтобы запретитьдля данного объекта наследование разрешений родительской папки.

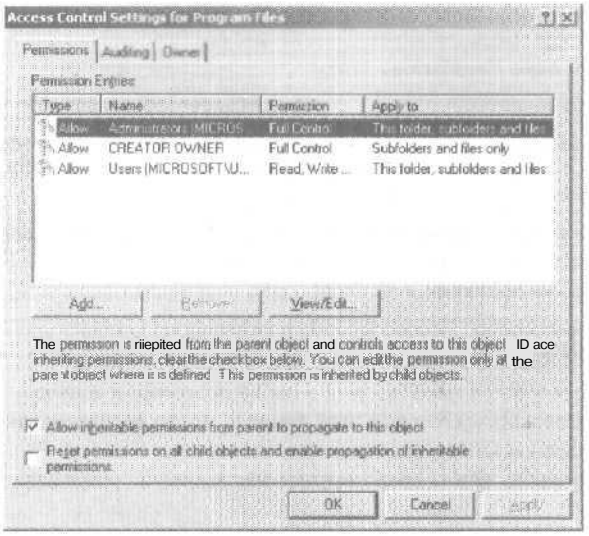


Рис. 9-5. **Диалоговое окно Access Control Settings (Параметры управления** доступом) для **папки Program Files**

5. Для флажка Reset Permissions On All Child Objects (Сбросить разрешения для всех дочерних объектов):
   - пометьте флажок, чтобы сбросить любые существующие разрешения для дочерних объектов так, чтобы эти объекты унаследовали разрешения родительского объекта, или
   - сбросьте флажок, чтобы не отменять существующие разрешения для дочерних объектов.
6. Щелкните View/Edit (Показать/Изменить), чтобы открыть диалоговое окно Permission Entry (Элемент разрешения) для файла или папки (рис. 9-6).

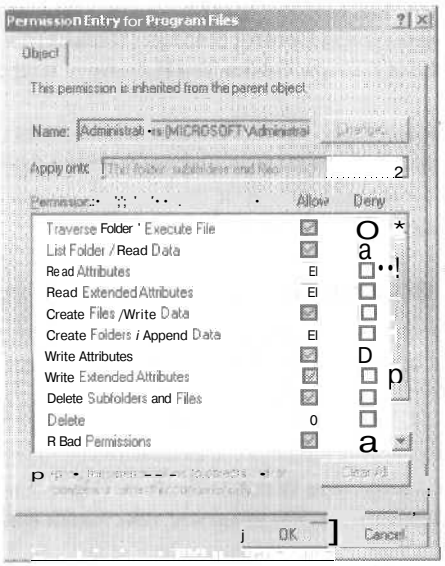


Рис. 9-6, Диалоговое окно Permission Entry для папки Program Files

Параметры диалогового окна Permission Entry описаны в табл. 9-10.

Табл. 9-10. Параметры в диалоговом окне Permissions Entry

Параметр	Описание
Name (Имя)	**Учетная** запись или имя группы. **Чтобы выбрать другую** учетную запись **или группу,** щелкните **кнопку** Change (Изменить)
Apply Onto (Применять)	Уровень иерархии папок, на котором унаследованы специальные разрешения NTFS. Значение по умолчанию — This Folder, Subfolders And Files (Для этой папки, ее подпапок и файлов)
Permissions (Разрешения)	Специальные разрешения. Чтобы включить разрешение Change Permissions или Take Ownership, пометьте флажок Allow (Разрешить)
Apply These Permissions To Objects And/Or Containers Within This Container Only (Применять эти разрешения к объектам и контейнерам только внутри этого контейнера)	Определяет, наследуют ли находящиеся в папке подпапки и файлы специальные разрешения. Отметьте этот флажок, чтобы распространить специальные разрешения доступа на вложенные файлы и папки. Сбросьте этот флажок, чтобы предотвратить наследование разрешений
Clear All (Очистить все)	Щелкните эту кнопку, чтобы отменить все выбранные разрешения

Получение файла или папки во владение

Чтобы стать владельцем файла или папки, пользователь или член группы с разрешением Take Ownership (Смена владельца) должен явно получить его во владение.

▶ **Получение прав владельца файла или папки**

1. На вкладке Owner (Владелец) диалогового окна Access Control Settings (Параметры управления доступом) выберите свое имя в списке Change Owner To (Изменить владельца на).
2. Пометьте флажок Replace Owner On Subcontainers And Objects (Заменить владельца субконтейнеров и объектов), чтобы стать владельцем всех содержащихся в папке файлов и подкаталогов.
3. Щелкните OK.

Практикум: получение файла во владение

Для получения файла во владение определите для него разрешения, назначьте разрешение Take Ownership учетной записи и возьмите файл во владение с помощью этой учетной записи.

▶ **Задание 1: определите разрешения для файла**

1. Зарегистрируйтесь в домене как Administrator и запустите Windows Explorer (Проводник).
2. В папке C:\Data (где C:\ — имя вашего системного диска) создайте текстовый файл с именем OWNER.
3. Щелкните правой кнопкой мыши файл OWNER.TXT и выберите команду Properties (Свойства).

Откроется окно свойств файла с активной вкладкой General (Общие).

4. Перейдите на вкладку Security (Безопасность), чтобы увидеть разрешения для файла OWNER.TXT.

   Каковы текущие разрешения для OWNER.TXT?

5. Щелкните кнопку Advanced (Дополнительно).

   Откроется диалоговое окно Access Control Settings For OWNER.TXT (Параметры управления доступом для OWNER.TXT) с активной вкладкой Permissions (Разрешения).

6. Перейдите на вкладку Owner (Владелец).

   Кто является текущим владельцем файла OWNER.TXT?

▶ Задание 2: назначьте пользователю разрешение Take Ownership

1. В диалоговом окне Access Control Settings For OWNER.TXT (Параметры управления доступом для OWNER.TXT) перейдите на вкладку Permissions (Разрешения).
2. Щелкните кнопку Advanced (Дополнительно).

   Откроется диалоговое окно Select User, Computer, Or Group (Выбор: Пользователи, Компьютеры или Группы).

3. В списке Look In (Искать в) выберите ваш домен.
4. В списке Name (Имя) выберите User83, затем щелкните OK.

   Откроется диалоговое окно Permission Entry For OWNER.TXT.

   Обратите внимание, что нет ни одного разрешения для User84.

5. В списке разрешений пометьте флажок Allow (Разрешить) у разрешения Take Ownership.
6. Щелкните OK.

   Откроется окно Access Control Settings For OWNER.TXT (Параметры управления доступом для OWNER.TXT) с выбранной вкладкой Permissions (Разрешения).

7. Щелкните OK, чтобы вернуться в диалоговое окно свойств.
8. Щелкните OK, чтобы сохранить изменения и закрыть диалоговое окно свойств OWNER.TXT.
9. Закройте все приложения и завершите сеанс работы с Windows 2000.

▶ Задание 3: станьте владельцем файла

1. Зарегистрируйтесь в системе как User83 и запустите Windows Explorer (Проводник).
2. Откройте папку C:\Data.
3. Щелкните файл OWNER.TXT правой кнопкой мыши и выберите в контекстном меню команду Properties (Свойства).

   Откроется окно свойств с активной вкладкой General (Общие).

4. Перейдите на вкладку Security (Безопасность) и изучите разрешения для файла OWNER.TXT.

   Появится сообщение, что вы можете лишь просматривать текущую информацию о защите файла OWNER.TXT.

5. Щелкните OK.

   Откроется диалоговое окно свойств с выбранной вкладкой Security (Безопасность).

6. Щелкните кнопку Advanced (Дополнительно), чтобы открыть диалоговое окно Access Control Settings For OWNER.TXT (Параметры управления доступом для OWNER.TXT), и перейдите на вкладку Owner (Владелец).

   Кто на данный момент владеет файлом OWNER.TXT?

7. В списке Name (Имя) выберите User83 и щелкните кнопку Apply (Применить).

   Назовите текущего владельца файла OWNER.TXT.

8. Щелкните кнопку OK, чтобы закрыть диалоговое окно Access Control Settings For OWNER.TXT (Параметры управления доступом для OWNER.TXT).

   Откроется диалоговое окно свойств OWNER.TXT с выбранной вкладкой Security (Безопасность).

9. Щелкните OK, чтобы закрыть диалоговое окно Properties (Свойства).

► **Задание 4: проверьте разрешения на доступ владельца к файлу**

1. Зарегистрируйтесь в системе как User83. Назначьте пользователю User83 разрешение Full Control для файла Owner.txt и щелкните кнопку Apply (Применить).
2. Сбросьте флажок Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект).
3. В диалоговом окне Security (Безопасность) щелкните кнопку Remove (Удалить), чтобы удалить разрешения групп Users (Пользователи) и Administrators (Администраторы) для файла OWNER.TXT.
4. Щелкните OK, чтобы закрыть окно свойств файла OWNER.TXT.
5. Удалите файл OWNER.TXT.
6. Закройте все приложения.

Резюме

На этом занятии мы рассказали о двух специальных разрешениях: Change Permissions и Take Ownership. Администраторам и другим пользователям можно предоставить право изменять разрешения доступа к файлу или папке, не предоставляя им разрешения Full Control для файла или папки. Это предотвращает удаление файла или папки или записи в них, но позволяет назначать разрешения файлу или папке.

Посредством специального разрешения Take Ownership пользователи и группы могут взять файл или папку во владение. Текущий владелец или любой пользователь с разрешением Full Control вправе назначать стандартное разрешение Full Control или специальное разрешение Take Ownership другой учетной записи или группе, которые способны взять во владение объект. Вам запрещено назначать кого-либо владельцем файла или папки. Чтобы стать владельцем файла или папки, пользователь или член группы с разрешением Take Ownership должен явно получить его во владение.

Администратор вправе взять во владение папку или файл независимо от назначенных разрешений. В таком случае группа Administrators (Администраторы) становится владельцем, и любой член этой группы может изменить разрешения для файла или папки и назначить другой учетной записи или группе разрешение.

При выполнении упражнений вы определили разрешения для файла, назначили учетной записи разрешение Take Ownership и затем стали владельцем этого файла с помощью этой учетной записи.

Занятие 4, Копирование и перемещение файлов и папок

При копировании или перемещении файлов и папок назначенные им разрешения изменяются. Порядок изменения разрешений определяется специальными правилами.

Изучив материал этого занятия, вы сможете:

- ✓ рассказать, как влияет копирование и перемещение на разрешения NTFS на доступ к файлам и папкам;
- ✓ перечислить требующиеся для копирования или перемещения файлов и папок разрешения.

Продолжительность занятия — около 15 минут.

Копирование файлов и папок

Изменение разрешений при копировании файлов и папок из одного каталога в другой или с одного тома на другой проиллюстрировано на рис. 9-7.

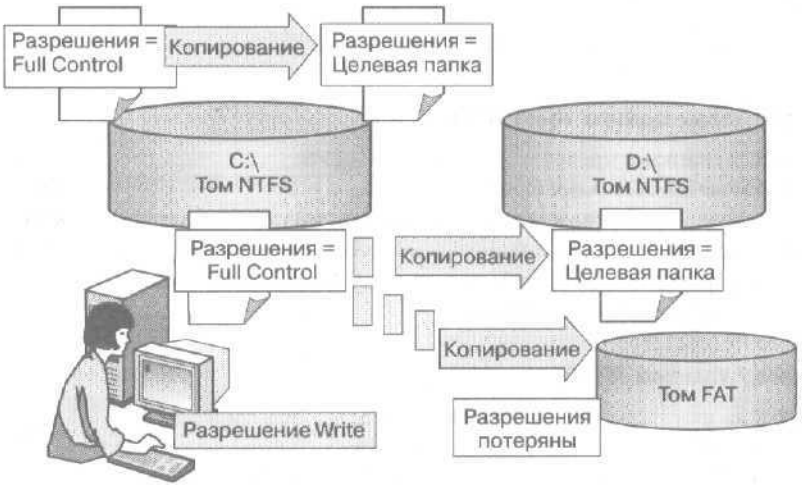


Рис. 9-7. Копирование файлов/папок между папками/томами

При копировании файла в пределах одного тома NTFS или на другой том NTFS:

- Windows 2000 обращается со скопированным файлом, как с новым; в соответствии с этим он получает разрешения целевой папки;
- необходимо иметь разрешение Write для конечной папки, чтобы скопировать в нее каталог или файл;
- вы становитесь пользователем CREATOR OWNER (Создатель-владелец) этого файла.

Примечание При копировании на том FAT файлы/папки теряют разрешения NTFS, поскольку тома FAT не поддерживают разрешения NTFS.

Перемещение файлов и папок

При перемещении файла или папки разрешения изменяются или не изменяются в зависимости от конечной папки или тома (рис. 9-8.).

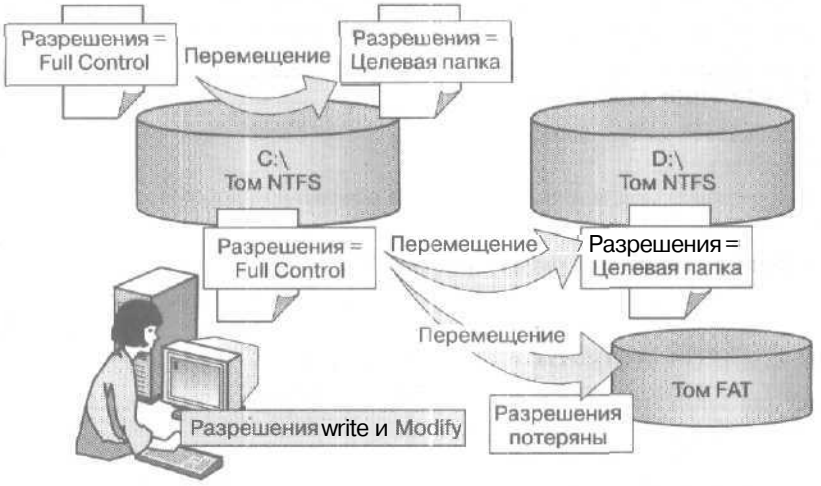


Рис. 9-8. Перемещение файлов/папок между папками/томами

Перемещение в пределах одного тома NTFS

При перемещении файла/папки в пределах одного тома NTFS:

- они сохраняют первоначальные разрешения;
- необходимо иметь разрешение Write для папки, в которую вы перемещаете папку/файл;
- необходимо иметь разрешение Modify для исходного файла/папки; поскольку после перемещения в целевую папку Windows 2000 удаляет файл или папку из исходной папки;
- смены владельца файла/папки не происходит.

Перемещение между томами NTFS

При перемещении файла или папки между томами NTFS:

- файл или папка наследуют разрешения целевой папки;
- необходимо иметь разрешение Write для целевой папки, чтобы переместить в нее папку/файл;
- необходимо иметь разрешение Modify для исходного файла или папки, поскольку Windows 2000 удаляет файл или папку из исходной папки *после* перемещения;
- вы становитесь пользователем CREATOR OWNER (Создатель-владелец).

Примечание При перемещении на том FAT файлы/папки теряют разрешения NTFS, тома FAT не поддерживают разрешения NTFS.

Практикум: копирование и перемещение папок

Вы определите, как изменяются разрешения и владельцы при копировании или перемещении файлов.

► Задание 1: создайте папку, зарегистрировавшись в системе как пользователь

1. Зарегистрируйтесь в системе как User83. В Windows Explorer (Проводник) создайте на диске C: папку с именем Tempi.

   Перечислите разрешения, назначенные этой папке.

   Кто является ее владельцем? Почему?
2. Закройте все приложения и рабочий сеанс.

► Задание 2: создайте папку, зарегистрировавшись как Administrator

1. Зарегистрируйтесь в системе как Administrator и запустите Windows Explorer (Проводник).
2. На диске C: создайте папки Тетр2 и Temp3.

   Перечислите назначенные им разрешения.

   Кто является владельцем папок Тетр2 и Тетр3? Почему?

   Удалите группу Everyone (Все) и назначьте для папок Тетр2 и Тетр3 разрешения доступа, указанные в табл. 9-11. Вам потребуется снять флажок Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект). Чтобы назначить разрешения для труппы, щелкните кнопку Add (Добавить), выберите группу (или группы) в диалоговом окне Select Users, Computers, Or Groups (Выбор: Пользователи, Компьютеры или Группы), щелкните кнопку Add (Добавить), затем щелкните OK. Назначьте соответствующие разрешения для группы в окне свойств.

Табл. 9-11. Разрешения папки для практикума

Папка	Назначьте разрешение
C:\Temp2	Administrators: Full Control
	UsersRead & Execute
C:\Temp3	Backup Operators (Операторы архива): Read & Execute
	Users: Full Control

► Задание 3: скопируйте папку в другую папку в пределах тома NTFS

1. Скопируйте папку C:\Temp2 в C:\Temp1.
2. Сравните разрешения и владельцев папок C:\Temp1\Temp2 и C:\Temp2.

   Кто является владельцем папки C:\Templ\Temp2 и каковы разрешения, назначенные ей? Почему?
3. Закройте все приложения и завершите рабочий сеанс.

► Задание 4: переместите папку в пределах тома NTFS

1. Войдите в домен как User83.
2. Выберите папку C:\Temp3 и переместите ее в папку C:\Templ.

   Что произошло с разрешениями и кто теперь является владельцем папки C:\Temp1\Temp3?
3. Закройте все приложения и завершите рабочий сеанс.

Резюме

Когда вы копируете или перемещаете файлы и папки, заданные для них разрешения могут измениться. Существуют правила, регулирующие, как и когда изменяются разрешения. Например, когда вы копируете файлы или папки из одной папки в другую или с

одного тома на другой, разрешения меняются. Windows 2000 обращается со скопированным файлом, как с новым, поэтому он получает разрешения целевой папки. Необходимо иметь разрешение Write для конечной папки, чтобы скопировать в нее каталог или файл. Когда вы копируете файл, вы становитесь пользователем CREATOR OWNER (Создатель-владелец) этого файла. Когда вы перемещаете файл или папку в пределах одного тома **NTFS,** они сохраняют первоначальные разрешения. Однако, когда вы перемещаете файл или папку между томами NTFS, они наследуют разрешения целевой папки.

Выполняя упражнения, вы наблюдали, как изменяются разрешения и права владения при копировании и перемещении папок.

Занятие 5. Устранение неполадок при задании разрешений

При назначении или изменении разрешений NTFS на доступ к файлам/папкам иногда возникают проблемы. Их важно вовремя устранить.

Изучив материал этого занятия, вы сможете:

- ✓ пояснить типичные причины, мешающие пользователям получить доступ к ресурсам;
- ✓ устранить проблемы доступа к ресурсам.

Продолжительность занятия — около 5 минут.

Типичные проблемы с разрешениями

В табл. 9-12 описаны некоторые типичные проблемы с разрешениями, с которыми вам, возможно, придется столкнуться, а также способы их устранения.

Табл. 9-12. Связанные *с* разрешениями проблемы и их решения

Проблема	Решение
Пользователь не может получить доступ к файлу или папке	Если файл или папка были скопированы или перемещены на другой том **NTFS,** разрешения могли **измениться.** Проверьте разрешения, назначенные учетной записи пользователя и группам, членом которых он является. Например, иногда пользователь не имеет разрешения или доступ для него запрещен в индивидуальном порядке или как члену группы
Вы добавили учетную запись пользователя в группу, чтобы предоставить этому пользователю доступ к файлу или папке, но он не может получить доступ	Чтобы войти в новую группу, в которую вы добавили учетную запись, пользователь должен или выйти из системы и затем войти в нее повторно, или закрыть все сетевые подключения к компьютеру, на котором размещены файл или папка и затем создать новое подключение
Пользователь с разрешением Full Control для папки удаляет файл в папке, хотя не имеет разрешения удалять этот файл. Вы хотите предотвратить дальнейшее удаление пользователем файлов	Вы должны отменить специальное разрешение для папки, сбросив флажок Delete Subfolders And Files, чтобы лишить пользователя с разрешением Full Control права удалять файлы в этой папке

Примечание Windows 2000 поддерживает POSIX-приложения, разработанные для UNIX. На системах под управлением UNIX разрешение Full Control позволяет удалять файлы в папке. В Windows 2000 разрешение Full Control включает специальное разрешение доступа Delete Subfolders And Files, позволяющее удалять файлы и подкаталоги независимо от наличия соответствующих разрешений.

Предотвращение проблем с разрешениями

Далее приведены рекомендации по внедрению разрешений NTFS, которые помогут вам избежать проблем.

- Назначайте наиболее строгие разрешения NTFS, позволяющие пользователям и группам выполнять только необходимые задачи.
- Назначайте все разрешения на уровне папок, а не на уровне файлов, Сгруппируйте файлы, доступ к которым требуется ограничить, в отдельную папку и ограничьте к ней доступ.
- Для всех исполняемых файлов приложений назначьте группе Administrators (Администраторы) разрешения Read & Execute и Change Permissions, а группе Users (Пользователи) — разрешение Read & Execute. Повреждение файлов приложений обычно является результатом деятельности вирусов и несанкционированных действий. Назначив группе Users (Пользователи) разрешение Read & Execute и разрешения Read & Execute и Change Permissions группе Administrators (Администраторы), вы можете предотвратить изменение или удаление исполняемых файлов. Для обновления файлов члены группы Administrators (Администраторы) могут предоставить своим учетным записям разрешение Full Control, внести требуемые изменения и затем вновь назначить своей учетной записи разрешение Read & Execute и Change Permission.
- Назначьте группе CREATOR OWNER (Создатель-владелец) разрешение Full Control для общих папок данных, чтобы пользователи могли удалять и изменять созданные ими файлы/папки. Данное разрешение предоставляет пользователю, создавшему файл/папку, полный доступ в общей папке данных только к тем файлам/папкам, которые созданы непосредственно им.
- Для общих папок группе CREATOR OWNER (Создатель-владелец) назначайте разрешение Full Control, а группе Everyone (Все) — разрешение Read and Write. Пользователи получат полный доступ к созданным ими файлам, однако члены группы Everyone (Все) смогут лишь считывать и добавлять файлы в каталог.
- Если к ресурсу не будут обращаться по сети, используйте длинные и подробные имена. Если вы собираетесь открыть к папке совместный доступ, имена папок/файлов должны поддерживаться всеми клиентскими компьютерами.
- Рекомендуется назначать, но не аннулировать разрешения. Если надо, чтобы пользователь или группа не имели доступа к конкретной папке или файлу, не назначайте им соответствующее разрешение. Отмена разрешений должна быть исключением, а не обычной практикой.

Практикум: удаление файла при отмене всех разрешений

В этом упражнении вы смоделируете третью проблему, описанную в табл. 9-12. Предоставьте пользователю разрешение Full Control для папки, но отмените все разрешения на доступ к файлу в этой папке. Затем посмотрите, что будет происходить, когда пользователь попытается удалить этот файл.

► Задание 1: назначьте разрешение Full Control для папки

1. Войдите в систему как администратор и запустите Windows Explorer (Проводник).
2. Откройте диск C и создайте папку с именем Fullaccess.
3. Проверьте, имеет ли группа Everyone (Все) разрешение Full Control для папки Fullaccess.

► Задание 2: создайте файл и запретите доступ к нему

1. В папке C:\Fullaccess создайте текстовый файл с именем NOACCESS.TXT,

2. Сбросьте флажок Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект). Отмените для группы Everyone (Все) разрешение Full Control для файла NOACCESS.TXT и щелкните OK.

   Откроется диалоговое окно Security (Безопасность) с сообщением, что вы запретили доступ к файлу NoAccess.txt. Никто не сможет получить доступ к этому файлу и только владелец файла сможет изменить его разрешения.
3. Щелкните Yes (Да), чтобы применить изменения и закрыть диалоговое окно Security (Безопасность).

▶ **Задание 3: протестируйте применение разрешения Full Control**

1. В Windows Explorer (Проводник) дважды щелкните файл NOACCESS.TXT в папке C:\Fullaccess, чтобы открыть его.

   Удалось ли вам это? Почему?
2. Раскройте меню Start (Пуск), выберите Programs (Программы), затем — Accessories и команду Command prompt.
3. Наберите cd c:\fullaccess, чтобы перейти в папку C:\Fullaccess.
4. Удалите NOACCESS.TXT, набрав del **noaccess.txt.**

   Удалось ли вам это? Почему?

   Как пользователю с разрешением Full Control для папки запретить удалять файл в этой папке?

Резюме

При назначении или изменении разрешений **NTFS** могут возникнуть проблемы. *Их* важно вовремя устранить. В этом занятии вы изучили некоторые обычные проблемы разрешений и некоторые возможные методы их устранения.

Выполняя упражнения, вы наблюдали, как пользователи могут удалить файл, для которого отменены все разрешения на доступ.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении А «Вопросы и ответы» в конце книги.

1. Какое разрешение задано по умолчанию, когда том отформатирован под NTFS? Кто имеет доступ к тому?

2. Какими разрешениями обладает пользователь, имеющий разрешение Write для папки и являющийся также членом группы с разрешением Read для той же папки?

3. Пользователь имеет разрешение Modify для папки и разрешение Read для файла. Файл копируется в эту папку. Какое разрешение для файла имеет пользователь?

4. Что происходит с разрешениями, назначенными для файла, когда файл перемещается из одной папки в другую на том же гоме NTFS? Что происходит, когда файл перемещается в папку на другом томе NTFS?

5. Как передать файлы и папки уволившегося сотрудника во владение другому сотруднику?

6. Какие три параметра следует проверить, когда пользователь не может получить доступ к ресурсу?

ГЛАВА 10

Администрирование общих папок

В этой **главе**

Из главы 9 вы узнали о разрешениях файловой системы NTFS, позволяющих регулировать доступ пользователей и групп к файлам и папкам. Разрешения NTFS применимы только к томам NTFS и действуют как при доступе к файлам и папкам на локальном компьютере, так и из сети.

Общие папки также позволяют защитить файловые ресурсы в разделах FAT или FAT32. Вы узнаете, как открыть доступ к файловым ресурсам и обеспечить их безопасность назначением разрешений.

Прежде **всего**

Для изучения материала этой главы необходимо:

- выполнить процедуру установки, описанную во вводной главе;
- изучить главы 7—9 и выполнить упражнения из них;
- настроить ваш компьютер как контроллер домена.

Занятие 1. Общие папки

В Microsoft Windows 2000 разрешается сделать папку общей для нескольких пользователей, которые смогут получать доступ к ней и ее содержимому со своих компьютеров. На этом занятии вы познакомитесь с общими папками и разрешениями на доступ к ним.

Изучив материал этого занятия, вы сможете:

- ✓ использовать общие папки для предоставления доступа к сетевым ресурсам;
- ✓ рассказать, как разрешения влияют на вид доступа к общим папкам.

Продолжительность занятия — около 15 минут.

Возможности общих папок

Общая папка может содержать приложения, данные или личную папку пользователя. Каждый тип данных требует различных разрешений доступа.

- Поскольку разрешения на доступ применяются ко всей общей папке, а не к отдельным файлам, они предоставляют менее избирательную защиту, чем разрешения NTFS.
- Разрешения на доступ к общей папке не ограничивают доступ пользователей, работающих на том компьютере, где расположена эта папка. Они применяются только к тем, кто обращается к папке по сети.
- Разрешения на доступ к общей папке — единственный способ обеспечить безопасность сетевых ресурсов на томе FAT. Разрешения NTFS на томах FAT недоступны.
- По умолчанию группа Everyone (Все) получает разрешение Full Control (Полный доступ) для всех новых общих папок.

Примечание В Windows Explorer (Проводник) общую папку легко узнать по специальному значку (рис. 10-1).

Доступ к общей папке регулируется разрешениями, перечисленными в таблице 10-1.

Табл. 10-1. Разрешения для доступа к общим папкам

Разрешение	Возможности
Read (Чтение)	Просмотр списка папок и файлов, содержимого файлов, доступ к вложенным папкам и запуск приложений
Change (Изменение)	Создание в общей папке вложенных папок, добавление к ним файлов, изменение и добавление данных в файлах, удаление файлов и вложенных папок и выполнение действий, допускаемых разрешением Read
Full Control (Полный доступ)	Изменение разрешений для файлов, назначение себя владельцем файлов и выполнение всех действий, допускаемых разрешением Change

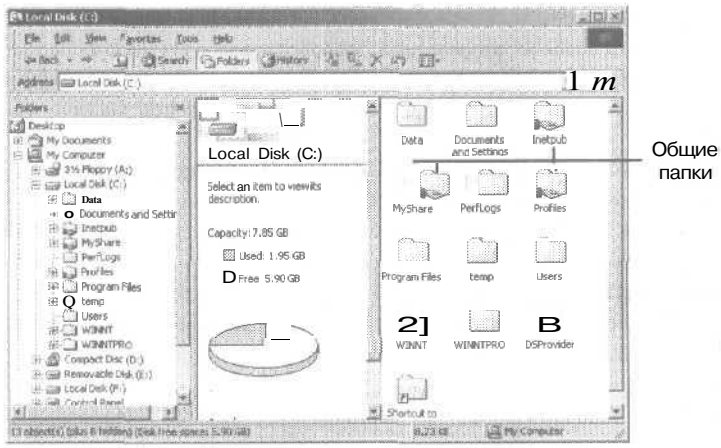


Рис. 10-1. Общие папки в Windows Explorer (Проводник)

Вы можете предоставлять и отменять разрешения на доступ к общей папке. Обычно удобнее назначать разрешения группе, чем отдельным пользователям. Отменять же разрешения необходимо, только если вероятно применение нежелательных разрешений. Обычно это происходит, когда в полномочную группу включен пользователь, которому надо ограничить доступ. Чтобы запретить *все* виды доступа к общей папке, отмените разрешение Full Control (Полный доступ).

Применение разрешений на доступ к общей папке

Вид доступа к общей папке зависит от разрешений, назначенных учетным записям пользователей и групп. Сейчас мы рассмотрим последствия применения разных разрешений.

- **Несколько разрешений совмещаются.** Пользователь может участвовать в нескольких группах, каждая из которых имеет разные разрешения с разными уровнями доступа к общей папке. Действующие разрешения пользователя являются комбинацией разрешений его собственных и группы, членом которой он является. Например, имея разрешение Read и будучи членом группы с разрешением Change, пользователь получит разрешение Change, включающее в себя Read.
- **Запрет приоритетнее разрешения.** Если пользователю запрещен доступ к общей папке, он не получит его, даже если это разрешено группе, к которой он принадлежит.
- **Для доступа к ресурсам на томах NTFS требуются разрешения NTFS.** Разрешений общей папки достаточно, чтобы получить доступ к ресурсам на томе FAT, но не на томе NTFS. Для доступа к общей папке на томе NTFS, помимо разрешения доступа к общей папке, требуются и соответствующие разрешения NTFS для каждого общего файла и папки.
- **Общий доступ к скопированным или перемещенным папкам прекращается.** При копировании общей папки общим останется оригинал, но не копия. Перемещенная или переименованная папка перестает быть общей.

Основные правила назначения разрешений на доступ к общей папке

Основные правила назначения разрешений на доступ к общей папке можно сформулировать следующим образом:

- **определите группы, которым необходим доступ к данному ресурсу, и требуемый уровень доступа.** Составьте документацию по группам и их разрешениям для каждого ресурса;

- **назначайте разрешения группам,** а не отдельным учетным записям пользователей;
- **назначайте для ресурса наиболее строгие разрешения, позволяющие пользователям выполнять только необходимые задачи.** Например, если вы хотите, чтобы пользователи только читали информацию в папке, но не удаляли и не создавали в ней файлы, назначьте разрешение Read;
- **папки с одинаковыми требованиями безопасности должны принадлежать одной папке.** Скажем, если пользователям требуется разрешение Read (Чтение) для нескольких папок приложения, поместите их в одну и предоставьте доступ ко всей этой папке (вместо предоставления доступа для каждой папки в отдельности);
- **задавайте общим объектам интуитивно понятные имена.** Так, при открытии доступа к папке Application назначьте ей сетевое имя Apps. Используйте такие имена общих ресурсов, чтобы к ним могли обращаться клиенты с любыми ОС.

В табл. 10-2 показаны правила назначения имен общих папок в различных ОС.

Табл. 10-2. Правила именования общих папок

Операционная система	Длина сетевого имени	Длина имени папки
Windows 2000/NT/9x	80 символов	255 символов
MS-DOS, Windows 3.1, Windows for Workgroups	Согласно правилу *«8.3»*	Согласно правилу «8.3»

Microsoft Windows 2000 предоставляет эквивалентные имена в формате «8.3», но пользователям такие имена могут быть непонятны. Скажем, папка Windows 2000 с именем Accountants Database на компьютерах с MS-DOS, Windows 3.x и Windows for Workgroups получит название Account~1.

Практикум: назначение разрешений

Пусть пользователю User1 назначены разрешения для получения доступа к ресурсам как отдельному пользователю и как члену группы (рис. 10-2). Определите, какие результирующие разрешения будут у User1 в следующих ситуациях.

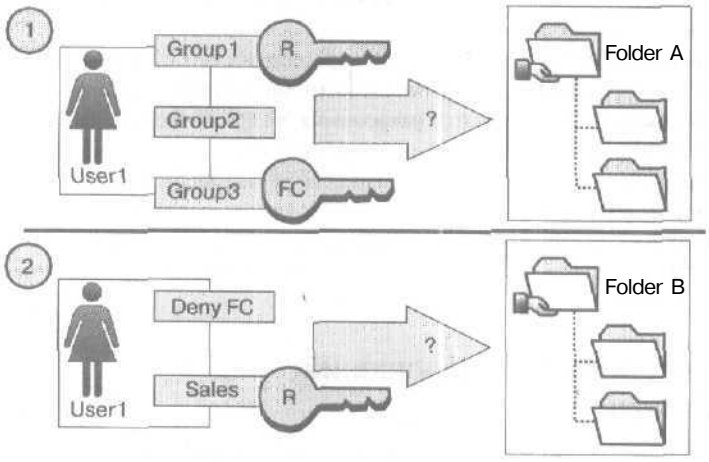


Рис. 10-2. Назначение разрешений

1. User1 — член групп Groupl, Group2 и Group3. Для папки FolderA у Groupl есть разрешение Read, у Group3 — Full Control (Полный доступ), а Group2 для нее разрешений не назначено. Какими результирующими разрешениями будет обладать Userl для FolderA?
2. Userl также является членом группы Sales, которой назначено разрешение Read (Чтение) для FolderB. Для Userl, как отдельного пользователя, отменено разрешение Full Control (Полный доступ) для FolderB. Какие результирующие разрешения будет иметь User101 для FolderB?

Резюме

Доступ к папке и ее содержимому можно открыть по сети. Применение разрешений на доступ к общей папке — единственный способ обеспечить безопасность файловых ресурсов на томах FAT. Разрешения доступа к общей папке применяются не к отдельным файлам, а только к папкам. Разрешения не ограничивают доступ пользователей, работающих на том компьютере, где эти папки находятся, а относятся только к тем, кто обращается к ней по сети.

Существует три вида разрешений общей папки: Read (Чтение), Change (Изменение) и Full Control (Полный доступ). Read позволяет просматривать списки файлов и папок, данные в файлах, а также запускать приложения и открывать вложенные папки. Change разрешает пользователям создавать папки, добавлять к ним файлы, изменять и добавлять данные в файлах, удалять файлы и вложенные папки, а также выполнять действия, допустимые разрешением Read. Разрешение Full Control позволяет изменять разрешения для файла, вступать во владение файлами (на томах NTFS) и выполнять все действия, допустимые разрешением Change. По умолчанию группа Everyone (Все) получает разрешение Full Control (Полный доступ) для всех новых общих папок.

Занятие 2, Планирование общих папок

Продуманная структура общих папок позволяет централизовать администрирование и упростить доступ к данным. Общие папки содержат приложения и данные и позволяют создать места для централизованного хранения пользователями своих данных. Файлы, собранные в одной общей папке, проще найти. Это занятие содержит основные принципы открытия доступа к папкам приложений и данных.

Изучив материал этого занятия, вы сможете:

- ✓ планировать, какие разрешения доступа к общей папке назначать пользователям и группам для папок данных и папок приложений.

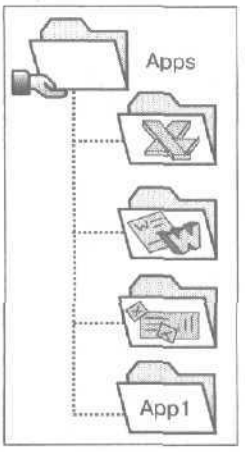
Продолжительность занятия — около 5 минут.

Папки приложений

Общие *папки приложении* (application folders) применяют для серверных приложений, к которым может обращаться компьютер клиента. Главный «плюс» общих приложений в том, что вам не нужно устанавливать и поддерживать их компоненты на каждом компьютере. В то время как файлы программ для приложений могут хранится на сервере, данные о конфигурации большинства сетевых программ, как правило, хранятся на компьютерах клиентов. Способ открытия доступа к папкам приложений во многом зависит от конкретного приложения, параметров сети и организации работы в компании.

На рис. 10-3 показано, как открыть доступ к папке приложений.

- Создайте одну папку и разместите в ней все ваши приложения. Таким образом вы установите единое место для размещения и модернизации ПО.
- Назначьте группе Administrators (Администраторы) разрешение Full Control (Полный доступ) для папки приложений, чтобы группа могла управлять прикладным ПО и контролировать разрешения пользователей.
- Отмените разрешение Full Control (Полный доступ) для группы Everyone (Все) и назначьте разрешение Read (Чтение) для группы Users (Пользователи). Это повысит безопасность, так как группа Users включает только созданные вами учетные записи, а группа Everyone — учетные записи любого пользователя, получившего доступ к сетевым ресурсам, в том числе учетную запись Guest (Гость).
- Назначьте разрешение Change (Изменение) группам, отвечающим за модернизацию приложений и устранение неполадок.
- Для приложений, требующих иных разрешений, создайте отдельную общую папку и назначьте для нее соответствующие разрешения.



- Создайте общие папки для приложений
- Назначьте группе Administrators разрешение Full Control
- Отмените разрешение Full Control для группы Everyone и назначьте разрешение Read для группы Users
- Назначьте разрешение Change группам, отвечающим за модернизацию приложений и устранение неполадок
- Создайте отдельную общую папку для каждого набора разрешений

Рис. 10-3. Создание общих папок программ

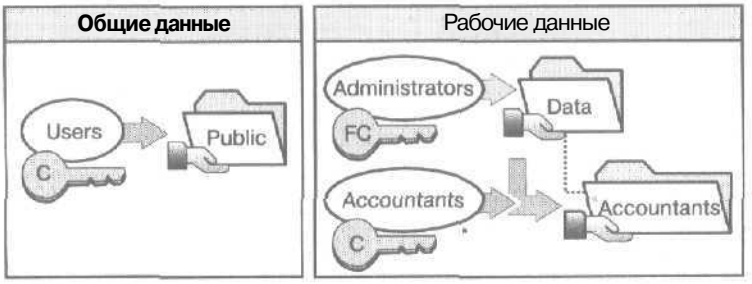
Папки данных

Для обмена по сети рабочими и общими данными служат *папки данных* (data folders). Их лучше хранить на отдельном томе, где не установлена ОС или приложения. Файлы данных рекомендуется регулярно архивировать, поэтому, если они будут храниться на отдельном томе, архивирование упростится. Кроме того, том с папками данных будет в безопасности, если вам потребуется переустановить ОС.

Общие данные

Предоставляя доступ к папкам общих данных:

- используйте централизованные папки данных, так как их легче архивировать;
- назначьте группе Users (Пользователи) разрешение Change (Изменение) — это обеспечит пользователям единое общедоступное место для хранения данных, которыми они хотят обмениваться; пользователи также смогут получать доступ к папкам, читать, создавать или изменять в них файлы (рис. 10-4).



- Согласованно архивируйте централизованные папки данных
- Откройте общий доступ к папкам нижнего уровня

Рис. 10-4. Папки общей и рабочей информации

Рабочие данные

Открывая доступ к папке рабочих файлов, необходимо:

- назначить группе Administrators (Администраторы) разрешение Full Control (Полный доступ) для главной папки данных, чтобы администраторы могли централизованно выполнять ее обслуживание;
- предоставить доступ к вложенным папкам данных, задав разрешение Change (Изменение) соответствующим группам.

Например, для защиты данных в папке Accountants, вложенной в папку Data, предоставьте доступ к папке Accountants и назначьте разрешение Change только группе Accountants (рис. 10-4).

Примечание Так как администратор всегда может стать владельцем файла, руководство фирмы может решить шифровать файлы и папки по соображениям безопасности. Информация о шифровании содержится в разделе «Обзор шифрования файлов» справочной системы Microsoft Windows 2000.

Резюме

Общие папки приложений позволяют централизовать управление и облегчают модернизацию ПО. Членам группы Administrators (Администраторы) нужно назначить для этих папок разрешение Full Control (Полный доступ), чтобы они могли управлять ПО и разрешениями пользователей. Сняв разрешение Full Control для группы Everyone (Все) и назначив Read (Чтение) группе Users (Пользователи), вы обеспечите наибольшую безопасность, так как группа Users содержит только созданные вами учетные записи, а Everyone включает учетную запись любого пользователя, получившего доступ к сетевым ресурсам, в том числе гостевую учетную запись Guest (Гость).

В общих папках данных хранятся данные пользователей и часто применяемые файлы. Регулярно архивируйте папки с файлами данных. Архивирование станет проще, если разместить эти папки на отдельном томе.

Занятие 3. Доступ к папкам

Для открытия доступа к ресурсам достаточно сделать общими содержащие их папки. Для этого вы должны быть членом одной или нескольких групп в зависимости от роли компьютера, на котором находятся общие папки. Доступом к папке и ее содержимому можно управлять, ограничивая количество пользователей, которые могут одновременно к ней обращаться, и назначая разрешения отдельным пользователям и группам. Вы вправе изменить параметры общей папки: закрыть к ней доступ, изменить ее сетевое имя, а также разрешения пользователей и групп.

Изучив материал этого занятия, вы сможете:

- ✓ создавать и модифицировать общие папки;
- ✓ подключаться к обидим папкам.

Продолжительность занятия — около 20 минут.

Требования для открытия доступа к папкам

Открыть доступ к папкам в Windows 2000 вправе только члены встроенных групп Administrators (Администраторы), Server Operators (Операторы сервера) и Power Users (Опытные пользователи). Причем при этом они обязаны соблюдать следующие правила:

- в домене Windows 2000 участникам групп Administrators и Server Operatorsразрешено открывать доступ к папкам на любой машине домена. Power Users могут открыть доступ к папкам только на изолированном сервере или компьютере с Windows 2000 Professional, где зарегистрирована эта группа;
- в рабочей группе Windows 2000 участникам групп Administrators и Power Users разрешено открывать доступ к папкам на изолированном сервере или на компьютере с Windows 2000 Professional, где зарегистрирована эта группа.

Примечание Для открытия доступа к папке на томе NTFS пользователи должны иметь для нее как минимум разрешение Read.

Административные общие папки

Windows 2000 автоматически открывает доступ к административным папкам. Эти папки обозначаются знаком доллара ($), который скрывает общие папки от пользователей, просматривающих содержимое компьютера. Корневая папка каждого тома, системная папка и местоположение драйверов принтеров — все это скрытые общие папки, к которым можно получить доступ по сети. Ниже перечислены основные административные общие папки Windows 2000.

Табл. 10-3. Административные общие папки Windows 2000

Ресурс	Назначение
C$, D$, E$ и т. д.	К корневой папке на каждом жестком диске автоматически открыт доступ, причем сетевое имя такого ресурса — это имя диска со значком доллара ($). Подключившись к этой папке, вы получите доступ ко всему тому. Административные ресурсы используются для удаленного администрирования компьютеров. Windows 2000 назначает группе Administrators разрешение Full Control.

Табл. 10-3. Административные общие папки Windows 2000 *(окончание)*

Ресурс	На значение
	Windows 2000 автоматически открывает доступ и к дисководам CD-ROM; сетевое имя такого ресурса также состоит из буквы диска и знака доллара
AdminS	Главная системная папка, по умолчанию C:\Winnt, открыта для доступа под именем Admin$. Члены группы Administrators могут обращаться к ней, не зная, где на самом деле она находится. Windows 2000 назначает группе Administrators разрешение Full Control
Print$	Когда вы установите первый общий принтер, папка *systemroot*\System32\Spool\Drivers будет открыта для доступа под именем Print$; она позволяет клиентам обращаться к файлам драйвера принтера. Члены групп Administrators, Server Operators (Операторы сервера) и Print Operators (Операторы печати) имеют разрешение Full Control, а группы Everyone (Все) — Read (Чтение)

Скрытые общие папки не ограничиваются теми, которые система создает автоматически. Можно открыть доступ к другим папкам, добавляя ($) в конце их сетевого имени, и тогда к ним смогут обратиться только пользователи, знающие их имена и имеющие соответствующие разрешения доступа.

Открытие доступа к папке

Когда Вы открываете доступ к папке, можно задать ей одно или несколько сетевых имен, снабдить описанием ее содержимого, ограничить число пользователей, имеющих к ней доступ, и предоставить им разрешения.

▶ **Предоставление доступа к папке**

1. Щелкните правой кнопкой нужную папку и выберите команду Properties (Свойства).
2. На вкладке Sharing (Доступ) окна свойств (рис. 10-5) щелкните переключатель Share This Folder (Открыть общий доступ к этой папке).

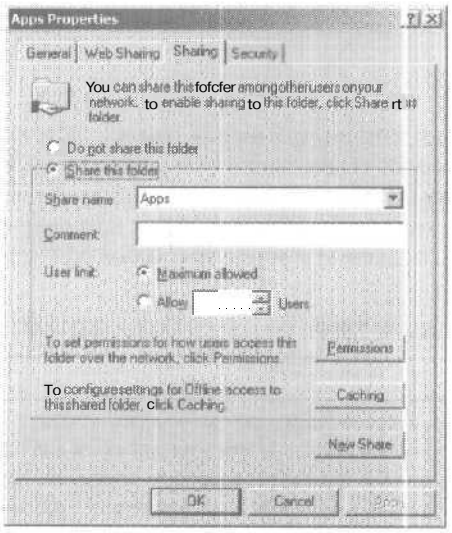


Рис. 10-5. Вкладка Sharing (Доступ) диалогового окна свойств папки

3. В поле Share Name (Сетевое имя) задайте имя. по которому пользователи будут по сети обращаться к этой папке.
4. При желании введите описание данного сетевого имени в поле Comment (Комментарий). Пользователи увидят его при просмотре списка общих папок на сервере и получат информацию о содержимом данной папки.
5. В разделе User Limit (Предельное число пользователей) введите число пользователей, одновременно обращающихся к данной общей папке. Если будет выбран переключатель Maximum Allowed (максимально возможное), то в Windows 2000 Professional это составит 10 соединений для всех ресурсов. В Windows 2000 Server вы можете предоставить любое количество соединений, ограниченное только установленным числом клиентских лицензий доступа.
6. Щелкните кнопку OK.

Назначение разрешений на доступ к общей папке

После предоставления доступа к папке надо назначить соответствующие разрешения учетным записям пользователей и группам,

▶ **Назначение разрешений на доступ к общей палке пользователям и группам**

1. На вкладке Sharing (Доступ) диалогового окна свойств папки щелкните кнопку Permissions (Разрешения).
2. В диалоговом окне Permissions For (Разрешения) (рис. 10-6) удостоверьтесь, что выбрана группа Everyone (Все), и щелкните кнопку Remove (Удалить).

Рис. 10-6. Диалоговое окно общей папки Permissions For (Разрешения)

3. В диалоговом окне Permissions щелкните кнопку Add (Добавить).
4. В диалоговом окне Select Users, Computers, Or Groups (Выбор: Пользователи, Компьютеры или Группы) щелкните учетные записи/группы, которым хотите назначить разрешения.
5. Щелкните кнопку Add (Добавить) или дважды щелкните нужный пункт, чтобы добавить учетные записи/группы в список доступа к данной папке. Повторите это для всех нужных учетных записей/групп.

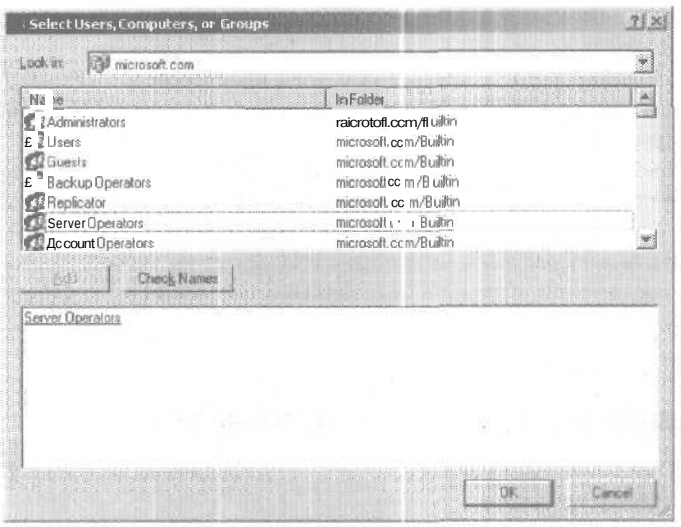


Рис. 10-7. Диалоговое окно Select Users, Computers, Or Groups (Выбор: Пользователи, Компьютеры или Группы)

6. Щелкните кнопку OK,
7. В окне Permissions для данной общей папки щелкните учетную запись/группу и, включив флажок Allow (Разрешить) или Deny (Запретить), укажите нужное разрешение.

Примечание В диалоговом окне Select Users, Computers, Or Groups (Выбор: Пользователи, Компьютеры или Группы) имеется список Look In (Искать в) для просмотра списка учетных записей/групп других доменов и локальных компьютеров, которым также можно задать разрешения для доступа к данной папке. Кроме этого, вы вправе просмотреть каталог службы Active Directory — для этого достаточно выбрать пункт Entire Directory.

Изменение параметров общих папок

Вы можете изменять параметры общих папок: отменять к ним доступ, изменять их сетевые имена и разрешения.

▶ **Изменение параметров общей папки**

1. Перейдите на вкладку Sharing (Доступ) в диалоговом окне свойств общей папки.
2. Далее руководствуйтесь указаниями, перечисленными в табл. 10-4.

Табл. **10-4. Этапы модификации общей папки**

Цель	Действия
Отмена доступа к папке	Щелкните переключатель Do Not Share This Folder (Отменить общий доступ к этой папке). Если в данный момент некий пользователь подключен к данной папке, то будет выведено предупреждение
Задание дополнительных сетевых имен	Щелкните кнопку New Share (Новый общий ресурс). Она появляется только после открытия доступа к папке, Это позволяет объединять несколько общих папок в одну, чтобы пользователи могли использовать их прежние сетевые имена

Табл. 10-4. Этапы модификации общей папки (*окончание*)

Цель	Действия
Удаление одного из сетевых **имен**	**Щелкните кнопку Remove** Share (Удалить общий ресурс) — **она появляется, только если папка имеет несколько** сетевых имен
Изменение разрешений на доступ к общей папке	Щелкните кнопку Permissions (Разрешения) и затем в одноименном диалоговом окне — кнопку Add (Добавить) или Remove (Удалить). В диалоговом окне Select Users. Computers, Or Groups (Выбор: Пользователи, Компьютеры или Группы) щелкните учетную запись/группу, чьи разрешения вы хотите изменить

Примечание Если пользователем открыт файл в папке, к которой вы закрываете доступ, пользователь может потерять данные. Поэтому, если вы щелкнете переключатель Do Not Share This Folder (Отменить общий доступ к этой папке), а пользователь подключен к этой папке, появится сообщение об этом подключении.

Подключение к общей папке

Подключаться к общей папке можно с помощью: мастера Map Network Drive (Подключение сетевого диска), мастера Add Network Place (Новое место в сетевом окружении), команды Run (Выполнить), ярлыка My Network Places (Мое сетевое окружение).

▶ **Подключение к общей папке с помощью мастера Map** Network **Drive**

1. На рабочем столе щелкните правой кнопкой ярлык My Network Places (Мое сетевое окружение) и выберите в контекстном меню команду Map Network Drive (Подключить сетевой диск).
2. В мастере Map Network Drive (Подключить сетевой диск) в поле Folder (Папка) введите UNC-путь к общей папке (например, *имя_компьютера**имя_общей_папки*) (рис. 10-8).

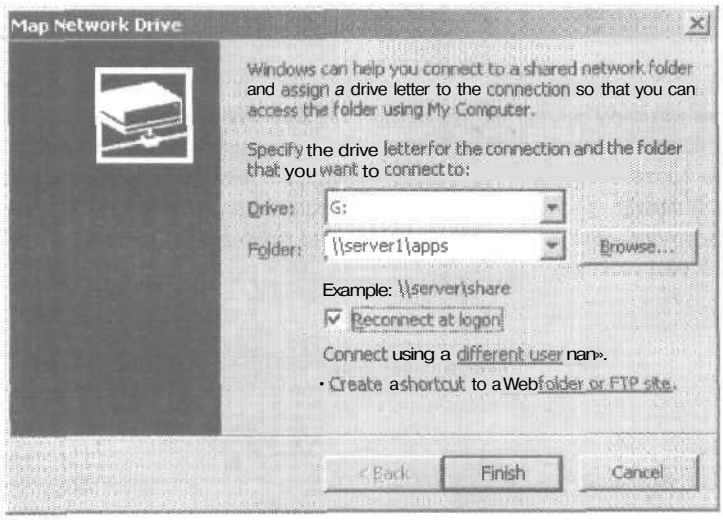


Рис. 10-8. Мастер Map Network Drive (Подключение сетевого диска)

3. В списке Drive (Диск) выберите диск для подключаемой папки.

4. Установите флажок Reconnect At Logon (Восстанавливать при входе в систему), если эта папка должна автоматически подключаться при каждом вашем входе в систему.
5. Щелкните ссылку Connect Using A Different User Name (Подключение под другим именем), чтобы подключиться к папке от имени другого пользователя, и в диалоговом окне Connect As (Подключиться как) введите нужные имя и пароль.

▶ **Подключение к общей папке с помощью мастера Add Network Place**

1. Дважды щелкните ярлык My Network Places (Мое сетевое окружение).
2. Дважды щелкните ярлык Add Network Place (Новое место в сетевом окружении).
3. На странице Welcome To The Add Network Place Wizard (Мастер добавления в сетевое окружение) введите путь к нужной общей папке в поле Type The Location Of The Network Place (Укажите место в сетевом окружении), затем щелкните кнопку Next (Далее).
4. На странице Completing The Add Network Place Wizard (Завершение работы мастера добавления в сетевое окружение) введите имя для подключаемой папки в поле Enter A Name For This Network Place (Введите имя для этого места в сетевом окружении), затем щелкните кнопку Finish (Готово).
5. Подключайтесь к этой папке, дважды щелкая ее ярлык в окне My Network Places (Мое сетевое окружение).

▶ **Подключение к** общей **папке посредством команды Run**

1. В меню Start (Пуск) выберите команду Run (Выполнить) и в поле Open (Открыть) введите *\\имя_компьютера* и щелкните кнопку OK.
2. В окне со списком общих папок на этом компьютере дважды щелкните подключаемую папку.

▶ **Подключение к общей папке средствами окна** My **Network Places**

1. Дважды щелкните значок My Network Places (Мое сетевое окружение).
2. Найдите компьютер, на котором находится нужная папка.
3. Дважды щелкните подключаемую папку.

Резюме

Чтобы предоставлять доступ к папке, нужно быть членом одной из групп в зависимости от роли компьютера, на котором хранится эта папка. Можно ограничивать число одновременно подключающихся к папке пользователей, а также управлять доступом к ней и ее содержимому, назначая соответствующие разрешения. Кроме того, вы вправе корректировать параметры общей папки, закрывать к ней доступ, изменять ее сетевое имя и разрешения пользователей и групп. Для доступа к общей папке надо подключиться к ней по сети, имея необходимое разрешение.

Занятие 4. Сочетание разрешений на доступ к общей папке и разрешений NTFS

На томе NTFS пользователям и группам назначают разрешения NTFS. При сочетании разрешений доступа к общей папке и разрешений NTFS приоритет имеет более строгое ограничение.

Изучив материал этого занятия, вы сможете:

- ✓ комбинировать разрешения на доступ к общей папке и разрешения NTFS.

Продолжительность занятия — около 45 минут.

Стратегии сочетания разрешений на доступ к общей папке и разрешений NTFS

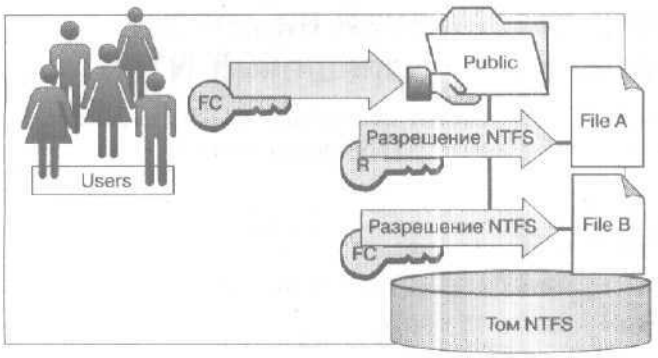
Один из вариантов предоставления доступа к ресурсам на томе NTFS — открыть доступ к папкам с разрешениями по умолчанию и корректировать их через разрешения NTFS. При этом разрешения на доступ к общей папке и разрешения NTFS комбинируются, обеспечивая нужный уровень безопасности.

Возможности разрешений на доступ к общей папке ограничены, разрешения же NTFS значительно более гибкие. К тому же, последние применяются как локально, так и при доступе по сети.

При открытии доступа к папке на томе NTFS действуют следующие правила:

- к файлам и папкам в общей папке можно применять разрешения NTFS, в том числе разные разрешения к разным файлам и папкам;
- кроме разрешений на доступ к общей папке пользователи должны иметь разрешения NTFS для доступа к ее содержимому. На томах FAT нет других разрешений на доступ к содержащимся в общей папке файлам и папкам, кроме разрешений на доступ к содержащей их папке;
- при сочетании разрешений на доступ к общей папке и разрешений NTFS приоритет всегда имеет более строгое ограничение.

На рис. 10-9 показано, что группа Everyone имеет разрешение Full Control (Полный доступ) для доступа к папке Public и разрешение NTFS Read для файла FileA. Результирующим разрешением на доступ к FileA для этой группы будет более строгое Read (Чтение), а к FileB — Full Control, так как и разрешения на доступ к общей папке, и разрешения NTFS позволяют этот доступ.



- Для доступа к томам NTFS требуются разрешения NTFS
- Применяйте разрешения NTFS для ограничения доступа к файлам и папкам
- Эффективным разрешением будет самое строгое

Рис. 10-9. Сочетание разрешений доступа к общей папке и разрешений NTFS

Практикум: управление доступом к общим папкам

Сейчас вы определите результирующие разрешения пользователей, спланируете совместное использование папок и разрешений на доступ к ним, назначите разрешения на доступ к папке, подключитесь к ней, отмените к ней доступ и проверите эффекты от сочетания разрешений на доступ к общей папке и разрешений NTFS.

Примечание Для выполнения дополнительных упражнений (5 и 8) желателен второй компьютер с Windows 2000, работающий как сервер домена. Можно, однако, выполнить эти упражнения и на одном компьютере.

Упражнение 1: сочетание разрешений

Общие папки на томе NTFS содержат вложенные папки, которым назначены разрешения NTFS (рис. 10-10). Определите результирующие разрешения пользователей в каждом случае.

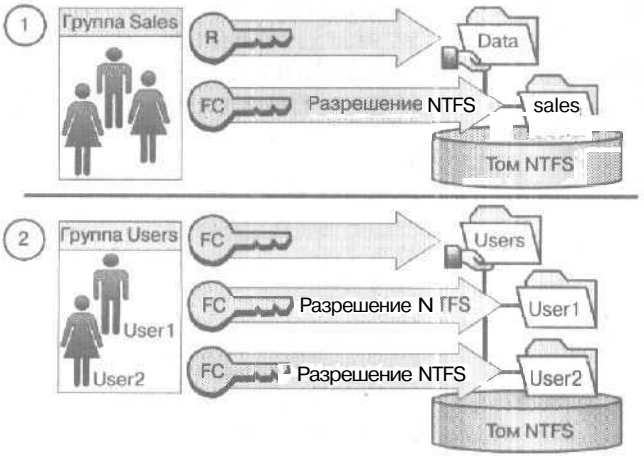


Рис. 10-10. Сочетание разрешений

1. В первом случае открыт доступ к папке Data. Группа Sales имеет для нее разрешение Read, а для вложенной в нее папки Sales — NTFS-разрешение Full Control.

   Каким будет результирующее разрешение группы Sales для доступа к папке Sales при подключении по сети к папке Data?

2. Во втором случае папка Users содержит личные папки пользователей. Каждая личная папка содержит данные, доступные только пользователю, именем которого она названа. Папка Users доступна группе Users с разрешением Full Control. User1 и User2 имеют разрешения NTFS Full Control только для своих личных папок и никаких разрешений NTFS для остальных. Эти пользователи — члены группы Users.

   Какими разрешениями доступа к папке Userl обладает Userl при подключении к общей папке Users? Каковы его разрешения для папки User2?

Упражнение 2: планирование общих папок

Спланируйте доступ к ресурсам на серверах главного офиса предприятия (рис. 10-11). Выполнив упражнение, занесите ваши ответы в таблицу.

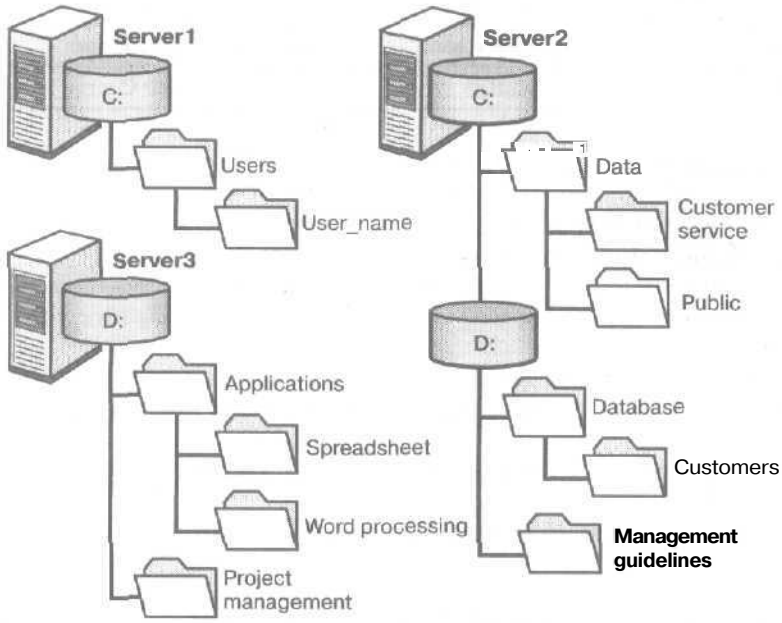


Рис. 10-11. Фрагмент структуры папок на серверах предприятия

Сделайте ресурсы на этих серверах доступными пользователям ЛВС компании, определив, к каким папкам открыть доступ и какие разрешения назначить группам, в том числе встроенным.

Ваши решения должны удовлетворять следующим критериям:

- членам группы Managers надо читать и вносить исправления в документы в папке Management Guidelines. Больше никто не должен иметь доступ к этой папке;
- администраторам нужен полный доступ ко всем общим папкам, кроме папки Management Guidelines;

- отделу по работе с клиентами требуется отдельное место в сети для хранения рабочих файлов. Все сотрудники этого отдела — члены группы Customer Service;
- всем сотрудникам компании необходимо место в сети для обмена информацией;
- всем сотрудникам требуются такие приложения, как электронные таблицы, базы данных и текстовые процессоры;
- только члены группы Managers должны иметь доступ к ПО управления проектами предприятия;
- членам группы CustomerDBFull необходимо иметь право читать и вносить информацию о клиентах в БД;
- членам группы CustomerDBRead надо предоставить право только на чтение информации о клиентах из БД;
- каждый пользователь сети должен иметь собственное место в сети для хранения файлов, доступное только ему;
- имена общих ресурсов должны быть доступны с компьютеров Windows2000/NT/98/95, а также с альтернативных платформ.

Запишите свои ответы в таблицу следующего вида.

Табл. 10-5. Общие папки и разрешения для упражнения 2

Имя и размещение папки	Сетевое имя	Группы и разрешения
Образец: Management Guidelines	MgmtGd	Managers: Full Control

Упражнение 3: предоставление доступа к папкам

► **Задание: предоставьте доступ к папкам**

1. Зарегистрируйтесь как Administrator (Администратор).
2. Запустите Windows Explorer (Проводник), создайте папку C:\Apps (где C:\ — имя вашего системного диска), щелкните ее правой кнопкой и выберите Sharing (Доступ).
3. Пока папка не является общей.
4. Щелкните переключатель Share This Folder (Открыть общий доступ к этой папке).
5. Поле Share Name (Сетевое имя) по умолчанию совпадает с именем папки; при желании его можно изменить.
6. В поле Comment (Комментарий) введите **shared productivity applications** и щелкните кнопку OK.

   Как Windows Explorer изменит значок папки Apps, иллюстрируя, что к папке открыт доступ?

Упражнение 4: назначение разрешений доступа к общей папке

Определите текущие разрешения доступа к общей папке и назначьте разрешения группам в вашем домене.

► **Задание 1: определите текущие разрешения для общей папки Apps**

1. В окне свойств папки Apps щелкните вкладку Sharing (Доступ) и затем — кнопку Permissions (Разрешения).

   Каковы разрешения по умолчанию для этой папки?

► **Задание 2: аннулируйте разрешения для группы**

1. Удостоверьтесь, что выбрана группа Everyone (Все).

2. Щелкните кнопку Remove (Удалить).

▶ **Задание 3: назначьте разрешение Full Control группе Administrators**

1. Щелкните кнопку Add (Добавить).

   Откроется диалоговое окно Select Users, Computers, Or Groups (Выбор: Пользователи, Компьютеры или Группы).
2. В списке Look In (Искать в) выберите ваш домен, в поле Name (Имя) щелкните Administrators, а затем — кнопку Add (Добавить).
3. Щелкните кнопку OK.

   Группа Administrators добавится в список групп, имеющих разрешения.

   Какой вид доступа будет назначен группе Administrators по умолчанию?
4. В столбце Allow (Разрешить) окна Permissions (Разрешения) установите флажок Full Control (Полный доступ).

   Почему также стало действующим разрешение Change (Изменение)?
5. Щелкните кнопку OK.
6. Щелкните кнопку OK, чтобы закрыть окно свойств Apps.

Упражнение 5 (дополнительное): подключение к общей папке

Подключитесь к общей папке. Опробуйте два способа.

Внимание! Дополнительное упражнение 5 желательно выполнять на двух компьютерах (второй — с Windows 2000, работающий как сервер домена). Можно, однако, выполнить эти упражнения и на одном компьютере.

▶ **Задание 1: подключите сетевой диск с помощью команды Run**

1. Зарегистрируйтесь на втором компьютере как Administrator.
2. В меню Start (Пуск) выберите команду Run (Выполнить).
3. В поле Open (Открыть) наберите **\\SERVER1** (если у контроллера вашего домена другое имя, используйте его здесь и далее) и щелкните кнопку OK.

   Откроется окно SERVER1. Заметьте, что пользователям сети видны только общие лапки.

   Какие папки доступны в данный момент?
4. Дважды щелкните папку Apps, чтобы убедиться, что вы можете получить доступ к ее содержимому.
5. Закройте окно Apps On SERVER1.

▶ **Задание 2: подключите общую папку как сетевой диск командой Map Network Drive**

1. Щелкните правой кнопкой значок My Network Places (Мое сетевое окружение) и выберите в контекстном меню команду Map Network Drive (Подключить сетевой диск).
2. В поле Folder (Папка) окна мастера Map Network Drive (Подключить сетевой диск), введите **\\SERVER1\Apps** (если у контроллера вашего домена другое имя, далее используйте именно его).
3. В списке Drive (Диск) выберите P:.
4. Сбросьте флажок Reconnect At Logon (Восстанавливать при входе в систему).

   Вам нужен доступ к данной папке только в этом упражнении. Выключение данного режима не позволит Windows 2000 снова подключаться к этой папке в дальнейшем.
5. Для завершения подключения щелкните кнопку Finish (Готово).
6. Закройте окно Apps On 'SERVER1' (P:).

7. Чтобы проверить, что сетевой диск успешно подключен, дважды щелкните значок My Computer (Мой компьютер) на рабочем столе — вы увидите, что появился новый логический диск P: Apps On Server1.

   Как Windows Explorer обозначает, что этот диск соответствует удаленной общей папке?

► **Задание 3: отключите сетевой диск в Windows Explorer**

1. В Windows Explorer щелкните правой кнопкой Apps On 'Server1' (P:) и выберите в контекстном меню команду Disconnect (Отключить).

   Windows 2000 удалит Apps On 'Server1' (P:) из окна My Computer.
2. Закройте Windows Explorer.

► **Задание 4: попытайтесь подключиться к общей палке на контроллере домена**

1. Завершите сеанс и войдите в ваш домен под именем User81.
2. Щелкните кнопку Start (Пуск), затем выберите команду Run (Выполнить).
3. В поле Open (Открыть) наберите **\\SERVER1** (если у контроллера вашего домена другое имя, далее используйте именно его) и щелкните кнопку OK.

   Появится сообщение, что доступ закрыт. Почему?
4. Закройте все окна.

► **Задание 5: подключитесь к общей папке от имени другого пользователя**

1. Щелкните правой кнопкой значок My Network Places (Мое сетевое окружение) и выберите в контекстном меню команду Map Network Drive (Подключить сетевой диск).
2. В окне мастера Map Network Drive (Подключить сетевой диск) в поле Folder (Папка) введите **\\SERVER1\Apps** (если у контроллера вашего домена другое имя, далее используйте именно его).
3. В списке Drive (Диск) выберите J:.
4. Щелкните ссылку Connect Using A Different User Name (Подключение под другим именем).

   В окне Connect As (Подключиться как) задаются параметры учетной записи для подключения к общей папке, в том числе для подключения к другим доменам (в ранних версиях Windows). Когда следует использовать этот режим?
5. В окне Connect As (Подключиться как) в поле User Name наберите domain1**\administrator** (где **domain**1 — имя вашего домена).
6. В поле Password (Пароль) наберите **password** и щелкните кнопку OK.
7. Удостоверьтесь, что флажок Reconnect At Logon (Восстанавливать при входе в систему) сброшен, и щелкните Finish (Готово).
8. Закройте все окна и завершите сеанс.

Упражнение 6: прекращение доступа к папке

► **Задание: закройте доступ к папке**

1. Зарегистрируйтесь в домене как Administrator на контроллере домена и запустите Windows Explorer.
2. Щелкните правой кнопкой папку C:\Apps и выберите в контекстном меню команду Properties (Свойства).
3. В диалоговом окне свойств Apps перейдите на вкладку Sharing (Доступ).
4. Щелкните переключатель Do Not Share This Folder (Отменить общий доступ к этой папке), затем — кнопку OK.

Под Apps больше нет «руки», означавшей, что папка была общей. Возможно, вам сначала понадобится обновить окно — в этом случае нажмите клавишу F5.

5. Закройте Windows Explorer.

Упражнение 7: назначение разрешений NTFS и открытие доступа к папкам

Вы назначите разрешения NTFS папкам Apps, Wordprocessing, Database, Public и Manuals и откроете доступ к Apps и Public.

Создайте с помощью Windows Explorer папки и назначьте им разрешения NTFS согласно таблице, приведенной ниже. Не допускайте наследования разрешений для вложенных объектов и снимите все ранее существовавшие разрешения NTFS.

Табл. 10-6. Папки и разрешения NTFS для упражнения 7

Путь	Группа или учетная запись	Разрешения NTFS
C:\Apps	Administrators Users	Full Control Read & Execute
C:\Apps\Word-prosessing	Administrators Users	Full Control Read & Execute
C:\Apps\Database	Administrators	Read & Execute
C:\Public	Administrators Users	Full Control Modify
C:\Public\Manuals	Administrators Users User83	Full Control Read & Execute Full Control

Откройте доступ к папкам и назначьте разрешения пользователям сети согласно таблице, приведенной ниже. Снимите все остальные разрешения на сетевой доступ.

Табл. 10-7. Папки и разрешения на доступ к общим папкам для упражнения 7

Путь и сетевое имя папки	Группа **или учетная запись**	**Разрешения доступа**
C:\Apps, сетевое имя — Apps	Administrators Users	Read Read
C:\Public, сетевое **имя** — Public	**Administrators** **Users**	Full **Control** Full **Control**

Упражнение 8 (дополнительное): проверка разрешений NTFS и разрешений на доступ к общей папке

Войдите в систему под разными именами, чтобы проверить разрешения, назначенные в упражнении 1. Для ответов на вопросы данного упражнения ссылайтесь на таблицы упражнения 7.

Внимание! Для выполнения дополнительного упражнения 8 вам потребуется второй компьютер с Windows 2000, работающий как сервер домена. Можно, однако, выполнить эти упражнения и на одном компьютере.

▶ **Задание 1: проверьте разрешения для папки Manuals при локальном входе в систему под именем User82**

1. Зарегистрируйтесь в домене как User82 на контроллере домена.
2. В Windows Explorer раскройте папку C:\Public\Manuals.
3. В папке Manuals попытайтесь создать какой-либо файл.
   Удалось ли вам это? Почему?
4. Закройте Windows Explorer,

▶ **Задание 2: проверьте разрешения для папки Manuals при подключении к ней по сети**

1. Зарегистрируйтесь в домене как User82 на втором компьютере (не контроллере домена).
2. Щелкните кнопку Start (Пуск) и выберите команду Run (Выполнить).
3. В поле Open (Открыть) введите **\\server1\public** (где **server1**— имя контроллера домена) и щелкните кнопку OK.
4. В окне Public On Server1 дважды щелкните папку Manuals,
5. Попробуйте создать в ней какой-либо файл.
   Удалось ли вам это? Почему?
6. Закройте все окна и завершите сеанс.

▶ **Задание 3: проверьте разрешения для папки Manuals при локальном доступе**

1. Зарегистрируйтесь при входе в ваш домен как User83 на контроллере домена,
2. В Windows Explorer раскройте папку C:\Public\Manuals.
3. В папке Manuals попытайтесь создать какой-либо файл.
   Удалось ли вам это? Почему?
4. Закройте все окна и завершите сеанс.

Резюме

К папкам можно открыть доступ пользователям сети. На томе FAT разрешения доступа к общим папкам — единственное средство защитить их. На томе NTFS можно назначать отдельным пользователям и группам разрешения NTFS для более гибкого управления доступом к файлам и папкам в обших папках. При сочетании разрешений доступа к общей папке и разрешений NTFS результирующим будет более строгое из них.

Выполняя упражнения, вы создавали папки, открывали и закрывали к ним доступ, а также создавали папки и сначала назначали разрешения NTFS, а затем открывали к ним доступ.

Занятие 5. Настройка DFS

Распределенная файловая система — Distributed file system, DFS — в Windows 2000 Server обеспечивает удобный доступ к общим папкам. Общая папка DFS является точкой входа к остальным общим папкам, распределенным по всей сети.

Изучив материал этого занятия, вы сможете:

- ✓ настраивать DFS в Windows 2000 Server.

Продолжительность занятия — около 40 минут.

Знакомство с DFS

Система Microsoft DFS в Windows 2000 Server облегчает пользователям сети доступ к файлам, находящимся в физически разных фрагментах сети. В этой системе распределенные по разным серверам файлы как бы находятся в одном месте (рис, 10-12). Пользователи легко перемещаются по общим папкам, даже не зная, где реально эти папки размещены. Соответственно упрощается и администрирование общих папок.

Рис. 10-12. Схема работы DFS

DFS реализует несколько функций.

- Организует иерархию ресурсов. Иерархия сетевых ресурсов в DFS состоит из *общих папок DFS* (DFS share). Первый этап при ее организации — создание *корня DFS* (DFS root). В него будут помещаться файлы и DFS-ссылки, которые указывают на общие папки, реально размещенные на разных серверах. Возможны два типа корней DFS, они описаны в таблице.

Табл. 10-8. Типы корней DFS

Тип	Описание
Доменный	Хранит топологию DFS в Active Directory. Ссылки могут указывать на несколько одинаковых папок, что увеличивает устойчивость при сбоях. Поддерживает службу формирования имен узлов Domain Name System (DNS), многоуровневые DFS-ссылки и репликацию файлов
Изолированный	Хранит топологию DFS на отдельном компьютере. Не обеспечивает устойчивости при сбоях компьютера, где размешен данный корень, а также тех компьютеров, на которых находятся используемые системой DFS общие папки. Поддерживает DFS-ссылки только первого уровня

- **Облегчает навигацию по сети.** Вместо соединения с каждым сервером пользователи подключаются только к корню DFS и перемещаются по его ресурсам, лаже не зная имен серверов, на которых эти ресурсы реально находятся.
- **Облегчает администрирование сети.** В случае сбоя сервера достаточно в DFS-ссылке задать новый сервер. Для пользователей имя этого ресурса в системе DFS не изменится.
- **Сохраняет разрешения доступа.** При соединении через DFS проверяются разрешения пользователей для общих папок и NTFS.

Примечание На компьютере клиента необходимо установить ПО клиента DFS. Этот клиент входит в состав Windows 98/NT 4.0/2000 и дополнительно устанавливается в Windows 95.

Использование DFS

DFS стоит применять в следующих случаях:

- пользователи подключаются к общим папкам через один или несколько узлов сети;
- большинствупользователей требуется доступ ко многим общим папкам;
- надо улучшить баланс загрузки серверов, перераспределив по ним общие папки;
- пользователям нужен непрерывный доступ к общим папкам;
- в вашейорганизации имеютсяWeb-узлы для внутреннего или внешнего использования.

Топология DFS

Топология DFS состоит из корня DFS, одной или нескольких DFS-ссылок и соответствующих каждой ссылке общих папок DFS (называемых также репликами).

В случае доменной DFS сервер домена, на котором размещен корень DFS, называется несущим сервером. Можно создать реплики корня на других серверах для случаев, когда несущий сервер занят.

Для пользователей такая топология DFS предоставляет однотипный и простой доступ к сетевым ресурсам. Для администраторов такая топология представляет собой как единое пространство имен DNS. В случае доменной DFS имена DNS корней DFS являются подпространствами для несущего сервера.

Так как несущий сервер доменной DFS является членом домена, топология DFS по умолчанию автоматически публикуется в службе Active Directory. Это обеспечивает синхронизацию топологий DFS для всех несущих серверов и, следовательно, отказоустойчивость для корня DFS, а также оптимальную репликацию общих папок DFS.

Создание системы DFS

Система DFS создается следующим образом:

- создается корень DFS;
- создается DFS-ссылка;
- добавляются общие папки DFS (если нужно);
- задается политика репликации.

Создание корня DFS

Корень DFS в Windows 2000 можно создавать и в разделе FAT, и в разделе NTFS (NTFS имеет дополнительные преимущества при настройке защиты). При создании корня указывается его тип — доменный или изолированный.

▶ **Создание корня** DFS

1. Щелкните кнопку Start (Пуск), выберите пункт Programs (Программы), затем — пункт Administrative Tools, затем — команду Distributed File System (Распределенная файловая система DFS).
2. В меню Action (Действие) щелкните пункт New DFS Root (Создать новый корень DFS) для запуска мастера New DFS Root Wizard (Мастер создания нового корня DFS). Его параметры описаны ниже.

Табл. 10-9. Параметры мастера создания корня DFS

Параметр	Описание
Select The DFS Root Type (Выбор типа корня DFS)	Задает тип корня DFS — доменный или изолированный
Specify The Host Domain For The DFS Root (Выбор несущего домена для корня DFS)	Задает несущий домен для доменного корня DFS
Specify The Host Server For The DFS Root (Выбор несущего сервера для корня DFS)	Задает несущий сервер (начальное соединение для ресурсов в дереве DFS). Это может быть любой компьютер с Windows 2000 Server
Specify The DFS Root Share (Выбор общего ресурса для корня DFS)	**Задает общую** папку для размещения корня **DFS.** Можно **использовать существующую или** создать **новую папку**
Name The DFS Root (Выбор имени для корня DFS)	Задает имя для корня DFS

Создание DFS-ссылки

После создания корня DFS генерируются DFS-ссылки. Их не может быть больше 1 000 в одном корне.

▶ **Создание DFS-ссылки**

1. Щелкните кнопку Start (Пуск), выберите пункт Programs (Программы), затем — пункт Administrative Tools, затем — команду Distributed File System (Распределенная файловая система DFS).
2. Щелкните корень DFS, в котором хотите поместить новую ссылку. Затем в меню Action (Действие) укажите пункт New DFS Link (Создать ссылку DFS).

3. В поле Link Name (Имя ссылки) окна Create A New DFS Link (Создание новой ссылки DFS) (рис. 10-13) введите имя, пол которым ссылка будет доступна пользователям.
4. В поле Send The User To This Shared Folder (Переадресовать пользователя на эту общую папку) введите или найдите с помощью кнопки Browse (Просмотр) сетевой адрес папки, которой должна соответствовать эта ссылка.

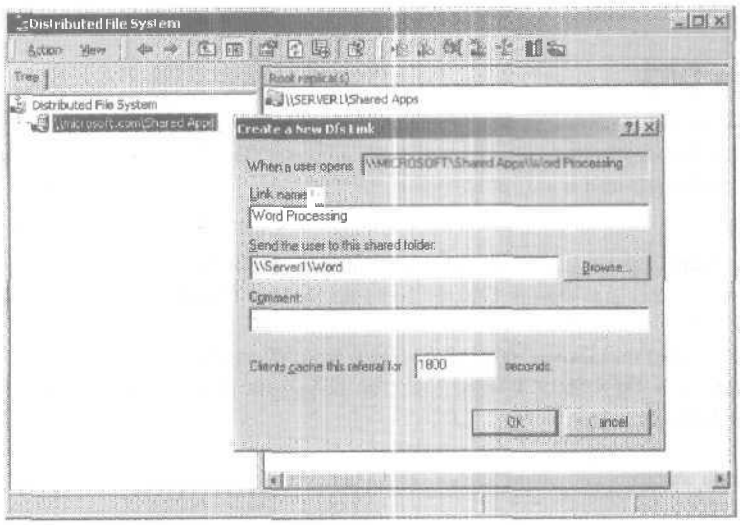


Рис. 10-13. Окно Create A New DFS Link

5. В поле Comment (Комментарий) укажите любую дополнительную информацию о данной общей папке (например, ее действительное сетевое имя).
6. В поле Clients Cache This Referral For *X* Seconds (Клиенты кэшируют ссылку каждые x секунд) введите временной интервал, в течение которого клиенты кэшируют информацию о DFS-ссылке. По истечении этого времени клиент еще раз запросит сервер DFS об адресе ссылки, даже если соединение уже установлено.
7. Щелкните кнопку OK.

   Ссылка появится под соответствующим корнем в дереве консоли DFS.

Добавление общей папки DFS

Для каждой DFS-ссылки можно задать одну или несколько общих папок DFS. Первая папка генерируется средствами консоли DFS при создании DFS-ссылки. Остальные папки добавляются в диалоговом окне Add A New Replica. Для одной ссылки можно задать не более 32 общих папок. Папку DFS разрешается реплицировать. В этом случае необходимо задать политику репликации.

► **Добавление общей папки DFS**

1. Щелкните кнопку Start (Пуск), выберите пункт Programs (Программы), затем — пункт Administrative Tools, затем — команду Distributed File System (Распределенная файловая система DFS).
2. В дереве консоли DFS правой кнопкой щелкните DFS-ссылку, к которой добавляется папка, и в контекстном меню выберите пункт New Replica (Создать реплику).
3. В поле Send The User To This Shared Folder (Переадресовать пользователя на эту общую папку) диалогового окна Add A New Replica (Добавить новую реплику) введите или найдите с помощью кнопки Browse (Просмотр) имя нужной общей папки (рис. 10-14).

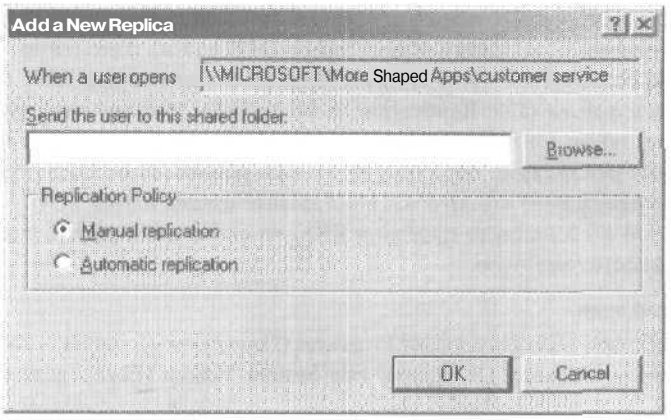


Рис. 10-14. Диалоговое окно Add A New Replica

4. В окне Replication Policy (Политика репликации):
   - выберите переключатель Manual Replication, если нужно, чтобы файлы из данной папки не участвовали в репликации;
   - установите переключатель Automatic Replication (этот режим недоступен для изолированных DFS), чтобы файлы из данной папки участвовали в репликации. Файлы необходимо расположить на томе NTFS сервера Windows 2000.
5. Щелкните кнопку OK.

Настройка политики репликации

Репликация содержимого корней и общих папок DFS в другие корни или папки DFS позволяет сделать их постоянно доступными для пользователей.

Репликация корня DFS

При репликации корня DFS связанная с ним структура DFS будет доступна для пользователей, даже если несущий сервер в момент соединения недоступен.

▶ **Репликация корня DFS**

1. Щелкните кнопку Start (Пуск), выберите пункт Programs (Программы), затем — пункт Administrative Tools, затем — команду Distributed File System (Распределенная файловая система DFS).
2. В дереве консоли DFS правой кнопкой щелкните корень DFS, который надо реплицировать, и в контекстном меню выберите пункт New Root Replica (Создать корневую реплику).
3. Следуйте инструкциям мастера New DFS Root Wizard (Мастер создания нового корня DFS).

Настройка политики репликации для общей папки DFS

При репликации общей папки DFS ее содержимое копируется в другую общую папку. Этот процесс состоит из двух стадий — сначала к DFS-ссылке добавляется общая папка с указанием, что она будет участвовать в репликации, а затем задается политика репликации для общих папок, связанных с данной ссылкой. Репликация бывает ручной и автоматической. Не устанавливайте разные типы репликации внутри одной DFS-ссылки, иначе содержимое папок может оказаться не синхронным.

Автоматическая репликация разрешена только для доменных корней DFS. Она осуществляет автоматическую синхронизацию копий общих папок DFS при их изменении. Автоматическая репликация не реализуется для изолированной DFS и для томов FAT. DFS использует *службу репликации файлов* (File Replication Service, FRS). Именно эта служба синхронизирует содержимое папок DFS. По умолчанию это происходит один раз в 15 минут. При задании политики репликации одна или несколько общих папок DFS объявляются главными. Затем их содержимое копируется в остальные общие папки DFS.

Если управление доменной DFS не было передано FRS, то синхронизировать содержимое общих папок DFS придется вручную.

► **Настройка политики репликации**

1. Щелкните кнопку Start (Пуск), выберите пункт Programs (Программы), затем — пункт Administrative Tools, затем — команду Distributed File System System (Распределенная файловая система DFS).
2. В дереве консоли DFS правой кнопкой щелкните DFS-ссылку, содержащую папки, которые надо реплицировать, и выберите команду Replication Policy (Политика репликации).
3. В диалоговом окне Replication Policy (Политика репликации) щелкните папку, которую вы хотите сделать главной при репликации, затем — кнопку Set Master (рис. 10-15).

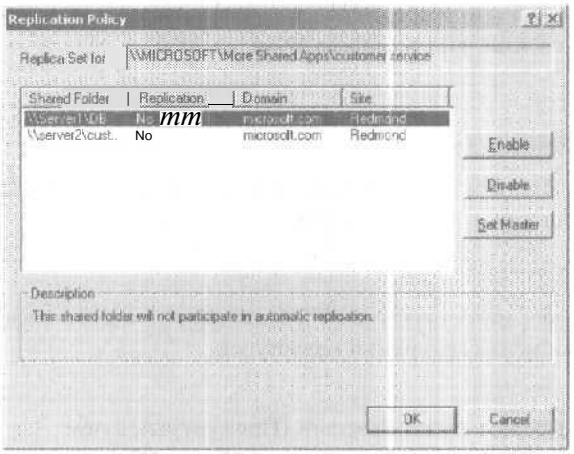


Рис. 10-15. Диалоговое окно Replication Policy (Политика репликации)

4. Щелкая каждую папку в списке, установите для них режим Enable. Затем щелкните кнопку OK.

Примечание Не устанавливайте разные типы репликации внутри одной DFS-ссылки, иначе содержимое папок синхронизируется не всегда.

Практикум: использование DFS

Сейчас вы откроете общий доступ к существующим папкам, создадите новые и откроете к ним доступ. Кроме того, вы создадите новый корень DFS и DFS-ссылки.

Примечание Для дополнительных упражнений требуется два компьютера с Windows 2000 Server — один контроллер домена, другой — сервер-член домена.

► Задание 1: открытие доступа к существующим папкам

1. Зарегистрируйтесь в домене на контроллере домена как администратор.
2. Запустите Windows Explorer и откройте общий доступ с полномочиями по умолчанию к папкам, созданным вами в упражнении 7 занятия 4.

Табл. 10-10. Общие папки для практикума

Папка	Сетевое имя
C:\Apps\Database	DB
C:\Apps\Wordprocessing	Word

► Задание 2: создание общей папки на удаленном компьютере

В Windows Explorer создайте папки согласно следующей таблице (где C:\ — имя системного диска) и откройте к ним общий доступ с полномочиями по умолчанию.

Табл. 10-11. Новые общие лапки для практикума

Папка	Сетевое имя
C:\MoreApps\Maintenance	Maint
C:\MoreApps\CustomerService	Custom

► Задание 3: создание нового корня DFS

1. На контроллере домена щелкните кнопку Start (Пуск), выберите пункт Programs (Программы), затем — пункт Administrative Tools, затем — команду Distributed File System (Распределенная файловая система DFS).

   Откроется консоль Distributed File System (Распределенная файловая система DFS).
2. В меню Action (Действие) выберите пункт New DFS Root (Создать новый корень DFS).

   Запустится мастер New DFS Root Wizard (Мастер создания нового корня DFS).
3. Щелкните Next.

   Мастер откроет страницу Select The DFS Root Type (Выбор типа корня DFS).
4. Щелкните переключатель Create A Domain DFS Root (Создать доменный корень DFS) для создания доменного корня, затем — Next.

   Мастер откроет страницу Select The Host Domain For The DFS Root.
5. Удостоверьтесь, что в поле Domain Name указано microsoft.com (или имя вашего домена) и щелкните Next.

   Мастер откроет страницу Specify The Host Server For The DFS Root (Выбор несущего сервера для корня DFS).
6. Для создания корня DFS на вашем сервере введите его имя в поле Server Name и щелкните Next.

   Мастер откроет страницу Specify The DFS Root Share (Выбор общего ресурса для корня DFS).
7. Можно использовать существующую общую папку или создать новую. Для создания новой корневой папки выберите переключатель Create A New Share. При этом надо задать и путь к папке на данном компьютере и ее сетевое имя. Введите **c:\apps-DFS** (где c:\ — имя вашего системного диска) в поле Path To Share и **Shared Apps** — в поле Share Name.

8. Щелкните кнопку OK.

   Появится окно сообщения системы DFS с запросом подтверждения о создании папки C:\App-DFS.

9. Щелкните кнопку Yes (Да).

   Мастер откроет страницу Name The DFS Root (Выбор имени для корня DFS). Поле DFS Root Name будет уже заполнено.

10. Щелкните Next.

    Мастер откроет страницу Completing The New DFS Root Wizard (Завершение работы мастера создания нового корня DFS) со сводкой выбранных параметров.

И. Удостоверьтесь, что все правильно, и щелкните Finish (Готово).

   Обратите внимание, что в дереве консоли DFS появился корень \\microsoft.com\Shared (где microsoft.com — имя вашего домена).

   Теперь создайте DFS-ссылки, пользуясь следующей таблицей (где C:\ — имя вашего системного диска).

Табл. 10-12. DFS-ссылки для практикума

Ссылка	Общая папка	Имя папки
Database	\\Server1\DB	C :\Apps\ Database
Word Processing	\\Server1\Word	C:\Apps\Wordprocessing
Maintenance	\\second_computer\Maint	C:\MoreApps\Maintenance
Customer Service	\\second_computer\Custom	C:\MoreApps\CustomerService

► **Задание 4: добавьте DFS-ссылки на контроллер домена**

1. В дереве консоли DFS щелкните \\microsoft.com\SharedApps (где microsoft.com — имя вашего домена).
2. В меню Action (Действие) выберите пункт New DFS Link (Создать ссылку DFS).

   Откроется диалоговое окно Create A New DFS Link (Создание новой ссылки DFS).
3. В поле Link Name (Имя ссылки) введите **Database.**
4. В поле Send The User To This Shared Folder (Переадресовать пользователя на эту общую папку) введите **\\server1\DB** (где **server1** — имя вашего контроллера домена).
5. Щелкните кнопку OK.
6. Повторите пункты 1 — 5 и добавьте еще одну ссылку с именем Word Processing, указывающую на общую папку \\Server1\Word (где server1 — имя вашего контроллера домена).

► **Задание 5: добавьте ссылки на удаленный компьютер**

1. В дереве консоли DFS щелкните \\microsoft.com\Shared Apps (где microsoft.com — имя вашего домена).
2. В меню Action (Действие) выберите пункт New DFS Link (Создать ссылку DFS).

   Откроется диалоговое окно Create A New DFS Link (Создание новой ссылки DFS).
3. В поле Link Name (Имя ссылки) введите Maintenance.
4. В поле Send The User To This Shared Folder (Переадресовать пользователя на эту общую папку) введите **\\второй_компьютер\maint** (где **второй_компьютер** — имя компьютера, отличного от контроллера домена) и щелкните кнопку OK.

5. Повторите пункты 1 — 4 и добавьте еще одну ссылку с именем Customer Service, указывающую на общую папку **\\второй_компьютер\Custom** (где **второй_компьютер** — имя компьютера, отличного от контроллера домена).
6. Закройте консоль DFS.

▶ **Задание 6: доступ к корню DFS**

1. На контроллере домена или другом компьютере последовательно дважды щелкните: значок My Network Places (Мое сетевое окружение), Entire Network (Вся сеть), Microsoft Windows Network (Сеть Microsoft Windows), имя вашего домена.
2. Дважды щелкните компьютер SERVER1.

   Windows Explorer выведет список всех общих папок на контроллере вашего домена. Одна из них — Shared Apps, созданный вами корень DFS.

   Обозначает ли как-либо Windows 2000, что Shared Apps не является обычной общей папкой?
3. Для просмотра DFS-ссылок дважды щелкните папку Shared Apps.

   Windows Explorer откроет окно Shared Apps On Server1 со списком всех ссылок этого корня.

   Обозначает ли как-либо Windows 2000, что DFS-ссылки в Shared Apps не являются обычными общими папками?
4. Закройте все окна.

Резюме

Распределенная файловая система Microsoft DFS в Windows 2000 Server обеспечивает удобный доступ к общим папкам, расположенным в разных местах сети. Ресурсы DFS состоят из корня и дерева ссылок, указывающих на общие папки в сети. DFS делает структуру сети незаметной для пользователей — им не нужно знать имена серверов и имена общих папок. В случае сбоя сервера достаточно в DFS-ссылке задать новый сервер. Для пользователей имя этого ресурса в системе DFS не изменится.

Выполняя задания практикума, вы открыли доступ к существующим и к новым папкам, создали корень DFS и DFS-ссылки.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. и приложении А «Вопросы и ответы» в конце книги.

1. Общая папка расположена на томе FAT, и пользователь имеет для нее разрешение Full Control. К каким объектам в этой папке получит доступ пользователь?

2. Назовите разрешения доступа к общей папке.

3. Какие разрешения назначаются общей папке по умолчанию?

4. Общая папка расположена на томе NTFS, и пользователь имеет для нее разрешение Full Control. К каким объектам в этой папке получит доступ пользователь?

5. Почему рекомендуется централизованно хранить общие папки данных?

6. Каков наилучший способ защиты общих файлов и папок на томе NTFS?

7. Как система DFS облегчает навигацию пользователей по сети?

ГЛАВА 11

Администрирование Active Directory

В этой **главе**

Администрирование Active Directory включает не только установку и настройку, но также поиск объектов, назначение им разрешений, публикацию ресурсов, перемещение объектов между доменами и в их пределах, делегирование административных полномочий организационным подразделениям (ОП), резервное копирование и восстановление БД, а также устранение проблем. Здесь подробно рассматриваются задачи администрирования Active Directory.

Прежде всего

Для изучения материалов этой главы необходимо:

- настроить компьютеры в соответствии с инструкциями вводной главы;
- настроить компьютер в качестве контроллера домена;
- установить пакет утилит Windows 2000 Support Tools в соответствии с инструкциями главы 3;
- изучить материалы глав 7, 8, 9 и 10 и выполнить упражнения из них.

Занятие 1. Поиск объектов Active Directory

Active Directory хранит информацию об объектах сети. Каждый объект — это определенный поименованный набор атрибутов, представляющих конкретный объект сети. Active Directory разработана для предоставления пользователям и приложениям информации об объектах каталога. Здесь рассказывается о поиске объектов Active Directory с помощью команды Find (Найти) консоли Active Directory Users and Computers (Active Directory — пользователи и компьютеры).

Изучив материал этого занятия, вы сможете:

- ✓ описать типы объектов Active Directory;
- ✓ найти объект Active Directory любого типа с помощью команды Find.

Продолжительность занятия — около 15 минут.

Наиболее распространенные объекты Active Directory

При добавлении в сеть новых ресурсов создаются представляющие их объекты Active Directory. Вам надо знать наиболее часто используемые типы объектов Active Directory. Они описаны в табл. 11-1.

Табл. 11-1. Наиболее часто используемые объекты Active Directory

Объект	Описание
Учетная запись пользователя	Сведения, позволяющие пользователю входить в систему Windows 2000 (например, имя пользователя для входа в систему). Данные сведения могут также включать имя, фамилию и отображаемое имя пользователя, номер телефона, адрес электронной почты, адрес домашней страницы и т. п.
Контакт	Сведения о пользователе, обращающемся в организацию: номер телефона, адрес электронной почты, домашний адрес, адрес домашней страницы и т. п.
Группа	Набор учетных записей пользователей, групп или компьютеров, упрощающий администрирование
Общая папка	*Указатель* (pointer) на общую папку компьютера. Содержит не сами данные, но путь к ним. Общая папка и указатели представлены в реестре компьютера. В результате публикации общей папки в Active Directory создается объект, содержащий указатель на нее
Принтер	Указатель на принтер компьютера. Принтеры компьютеров, не входящих в Active Directory, необходимо опубликовать вручную. Microsoft Windows 2000 автоматически добавляет в Active Directory принтеры, подключаемые к контроллеру домена
Компьютер	Информация о компьютере — члене домена
Контроллер домена	Информация о контроллере домена, включающая необязательное описание, DNS-имя, имя, которое контроллер имел, когда работал под управлением предыдущей версии Windows, сведения о версии установленной ОС, местоположении и администраторе контроллера домена
Организационное подразделение (ОП)	Содержит объекты, **в том числе и другие ОП, позволяет** структурировать **объекты Active** Directory

Команда Find

Для поиска объектов откройте консоль Active Directory Users and Computers (Active Directory — пользователи и компьютеры), щелкните домен или контейнер дерева консоли правой кнопкой и выберите в контекстном меню команду Find (Найти). Откроется диалоговое окно Find (Поиск), позволяющие искать объекты в глобальном каталоге (рис. 11-1). Здесь можно создать LDAP-запрос к каталогу или специальному ОП. В глобальном каталоге хранится частичная реплика всего каталога с информацией обо всех объектах дерева доменов/леса. Таким образом, пользователь может найти необходимую информацию независимо от того, какой домен дерева/леса содержит требуемые данные. Active Directory автоматически генерирует содержимое глобального каталога на основе данных доменов, составляющих каталог.

Ниже описываются элементы диалогового окна Find (Поиск).

Табл. 11-2. Элементы диалогового окна Find

Элемент	Описание
Список In (в)	**Список доступных** для поиска **мест,** включая **весь** каталог **Active** Directory, **конкретные** домены и ОП
Кнопка Browse (Обзор)	Позволяет указать путь для поиска
Список Find (Найти)	Список доступных для поиска типов объектов, включая пользователей, контакты, группы, компьютеры, принтеры, общие папки, ОП, а также дополнительные параметры. В последнем случае система позволяет пользователю создать LDAP-запрос на основе введенных им параметров. Так, LDAP-запрос ОП=*er* (введенный на вкладке Advanced) вернет имена ОП, содержащие комбинацию символов «er». например Domain Controllers
Вкладка Advanced (Дополнительно)	Контекстно-зависимая вкладка для определения условий поиска, предоставляющая множество параметров отбора пользователей, контактов, групп, компьютеров, общих папок и ОП. При поиске по дополнительным параметрам вкладка Advanced позволяет со дать запрос вручную или на основе атрибутов, распределенных по типам объектов на вкладке Custom Search (Особый поиск). Вкладка Custom Search предоставляет те же параметры поиска, что и вкладка Advanced
Список Field (Поле)	Контекстно-зависимый перечень атрибутов для поиска выбранного типа объектов. Расположен на вкладке Advanced
Список Condition (Условие)	Контекстно-зависимый перечень способов дальнейшей настрой ки поиска по атрибутам. Расположен на вкладке Advanced
Поле Value (Значение)	Позволяет указать значение поля (атрибута), используемого для поиска объекта в Active Directory. Находится на вкладке Advanced. Для поиска объекта по атрибуту необходимо указать значение этого атрибута. Например, при поиске пользователей, имя которых начинается с буквы R, необходимо в списке Field выбрать поле First Name (Имя), в списке Condition выбрать условие Starts With (начинается) и в поле Value ввести R
Кнопка Find Now (Найти)	Инициирует поиск с заданными параметрами
Кнопка Stop (Остановить)	Останавливает поиск. Когда вы щелкнете эту кнопку, будут выведены элементы, найденные на текущий момент

Табл. 11-2. Элементы диалогового окна Find (*окончание*)

Элемент	Описание
Список условий поиска	В списке в нижней части вкладки Advanced перечислены все заданные вами условия поиска. Для задания условия поиска используются списки Field и Condition, а также поле Value. Чтобы удалить условие поиска, выберите его из списка и щелкните кнопку Remove (Удалить). Добавляя или удаляя условия, можно расширить или сузить область поиска
Кнопка Clear All (Очистить все)	Отменяет заданные параметры поиска
Панель результатов	Панель в нижней части окна Find, где отображаются результаты поиска

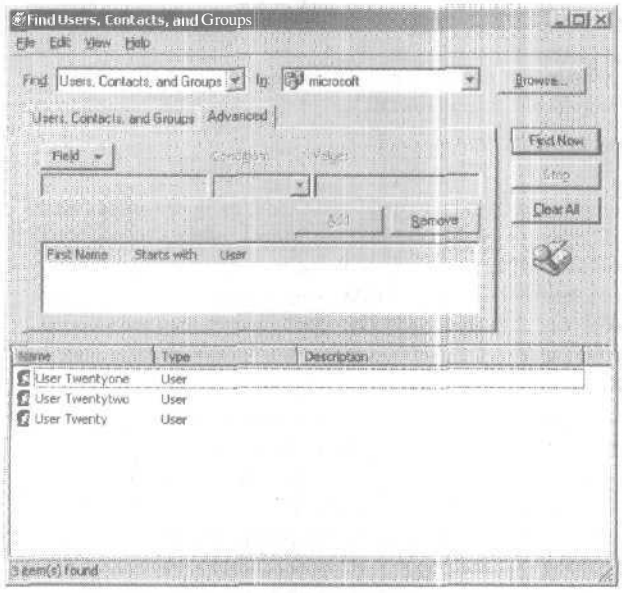


Рис. 11-1. Поиск объектов Active Directory с помощью команды Find

Практикум: поиск в Active Directory

Сейчас вы попробуете найти в Active Directory объекты, соответствующие заданным вами параметрам. Вы создадите учетные записи пользователей и попробуете найти их по номеру телефона. Затем вы найдете принтер, позволяющий брошюровать печатаемые страницы.

Внимание! На вашем компьютере необходимо установить локальный принтер. Впрочем, реальное устройство печати вам не потребуется. Если локальный принтер еще не установлен, сделайте это. Помните, что термин *«устройство печати»* означает физическое устройство печати, а термин *«локальный принтер»* — программное обеспечение, необходимое Windows 2000 для передачи данных на печать.

► Задание 1; создайте учетные записи пользователей

1. Зарегистрируйтесь в домене как Administrator (Администратор) и откройте оснастку Active Directory Users and Computers (Active Directory — пользователи и компьютеры).
2. В дереве консоли щелкните Users.
3. В меню Action (Действие) выберите команду New\User (Создать\Пользователь).

   Обратите внимание — диалоговое окно New Object — User (Новый объект —пользователь) сообщает, что новая учетная запись пользователя создается в папке Users вашего домена.
4. Создайте учетные записи, пользуясь данными табл. 11-3.

Табл. 11-3. Учетные записи пользователей для данного упражнения

First Name (Имя)	Last Name (Фамилия)	User Logon Name (Имя входа пользователя)	Password (Пароль)	Change Password (Изменить пароль)
User	Twenty	User20	Password	По умолчанию
User	Twentyone	User21	Password	По умолчанию
User	Twentytwo	User22	Password	По умолчанию

   Включите всех пользователей в группу Print Operators (Операторы печати) или в другую группу, обладающую правом локально регистрироваться на котроллере домена.
5. Откройте окно свойств учетной записи User20 и на вкладке General (Общие) в поле Telephone Number (Номер телефона) наберите **555-1234.**

► Задание 2: найдите учетную запись пользователя в домене

1. В дереве консоли щелкните свой домен правой кнопкой и выберите команду Find (Найти).

   Откроется диалоговое окно Find (Поиск).

   Какие типы объектов доступны для поиска?
2. Убедитесь, что в поле Find выбран элемент Users, Contacts, And Groups (Пользователи, контакты и группы), и щелкните кнопку Find Now (Найти). Что вы увидите?

   Заметьте, что в Windows 2000 можно выполнять поиск объектов, например учетных записей пользователей, независимо от их размещения.
3. В диалоговом окне Find Users, Contacts. And Groups (Поиск: Пользователи, контакты и группы) щелкните кнопку Clear All (Очистить все) и затем — OK, чтобы подтвердить отмену результатов поиска.
4. В списке In (в) выберите свой домен.
5. Перейдите на вкладку Advanced (Дополнительно).
6. Щелкните список Field, выберите элемент User (Пользователь), при необходимости прокрутите список и щелкните Telephone Number (Номер телефона).

   Заметьте: Windows 2000 выберет в списке Condition (Условие) элемент Starts With (начинается).
7. В поле Value (Значение) наберите 555 и щелкните кнопку Add (Добавить).
8. Щелкните кнопку Find Now (Найти).

   В диалоговом окне Find Users, Contacts, And Groups появится учетная запись пользователя User20, для которого был задан номер телефона 555-1234.
9. Закройте диалоговое окно Find Users, Contacts, And Groups.

▶ **Задание 3: просмотрите сведения о принтерах в оснастке Active Directory Users and Computers**

1. В меню View (Вид) выберите команду Users, Groups, And Computers As Containers (Пользователи, группы и компьютеры как контейнеры).

   По умолчанию оснастка Active Directory Users and Computers не отображает принтеры. Вам придется изменить параметры просмотра.
2. В дереве консоли раскройте узел Domain Controllers, чтобы увидеть свой компьютер.

   Оснастка Active Directory Users and Computers отобразит ваш компьютер в дереве консоли. Заметьте, что узел компьютера можно раскрыть, поскольку компьютер представлен в виде контейнера.
3. В дереве консоли щелкните имя своего компьютера.

   Оснастка Active Directory Users and Computers отобразит все принтеры вашего компьютера как связанные с ним объекты.
4. Для просмотра свойств принтера дважды щелкните требуемый принтер.
5. В диалоговом окне свойств принтера щелкните флажок Staple (Сшиватель), чтобы указать, что данный принтер может брошюровать печатаемые страницы, и затем щелкните OK.
6. Сверните оснастку Active Directory Users and Computers.
7. Раскройте меню Start\Search\For Printers (Пуск\Поиск\Принтеры).
8. В диалоговом окне Find Printers (Поиск: Принтеры) перейдите на вкладку Features (Возможности).
9. Щелкните флажок Can Staple (Сшивка).
10. В списке In (в) выберите свой домен и затем щелкните кнопку Find Now.

    На панели результатов появятся сведения о принтере, свойства которого вы изменили.
11. Закройте диалоговое окно Find Printers.

Резюме

Наиболее распространенные объекты Active Directory — это учетные записи пользователей, контакты, группы, общие папки, принтеры, компьютеры, контроллеры домена и ОП. Для поиска объектов надо открыть оснастку Active Directory Users and Computers, щелкнуть элемент дерева консоли правой кнопкой мыши и выбрать команду Properties (Свойства). Диалоговое окно Find (Поиск) позволяет искать объекты Active Directory.

В практической части занятия вы выполнили поиск объектов Active Directory по заданным вами условиям.

Занятие 2. Управление доступом к объектам Active Directory

Для управления доступом к объектам Active Directory в Windows 2000 используется основанная на объектах модель безопасности, аналогичная применяемой Windows 2000 при реализации защиты NTFS. У каждого объекта Active Directory имеется дескриптор безопасности, который определят список обладающих доступом лиц и предоставленный им тип доступа. Windows 2000 использует эти дескрипторы для управления доступом к объектам. Здесь обсуждается назначение разрешений объектам Active Directory.

Изучив материал этого занятия, вы сможете:

- ✓ назначать разрешения для управления доступом к объектам Active Directory.

Продолжительность занятия — около 20 минут.

Основы разрешений Active Directory

Разрешения Active Directory обеспечивают защиту ресурсов, позволяя вам управлять доступом пользователей к отдельным объектам и их атрибутам.

Безопасность Active Directory

Для определения круга лиц, обладающих доступом к объекту, а также типа предоставляемого доступа воспользуйтесь разрешениями Active Directory. Чтобы пользователи могли обращаться к объекту, администратор или владелец объекта должен настроить разрешения доступа. Windows 2000 хранит список разрешений доступа, называемый *списком управления доступом* (access control list, ACL) для каждого объекта. Список ACL объекта содержит перечень лиц, обладающих доступом к объекту, а также перечень прав каждого из этих пользователей.

Разрешения применяются для предоставления пользователю или группе прав управления ОП, иерархией ОП или отдельным объекта без назначения административных разрешений на управление другими объектами Active Directory.

Разрешения для объектов

Предоставляемые разрешения зависят от типа объекта. Разрешения, назначаемые различным типам объектов, иногда отличаются. Например, объекту-пользователю можно назначить разрешение Reset Password, а объекту-принтеру — нельзя.

Пользователь может состоять в нескольких группах, каждая из которых обладает разными разрешениями, предоставляющими разные уровни доступа к объектам. Если вы назначаете пользователю разрешение для доступа к объекту и он является членом группы, которой было назначено другое разрешение, для доступа к объекту пользователю будет предоставлена совокупность разрешений группы и его собственных. Например, если пользователь с разрешением Read состоит в группе, обладающей разрешением Write для того же объекта, действительными разрешениями пользователя будут Read и Write.

Разрешения можно активизировать или блокировать. Заблокированное разрешение перекрывает любые другие разрешения, которые позволили бы пользователю обратиться к объекту. Если вы заблокируете доступ к объекту, пользователь не сможет обратиться к нему, даже если он состоит в полномочной группе. Блокирование следует применять, только если действительно необходимо запретить доступ к объекту пользователю, входящему в полномочную группу.

Примечание Убедитесь, что для каждого объекта определен хотя бы один пользователь с разрешением Full Control. Иначе возможна ситуация, когда пользователь (даже администратор) не сможет обратиться к объекту с помощью оснастки Active Directory Users and Computers, пока не сменится владелец объекта.

Обычные и специальные разрешения

Разрешения бывают обычные и специальные. Как правило, объектам присваиваются стандартные разрешения, состоящие из специальных. Специальные разрешения позволяют более тонко настраивать доступ к объектам.

Например, стандартное разрешение Write состоит из специальных разрешений Write All Properties (Запись всех свойств), Add/Remove Self As Member (Добавить или удалить самого себя как члена) и Read (Чтение).

Ниже перечислены применяемые к большинству объектов обычные разрешения (у многих объектов также имеются специальные разрешения) и вид доступа, предоставляемого каждым из разрешений.

Табл. 11-4. Обычные разрешения для объектов и предоставляемый ими вид доступа

Разрешение для объекта	Права пользователя
Full Control (Полный доступ)	Позволяет изменять разрешения и становиться владельцем объекта, а также выполнять задачи, допускаемые остальными обычными разрешениями
Read (Чтение)	Позволяет просматривать объект, его атрибуты, сведения о владельце и разрешения Active Directory
Write (Запись)	Позволяет изменять атрибуты объекта
Create All Child Objects (Создание всех дочерних объектов)	Позволяет добавлять в ОП дочерние объекты любых типов
Delete All Child Objects (Удаление всех дочерних объектов)	Позволяет удалять из ОП дочерние объекты любых типов

Назначение разрешений Active Directory

Для задания атрибутов и стандартных разрешений объектам применяется оснастка Active Directory Users and Computers. Разрешения назначаются на вкладке Security (Безопасность) диалогового окна свойств объекта (рис. 11-2). Диалоговые окна свойств для каждого типа объектов различны.

Внимание! Для доступа к вкладке Security и назначения атрибутов стандартных разрешений необходимо выбрать в меню View (Вид) команду Advanced Features (Дополнительные функции).

Если флажки в списке Permissions (Разрешения) выделены серым цветом, значит объект унаследовал соответствующие разрешения от родительского объекта. Чтобы запретить наследование разрешений от родительской папки, снимите флажок Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект).

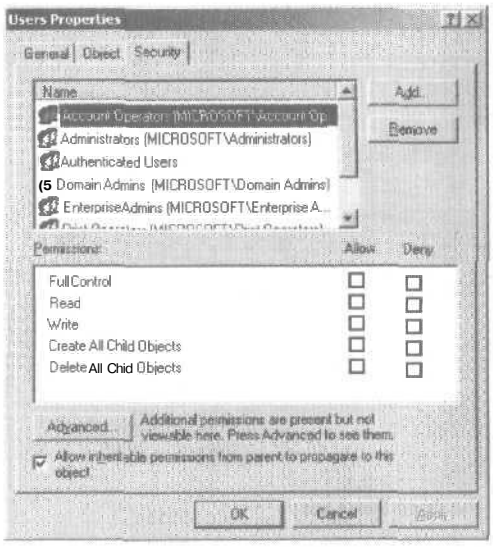


Рис. 11-2. Задание разрешений Active Directory

▶ Назначение объекту стандартных разрешений

1. Убедитесь, что в меню View (Вид) оснастки Active Directory Users and Computers команда Advanced Features (Дополнительные функции) помечена галочкой.
2. Щелкните объект, выберите в меню Action команду Properties и затем перейдите на вкладку Security (Безопасность) открывшегося окна свойств объекта.
3. Чтобы:
   - добавить новое обычное разрешение, щелкните кнопку Add (Добавить), выберите требуемую учетную запись пользователя или группу, шелкните кнопку Add и затем шелкните OK;
   - изменить существующее обычное разрешение, шелкните учетную записьпользователя или группы.
4. В списке Permissions пометьте для каждого добавляемого или удаляемого разрешени я флажок Allow (Разрешить) или Deny (Запретить).

Обычные разрешения позволяют выполнять большинство административных задач. Тем не менее иногда требуется просмотреть составляющие обычное разрешение специальные разрешения. На вкладке Security отображаются пользователи или группы, для которых не разрешены и не отменены стандартные разрешения; это означает, что пользователю/группе предоставлены специальные разрешения. Для их просмотра следует щелкнуть кнопку Advanced (Дополнительно).

▶ Просмотр специальных разрешений

1. На вкладке Security диалогового окна свойств щелкните кнопку Advanced.
2. В диалоговом окне Access Control Settings For (Параметры управления доступом для), аналогичном показанному на рис. 11-3, на вкладке Permissions (Разрешения) щелкните элемент, который вы хотите просмотреть в списке Permission Entries (Элементы разрешений), и затем шелкните кнопку View/Edit (Показать/Изменить).

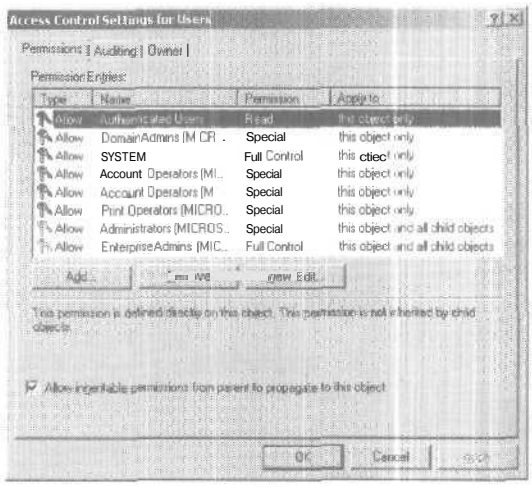


Рис. 11-3. Диалоговое окно Access Control Settings For Users

3. В диалоговом окне Permission Entry For (Элемент разрешения для) данного объекта изучите специальные разрешения на следующих вкладках (рис. 11-4):
   - Object (Объект) — специальные разрешения объекта, назначенные отдельному пользователю/группе;
   - Properties (Свойства) — тип доступа(чтение или запись) пользователя/группы кконкретным свойствам объекта.

Примечание Избегайте назначать разрешения доступа к специальным свойствам объекта — это усложняет администрирование сисгемы, так как возникают разного рода ошибки (например, не удается просмотреть объекты Active Directory и т. п.), не позволяющие пользователям выполнять свои задачи.

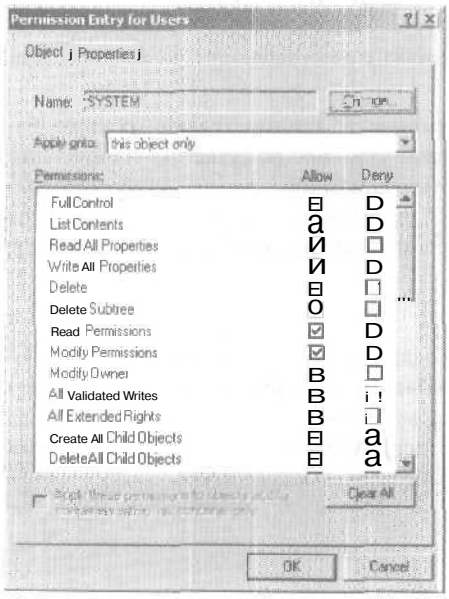


Рис. 11-4. Диалоговое окно Permission Entry For Users

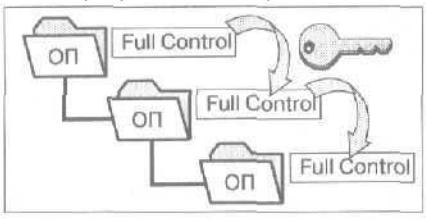
Использование наследования разрешений

Аналогично наследованию разрешений папок и файлов, наследование разрешений объектов Active Directory позволяет упростить назначение необходимых разрешений доступа. Назначаемые разрешения распространяются на дочерние объекты, то есть наследуются всеми дочерними объектами от данного родительского объекта (рис. 11-5). Флажки наследуемых разрешений затенены.

Например, группе можно назначить разрешение Full Control для доступа к содержащему принтеры ОП и распространить это разрешение на все дочерние объекты группы. В результате все члены группы смогут администрировать все принтеры данного ОП.

Можно указать, что разрешения для данного объекта распространяются на все его дочерние объекты или запретить наследование разрешений. При копировании унаследованных разрешений объект изначально получает все разрешения родителя. Тем не менее любые разрешения для родительского объекта, измененные после запрета наследования, уже не распространяются на дочерние объекты. При удалении унаследованных разрешений Windows 2000 удаляет существующие разрешения для объекта и не назначает ему дополнительных разрешений. Вам потребуется вручную задать все необходимые разрешения.

- Наследование разрешений дочерними объектами



- Запрет наследования отменяет распространение разрешений

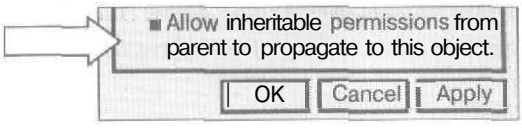


Рис. 11-5. Наследование разрешений и запрет наследования

Запрет наследования разрешений

Если флажок Allow Inheritable Permissions From Parent To Propagate **To** This Object снят, наследование разрешений блокируется, то есть дочерние объекты не получают никаких разрешений от родителя. При запрете наследования действуют лишь те разрешения, которые вы явно назначили объекту. Запретить наследование разрешений можно в диалоговом окне свойств на вкладке Security.

При запрете наследования Windows 2000 позволяет:

- скопировать для объекта унаследованные разрешения. Новые явные разрешения — это копия унаследованных разрешений для родительского объекта. После копирования вы сможете изменить разрешения согласно собственным требованиям;
- удалить унаследованные разрешения для объекта. Windows 2000 удаляет все унаследованные разрешения, и у объекта не остается каких-либо разрешений. Затем вы вправе назначить все необходимые разрешения.

Практикум: управление доступом к объектам Active Directory

Сейчас вы создадите ОП, включающее двух пользователей, и изучите параметры зашиты по умолчанию для этих объектов Active Directory.

Внимание! Во избежание потери доступа к разделам Active Directory не изменяйте какие-либо параметры безопасности Active Directory при выполнении данного упражнения.

▶ Задание 1: создайте ОП, включающее две учетные записи пользователей

1. Зарегистрируйтесь в домене как Administrator и откройте оснастку Active Directory Users and Computers.
2. В дереве консоли щелкните свой домен.
3. В меню Action выберите команду New\Organizational Unit (Создать\Подразделение).
4. В диалоговом окне New Object — Organizational Unit (Новый объект — Подразделение) в поле Name (Имя) наберите **security1** и щелкните OK.
5. Создайте в ОП Security1 учетную запись пользователя, набрав в поле First Name (Имя) и в поле User Logon Name (Имя входа пользователя) слово **Assistant 1.** Наберите пароль **password** и примите остальные значения по умолчанию.
6. В том же ОП создайте еще одну учетную запись, набрав в поле First Name и в поле User Logon Name слово **Secretary1**. Наберите пароль **password** и примите остальные значения по умолчанию.
7. Добавьте обоих пользователей в группу Print Operators (Операторы печати) или другую группу, обладающую правом локального входа на контроллер домена.

▶ Задание 2: просмотрите разрешения, заданные Active Directory по умолчанию для ОП

1. В меню View (Вид) выберите команду Advanced Features (Дополнительные функции).

   После этого вы сможете просматривать и настраивать разрешения Active Directory.
2. В дереве консоли щелкните объект Security1 правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
3. Перейдите на вкладку Security (Безопасность).
4. Запишите в приведенную ниже таблицу группы, обладающие разрешениями доступа к ОП Security1. Эта информация понадобится на занятии 5.

Табл. 11-5. Группы, обладающие разрешениями доступа к ОП Securityl

Учетная запись или группа	Установленные разрешения

Как узнать, не наследуются ли какие-либо разрешения от домена (родительского объекта)?

▶ Задание 3: просмотрите специальные разрешения ОП

1. В диалоговом окне свойств ОП Securityl на вкладке Security (Безопасность) щелкните кнопку Advanced (Дополнительно).

   Откроется диалоговое окно Access Control Settings For Securityl (Параметры управления доступом для Securityl).
2. Чтобы просмотреть специальные разрешения группы Account Operators (Операторы учета), в списке Permission Entries (Элементы разрешений) выделите каждый элемент, относящийся к данной группе, и затем щелкните кнопку View/Edit (Показать/Изменить).

Откроется окно Permission Entry For Security1 (Элемент разрешения для Security1).

Какие разрешения объекта назначены группе Account Operators? Какие действия могут выполнять члены группы Account Operators в данном ОП? (Совет: проверьте в поле Permission Entries каждую запись разрешения, относящуюся к группе Account Operators).

Все ли объекты данного ОП наследуют разрешения, назначенные для группы Account Operators? Почему?

3. Закройте все диалоговые окна; оснастку Active Directory Users and Computers не закрывайте.

▶ **Задание 4: просмотрите разрешения, назначаемые Active Directory по умолчанию для объекта-пользователя**

1. В дереве консоли оснастки Active Directory Users and Computers щелкните Security1.
2. В правой панели щелкните Security1 правой кнопкой и выберите команду Properties.
3. Перейдите на вкладку Security.
4. Запишите в приведенную ниже таблицу группы, обладающие разрешениями доступа к учетной записи Secretary1. Эта информация понадобится вам на занятии 5. Если в диалоговом окне для какой-либо группы отображаются специальные разрешения, не включайте в список разрешения, для просмотра которых необходимо щелкнуть кнопку Advanced.

Табл. 11-6. Разрешения для объекта Security1

Группа	Установленные разрешения

Одинаковы ли обычные разрешения для объекта-пользователя и объекта-ОП? Почему?

Унаследованы ли какие-нибудь разрешения от родительского объекта Security1? Как это узнать?

Какими правами обладают члены группы Account Operators в отношении объекта-пользователя?

5. Закройте все программы и завершите рабочий сеанс.

Резюме

У каждого объекта Active Directory имеется дескриптор безопасности, который определяет список обладающих доступом лиц и предоставленный им тип доступа. Чтобы пользователи могли обращаться к объекту, администратор или владелец объекта должен настроить разрешения доступа. Windows 2000 хранит список разрешений доступа, называемый *списком управления доступом* (access control list, ACL) для каждого объекта Active Directory.

Вы научились назначать объектам обычные и специальные разрешения. Стандартные разрешения — Full Control, Write, Read, Create All Child Objects и Delete All Child Objects. Специальные разрешения позволяют более тонко настраивать доступ к объектам. Механизм наследования разрешений объектов Active Directory позволяет упростить назначение необходимых разрешений доступа. Назначаемые разрешения распространяются и на дочерние объекты, то есть они наследуются всеми дочерними объектами данного родительского объекта. Наследование разрешений можно запретить.

Выполняя практикум, Вы создали ОП, включающее двух пользователей, и изучили стандартные параметры безопасности этих объектов.

Занятие 3. Публикация ресурсов в Active Directory

Как администратору, вам надо обеспечить безопасную и выборочную публикацию сетевых ресурсов пользователям сети, а также упростить пользователям поиск информации. Каталог содержит необходимую информацию, позволяет быстро ее искать, а также применяет встроенные механизмы безопасности Windows 2000 для управления доступом. Здесь рассказывается о публикации ресурсов в Active Directory.

Изучив материал этого занятия, вы сможете:

- ✓ публиковать общие папки, принтеры и сетевые службы.

Продолжительность занятия — около 10 минут.

Публикация ресурсов в Active Directory

К ресурсам, которые можно опубликовать в Active Directory, относятся такие объекты, как учетные записи пользователей, компьютеры, принтеры, папки, файлы и сетевые службы.

Публикация учетных записей пользователей и компьютеров

Для добавления в каталог учетных записей пользователей и компьютеров применяется консоль Active Directory Users and Computers (Active Directory — пользователи и компьютеры). Сведения об учетных записях, полезных другим пользователям сети, публикуются автоматически. Прочая информация, например о системе безопасности, доступна лишь определенным административным группам.

Публикация общих ресурсов

Публикация данных об общих ресурсах (принтерах, папках и файлах) упрощает пользователям поиск этих ресурсов в сети. Сетевые принтеры Windows 2000 автоматически публикуются в каталоге при установке. Для публикации сведений о принтерах и общих папках Windows NT применяется консоль Active Directory Users and Computers.

▶ **Публикация общей папки**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Active Directory Users And Computers (Active Directory — пользователи и компьютеры).
2. В дереве консоли дважды щелкните узел домена.
3. Щелкните правой кнопкой контейнер, в который требуется добавить общую папку, и выберите команду New\Shared Folder (Создать\Общая папка).
4. В диалоговом окне New Object-Shared Folder (Новый объект — Общая папка) введите в поле Name (Имя) имя папки.
5. В поле Network Path (Сетевой путь) введите UNC-имя (*сервер**общий_ресурс*\), которое требуется опубликовать в каталоге, и щелкните OK.

   Общая папка отобразится в выбранном вами контейнере каталога.

▶ **Публикация принтера Windows NT**

Примечание Перед публикацией в Active Directory необходимо установить принтер Windows NT. Для этого раскройте меню Start\Settings\ Printers (Пуск\Настройка\Принтеры).

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers.
2. В дереве консоли дважды щелкните узел домена.
3. В дереве консоли щелкните правой кнопкой контейнер, в котором требуется опубликовать принтер, выберите в контекстном меню команду New\Printer (Создать\Принтер).
4. В диалоговом окне New Object-Printer (Новый объект — Принтер) в поле Network Path Of The Pre-Windows 2000 Print Share (Сетевой путь к пред-Windows 2000 общему ресурсу печати) наберите UNC-имя, которое требуется опубликовать в каталоге, и щелкните OK.

   Принтер Windows NT отобразится в выбранном вами контейнере каталога.

Публикация сетевых служб

Публикация сетевых служб (например, служб сертификации) в каталоге позволит администраторам находить и управлять ими с помощью консоли Active Directory Sites and Services (Active Directory — сайты и службы). Публикуя службу, а не компьютер или сервер, администраторы получают возможность управлять этой службой независимо от того, какой компьютер ее предоставляет и где он расположен. Для публикации в каталоге дополнительных служб и приложений можно воспользоваться API-интерфейсами Active Directory.

Далее рассказано, как выполнить публикацию в каталоге. Постарайтесь уяснить, как Active Directory работает со службами.

Типы сведений о службе

Наиболее часто в Active Directory публикуются сведения о привязке и конфигурации.

- Сведения о привязке позволяют пользователям подключаться к службам, не имеющим известных привязок. Публикуя привязки для таких служб, Windows 2000 получает возможность автоматически к ним подключаться. Службы, ассоциируемые с конкретными машинами, обычно управляются в индивидуальном порядке и не должны публиковаться в каталоге.
- Конфигурационные сведения могут совместно использоваться клиентскими приложениями. Публикация этой информации позволяет знакомить с текущей конфигурацией этих приложений всех клиентов домена. Клиентские приложения по мере необходимости обращаются к конфигурационным сведениям. Это упрощает пользователям настройку приложения и позволяет администратору более эффективно управлять его работой.

Параметры сведений о службе

Публикуемые в каталоге сведения о службе наиболее эффективны, если они:

- **полезны многим клиентам.** Информацию, полезную лишь небольшому кругу пользователей или пользователям отдельных сегментов сети, публиковать не стоит;
- **относительно стабильны и неизменны.** Конечно, бывают и исключения из этого правила, однако в большинстве случаев рекомендуется публиковать сведения, изменяющиеся за три и более интервалов репликации. Для внутрисайтовой репликации максимальный временной интервал составляет 15 минут, а для межсайтовой репликации OF задается в соответствии с интервалом репликации используемой связи сайтов. Репликация часто меняющихся свойств объектов требует дополнительных сетевых ресурсов. Значения свойств остаются неизменными, пока не будут опубликованы обновления. Иногда публикация осуществляется лишь по прошествии максимального времени реплика-

ции. Соответственно, наличие устаревших значений свойств в этот период не должно вызывать проблем. Например, некоторые сетевые службы при каждом запуске выбирают для себя действительный TCP-порт. Далее служба обновляет соответствующую информацию в каталоге Active Directory и сохраняет новые сведения как объект Service Connection Point (SCP). **Если** клиенту необходимо воспользоваться данной службой, он обращается к объекту SCP. Тем не менее, если к этому моменту новый объект SCP не был реплицирован, клиент получит устаревший номер порта, при подключении по которому сообщается о временной недоступности службы;

- **четко определены и обоснованы.** Согласованность представления сведений упрощает их использование службами. Объем информации должен быть относительно небольшим.

Пример публикации службы

▶ **Настройка разрешений безопасности и делегирование управления шаблонами сертификатов**

1. Зарегистрируйтесь в системе как Administrator.
2. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Sites And Services (Active Directory — сайты и службы).
3. В дереве консоли щелкните Active Directory Sites And Services (Active Directory — сайты и службы).
4. В меню View (Вид) выберите команду Show Services Node (Показать узел служб).
5. В дереве консоли раскройте узел Active Directory Sites And Services\Services\Public Key Services и щелкните Certificate Templates.
6. Дважды щелкните каждый шаблон сертификата, для которого требуется настроить разрешения безопасности. Откроется соответствующее окно свойств.
7. В окне свойств шаблона сертификата перейдите на вкладку Security (Безопасность) и задайте необходимые разрешения.
8. Щелкните OK.

Изменения распространяются лишь на шаблоны сертификатов текущего домена.

Резюме

Вы научились публиковать общие папки, принтеры и сетевые службы в Active Directory.

Занятие 4. Перемещение объектов Active Directory

При изменении организационной или административной структуры, например при переходе сотрудника из одного отдела в другой, вам приходится перемещать объекты Active Directory. Сейчас мы расскажем о перемещении объектов Active Directory в пределах домена и между доменами.

Изучив материал этого занятия, вы сможете:

- ✓ перемещать объекты в пределах домена и между доменами;
- ✓ перемешать рабочие станции и рядовые серверы между доменами;
- ✓ перемешать контроллеры домена между сайтами.

Продолжительность занятия — приблизительно 20 минут.

Перемещение объектов

В логической среде объекты службы Active Directory можно перемещать в пределах домена и между доменами. В физической среде разрешается перемещать контроллеры доменов между сайтами.

Перемещение объектов в пределах домена

Для упрощения администрирования объекты домена с идентичными требованиями безопасности можно поместить в единый контейнер или ОП. После этого Вы вправе назначать разрешения этому контейнеру или ОП и всем расположенным в них объектам.

► **Перемещение объектов в пределах домена**

1. В оснастке Active Directory Users and Computers выделите перемещаемый объект и выберите в меню Action команду Move (Переместить).
2. В одноименном окне выберите ОП или контейнер, в который требуется переместить объект, и щелкните OK (рис. 11-6).

Помните, что при перемещении:

- разрешения, назначенные непосредственно объектам, не изменяются;
- объекты наследуют разрешения нового ОП или контейнера. Разрешения старого контейнера или ОП перестают действовать;
- можноработать с несколькими объектами.

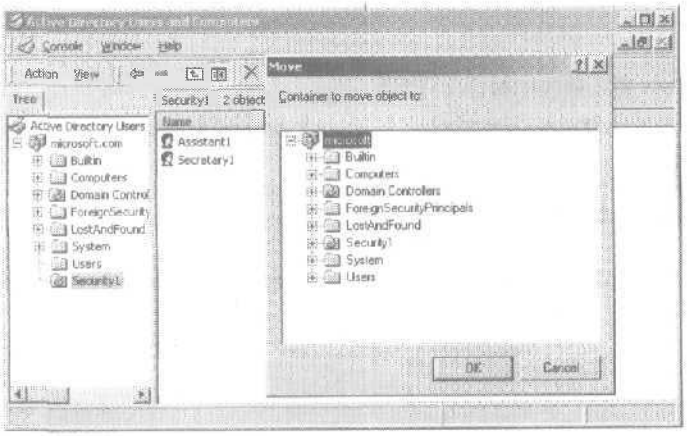


Рис. 11-6. Диалоговое окно Move (Переместить)

Примечание Чтобы упростить назначение разрешений принтерам, переместите принтеры, подключенные к разным серверам печати и требующие одинаковых разрешений, в одно ОП или контейнер. Принтеры сервера печати находятся в объекте Computer. Чтобы просмотреть принтеры, в меню View выберите команду Users, Groups, And Computres As Containers (Пользователи, группы и компьютеры как контейнеры).

Перемещение объектов между доменами

Для поддержки консолидации доменов или отражения изменений в структуре предприятия Windows 2000 позволяет перемещать объекты между доменами. Средствами утилиты командной строки MOVETREE вы сможете с некоторыми исключениями перемещать различные объекты Active Directory, например ОП, учетные записи пользователей и группы, между доменами одного леса. Утилита MOVETREE входит в состав набора утилит Windows 2000 Support Tools, расположенного в папке \SUPPORT\TOOLS компакт-диска Windows 2000. Подробнее об установке Windows 2000 Support Tools — в главе 3.

Процедура перемещения объекта (подчиненного или корневого) подразумевает выделение существующего объекта и перемещение его в существующий корень. Составное имя объекта отражает его новое положение в иерархии. *Глобально уникальный идентификатор* (globally unique identifier, GUID) объекта при перемещении или переименовании не изменяется.

После перемещения из одного домена в другой объектам пользователей и групп присваивается новый *идентификатор безопасности* (security identifier, SID). Для сохранения реквизитов безопасности учетной записи, перемещаемой между доменами, Windows 2000 поддерживает SIDHistory — атрибут безопасности, доступный только в основном режиме Windows 2000. Чтобы упростить изменение *списков управления доступом* (access control list, ACL) и повторное назначение прав доступа к ресурсам при перемещении пользователей и групп из одного домена в другой, прежний SID добавляется к атрибуту SIDHistory нового объекта. При входе пользователя в систему все идентификаторы безопасности из его *журнала SID* (SID history), а также все идентификаторы из журнала SID его группы добавляются к маркеру доступа, и пользователю назначаются все ранее имевшиеся у него разрешения и права собственности на ресурсы.

Утилита MOVETREE позволяет переместить ОП в другой домен, не затрагивая при этом связанные объекты групповой политики (group policy object, GPO) старого домена. Ссылка на прежний GPO также перемещается и продолжает работать, и клиенты получают параметры групповой политики от объектов GPO в старом домене. Подробнее о групповой политике — в главе 12.

Операции, поддерживаемые утилитой MOVETREE

- Перемещение объекта или непустого контейнера в другой домен в пределах одного леса.
- Перемещение локальных и глобальных групп домена *между* доменами без перемещения их членов и *в пределах* домена с перемещением членов; возможно лишь в пределах одного леса.
- Перемещение универсальных групп со всеми членами *в пределах* и *между* доменами одного леса.

Операции, не поддерживаемые утилитой MOVETREE

Некоторые объекты и сведения не перемещаются. Такие объекты называются *потерянными* (orphaned) и помещаются в соответствующий подконтейнер контейнера LostAndFound исходного домена. Чтобы увидеть данный контейнер, включите в меню View оснастки Active Directory Users and Computers отображение дополнительных сведений. Имя контейнера для потерянных объектов соответствует GUID перемещаемого родительского контейнера, последний содержит объекты, перемещенные с помощью MOVETREE. В частности, MOVETREE не способна перемещать:

- локальные и глобальные группы домена. Универсальные группы перемещаются вместе со всеми членами, и поэтому проблем с системой безопасности не возникает;
- сведения о членстве в домене для объектов Computer. Утилита MOVETREE способна переместить объект Computer из одного домена в другой вместе с подчиненными объектами. Тем не менее MOVETREE не отключает компьютер от исходного и не делает его членом конечного домена. В связи с этим для перемещения объектов Computer рекомендуется использовать утилиту NETDOM;
- данные, связанные с объектом, в том числе групповые политики, профили пользователей, сценарии входа в систему, личные данные пользователей, зашифрованные файлы, смарт-карты и сертификаты открытого ключа. Групповые политики должны распространяться на пользователей, группы и компьютеры. Обязательное условие, чтобы новые смарт-карты и сертификаты были выданы центром сертификации в новом домене. Для этого утилиту MOVETREE рекомендуется использовать совместно с дополнительными сценариями или административными утилитами, например с Remote Administration Scipts;
- системные объекты — объекты, атрибут objectClass которых помечен как systemOnly;
- объекты в контекстах конфигурации и схем именования;
- объекты из специальных контейнеров домена (Builtin, ForeignSecurityPrincipals и LostAndFound);
- контроллеры домена, а также их прямых потомков;
- объекты с именами, идентичными имеющимся в конечном домене.

Ниже описываются ситуации, вызывающие сбои в работе MOVETREE:

- контроллер исходного домена не может перенести владельца роли хозяина относительных идентификаторов;
- исходный объект заблокирован другой операцией. Например, пользователь в текущий момент создает дочерние объекты для перемещаемого объекта;
- реквизиты исходного или конечного домена неверны;
- в отличие от исходного домена, конечный домен знает, что исходный объект удален, Например, исходный объект был удален на контроллере другого домена, однако из-за задержек в репликации контроллер исходного домена еще не извещен об этом;
- сбой на контроллере конечного домена. Например, диск заполнен;
- не совпадают схемы на исходном и конечном доменах.

Перемещение объектов пользователей

Помните, что перемещение не выполняется:

- если объект User содержит какие-либо вложенные объекты. Данный объект не должен иметь потомков;
- если не соблюдены ограничения, накладываемые диспетчером *учетных записей безопасности* (security accounts manager, SAM). Например, *samAccountName* пользователя уже существует в конечном домене или длина пароля пользователя не соответствует требованиям конечного домена;

- объект User является членом глобальной группы исходного домена. При этом также аннулируется членство пользователя в группе. Настоящее ограничение вызвано тем, что глобальная группа не может включать членов из других доменов.

Тем не менее существует и одно исключение: если пользователь состоит в группе Domain Users (не являясь одновременно членом других глобальных групп) и та входит в основную группу объекта User, перемещение выполняется. Это связано с тем, что при создании объекта User система автоматически помещает его в группу Domain Users и назначает ее основной группой для данного пользователя.

Перемещение групп

Помните, что перемещение не выполняется, если:

- объект Group содержит вложенные объекты;
- прямое и обратное членство группы не соответствуют требованиям к ее типу;
- идентичный атрибут *samAccountName* группы уже существует в конечном домене.

Перемещение объектов между доменами с помощью утилиты MOVETREE

Прежде чем воспользоваться утилитой MOVETREE, убедитесь, что вы обладаете всеми необходимыми разрешениями. Например, проверьте, есть ли у вас права на создание объектов в исходном и конечном доменах. С утилитой MOVETREE можно работать из командной строки; кроме того, ее разрешается вызывать в пакетных файлах для разработки сценариев создания учетных записей пользователей и групп.

▶ **Перемещение объектов между доменами с помощью MOVETREE**

1. Откройте сеанс MS-DOS и наберите в командной строке **movetree {/start | /startnocheck | /continue | /check} /s *SrcDSA* /d *DstDSA* /sdn *SrcDN* /ddn *DstDN* [/u [*Domain*\]*Username* /p *Password*] [/verbose] [{/? [/help}]**

   Используемые параметры:

- **/start** — запускает операцию перемещения. По умолчанию также используется параметр /check. Чтобы выполнить перемещение объекта без проверки, запустите MOVETREE с параметром /startnocheck;
- **/continue** — продолжает выполнение ранее приостановленной или отказавшей операции MOVETREE;
- **/check** — тестирует операцию MOVETREE (проверяет дерево без перемещения каких-либо объектов);
- /s *SrcDSA* — полное основное DNS-имя исходного сервера;
- **/s *DstDSA*** — полное основное DNS-имя конечного сервера;
- **/snd *SrcDN*** — составное имя объекта, контейнера или поддерева, перемещаемого из исходного домена;
- **/snd *DstDN*** — составное имя объекта, контейнера или поддерева, перемещаемого в конечный домен;
- **/u [*Domain*\]*Username* /p *Password*** — запускает утилиту MOVETREE с переданными именем пользователя *(Username)* и паролем (*Password*). Также можно указать домен (*Domain*). Если эти аргументы не заданы, MOVETREE работает с реквизитами текущего пользователя;
- **/verbose** — запускает MOVETREE в режиме вывода информации о выполняемой операции (необязательный параметр);
- **/? или /help** — выводит справку по синтаксису.

Пример использования команды MOVETREE

В домене Marketing имеется сервер Server1 и ОП Promotions. В домене Sales существует сервер Server2. Вам необходимо переместить ОП Promotions из домена Marketing в домен Sales и переименовать его в Sales Promotions. Утилита MOVETREE выполняет предварительную проверку и при отсутствии ошибок выполняет требуемую операцию:

```
movetree /start /s Server1.Marketing.Reskit.Com /d Server2.Sales.Reskit.cor /
sdn OU=Promotions,DC=Marketing,DC=Reskit,DC=Com /ddn OU=Sales -
Promotions,DC=Sales.DC=Reskit,DC=Com
```

Файлы журнала MOVETREE

При работе MOVETREE в папке, где выполнялась операция, создаются следующие файлы журнала:

- **MOVETREE.ERR** — содержит сведения обо всех ошибках в процессе перемещения;
- **MOVETREE.LOG** — содержит статистические данные о результатах перемещения;
- **MOVETREE.CHK** — содержит сведения обо всех ошибках и конфликтах, выявленных в ходе предварительной проверки.

Перемещение рабочих станций и рядовых серверов между доменами

Для перемещения рабочих станций и рядовых серверов между доменами можно воспользоваться приложением NETDOM: Windows 2000 Domain Manager. NETDOM входит в состав комплекта утилит Windows 2000 Support Tools, записанного в папке \SUPPORT\TOOLS компакт-диска Windows 2000. Подробнее об установке Windows 2000 Support Tools — в главе 3.

▶ **Перемещение рабочих станций и рядовых серверов между доменами**

1. Откройте сеанс MS-DOS и наберите в командной строке **netdom move /D:*domain* [/OU:*ou_path*] [/Ud:*User* /Pd:{*Password*|*}] [/Uo:*User* /Po:{Password|*}] [/Reboot:[*time_in_seconds*]]**

   Используемые параметры:

- */domain* — имя домена, в который перемещается рабочая станция или рядовой сервер;
- **/OU:*ou_path*** — имя конечного ОП в новом домене (/D:domain);
- **/Ud:*User*** — учетная запись пользователя для подключения к домену, указываемому в параметре /D. Если данный параметр не задан, применяется учетная запись текущего пользователя;
- **/Pd:{*password*|*}** — пароль пользователя, чья учетная запись указана в параметре /Ud. Если указана звездочка (*), вам будет предложено ввести пароль;
- **/Uo:*User*** — учетная запись пользователя для подключения к перемещаемому объекту. Если данный параметр не задан, применяется учетная запись текущего пользователя;
- **/Pd:{*password*|*}** — пароль пользователя, чья учетная запись указана в параметре /Uo. Если указана звездочка (*), вам будет предложено ввести пароль;
- **/Reboot:[*time_in_seconds*]** — интервал времени в секундах, по истечении которого перемещаемый компьютер после завершения операции перезагрузится. По умолчанию — 20 секунд.

Пример использования команды NETDOM

Следующая команда перемещает рабочую станцию mywksta из текущего домена в домен mydomain.

```
netdom move /d:mydomain mywksta /ud:mydomain\admin /pd:password
```

Если конечный домен является доменом Windows 2000, журнал SID рабочей станции обновляется, и за учетной записью компьютера сохраняются все старые разрешения.

Перемещение контроллеров домена между сайтами

В большинстве случаев контроллер домена устанавливается в дополнение к имеющимся в сайте контроллерам. Исключением является ситуация, когда вы устанавливаете первый контроллер домена; при этом автоматически создается сайт с именем Default-First-Site-Name. Первый контроллер домена нельзя создать в каком-либо сайте, кроме Default-First-Site-Name; тем не менее вы вправе создать контроллер домена в сайте с имеющимися контроллерами и затем переместить его в другой сайт. Таким образом, после установки первого контроллера домена и создания сайта Default-First-Site-Name разрешается создавать дополнительные контроллеры и перемещать их в другие сайты.

Аналогичную процедуру используют и для перемещения рядовых серверов между доменами.

▶ **Перемещение контроллеров домена между сайтами**

1. В оснастке Active Directory Sites and Services выделите требуемый контроллер домена и в меню Action выберите команду Move (Переместить).
2. В диалоговом окне Move Server (Перемещение сервера) выберите сайт, куда требуется переместить контроллер, и щелкните OK (рис. 11-7).

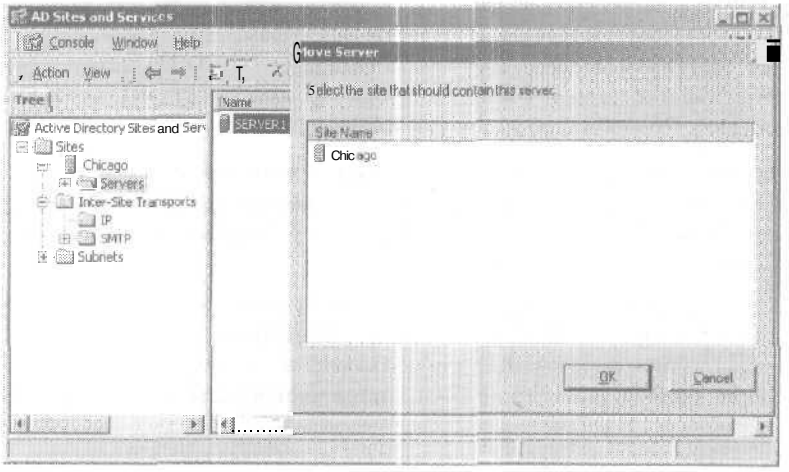


Рис. 11-7. Диалоговое окно Move Server (Перемещение сервера)

Практикум: перемещение объектов в пределах домена

Вы переместите три учетных записи пользователей из одного ОП в другое и затем попытаетесь зарегистрироваться в системе под новой учетной записью.

▶ **Задание 1: переместите объекты в пределах домена**

1. Зарегистрируйтесь в системе как Administrator и запустите оснастку Active Directory Users and Computers.
2. В дереве консоли щелкните узел Users.
3. Выделите учетные записи User20, User21, User22, созданные вами на занятии 1. Для этого удерживайте клавишу Ctrl и поочередно щелкните все три записи.

4. В меню Action выберите команду Move (Переместить).
5. В одноименном окне раскройте узел своего домена, выделите Securityl (ОП, созданное на занятии 2) и щелкните OK.

   Заметьте, что перемещенные учетные записи больше не отображаются в контейнере Users.
6. Убедитесь, что учетные записи перемешены, раскрыв в дереве консоли узел Securityl.

   Заметьте, что учетные записи теперь находятся в ОП Securityl.
7. Закройте окно оснастки Active Directory Users and Computers.

► **Задание 2: зарегистрируйтесь в системе как пользователь, состоящий в нестандартном ОП**

1. Зарегистрируйтесь в системе как User21.

   Потребовала ли Windows 2000 указать ОП, к которому относится данная учетная запись? Почему?
2. Завершите рабочий сеанс.

Резюме

Вы научились перемешать объекты в пределах доменов службы Active Directory с помощью диалогового окна Move, объекты между доменами средствами утилиты командной сфоки MOVETREE, а также рабочие станции и рядовые серверы между доменами с применением утилиты NETDOM. Кроме того, вы узнали, как перемещать контроллеры домена между сайтами с помощью диалогового окна Move Server.

Выполняя практикум, вы переместили объект домена, воспользовавшись диалоговым окном Move оснастки Active Directory Users and Computers, из одного контейнера в другой.

Занятие 5. Делегирование управления объектами Active Directory

Здесь рассказано о делегировании управления объектами пользователям. Вы научитесь работать с мастером Delegation Of Control, а также изучите рекомендации по делегированиюуправления.

Изучив материал этого занятия, вы сможете:

✓ делегировать управление ОП и объектами.

Продолжительность занятия — около 20 минут.

Рекомендации по делегированию управления

Для делегирования управления объектом вы назначаете ему разрешения, позволяющие пользователям и группам администрировать это объект. Администратор вправе назначить пользователю разрешение на:

- изменение свойств определенного контейнера;
- создание, изменение или удаление объектов определенного типа в конкретном ОП или контейнере;
- изменение определенныхсвойств объектов заданного типа в специальном ОП или контейнере.

Поскольку контролировать разрешения на уровне ОП или контейнера проще, чем на уровне объектов или их атрибутов, наиболее распространенный метод делегирования управления — назначение разрешений на уровне ОП или контейнера. Это позволит вам делегировать управление объектами, содержащимися в ОП или в контейнере. Для назначения разрешений на уровне ОП или контейнера применяется мастер Delegation Of Control.

Например, для делегирования управления можно назначить администратору разрешение Full Control для ОП, причем только в пределах его ответственности. Делегируя управление ОП администраторам, вы децентрализуете администрирование, что помогает снизить связанные с ним затраты времени и денег.

Для делегирования управления рекомендуется:

- при каждой возможности назначать управление на уровне ОП или контейнера — это упрощает контроль разрешений. Контроль разрешений для объектов и их атрибутов сложен;
- использовать мастер Delegation Of Control, назначающий разрешения исключительно на уровне ОП или контейнера. Его применение упростит процесс назначения разрешений для объектов;
- контролировать делегирование назначений разрешений. Это позволит вести журнал, в котором можно быстро выяснить параметры безопасности;
- придерживаться бизнес-требований. Следуйте всем существующим в компании правилам делегирования управления.

Мастер Delegation Of Control

Мастер Delegation Of Control (Мастер делегирования управления) шаг за шагом проведет вас через все этапы назначения разрешений на уровне ОП или контейнера. Более сложные разрешения придется назначать вручную.

В окне Active Directory Users and Computers щелкните ОП или контейнер, для которого требуется делегировать управление, и выберите в меню Action команду Delegate Control (Делегирование управления). Запустится мастер Delegation Of Control, параметры которого описаны в табл. 11-7.

Табл. 11-7. Параметры мастера Delegation Of Control

Параметр	Назначение
Users Or Groups (Пользователи или группы)	Позволяет выбрать учетные записи или группы, которым требуется делегировать управление
Tasks To Delegate (Делегируемые задачи)	Позволяет выбрать обычные задачи из списка или создать собственные делегируемые задачи
Active Directory Object Type (Тип объекта Active Directory) (параметр доступен, только если выбраны конкретные делегируемые задачи)	Позволяет выбрать область действия делегируемых задач: This Folder, Existing Objects In This Folder, And Creation Of New Objects In This Folder (Этой папкой и существующими в ней объектами, созданием новых объектов в новой папке) или Only The Following Objects In This Folder (Только следующими объектами в этой папке)
Permissions (Разрешения) (параметр доступен, только если выбраны конкретные делегируемые задачи)	Позволяет выбрать одно из следующих разрешений для делегирования: General (Общие) — обычно назначаемые разрешения, доступные для данного объекта; Property-Specific (Разрешения для свойств) — разрешения, которые можно назначить атрибутам объекта; Creation/Deletion Of Specific Child Objects (Разрешения для создания или удаления дочерних объектов) — разрешения для создания и удаления дочерних объектов

Рекомендации по администрированию Active Directory

- В больших организациях координируйте структуру Active Directory с другими администраторами. Вы можете переместить объекты и позже, однако это, скорее всего, приведет к лишней работе.
- При создании объектов Active Directory (учетных записей пользователей и т. п.) укажите все значимые для вашей организации атрибуты. Это значительно расширит возможности поиска объектов.
- Избегайте блокировать разрешения. Если разрешения назначены правильно, блокировать их не придется. В большинстве случаев необходимость блокирования разрешений указывает на ошибки распределения пользователей по группам.
- Убедитесь, что для каждого объекта определен хотя бы один пользователь с разрешением Full Control (Полный доступ). Иначе могут появиться недоступные объекты.
- Убедитесь, что пользователи, которым делегировано управление,— ответственные люди и на них можно положиться. Вы, как администратор, в конечном счете, несете ответственность за все административные изменения. Если пользователи, которым делегировано управление, не выполняют административных задач, вам придется исправлять их ошибки.
- Обеспечьте обучение пользователей, управляющих объектами. Добейтесь, чтобы пользователи, которым делегирована ответственность, понимали свои обязанности и знали, как выполнять задачи администрирования.

Практикум: делегирование управления в Active Directory

Сейчас вы попробуете делегировать пользователю управление объектами, содержащимися в ОП. Для ответов на вопросы данного упражнения обратитесь к таблицам, заполненным на занятии 2.

▶ Задание 1: проверьте текущие разрешения

1. Зарегистрируйтесь в домене, используя учетную запись Assistant1 и пароль password.
2. Откройте консоль Active Directory Users and Computers.
3. В дереве консоли раскройте свой домен и щелкните Security1.

   Какие объекты-пользователи отображаются в ОП Securityl?

   Какие разрешения позволяют вам видеть эти объекты? (Совет: см. таблицы, заполненные вами на занятии 2.)

   Для учетной записи Secretary1 измените время входа в систему. Удалось ли вам это? Почему?

   Измените время входа в систему для учетной записи Assistant1. Удалось ли вам это? Почему?
4. Закройте консоль Active Directory Users and Computers и завершите рабочий сеанс.

▶ Задание 2: назначьте разрешения Active Directory с помощью мастера Delegation Of Control

1. Зарегистрируйтесь в домене как Administrator и откройте консоль Active Directory Users and Computers.
2. В дереве консоли разверните свой домен.
3. Щелкните Securityl и выберите в меню Action команду Delegate Control (Делегирование управления).
4. В окне мастера Delegation Of Control щелкните Next.

   Откроется окно Users Or Groups (Пользователи или группы).

   Обратите внимание, что мастер не отображает какие-либо учетные записи или группы. Вы добавите учетную запись и затем делегируете ей управление.
5. Щелкните кнопку Add.

   Откроется диалоговое окно Select Users, Computers, Or Groups.
6. Выберите Assistant1, щелкните кнопку Add и затем — OK.
7. Щелкните Next.

   Откроется окно Tasks To Delegate (Делегируемые задачи). Здесь можно выбрать для делегирования обычные задачи или создать собственную.
8. Убедитесь, что выбран переключатель Delegate The Following Common Tasks (Делегировать следующие обычные задачи) (это необходимо только для данного упражнения), пометьте флажок Create, Delete, And Manage User Accounts (Создание, удаление и управление учетными записями пользователей) и щелкните Next.

   Откроется окно Completing The Delegation Of Control Wizard (Завершение работы мастера делегирования управления).
9. Изучите данные.
   - Если все параметры указывают, что пользователюAssistant1 делегировано управление всеми объектами, щелкните кнопку Finish (Готово).
   - Для изменения параметров щелкните Back (Назад).
10. Закройте консоль Active Directory Users and Computers и завершите рабочий сеанс.

Задание 3: проверьте делегированные разрешения

1. Зарегистрируйтесь в домене как Assistant1 с паролем password.
2. Откройте консоль Active Directory Users and Computers.
3. В дереве консоли раскройте свой домен и щелкните Security1.
4. Попытайтесь изменить время входа в систему для учетных записей из ОП Security1. Удалось ли вам это? Почему?
5. Попытайтесь изменить время входа в систему для учетной записи из контейнера Users. Удалось ли вам это? Почему?

Резюме

Вы можете делегировать административный контроль над объектами пользователям, чтобы разрешить им выполнение административных задач.

Назначение разрешений на уровне ОП или контейнера позволяет делегировать администрирование над содержащимися в ОП или в контейнере объектами. Вы научились использовать мастер Delegation Of Control для делегирования управления объектами. Также вы изучили рекомендации по делегированию контроля. Выполняя практикум, вы использовали мастер Delegation Of Control для делегирования пользователю контроля над объектами в ОП.

Занятие 6, Резервное копирование Active Directory

Это занятие посвящено резервному копированию данных. Для архивации необходимо выполнить некоторые подготовительные операции, а затем воспользоваться мастером Backup. На этом занятии вы также научитесь планировать и применять автоматическое резервное копирование.

Изучив материал этого занятия, вы сможете:

- ✓ создать резервную копию Active Directory на локальном компьютере;
- ✓ спланировать резервное копирование Active Directory.

Продолжительность занятия — около 20 минут.

Подготовительные операции

Важная часть резервного копирования Active Directory — выполнение подготовительных операций. Например, следует проверить, закрыты ли файлы, которые вы собираетесь архивировать. Прежде чем начать резервное копирование, отправьте пользователям сообщение с просьбой закрыть файлы. Сеансы приложений, запущенных системами или пользователями, известить которых не представляется возможным (например, пользователь подключился через Интернет), будут завершены, Windows Backup не архивирует файлы, заблокированные приложениями. Для рассылки административных сообщений стоит воспользоваться электронной почтой или диалоговым окном Send Console Message (Отправка сообщения консоли); последнее доступно в оснастках Computer Management (Управление компьютером), Services (Службы) и Shared Folders (Общие папки).

При использовании съемных носителей убедитесь, что:

- устройство резервного копирования подсоединено к компьютеру сети и включено. При архивировании на ленту ленточный накопитель следует подключить к системе, на которой запущено приложение Windows Backup;
- соответствующее устройство перечислено в списке совместимых с Windows 2000 устройств (Hardware Compatibility List, HCL);
- носитель вставлен в устройство. Например, кассета магнитной ленты — в ленточный накопитель.

Мастер архивации

Завершив подготовительные операции, можно архивировать Active Directory с помощью мастера Backup.

▶ **Запуск мастера архивации**

1. Зарегистрируйтесь в домене как Administrator. Раскройте меню Start\Programs\Accessories\System Tools (Пуск\Программы\Стандартные\Служебные) и щелкните Backup (Архивация данных).
2. Щелкните кнопку Backup (Мастер архивации) на вкладке Welcome (Добро пожаловать).
3. Щелкните Next, чтобы начать работу с мастером. Укажите требуемые параметры в окнах What To Back Up (Что следует архивировать), Where To Store The Backup (Где хранить архив) и при необходимости задайте дополнительные параметры архивации.
4. В окне Completing The Backup Wizard (Завершение работы мастера архивации) щелкните кнопку Finish (Готово).

Окно What to Back Up

Первое, что надо сделать, начав резервное копирование Active Directory с помощью мастера архивации, — указать, что вы собираетесь архивировать лишь данные состояния системы (System State) (рис. 11-8).

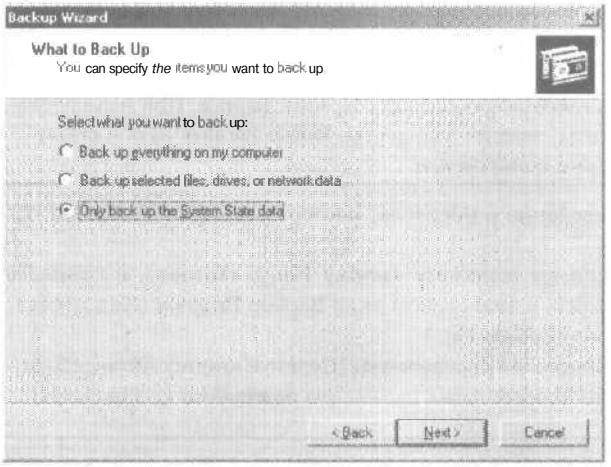


Рис. 11-8. Окно What To Back Up (Что следует архивировать) мастера архивации

В серверных ОС Windows 2000 данные о состоянии системы включают реестр, базу данных регистрации классов COM+, системные загрузочные файлы и базу данных служб сертификации (если это сервер сертификации), Если сервер — контроллер домена, данные о состоянии системы также содержат Active Directory и каталог SYSVOL. Архивирование или восстановление данных о состоянии системы касается всего локального компьютера; нельзя выполнить эти операции только для отдельных данных, так как они взаимосвязаны. Разрешено архивировать данные о состоянии только локальной, но не удаленной системы,

Окно Where to Store the Backup

Сейчас мы расскажем о носителях для резервного копирования (рис. 11-9).

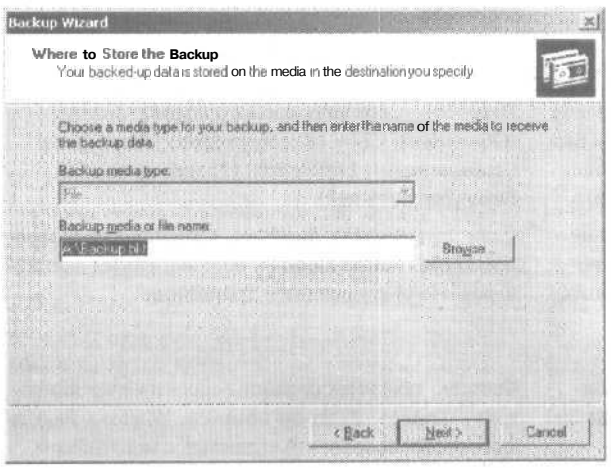


Рис. 11-9, Окно Where To Store The Backup (Где хранить архив) мастера архивации

В табл. 11-8 описаны параметры носителя, которые следует указать.

Табл. 11-8. Параметры носителя для резервного копирования

Параметр	Описание
Backup Media Type (Тип носителя архива)	Используемый носитель (например, лента или файл). Файл может находиться на любом дисковом носителе, включая жесткий диск, общую сетевую папку или съемный диск
Backup Media Or File Name (Носитель архива или имя файла)	Место, где Windows Backup сохранит данные. При использовании ленты введите имя ленты. Иначе введите путь к файлу резервного копирования

После того как вы предоставите сведения о носителе, мастер архивации отобразит отчет о параметрах и предложит:

- **начать резервное копирование.** Если вы щелкнете кнопку Finish (Готово), в процессе архивирования мастер будет выводить в диалоговом окне Backup Progress (Ход архивации) сведения о ходе резервного копирования;
- **задать дополнительные параметры резервного копирования.** Щелкнув кнопку Advanced (Дополнительно), вы сможете задать дополнительные параметры резервного копирования.

Примечание По завершении архивирования вы можете просмотреть отчет — файл журнала резервного копирования. Это хранимый на жестком диске текстовый файл, в который заносятся сведения о резервном копировании.

Задание дополнительных параметров резервного копирования

Настраивая дополнительные параметры резервного копирования, вы изменяете стандартные параметры только для текущего задания копирования. Дополнительные параметры описаны в табл. 11-9.

Табл. 11-9. Дополнительные параметры резервного копирования

Страница дополнительных параметров	Дополнительный параметр	Описание
Type **Of Backup** (Тип архива)	Select The Type Of Backup Operation To Perform (Выберите нужный тип операции архивирования)	Перечень типов создаваемого архива: Normal (Обычный), Copy (Копирующий), Incremental (Добавочный), Differential (Разностный) или Daily (Ежедневный)
	Backup Migrated Remote Storage Data (Архивировать данные из внешних хранилищ)	Если этот флажок помечен, выполняется резервное копирование данных, перемещенных диспетчером HSM в удаленное хранилище
How To Backup (Способы архивации)	Verify Data After Backup (Проверить данные после архивации)	Флажок, подтверждающий корректное архивирование файлов. Если он помечен, Windows Backup сравнивает сохраненные данные с источником, проверяя их идентичность. *Microsoft рекомендует помечать этот флажок*

Табл. 11-9. Дополнительные параметры резервного копирования *(продолжение)*

Страница дополнительных параметров	Дополнительный параметр	Описание
	Use Hardware Compression, If Available (Использовать аппаратное сжатие, если возможно)	Флажок, включающий поддержку аппаратного сжатия для ленточных накопителей. Если ваше устройство не поддерживает аппаратное сжатие, флажок недоступен
Media Options (Параметры носителей)	If The Archive Media Already Contains Backups (Если носитель уже содержит архивы)	Параметр, определяющий, будет ли хранимая на носителе резервная копия дополнена или перезаписана. Выберите Append This Backup To Media (Дозаписьтвать этот архив к данным носителя), чтобы хранить множество резервных копий. Выберите Replace The Data On The Media With This Backup (Затереть данные носителя этим архивом), если вам не нужны устаревшие резервные копии и вы хотите сохранить только самую новую резервную копию
	Allow Only The Owner And The Administrator Access To The Backup Data And To Any Backups Appended To This Media (Разрешать доступ к данным этого архива и всем дозаписываемым на этот носитель архивам только владельцу и администратору)	Флажок, ограничивающий круг лиц, обладающих доступом к файлу или ленте с резервной копией. Флажок доступен только при перезаписи существующих резервных копий. Пометьте этот флажок при резервном копировании реестра или Active Directory, чтобы предотвратить несанкционированное получение копий сохраненных данных
Backup Label (Метка архива)	Backup Label (Метка архива)	Поле, в котором можно указать имя и описание операции резервного копирования. Имя и описание появятся в регистрационном файле сохранения. Содержание по умолчанию: Set Created *Дата* At *Время*. Вы можете изменить *имя* и описание на более понятные (например Active Directory backup 09-12-00)
	Media Label (Метка носителя)	Поле, в котором указывают имя носителя резервной копии (например, имя ленты). Имя по умолчанию: Media Created *Дата* At *Время*. Если резервное копирование на новый носитель осуществляется впервые или вы перезаписываете имеющийся архив, можно указать имя носителя, например Active Directory
When To Back Up (Когда архивировать)	When To Back Up (Когда архивировать)	Допустимые значения этого параметра: Now (Сейчас) и Later (Позже). Если вы выбрали Later, укажите имя и дату начала выполнения задания резервного копирования. Кроме: того, можно задать расписание архивирования

Табл. 11-9. Дополнительные параметры резервного копирования *(окончание)*

Страница дополнительных параметров	Дополнительный параметр	Описание
	Job Name (Имя задания)	Имя задания резервного копирования
	Start Date (Дата запуска)	Дата запуска задания резервного копирования
	Set Schedule (Установить расписание)	Кнопка для настройки расписания резервного копирования

В зависимости от выбранного вами времени запуска задания резервного копирования (сейчас или позже) мастер архивации:

- отображает параметры и предлагает немедленно начать архивирование. В процессе резервного копирования будут выводиться сведения о ходе выполнения задания;
- открывает дополнительные диалоговые окна для настройки расписания резервного копирования. Подробности см. в разделе ниже.

Настройка расписания резервного копирования Active Directory

Позволяет автоматически проводить архивирование файлов в периоды низкой нагрузки на систему. Кроме того, задания резервного копирования Active Directory можно настроить для выполнения через регулярные интервалы времени, Для этого Windows 2000 интегрирует приложение Windows Backup со службой Task Scheduler (Планировщик заданий).

▶ **Настройка расписания резервного копирования**

1. В окне мастера архивации When To Back Up (Когда архивировать) щелкните кнопку Later (Позже).

   Служба Task Scheduler открывает диалоговое окно Set Account Information (Указание учетной записи), запрашивая пароль. Для выполнения задания резервного копирования учетная запись должна обладать соответствующими полномочиями.

   Примечание Если служба Task Scheduler не выполняется или не настроена для автоматического запуска, Windows 2000 открывает диалоговое окно с предложением запустить эту службу. Щелкните OK. Откроется диалоговое окно Set Account Information.

2. Введите в полях Password (Пароль) и Confirm Password (Подтверждение) свой пароль и щелкните OK.

   Откроется окно When To Back Up, где необходимо указать имя задания резервного копирования. По умолчанию мастер в качестве даты и времени запуска назначает текущие дату и время.

3. Введите в поле Job Name (Имя задания) имя задания.
4. Щелкните кнопку Set Schedule (Установить расписание), чтобы задать другие начальные дату и время запуска. Служба Task Scheduler откроет диалоговое окно Schedule Job (Запланированное задание).

   Например, настройте задание для выполнения в 22:00 по пятницам. Кроме того, можно отобразить все задания, назначенные для данного компьютера, пометив флажок Show Multiple Schedules (Показывать несколько расписаний). Так вы предотвратите назначение на одно и то же время нескольких задач.

Щелкнув кнопку Advanced (Дополнительно), вы можете указать, как долго должно продолжаться резервное копирование и какой период времени будет действовать расписание.

После того как вы назначите задание резервного копирования и завершите работу с мастером архивации, приложение Windows Backup поместит созданное задание в календарь на вкладке Schedule Jobs (*Запланированные* задания) своего окна. Резервное копирование будет автоматически начато в указанное вами время.

Резюме

Теперь вы знаете, что следует проверить, закрыты ли файлы, резервные копии которых вы собираетесь создать, поскольку Windows Backup не архивирует файлы, заблокированные приложениями. Вы также узнали, что первый этап резервного копирования с помощью мастера архивации — выбор архивируемых объектов. Для резервного копирования Active Directory необходимо указать, что вы собираетесь архивировать данные о состоянии системы. После этого надо выбрать устройство резервного копирования и указать имя носителя или файла. Затем можно задать дополнительные параметры или начать архивирование. Используя службу Task Scheduler, Windows Backup позволяет создавать расписания запусков заданий резервного копирования.

Занятие 7. Восстановление Active Directory

Существует два способа восстановления Active Directory: *принудительное* (authoritative) и *непринудительное* (nonauthoritative). На этом занятии вы научитесь восстанавливать Active Directory.

Изучив материал этого занятия, вы сможете:

- ✓ объяснить различие между принудительным и непринудительным восстановлением;
- ✓ восстановить Active Directory.

Продолжительность занятия — около 25 минут.

Подготовка к восстановлению Active Directory

Как и в процессе резервного копирования, когда вы восстанавливаете Active Directory, разрешается восстановить только все данные о состоянии системы, которые были скопированы, включая системный реестр, базу данных регистрации классов COM+, каталог SYSVOL, Active Directory и базу данных служб сертификации (если это сервер сертификации). Вы не можете восстановить отдельные компоненты системы (например, только Active Directory).

Если вы восстанавливаете данные о состоянии системы на контроллере домена, следует выбрать между принудительным и непринудительным восстановлением. По умолчанию на контроллере домена выполняется непринудительное восстановление системы.

Непринудительное восстановление

Любой компонент состояния системы, реплицируемый другим контроллером домена, типа службы каталогов Active Directory, обновляется репликацией после того, как вы восстановите данные. Например, если последняя резервная копия сделана неделю назад и система восстановлена непринудительно, любые изменения, выполненные после резервного копирования, будут реплицированы с других контроллеров домена. Система репликации Active Directory обновит восстановленные данные, воспользовавшись более новыми данными с других ваших серверов.

Принудительное восстановление

Если вы не хотите реплицировать изменения, сделанные после последнего архивирования, используйте принудительное восстановление. Например, именно этим способом следует воспользоваться, если вы по неосторожности удалили учетные записи пользователей, группы или ОП из Active Directory и хотите восстановить систему так, чтобы удаленные объекты были перезаписаны и реплицированы.

Для принудительного восстановления данных Active Directory необходимо после восстановления данных о состоянии системы (но до перезагрузки сервера) запустить служебную программу Ntdsutil. Она позволяет отметить объекты Active Directory для принудительного восстановления. Если объект отмечен для принудительного восстановления, его *порядковый номер обновления* (update sequence number, USN) меняется и становится больше всех остальных номеров последовательного обновления в системе репликации Active Directory. Это гарантирует, что все реплицируемые или распространяемые восстанавливаемые данные будут реплицированы правильно или распространены внутри данной орга-

низации. Утилита NTDSUTIL расположена в папке *systemroot*\system32, а соответствующая документация — в справочной системе Windows 2000 (доступна из меню Start).

Предположим, вы заархивировали систему в понедельник, а затем во вторник создали учетную запись нового пользователя с именем Максим, сведения о котором были реплицированы на другие контроллеры домена. В среду вы случайно удалили учетную запись другого пользователя — Алексея. Чтобы полномочно восстановить учетную запись Алексея без повторного ввода информации, можно непринудительно восстановить контроллер домена из архива, созданного в понедельник. Далее, используя NTDSUTIL, надо пометить учетную запись Алексея для принудительного восстановления. В результате учетная запись Алексея будет восстановлена, никоим образом не затронув учетную запись Максима.

Выполнение непринудительного восстановления

Для восстановления данных о состоянии системы контроллера домена необходимо запустить компьютер в специальном безопасном режиме — режиме восстановления службы каталогов. Это позволит восстановить каталог SYSVOL и базу данных службы каталогов Active Directory. Разрешается восстановить состояние системы только на локальном компьютере. Вы не можете выполнить эту операцию на удаленном компьютере.

Примечание Если при восстановлении состояния системы вы не определили альтернативного места для восстановленных данных, резервная копия сотрет сведения о текущем состоянии системы и заменит их данными о восстановленном состоянии системы. Если же вы восстанавливаете состояние системы в другое место, в него восстанавливаются только файлы системного реестра, файлы каталога SYSVOL и системные загрузочные файлы, Базы данных службы каталогов Active Directory, службы сертификации и регистрации классов COM+ в таком случае не восстанавливаются.

▶ **Непринудительное восстановление Active Directory**

1. Перезагрузите компьютер.
2. На стадии загрузки, когда обычно выбирается операционная система, нажмите F8.
3. В меню загрузки Windows 2000 выберите режим восстановления службы каталогов и нажмите Enter. В результате контроллер домена будет изолирован от сети.
4. Выберите для запуска Microsoft Windows 2000 Server и нажмите Enter.
5. Зарегистрируйтесь в системе как Administrator (Администратор).
6. Появится сообщение, что Windows работает в безопасном режиме. Щелкните OK.

Примечание Перезагружая компьютер в режиме восстановления службы каталогов, вы должны войти как Administrator, используя соответствующие учетную запись SAM и пароль, а не имя и пароль администратора Active Directory. Это вызвано тем, что служба Active Directory автономна и проверка учетной записи невозможна. Вместо этого для управления доступом к Active Directory применяется база данных учетных записей SAM. Настройка пароля SAM выполнялась при установке Active Directory.

---

7. Раскройте меню Start\Programs\Accessories\System Tools (Пуск\Программы\Стандартные\Служебные) и щелкните Backup (Архивация данных).
8. В окне утилиты Backup щелкните кнопку Restore Wizard (Мастер восстановления).
9. Щелкните Next.
10. В окне What To Restore (Что следует восстановить) раскройте узел типа носителя, содержащий данные, которые вы хотите восстановить или щелкните Import File (Файл импорта). Это может быть файловый или ленточный носитель (рис. 11-10).

11. Раскройте набор носителей до данных, которые вы хотите восстановить. Вы можете восстановить набор целиком или определенные файлы и папки.
12. Выберите данные, которые вы хотите восстановить, и щелкните Next.

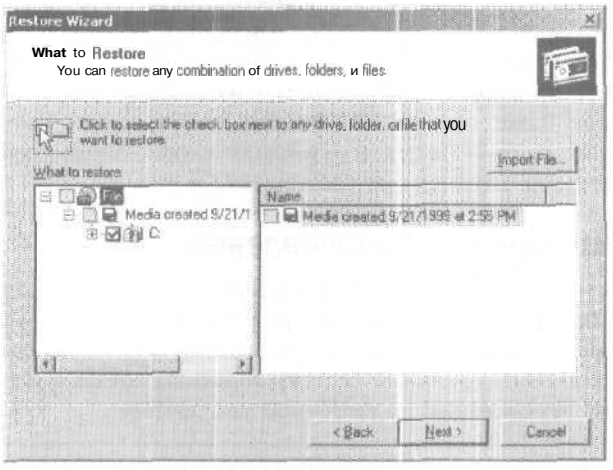


Рис. 11-10. Окно What To Restore (Что следует восстановить)

13. Выполните одно из следующих действий:
    - щелкните кнопку Finish (Готово), чтобы запустить восстановление. Мастер восстановления запросит подтверждение источника и затем выполнит восстановление. В ходе восстановления мастер Restore отображает информацию о процессе восстановления;
    - щелкните кнопку Advanced (Дополнительно), чтобы задать дополнительные параметры восстановления.

Настройка дополнительных параметров восстановления

Набор дополнительных параметров мастера восстановления зависит от типа носителя, с которого восстанавливаются данные. В табл. 11-10 описаны эти параметры.

Табл. 11-10. Дополнительные параметры восстановления

Окно дополнительных параметров	Параметр	Описание
Where To Restore (Выбор места для восстановления)	Restore Files To (Восстановить файлы в)	Целевое местоположение для сохраняемых данных. В этом списке можно выбрать: Original Location (Исходное размещение) — заменяет испорченные или утерянные данные; Alternate Location (Альтернативное размещение) — восстанавливает прежнюю версию файла в указанную вами папку; Single Folder (Единственную папку) — объединяет файлы дерева в одну папку Используйте этот параметр, например, если собираетесь копировать конкретные файлы, но не хотите восстанавливать иерархическую структуру файлов. Если вы выбрали альтернативное место или отдельную папку, вам придется также указать путь

Табл. 11-10. Дополнительные параметры восстановления *(окончание)*

Окно дополнительных параметров	Параметр	Описание
How To Restore (Способ восстановления)	When Restoring Files That Already Exist (Если восстанавливаемый файл уже существует)	Перезаписывать ли существующие файлы. Можно выбрать: Do Not Replace The File On My Disk (Не заменять имеющийся на диске файл) — предотвращает случайную перезапись существующих данных (по умолчанию); Replace The File On Disk Only If It Is Older Than The Backup Copy (Заменять файл на диске, только если он старее архивной копии) — проверяет наличие на компьютере самых новых копий; Always Replace The File On Disk (Всегда заменять имеющийся на диске файл) — Windows Backup не запрашивает подтверждения для перезаписи, встречая одинаковые имена файлов в ходе восстановления
Advanced Restore Options (Дополнительные параметры восстановления)	Select The Special Restore Options You Want To Use (Установите дополнительные параметры восстановления, если это необходимо)	Восстанавливать ли специальные системные файлы или файлы безопасности. Можно выбрать: Restore Security (Восстановление безопасности) — применяет исходные разрешения к файлам, восстанавливаемым на том NTFS. Этот вариант доступен, только если вы копировали данные с тома NTFS и восстанавливаете их на том NTFS; Restore Removable Storage Database (Восстановление базы данных съемных носителей) — восстанавливает базу данных конфигурации для устройств RSM и настройки пула носителей. База данных находится в папке *systemroot*\system32\Ntmsdata; Restore Junction Points, Not The Folders And File Data They Reference (Восстановление точек соединения, а не папок и файлов, на которые они ссылаются) — если у вас есть монтируемые диски и вы хотите восстановить данные, на которые они указывают, следует пометить этот флажок. Иначе *точки соединения* (junction points) будут восстановлены, но данные, на которые ссылается ваша точка соединения останутся недоступными

По завершении работы с мастером восстановления, Windows Backup делает следующее:

- предлагает вам подтвердить ваш выбор исходных носителей, используемых для восстановления данных. После этого Windows Backup начинает процесс восстановления;
- отображает информацию о процессе восстановления. Как и при резервном копировании, вы можете вызвать отчет (файл регистрации) о восстановлении. Он содержит информацию о числе файлов, которые были восстановлены, и продолжительности процесса восстановления.

Выполнение принудительного восстановления

Принудительное восстановление происходит после непринудительного и задает приоритетность восстановленных данных всего каталога, поддерева или отдельного объекта над их репликами на контроллерах домена в лесу. Утилита NTDSUTIL позволяет отмечать приоритетные объекты, чтобы они были реплицированы поверх их существующих копий во всем лесу.

► **Принудительное восстановление Active Directory**

1. Выполните непринудительное восстановление, как описано выше.
2. Перезагрузите компьютер.
3. На стадии загрузки, когда обычно выбирается операционная система, нажмите F8.
4. Выберите режим восстановления службы каталогов и нажмите Enter. В результате контроллер домена будет изолирован от сети.
5. Выберите для загрузки Windows 2000 Server.
6. Зарегистрируйтесь как Administrator.

Примечание Перезагружая компьютер в режиме восстановления службы каталогов, войдите как Administrator, используя соответствующие учетную запись SAM и пароль, а не имя и пароль администратора Active Directory. Это вызвано тем, что служба Active Directory автономна, и проверка учетной записи невозможна. Вместо этого для управления доступом к Active Directory применяется база данных учетных записей SAM. Настройка пароля SAM производилась при установке Active Directory.

---

7. Появится сообщение, что Windows работает в безопасном режиме. Щелкните OK.
8. Раскройте меню Start\Programs\Accessories и щелкните Command prompt (Командная строка).
9. В командной строке наберите **ntdsutil** и нажмите Enter.
10. В строке NTDSUTIL наберите **authoritative restore** и нажмите Enter.
11. В строке принудительного восстановления:
    - чтобы принудительно восстановить весь каталог, наберите **restore database** и нажмите Enter;
    - чтобы принудительно восстановить часть каталога или его поддерево, например ОП, используйте известное имя ОП, наберите **restore subtree** <*имя_поддерева*> и нажмите Enter.

      Например, чтобы восстановить ОП Security1 в домене microsoft.com, введите команды:

```
ntdsutil
authoritative restore
restore subtree
OU=Security1, DC=Microsoft, DC=COM
```

    - чтобы принудительно восстановить весь каталог и обновить номер версии, введите **restore database verinc** <*номер_версии*> и нажмите Enter;
    - чтобы принудительно восстановить поддерево каталога и обновить номер версии, введите **restore subtree** <*составное_имя_поддерева*>**verinc** <*номер_версии*> и нажмите Enter.

При принудительном восстановлении открывается файл NTDS.DIT, увеличивается номер версии, пересчитываются записи, нуждающиеся в обновлении, проверяется число обновляемых записей, и затем появляется сообщение о завершении. Если номер версии не задан, он вычисляется автоматически.

12. Наберите quit и нажмите Enter, чтобы выйти из утилиты NTDSUTIL. Затем закройте окно командной строки.
13. Перезагрузите контроллер домена в обычном режиме и подсоедините восстановленный контроллер домена к сети,

Когда восстановленный контроллер домена подключен к сети, в ходе обычной репликации состояние восстановленного контроллера исправляется с учетом всех изменений на дополнительных контроллерах домена, не отмененными принудительным восстановлением. Репликация также распространяет принудительно восстановленные объекты на остальные контроллеры в лесе. Удаленные объекты, отмеченные для принудительного восстановления, реплицируются с восстановленного контроллера домена на дополнительные контроллеры домена. Поскольку восстановленные объекты имеют одни и те же GUID и SID, защита и связи между объектами остаются неповрежденными.

Дополнительные задачи для принудительного восстановления всей базы данных Active Directory

Принудительно восстанавливая всю базу данных Active Directory, вы должны выполнить дополнительную процедуру с каталогом Sysvol. Это необходимо для обеспечения целостности групповой политики компьютера. Чтобы обеспечить полномочное восстановление надлежащих элементов, необходимо скопировать каталог Sysvol в другое место поверх существующего *после* публикации общего каталога Sysvol.

При принудительном восстановлении части БД Active Directory (включая объекты политики) вам придется выполнить дополнительную процедуру с каталогом Sysvol. Чтобы обеспечить полномочное восстановление надлежащих элементов, вы должны скопировать только папки политики (определяемые GUID), соответствующие восстановленным объектам политики, из другого места после публикации общего каталога Sysvol. Затем скопируйте их поверх существующих.

При принудительном восстановлении всей базы Active Directory либо выбранных объектов важно, что вы копируете Sysvol и данные политики из другого места после публикации общего каталога Sysvol. Если компьютер находится в реплицированном домене, до публикации общего каталога Sysvol может пройти несколько минут, так как требуется синхронизация с его партнерами по репликации. Если все компьютеры в домене принудительно восстановлены и перезапущены в одно и то же время, то каждый будет безуспешно ждать синхронизации друг с другом. В этом случае сначала восстановите один из контроллеров домена так, чтобы его общий каталог Sysvol удалось опубликовать; затем непринудительно восстановите другие компьютеры.

Резюме

Мы рассказали о том, как принудительно и непринудительно восстанавливать Active Directory. Сначала надо выбрать режим. При непринудительном режиме восстановления любой компонент состояния системы, реплицированный другим контроллером домена, типа службы каталогов Active Directory, обновляется в ходе репликации после восстановления данных. При принудительном режиме сделанные после последнего архивирования изменения не восстанавливаются; удаленные объекты восстанавливаются и реплицируются.

Для восстановления состояния системы на контроллере домена вам надо сначала загрузить компьютер в специальном режиме восстановления службы каталогов. Это позволит восстановить базы данных служб каталогов SYSVOL и Active Directory. Разрешается восстановить состояние системы только локально. Проделать эту операцию на удаленном компьютере невозможно.

Непринудительное восстановление помогает выполнить мастер. Для принудительного восстановления надо сначала выполнить непринудительное восстановление, а затем воспользоваться утилитой NTDSUTIL, чтобы отметить объекты для принудительного восстановления. Эти объекты будут реплицированы.

Занятие 8. Устранение неполадок Active Directory

На этом занятии описываются некоторые проблемы Active Directory, с которыми вы можете столкнуться, и их возможные решения.

Изучив материал этого занятия, вы сможете:

- ✓ устранить неполадки Active Directory.

Продолжительность занятия — около 10 минут.

В табл. 11-11 описываются возможные способы устранения неполадок Active Directory.

Табл. 11-11. Сценарии устранения неполадок Active Directory

Невозможно добавить или удалить домен

Причина	Решение
Хозяин именования доменов недоступен. Это может быть вызвано проблемами с сетевым соединением или отказом компьютера, играющего роль хозяина именования доменов	Решите проблему с сетевым соединением либо почините или замените компьютер, играющий роль хозяина именования доменов. Иногда стоит переназначить роль хозяина именования доменов

Невозможно создать объекты в Active Directory

Причина	Решение
Недоступен мастер относительных идентификаторов. Это может быть вызвано проблемами с сетевым соединением или отказом компьютера, играющего роль хозяина относительных идентификаторов	Решите проблему с сетевым соединением либо почините или замените компьютер, выполняющий роль хозяина относительных идентификаторов. Иногда стоит переназначить роль хозяина относительных идентификаторов;

Невозможно изменить схему

Причина	Решение
Недоступен хозяин схемы. Это может быть вызвано проблемами с сетевым соединением или отказом компьютера, играющего роль хозяина схемы	Решите проблему с сетевым соединением либо почините или замените компьютер, выполняющий роль хозяина схемы. Иногда стоит присвоить роль хозяина схемы

Табл. 11-11. Сценарии устранения неполадок Active Directory *(окончание)*

Изменения членства в группе не вступают **в силу**

Причина	Решение
Недоступен хозяин инфраструктуры. Это может быть вызвано проблемами с сетевым соединением или отказом компьютера, играющего роль хозяина инфраструктуры	Решите проблему с сетевым соединением либо почините или замените компьютер, выполняющий роль хозяина инфраструктуры. Иногда стоит переназначить роль хозяина инфраструктуры

Клиенты без программного обеспечения Active Directory не могут войти в систему

Причина	Решение
Недоступен эмулятор основного контроллера домена. Это может быть вызвано проблемами с сетевым соединением или отказом компьютера, играющего роль эмулятора основного контроллера домена	Решите проблему с сетевым соединением либо почините или замените компьютер, выполняющий роль эмулятора основного контроллера домена. Иногда стоит переназначить роль эмулятора основного контроллера домена

Клиенты не могут обратиться к ресурсам в другом домене

Причина	Решение
Произошел разрыв доверительных отношений между доменами	Восстановите и проверьте доверительные отношения между доменами. Для успешного восстановления доверия требуется эмулятор PDC

Резюме

На этом занятии вы изучили некоторые неполадки Active Directory, с которыми можете столкнуться, и возможные способы их решения.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении А «Вопросы и ответы» в конце книги.

1. Как глобальный каталог помогает пользователям искать объекты Active Directory?

2. Вы хотите разрешить руководителю отдела продаж создавать, изменять и удалять учетные записи для подчиненных ему сотрудников. Как это сделать?

3. Что происходит с разрешениями объекта при перемещении его из одного ОП в другой?

4. На каком уровне позволяет настраивать административный контроль мастер Delegation Of Control?

5. Какие данные надо архивировать для восстановления Active Directory? Что относится к этим данным?

6. Как надо зарегистрироваться в системе при ее перезагрузке в режиме восстановления служб каталога? Почему?

ГЛАВА 12

Администрирование групповой политики

В этой главе

Средствами групповой политики администраторы могут управлять параметрами рабочего стола для групп компьютеров и пользователей. Групповая политика очень гибка и включает параметры реестра, системы защиты, настройку управления приложениями, параметры сценариев, настройку запуска и выключения системы, входа в систему и завершения сеанса работы, а также параметры перенаправления папок. В Microsoft Windows 2000 имеются сотни параметров групповой политики. Их настройка позволяет снизить общую стоимость владения компьютерным парком,

Прежде всего

Для изучения материалов этой главы необходимо:

- выполнить процедуру установки, описанную во вводной главе;
- настроить компьютер в качестве контроллера домена;
- выполнить **упражнения из глав 8 и** 11.

Занятие 1. Концепции групповой политики

Прежде чем внедрять групповую политику, необходимо изучить концепции, определяющие порядок ее работы. На этом занятии мы дадим определение групповой политики, расскажем об администрировании такой политики, а также перечислим параметры политики. Кроме того, вы узнаете о влиянии групповой политики на запуск и вход в систему, о порядке обработки групповой политики и фильтрования групповой политики с помощью групп безопасности.

Изучив материал этого занятия, вы сможете:

- ✓ описать назначение и функции групповой политики;
- ✓ рассказать, как передать права администрирования политики другому лицу;
- ✓ описать параметры групповой политики;
- ✓ рассказать, как групповая политика влияет на запуск и вход в систему;
- ✓ описать порядок обработки групповой политики;
- ✓ рассказать о фильтровании групповой политики с помощью групп безопасности.

Продолжительность занятия — около 35 минут.

Что такое групповая политика

Групповая политика (group policy) представляет собой набор конфигурационных параметров компьютера и пользовательских параметров. Она позволяет определить программы, доступные пользователям, приложения, значки которых отображаются на рабочем столе, элементы меню Start (Пуск), а также функциональность компьютера.

Объекты групповой политики

Чтобы создать конфигурацию рабочего стола для некоторой группы пользователей, вы создаете *объекты групповой политики* (ОГП) — наборы параметров политики. На каждом компьютере с Windows 2000 имеется один *локальный* (local) ОГП; кроме того, на компьютер может распространяться действие неограниченного числа *нелокальных* (nonlocal) ОГП, основанных на службе каталогов Active Directory.

Локальный ОГП хранится на компьютере независимо от того, работает ли последний в сети и есть ли сведения о нем в Active Directory. Тем не менее, поскольку нелокальные ОГП могут перекрывать параметры локального ОГП, в среде Active Directory эти параметры меньше всего влияют на конфигурацию рабочего стола. В изолированной среде (или в сети без контроллера домена Windows 2000) параметры локального ОГП приоритетнее, поскольку нелокальные ОГП не могут их перекрыть.

Нелокальные ОГП связаны с объектами Active Directory (сайтами, доменами или ОП), и их действие может распространяться на компьютеры или пользователей. Для работы с нелокальными ОГП вам потребуется контроллер домена Windows 2000. В Active Directory правила из нелокальных ОГП суммируются и применяются в соответствии с иерархией: от более крупных группировок (от сайта) к малым (к подразделению).

На этом занятии мы будем говорить о локальных ОГП, если не указано обратное.

Делегирование управления групповой политикой

Чтобы задать перечень административных групп, обладающих правами управления ОГП (создание, изменение и удаление), определите для каждого ОГП разрешения доступа.

Административная группа с разрешениями Read и Write для ОГП может передавать нрава управления этим объектом.

Оснастка Group Policy

Используется для организации и управления параметрами групповой политики каждого ОГП. На рис. 12-1 показана оснастка для ОГП Default Domain Controllers Policy.

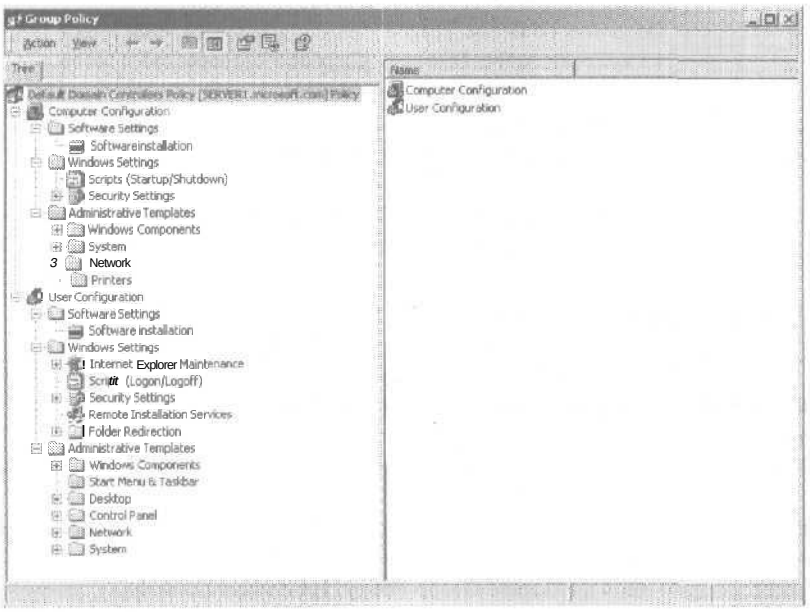


Рис. 12-1. Оснастка Group Policy (Групповая политика)

Запуск оснастки Group Policy

В табл. 12-1 перечислены способы запуска оснастки Group Policy, используемые при выполнении различных действий.

Табл. 12-1, Способы запуска оснастки Group Policy

Применение групповой политики	Порядок действий
К локальному компьютеру (локальный ОГП)	Откройте локальный ОГП компьютера (см. раздел «Запуск оснастки Group Policy для настройки локальной групповой политики») и выберите требуемые параметры политики в оснастке Group Policy. Для изменения локальных параметров безопасности в программной группе Administrative Tools (Администрирование) щелкните Local Security Policy (Локальная политика безопасности)
К другому компьютеру (локальный ОГП)	Откройте локальный ОГП на компьютере с Windows 200С (см. раздел «Запуск оснастки Group Policy для настройки локальной групповой политики») и затем выберите компьютер в сети. Вам потребуются права администратора для этого компьютера

Табл. 12-1, Способы запуска оснастки Group Policy *(окончание)*

Применение групповой политики	Порядок действий
К сайту	Откройте ОГП (см. раздел «Запуск оснастки Group Policy из консоли Active Directory Sites and Services») и затем свяжите ОГП с требуемым сайтом
К домену	Откройте ОГП (см. раздел «Запуск оснастки Group Policy из консоли Active Directory Users and Computers») и затем свяжите ОГП с требуемым доменом
К организационному подразделению (ОП)	Откройте ОГП (см. раздел «Запуск оснастки Group Policy из консоли Active Directory Users and Computers») и затем свяжите ОГП с требуемым ОП. Кроме того, можно связать ОГП с подразделением, расположенным выше по иерархии, чтобы нужное вам ОП наследовало параметры групповой политики
К существующему ОГП или набору ОГП	Создайте и сохраните собственную консоль MMC

▶ Запуск оснастки Group Policy для настройки локальной групповой политики

1. Запустите Microsoft Management Console.
2. В меню Console (Консоль) выберите команду Add/Remove Snap-In (Добавить/удалить оснастку).
3. В открывшемся окне перейдите на вкладку Standalone (Изолированная оснастка) и щелкните кнопку Add (Добавить),
4. В открывшемся диалоговом окне щелкните Group Policy (Групповая политика), затем — кнопку Add.
5. Убедитесь, что в поле Group Policy Object (Объект групповой политики) диалогового окна Select Group Policy Object (Выбор объекта групповой политики) отображается Local Computer (Локальный компьютер).
6. Щелкните кнопку Finish (Готово). Затем в диалоговом окне Add Standalone Snap-In (Добавить изолированную оснастку) щелкните кнопку Close (Закрыть).
7. В диалоговом окне Add/Remove Snap-In щелкните OK.

▶ Запуск оснастки Group Policy из консоли Active Directory Sites and Services

1. Откройте консоль Active Directory Sites and Services (Active Directory — сайты и службы).
2. В дереве консоли щелкните правой кнопкой мыши сайт, для которого необходимо определить политику, и выберите команду Properties (Свойства).
3. Перейдите на вкладку Group Policy (Групповая политика), выберите в списке Group Policy Object Links (Ссылки на объекты групповой политики) существующий ОГП и щелкните кнопку Edit (Изменить). Для создания нового ОГП щелкните кнопку New (Создать) и затем — кнопку **Edit.**

   После этого оснастка Group Policy станет доступной для сайта.

▶ Запуск оснастки Group Policy из консоли Active Directory Users and Computers

1. Откройте консоль Active Directory Users and Computers (Active Directory — пользователи и компьютеры).
2. В дереве консоли щелкните правой кнопкой мыши ОП или домен, для которого требуется определить политику групп, и выберите в контекстном меню команду Properties.

3. Перейдите на вкладку Group Policy, выберите в списке Group Policy Object Links существующий ОГП и щелкните кнопку Edit (Для создания нового ОГП щелкните кнопку New и затем — кнопку Edit).

Параметры групповой политики

Они хранятся в ОГП и определяют конфигурацию рабочего стола пользователя. Существует два вида параметров групповой политики: конфигурационные параметры компьютера и пользовательские параметры.

Конфигурационные параметры компьютера (computer configuration settings) служат для настройки политик, действие которых распространяется на компьютеры независимо от того, какой пользователь входит в систему; они применяются при инициализации системы.

Пользовательские параметры служат для настройки политик, распространяющихся на пользователей, независимо от компьютеров, на которых те регистрируются; они применяются при регистрации пользователя на компьютере.

Примечание Хотя некоторые параметры регулируют настройки пользовательского интерфейса, например фоновый рисунок рабочего стола или наличие команды Run (Выполнить) в меню Start (Пуск), их можно применять и по отношению к компьютерам — в виде конфигурационных параметров компьютера.

Для настройки конфигурационных и пользовательских параметров используются узлы Software Settings (Конфигурация программ), Windows Settings (Конфигурация Windows) и Administrative Templates (Административные шаблоны) оснастки Group Policy.

Узел Software Settings

При настройке конфигурационных параметров компьютера и пользовательских параметров по умолчанию этот узел содержит лишь подузел Software Installation (Установка программ), который позволяет определить порядок установки и поддержки приложений в вашей организации (рис. I2-2). Кроме того, в этот подузел независимые разработчики ПО могут добавлять собственные параметры.

Вы управляете приложением из ОГП, который, в свою очередь, связан с определенным контейнером Active Directory — сайтом, доменом или ОП. Для управления приложением его можно назначить или опубликовать. Назначьте приложение компьютеру, если хотите, чтобы оно было доступно всем пользователям или компьютерам, управляемым данным ОГП. Если вам необходимо предоставлять пользователям, управляемым ОГП, какое-либо приложение по запросу, опубликуйте его. Опубликовать приложение для компьютеров нельзя. Подробнее о конфигурировании процесса установки ПО с использованием групповой политики — на занятии 4.

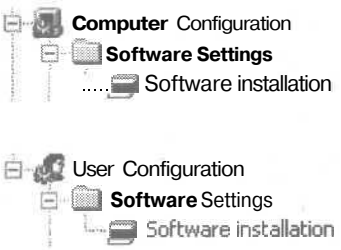


Рис. 12-2. Узел Software Settings (Конфигурация программ)

Узел Windows Settings

При настройке конфигурационных параметров компьютера и пользовательских параметров этот узел содержит подузлы Scripts (Сценарии) и Security Settings (Параметры безопасности) (рис. 12-3).

Узел Scripts позволяет определить сценарии запуска/выключения компьютера и сценарии входа в систему/завершения сеанса работы. Если компьютеру назначено несколько сценариев запуска/выключения и входа в систему/завершения сеанса работы, Windows 2000 выполняет их по порядку, задать который можно в диалоговом окне свойств соответствующего типа сценариев. При выключении компьютера Windows 2000 обрабатывает сценарии завершения сеанса работы и затем — сценарии выключения системы. По умолчанию тайм-аут при обработке сценариев равен 10 минутам. Если на обработку ваших сценариев завершения сеанса работы и выключения компьютера требуется более 10 минут, измените значение тайм-аута в политике программного обеспечения.

Администраторы могут использовать любой удобный для них язык сценариев ActiveX, в том числе VBScript, JScript, Perl и пакетные файлы MS-DOS (с расширениями .bat и .cmd).

Узел Security Settings (Параметры безопасности) позволяет администратору вручную настроить уровни безопасности для локальных и нелокальных ОГП. Это делается после или вместо настройки системы защиты компьютера с применением шаблона безопасности. Подробнее о системе защиты — в главе 13.

При конфигурировании пользовательских Параметров узел Windows Settings также включает подузлы Internet Explorer Maintenance (Поддержка Internet Explorer), Remote Installation Services (Службы удаленной установки) и Folder Redirection (Перенаправление папки). Узел Internet Explorer Maintenance позволяет администрировать и настраивать Microsoft Internet Explorer на компьютерах с Windows 2000. Службы Remote Installation Services управляют процессом удаленной установки ОС. Кроме того, эти службы можно использовать для предоставления заказных пакетов клиентам Active Directory с операционными системами, отличными от Windows 2000 (впрочем, для применения групповой политики требуется клиентский компьютер с Windows 2000, а не просто клиент Active Directory с предыдущей версией Windows). Узел Folder Redirection позволяет перенаправлять специальные папки Windows 2000 — My Documents (Мои документы), Application Data, Desktop (Рабочий стол) и меню Start (Главное меню) — из исходной папки, заданной в профиле пользователя, в альтернативное место в сети, откуда этими папками можно управлять централизованно. Подробнее о перенаправлении специальных папок с использованием групповой политики — на занятии 5.

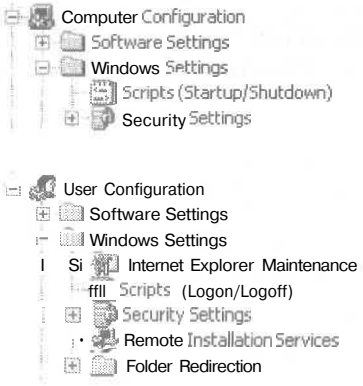


Рис. 12-3. Узел Windows Settings (Конфигурация Windows)

Узел Administrative Templates

При настройке конфигурационных параметров компьютера и пользовательских параметров этот узел содержит все параметры политики, хранящиеся в реестре, в том числе параметры из подузлов Windows Components (Компоненты Windows), System (Система) и Network (Сеть) (рис. 12-4). Узел Windows Components позволяет администрировать компоненты Windows 2000, включая NetMeeting, Internet Explorer, Windows Explorer (Проводник), Microsoft Management Console (Консоль управления Microsoft), Task Scheduler (Планировщик заданий) и Windows Installer (Установщик Windows), Узел System применяется для управления функциями входа в систему и завершения сеанса работы, а также для управления самой групповой политикой. Узел Network содержит подузлы Offline Files (Автономные файлы) и Network and Dial-Up Connections (Сеть и удаленный доступ к сети).

При настройке конфигурационных параметров компьютера узел Administrative Templates содержит также подузел Printers (Принтеры). Кроме того, узел System содержит подузлы Disk Quotas (Дисковые квоты), Domain Name System (DNS) Client (DNS-клиент) и Windows File Protection (Защита файлов Windows).

При конфигурировании пользовательских параметров узел Administrative Templates также содержит дополнительные параметры групповой политики, хранимые в реестре, включая подузлы Start Menu & Taskbar (Панель задач и меню «Пуск»), Desktop (Рабочий стол) и Control Panel (Панель управления). Узел Start Menu & Taskbar позволяет настроить меню Start и панель задач; узел Desktop применяется для конфигурирования рабочего стола. В узле Control Panel можно определить, какие программы из панели управления Windows будут доступны пользователю.

В узле Administrative Templates более 450 параметров предназначены для конфигурирования среды пользователя. Конфигурационные параметры компьютера сохраняются в разделе реестра HKEY_LOCAL_MACHINE (HKLM), а пользовательские - в разделе HKEY_CURRENT_USER (HKCU).

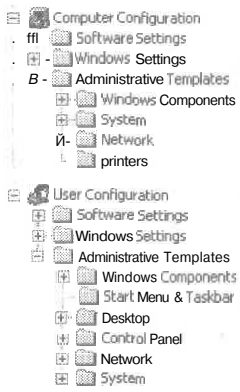


Рис. 12-4. Узел Administrative Templates (Административные шаблоны)

Примечание Для отображения административных шаблонов раскройте узел Administrative Templates и выберите в меню View (Вид) команду Show Policies Only (Показывать только политики) для просмотра всех параметров или Show Configured Policies Only (Отображать только заданные политики) для просмотра используемых параметров.

Модель оснасток MMC

Узлы оснастки Group Policy сами по себе являются расширениями оснастки MMC. По умолчанию при запуске оснастки Group Policy загружаются все доступные ее расширения. Для изменения этой модели поведения создайте собственную консоль и настройте параметры политики в соответствии с собственными требованиями. Конфигурируют параметры средствами узла Administrative Templates.

Используя такую модель, разработчики могут создавать расширения оснастки Group Policy для создания дополнительных политик. В свою очередь, и эти расширения разрешается дополнять. В качестве примера такой оснастки можно назвать Security Settings, включающую несколько оснасток-расширений.

Пространство имен оснастки Group Policy

Имя корневого узла оснастки Group Policy отображается в следующем формате:

Имя_ОГП [имя_домена] Policy

Например: Default Domain Controllers Policy [serverl.microsoft.com] Policy

Влияние групповой политики на загрузку компьютера и регистрацию пользователя в системе

Итак, как же действуют конфигурационные параметры компьютера и пользовательские параметры при регистрации пользователя в системе?

1. Восстанавливаются сетевые подключения. Загружаются службы Remote Procedure Call System Service (RPCSS) и Multiple Universal Naming Convention Provider (MUP).
2. Для компьютера загружается упорядоченный список ОГП, содержимое которого зависит от следующих факторов:
   - состоит ли компьютер в домене Windows 2000 и распространяется ли на него действие групповой политики через службу Active Directory;
   - от местоположения компьютера в службе каталогов Active Directory;
   - если список ОГП не изменился, он не обрабатывается. Для изменения этого поведения настройте соответствующим образом параметры групповой политики.
3. Обрабатываются конфигурационные параметры компьютера. По умолчанию это выполняется синхронно и в следующем порядке: локальный ОГП, ОГП сайта, ОГП домена, ОГП подразделения и т. д. До завершения обработки интерфейс пользователя не отображается. Подробнее об обработке ОГП — в разделе «Порядок обработки групповой политики».
4. Выполняются сценарии загрузки. По умолчанию это происходит в скрытом режиме и синхронно; перед выполнением следующего сценария должен завершиться текущий сценарий, или должен наступить тайм-аут для текущего сценария. По умолчанию тайм-аут составляет 600 секунд (10 минут). Чтобы изменить его, настройте групповую политику.
5. Пользователь нажимает Ctrl+Alt+Del для входа в систему.
6. После проверки имени и пароля загружается профиль пользователя, на который распространяются параметры локальной групповой политики.
7. Для пользователя загружается упорядоченный список ОГП, содержимое которого зависит от следующих факторов:
   - является ли пользователь членом домена Windows 2000 и распространяется ли на него действие групповой политики через службы Active Directory;

- включено ли замыкание на себя, а также в каком режиме (Merge или Replace). Подробнее о замыкании на себя — в разделе «Порядок обработки групповой политики»;
- от местоположения пользователя в службе каталогов Active Directory;
- если список ОГП не изменился, он не обрабатывается. Для изменения этой ситуации настройте соответствующим образом параметры групповой политики.

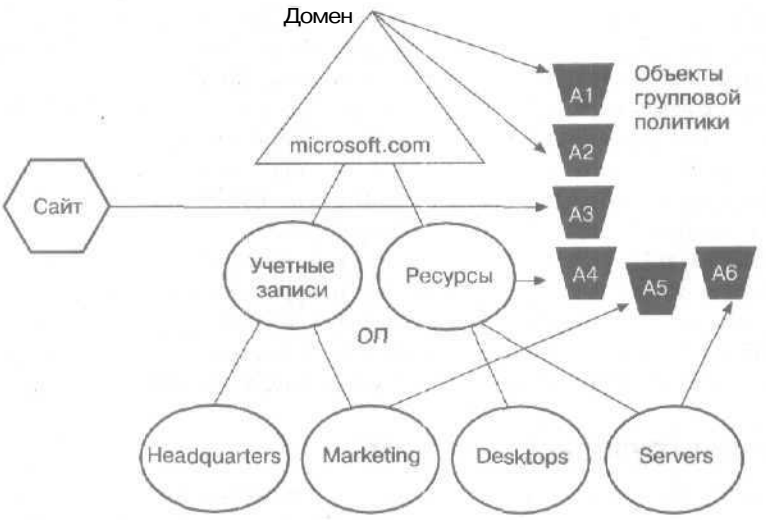
8. Обрабатываются пользовательские параметры. По умолчанию это выполняется синхронно и в следующем порядке: локальный ОГП, ОГП сайта, ОГП домена, ОГП подразделения и т. д. До завершения обработки интерфейс пользователя не отображается. Подробнее об обработке ОГП — в разделе «Порядок обработки групповой политики».
9. Выполняются сценарии входа в систему. В отличие от сценариев Windows NT 4.0 сценарии входа, основанные на групповой политике, по умолчанию выполняются в скрытом режиме и асинхронно. Сценарий объекта пользователя выполняется последним.
10. Отображается пользовательский интерфейс ОС, соответствующий групповой политике.

Порядок обработки групповой политики

Настройки групповой политики обрабатываются в порядке, описанном ниже.

1. Локальный ОГП — на каждом компьютере с Windows 2000 имеется один ОГП, хранящийся локально.
2. ОГП сайта — следующими обрабатываются любые ОГП, настроенные для сайта. Обработка осуществляется синхронно; порядок обработки определяется администратором.
3. ОГП домена — обработка всех ОГП, настроенных для домена, осуществляется синхронно; порядок обработки определяется администратором.
4. ОГП организационной единицы — первыми обрабатываются ОГП, связанные с ОП, расположенными выше всех в иерархии Active Directory. Затем обрабатываются ОГП ОП более низкого уровня и т. д. Последними обрабатываются ОГП, связанные с ОП. куда входят пользователи или компьютеры. С каждым ОП в Active Directory могут быть связаны один или несколько ОГП. Обработка нескольких ОГП, настроенных для одного ОП, ведется синхронно и в порядке, определяемом администратором.

Видно, что первым обрабатывается локальный ОГП, а ОГП подразделений, к которым непосредственно относится пользователь или компьютер, обрабатываются последними и перекрывают параметры вышестоящих ОГП. Например, вы создали ОГП домена, позволяющий всем пользователям интерактивно регистрироваться в системе. Тем не менее ОГП подразделения, в которое входит контроллер домена, разрешает регистрироваться в системе лишь администраторам. На рис. 12-5 проиллюстрирована взаимосвязь групповой политики и Active Directory.



Порядок обработки ОГП для ОП Marketing = A3, A1, A2, A5
Порядок обработки ОГП для ОП Servers = A3, A1, A2, A4, A6

Рис. 12-5. Групповая политика и Active Directory

Исключения **в порядке** обработки **по умолчанию**

- **Компьютер, состоящий в рабочей группе, обрабатывает только локальный ОГП.**
- **No Override (Не перекрывать).** Для любого ОГП, связанного с сайтом, доменом или подразделением (но не локальным ОГП), разрешается задать параметр No Override по отношению к сайгу, домену или подразделению так, что ни один из параметров политики не будет перезаписан. При назначении более чем одному ОГП параметра No Override приоритет имеет наивысший в иерархии Active Directory параметр (или наивысший в иерархии, заданной администратором на каждом определенном уровне в Active Directory).
- **Block Policy Inheritance (Блокировать наследование политики).** Для наследования групповой политики любого сайта, домена или подразделения достаточно выборочно пометить флажок Block Policy Inheritance. Впрочем, параметры ОГП, для которых задан параметр No Override, применяются всегда, их нельзя блокировать.

  Параметр Block Policy Inheritance применяется непосредственно к сайту, домену или подразделению. Он неприменим ни к ОГП, ни к ссылкам на ОГП. Таким образом, Block Policy Inheritance предотвращает *все* попытки распространения параметров групповой политики на сайт, домен или подразделение от высшего иерархического уровня (по ссылке на родительский объект в иерархии Active Directory), вне зависимости от того, где в иерархии были заданы эти параметры.
- **Loopback (Замыкание на себя)** — дополнительный параметр групповой политики, который необходим на компьютерах в среде, требующей нестандартной организации управления (например, киоски, лаборатории, аудитории). Замыкание на себя — альтернативный способ получения упорядоченного списка ОГП, параметры пользовательской конфигурации которых влияют на среду пользователя. По умолчанию пользовательские параметры берутся из списка ОГП, зависящего от расположения объекта пользователя в иерархии Active Directory. Упорядоченный список начинается с ОГП,

связанных с сайтом, затем с доменом и, наконец, с подразделением и применяется согласно условиям наследования, зависящим от расположения объекта пользователя в иерархии Active Directory и в порядке, заданном администратором на каждом уровне. Параметр замыкания на себя, как и любой другой параметр политики, может иметь одно из трех состояний: Not Configured (Не задана), Enabled (Включена) или Disabled (Отключена). В состоянии Enabled действуют параметры Merge (Слияние) или Replace (Замена).

- **Замыкание на себя с заменой. В** этом случае список ОГП для данного пользователя полностью заменяется списком ОГП, полученным для компьютера при его загрузке (см. пункт 2 в разделе «Влияние групповой политики на загрузку компьютера и регистрацию пользователя в системе»). ОГП компьютера заменяют пользовательские ОГП, которые обычно применяются к данному пользователю.
- **Замыкание на себя со слиянием.** В этом случае список ОГП объединяется. Список ОГП, полученный для компьютера при его загрузке (см. пункт 2 в разделе «Влияние групповой политики на загрузку компьютера и регистрацию пользователя в системе») добавляется к списку ОГП, полученному для пользователя при его регистрации (пункт 7). Список ОГП для компьютера применяется позже и поэтому при возникновении конфликтов с параметрами, указанными в пользовательском списке, имеет приоритет.

Наследование групповой политики

В обшем, групповая политика передается от родительских к дочерним контейнерам. Если определенная групповая политика назначена на верхнем уровне родительского контейнера, то она применяется для всех контейнеров ниже родительского, включая объекты пользователей и компьютеров в каждом контейнере. Однако при применении определенной групповой политики к дочернему контейнеру эта политика будет более приоритетной, чем наследуемая от родительского контейнера.

Ненастроенные параметры политики для родительского подразделения не наследуются дочерним подразделением. Отключенные параметры политики наследуются как отключенные. Если политика настроена для родительского подразделения, но не настроена для дочернего, то дочернее подразделение наследует ее от родительского.

Если родительская и дочерняя политики совместимы, то помимо параметров родительской политики применяются и параметры дочерней. Политики наследуются до тех пор. пока они совместимы. Например, если родительская политика помещает определенную папку на рабочий стол, а дочерняя политика помещает на рабочий стол еше одну папку, то пользователь увидит обе папки.

Если политика, настроенная для родительского подразделения, несовместима с той же политикой, настроенной для дочернего подразделения, то дочернее подразделение не наследует политику от родительского. В этом случае применяются параметры дочерней политики.

Фильтрование групповой политики с помощью групп безопасности

Поскольку групповая политика может применять параметры нескольких объектов групповой политики к сайту, домену или подразделению, то можно добавить объекты групповой политики, связанные с объектами другого каталога. Задавая соответствующие разрешения для групп безопасности, можно отфильтровать групповую политику, чтобы она влияла только на указанных вами пользователей и компьютеры.

Резюме

Групповая политика — это набор конфигурационных параметров компьютера и пользовательских параметров, который можно сопоставить компьютерам, сайтам, доменам или ОП для настройки параметров компонентов, составляющих рабочую среду пользователя. Чтобы создать конфигурацию рабочего стола для некоторой группы пользователей, вы создаете объекты групповой политики (ОГП). Чтобы определить список групп, обладающих правами администрирования ОГП (создание, изменение, удаление), следует назначить права доступа к ОГП.

Существует два вида параметров групповой политики: конфигурационные параметры компьютера и пользовательские параметры. Для настройки обоих этих типов применяются узлы Software Settings, Windows Settings и Administrative Templates оснастки Group Policy.

Групповая политика влияет на процесс загрузки компьютера и регистрации пользователя в системе. Сначала обрабатываются конфигурационные параметры компьютера, а затем — пользовательские параметры. По умолчанию обработка выполняется синхронно и в следующем порядке: локальный ОГП, ОГП сайта, ОГП домена и ОГП ОП. Использование параметров No Override, Block Policy Inheritance, а также Loopback позволяет изменить стандартный порядок обработки политики.

Назначая группам безопасности соответствующие разрешения, вы можете фильтровать групповую политику, чтобы она влияла лишь на указанных пользователей и компьютеры.

Занятие 2. Планирование внедрения групповой политики

Внедрение групповой политики необходимо тщательно подготовить: спланируйте параметры и способы реализации ОГП. Здесь рассматриваются стратегии внедрения и параметры ОГП.

Изучив материал этого занятия, вы сможете:

- ✓ перечислить параметры управления групповой политикой;

Продолжительность занятия — около 15 минут.

Выбор типа ОГП

Выбор ОГП обусловлен типом параметров, которые они содержат. Существует три основных схемы организации параметров ОГП:

- **однородная** — включает ОГП, содержащие один тип параметров групповой политики. Например, это может быть ОГП, в который входят лишь параметры защиты;
- **комбинированная** — включает ОГП, содержащие разные типы параметров групповой политики. Например, ОГП, в который входят параметры программ и развертывания приложений или содержащая параметры безопасности и сценариев;
- **раздельная** — включает ОГП, предназначенные либо для конфигурации компьютера, либо для параметров пользователей.

Эти типы параметров проиллюстрированы на рис. 12-6.

Рис. 12-6. Типы настроек ОГП

Однородная политика

Основная цель данного подхода — выделить каждый тип параметров групповой политики в отдельный ОГП. Для этого создается ОГП для параметров управления приложениями, ОГП для документов и параметров пользователей, ОГП для политик приложений и т. д. Доступ Read/Write следует предоставлять лишь пользователям, которые будут администрировать ОГП.

Такая модель наилучшим образом подходит организациям, в которых администрированием занимается несколько ответственных лиц.

Комбинированная политика

Основная цель данного подхода — объединить в одном ОГП различные типы параметров групповой политики.

Такая модель оптимальна для организаций, где административные полномочия централизованы, и на администратора возложена обязанность управлять большинством или всеми групповыми политиками.

Раздельная политика

Основная цель данного подхода — объединить все параметры групповой политики, связанные с рабочей средой пользователя, в одном ОГП, а все параметры, связанные с конфигурацией компьютера, — в другом ОГП. При этом увеличивается количество ОГП, обрабатываемых при входе в систему, и следовательно, возрастает время регистрации в системе. Тем не менее такая модель упрощает решение проблем. Например, при подозрении на сбой в конфигурации компьютера администратор может зарегистрироваться в системе как пользователь, на которого не распространяется конфигурационная политика и, таким образом, исключить такую причину сбоя, как политика пользователя.

Стратегии внедрения ОГП

Планируя структуру Active Directory, оцените, как вы будете развертывать в организации групповую политику. Важно при этом учитывать предоставление полномочий, разделение административных обязанностей, выбор типа администрирования (централизованное или децентрализованное), а также гибкость разработанной структуры.

Ниже приводятся примеры стратегий развертывания групповых политик. При создании собственных решений, как правило, элементы описываемых стратегий комбинируются.

Многоуровневая и единая структура ОГП

Данные стратегии определяют, как в ОГП хранятся параметры политики — централизованно (многоуровневая структура) или децентрализовано (единая структура).

Многоуровневая структура

Основная цель этого способа (рис. 12-7) — постараться сделать так, чтобы определенный параметр политики присутствовал в как можно меньшем числе ОГП. В случае необходимости вам потребуется изменить лишь один (или небольшое число) ОГП. Администрирование упрощается, но за это приходится платить увеличением времени на вход в систему (из-за обработки множества ОГП).

Создайте для домена базовый ОГП, который содержит параметры для как можно большего числа пользователей и компьютеров. Например, базовый ОГП мог бы содержать параметры безопасности масштаба предприятия или масштаба группы, такие, как ограничения учетных записей и паролей.

Затем создайте дополнительные ОГП, увязанные с общими требованиями каждой корпоративной группы (например, для инженеров, отделов сбыта и маркетинга, руководящих работников и ассистентов), и распространите их действие на соответствующие ОП.

Такая модель наилучшим образом подходит для сред, где в различных подразделениях организации предъявляются общие требования к безопасности и где групповая политика часто изменяется.

Единая структура

Основная цель данного способа (рис. 12-7) — назначить конкретному пользователю или компьютеру как можно меньше (в идеале — один) ОГП. Все необходимые параметры политики сайта, домена или ОП должны реализовываться одним ОГП. Если сайт, домен или ОП включает пользователей или компьютеры с разными требованиями к политике, попробуйте разделить контейнер на несколько дочерних ОП и распространить на них действие отдельных ОГП.

Внесение изменений требует от администратора больше усилий, чем при многоуровневой структуре ОГП, поскольку приходится модифицировать параметры нескольких ОГП; тем не менее время регистрации в системе сокращается.

Такая модель оптимальна для сред, где пользователей и компьютеры можно разделить на небольшие подгруппы для назначения политик.

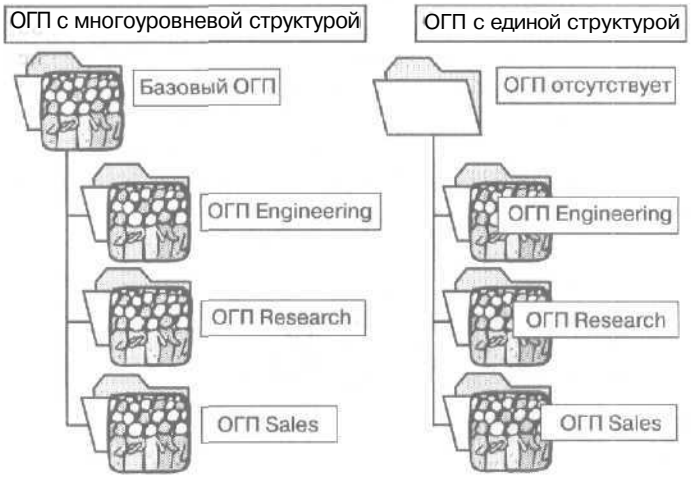


Рис. 12-7. Многоуровневая и единая структура

Структурирование по функциональным ролям и командам

Структура ОП в рамках службы Active Directory разрабатывалась для упрощения администрирования и предоставления полномочий. Структура ОП отражает функциональные роли в организации. При создании групповой политики для организации со структурой ОП, отражающей функциональные роли, следует делегировать полномочия разным уровням ОП. Если структура ОП не отражает разбиение на группы, делегируйте полномочия точно таким же образом, но фильтруйте политику на основе членства в группах безопасности.

Структурирование по функциональным ролям

Основное преимущество данного метода (рис. 12-8) — учет в групповых политиках структуры ОП, отражающей внутренние взаимосвязи в организации. При этом используется минимальное количество ОГП, каждый из которых отражает потребности конкретной группы.

Создайте отдельный ОГП для каждого ОП. Администраторы сети могут определить ACL-разрешения для администрирования ОГП на уровне домена или на уровне отдельных ОП.

Такая модель наилучшим образом подходит для организаций, подразделения которых структурированы по функциональным ролям — в них пользователи разделены на группы со-

гласно выполняемым обязанностям: инженерный отдел, отдел продаж, отдел маркетинга и т. п. Каждой функциональной роли требуются отдельные групповые политики. Архитектура ОП отражает функции, выполняемые организацией.

Структурирование по командам

Цель этого метода — фильтровать политику на основе членства в группах (рис. 12-8). Он применяется в организациях, где широко используется концепция виртуальных команд. Отдельные пользователи создают команды для выполнения различных задач или для совместной работы над проектами; каждый пользователь состоит в нескольких командах. Всем командам требуются разные групповые политики.

Создайте отдельный ОГП для каждой виртуальной команды. Поскольку пользователи в текущий момент времени могут работать лишь в одном ОП, стоит создать один ОГП на вершине иерархии; затем этот объект будет фильтроваться для каждого ОП. После этого создайте ОГП для каждой команды, которой он необходим. Такой способ упрощает администрирование: параметры ОГП применяются лишь в одном месте и администраторы могут централизованно управлять ОГП и уменьшить число объектов групповой политики, назначенныхОП.

Данная модель наилучшим образом подходит для организаций, которым требуется эффективный и гибкий метод управления групповой политикой в динамической среде и в которых архитектура ОП не отражает структуру команд.

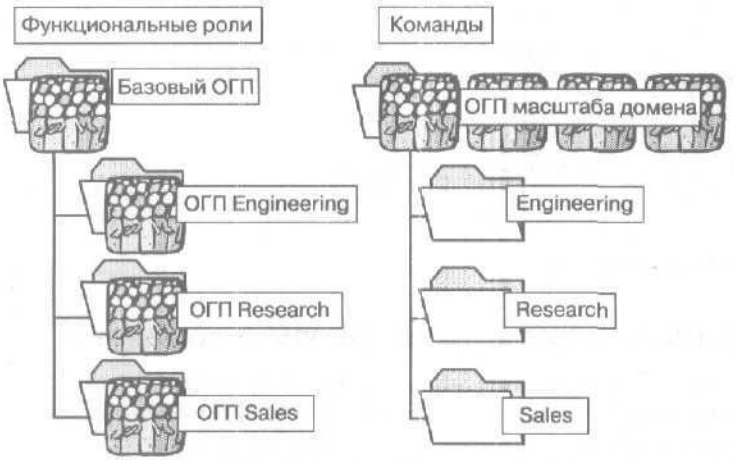


Рис. 12-8. Структурирование по функциональным ролям и командам

Делегирование управления ОП с центральным или распределенным администрированием

Права администрирования ОП можно делегировать, и в некоторых случаях администраторы ОП должны обладать правами, которые позволили бы им блокировать групповые политики, назначенные их ОП на более высоком уровне сетевой иерархии. Тем не менее параметры некоторых политик реализуются в обязательном порядке, и администраторы не смогут заблокировать их. Этого можно достичь как в централизованной, так и в распределенной структуре управления.

Централизованное администрирование

В этом методе административные полномочия делегируются администраторам ОП и сохраняется централизованное управление (рис. 12-9).

Задайте для ОП параметр No Override (Не перекрывать). Например, создайте ОГП, содержащий лишь параметры безопасности домена, и затем установите параметр No Override, чтобы эти параметры распространялись на все дочерние ОП. Для политик других типов права управления в отношении ОГП можно делегировать администраторам конкретных ОП.

Такая модель оптимальна для организаций, где администрирование ОП делегируется, а действие определенных групповых политик (например, некоторых политик безопасности) должно распространяться на весь домен.

Распределенное управление

Здесь администраторы ОП могут блокировать распространение параметров групповой политики на их подразделение (рис. 12-9). Однако администратору запрещено блокировать наследование политик с параметром No Override.

Создайте ОГП для каждого ОП. Определите ACL-разрешения, предоставляющие администратором полный контроль над ОГП. Затем задайте для каждого ОП параметр Block Policy Inheritance (Блокировать наследование политики).

Такая модель наилучшим образом подходит для организаций, которые хотели бы уменьшить число доменов, сохранив при этом автономность администрирования ОП. Данная модель позволяет администраторам распространить действие определенных групповых политик на весь домен.

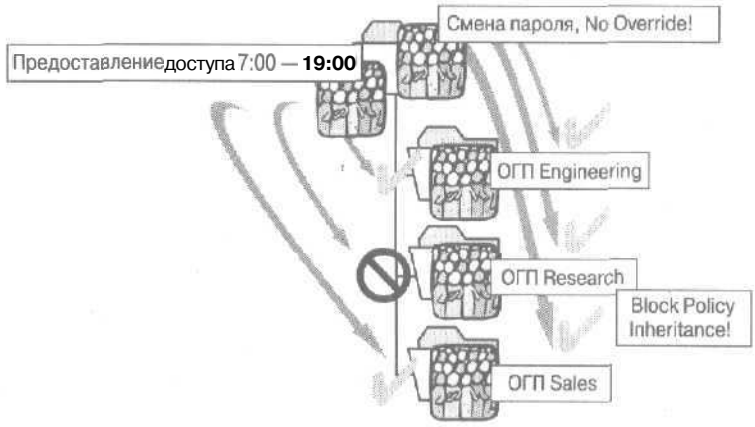


Рис. 12-9. Централизованное и распределенное управление

Резюме

Можно создавать ОГП, содержащие параметры одного или нескольких типов. Кроме того, ОГП могут включать лишь конфигурационные параметры компьютера или пользовательские параметры.

Здесь описаны разные стратегии внедрения групповой политики. Многоуровневая структура ОГП наилучшим образом подходит для сред, где разные группы организации предъявляют общие требования к безопасности и где часто изменяются параметры групповой политики. Единая структура ОГП оптимальна для сред, где пользователей и компьютеры можно разделить на небольшие подгруппы для назначения политик.

Структурирование по функциональным ролям наилучшим образом подходит для компаний, в которых пользователи разделены на группы по обязанностям: инженерный отдел, отдел сбыта, отдел маркетинга и т. д. Структурирование по командам оптимально для организаций, которым требуется эффективный и гибкий метод управления групповой политикой в динамической среде и в которых архитектура ОП не отражает структуру команд.

Централизованное управление наилучшим образом подходит для организаций, в которых администрирование ОП делегируется и необходимо, чтобы действие определенных групповых политик (например, некоторых политик безопасности) распространялось на весь домен. Распределенное управление оптимально, когда необходимо уменьшить число доменов, сохранив при этом автономность администрирования ОП.

Занятие 3, Внедрение групповой политики

Средствами групповой политики можно развернуть в организации конфигурационные параметры. Сейчас вы узнаете о задании групповой политики с использованием вкладки Group Policy и оснастки Group Policy. Вы также научитесь редактировать групповую политику.

Изучив материал этого занятия, вы сможете:

- ✓ внедрить и настроить групповую политику.

Продолжительность занятия — около 60 минут.

Развертывание групповой политики

Задач по внедрению групповой политики несколько:

1. создание ОГП;
2. создание консоли для ОГП;
3. предоставление прав управления ОГП;
4. определение параметров групповой политики для ОГП;
5. отключение неиспользуемых параметров групповой политики;
6. настройка всех исключений в порядке обработки ОГП;
7. фильтрование области действия ОГП;
8. привязка ОГП к сайту, домену или ОП.

Создание ОГП

Первый этап внедрения групповой политики — создание ОГП. Как вы помните, ОГП представляет собой набор параметров групповой политики.

► **Создание ОГП**

1. Определите, ОГП какого типа вы хотите создать.
   - Чтобы создать ОГП для к домена или ОП, откройте оснастку Active Directory Users and Computers.
   - Чтобы создать ОГП для сайта, откройте оснастку Active Directory Sites and Services.
2. Щелкните правой кнопкой мыши сайт, домен или ОП, для которого требуется создать ОГП, и выберите команду Properties (Свойства). Затем перейдите на вкладку Group Policy (Групповая политика) (рис. 12-10).
3. Щелкните кнопку New (Создать) и введите имя нового ОГП.

   По умолчанию новый ОГП сопоставляется текущему сайту, домену или ОП в консоли MMC, и его параметры будут распространяться на этот сайт, домен или ОП.
4. Щелкните кнопку Close (Закрыть).

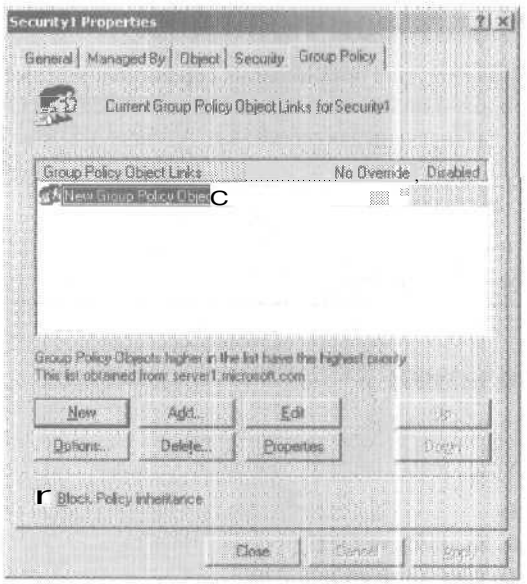


Рис. 12-10. Вкладка Group Policy (Групповая политика)

Создание консоли для ОГП

После создания ОГП вам необходимо добавить оснастку Group Policy в MMC и создать отдельную консоль для управления ОГП. Сохранив созданную консоль, вы всегда сможете открыть ее из программной группы Administrative Tools (Администрирование).

► **Создание консоли для ОГП**

1. Раскройте меню Start (Пуск) и выберите команду Run (Выполнить).
2. В поле Open (Открыть) диалогового окна Run (Запуск программы) введите **mmc** и щелкните OK.
3. В меню Console (Консоль) новой консоли выберите команду Add/Remove Snap-In (Добавить/удалить оснастку).
4. В открывшемся окне щелкните кнопку Add (Добавить).
5. В диалоговом окне Add Standalone Snap-In (Добить изолированную оснастку) щелкните Group Policy (Групповая политика) и затем — кнопку Add.
6. В окне Select Group Policy Object (Выбор объекта групповой политики) щелкните кнопку Browse (Обзор), чтобы выбрать ОГП, для которого создается оснастка.
7. В окне Browse For A Group Policy Object перейдите на вкладку All, щелкните имя ОГП, а затем — OK.
8. В окне Select Group Policy Object щелкните кнопку Finish (Готово), а затем — кнопку Close (Закрыть) в окне Add Standalone Snap-In.
9. В диалоговом окне Add/Remove Snap-In щелкните OK.
10. В меню Console выберите команду Save As (Сохранить как).
11. В поле File Name (Имя файла) введите имя ОГП и щелкните кнопку Save (Сохранить). Теперь вы можете настраивать данный ОГП, вызвав консоль из меню Administrative Tools.

Делегирование прав управления ОГП

После создания ОГП важно определить, какие группы и администраторы обладают правами доступа к этому объекту. Разрешения доступа по умолчанию перечислены в табл. 12-2.

Табл. 12-2. Разрешения ОГП по умолчанию

Группа безопасности	Параметры по умолчанию
Authenticated Users (Прошедшие проверку)	Разрешения Read (Чтение), Apply Group Policy (Применение групповой политики) и Special (Особые)
CREATOR OWNER (Создатель-владелец)	Разрешения Special (Особые)
Domain Administrators (Администраторы домена)	Разрешения Read (Чтение), Write (Запись), Create All Child Objects (Создание всех дочерних объектов), Delete All Child Objects (Удаление всех дочерних объектов) и Special
Enterprise Administrators (Администраторы предприятия)	Разрешения Read, Write, Create All Child Objects, Delete All Child Objects и Special
SYSTEM (Система)	Разрешения Read, Write, Create All Child Objects, Delete All Child Objects и Special

По умолчанию администратор не может удалить ОГП Default Domain Policy. Это позволяет исключить случайное удаление ОГП, содержащего важные параметры домена.

При работе с ОГП из стандартной консоли, например Active Directory Users And Computers, мастер делегирования позволяет лишь управлять параметрами безопасности объекта; предоставить с его помощью права управления объектом нельзя.

▶ **Предоставление прав управления ОГП**

1. Откройте оснастку Group Policy для ОГП.
2. Щелкните корневой узел консоли правой кнопкой мыши и выберите команду Properties.
3. Перейдите на вкладку Security (Безопасность) и выберите группу безопасности, которой требуется предоставить или заблокировать административный доступ к ОГП (рис. 12-11).
   Для изменения списка групп безопасности, которым необходимо предоставить или заблокировать административный доступ к ОГП, воспользуйтесь кнопками Add и Remove.
4. Чтобы предоставить полные права управления ОГП, разрешите чтение и запись
   Пользователь или администратор, не имеющий разрешения Write, не сможет просмотреть параметры ОГП средствами оснастки Group Policy. Для открытия ОГП все расширения оснастки Group Policy требуют наличия разрешения Write.
5. Щелкните OK.

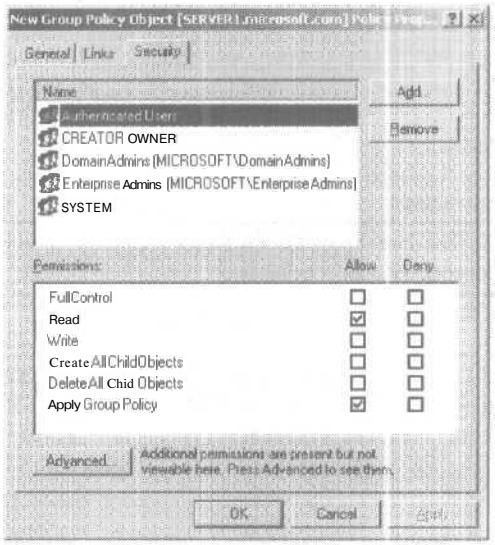


Рис. 12-11. Вкладка Security (Безопасность) окна свойств ОГП

Определение параметров групповой политики

Создав ОГП и указав, кто из администраторов обладает правами доступа к данному объекту, определите параметры групповой политики.

► **Определение параметров групповой политики для ОГП**

1. Откройте оснастку Group Policy для ОГП (рис. 12-12).

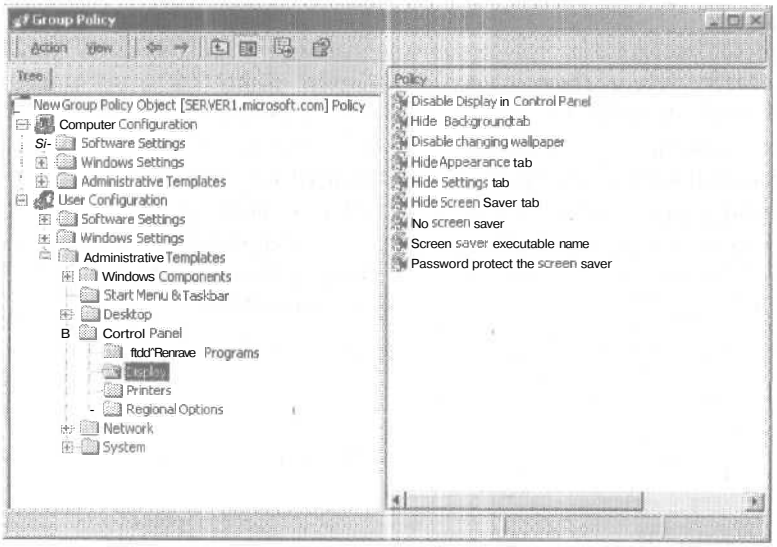


Рис. 12-12. Оснастка Group Policy

2. В дереве консоли раскройте узел требуемой групповой политики.

Например, на рис. 12-12 раскрыты узлы User Configuration (Конфигурация пользователя), Administrative Templates (Административные шаблоны), Control Panel (Панель управления) и Display (Экран).

3. В правой панели щелкните требуемую политику правой кнопкой мыши и выберите в контекстном меню команду Properties. На рис. 12-13 в правой панели выбрана политика Hide Screen Saver Tab (Скрыть вкладку выбора заставки).
4. Щелкните Enabled (Включена), чтобы применить политику к пользователям и компьютерам, относящимся к данному ОГП, и затем щелкните OK.

   Not Configured (Не задана) означает, что в реестр не будут вноситься изменения, связанные с данным параметром. Disabled (Отключена) указывает, что политика не распространяется на пользователей и компьютеры, относящиеся к данному ОГП.

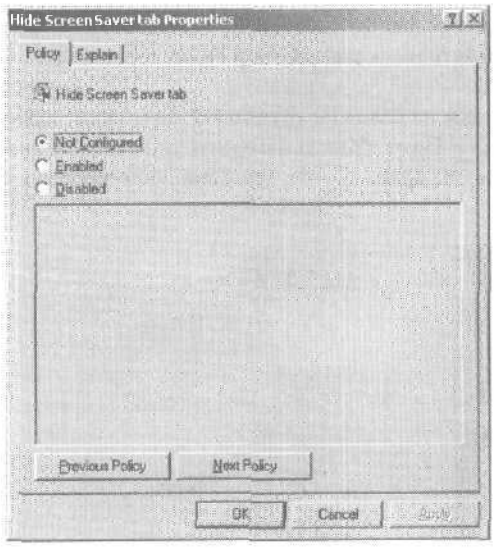


Рис. 12-13. Скрытие вкладки выбора программы-заставки

Отключение неиспользуемых параметров групповой политики

Если в узле Computer Configuration или User Configuration объекта групповой политики для всех параметров указано Not Configured (Не задана), то для предотвращения их обработки узел можно отключить. Это ускоряет загрузку и регистрацию в системе пользователей и компьютеров, на которые распространяется действие ОГП.

▶ **Отключение узла Computer Configuration или User Configuration ОГП**

1. Откройте оснастку Group Policy для ОГП.
2. Щелкните корневой узел консоли правой кнопкой мыши и выберите команду Properties.
3. На вкладке General диалогового окна свойств:
   - чтобы отключить узел Computer Configuration, щелкните флажок Disable Computer Configuration Settings (Отключить параметры конфигурации компьютера);
   - чтобы отключить узел UserConfiguration, щелкните флажок Disable User Configuration Settings (Отключить параметры конфигурации пользователя).
4. Щелкните кнопку OK.

Настройка исключений в порядке обработки ОГП

ОГП обрабатываются в соответствии с иерархией Active Directory; локальный ОГП, ОГП сайта, ОГП домена и ОГП ОП. Порядок обработки параметров групповых политик по умолчанию можно изменить, модифицировав порядок ОГП для объекта, задав параметр Block Policy Inheritance, указав параметр No Override или включив параметр Loopback (Замыкание на себя).

▶ **Изменение порядка обработки ОГП для объекта**

1. Чтобы задать порядок ОГП для домена или ОП, откройте оснастку Active Directory Users and Computers (Active Directory — пользователи и компьютеры). Чтобы изменить порядок ОГП для сайта, откройте оснастку Active Directory Sites and Services (Active Directory — сайты и службы).
2. В дереве консоли щелкните правой кнопкой мыши требуемый сайт, домен или ОП и выберите команду Properties. Затем перейдите на вкладку Group Policy (Групповая политика).
3. В списке Group Policy Object Links (Ссылки на объекты групповой политики) выберите ОГП и с помощью кнопок Up (Вверх) и Down (Вниз) измените приоритет данного ОГП для выбранного сайта, домена или ОП (рис. 12-14). Windows 2000 обрабатывает ОГП, начиная с верхней части списка.

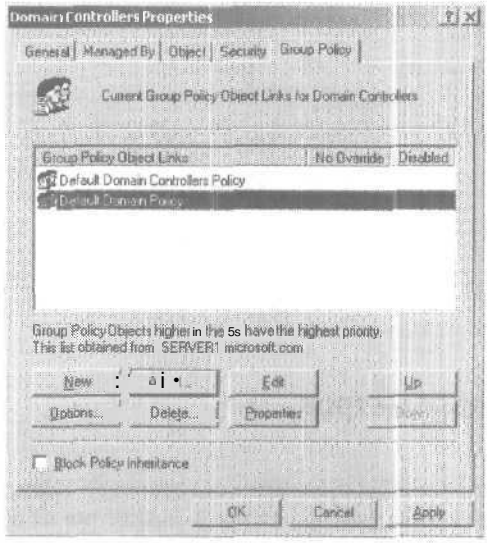


Рис. 12-14, Изменение порядка обработки ОГП

▶ **Запрет наследования политики**

1. Чтобы запретить наследование групповой политики для домена или ОП, откройте оснастку Active Directory Users and Computers. Чтобы запретить наследование политики для сайта, откройте оснастку Active Directory Sites and Services.
2. В дереве консоли щелкните требуемый сайт, домен или ОП правой кнопкой мыши и выберите команду Properties. Затем перейдите на вкладку Group Policy (Групповая политика).
3. Пометьте флажок Block Policy Inheritance (Блокировать наследование политики), чтобы запретить привязку к выбранному сайту, домену или ОП всех ОГП, связанных с

элементами, расположенными выше по иерархии Active Directory. Запретить наследование ОГП, для которых задан параметр No Override (Не перекрывать), нельзя.

▶ **Запрет переопределения параметров политики**

1. Чтобы запретить переопределение параметров групповой политики для домена или ОП, откройте оснастку Active Directory Users and Computers. Чтобы запретить переопределение параметров политики для сайта, откройте оснастку Active Directory Sites and Services.
2. В дереве консоли щелкните правой кнопкой мыши требуемый сайт, домен или ОП и выберите команду Properties. Затем перейдите на вкладку Group Policy.
3. Выберите ОГП и шелкните кнопку Options (Параметры). В диалоговом окне Options (рис. 12-15) шелкните флажок No Override (Не перекрывать), чтобы запретить изменение параметров данного ОГП другими ОГП. После этого щелкните кнопку OK.

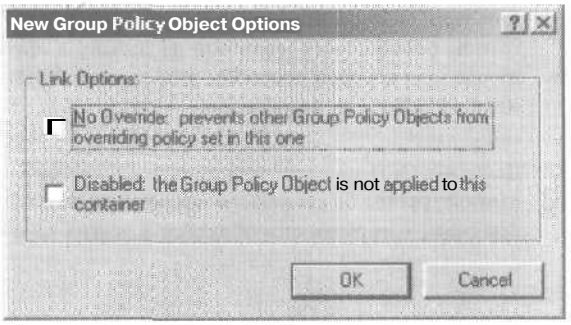


Рис. 12-15. Диалоговое окно Options (Параметры)

▶ **Включение параметра Loopback (Замыкание на себя)**

1. Откройте оснастку Group Policy для ОГП.
2. В дереве консоли раскройте узел Computer Configuration\Administrative Templates\System\Group Policy (Конфигурация компьютера\Административные шаблоны\Система\-Групповая политика).
3. В правой панели дважды шелкните User Group Policy Loopback Processing Mode (Режим обработки замыкания пользовательской групповой политики).
4. В диалоговом окне свойств этой политики шелкните флажок Enabled (Включена).
5. В списке Mode (Режим) выберите требуемый режим:
   - Replace (Замена) — список ОГП для пользователя будет заменен списком ОГП, полученным для системы при загрузке компьютера;
   - Merge (Слияние) — список ОГП, полученный для пользователя при регистрации, будет дополнен списком ОГП, полученным для системы при загрузке компьютера.
6. Щелкните OK.

Фильтрование области действия ОГП

Политики ОГП распространяются только на пользователей, обладающих разрешением Read для данного объекта. Чтобы отфильтровать область действия ОГП, можно создать группы безопасности и назначить отдельным группам разрешения Read. После этого вы исключите требуемые группы из области действия политики, отозвав у них разрешения Read.

► **Фильтрование области действия ОГП**

1. Откройте оснастку Group Policy для ОГП.
2. Щелкните корневой узел дерева консоли правой кнопкой мыши и выберите команду Properties.
3. Перейдите на вкладку Security (Безопасность) и выберите группу безопасности для фильтрования ОГП (рис. 12-11).

   Чтобы изменить список групп безопасности, воспользуйтесь кнопками Add и Remove.
4. Задайте разрешения в соответствии с табл. 12-3 и щелкните OK.

Табл. 12-3. Разрешения для областей действия ОГП

Задача	Необходимые разрешения	Результат
Необходимо применить ОГП к членам этой группы безопасности	Предоставьте им разрешения Allow Group Policy (AGP) и Read	Действие ОГП распространяется на членов данной группы безопасности, если они не состоят в другой группе, для которой отменены разрешения AGP, Read или оба этих разрешения
Члены этой группы безопасности освобождены от этого ОГП	Отмените для них разрешения AGP и Read	Действие ОГП не распространяется на членов данной группы безопасности независимо от разрешений, которыми они обладают в других группах
Членство в этой группе безопасности никак не связано с применением ОГП	Для разрешений AGP и Read не выбирайте значения Allow (Разрешить) или Deny (Запретить)	Действие ОГП распространяется на членов данной группы безопасности, только если они состоят в другой группе, для которой разрешения AGP и Read заданы как Allow. Кроме того, эти лица не должны состоять в группах, для которых разрешение AGP или Read задано как Deny

Привязка ОГП

По умолчанию новый ОГП сопоставляется сайту, домену или ОП, выбранному в консоли MMC в момент его создания, и его параметры распространяются на этот сайт, домен или ОП. Чтобы связать ОГП с дополнительными сайтами, доменами или ОП, воспользуйтесь вкладкой Group Policy диалогового окна свойств требуемого сайта, домена или ОП.

► **Привязка ОГП к сайту, домену или ОП**

1. Для привязки ОГП к домену или ОП откройте оснастку Active Directory Users and Computers. Для привязки ОГП к сайту откройте оснастку Active Directory Sites and Services.
2. В дереве консоли щелкните требуемый сайт, домен или ОП правой кнопкой мыши.
3. Выберите в контекстном меню команду Properties и затем перейдите на вкладку Group Policy (Групповая политика).
4. Если ОГП уже указан в списке Group Policy Object Links (Ссылки на объекты групповой политики), щелкните кнопку Cancel (Отмена). Иначе щелкните кнопку Add (Добавить).
5. В диалоговом окне Add A Group Policy Object Link (Добавить ссылку на объект групповой политики) перейдите на вкладку All (Все), щелкните требуемый ОГП, затем — OK (рис.12-16).

Рис. 12-16. Диалоговое окно Add A Group Policy Object Link (Добавить ссылку на объект групповой политики)

6. В диалоговом окне свойств сайта, домена или ОП щелкните OK.

Изменение групповой политики

Изменение групповой политики подразумевает:

- удаление ссылки на ОГП;
- удаление ОГП;
- изменение ОГП или его параметров.

Удаление ссылки на ОГП

При удалении ссылки ОГП отключается от выбранного сайта, домена или ОП и продолжает храниться в Active Directory, пока не будет удален.

► **Удаление ссылки на ОГП**

1. Для отключения ОГП от домена или ОП откройте оснастку Active Directory Users and Computers. Для отключения ОГП от сайта откройте оснастку Active Directory Sitt:s and Services.
2. В дереве консоли щелкните правой кнопкой мыши требуемый сайт, домен или ОП.
3. Выберите в контекстном меню команду Properties и затем перейдите на вкладку Group Policy.
4. На вкладке Group Policy выберите требуемый ОГП и щелкните кнопку Delete (Удалить).
5. В диалоговом окне Delete (Удаление) щелкните Remove The Link From The List (Изъять ссылку из списка, не удаляя объект).

   ОГП останется в службе Active Directory, однако более не будет связан с сайтом, доменом или ОП.

Удаление ОГП

ОГП удаляется из службы Active Directory и перестает действовать на все сайты, домены и ОП, с которыми он связан. Вы, вероятно, захотите просто удалить ссылку на ОГП — отключить ОГП от ОП, не удаляя сам объект из Active Directory.

> **Удаление ОГП**

1. Для удаления ОГП из домена или ОП откройте оснастку Active Directory Users and Computers. Для удаления ОГП из сайта откройте оснастку Active Directory Sites and Services.
2. В дереве консоли щелкните правой кнопкой мыши требуемый сайт, домен или ОП.
3. Выберите в контекстном меню команду Properties и затем перейдите на вкладку Group Policy.
4. На вкладке Group Policy выберите требуемый ОГП и щелкните кнопку Delete (Удалить).
5. В диалоговом окне Delete щелкните Remove The Link And Delete The Group Policy Object Permanently (Изъять ссылку из списка и окончательно удалить объект групповой политики). Затем щелкните OK.

   ОГП будет удален из службы каталогов Active Directory.

Изменение ОГП или его параметров

Чтобы изменить ОГП или его параметры, выполните описанные ранее процедуры создания ОГП и определения параметров групповой политики.

Практикум: развертывание групповой политики

Сейчас вы реализуете групповую политику для своего домена. В упражнениях I — 8 вы создадите ОГП, консоль ОГП, предоставите административные полномочия, определите параметры групповой политики, отключите неиспользуемые параметры, настроите исключения в порядке обработки ОГП, отфильтруете область действия ОГП и сопоставите ОГП дополнительному ОП. В упражнении 9 вы проверите созданную групповую политику.

Упражнение 1: создание ОГП

Сейчас вы создадите ОГП на уровне ОП.

> **Задание: создайте ОГП для собственного ОП**

1. Зарегистрируйтесь в домене как Administrator (Администратор).
2. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers.
3. Дважды щелкните microsoft.com (или имя вашего домена).
4. Создайте новый ОП с именем Dispatch.
5. Щелкните ОП Dispatch правой кнопкой мыши, выберите команду Properties и перейдите на вкладку Group Policy.
6. Щелкните кнопку New (Создать) и введите имя нового ОГП — **DispatchPolicy.**
7. Щелкните Close.

Упражнение 2: создание консоли ОГП

Вы создадите консоль для ОГП DispatchPolicy. Сохранив консоль, вы всегда сможете открыть ее из меню Administrative Tools.

> **Задание: создайте консоль ОГП DispatchPolicy**

1. В меню Stan выберите команду Run.
2. В поле Open (Открыть) введите mmc и щелкните OK.

   Откроется новая консоль управления.
3. В меню Console выберите команду Add/Remove Snap-In.

   Откроется одноименное диалоговое окно.

4. Щелкните кнопку Add.

   Откроется диалоговое окно Add Standalone Snap-In.

5. Щелкните Group Policy и затем — кнопку Add.

   Откроется окно Select Group Policy Object.

6. Щелкните кнопку Browse (Обзор), чтобы найти ОГП DispatchPolicy.
7. В открывшемся окне перейдите на вкладку All (Все), щелкните ОГП Dispatch Policy, затем OK.
8. Щелкните кнопку Finish (Готово), затем — кнопку Close (Закрыть) в диалоговом окне Add Standalone Snap-In.
9. В диалоговом окне Add/Remove Snap-In щелкните OK.
10. В меню Console выберите команду Save As (Сохранить как).
11. В окне Save As (Сохранить как) в поле File Name (Имя файла) введите **Dispatch Policy GPO** и щелкните кнопку Save (Сохранить).

    Ярлык для оснастки DispatchPoticy GPO появится в программной группе Administrative Tools (Администрирование).

Упражнение 3: делегирование управления ОГП

Вы предоставите группе Administrators административные полномочия в отношении ОГП DispathPolicy.

► **Задание: делегируйте управление ОГП**

1. Откройте консоль ОГП Dispatch Policy.
2. Щелкните корневой узел (DispatchPolicy [server1.microsoft.com] Policy) консоли правой кнопкой мыши, выберите команду Properties и перейдите на вкладку Security (Безопасность).

   Откроется диалоговое окно свойств для ОГП DispathPolicy.

   Какие группы безопасности обладают административными полномочиями в отношении ОГП Dispatch Policy?

3. Добавьте группу Administrators (Администраторы), щелкнув кнопку Add.
4. Чтобы предоставить группе Administrators полные административные полномочия, предоставьте разрешения Read, Write, Create All Child Objects и Delete All Child Objects.
5. Щелкните OK.

Упражнение 4: определение параметров групповой политики

Вы настроите некоторые параметры ОГП DispatchPolicy.

► **Задание: настройте параметры групповой политики для ОГП**

1. В дереве консоли ОГП DispatchPolicy раскройте корневой узел.
2. Раскройте узел User Configuration\Administrative Templates (Конфигурация пользователя\Административные шаблоны).
3. Щелкните элемент Start Menu & Task Bar (Панель задач и меню «Пуск»).

   Что отображается в правой панели?

4. В правой панели дважды щелкните Remove Search Menu From Start Menu (Удалить меню «Найти» из главного меню).

   Откроется одноименное диалоговое окно.

5. Щелкните переключатель Enabled (Включена), затем — OK.

   Как быстро определить, что этот параметр включен?

6. Повторите пункты 4 и 5, чтобы включить политику Remove Run Menu From Start Menu (Удалить команду «Выполнить» из меню «Пуск») (там же, в узле User Configuration).
7. В дереве консоли раскройте узел System (Система) и щелкните Logon/Logoff (Вход/выход из системы).

   В правой панели отобразятся соответствующие политики.
8. В правой панели дважды щелкните политику Disable Lock Computer (Запретить блокировку компьютера), затем — OK.

Упражнение 5: отключение неиспользуемых параметров групповой политики

Вы отключите узел Computer Configuration дерева консоли, поскольку все параметры в нем не заданы. Это ускорит загрузку и регистрацию в системе пользователей и компьютеров, на которые распространяется действие вашего ОГП.

▶ **Задание: отключите узел Computer Configuration для вашего ОГП**

1. Откройте консоль Dispatch Policy, щелкните корневой узел правой кнопкой мыши и выберите команду Properties.

   Откроется диалоговое окно свойств ОГП Dispatch Policy.
2. На вкладке General щелкните Disable Computer Configuration Settings (Отключить параметры конфигурации компьютера).

   Откроется диалоговое окно Confirm Disable (Подтвердить отключение), предлагающее подтвердить отключение *узла* Computer Configuration.
3. Щелкните Yes (Да), затем OK.

Упражнение 6: выявление исключений в порядке обработки ОГП

Вы настроите ОГП DispatchPolicy так, чтобы другие ОГП не могли переопределять его параметры.

▶ **Задание: задание параметра No Override для вашего ОГП**

1. Раскройте меню Start\Programs\Administrative TooIs\Active Directory Users And Computers.
2. Щелкните ОП Dispatch правой кнопкой мыши и выберите команду Properties.
3. Перейдите на вкладку Group Policy, щелкните ОГП DispatchPolicy и затем — кнопку Options (Параметры).

   Откроется одноименное диалоговое окно.
4. Щелкните флажок No Override (Не перекрывать), затем — OK.
5. В диалоговом окне свойств ОГП Dispatch щелкните OK.

Упражнение 7: фильтрование области действия ОГП

Вы заблокируете наследование политики для группы Sales, отозвав у последней разрешение Read для ОГП. Группа Sales и ее участники были созданы при выполнении упражнений главы 8.

▶ **Задание: отфильтруйте область действия ОГП**

1. Щелкните корневой узел консоли ОГП DispatchPolicy правой кнопкой мыши и выберите команду Properties.

   Откроется одноименное диалоговое окно.
2. Перейдите на вкладку Security и щелкните группу безопасности Sales. Вам надо будет добавить данную группу с помощью кнопки Add.

3. Отмените для группы Sales разрешения Apply Group Policy и Read. Затем щелкните OK.
   Откроется диалоговое окно, предлагающее подтвердить отзыв разрешений.
4. Щелкните кнопку Yes,

Упражнение 8: привязка ОГП

По умолчанию параметры ОГП Dispatch Policy распространяются на ОП Dispatch. Вы создадите ссылку на ОГП DispatchPolicy для ОП Security 1, созданного в главе 11.

▶ **Задание: сопоставьте ОГП дополнительному ОП**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers.
2. Щелкните ОП Security 1 правой кнопкой мыши и выберите команду Properties
   Откроется одноименное диалоговое окно.
3. Перейдите на вкладку Group Policy и щелкните кнопку Add.
   Откроется диалоговое окно Add A Group Policy Object Link (Добавить ссылку на объект групповой политики).
4. Перейдите на вкладку All (Все), щелкните ОГП DispatchPolicy, затем — OK.
5. В диалоговом окне свойств ОП Security ! щелкните OK.

Упражнение 9: тестирование ОГП

Сейчас вы проверите, как работает созданный вами ранее ОГП.

▶ **Задание: проверьте ОГП DispatchPolicy**

1. Зарегистрируйтесь в системе как Assistant 1, член ОП Security1.
2. Нажмите комбинацию клавиш Ctrl+Alt+Delete.
   Откроется диалоговое окно Windows Security (Безопасность Windows).
   Можете ли вы заблокировать рабочую станцию? Почему?
3. Щелкните кнопку Cancel (Отмена) и раскройте меню Start.
   Отображаются ли в меню Start команды Search (Найти) и Run (Выполнить)?
4. Завершите сеанс работы Assistantl и затем зарегистрируйтесь в системе как Administrator.
5. Сделайте учетную запись Assistantl членом группы безопасности Sales.
6. Завершите сеанс работы Administrator и затем зарегистрируйтесь в системе как Assistant 1.
7. Нажмите комбинацию клавиш Ctrl+Alt+Delete.
   Можете ли вы заблокировать рабочую станцию? Почему?
8. Завершите текущий сеанс работы.

Резюме

Вы изучили этапы внедрения групповой политики: создание ОГП, создание консоли ОГП, делегирование административных полномочий на управление ОГП, определение параметров групповой политики, отключение неиспользуемых параметров, настройку исключений в порядке обработки ОГП, фильтрование области действия ОГП и привязку ОГП к сайту, домену или ОП.

Выполняя практическую часть занятия, вы назначили групповую политику в своем домене, создав ОГП, консоль ОГП, делегировав полномочия в отношении ОГП, определив параметры групповой политики, отключив неиспользуемые параметры, настроив исключения в порядке обработки ОГП, отфильтровав область действия ОГП и сопоставив ОГП дополнительному ОП. Кроме того, вы проверили работу ОГП.

Занятие 4, Управление программным обеспечением с помощью групповой политики

Расширение Software Installation (Установка программ) — основная функция Windows 2000, с помощью которой администратор управляет программным обеспечением в организации. При этом пользователям предоставляется немедленный доступ к ПО, необходимому им для выполнения различных задач; кроме того, пользователям гарантируется простота и удобство работы в течение жизненного цикла ПО. Теперь пользователям не надо искать сетевые ресурсы или компакт-диски, не придется им и самостоятельно устанавливать и обновлять ПО. На этом занятии рассказывается о внедрении Software Installation.

Изучив материал этого занятия, вы сможете:

- ✓ развернуть ПО с помощью групповой политики;
- ✓ настроить параметры развертывания;
- ✓ поддерживать ПО с помощью групповой политики

Продолжительность занятия — около 75 минут.

Средства управления программным обеспечением

В Windows 2000 Server имеется три утилиты для установки и поддержки ПО (табл. 12-4)

Табл. **12-4.** Утилиты для установки и поддержки ПО в Windows 2000

Средство	Назначение
Расширение Software Installation (Установка программ) оснастки Group Policy (Групповая политика)	Используется администраторами для управления ПО
Windows Installer (Установщик Windows)	Устанавливает ПО, упакованное в файлы формата Windows Installer
Программа Add/Remove Programs (Установка и удаление программ) из Control Panel (Панель управления)	Применяется пользователями для управления ПО на собственных компьютерах

Расширение Software Installation

Это основной инструмент, применяемый администраторами для управления ПО в организации. Software Installation работает совместно с групповой политикой и службой Active Directory, реализуя основанную на групповых политиках систему администрирования ПО, позволяющую централизованно управлять:

- начальным развертыванием ПО;
- обязательными и необязательными обновлениями, а также пакетами исправлений. Вы сможете обновить версию приложения или заменить его или же обновить ОС с помощью сервисных пакетов;
- удалением ПО.

Software Installation позволяет централизованно управлять установкой приложений на клиентской системе, назначая приложения пользователям и компьютерам или публикуя

приложения пользователям. Обязательное или необходимое ПО пользователям и компьютерам следует *назначать* (assign). А необязательное ПО следует *публиковать* (publish).

Назначение обязательных приложений

Если приложение необходимо установить на компьютере, пользователю предлагается это сделать при следующем входе на рабочую станцию. Оповещение приложения пользователь получит независимо от того, на каком компьютере он работает в настоящее время. Установка приложения начинается, как только пользователь первый раз активизирует приложение на компьютере, выбрав его в меню Start или открыв связанный с ним документ.

Приложение, которое необходимо установить на компьютере, устанавливается, когда это безопасно — обычно при запуске компьютера, дабы не возникла конфликтная ситуация.

Публикация приложений

Опубликованное приложение не появляется среди установленного на компьютерах ПО. Ни на рабочем столе, ни в меню Start ярлыков не видно, и в локальный реестр на компьютерах пользователей изменения не вносятся. Вместо этого опубликованные приложения хранят свои атрибуты оповещения в хранилище Active Directory. Затем информация, например имя приложения и файловые ассоциации, предоставляется пользователям в контейнере Active Directory. Когда пользователь решит установить приложение, ему достаточно щелкнуть значок Add/Remove Programs в Control Panel или файл, связанный с приложением (например, .xls для Microsoft Excel).

Как работает расширение Software Installation

Расширение Software Installation систематически обслуживает ПО с помощью службы Windows Installer (Установщик Windows), которая позволяет ОС управлять процессом установки. Windows Installer включает три основных компонента:

- службу ОС, выполняющую установку, изменение и удаление в соответствии с информацией из пакета Windows Installer;
- пакет установки — БД реляционного типа, в которой хранятся все инструкции и данные, описывающие состояние установленного приложения;
- API-интерфейс, позволяющий приложениям взаимодействовать с Windows Installer для добавления или удаления дополнительных компонентов после завершения начальной установки приложения.

Поскольку Software Installation взаимодействует с Windows Installer, пользователи могут работать с *самовосстанавливающимися* (self-repairing) приложениями. Windows Installer определяет, что один из файлов приложения отсутствует, и немедленно копирует отсутствующие или поврежденные файлы, то есть восстанавливая приложение.

Пакет установки — это файл, содержащий все инструкции и данные, необходимые для установки или удаления программы. Разработчик приложения создает .msi-файл пакета Windows Installer и поставляет его с приложением. Если такой файл с приложением не поставляется, попробуйте создать его самостоятельно или заново упакуйте программу с помощью утилит сторонних фирм.

Развертывать приложения с помощью Software Installation стоит, только если файл относится к одному из перечисленных ниже типов:

- собственные файлы пакетов Windows Installer (.msi). Их обычно распространяют поставщики ПО для упрощения установки определенных приложений;
- файлы заново упакованных приложений (.msi) позволяют повторно упаковывать приложения, не имеющие родных пакетов Windows Installer, точно так же, как вы упаковываете обычные программы для дальнейшей установки;

- файлы существующей программы установки(.zap) — устанавливают приложение с использованием оригинального файла SETUP.EXE.

Кроме того, вы можете корректировать порядок установки пакета Windows Installer в момент назначения или публикации. Эти *преобразования* (modifications) сохраняются в виде файлов с расширением .mst.

При работе с Software Installation вам могут **также встретиться** следующие **файлы:**

- исправления (.msp) — содержат исправленные ошибки, пакеты обновлений и другие похожие файлы;
- сценарии назначения приложений (.aas) — содержатинструкции по назначению и публикации пакетов.

Настройка пакетов Windows Installer

Можно управлять процессом установки, применяя файлы *преобразования* (modifications) к установочной базе данных. Преобразования делают изменения элементами базы данных. Некоторые приложения предоставляют специальные мастера, позволяющие создавать преобразования.

Например, в пакете Microsoft Office 2000 для создания преобразований предусмотрен мастер Customization, позволяющий управлять конфигурацией этого пакета при развертывании его пользователям. Преобразование может включать Microsoft Word в качестве ключевого элемента и копировать его при первой установке. Возможности, используемые реже, например проверка версий и конвертеры документов, устанавливаются при первом запросе, а другие компоненты, например набор картинок, в некоторых случаях не устанавливаются вообще. В вашей воле также создать другое преобразование, устанавливающее все компоненты Word и не устанавливающее Microsoft PowerPoint. Точный состав устанавливаемых компонентов зависит от конечных пользователей и от того, как они работают с приложениями.

Внедрение Software Installation

При внедрении Software Installation необходимо предусмотреть:

1. планирование и подготовку установки приложений;
2. настройку точки распространения приложений;
3. выбор параметров по умолчанию, используемых при установке приложений;
4. порядок развертывания приложений;
5. выбор параметров автоматической установки;
6. **создание категорий программ;**
7. настройку свойств приложений;
8. управление приложениями.

Планирование и подготовка установки приложений

Планируя установку приложений:

- изучите требования организации к ПО на основе организационной структуры в Active Directory, а также имеющихся ОГП;
- определите порядок развертывания;
- создайте пилотный проект, чтобы проверить порядок назначения или публикации приложений;
- подготовьте приложения таким образом, чтобы они соответствовали требованиям организации. Проверьте все пакеты Windows Installer и заново упакованное ПО.

В табл. 12-5 описываются способы внедрения установки приложений. Некоторые из них могут показаться противоречивыми — выбирайте лишь те из них, что соответствуют вашим бизнес-целям.

Табл. 12-5. Способы внедрения установки приложений

Способ	Особенности
Создание ОП в соответствии с потребностями управления приложениями	Вы сможете развертывать приложения для определенных групп пользователей. Параметры безопасности групповой политики в некоторых случаях не распространяются на эту Группу лиц
Развертывание приложений на высоком уровне иерархии дерева Active Directory	Упрощает доступ пользователей к приложению. Кроме того, снижает нагрузку на администратора, поскольку в этом случае достаточно развернуть лишь один ОГП вместо того, чтобы многократно создавать его в контейнерах, расположенных ниже по иерархии Active Directory
Развертывание нескольких приложений с помощью одного ОГП	Снижает нагрузку на администратора — вы сможете создавать и управлять одним, а не несколькими ОГП. Регистрация в системе происходит быстрее, так как обработка одного ОГП, развертывающего 10 приложений, осуществляется быстрее, чем обработка 10 ОГП, развертывающих по одному приложению. Данный способ подходит для организаций, где пользователям требуется одинаковый набор основных приложений
Только один раз назначать или публиковать установленные программы в ОГП или наборе ОГП, распространяющемся на пользователя/компьютер	В этом случае легче определить, какой экземпляр приложения распространяется на пользователя/компьютер

Для приложений сторонних поставщиков, распространяемых через *точки распространения программ* (software distribution point, SDP), необходимы лицензии. Ответственность за соответствие количества пользователей, одновременно обращающихся к приложению, и имеющегося числа лицензий, лежит целиком на вас. Вы также отвечаете за то, что приложение используется согласно рекомендациям независимого поставщика.

Соберите форматы пакетов ПО и внесите необходимые изменения.

Настройка точки распространения приложений

Следующий этап после подготовки и планирования управления ПО: копирование программ на одну или несколько SDP — мест в сети, с которых пользователи могут получить необходимое ПО.

▶ **Настройка SDP**

1. Создайте на файловом сервере, который будет считаться точкой SDP, папки для программ и откройте к ним общий доступ в сети. Например, *\\сервер\общий_ресурс*.
2. Реплицируйте ПО на SDP, поместив или скопировав программы, пакеты, преобразования, необходимые файлы и компоненты в общие папки. Помещайте каждое приложение (пакет и все связанные файлы установки) в отдельную папку SDP.
3. Задайте для папок SDP административные разрешения, чтобы изменять файлы имели право только администраторы (Read и Write), а пользователи обладали разрешениями

лишь на считывание файлов. Для управления приложениями в соответствующем ОГП применяйте групповую политику.

Примечание Некоторые приложения поддерживают специальные команды, упрощающие создание SDP. Например, для подготовки Microsoft Office следует набрать в командной строке SETUP /A. После этого вы сможете ввести ключ приложения сразу для всех пользователей, а также указать размещение сетевой папки (SDP), куда следует скопировать файлы установки. В прочих приложениях предусмотрены иные способы для разархивирования сжатых файлов с носителей распространения, а также для копирования установочных файлов в папки распространения.

Выбор параметров по умолчанию, используемых при установке приложений

ОГП может включать некоторые параметры, влияющие на установку, управление и удаление приложения. Для глобального определения параметров новых пакетов в ОГП воспользуйтесь вкладкой General (Общие) диалогового окна свойств Software Installation. Затем некоторые из этих свойств разрешается изменить, отредактировав свойства пакета в расширении Software Installation.

▶ **Определение параметров по умолчанию, используемых при установке приложений**

1. Откройте оснастку Group Policy (Групповая политика) и затем в узле Computer Configuration (Конфигурация компьютера) или User Configuration (Конфигурация пользователя) откройте папку Software Settings (Конфигурация программ).
2. Щелкните узел Software Settings правой кнопкой мыши и выберите команду Properties.
3. В диалоговом окне Software Installation Properties (Свойства: Установка программ) на вкладке General (Общие) в поле Default Package Location (Расположение по умолчанию для новых программ) укажите для пакетов (файлы .msi) путь к SDP по умолчанию (рис. 12-17).

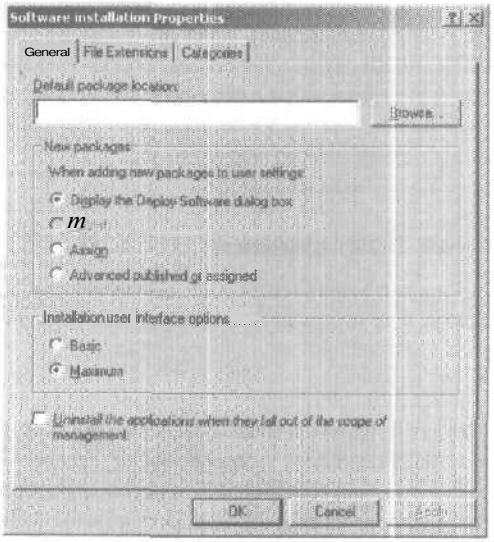


Рис. 12-17. Вкладка General (Общие) окна Software Installation Properties

4. В области New Packages (Добавление новых программ) выберите один из следующих параметров:
   - **Display The Deploy Software Dialog Box** (Открывать диалоговое окно «Развертывание программ») — при добавлении нового пакета откроется диалоговое окно, где можно назначить, опубликовать или изменить свойства пакета;
   - **Publish** (Запускать мастер «Установка и удаление программ») — новый пакет публикуется со стандартными свойствами. Пакеты предназначены лишь пользователям, но не компьютерам. Если пакет добавляется в узле Computer Configuration оснастки Group Policy, переключатель Publish недоступен.
   - Assign (Назначать программам ярлыки в главном меню) — новый пакет назначается со стандартными свойствами. Пакеты предназначены как пользователям, так и компьютерам.
   - **Advanced Published Or Assigned** — при добавлении нового пакета откроется форма Configure Package Properties.
5. В области Installation User interface Options (Пользовательский интерфейс при установке) выберите один из следующих параметров:
   - **Basic** (Простой) — отображаются лишь основные сообщения и окна мастера установки.
   - **Maximum** (Полный) — при установке пакета отображаются все сообщения и окна.
6. Щелкните флажок, чтобы указать, что после того, как ОГП перестанет распространяться на пользователей/компьютеры, пакет должен быть удален.
7. Щелкните OK.

Развертывание приложений

Программы можно назначать или публиковать для пользователей и компьютеров, и вы вправе создать рабочую комбинацию, предназначенную для решения ваших задач управления ПО. В табл. 12-6 описываются различные способы развертывания программ,

Табл. 12-6. Способы развертывания приложений

Способ	Публикация (только пользователям)	Назначение (пользователям)	Назначение (компьютерам)
По завершении развертывания ПО доступно для установки после:	Следующего входа в систему	Следующего входа в систему	Следующего запуска компьютера
Обычно пользователь устанавливает приложение с помощью:	Программы Add/Remove Programs из Control Panel	Меню Start или ярлыка на рабочем столе	ПО уже установлено (приложение автоматически устанавливается при перезагрузке компьютера)
Если приложение не установлено и пользователь открывает связанный с этим приложением файл, приложение:	Устанавливается (если включена поддержка автоматической установки)	Устанавливается	Приложение уже установлено

Табл. 12-6. Способы развертывания приложений *(окончание)*

Способ	Публикация (только пользователям	Назначение (пользователям)	Назначение (компьютерам)
Может ли пользователь удалить приложение с помощью программы Add/Remove Programs из Control Panel?	Да. Кроме того, он может повторно установить приложение средствами этой же программы	Да. Приложение разрешается повторно установить из стандартных точек распространения	Нет. Удалить приложение вправе только администратор. Пользователи могут лишь запускать и исправлять приложения
Поддерживаемые установочные файлы	Пакеты Windows Installer, .zap файлы	Пакеты Windows Installer	Пакеты Windows Installer

Преобразования (файлы .msi) применяются к пакетам Windows Installer во время назначения или публикации, но не при установке.

Назначение приложений

Если вам необходимо, чтобы приложение было доступно всем пользователям на их компьютерах, назначьте его. Приложение разрешается назначать как для компьютеров, так и для пользователей.

► **Назначение приложений**

1. Откройте оснастку Group Policy и затем в узле Computer Configuration или User Configuration откройте Software Settings.
2. Щелкните узел Software Settings правой кнопкой мыши и выберите команду New\Package (Создать\Пакет).

   В списке File Name (Имя файла) диалогового окна Open (Открыть) перечислены пакеты Windows Installer, имеющиеся на SDP по умолчанию. Чтобы найти пакет Windows Installer на каком-либо другом сетевом ресурсе, щелкните кнопку Browse (Обзор).
3. В списке File Name диалогового окна Open выберите назначаемый пакет и щелкните кнопку Open (Открыть).
4. В диалоговом окне Deploy Software (Развертывание программ) щелкните переключатель Assigned (Назначенный) и затем — OK. Если приложение находится в узле Computer Configuration оснастки Group Policy, переключатель Published (Публичный) недоступен (рис. 12-18).

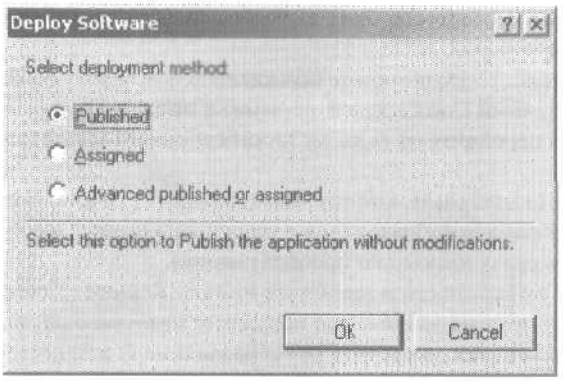


Рис. 12-18. Диалоговое окно Deploy Software (Развертывание программ)

Публикация приложений

Если вам необходимо, чтобы пользователи, управляемые ОГП, имели возможность при первой необходимости обратиться к приложению, опубликуйте его. При публикации каждый пользователь сам решает, устанавливать ему приложение или нет. Приложение разрешается публиковать лишь для пользователей.

► **Публикация приложений**

1. Откройте оснастку Group Policy и затем в узле Computer Configuration или User Configuration откройте Software Settings.
2. Щелкните узел Software Settings правой кнопкой мыши и выберите команду New\Package (Создать\Пакет).

   В списке File Name диалогового окна Open перечислены пакеты Windows Installer, имеющиеся на SDP по умолчанию. Чтобы найти пакет Windows Installer размещающийся на каком-либо другом сетевом ресурсе, щелкните кнопку Browse.
3. В списке File Name диалогового окна Open выберите публикуемый пакет и щелкните кнопку Open.
4. В диалоговом окне Deploy Software (рис. 12-18) щелкните переключатель Published (Публичный) и затем — OK.

   Пользователи имеют право установить приложение с помощью программы Add/Remove Programs из Control Panel или открыв связанный с приложением файл.

Развертывание приложений с преобразованиями

Преобразования связываются с пакетом Windows Installer в процессе развертывания, а не при использовании пакета для установки или модификации приложения. Преобразования (файлы .mst) применяются к пакетам windows Installer (файлам .msi) в порядке, определяемом администратором. Этот порядок следует задать, прежде чем приложение будет назначено или опубликовано.

► **Публикация приложения**

1. Откройте оснастку Group Policy и затем в узле Computer Configuration или User Configuration откройте Software Settings.
2. Щелкните узел Software Settings правой кнопкой мыши и выберите команду New\Package.

3. В списке File Name (Имя файла) открывшегося окна выберите публикуемый пакет и щелкните кнопку Open (Открыть).
4. В диалоговом окне Deploy Software (рис. 12-18) щелкните переключатель Advanced Published Or Assigned (Публичный или назначенный с особыми свойствами) и затем — OK.
5. В диалоговом окне свойств пакета перейдите на вкладку Modifications (Модификации) (рис. 12-19).
   - Для добавления преобразований щелкните кнопку Add (Добавить). В диалоговом окне Open (Открыть) выберите файл преобразования и щелкните кнопку Open (Открыть). Разрешается добавлять сразу несколько преобразований.
   - Для удаления преобразования выберите его и щелкните кнопку Remove (Удалить). Повторяйте данную операцию, пока не удалите все ненужные преобразования.
   - Чтобы задать порядок преобразований, выделите преобразование и измените его положение в списке с помощью кнопки Move Up (Вверх) или Move Down (Вниз). Преобразования применяются согласно их положению в списке.
6. Убедитесь, что преобразования расположены в нужном порядке, и щелкните кнопку OK.

Внимание! Щелкайте OK лишь по завершении настройки преобразований. После того как вы щелкните OK, пакет немедленно публикуется или назначается. Если преобразования настроены неверно, вам придется удалить пакет или обновить его с помощью корректной версии.

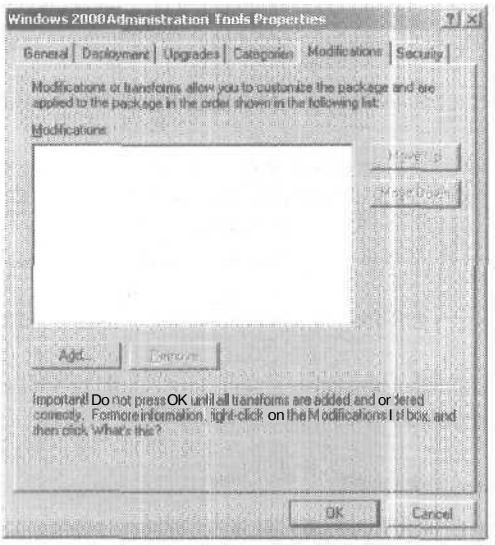


Рис. 12-19, Вкладка Modifications (Модификации) окна свойств пакета

Выбор параметров автоматической установки

Чтобы определить, какое приложение будет установлено при выборе файла, выделите расширение файла и настройте на вкладке File Extensions (Расширения файлов) диалогового окна Software Installation связанный с этим расширением приоритет установки приложений. Начнется установка первого приложения из списка.

Например, вы развертываете с помощью ОГП Microsoft Word 2000 и Microsoft FrontPage 2000. Оба эти приложения позволяют редактировать HTML-документы (.htm файлы).

Дабы изменить приоритет расширения файла таким образом, чтобы пользователи, управляемые ОГП, всегда устанавливали Microsoft FrontPage, сделайте FrontPage для .htm-файлов приложением с наивысшим приоритетом. Когда пользователь, не установивший ни Microsoft Word 2000, ни Microsoft FrontPage 2000, откроет .htm-файл, Software Installation установит FrontPage 2000 и откроет .htm-файл для редактирования. При отсутствии Software Installation будет выведено диалоговое окно Open With (Открыть с помощью), предлагающее пользователю выбрать приложение для открытия файла.

Управление связями с расширениями файлов осуществляется отдельно для каждого ОГП. Изменения в приоритетах приложений для ОГП воздействуют лишь на тех пользователей, на кого распространяется действие этой групповой политики.

▶ **Выбор параметров автоматической установки для расширения файла**

1. Откройте оснастку Group Policy и затем в узле Computer Configuration или User Configuration откройте Software Settings.
2. Щелкните узел Software Settings правой кнопкой мыши и выберите команду Properties.
3. В окне свойств Software Installation на вкладке File Extensions в списке Select File Extension (Выберите расширение) выберите требуемое расширение файла (рис. 12-20).
4. В списке Application Precedence (Порядок приложений) переместите с помощью кнопок Up (Вверх) или Down (Вниз) приложение с наивысшим приоритетом по умолчанию в начало. Если пользователь пытается открыть связанный с приложением файл, а это приложение не установлено, начнется установка первой программы из списка Application Precedence.
5. Щелкните OK.

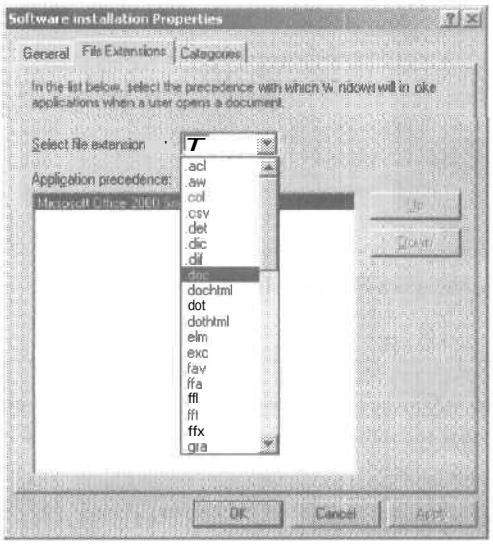


Рис. 12-20. Вкладка File Extensions (Расширения файлов) диалогового окна Software Installation Properties

Создание категорий приложений

Назначенные и опубликованные приложения можно организовать в логические категории, упрощающие пользователям поиск требуемых программ в программе Add/Remove Programs из Control Panel. В Windows 2000 нет готовых категорий.

Категории создаются для доменов, но не для ОГП. Вам потребуется лишь однажды определить категории приложений для всего домена.

▶ **Создание категорий управляемых приложений**

1. Откройте оснастку Group Policy и затем в узле Computer Configuration или User Configuration откройте Software Settings.
2. Щелкните узел Software Settings правой кнопкой мыши и выберите команду Properties.
3. В окне свойств Software Installation на вкладке Categories (Категории) щелкните кнопку Add (рис. 12-21).
4. В окне Enter New Category (Ввод новой категории) в поле Category (Категория) введите имя категории программ. Затем щелкните OK.
5. В диалоговом окне свойств Software Installation щелкните OK.

Рис. 12-21. Вкладка Categories (Категории) окна Software Installation Properties

Задание свойств приложений

Для более точной настройки приложений вы можете отредактировать параметры установки, задав используемые категории программ и назначив разрешения для установки приложений.

Редактирование параметров установки приложений

Хотя вы и могли глобально задать в ОГП параметры по умолчанию для новых пакетов на вкладке General диалогового окна свойств Software Installation, некоторые из этих параметров в дальнейшем разрешается редактировать. Параметры установки влияют на установку, управление и удаление приложений.

▶ **Редактирование параметров установки приложений**

1. Откройте оснастку Group Policy и затем в узле Computer Configuration или User Configuration откройте Software Settings.
2. Щелкните узел Software Installation.

3. В правой панели щелкните требуемое приложение правой кнопкой мыши и выберите команду Properties.
4. В окне свойств приложения на вкладке Deployment (Развертывание) в области Deployment Type (Тип развертывания) выберите один из следующих параметров (рис. 12-22);

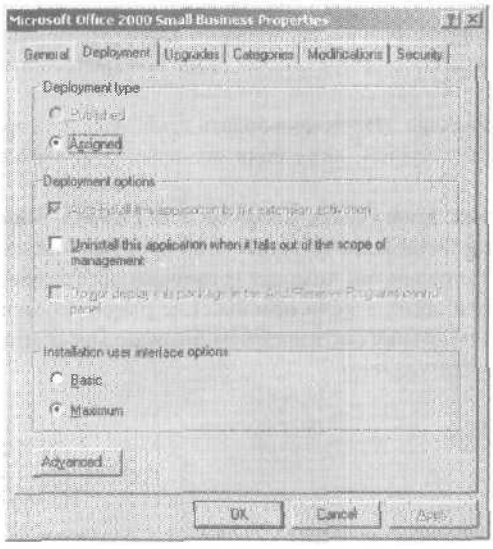


Рис. 12-22. Вкладка Deployment (Развертывание) диалогового окна свойств приложения

- **Published** (Публичный) — пользователи выбранного сайта, домена или ОП получают возможность установить приложение средствами программы Add/Remove Programs из Control Panel или открыв связанный с приложением файл;
- **Assigned** (Назначенный) — пользователи выбранного сайта, домена или ОП запустят установку приложения при следующем входе в систему (если приложение назначено пользователям) или при перезапуске компьютера (если приложение назначено компьютерам).

5. В области Deployment Options (Параметры развертывания) выберите один из следующих параметров:
   - **Auto-Install This Application By File Extension Activation** (Автоматически устанавливать приложение при обращении к файлу с соответствующим расширением) - - используется приоритет приложений для расширения файла, заданный на вкладке File Extensions окна свойств Software Installation. Если приложение расположено в узле Computer Configuration оснастки Group Policy, флажок останется недоступным и помеченным, так как по умолчанию приложение устанавливается автоматически;
   - **Uninstall This Application When It Falls Out Of The Scope Of Management** (Удалять это приложение, если его использование выходит за рамки, допустимые политикой управления) — при переходе пользователя/компьютера в сайт, домен или ОП, где приложение не развернуто, оно будет удалено при входе в систему (для пользователей) или при загрузке (для компьютеров);
   - **Do Not Display This Package In The Add/Remove Programs Control Panel** (Не отображать этот пакет в окне мастера установки и удаления программ панели управления) - пакет не будет отображаться программой Add/Remove Programs из Control Panel.

6. В области Installation User Interface Options (Пользовательский интерфейс при установке) выберите один из следующих параметров:
   - **Basic** (Простой) — отображаются лишь основные сообщения и окна мастера установки;
   - **Maximum** (Полный) — при установке пакета отображаются все сообщения и окна.
7. Щелкните кнопку Advanced (Дополнительно). В области Advanced Deployment Options (Дополнительные параметры развертывания) одноименного окна выберите один из следующих параметров:
   - **Ignore Language When Deploying This Package** (Не использовать языковые установки при развертывании) — пакет будет установлен, даже если его язык отличается от текущего;
   - **Remove Previous Installs Of This Product From (Users/Computers) If Product Was Not Installed By Group Policy-Based Software Installation** (Удалите этот продукт с компьютеров пользователей, если он был установлен без помощи установки программного обеспечения на основе групповой политики) — если приложение ранее устанавливалось не основанным на групповой политике расширением Software Installation, а каким-либо другим способом, оно будет удалено.
8. Щелкните OK.
9. В диалоговом окне свойств щелкните OK.

Выбор категорий приложений

Приложение необходимо отнести к одной из существующих категорий. Создаваемые категории обычно относятся лишь к опубликованным приложениям. Программы в окне Add/Remove Programs распределены по категориям.

▶ **Определение категорий для приложений, отображаемых в окне Add/Remove Programs из Control Panel**

1. Откройте оснастку Group Policy и затем в узле Computer Configuration или **User** Configuration откройте Software Settings.
2. Щелкните узел Software Installation.
3. В правой панели щелкните требуемое приложение правой кнопкой мыши и выберите команду Properties.
4. В окна свойств приложения на вкладке Categories (Категории) в списке Available Categories (Доступные категории) выделите категорию и щелкните кнопку Select (Выбрать) (рис. 12-23).
5. Для выбора дополнительных категорий повторите пункт 4. Завершив добавление категорий, щелкните OK.

Задание разрешений для установки ПО

Разрешения, заданные для установки ПО, распространяются лишь на установку приложения.

▶ **Задание разрешений для установки ПО**

1. Откройте оснастку Group Policy и затем в узле Computer Configuration или **User** Configuration откройте Software Settings.
2. Щелкните узел Software Installation.
3. В правой панели щелкните требуемое приложение правой кнопкой мыши и выберите в контекстном меню команду Properties.
4. На вкладке Security (Безопасность) диалогового окна свойств приложения выберите нужную группу безопасности.

Администраторам, управляющим установкой приложения, необходимо предоставить разрешение Full Control, а пользователям, работающим с назначенным или опубликованным приложением — разрешение Read.

5. Щелкните OK.

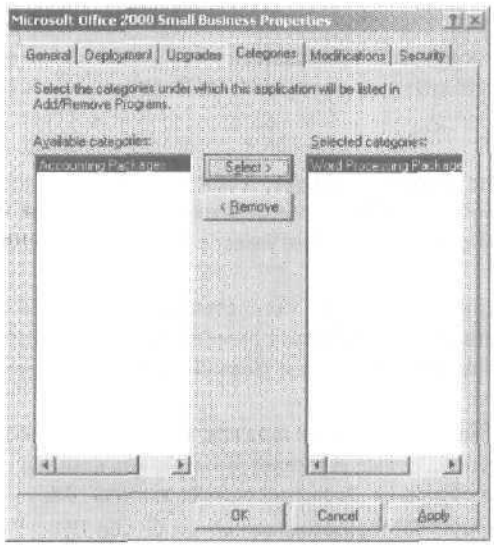


Рис. 12-23. Вкладка Categories **(Категории) окна свойств приложения**

Поддержка приложений

После развертывания приложений вам в какой-то момент, возможно, потребуется обновить или удалить их.

Обновление приложений

Обновление требуется в следующих ситуациях:

- разработчик создал новую версию программы, включающую дополнительные функции;
- организация переходит на приложение другого поставщика.

Обычно обновление приводит к значительным изменениям приложения и установке новой версии программы. В большинстве случаев обновляется значительное количество файлов. Для разработки процедуры обновления существующего приложения можно воспользоваться расширением Software Installation.

▶ **Обновление приложений**

1. Откройте оснастку Group Policy и затем в узле Computer Configuration или User Configuration откройте Software Settings.
2. Щелкните узел Software Installation.
3. В правой панели щелкните пакет-обновление Windows Installer (необновляемый пакет) правой кнопкой мыши и выберите команду Properties. Данный пакет необходимо предварительно опубликовать или назначить.
4. На вкладке Upgrades (Обновления) окна свойств приложения щелкните кнопку Add (Добавить), чтобы создать или дополнить текущим пакетом список обновляемых пакетов.

5. В диалоговом окне Add Upgrade Package (Добавление обновления) (рис. 12-24) укажите источник обновляемого пакета — Current Group Policy Object [из текущего объекта групповой политики (GPO)] или A Specific GPO (из указанного объекта групповой политики). В последнем случае щелкните кнопку Browse (Обзор), выберите требуемый ОГП и затем в диалоговом окне Browse For A Group Policy Object (Поиск объекта групповой политики) щелкните OK.

   Под заголовком Package To Upgrade (Обновляемое приложение) отображается полный список всех пакетов, назначенных для публикации в текущем ОГП. В зависимости от ОГП список может быть пустым.
6. Щелкните обновляемый пакет,
7. Щелкните переключатель Uninstall The Existing Package, Then Install The Upgrade Package (Удалить приложение, затем установить его обновление) или Package Can Upgrade Over The Existing Package (Обновление возможно поверх имеющегося приложения). Затем щелкните OK.

   Удаление обычно используется для замены приложения полностью новой версией (например, приложением другого поставщика). Обновление применяется для установки более новой версии текущего приложения с сохранением пользовательских параметров, связей с типами документов и т. п.
8. На вкладке Upgrades диалогового окна свойств щелкните флажок Required Upgrade For Existing Packages (Обязательное обновление для уже установленных приложений), если вы хотите, чтобы обновление было обязательным. Затем щелкните кнопку OK.

   Если обновление находится в узле Computer Configuration оснастки Group Policy, данный флажок останется недоступным и помеченным, поскольку для компьютеров пакеты можно лишь назначать, но не публиковать.

Рис. 12-24. Диалоговое окно Add Upgrade Package (Добавление обновления)

Удаление приложений

Иногда приложение становится ненужным, и вы хотите удалить его. Расширение Software Installation позволяет удалить приложение, если:

- **текущая версия больше не поддерживается.** Администратор может удалить версию приложения из Software Installation, не удаляя физически само приложение с компьюте-

ров. Пользователи смогут и дальше работать с данной программой и при необходимости самостоятельно удалить ее. Установить версию приложения (из меню Start, средствами программы Add/Remove Programs из Control Panel или открыв связанный с программой файл) пользователь не вправе;

- **оно больше не используется.** Администратор может принудительно удалить программу. Программа будет автоматически удалена с компьютера при следующем запуске (если приложение назначено компьютеру) или при входе пользователя в систему (если приложение назначено пользователю). Пользователям в этом случае запрещено запускать или устанавливать программу.

Примечание Если вы хотите, чтобы приложение было удалено после того, как на пользователей/компьютеры перестанет распространяться ОГП, пометьте переключатель Uninstall This Application When It Falls Out Of The Scope of Management при развертывании приложения.

▶ **Удаление приложений**

1. Откройте оснастку Group Policy и затем в узле Computer Configuration или User Configuration откройте Software Settings.
2. Щелкните узел Software Installation.
3. В правой панели выделите требуемое приложение и выберите команду All Tasks\Remove (Все задачи\Удалить).
4. В диалоговом окне Remove Software (Удаление приложений) щелкните один из следующих переключателей:
   - **Immediately Uninstall The Software From Users And Computers** (Немедленное удаление этого приложения с компьютеров всех пользователей) — приложение будет удалено при следующем входе пользователя в систему или при запуске компьютера;
   - **Allow Users To Continue To Use The Software, But Prevent New Installations** (Разрешить использование уже установленного приложения, но запретить новую установку) — пользователи смогут продолжить работу с уже установленным приложением. Если же они удалят программу или никогда не устанавливали ее, установить приложение они не смогут.
5. Щелкните OK.

Резюме

Расширение Software Installation упрощает установку и поддержку приложений. Вы можете централизованно управлять установкой приложений на клиентской системе, назначая программы пользователям/компьютерам или публикуя приложения для пользователей. Необходимое или обязательное ПО следует *назначать*. Приложения, которые могут оказаться полезными пользователям, рекомендуется *публиковать*.

Для систематической поддержки приложений расширение Software Installation использует Windows Installer. Пакет Windows Installer — это файл, содержащий необходимые инструкции по установке и удалению приложений.

Вы также изучили задачи по установке приложений: планирование и подготовку, настройку SDP, выбор параметров, используемых при установке по умолчанию, развертывание программ, выбор параметров автоматической установки, создание категорий программ, настройку свойств приложений и поддержку программ.

Занятие 5. Управление специальными папками с помощью групповой политики

В Microsoft Windows 2000 можно перенаправлять специальные папки с профилями пользователей в сеть средствами расширения Folder Redirection (Перенаправление папки) оснастки Group Policy. На этом занятии рассказывается о перенаправлении специальных папок и настройке такого перенаправления с использованием групповой политики.

Изучив материал этого занятия, вы сможете:

- ✓ перенаправлять специальные папки.

Продолжительность занятия - около 15 минут.

Перенаправление папок

Расширение Folder Redirection оснастки Group Policy позволяет перенаправлять специальные папки Windows 2000 в определенные места сети. Специальные папки, например My Documents и My Pictures, находятся в каталоге C:\Documents and Settings (здесь C:\ — буква вашего системного диска).

В Windows 2000 разрешается перенаправлять следующие специальные папки:

- Application Data;
- Desktop (Рабочий стол);
- My documents (Мои документы);
- My Pictures (Мои рисунки);
- Start Menu (Главное меню).

Расширение Folder Redirection доступно в узле User Configuration\Windows Settings оснастки Group Policy.

Преимущества **перенаправления папки My Documents**

Перечисленные ниже преимущества относятся к перенаправлению любой папки, однако перенаправление папки My Documents дает особые преимущества, поскольку ее размер со временем значительно увеличивается.

- Даже если пользователь входит в сеть с разных компьютеров, его документы всегда доступны.
- При использовании перемешаемого профиля пользователя только сетевой путь к папке My Documents является его частью, а не сама папка. Поэтому ее содержимое не придется копировать и перемещать между клиентом и сервером каждый раз при входе пользователя в систему или его выходе, что убыстряет процесс входа и выхода по сравнению с Windows NT 4.0.
- Сетевой администратор может архивировать данные, хранящиеся на сервере. Это более безопасный способ, поскольку не требуется вмешательство пользователя.
- Системный администратор вправе устанавливать дисковые квоты с помощью групповой политики, ограничивая дисковое пространство, выделенное пользователю для специальных папок.
- Данные пользователя разрешается перенаправлять на жесткий диск локального компьютера с другого жесткого диска, на котором хранятся системные файлы. Это обезопасит пользовательские файлы, если придется переустановить ОС.

Расположение специальных папок по умолчанию

Расположение не перенаправлявшихся специальных папок по умолчанию зависит от ранее установленной ОС (табл. 12-7).

Табл. 12-7. Расположение специальных папок по умолчанию

Операционная система	Размещение специальных папок
Заново установленная Windows 2000, обновление Windows 95 или Windows 98 с отключенными профилями пользователей до Windows 2000	C:\Documents and Settings (здесь C:\ — ваш системный диск). Например, C:\Documents and Settings
Обновление Windows NT 3.51 или Windows NT 4.0 до Windows 2000	*systemroot*\Profiles. Например, C:\WinNT\Profiles
Обновление Windows 95 или Windows 98 с включенными профилями пользователей до Windows 2000	*systemroot*\Profiles Например, C:\Windows\System\Profiles

Настройка перенаправления папок

Существует два способа переправления папок:

- в соответствии с членством в группе безопасности;
- для всех пользователей сайта, домена или ОП.

Кроме того, папку My Pictures разрешается перенаправлять вслед за папкой My Documents (при этом My Pictures останется подкаталогом My Documents, что и реализовано по умолчанию).

Примечание Перенаправлять папку My Pictures отдельно от My Documents рекомендуется лишь в особых случаях, например для упрощения общего доступа. Если указанные папки перенаправляются раздельно, в папку My Documents помещается ярлык папки My Pictures.

▶ Перенаправление специальных папок в различные места в соответствии с членством в группе безопасности

1. Откройте ОГП, связанный с сайтом, доменом или ОП, содержащим учетные записи пользователей, чьи папки необходимо перенаправить в другое место в сети.
2. Чтобы отобразить папку, которую необходимо перенаправить, в дереве консоли раскройте узел User Configuration\Windows Settings\Folder Redirection (Конфигурация пользователя\Конфигурация Windows\Перенаправление папки).
3. Щелкните правой кнопкой необходимую папку (Desktop, My Documents и т. д.) и выберите команду Properties.
4. Перейдите на вкладку Target (Размещение). В списке Setting (Политика) выберите Advanced — Specify Locations For Various User Groups (Указать различные места для разных групп пользователей) и щелкните кнопку Add (Добавить).
5. В окне Specify Group And Location (Выбор группы и размещения) в области Security Group Membership (Членство в группе безопасности) щелкните кнопку Browse (Обзор) (рис. 12-26).

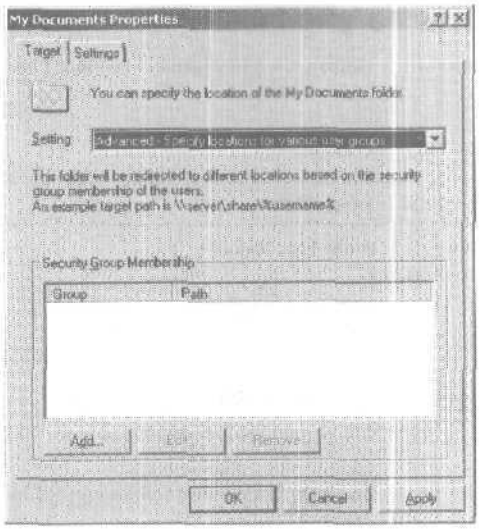


Рис. 12-25. Вкладка Target (Размещение) диалогового окна свойств перенаправляемой папки

6. В диалоговом окне Select Group (Выбор: Группа) выберите необходимую группу и щелкните OK.
7. В окне Specify Group And Location (Выбор группы и размещения) в области Target Folder Location (Размещение конечной папки) щелкните кнопку Browse (Обзор).
8. В окне Browse For Folder (Обзор папок) выберите для этой группы безопасности место для перенаправления. Затем щелкните OK.

   Если ввести имя диска, например D:\, оно должно указывать путь к локальному компьютеру пользователя. Рекомендуется вводить путь в формате UNC.

   Если необходимо, чтобы каждый пользователь сайта, домена или подразделения имел собственную подпапку в этом расположении, можно включить %username% в UNC-путь, например *сервер**общий_ресурс*\%username%.Рекомендуется включать %username% в указание пути. Например, папку My Documents пользователя SecUser, состоящего в группе безопасности Users, разрешается перенаправлять в \\server1\share\secuser\My Documents (\\server1\ share\%username%\My Documents),
9. В диалоговом окне Specify Group And Location (Выбор группы и размещения) щелкните OK.
10. Если необходимо перенаправить папки членов других групп безопасности, то повторяйте пункты 2—9, пока не введете все группы.
11. Перейдите на вкладку Settings (Параметры) и задайте каждый из следующих параметров. Рекомендуется выбрать режим по умолчанию;
    - **Grant The User Exclusive Rights To** (Предоставить исключительные права для *специальная папка)*. Включен по умолчанию. Пользователь и локальная система имеют полные права на папку, а администратор не имеет никаких прав. Если этот параметр отключен, то не удастся изменять разрешения для папки, а разрешения, применяемые по умолчанию, продолжают действовать;
    - **Move The Contents Of** *(текущая специальная папка пользователя)* **To The** New **Location** (Перенести содержимое *специальная папка* в новое место). Включен по умолчанию.

Рис. 12-26. Диалоговое окно Specify Group And Location (Выбор группы и размещения)

12. Выберите один из двух параметров в области Policy Removal (рекомендуется оставить значение по умолчанию):
    - **Leave The Folder In The New Location When Policy Is Removed** (После удаления политики переместить папку). Включен по умолчанию;
    - **Redirect The Folder Back To The Local User Profile Location When Policy Is Removed** (После удаления политики перенаправить папку обратно в локальный профиль пользователя).
13. Для папки My Documents доступны дополнительные возможности перенаправления папки My Pictures:
    - **Make My Pictures A Subfolder Of My Documents** (Сделать «Мои рисунки» подпапкой папки «Мои документы») — папка My Pictures будет автоматически перенаправляться вслед за папкой My Documents;
    - **Do Not Specify Administrative Policy For My Pictures** (Не указывать политику для папки «Мои рисунки») — папка My Pictures не будет являться подкаталогом папки My Documents, и ее расположение определяется профилем пользователя.

Примечание При желании вы можете настроить свойства папки My Pictures, чтобы она автоматически перенаправлялась вслед за папкой My Documents. Подробности см. в упражнении «Настройка папки My Pictures для перенаправления вслед за папкой My Documents».

---

14. Щелкните кнопку OK.

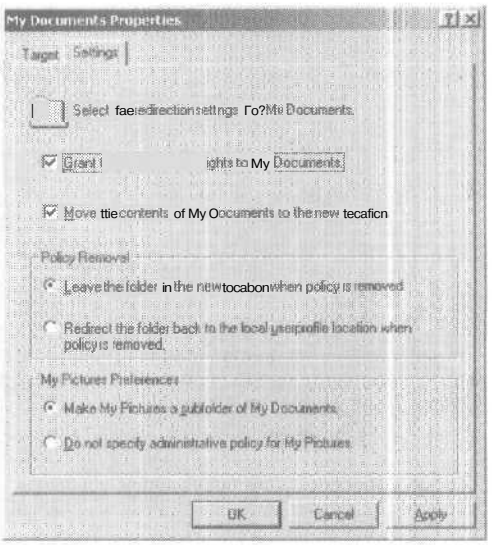


Рис. 12-27. Вкладка Settings (Параметры) окна свойств перенаправляемой папки

▶ **Перенаправление специальных папок в общее расположение для всех пользователей сайта, домена или ОП**

1. Откройте ОГП, связанный с сайтом, доменом или подразделением, содержащим учетные записи пользователей, чьи папки необходимо перенаправить в сетевое расположение.
2. Чтобы отобразить папку, которую необходимо перенаправить, в дереве консоли раскройте узел User Configuration\Windows Settings\Folder Redirection (Конфигурация пользователя\Конфигурация Windows\Перенаправление папки).
3. Щелкните правой кнопкой необходимую папку (Desktop, My Documents и т. д.) и выберите команду Properties,
4. Перейдите на вкладку Target. В списке Setting (Политика) выберите Basic-Redirect Everyone's Folder To The Same Location (Перенаправлять папки всех пользователей в одно место) и щелкните кнопку Browse (Обзор).
5. В диалоговом окне Browse For Folder (Обзор папок) выберите для этого ОГП размещение для перенаправления.

   Введенное имя диска, например D:\, должно указывать путь к локальному компьютеру пользователя. Рекомендуется указывать путь в формате UNC.

   Если необходимо, чтобы каждый пользователь сайта, домена, подразделения имел собственную подпапку в этом расположении, можно включить %username% в UNC-путь, например *сервер**общий_ресурс*\%username% Рекомендуется включать %username% в указание пути. Например, папку My Documents пользователя SecUser, состоящего в группе безопасности Users, разрешается перенаправлять в \\server1\share\secuser\My Documents (\\server1\share\%username%\My Documents).
6. В диалоговом окне Browse For Folder щелкните OK.
7. Перейдите на вкладку Settings (Параметры) и задайте каждый из следующих параметров. Рекомендуется задавать их по умолчанию.
   - **Grant The User Exclusive Rights To** (Предоставить исключительные права для *специальная папка).* Включен по умолчанию. Пользователь и локальная система имеют полные права на папку, а администратор не имеет никаких прав. Если этот пара-

метр отключен, то не удастся изменять разрешения для папки, а разрешения, применяемые по умолчанию, продолжают действовать.

- **Move The Contents Of** *(текущая специальная папка пользователя)* **To The New Location** (Перенести содержимое специальной папки в новое место). Включен по умолчанию.

8. Выберите один из двух параметров в области Policy Removal (рекомендуется оставить значение по умолчанию).
   - **Leave The Folder In The** New **Location When Policy Is Removed** (После удаления политики переместить папку). Включен по умолчанию.
   - **Redirect The Folder Back To The Local User Profile Location When Policy Is Removed** (После удаления политики перенаправить папку обратно в локальный профиль пользователя).

Внимание! Подробнее о выборе параметра удаления политики — в разделе «Последствия удаления политики».

---

9. Для папки My Documents доступны дополнительные возможности перенаправления папки My Pictures:
   - **Make My Pictures A Subfolder Of My Documents** (Сделать «Мои рисунки» полпапкой папки «Мои документы») — папка My Pictures будет автоматически перенаправляться вслед за папкой My Documents;
   - **Do Not Specify Administrative Policy For My Pictures** (Не указывать политику для папки «Мои рисунки») — папка My Pictures не будет являться подкаталогом папки My Documents, и ее расположение определяется профилем пользователя.

Примечание При желании вы можете настроить свойства папки My Pictures таким образом, чтобы она автоматически перенаправлялась вслед за папкой My Documents. Подробности см. в упражнении «Настройка папки My Pictures для перенаправления вслед за папкой My Documents».

---

10. Щелкните OK.

▶ **Настройка папки My Pictures для перенаправления вслед за папкой My Documents**

1. Откройте ОГП, связанный с сайтом, доменом или подразделением, содержащим учетные записи пользователей, чьи папки My Pictures необходимо перенаправить в сетевое расположение.
2. В дереве консоли раскройте узел User Configuration\Windows Settings\Folder Redirection.
3. Щелкните правой кнопкой папку My Pictures и выберите команду Properties.
4. В списке Setting (Политика) окна свойств папки My Pictures выберите Follow The My Documents Folder (Следовать за папкой «Мои документы») и щелкните OK.

Последствия удаления политики

В табл. 12-8 показано, что произойдет с перенаправленными папками и их содержимым, если к ним больше не применяется ОГП.

Табл. 12-8. Последствия удаления политики

Параметр «Перемещение содержимого специальной папки на новое место»	Параметр «Удаление политики»	**Результаты действия политики удаления**
Включен	При удалении политики перенаправить папку назад в размещение профиля пользователя	Специальная папка вернется на место профиля пользователя. Содержимое будет скопировано, а не перемещено назад на место профиля пользователя. Содержимое не будет удалено из места перенаправленной папки. Пользователь сохранит доступ к содержимому, но только на локальном компьютере
Отключен	При удалении политики папка перенаправляется назад, на место профиля пользователя	Специальная папка вернется на место профиля пользователя. Содержимое будет скопировано или перемещено назад на место профиля пользователя. Внимание! Если содержимое папки не скопировано на место профиля пользователя, пользователь его не видит
Или включен, или отключен	При удалении политики папка останется в новом месте	Специальная папка остается в перенаправленном месте. Ее содержимое остается в перенаправленном месте. Пользователь продолжает иметь доступ к содержимому в перенаправленной папке

Резюме

Вы научились перенаправлять папки с профилями пользователей в другие места в сети. В Windows 2000 разрешается перенаправлять следующие специальные папки: Application Data, Desktop, My Documents, My Pictures и Start Menu. Переправление папок осуществляется в соответствии с членством в группе безопасности или для всех пользователей сайта, домена или ОП.

Занятие 6, Устранение проблем при использовании групповой политики

На этом занятии обсуждаются возможные проблемы с использованием групповой политики, а также приводятся некоторые рекомендации, позволяющие упростить их устранение.

Изучив материал этого занятия, вы сможете:

- устранять неполадки групповой политики;
- усовершенствовать технику работы с групповыми политиками.

Продолжительность занятия — около 10 минут.

Важная составляющая процесса устранения неполадок групповой политики — выявление зависимостей между компонентами. Например, расширение Software Installation зависит от групповой политики, а групповая политика связана со службой каталогов Active Directory. Та, в свою очередь, зависит от корректной конфигурации сетевых служб. При устранении неполадок какого-либо компонента рекомендуется проверить работу связанных с ним элементов. Журналы событий помогают выявить проблемы, вызываемые данным типом иерархической зависимости.

В табл. 12-9 описываются типичные проблемы, возникающие при работе с оснасткой Group Policy.

Табл. 12-9. Проблемы при работе *с* оснасткой Group Policy

Пользователь не может открыть ОГП, хотя и обладает разрешением Read для него

Причина	Решение
Чтобы открыть ОГП в оснастке Group Policy администратор должен обладать для него разрешениями Read и Write	Сделайте администратора членом группы безопасности, обладающей разрешениями Read и Write для данного ОГП. Например, администратор домена может управлять нелокальными ОГП. Администратор компьютера вправе управлять лишь локальным ОГП этой системы

При попытке редактирования ОГП выдается сообщение «Failed To Open The Group Policy Object» (невозможно открыть ОГП)

Причина	Решение
Проблемы с сетью, в частности проблемы с конфигурацией DNS	Убедитесь в корректной работе DNS

В табл. 12-10 описаны ситуации, когда параметры групповых политик не действуют.

Табл. 12-10. Проблемы с групповой политикой

Групповая политика не распространяется на пользователей и компьютеры в группе безопасности, хотя ОГП и связан с ОП, содержащим данную группу

Причина	Решение
Это вполне нормальное явление. Групповая политика распространяется лишь на пользователей и компьютеры сайтов, доменов и ОП. ОГП не распространяются на группы безопасности	ОГП следует сопоставлять только сайтам, доменам и ОП. Помните, что расположение группы безопасности в иерархии Active Directory не связано с распространением групповой политики на пользователей и компьютеры данной группы

Групповая политика не распространяется на пользователей и компьютеры сайта, домена или ОП

Причина	Решение
Распространение параметров групповой политики на пользователей и компьютеры случайно или намеренно блокируется. Наследование ОГП блокируется для пользователей, компьютеров или и тех. и других одновременно. Кроме того, для распространения параметров путем наследования ОГП должен быть связан непосредственно с ОП, содержащим пользователей и компьютеры, или с родительским доменом/ОП. Если распространяются параметры нескольких ОГП, их обработка производится в следующем порядке: локальный ОГП, ОГП сайта, ОГП домена, ОГП ОП. По умолчанию преимущество имеют параметры, применяемые последними. Групповая политика иногда также блокируется на уровне любого ОП или распространяется принудительно, если для конкретной ОГП-ссылки задан параметр No Override (Не перекрывать). Наконец, пользователь или компьютер должен состоять в одной или нескольких группах безопасности, обладающих соответствующими разрешениями	Убедитесь, что наследование требуемой политики не заблокировано. Проверьте, не задан ли для политики, стоящей выше по иерархии, параметр No Override. Если используются параметры Block Policy Inheritance (Блокировать наследование политики) и No Override, помните, что преимущество отдается параметру No Override. Убедитесь, что пользователь/компьютер не состоит в группе безопасности с отозванным разрешением AGP. Удостоверьтесь, что пользователь/компьютер состоит в хотя бы одной группе безопасности, которой предоставлено разрешение AGP Убедитесь, что пользователь/компьютер состоит в хотя бы одной группе безопасности, обладающей разрешением Read

Табл. 12-10. Проблемы с групповой политикой *(окончание)*

Групповая политика не распространяется на пользователей и компьютеры контейнера Active Directory

Причина	Решение
ОГП нельзя сопоставить с какими-либо контейнерами Active Directory, кроме сайтов, доменов и ОП	Создайте ссылку на ОГП для ОП, который является родителем требуемого контейнера Active Directory. После этого параметры групповой политики будут распространяться на пользователей и компьютеры контейнера за счет наследования

Групповая политика не действует на локальном компьютере

Причина	Решение
Локальные политики имеют наименьший приоритет — их может переопределить любой нелокальный ОГП	Проверьте, какие ОГП распространяются через службу Active Directory и не конфликтуют ли их параметры с параметрами локального ОГП

В табл. 12-11 рассматриваются проблемы, возникающие при работе с расширением Software Installation.

Табл. 12-11. Проблемы, возникающие при работе с расширением Software Installation

Опубликованные приложения не отображаются программой Add/Remove Programs из Control Panel

Причина	Решение
Проблемы с сервером: не распространяется групповая политика. Невозможно обратиться к Active Directory. У пользователя нет в ОГП опубликованных для него приложений. Клиент работает под управлением Terminal Server (Сервера терминалов)	Изучите все возможные ситуации. Помните, что расширение Software Installation для клиентов Terminal Server не поддерживается

При открытии документа, связанного с опубликованными приложением, приложение не устанавливается

Причина	Решение
Администратор не настроил автоматическую установку	Убедитесь, что на вкладке Deployment (Развертывание) окна свойств приложения помечен флажок Auto-Install This Application By File Extension Activation (Автоматически устанавливать приложение при обращении к файлу с соответствующим расширением).

Табл. 12-11. Проблемы, возникающие при работе с расширением Software Installation *(окончание)*

Выдается сообщение «The feature you are trying to install cannot be found in the source directory» (компонент, который вы путаетесь установить, не найден в исходном каталоге)

Причина	Решение
Проблемы с сетью или разрешениями	Убедитесь в корректной работе сети. Удостоверьтесь, что пользователь обладает для ОГП разрешениями AGP и Read. Убедитесь, что у пользователя имеется разрешение Read для SDP. Проверьте, обладает ли пользователь разрешением Read для приложения

После удаления приложения его ярлыки по-прежнему отображаются на рабочем столе пользователя

Причина	Решение
Пользователь создал ярлыки, о которых Windows Installer не знает	Удалите **ярлыки** вручную

Выдается сообщение «Another Installation Is Already In Progress» (установка этого приложения уже выполняется)

Причина	Решение
Возможно, в фоновом режиме выполняется удаление приложения без вывода пользовательского интерфейса или пользователь случайно запустил два процесса установки	Попробуйте еще раз

При запуске уже установленного приложения запускается Windows Installer

Причина	Решение
Автоматическое восстановление приложения или добавление пользовательского компонента	Предпринимать ничего не надо

Выдается сообщение «Active **Directory Will Not Allow The Package To Be Deployed» (Active Directory не допускает обновления пакета) или «Cannot Prepare Package For Deployment» (невозможно подготовить пакет для развертывания)**

Причина	Решение
Повреждение пакета или проблемы с сетью	Изучите ситуацию и примите соответствующие меры

Рекомендации по использованию групповой политики

Приведенные ниже рекомендации помогут упростить устранение неполадок при применении групповой политики.

Общие рекомендации

- **Отключите неиспользуемые части ОГП.** Если в узле User Configuration или Computer Configuration ОГП параметры не заданы, во избежание их обработки отключите этот узел. Это убыстряет загрузку и регистрацию в системе для пользователей и компьютеров, на которые распространяется ОГП.
- **Не используйте слишком часто параметры Block Policy Inheritance и No Override.** Иначе устранение неполадок групповой политики серьезно затруднится.
- **Минимизируйте число ОГП, сопоставленных пользователям и компьютерам домена/ОП.** Чем больше ОГП сопоставлено пользователю/компьютеру, тем больше требуется времени на запуск и вход в систему.
- **Фильтруйте политики на основе членства в группах безопасности.** Если на пользователей, в соответствии с параметрами системы, не распространяются определенные ОГП, то эти пользователи могут избежать задержек при регистрации в системе, поскольку для них эти ОГП обрабатываться не будут.
- **Используйте замыкание на себя лишь при необходимости.** Например, это следует делать, когда всем пользователям нужна одинаковая конфигурация рабочего стола.
- **Избегайте перекрестных привязок ОГП между доменами.** Если групповая политика запрашивается из другого домена, обработка ОГП значительно увеличит время загрузки и регистрации в системе.

Рекомендации по работе с расширением Software Installation

- **Определите категории приложений для организации.** Так вы упростите пользователям поиск приложений средствами программы Add/Remove Programs из Control Panel. Например, можно разделить приложения для отдела сбыта, бухгалтерии и т. д.
- **Помните, что преобразования нельзя применять во время развертывания.** Преобразования разрешается применять во время назначения или публикации и не разрешается во время установки. На практике это означает, что перед тем как щелкнуть OK, необходимо убедиться, что на вкладке Modifications (Модификации) диалогового окна свойств пакета задан необходимый путь. Если это не сделано и развернут неправильно преобразованный пакет, надо либо удалить его и раскрыть заново, либо обновить его правильно преобразованной версией.
- **Назначайте и публикуйте установленные программы в ОГП только один раз.** Например, если вы назначили пакет Microsoft Office для компьютеров, которым сопоставлен ОГП, не назначайте и не публикуйте этот пакет для пользователей, которым сопоставлен тот же ОГП.
- **Используйте преимущества средств разработки.** Разработчики, знакомые с файлами, записями реестра и другими требованиями для корректной работы приложения, могут создать простые пакеты Windows Installer, используя доступные авторские инструменты от разных поставщиков ПО.
- **Заново упаковывайте существующее ПО.** Для пакетов ПО, с которыми не поставляются файлы .msi, можно создать пакеты Windows Installer с помощью сторонних авторских программ, которые сравнивают состояние компьютера до и после установки. Для достижения наилучших результатов устанавливайте требуемый пакет на компьютер, на котором нет других приложений (чистая установка).
- **Используйте System Management Server и DFS.** Microsoft Systems Management Server и Windows 2000 Distributed File System (DFS) полезны для управления точками SDP — общими ресурсами сети, откуда пользователи устанавливают ПО.

- **Назначайте и публикуйте приложения на высоком уровне иерархии Active Directory.** Поскольку параметры групповой политики применяются по умолчанию к дочерним контейнерам Active Directory, лучше всего назначать или публиковать приложения путем привязки ОГП к родительскому ОП или домену. Для тонкой настройки списка пользователей, получающих ПО, настройте записи управления доступом для ОГП.
- **Используйте свойства Software Installation для улучшения управления.** Это упростит администрирование процесса назначения или публикации большого числа пакетов с одинаковыми свойствами в одном ОГП. Например, это удобно, если нужно опубликовать все ПО, относящееся к одной точке SDP.
- **Используйте** свойства **пакета Windows Installer для улучшения управления.** Советуем вам именно таким образом назначать и публиковать отдельные пакеты.

Рекомендации по перенаправлению папок

- **Включайте переменную среды %username% в UNC-путь.** Это даст пользователям возможность работать с собственными папками. Например, *сервер**общий_ресурс*\%username%\My Documents.
- **Перенаправляйте папку My Pictures** вслед **за папкой My Documents.** Поступать иначе следует лишь в особых случаях.
- **Помните о последствиях удаления политики.** Не забывайте, как будут вести себя ваши папки при удалении политики. См. раздел «Последствия удаления политики».
- **Используйте параметры по умолчанию.** Это рекомендуется в большинстве ситуаций.

Резюме

Вы узнали о возможных проблемах, с которыми можно столкнуться при использовании групповой политики, а также о способах их устранения. Кроме того, здесь были описаны некоторые рекомендации по использованию групповой политики.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении А «Вопросы и ответы» в конце книги,

1. Что такое ОГП?

2. Назовите два вида параметров групповой политики и расскажите, как они используются.

3. Опишите порядок применения групповой политики в структуре Active Directory.

4. Перечислите задачи по внедрению групповой политики.

5. В чем отличие параметров Block Policy Inheritance и No Override?

6. Чем отличается публикация приложения от его назначения?

7. Какие папки можно перенаправлять?

ГЛАВА 13

Администрирование конфигурации безопасности

В этой главе

Параметры безопасности определяют степень защиты системы. Создавая и настраивая *объекты групповой политики* (group policy object, GPO) Active Directory, администраторы могут централизованно управлять уровнями безопасности в корпоративных системах. Локальные объекты групповой политики (ОГП) используются для обеспечения безопасности в системах на основе рабочих групп. В этой главе обсуждаются параметры, необходимые для настройки безопасности системы.

Прежде всего

Для изучения материалов этой главы необходимо:

- выполнить процедуру установки, описанную во вводной главе;
- настроить компьютер как контроллер домена;
- изучить материалы главы 12.

Занятие 1. Конфигурация безопасности

Расширение Security Settings (Параметры безопасности) оснастки Group Policy (Групповая политика) применяется для настройки конфигурации безопасности компьютеров и групп. На этом занятии рассматриваются параметры конфигурации безопасности.

Изучив материал этого занятия, вы сможете:

✓ описать параметры конфигурации безопасности, реализуемые в ОГП.

Продолжительность занятия — около 10 минут.

Параметры конфигурации безопасности

Конфигурация безопасности (security configuration) содержит параметры для всех *областей безопасности* (security area) Windows 2000. В расширении Security Settings оснастки Group Policy можно настроить параметры безопасности для нелокальных ОГП из следующих узлов:

- Account policies (Политики учетных записей);
- Local policies (Локальные политики);
- Event log (Журнал событий);
- Restricted groups (Группы с ограниченным доступом);
- System services (Системные службы);
- Registry (Реестр);
- File system (Файловая система);
- Public key policies (Политики открытого ключа);
- IP security policies (Политики безопасности IP).

Узел Account Policies

Политики из этого узла распространяются на учетные записи пользователей. К атрибутам этого узла относятся:

- **Password Policy (Политика паролей)** — определяет параметры парольной защиты для доменных или локальных учетных записей, например обязательный ввод пароля или срок его действия;
- **Account Lockout Policy (Политика блокировки учетной записи)** — определяет, когда и какие доменные или локальные учетные записи будут заблокированы;
- **Kerberos Policy (Политика Kerberos)** — определяет параметры протокола Kerberos для доменных учетных записей, например срок жизни билета или принудительные ограничения на вход пользователей.

Внимание! Нет смысла настраивать учетные политики для организационных подразделений (ОП), не содержащих компьютеры, так как ОП, содержащие только пользователей, всегда получают учетную политику от домена.

При настройке политик учетных записей в Active Directory необходимо помнить, что Windows 2000 поддерживает только одну учетную политику домена — назначенную корневому домену в дереве доменов. Такая политика становится стандартной для каждой рабочей станции или сервера, относящихся к этому домену. Единственное исключение из этого правила делается для ОП. Параметры учетной политики для ОП влияют на локальную политику каждого входящего в него компьютера; например, это касается ОП Domain Controllers.

Узел Local Policies

Содержит параметры безопасности компьютера, на котором работает приложение или пользователь. Локальные политики определяются компьютером, на котором регистрируется пользователь, и разрешениями, которые ему предоставлены на данном компьютере. Данная область безопасности содержит следующие атрибуты:

- Audit Policy (Политика аудита) — определяет события, которые регистрируются в журнале безопасности (успешные, неудачные и те и другие), Журнал безопасности является частью оснастки Event Viewer (Просмотр событий);
- **User Rights Assignment (Назначение прав пользователя)** — определяет, какие пользователи и группы обладают правами на вход в систему и выполнение задач;
- **Security Options (Параметры безопасности)** — включают или отключают такие параметры безопасности для компьютера, как цифровая подпись данных, имена учетных записей Administrator (Администратор) и Guest (Гость), доступ к флоппи-дисководам и приводам CD-ROM, установка драйверов и приглашения на вход в систему.

Локальные политики, по определению, применяются к локальному компьютеру. Локальные параметры, импортированные в ОГП Active Directory, влияют на локальные параметры безопасности каждого компьютера, к которому применяется данный ОГП.

Узел Event Log

В этой области безопасности определяются атрибуты, относящиеся к журналам Application (Журнал приложений), Security (Журнал безопасности) и System (Журнал системы): максимальный размер, права доступа к каждому журналу, а также способы их хранения (рис. 13-1).

При разработке плана безопасности предприятия следует определить размер и способ отображения журнала событий согласно требованиям к работе и безопасности. Для реализации преимуществ групповой политики используйте эти параметры просмотра событий на уровне сайта, домена или ОП.

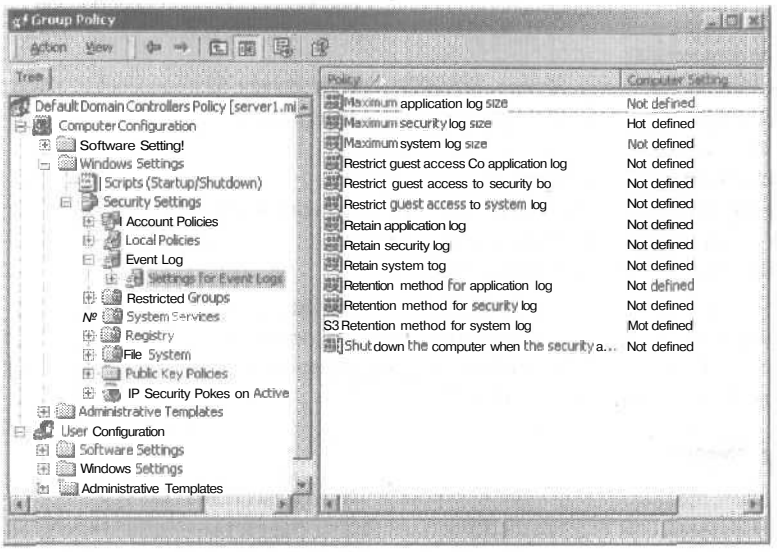


Рис. 13-1. Параметры журналов событий

Узел Restricted Groups

Данная возможность является новым важным средством безопасности, распространяющимся на членов группы. Группы с ограниченным доступом автоматически обеспечивают безопасность на основе членства в стандартных группах Windows 2000, таких, как Administrators (Администраторы), Power Users (Опытные пользователи), Print Operators (Операторы печати), Server Operators (Операторы сервера) и Domain Admins (Администраторы домена), автоматически включены в состав Restricted Groups. Позже в список безопасности групп с ограниченным доступом можно добавить другие требуемые группы или разрешения.

Например, группа Power Users автоматически входит в состав Restricted Groups, так как это стандартная группа Windows 2000. Предположим, в нее включены два пользователя: Алексей и Борис. С помощью оснастки Active Directory Users and Computers (Active Directory — пользователи и компьютеры) Борис добавляет в эту группу Сергея, чтобы тот заменил его во время отпуска. Однако после отпуска он забывает удалить Сергея из этой группы. В итоге в группе Power Users останется не уполномоченный пользователь. Настройка безопасности средствами Restricted Groups поможет предотвратить такую ситуацию. Поскольку узел Power Users ниже Restricted Groups содержит сведения только об Алексее и Борисе, Сергей будет автоматически удален из группы.

Такой механизм гарантирует соблюдение заданного состава групп. Группы и пользователи, не перечисленные в узле Restricted Groups, удаляются при повторном применении политики. Кроме того, вариант восстановления членства гарантирует, что каждая группа с ограниченным доступом является членом только групп, присутствующих в столбце Member Of (Входит в состав), Поэтому группы с ограниченным доступом должны применяться главным образом для настройки членства в локальных группах на рабочих станциях и серверах.

Узел System Services

Эта область безопасности применяется для настройки параметров безопасности и загрузки системных служб компьютера.

Отсюда вы вправе задать свойства объекта-службы, касающиеся безопасности: какие учетные записи обладают разрешениями на его чтение/запись/удаление/выполнение, параметры наследования, аудита и владения.

Возможны следующие режимы запуска:

- Automatic (автоматически) — служба автоматически запускается при загрузке системы;
- Manual (вручную) — служба запускается только вручную;
- Disabled (запрещен) — службу нельзя запустить.

Если запуск системной службы выполняется автоматически, проверьте, чтобы для запуска службы не требовалось вмешательство пользователя. Проследите, какие системные службы работают на компьютере. Для повышения производительности настройте запуск вручную для ненужных или неиспользуемых служб.

Узлы Registry и File System

Эти области безопасности предназначены для настройки зашиты разделов реестра и объектов файловой системы. Отсюда вы вправе настроить свойства соответствующих объектов, касающиеся безопасности: какие учетные записи обладают разрешениями на его чтение/запись/удаление/выполнение, параметры наследования, аудита и владения.

Узел Public Key Policies

Эта область безопасности предназначена для настройки агентов восстановления шифрованных данных, доменных корней и доверенных центров сертификации.

Узел IP Security Policies

Эта область безопасности предназначена для настройки безопасного обмена данными в IP-сетях.

Резюме

На этом занятии вы познакомились с параметрами конфигурации безопасности нелокальных ОГП.

Занятие 2. **Аудит**

Это занятие посвящено аудиту Windows 2000, как средству управления сетевой безопасностью. Аудит позволяет следить за действиями пользователей и общесистемными событиями. Вы узнаете о политиках аудита, факторах, которые необходимо учитывать при их настройке, и о том, как настроить аудит ресурсов.

Изучив материал этого **занятия,** вы сможете:

- ✓ описать цель аудита;
- V спланировать стратегию аудита и определить события, подлежащие аудиту;
- ✓ настроить политику аудита;
- ✓ настроить аудит файлов и папок, объектов Active Directoryи принтеров.

Продолжительность **занятия** — около 60 **минут.**

Общие сведения

Под *аудитом* (auditing) в Windows 2000 подразумевается процесс контроля действий пользователей и операционной системы, которые называются *событиями* (events). Посредством аудита определяются события, которые необходимо записать в журнал безопасности, например попытки законного и незаконного входа в систему, события, связанные с созданием, открытием или удалением файлов, и др. Каждая запись в журнале безопасности содержит следующую информацию:

- описание действия;
- имя пользователя, который его совершил;
- время и результат (успех или неудача) события.

Использование политики аудита

Политика аудита (audit policy) определяет категории событий, которые записываются в журнал безопасности каждого компьютера. Журнал безопасности позволяет регистрировать любые события, которые вы укажете.

Событие записывается в журнал безопасности того компьютера, где оно произошло. Например, неудачная попытка войти в компьютер домена фиксируется в журнале безопасности контроллера домена, так как именно он не смог удостовериться в личности пользователя.

Политика аудита позволяет:

- выявить успешные и неудачные события, например попытки войти в систему, доступ к определенным файлам, изменение учетных записей пользователей, членство групп и другие параметры безопасности;
- устранить или минимизировать риск непредусмотренного использования ресурсов.

Для просмотра событий, записанных в журнал безопасности, применяется консоль Event Viewer. Кроме того, консоль позволяет архивировать журналы. Это дает возможность проследить тенденции, например определить использование принтеров или файлов или выявить динамику попыток несанкционированного доступа к ресурсам.

Рекомендации по настройке политики аудита

При планировании политики аудита необходимо определить компьютеры, подлежащие аудиту, и события, которые требуется на них регистрировать. По умолчанию аудит выключен.

После определения подлежащих аудиту событий необходимо выбрать, какие события стоит регистрировать: успешные, неудачные или и те, и другие. Регистрация успешных событий покажет, как часто пользователи и операционная система обращаются к файлам, принтерам и другим объектам. Эта информация пригодится при планировании использования ресурсов. Регистрация неудачных событий выявит нарушения безопасности. Например, при обнаружении нескольких неудачных попыток доступа, особенно в нерабочее время, можно сделать вывод, что кто-то пытается проникнуть в систему.

Ниже перечислены правила, которыми следует руководствоваться при настройке политики аудита.

- **Определите, собираетесь ли вы контролировать тенденции использования системы.** В этом случае надо архивировать журналы событий. Это позволит проследить изменение использования системных ресурсов во времени и нарастить их до того, как выявится их нехватка.
- **Регулярно просматривайте** журнал **безопасности.** Для этого составьте расписание и следуйте ему. Ведь одного аудита недостаточно для обнаружения нарушений режима безопасности.
- **Политика аудита должна быть полезна и управляема.** Всегда выполняйте аудит уязвимых и конфиденциальных данных. Регистрируйте только те события, которые содержат существенную информацию. Это сократит использование ресурсов сервера и время поиска необходимых данных. Аудит слишком большого числа событий приведет к чрезмерной нагрузке на ресурсы Windows 2000.
- **Настройте аудит доступа к ресурсам для группы Everyone, а не для группы Users.** Таким образом, вы проведете аудит доступа, всех, кто подключается по сети, а не только пользователей, для которых созданы учетные записи. Настройте также аудит неудачных попыток доступа для группы Everyone.
- **Настройте аудит всех действий администраторов.** Это позволит выявить все дополнения или изменения, сделанные администраторами.

Виды аудита

Политика аудита зависит от роли компьютера в сети и различается для следующих типов компьютеров:

- для изолированного/рядового сервера или компьютера под управлением Windows 2000 Professional политика аудита задается индивидуально. Для аудита локальных событий назначается локальная групповая политика, которая распространяется только на один компьютер;
- для контроллеров домена определяется общая для всего домена политика аудита. Она настраивается для нелокального ОГП домена, который применяется ко всем контроллерам домена и доступен в окне свойств ОП Domain Controllers.

И контроллеры домена, и остальные компьютеры в сети имеют одинаковые категории событий.

Требования к аудиту

Для настройки и администрирования аудита требуется:

- для настройки политики аудита и просмотра журнала безопасности необходимо иметь право Manage Auditing And Security Log (Управление аудитом и журналом безопасное-

ти). По умолчанию оно предоставлено группе Administrators (подробнее о правах пользователей — на занятии 4);

- файлы и папки, подлежащие аудиту, надо расположить на томе NTFS.

Настройка аудита

Процесс настройки аудита состоит из двух частей.

1. Задание политики аудита. Разрешает аудит объектов, но не активизирует его.
2. **Активизация аудита.** Здесь надо указать события файлов, папок, принтеров и объектов Active Directory, которые будет выявлять и регистрировать операционная система.

Настройка политики аудита

Первый этап настройки аудиторского ОГП (объекта групповой политики) заключается в выборе категорий событий. Для каждой категории необходимо определить, какие события будут регистрироваться: успешные, неудачные или и те, и другие. Для назначения политики аудита применяется оснастка Group Policy. Журнал безопасности имеет ограниченный объем, поэтому внимательно выбирайте события и учитывайте размер дискового пространства, которое вы можете под него выделить. В табл. 13-1 перечислены категории событий, подлежащие аудиту в Windows 2000.

Табл. 13-1. События, подлежащие аудиту в Windows 2000

Категория событий	Описание
Account logon events (Аудит входа в систему)	Контроллер домена получает запрос на подтверждение учетной записи пользователя
Account management (Аудит управления учетными записями)	Администратор создает, изменяет или удаляет учетную запись пользователя или группы. Под этим подразумевается включение, отключение или изменение имени учетной записи, задание или изменение пароля
Directory service access (Аудит доступа к службе каталогов)	Пользователь получает доступ к объекту Active Directory. Аудиту подвергаются только указанные объекты Active Directory
Logon events (Аудит событий входа в систему)	Пользователь входит или выходит из системы, устанавливает или закрывает сетевое соединение
Object access (Аудит доступа к объектам)	Пользователь получает доступ к файлу, папке или принтеру. Аудиту подвергаются только указанные объекты
Policy change (Аудит **изменения** политики)	**События, связанные с изменением параметров безопасности, прав** пользователей **и политик** аудита
Privilege use (Аудит использования привилегий)	Пользователь применяет предоставленное ему право, например изменяет системное время (к ним не относятся права, связанные с входом и выходом из системы)
Process tracking (Аудит **отслеживания процессов)**	События, сгенерированные программами. В основном эта информация требуется программистам для отладки своих приложений
System events (Аудит системных событий)	Перезагрузка или выключение компьютера и события, связанные с безопасностью Windows 2000 или журналом безопасности (например, удаление ненужных записей вследствие переполнения журнала)

► Настройка политики аудита для контроллера домена

1. Откройте оснастку Active Directory Users and Computers (Active Directory — пользователи и компьютеры).
2. В дереве консоли щелкните правой кнопкой мыши ОП Domain Controllers и выберите команду Properties (Свойства).
3. Перейдите на вкладку Group Policy (Групповая политика), выберите политику и щелкните кнопку Edit (Изменить).
4. Откроется оснастка Group Policy (Групповая политика). В дереве консоли раскройте узел Computer Configuration\Windows Settings\Security Settings\Local Policies (Конфигурация компьютера\ Параметры Windows\Параметры безопасности\Локальные политики) и щелкните папку Audit Policy (Политика аудита).

   В правой панели появятся текущие параметры политики аудита (рис. 13-2).

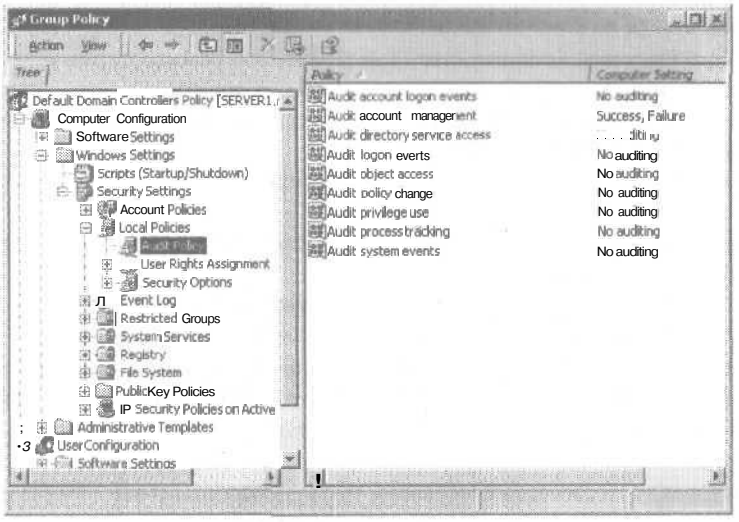


Рис. 13-2. Пользовательская консоль, где отображаются события, подлежащие аудиту в Windows 2000

5. В правой панели щелкните правой кнопкой мыши нужную категорию событий и выберите команду Security (Безопасность).
6. В диалоговом окне Template Security Policy Setting (Параметр шаблона политики безопасности) отметьте флажок Define These Policy Settings In The Template (Определить следующий параметр политики в шаблоне), а затем — следующие флажки (рис. 13-3):
   - Success (Успех) — для аудита успешных событий из выбранной категории;
   - Failure (Отказ) — для аудита неудачных событий из выбранной категории.
7. Щелкните OK.
8. Изменения вступят в силу только при следующем применении политики. Чтобы инициировать политику, выполните одно из следующих действий:
   - в командной строке наберите **secedit /refreshpolicy machine_policy** и нажмите Enter;
   - перезагрузите компьютер;
   - дождитесь автоматического применения политики. Период применения политики настраивается, по умолчанию он равен 8 часам.

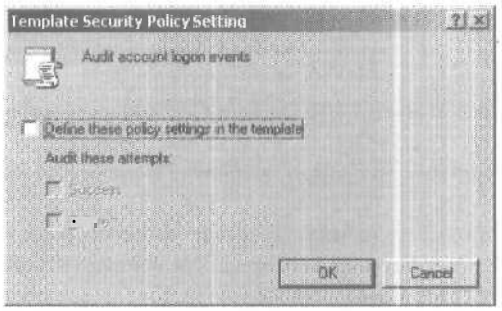


Рис. 13-3. Диалоговое окно Template Security Policy Setting (Параметр шаблона политики безопасности)

► **Настройка политики аудита на компьютере, не входящем в домен**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и выберите команду Local Security Policy (Локальная политика безопасности).
2. В дереве консоли дважды щелкните папку Local Policies (Локальные политики), а затем — Audit Policy (Политика аудита).
3. В правой панели щелкните правой кнопкой мыши нужную категорию событий и выберите команду Security (Безопасность).
4. В диалоговом окне Local Security Policy Setting (Параметр локальной политики безопасности) (рис. 13-4) отметьте:
   - Success (Успех) — для аудита успешных событий из выбранной категории;
   - Failure (Отказ) — для аудита неудачных событий из выбранной категории.

   Окно Effective Policy Setting (Параметр действующей политики) показывает текущие значения параметров безопасности системы. Если политика аудита уже задана на уровне домена или ОП, она заменит локальную политику аудита.
5. Щелкните OK.
6. Изменения вступят в силу только при следующем применении политики. Чтобы принудительно обновить политику, выполните одно из следующих действий:
   - в командной строке наберите **secedit /refreshpolicy machine_policy** и нажмите Enter;
   - перезагрузите компьютер;
   - дождитесь автоматического применения политики. Период применения политики настраивается, по умолчанию он равен 8 часам.

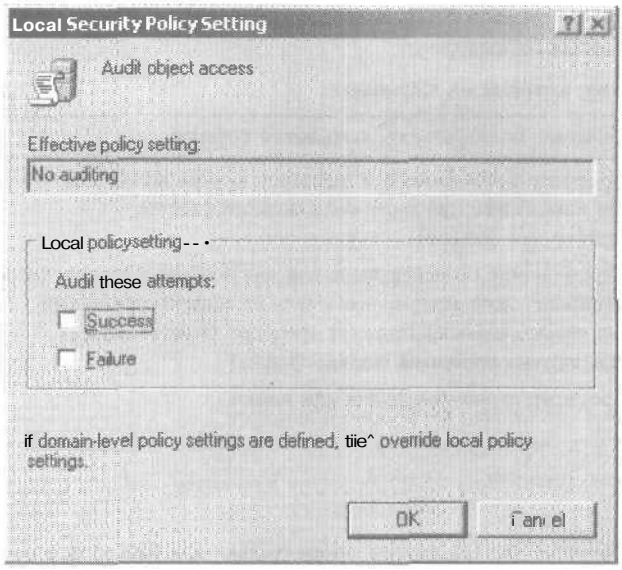


Рис. 13-4. Диалоговое окно Local Security Policy Setting (Параметр локальной политики безопасности)

► **Настройка политики аудита на рядовом сервере или рабочей станции домена**

1. Создайте ОП для удаленного компьютера и добавьте в него учетные записи нужных машин.
2. С помощью оснастки Active Directory Users and Computers настройте политику аудита, как описано выше в разделе «Настройка политики аудита».

Примечание Аудит событий для рабочих станций, рядовых серверов и контроллеров домена разрешено удаленно настраивать только администраторам домена или предприятия.

Аудит доступа к файлам и папкам

Если вы хотите обезопасить систему, настройте аудит файлов и папок на разделах NTFS. Для этого политика аудита должна включать категорию событий Audit Object Access (Лудит доступа к объектам). После настройки политики аудита необходимо назначить аудит файлов и папок. Для этого укажите виды доступа, пользователей и группы, для которых будет выполняться аудит.

► **Настройка аудита файлов и папок**

1. Откройте Windows Explorer, щелкните правой кнопкой мыши файл или папку и выберите команду Properties (Свойства).
2. На вкладке Security (Безопасность) щелкните кнопку Advanced (Дополнительно).
3. В окне Access Control Settings For (Параметры управления доступом для) на вкладке Auditing (Аудит) щелкните кнопку Add (Добавить). Выберите пользователей и группы, для которых хотите выполнить аудит, и щелкните OK.
4. В окне Auditing Entry For (Элемент аудита для) отметьте нужные события флажками Successful и(или) Failed (рис. 13-5).

В табл. 13-2 перечислены события файлов и папок, подлежащие аудиту в Windows 2000, и действия пользователя, которые их вызывают.

Табл. 13-2. События и действия, которые их вызывают

Событие	Действие пользователя, вызвавшее событие
List Folder/Read Data (Содержание папки/ Чтение данных)	Просмотр имен файлов и подпапок внутри папки (только для папок) или просмотр содержимого файлов (только для файлов)
Traverse Folder/Execute File (Обзор папок/Выполнение файлов)	Перемещение по иерархии папок для доступа к другим файлам и папкам, даже если пользователь не имеет разрешений для папок, через которые он проходит (только папки) или запуска программ (только файлы)
Read Attributes (Чтение атрибутов) и Read Extended Attributes (Чтение дополнительных атрибутов)	Просмотр атрибутов файла или папки
Create Files/Write Data (Создание фалов/Запись данных)	Создание файлов внутри папки (только для папок) или изменение содержимого файла (только для файлов)
Create Folders/Append Data (Создание папок/ Дозаписьданных)	Создание подпапок внутри папки (только для папок) и добавление данных к концу файла, но не изменение или удаление существующих данных (только для файлов)
Write Attributes (Запись атрибутов) и Write Extended Attributes (Запись дополнительных атрибутов)	Изменение атрибутов файла или папки
Delete Subfolders And Files (Удаление подпапок и файлов)	Удаление файла или подпапки внутри папки
Delete (Удаление)	Удаление файла или папки
Read Permissions (Чтение разрешений)	Просмотр разрешений или владельца файла или папки
Change Permissions (Смена разрешений)	Изменение разрешений файла или папки
Take Ownership (Смена владельца)	Смена владельца файла или папки

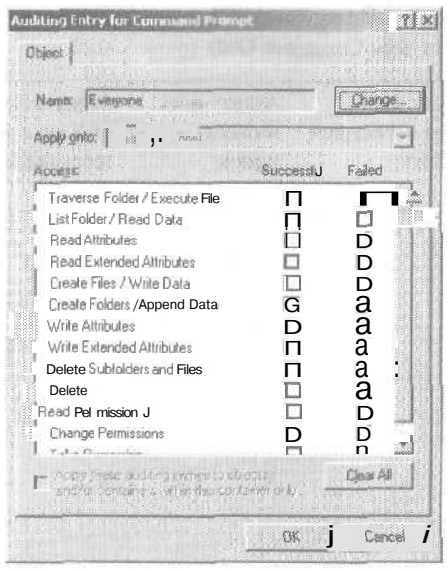


Рис. 13-5. Диалоговое окно Auditing Entry (Элемент аудита) для файла Command Prompt

5. В списке Apply Onto (Применять) (доступен только для папок) выберите область применения аудита. По умолчанию — This Folder, Subfolders And Files (Для этой папки, ее подпапок и файлов). Это значит, что все изменения свойств текущей папки, связанные с аудитом, охватывают вложенные файлы и папки. Кроме значения, выбранного из списка Apply Onto, на область аудита влияет флажок Apply These Auditing Entries To Objects And/Or Containers Within This Container Only (Применять этот аудит к объектам и контейнерам только внутри этого контейнера) (табл. 13-3).

Табл. 13-3. Результат сброса флажка Apply These Auditing Entries To Objects And/Or Containers Within This Container Only

Значение из списка Apply Onto (Применять)	Аудит текущей папки	Аудит подпапок в текущей папке	Аудит файлов в текущей папке	Аудит всех нижестоящих папок	Аудит всех файлов в нижестоящих папках
This folder only (Только для этой папки)	X				
This folder, subfolders, and files (Для этой папки, ее подпапок и файлов)	X	X	X	X	X

Табл. 13-3. Результат сброса флажка Apply These Auditing Entries To Objects And/Or Containers WithinThis Container Only *(окончание)*

Значение из списка Apply Onto (Применять)	Аудит текущей папки	Аудит подпалок в текущей папке	Аудит файлов в текущей папке	Аудит всех нижестоящих папок	Аудит всех фактов в нижестоящих папках
This folder and subfolders (Для этой папки и ее подпапок)	X	X		X	
This folder and files (Для этой папки и ее файлов)	X		X		X
Subfolders and files only (Только для подпапок и файлов)		X	X	X	X
Subfolders only (Только для подпапок)		X		X	
Files only (Только для файлов)			X		X

Когда отмечен флажок Apply These Auditing Entries To Objects And/Or Containers Within This Container Only, аудит распространяется на объекты, указанные в поле Apply Onto и все вложенные объекты.

6. Щелкните OK, чтобы вернуться в диалоговое окно Access Control Settings For.
7. Чтобы выбранный объект не наследовал свойств родительской папки, снимите флажок Allow Inheritable Auditing Entries From Parent To Propagate To This Object (Переносить наследуемый от родительского объекта аудит на этот объект).

   Если в диалоговом окне Auditing Entry For флажки затемнены или в диалоговом окне Access Control Settings For (Параметры управления доступом для) недоступна кнопка Remove (Удалить), значит, аудит наследуется от родительской папки.
8. Щелкните OK.

Аудит доступа к объектам Active Directory

По аналогии с файлами и лапками для аудита доступа к объектам Active Directory необходимо настроить политику аудита и назначить аудит определенных объектов, например пользователей, компьютеров, ОП, групп.

▶ **Настройка аудита объектов Active Directory**

1. Откройте оснастку Active Directory Users and Computers (Active Directory — пользователи и компьютеры) и выберите в меню View (Вид) команду Advanced Features (Дополнительные функции).

2. Выберите нужный объект, в меню Action (Действие) щелкните команду Properties (Свойства), перейдите на вкладку Security (безопасность) и щелкните кнопку Advanced (Дополнительно).
3. В диалоговом окне Access Control Settings (Параметры управления доступом) перейдите на вкладку Auditing (Аудит) и щелкните кнопку Add. Укажите пользователей и группы, для которых вы собираетесь вести аудит, и щелкните OK.
4. В диалоговом окне Auditing Entry For (рис. 13-6) отметьте нужные события флажками Successful и(или) Failed.

В табл. 13-4 перечислены события объектов Active Directory, подлежащие аудиту в Windows 2000, и действия пользователя, которые их вызывают.

Табл. 13-4. События объектов Active Directory и действия пользователей, которые их вызывают

Событие	Действие пользователя, вызвавшее событие
Full Control (Полный доступ)	Любой вид доступа к объекту аудита
List Contents (Список содержимого)	Просмотр объектов внутри объекта аудита
Read All Properties (Чтение всех свойств)	Просмотр атрибутов объекта аудита
Write All Properties (Запись всех свойств)	Изменение атрибутов объекта аудита
Create All Child Objects (Создание всех дочерних объектов)	Создание объектов внутри объекта аудита
Delete All Child Objects(Удаление всех дочерних объектов)	Удаление объектов внутри объекта аудита
Read Permissions (Чтение разрешений)	Просмотр разрешений объекта аудита
Modify Permissions (Смена разрешений)	Изменение разрешений объекта аудита
Modify Owner (Смена владельца)	Смена владельца объекта аудита

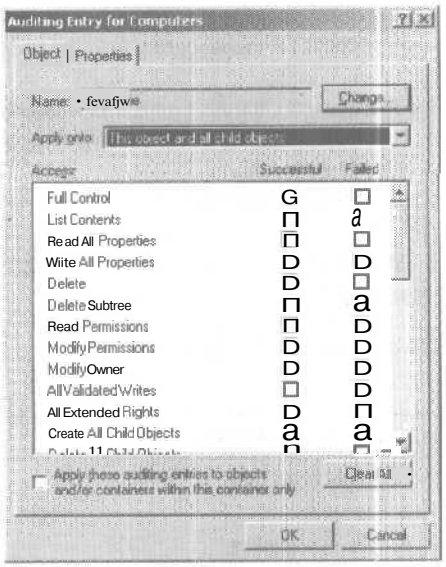


Рис. 13-6. Диалоговое окно Auditing Entry For для папки Computers

5. В списке Apply Onto выберите область распространения аудита. По умолчанию — This Object And All Child Objects (Этот объект и все дочерние объекты). Это значит, что все изменения свойств текущей папки, связанные с аудитом, распространяются на вложенные файлы и папки. Кроме значения, выбранного в списке Apply Onto, на область распространения аудита влияет флажок Apply These Auditing Entries To Objects And/Or Containers Within This Container Only (табл. 13-3). Оба параметра доступны для объектов, служащих контейнерами.
6. Щелкните OK, чтобы вернуться в диалоговое окно Access Control Settings For.
7. Чтобы выбранный объект не наследовал свойств родительской папки, снимите флажок Allow Inheritable Auditing Entries From Parent To Propagate To This Object.

   Если в диалоговом окне Auditing Entry For флажки затемнены или в диалоговом окне Access Control Settings For недоступна кнопка Remove, то аудит наследуется от родительского объекта.
8. Щелкните OK.

Аудит доступа к принтерам

Чтобы назначить аудит принтеров, политика аудита должна включать категорию событий Audit Object Access (Аудит доступа к объектам). После настройки политики аудита надо включить аудит принтеров, то есть указать виды доступа, пользователей и группы, для которых он будет выполняться. Порядок действий совпадает с порядком при настройке аудита файлов и папок.

▶ **Настройка аудита принтеров**

1. Раскройте меню Start\Settings (Пуск\Настройка) и выберите команду Printers (Принтеры).
2. В системной папке Printers щелкните правой кнопкой мыши принтер и затем в контекстном меню — команду Properties.
3. В окне свойств принтера выберите вкладку Security и щелкните кнопку Advanced.

4. В диалоговом окне Access Control Settings выберите вкладку Auditing и щелкните кнопку Add. Укажите пользователей и группы, для которых вы собираетесь выполнить аудит, и щелкните OK.
5. В диалоговом окне Auditing Entry For (рис. 13-7) отметьте нужные события флажками Successful и(или) Failed.

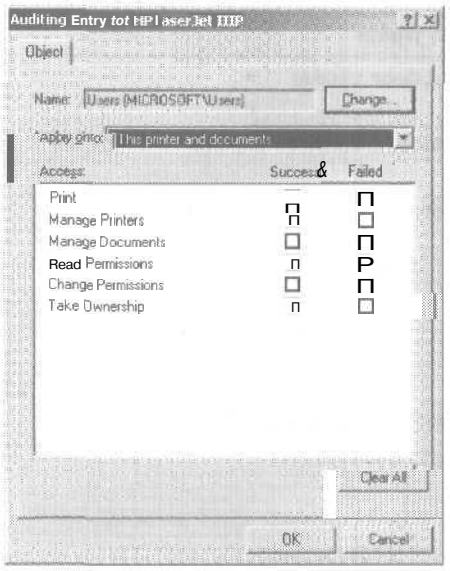


Рис. 13-7. Диалоговое окно Auditing Entry For для принтера

В табл. 13-5 перечислены события принтеров и действия пользователя, которые их вызывают.

Табл. 13-5. События принтера и действия пользователей, которые их вызывают

Событие	Действие пользователя, вызвавшее событие
Print (Печать)	Печать файла
Manage Printers (Управление принтерами)	Изменение параметров принтера, остановка приостановка печати, открытие доступа к принтеру или удаление принтера
Manage Documents (Управление документами)	Изменение параметров задания, остановка, повторный запуск, перемещение или удаление документов, выделение общего принтера и изменение свойств принтера
Read Permissions (Чтение разрешений)	Просмотр разрешений принтера
Change Permissions (Смена разрешений)	Изменение разрешений принтера
Take Ownership (Смена владельца)	Смена владельца принтера

6. В списке Apply Onto выберите область распространения аудита.
7. **Щелкните OK.**

Практическая польза от аудита

В табл. 13-6 перечислены события и соответствующие им угрозы безопасности, ликвидируемые посредством аудита.

Табл. 13-6. События, аудит которых рекомендован

Событие, подлежащее аудиту	Потенциальная угроза
Неудачные попытки входа/выхода из системы	Взлом путем подбора пароля
Успешные попытки входа/выхода из системы	Взлом с помощью украденного пароля
Применение пользователем своих прав, управление пользователями и группами, изменение политики безопасности, включение и выключение компьютера, системные события	Злоупотребление привилегиями
События, связанные с доступом к файлам и другим объектам. Аудит доступа на чтение или запись секретных файлов из диспетчера файлов подозрительными пользователями или группами	Несанкционированный доступ к файлам
Аудит успешного и неуспешного доступа к файловым принтерам, а также аудит событий доступа к объектам. Аудит доступа к принтерам через диспетчер печати подозрительными пользователями или группами	Несанкционированный доступ к принтерам
События, связанные с записью программных файлов (.exe или .dll). События, генерируемые процессами. Запуск определенных программ. Попытки изменения программных файлов и создания непредусмотренных процессов	Заражение данных вирусом

Практикум: аудит ресурсов и событий

Спроектируйте политику аудита и настройте ее для контроллера домена. Назначьте аудит файла, принтера и объекта Active Directory.

Упражнение 1: проектирование политики аудита домена

Спроектируйте политику аудита для вашего сервера. Для этого определите;

- типы событий, для которых вы хотите вести аудит;
- результат событий (успех, неудача), для которых вы хотите выполнить аудит.

Подумайте, какие операции вы хотите осуществить:

- аудит непредусмотренных попыток доступа к сети;
- запись событий неавторизованного доступа к файлам, составляюшим БД Customer;
- аудит использования цветного принтера;
- выявление попыток нанести ущерб оборудованию сервера;
- запись действий, которые администратор предпринимает для выявления неавторизованных изменений;
- аудит резервного копирования, препятствующий краже информации;
- аудит неавторизованного доступа к объектам Active Directory.

Принятые решения запишите в таблицу (табл. 13-7).

Табл. 13-7. План политики аудита для упражнения 1

Действие, подлежащее аудиту	Успех	Неудача
Account logon events (Аудит входа в систему)		
Account management (Аудит управления учетными записями)		
Directory service access (Аудит доступа к службе каталогов)		
Logon events (Аудит событий входа в систему)		
Object access (Аудит доступа к объектам)		
Policy change (Аудит изменения политики)		
Privilege use (Аудит использования привилегий)		
Process tracking (Аудит отслеживания процессов)		
System events (Аудит системных событий)		

Упражнение 2: настройка политики аудита

Включите аудит выбранных категорий событий.

▶ **Задание: активизируйте политику аудита**

1. Откройте оснастку Active Directory Users and Computers (Active Directory — пользователи и компьютеры).
2. В дереве консоли щелкните правой кнопкой мыши ОП Domain Controllers и выберите команду Properties.
3. В окне свойств перейдите на вкладку Group Policy (Групповая политика), выберите групповую политику Default Domain Controllers Policy и щелкните кнопку Edit (Изменить).
4. Откроется оснастка Group Policy. В дереве консоли раскройте узел Computer Configuration\ Windows Settings\Security Settings\Local Policies и щелкните папку Audit Policy.
5. Чтобы установить политику аудита, дважды щелкните каждую категорию событий в правой панели и отметьте флажок Success или Failure, используя табл. 13-8.

Табл. 13-8. Параметры политики безопасности для упражнения 2

Категория события	Успех	Неудача
Account logon events		
Account management	X	
Directory service access		X
Logon events		X
Object access	X	X
Policy change	X	
Privilege use	X	
Process tracking		
System events	X	X

6. Закройте оснастку Group Policy.
7. Закройте окно свойств контроллера домена.
8. В меню Start выберите команду Run (Выполнить).
9. В командной строке наберите **secedit /refreshpolicy machine_policy** и нажмите Enter.
   Новые параметры политики аудита вступят в силу.
10. Закройте окно Run.

Упражнение 3: аудит файлов

Настройте аудит файла.

► Задание 1: настройте аудит файла

1. В Windows Explorer выберите простой текстовый файл.
2. Щелкните правой кнопкой имя файла и из контекстного меню выберите команду Properties.
3. В диалоговом окне свойств выберите вкладку Security (Безопасность) и щелкните кнопку Advanced (Дополнительно).
4. В диалоговом окне Access Control Settings For (Параметры управления доступом для) выберите вкладку Auditing (Аудит).
5. Щелкните кнопку Add (Добавить).
6. В окне Select User, Computer, Or Group (Выбор: Пользователь, Компьютер или Группа) дважды щелкните в списке группу Everyone (Все).
7. В диалоговом окне Auditing Entry For (Элемент аудита) отметьте флажки Successful (Успех) и Failed (Отказ) для каждого из следующих событий:
   - Create Files/Write Data (Создание файлов/Запись данных);
   - Delete (Удаление);
   - Change Permissions (Смена разрешений);
   - Take Ownership (Смена владельца).
8. Щелкните OK.
   Группа Everyone появится в диалоговом окне Access Control Settings For.
9. Щелкните OK, чтобы внести изменения.

► Задание 2: измените разрешения файла

1. В диалоговом окне свойств выберите вкладку Security (Безопасность) и добавьте группу Everyone (Все).

2. Предоставьте разрешения Read (Чтение) группе Everyone и снимите флажок Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект).

   Появится сообщение с просьбой подтвердить ваши действия.
3. Щелкните кнопку Remove (Удалить), затем — OK.

   Все разрешения будут удалены.
4. Щелкните OK, чтобы закрыть окно свойств. Закройте Windows Explorer.

Упражнение 4: аудит принтеров

Настройте аудит принтера.

Примечание Как и для упражнений главы 11, на вашем компьютере должен быть установлен локальный принтер. Однако само устройство печати подключать не обязательно. *Устройство печати* (printing device) ссылается на физическое устройство, предназначенное для печати, а *локальный принтер* (local printer) ссылается на программное обеспечение, которое Windows 2000 использует для отправки данных устройству печати. Если на вашем компьютере не установлен локальный принтер, сделайте это сейчас.

▶ **Задание: настройте аудит принтера**

1. В меню Start\Settings (Пуск\Настройка) выберите команду Printers (Принтеры).
2. В системной папке Printers щелкните правой кнопкой принтер, ассоциированный с вашим компьютером, и выберите команду Properties.
3. Перейдите на вкладку Security и щелкните кнопку Advanced,
4. В диалоговом окне Access Control Settings For выберите вкладку Auditing и щелкните кнопку Add.
5. В диалоговом окне Select User, Computer, Or Group дважды щелкните группу Everyone.
6. В диалоговом окне Auditing Entry For отметьте флажок Successful для всех типов доступа.
7. Щелкните OK.

   Группа Everyone появится в диалоговом окне Access Control Settings For.
8. В диалоговом окне Access Control Settings For щелкните OK, чтобы внести изменения.
9. Щелкните OK, чтобы закрыть окно свойств принтера.
10. Закройте системную папку Printers.

Упражнение 5: аудит объектов Active Directory

Настройте аудит объекта Active Directory.

▶ **Задание: проверьте аудит объекта Active Directory**

1. Откройте оснастку Active Directory Users and Computers.
2. В меню View (Вид) выберите команду Advanced Features (Дополнительные функции).
3. В дереве консоли выберите свой домен.
4. В правой панели выберите ОП Users, а затем в меню Action (Действие) — команду Properties.
5. В диалоговом окне Users Properties (Свойства: Users) перейдите на вкладку Security и щелкните кнопку Advanced.
6. В диалоговом окне Access Control Settings For Users перейдите на вкладку Auditing и дважды щелкните группу Everyone.

   Откроется диалоговое окно Auditing Entry For Users.

Просмотрите стандартные параметры аудита доступа к объекту для группы Everyone. Чем отличаются виды доступа, для которых выполняется аудит, от тех, для которых он не выполняется?

7. Щелкайте OK, чтобы закрыть окна Auditing Entry For Users, Access Control Settings For Users и Users Properties.

   На каких компьютерах будет регистрироваться доступ к объекту Active Directory? Сможете ли вы просмотреть журнал?

8. Закройте оснастку Active Directory Users and Computers.

Резюме

На этом занятии рассказано, как назначить политику аудита. Первый этап настройки политики аудита заключается в выборе категорий событий, подлежащих аудиту в Windows 2000. Для каждой категории необходимо определить, какие события будут регистрироваться: успешные, неудачные или и те, и другие.

Для изолированного/рядового сервера и обычного компьютера под управлением Windows 2000 Professional политика аудита задается индивидуально. Для аудита локальных событий задается локальная групповая политика, которая распространяется только на один компьютер.

Для контроллеров домена задается общая для всего домена политика аудита. Для этого настраивается нелокальная групповая политика, которая распространяется на все контроллеры домена.

Выполняя практикум, вы спроектировали политику аудита для домена, установили ее для контроллеров домена, файла, принтера и объекта Active Directory.

Замятие 3, Использование журнала безопасности

Журнал безопасности содержит информацию о событиях, которые регистрируются в процессе аудита. Для просмотра журнала безопасности применяется консоль Event Viewer (Просмотр событий). Кроме того, консоль позволяет найти и отфильтровать события в журнале и архивировать файлы журнала.

Изучив материал этого занятия, вы сможете:

- ✓ просмотреть журнал;
- ✓ найти события в журнале;
- ✓ фильтровать события в журнале;
- ✓ настроить размер журналов;
- ✓ заархивировать журнал.

Продолжительность занятия — около 25 минут.

Журналы Windows 2000

Консоль Event Viewer применяется для просмотра журналов Windows 2000. По умолчанию в консоли Event Viewer доступны три журнала (табл. 13-9).

Табл. 13-9. Журналы Windows 2000

Журнал	Содержание
Application (Журнал приложений)	Ошибки, предупреждения и информационные сообщения. которые генерируют различные программы, например приложения для работы с базами данных или электронной почты. События, подлежащие регистрации, определяет разработчик программы
Security (Журнал безопасности)	Информация об успешных и неудачных событиях, регистрируемых в ходе аудита. События, подлежащие регистрации, определяются политикой аудита
System (Журнал системы)	Ошибки, предупреждения или информационные сообщения, которые генерирует Windows 2000. События, подлежащие регистрации. определяет операционная система

Системный журнал и журнал приложений доступны для просмотра любым пользователям, в отличие от журнала безопасности, доступ к которому имеют только системные администраторы. По умолчанию регистрация событий в журнале безопасности отключена. Чтобы ее активизировать, необходимо на соответствующем уровне средствами групповой политики назначить политику аудита.

Примечание Установка служб может привести к появлению дополнительных журналов. Например, служба DNS регистрирует свои события в журнале DNS server.

Просмотр журналов безопасности

Журнал безопасности содержит информацию о событиях, регистрируемых в процессе аудита, например успешные и неудачные попытки доступа.

► Просмотр журнала безопасности

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Event Viewer (Просмотр событий).
2. В дереве консоли выберите Security Log (Журнал безопасности).

   В правой панели появится список записей журнала и итоговая информация по каждому пункту (рис. 13-8).

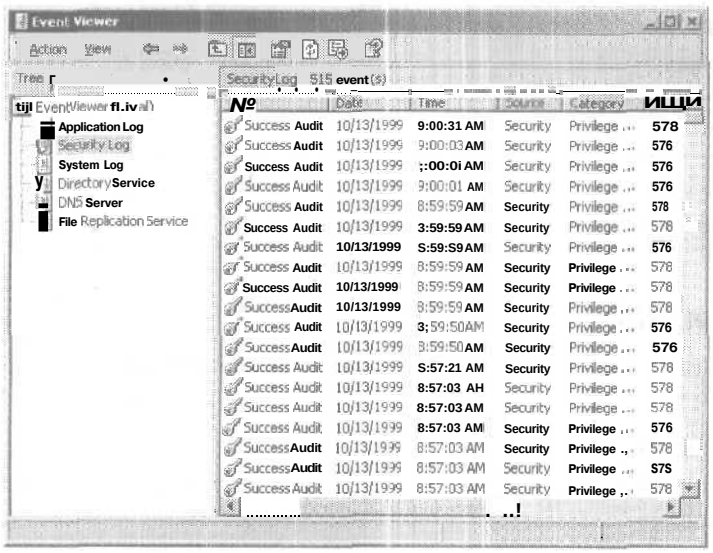


Рис. 13-8. Пример журнала безопасности

Успешные события обозначаются значком ключа, а неудачные — замка. Остальная информация — это дата и время возникновения события, категория события и пользователя, который его сгенерировал.

Поле Category (Категория) означает категорию события, например Object access (Доступ к объекту) или Logon events (События входа).

3. Для просмотра дополнительной информации о событии дважды щелкните его значок.

   Событие записывается в журнал безопасности того компьютера, где оно произошло. При наличии прав администратора журнал безопасности можно просмотреть с удаленного компьютера.

► Просмотр журнала безопасности удаленного компьютера

1. Убедитесь в том, что на удаленном компьютере включен аудит события (см. занятие 2).
2. Раскройте меню Start\Programs\Administrative Tools и щелкните Event Viewer.
3. Щелкните правой кнопкой мыши узел Event Viewer (Local) и выберите команду Connect To Another Computer (Подключиться к другому компьютеру).
4. В поле Another Computer (другим компьютером) диалогового окна Select Computer (Выбор компьютера) введите нужное имя сети, IP-адрес или DNS-имя. Вы можете также выбрать имя компьютера в стандартном диалоговом окне.
5. Щелкните OK.

Поиск событий

По умолчанию Event Viewer показывает все события, записанные в журнал безопасности. Для поиска определенных событий используется команда Find (Найти).

▶ **Поиск событий**

1. Откройте Event Viewer, в дереве консоли выберите Security Log, а затем в меню View (Вид) — команду Find (Найти).
2. В диалоговом окне Find In (Поиск) настройте условия поиска (рис. 13-9, табл. 13-10).

Табл. 13-10. Параметры диалогового окна Find In

Элемент управления	Описание
Event Types (Типы событий)	Здесь можно указать любое событие, подлежащее аудиту в Windows 2000
Event Source (Источник события)	Программы и драйверы, сгенерировавшие событие
Category (Категория)	Категория событий, например попытки входа/выхода или системные события
Event ID (Код события)	Идентификатор события. Применяется специалистами, отвечающими за поддержку программного обеспечения, для наблюдения за событиями
User (Пользователь)	Имя пользователя
Computer (Компьютер)	Имя компьютера
Description (Описание)	Поиск текста в описании события
Search Direction (Направление поиска)	Направление поиска (вверх, вниз)
Find Next (Найти далее)	Запускает поиск события, удовлетворяющего указанным условиям

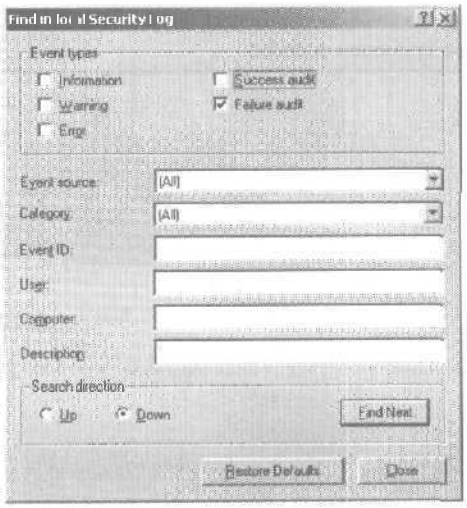


Рис. 13-9. Диалоговое окно Find In (Поиск)

Фильтрование событий

Фильтрование позволяет отображать события, удовлетворяющие определенным условиям, например попытки редактирования текстового файла без соответствующего разрешения.

▶ **Фильтрование событий**

1. Откройте Event Viewer, в дереве консоли выберите Security Log, а затем в меню View — команду Filter (Фильтр).
2. В диалоговом окне Security Log Properties (Свойства: Журнал системы) выберите вкладку Filter (Фильтр) и настройте параметры фильтра (рис. 13-10, табл. 13-11).

Табл. 13-11. Параметры вкладки Filter диалогового окна свойств журнала

Параметр	Описание
Event Types (Типы событий)	Здесь можно указать любое событие, подлежащее аудиту в Windows 2000
Event Source (Источник события)	Программы и драйверы, сгенерировавшие событие
Category (Категория)	Категория событий, например, попытки входа/выхода или системные события
Event ID (Код события)	Идентификатор события. Применяется специалистами, отвечающими за поддержку программного обеспечения, для наблюдения за событиями
User (Пользователь)	Имя пользователя
Computer (Компьютер)	Имя компьютера
From (С)	Верхняя граница интервала событий. Принимает два значения: First Event (первого) — все события, начиная с первого, и Events On (момента) — начиная с указанного времени и даты
To (По)	Нижняя граница интервала событий- Принимает два значения: Last Event (последнего) — все события, заканчивая последним, и Events On (момента) — заканчивая указанным временем и датой

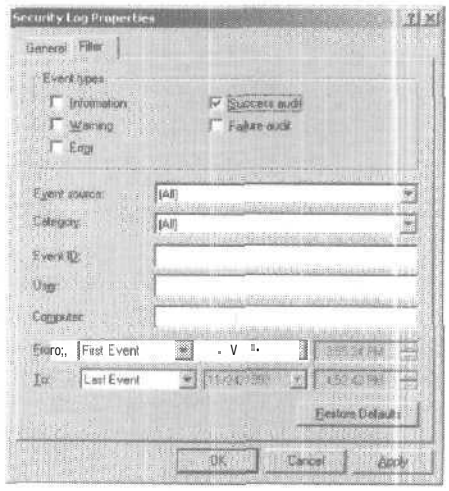


Рис. 13-10. Вкладка Filter (Фильтр) окна свойств журнала

Настройка журнала безопасности

Регистрация событий начинается после настройки политики аудита на контроллере домена или локальном компьютере и прекращается при заполнении журнала в том случае, если не задана автоматическая очистка журнала или если событий много, но они не такие старые, чтобы их удалять. При прекращении регистрации событий в журнал приложений записывается ошибка. Чтобы избежать переполнения журнала, регистрируют только ключевые события. Вы можете сами настроить свойства каждого журнала.

► **Настройка журналов безопасности**

1. Откройте консоль Event Viewer.
2. Щелкните правой кнопкой мыши журнал безопасности в дереве консоли и выберите команду Properties.
3. В диалоговом окне Security Log Properties на вкладке General (Общие) выберите нужную конфигурацию (рис. 13-11, табл. 13-12).

Табл. 13-12. Параметры вкладки General

Параметр	Описание
Display Name (Выводимое имя)	Вы можете создать несколько различных отображаемых имен для одного журнала или журналов других компьютеров
Log Name (**Имя** журнала)	Полный путь к файлу журнала
Maximum Log Size (Максимальный размер журнала)	**Размер журнала.** Принимает **значения от 64 кб до 4 194 240 кб** (4Гб). **По умолчанию — 512** кб
Overwrite Events As Needed (Затирать старые события по необходимости)	Указывает, что при переполнении журнала старые события будут заменяться новыми. Будьте внимательны при использовании этого параметра, так как можно не заметить подозрительные события
Overwrite Events Older Than *X* Days (Затирать события старее *X* дней)	Определяет, сколько дней (1—365) событие должно храниться в журнале. Новые события не будут регистрироваться, если журнал полностью заполнен, но не содержит событий старше указанной даты
Do Not Overwrite Events (Clear Log Manually) [Не затирать события (очистка журнала вручную)]	Указывает, что события не должны перезаписываться при переполнении журнала. В этом случае придется очищать журнал вручную
Using A Low Speed Connection (Подключение по медленной линии)	Указывает, что файл журнала хранится на другом компьютере, а для соединения с ним используется низкоскоростное устройство, например модем

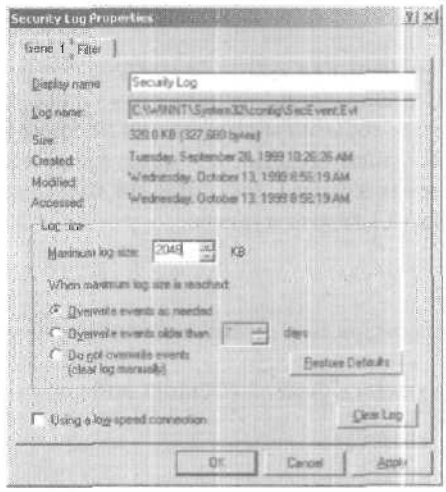


Рис. 13-11. Вкладка General (Общие) окна свойств журнала безопасности

Заполненный журнал можно очистить вручную. При очистке журнала информация о событии удаляется безвозвратно. Чтобы освободить место в журнале для записи новых событий, стоит сократить время хранения события.

▶ **Очистка журнала вручную**

1. Откройте консоль Event Viewer.
2. В дереве консоли щелкните правой кнопкой мыши журнал безопасности и выберите команду Clear Ail Events (Стереть все события).
3. В окне Event Viewer (Просмотр событий);
   - щелкните кнопку Yes, чтобы создать архив журнала перед очисткой;
   - щелкните кнопку No, чтобы немедленноочистить журнал безопасности.
4. В первом случае откроется стандартное диалоговое окно сохранения файла. В поле File Name (Имя файла) наберите имя архива.
5. В раскрывающемся списке Save As Type (Тип файла) выберите формат файла и щелкните кнопку Save (Сохранить).

Архивирование журналов безопасности

Архивирование журналов безопасности позволяет вести историю событий. Многие администраторы хранят архивы журналов в течение определенного периода и время от времени сравнивают накопившуюся информацию. Архив журнала содержит все события, независимо от параметров фильтрования.

▶ **Архивирование журнала безопасности**

1. Откройте консоль Event Viewer.
2. В дереве консоли щелкните правой кнопкой мыши журнал безопасности и выберите команду Save Log File As (Сохранить файл журнала как).
3. В открывшемся окне в поле File Name введите имя файла.
4. В списке Save As Type выберите формат файла и щелкните кнопку Save.

Для архивирования журнала применяется специальный формат (*.evt), который можно просмотреть в Event Viewer. Архивы такого формата имеют двоичную структуру. Журналы, сохраненные в текстовом формате или в текстовом файле с разделением запятыми

(*.txt и *.csv соответственно), можно просмотреть из текстового редактора, например Word. Такие архивы не содержат двоичных данных.

► **Просмотр архива журнала безопасности**

1. Откройте консоль Event Viewer.
2. В дереве консоли щелкните правой кнопкой мыши журнал безопасности и выберите команду Open Log File (Открыть файл журнала).
3. Выберите файл. Возможно, вам понадобится найти его в текущей папке или в другом месте на диске.
4. В списке Log Type (Тип журнала) выберите Security (Безопасность).
5. В поле Display Name (Выводимое имя) наберите имя, которое будет соответствовать данному журналу в дереве консоли и шелкните кнопку Open (Открыть).
   Архивный файл можно удалить в Windows Explorer.

Практикум: использование журнала безопасности

Просмотрите файл журнала безопасности. Настройте консоль Event Viewer так, чтобы при переполнении файла журнала события переписывались. Заархивируйте и очистите файл журнала безопасности.

Внимание! Обязательно выполните все упражнения занятия 2.

Упражнение 1: просмотр журнала безопасности

Просмотрите журнал безопасности. Используйте консоль Event Viewer для фильтрования событий и поиска потенциальных нарушений безопасности.

► **Задание: просмотрите журнал безопасности**

1. Раскройте меню Start\Programs\Administrative Tools и выберите команду Event Viewer.
2. В дереве консоли выберите журнал безопасности и просмотрите его содержимое. Дважды шелкните любое событие, чтобы увидеть его описание.

Упражнение 2: управление журналом безопасности

Настройте консоль Event Viewer так, чтобы при переполнении файла журнала события перезаписывались.

► **Задание: настройте размер и содержимое файла журнала безопасности**

1. В дереве консоли шелкните правой кнопкой мыши журнал безопасности и выберите команду Properties.
2. В окне свойств журнала отметьте флажок Overwrite Events As Needed (Затирать события по необходимости).
3. Измените максимальный размер журнала в поле Maximum Log Size на 2048 кб и щелкните OK.
   Старые события будут заменяться новыми, когда размер журнала достигнет 2048 кб.

Упражнение 3: архивирование и очистка журнала безопасности

Заархивируйте и очистите журнал безопасности. Просмотрите архив журнала.

Задание 1: заархивируйте и очистите журнал безопасности

1. Откройте консоль Event Viewer.
2. В дереве консоли щелкните правой кнопкой мыши журнал безопасности и выберите команду Clear All Events (Стереть все события).
3. Щелкните кнопку Yes, чтобы заархивировать журнал перед очисткой
4. В диалоговом окне Save As в поле File Name наберите имя файла, например archive.
5. Убедитесь, что в списке Save As Type выбран пункт Event Log (*.evt) и щелкните кнопку Save.

Задание 2: просмотрите архив журнала безопасности

1. В дереве консоли щелкните правой кнопкой мыши журнал безопасности и выберите команду Open Log File (Открыть файл журнала).
2. Выберите файл ARCHIVE.EVT (файл, в котором вы сохранили архив в предыдущем задании).
3. В списке Log Type выберите Security.
4. Убедитесь, что поле Display Name приняло значение Saved Security Log, и щелкните кнопку Open.

   Откроется архив журнала. Обратите внимание, что команды Refresh (Обновление) и Clear All Events (Стереть все события) недоступны, так как невозможно обновить или очистить архив.
5. Закройте консоль Event Viewer.

Резюме

На этом занятии вы познакомились с журналом безопасности Windows 2000 и консолью Event Viewer, которая применяется для просмотра, настройки, архивирования журнала и поиска событий.

Выполняя практическую часть занятия, вы научились просматривать журнал безопасности, настраивать консоль Event Viewer так, чтобы события перезаписывались при переполнении журнала, архивировать и очищать журнал.

Занятие 4. Права пользователя

Кроме разрешений, контролирующих доступ к файлам, папкам и принтерам, в Windows 2000 существуют права пользователя, которые предоставляют дополнительные привилегии и права входа.

Изучив материал этого занятия, вы сможете:

- ✓ объяснить возможности, которые дает каждое право пользователя;
- ✓ объяснить возможности, предоставляемые привилегиями и правами входа;
- ✓ предоставлять права пользователям и группам.

Продолжительность занятия — около 10 минут.

Действие прав пользователя

Администраторы могут предоставлять определенные права пользователям и группам. Эти права разрешают пользователям выполнять определенные действия, например входить в систему, архивировать файлы и папки. *Права пользователя* (user rights) отличаются от разрешений тем, что распространяются на учетные записи пользователей, тогда как первые прикреплены к объектам. Кроме того, права пользователя являются частью ОГП, поэтому могут не приниматься во внимание в зависимости от влияния ОГП на пользователя.

Права пользователя определяют возможности на локальном уровне. Если всем пользователям одной группы нужны одинаковые права, можно упростить администрирование учетных записей, предоставив их всей группе, а не каждому пользователю в отдельности. В этом случае права пользователя распространятся на каждого члена группы.

Права пользователя, предоставленные группе, распространяются на всех ее пользователей. Если пользователь является членом нескольких групп, его права представляют собой совокупность прав каждой группы. Иногда при предоставлении определенных прав входа, права двух групп могут вступать в конфликт друг с другом. Однако в обшем случае, права пользователя, предоставленные одной группе, не противоречат правам другой группы. Чтобы лишить пользователя прав, предоставленных какой-либо группе, администратор просто удаляет этого пользователя из данной группы.

Существует два типа прав пользователя: привилегии и права на вход в систему.

Привилегии

Привилегии (privileges) определяют действия, доступные пользователю в сети. В табл. 13-13 перечислены привилегии, которые можно предоставить пользователю в Windows 2000.

Табл. 13-13. Привилегии

Привилегия	Описание
Act As Part Of The Operating System (Работа в режиме операционной системы)	Позволяет процессу пройти аутентификацию и получить доступ к ресурсам под именем любого пользователя. Эту привилегию следует назначать только службам, которым необходима аутентификация низкого уровня. Возможный уровень доступа не ограничен правами пользователя, поскольку вызывающий процесс может запросить, чтобы в маркер доступа были добавлены дополнительные привилегии. Больше беспокоит то, что запрашивающий процесс вправе создать анонимный маркер, обеспечивающий любой уровень доступа. Кроме того, сведения о таком маркере не попадут в журнал аудита. Процессы, требующие этой привилегии, должны использовать учетную запись LocalSystem, которая уже обладает этой привилегией
Add Workstations To Domain (Добавление рабочих станций к домену)	Позволяет пользователю добавить компьютер к домену. На этом компьютере пользователь должен создать объект в контейнере Computer в Active Directory для данного домена. Эта привилегия дублируется в Windows 2000 разрешениями контейнера Computer и ОП
Back Up Files And Directories (Архивирование файлов и каталогов)	Позволяет пользователю архивировать файлы и папки вне зависимости от разрешений доступа. Предоставление этой привилегии равносильно назначению разрешений Traverse Folder/Execute File (Обзор папок/Выполнение файлов), List Folder/Read Data (Содержание папки/Чтение данных), Read Attributes (Чтение атрибутов), Read Extended Attributes (Чтение дополнительных атрибутов) и Read Permissions (Чтение разрешений) на все файлы и папки локального компьютера. См. также привилегию Restore Files And Directories
Bypass Traverse Checking (Обход перекрестной проверки)	При навигации по объектам файловой системы или системного реестра пользователь может перемешаться по папкам, к которым при отсутствии этой привилегии доступ закрыт. Данная привилегия не позволяет пользователю просматривать содержимое папки, ему разрешено только перемешаться по ним
Change The System Time (Изменение системного времени)	Позволяет пользователю изменять системное время
Create A Pagefile (Создание страничного файла)	Позволяет пользователю корректировать размер файла подкачки для заданного диска из окна свойств системы
Create A Token Object (Создание маркерного объекта)	Позволяет процессу создавать маркер для доступа к любым локальным ресурсам средствами API-функций, например NtCreateToken(). Для процессов, которым необходима данная возможность, рекомендуется использовать учетную запись LocalSystem, которая уже обладает этой привилегией
Create Permanent Shared Objects (Создание постоянных объектов совместного использования)	Позволяет пользователю создать объект каталога в диспетчере объектов Windows 2000. Эта привилегия полезна для компонентов, которые работают в режиме ядра и собираются расширить пространство имен объектов Windows 2000. Такие компоненты по умолчанию обладают данной привилегией, поэтому предоставлять ее нет необходимости
Debug Programs (Отладка программ)	Позволяет пользователю применить отладчик к любому процессу, открывая доступ к наиболее важным компонентам системы

Табл. 13-13, Привилегии *(продолжение)*

Привилегия	Описание
Force Shutdown From A Remote System (Принудительное удаленное завершение)	Позволяет пользователю выключить компьютер из любой точки сети. См. также привилегию Shut Down The System
Generate Security Audits (Создание журналов безопасности)	Позволяет процессу вносить изменения в журнал безопасности и вести аудит различных ресурсов. Журнал безопасности применяется для регистрации попыток несанкционированного доступа. См. также привилегию Manage Auditing And Security Log
Enable Computer And User Accounts To Be Trusted For Delegation (Разрешение доверия к учетным записям при делегировании)	Позволяет пользователю задавать параметр Trusted For Delegation для объектов «компьютер» или «пользователь». Обладатель данной привилегии должен иметь права записи флагов управления доступом для этих объектов. Процесс-сервер, запущенный на доверенном компьютере или доверенным пользователем, может получить доступ к ресурсам другого компьютера. Этот компьютер применяет делегированные реквизиты клиента, пока в параметрах учетной записи клиента не задан флаг Account Cannot Be Delegated. Злоупотребление данной привилегией или параметром Trusted For Delegation может сделать сеть уязвимой для сложных атак с применением «троянских коней», позволяющих их создателям получить доступ к сетевым ресурсам
Increase Quotas (Увеличение квот)	Позволяет процессу с правом записи увеличить квоту процессора, назначенную другому процессу. Эта привилегия полезна при настройке системы, но применяется и при атаках типа *«отказ в обслуживании»* (denial-of-service, DoS)
Increase Scheduling Priority (Увеличение приоритета диспетчирования)	Позволяет процессу с правом записи увеличить приоритет выполнения другого процесса. Пользователь, обладающей этой привиле ией, имеет право изменить приоритет процесса с помощью пользовательского интерфейса Task Manager
Load and Unload Device Drivers (Загрузка и выгрузка драйверов устройств)	Позволяет пользователю устанавливать и удалять драйверы PnP-устройств. Данная привилегия не распространяется на драйверы устройств, не соответствующих спецификации Plug and Play. Такие устройства разрешено устанавливать только администраторам. Драйверы устройств относятся к доверенным (привилегированным) программам, поэтому пользователь, злоупотребляющий этой привилегией, может установить программы, которые будут в состоянии получить доступ к любым ресурсам
Modify Firmware Environment Values (Изменение параметров среды оборудования)	Позволяет пользователю и процессу менять переменные среды оборудования
Lock Pages In Memory (Закрепление страниц в памяти)	Позволяет процессу хранить данные в физической памяти, избавляя систему от необходимости использовать виртуальную память на диске. Данная привилегия ранее сильно увеличивала производительность системы, но сейчас она устарела и не применяется

Табл. 13-13. Привилегии *(окончание)*

Привилегия	Описание
Manage Auditing And Security Log (Управление аудитом и журналом безопасности)	Позволяет пользователю устанавливать аудит доступа к индивидуальным ресурсам, например файлам, объектам Active Directory и разделам реестра. Аудит доступа не начнется до тех пор, пока его не включат в групповую политику компьютера или групповую политику Active Directory. Данная привилегия не разрешает доступ к групповой политике компьютера. Пользователь, обладающий данной привилегией, вправе просматривать и очищать журнал безопасности с помощью консоли Event Viewer
Profile Single Process (Профилирование одного процесса)	Позволяет пользователю использовать средства мониторинга Windows NT и Windows 2000 для наблюдения за выполнением несистемных процессов
Profile System Performance (Профилирование загруженности системы)	Позволяет пользователю задействовать средства мониторинга Windows NT и Windows 2000 для наблюдения за выполнением системных процессов
Remove Computer From Docking Station (Извлечение компьютера из стыковочного узла)	Позволяет пользователю отключать компьютер от стыковочной станции через пользовательский интерфейс Windows 2000
Replace A Process Level Token (Замена маркера уровня процесса)	Позволяет процессу заменять маркер, по умолчанию связанный с начатым подпроцессом
Restore Files And Directories (Восстановление файлов и каталогов)	Позволяет пользователю разархивировать файлы и папки независимо от разрешений доступа и назначить любого участника безопасности владельцем объекта. См. также привилегию Back Up Files And Directories
Shut Down The System (Завершение работы системы)	Позволяет пользователю выключить локальный компьютер
Synchronize Directory Service Data (Синхронизация данных службы каталогов)	Позволяет процессу предоставлять службы синхронизации каталогов. Используется только для контроллеров домена. По умолчанию предоставляется учетным записям Administrator и LocalSystem контроллера домена
Take Ownership Of Files Or Other Objects (Овладение файлами или иными объектами)	Позволяет пользователю стать владельцем любого объекта системы, в том числе объектов Active Directory, файлов, папок, принтеров, разделов реестра, процессов и потоков

Некоторые из этих привилегий имеют более высокий приоритет, чем разрешения объекта. Например, пользователь домена может являться членом группы Backup Operators (Операторы архива), которая имеет право выполнения задач архивирования на всех серверах домена. Однако для этого требуется наличие разрешения на чтение всех файлов на этих серверах, в том числе и тех файлов, для которых владельцы установили разрешения, явно запрещающие доступ других пользователей, включая и членов группы Backup Opera-

tors. В данном случае право пользователя выполнять архивирование получает приоритет над всеми разрешениями для файлов и каталогов.

Права на вход в систему

Права на вход в систему (logon rights) определяют способы входа в систему. В табл. 13-14 перечислены права на вход, которые можно предоставить пользователю в Windows 2000.

Табл. 13-14. Права на вход в систему

Право входа	Описание
Access This Computer From The Network (Доступ к компьютеру из сети)	Позволяют подключиться к компьютеру по сети. По умолчанию предоставляется группам Administrators, Everyone и Power Users
Deny Access To This Computer From The Network (Отказ в доступе к компьютеру из сети)	Запрещает подключиться к компьютеру по сети. По умолчанию никому не запрещено
Deny Logon Locally (Отклонить локальный вход)	Запрещает входить в локальный компьютер. По умолчанию никому не запрещено
Deny Logon As A Batch Job (Отказ во входе в качестве пакетного задания)	Запрещает вход через путем выполнения очереди команд. По умолчанию никому не запрещено
Deny Logon As A Service (Отказать во входе в качестве службы)	Запрещает вход в качестве службы. По умолчанию никому не запрещено
Log On As A Batch Job (Вход в качестве пакетного задания)	Разрешает вход путем выполнения очереди команд. По умолчанию предоставляется группе Administrators
Log On As A Service (Вход в качестве службы)	Разрешает участнику безопасности регистрироваться в качестве службы. Данным правом всегда обладает учетная запись LocalSystem. Любой службе, запускаемой под отдельной учетной записью, надо предоставить это право. По умолчанию таким службам оно не предоставлено
Log On Locally (Локальный вход в систему)	Разрешает входить в локальный компьютер. По умолчанию предоставляется группам Administrators (Администраторы), Account Operators (Операторы учета), Backup Operators (Операторы архива), Print Operators (Операторы печати) и Server Operators (Операторы сервера)

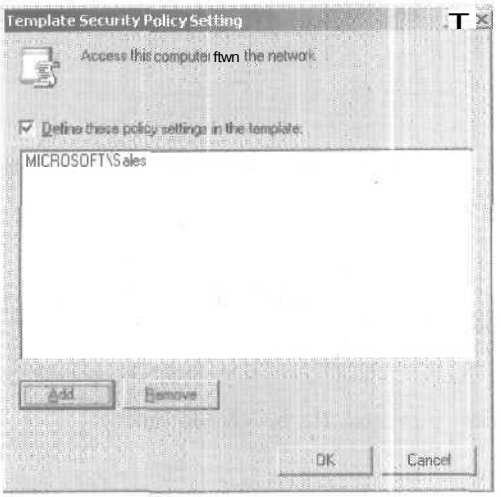
Специальная учетная запись LocalSystem наделена практически всеми привилегиями и правами на вход в систему, поскольку все процессы, работающие в режиме операционной системы, связываются с этой учетной записью, и для них необходим полный набор прав пользователей,

Предоставление прав пользователя

Чтобы упростить администрирование учетных записей, права пользователя лучше предоставлять группам, а не отдельным пользователям. В этом случае привилегии распространяются на каждого члена группы.

▶ **Предоставление прав пользователя**

1. Откройте оснастку Group Policy (Групповая политика).
2. В дереве консоли раскройте узел Computer Configuration\Windows Settings\Security Settings\Local Policies и щелкните User Rights Assignment (Назначение прав пользователя).
3. В правой панели щелкните правой кнопкой мыши нужное право пользователя и выберите команду Security (Безопасность).
4. В диалоговом окне Template Security Policy Setting (рис. 13-12) отметьте флажок Define These Policy Settings и щелкните кнопку Add.



Рис, 13-12. Диалоговое окно Template Security Policy Setting (Параметр шаблона политики безопасности)

5. В диалоговом окне Add User Or Group (Выбор: Пользователи или Группы) укажите пользователей и группы, на которых будет распространяться данное право пользователя, и щелкните OK.
6. Когда закончите добавление пользователей и групп, два раза щелкните OK.
7. Список пользователей и групп появится в правой панели в столбце Computer Setting.

Резюме

Права пользователя состоят из привилегий и прав на вход в систему. Привилегии определяют действия, доступные пользователю в сети. Права на вход задают способы входа пользователя в систему. Чтобы упростить администрирование учетных записей, права пользователя лучше предоставлять группам, а не отдельным пользователям. В этом случае привилегии распространяются на каждого члена группы. Для предоставления прав пользователя применяется оснастка Group Policy.

Занятие 5. Использование шаблонов безопасности

Сейчас мы познакомим вас с методами централизованной настройки параметров безопасности с помощью шаблонов безопасности.

Изучив материал этого занятия, вы сможете:

- ✓ объяснить назначение шаблонов безопасности;
- ✓ объяснить назначение стандартных шаблонов безопасности;
- ✓ управлять шаблонами безопасности.

Продолжительность занятия — около 25 минут.

Что такое шаблон безопасности

Под *шаблоном безопасности* (security template) понимается физическое представление конфигурации безопасности, то есть отдельный файл, в котором записаны параметры безопасности. Хранение всех параметров безопасности в одном месте упрощает администрирование. Каждый шаблон хранится в обычном текстовом файле с расширением .inf, что позволяет копировать, импортировать и экспортировать параметры. Шаблон безопасности содержит все параметры, кроме относящихся к политикам открытых ключей и политике IPSec.

Применение шаблонов безопасности

Шаблоны безопасности импортируются в локальные и нелокальные ОГП. В этом случае все компьютеры и учетные записи пользователей сайта, домена или ОП, на которые распространяется ОГП, применяют конфигурацию безопасности, описанную с помощью данного шаблона. Импорт шаблонов безопасности упрощает администрирование, так как конфигурация безопасности настраивается сразу для нескольких объектов.

Первоначальная конфигурация безопасности компьютера состоит из параметров локальных ОГП. Для ее сохранения, параметры безопасности можно экспортировать в шаблон. Это позволит при необходимости восстановить первоначальную конфигурацию безопасности.

Стандартные шаблоны безопасности

В Windows 2000 есть несколько стандартных шаблонов безопасности для разных ролей и уровней безопасности компьютера. Такие шаблоны можно задавать в готовом виде, изменять или использовать в качестве основы для создания собственных шаблонов безопасности. В промышленных системах стандартные шаблоны безопасности не следует применять без предварительного тестирования, которое позволяет достигнуть требуемого именно для вашей сети и системной архитектуры уровня защиты.

Ниже перечислены стандартные шаблоны безопасности Windows 2000:

- стандартные параметры безопасности контроллера домена (BASICDC.INF);
- стандартные параметры безопасности сервера (BASICSV.INF);
- стандартные параметры безопасности рабочей станции (BASICWK.INF);
- совместимые параметры безопасности рабочей станции или сервера (COMPATWS.INF);
- стандартные параметры безопасности, обновленные для контроллеров домена (DC SECURITY.INF);
- параметры усиленной безопасности контролера домена (HISECDC.INF);

- параметры усиленной безопасности рабочей станции или сервера (HISECWS.INF);
- стандартные параметры сервера, исключая Terminal Server User SID (NOTSSID.INF);
- Optional Component File Security для сервера (OCFILESS.INF);
- Optional Component File Security для рабочей станции (OCFILESW.INF);
- надежные параметры безопасности контролера домена (SECUREDC.INF);
- надежные параметры безопасности рабочей станции или сервера (SECUREWS.INF);
- используемые по умолчанию параметры безопасности (SETUP SECURITY.INF).

Все шаблоны хранятся в папке *systemroot*\Security\Templates.

Уровни безопасности

Стандартные шаблоны удовлетворяют наиболее распространенным требованиям безопасности.

- Обычный (**basic*.inf**). Шаблоны обычной безопасности предназначены для восстановления параметров безопасности приложения, если они были изменены. Такой шаблон применяет стандартные параметры безопасности Windows 2000 ко всем областям безопасности, исключая относящиеся к правам пользователей. Они не изменяются в шаблонах обычной безопасности, так как программы установки приложений обычно корректируют права пользователей, чтобы гарантировать правильную работу приложения. Как правило, шаблоны обычной безопасности применяют не для того, чтобы отменить эти коррективы.
- Совместимый (**compat*.inf**). Стандартные условия безопасности Windows 2000 ограничивают членов локальной группы Users (Пользователи) строгими параметрами безопасности, а членов локальной группы Power Users (Опытные пользователи) — параметрами безопасности, совместимыми с системой управления пользователями Windows NT 4.0. Эти стандартные параметры позволяют приложениям, сертифицированным для Windows 2000, работать в обычной среде Windows для пользователей, а приложениям, не сертифицированным для Windows 2000, — в менее защищенной среде, предназначенной для опытных пользователей. В некоторых организациях лучше по умолчанию назначить пользователей только членами группы Users и сузить привилегии безопасности для группы Users до уровня, на котором смогут нормально работать приложения, не сертифицированные для Windows 2000. Для таких организаций и предназначены совместимые шаблоны. Снижая уровни безопасности определенных файлов, папок и параметров реестра, используемых приложениями, совместимые шаблоны позволяют большинству приложений нормально работать в контексте группы Users. Кроме того, поскольку после применения совместимого шаблона пользователи не должны присоединяться к группе Power Users, все члены этой группы удаляются.
- Защита (**secure*.inf**). Шаблоны с защитой применяют рекомендуемые параметры защиты ко всем областям безопасности, кроме файлов, папок и параметров реестра. Эти объекты не изменяются, так как файловая система и реестр защищены изначально.
- Повышенная защита (**hisec*.inf**). Шаблоны с повышенной защитой задают параметры сетевой защиты Windows 2000. Обеспечивается максимальная защита сетевого трафика и используемых протоколов между компьютерами, работающими под управлением Windows 2000. В результате такие компьютеры настраиваются так, чтобы бы взаимодействовать только с другими компьютерами, работающими под управлением Windows 2000. Их взаимодействие с компьютерами, работающими под управлением Windows 9x или Windows NT, невозможно.

Управление шаблонами безопасности

Управление шаблонами безопасности подразумевает несколько операций.

1. Вызов консоли Security Templates.
2. Настройка предопределенных шаблонов безопасности,
3. Создание новых шаблонов безопасности.
4. Импорт шаблонов безопасности в локальные и нелокальные ОГП.
5. Экспорт параметров в шаблоны безопасности,

Доступ к консоли Security Templates

Консоль Security Templates (Шаблоны безопасности) является основным средством управления шаблонами безопасности.

▶ **Доступ к консоли Security Templates**

1. Решите, что вам нужно: добавить консоль Security Templates к существующей консоли или создать новую консоль.
   - чтобы создать новую консоль, в меню Start (Пуск) выберите команду Run (Выполнить), наберите **mmc** и щелкните OK.
   - чтобы добавить консоль Security Templates ксуществующей консоли, откройте ее и выполните пункт 2.
2. В меню Console (Консоль) выберите команду Add/Remove Snap-In (Добавить/удалить оснастку) и щелкните кнопку Add (Добавить).
3. В диалоговом окне Add Standalone Snap-In (Добавить изолированную оснастку) выберите Security Templates (Шаблоны безопасности), щелкните кнопку Add, затем — Close, затем — OK.
4. В меню Console выберите команду Save (Сохранить).
5. Введите имя новой консоли и щелкните кнопку Save.

   Ярлык новой консоли появится в меню Administrative Tools.

Настройка стандартных шаблонов безопасности

Под настройкой стандартных шаблонов безопасности понимается создание нового шаблона безопасности на основе стандартного. Для этого необходимо сохранить стандартный шаблон под другим именем (чтобы сохранить исходный шаблон), а затем изменить конфигурацию безопасности согласно вашим требованиям.

▶ **Настройка стандартных шаблонов безопасности**

1. В консоли Security Templates (рис. 13-13) дважды щелкните узел Security Templates.
2. Дважды щелкните стандартную папку *systemroot*\Security\Templates, щелкните нужный стандартный шаблон правой кнопкой и выберите команду Save As (Сохранить как).
3. В диалоговом окне Save As (Сохранить как) в поле File Name (Имя файла) введите новое имя шаблона и щелкните кнопку Save (Сохранить).
4. В дереве консоли щелкните правой кнопкой мыши новый шаблон безопасности и выберите команду Set Description (Задать описание).
5. В диалоговом окне Security Template Description (Описание шаблона безопасности) введите описание нового шаблона и щелкните OK.
6. В дереве консоли дважды щелкните новый шаблон, а затем — область безопасности, которую необходимо настроить, например Account Policies (Политики учетных записей).

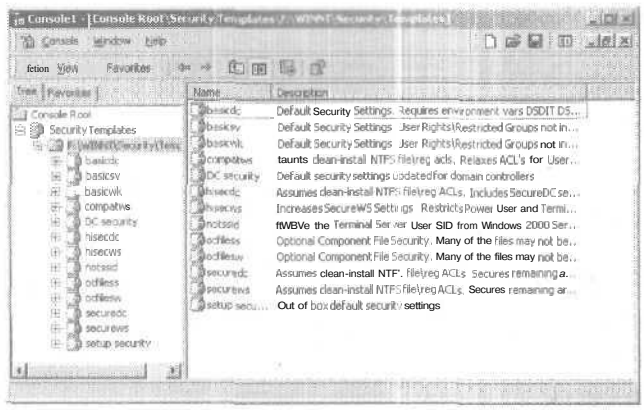


Рис. 13-13. Консоль Security Templates (Шаблоны безопасности)

7. Выберите политику безопасности, которую необходимо настроить, например Password Policy (Политика паролей), и дважды щелкните нужный параметр безопасности, например Minimum Password Length (Минимальная длина пароля).
8. В диалоговом окне Template Security Policy Setting (Параметр шаблона политики безопасности) отметьте флажок Define This Policy Setting In The Template (Определить следующий параметр политики в шаблоне) и измените параметр.
9. Щелкните OK.
10. При необходимости измените другие параметры безопасности.
11. Закройте консоль Security Templates.
12. В диалоговом окне Save Security Templates щелкните Yes, чтобы сохранить изменения.

Создание нового шаблона безопасности

Вы можете создать новый шаблон безопасности и изменить стандартные параметры согласно вашим требованиям.

▶ **Создание нового шаблона безопасности**

1. В консоли Security Templates дважды щелкните узел Security Templates.
2. Щелкните правой кнопкой мыши путь к папке шаблонов и выберите команду New Template (Создать шаблон).
3. Введите имя нового шаблона безопасности и щелкните OK.
4. В дереве консоли щелкните новый шаблон безопасности правой кнопкой мыши и выберите команду Set Description.
5. В диалоговом окне Security Template Description введите описание нового шаблона и щелкните OK.
6. В дереве консоли дважды щелкните новый шаблон, а затем — область безопасности, которую необходимо настроить, например Account Policies.
7. Выберите политику безопасности, например Password Policy и дважды щелкните нужный параметр безопасности, например Minimum Password Length.
8. В диалоговом окне Template Security Policy Setting отметьте флажок Define This Policy Setting In The Template и введите значение параметра.
9. Щелкните OK.
10. При необходимости измените другие параметры безопасности.
11. Закройте консоль Security Templates.
12. В открывшемся окне щелкните кнопку Yes, чтобы сохранить изменения.

Импорт шаблонов безопасности в ОГП

Шаблоны безопасности импортируются в локальные и нелокальные ОГП. Импорт шаблонов упрощает администрирование, так как конфигурация безопасности настраивается сразу для нескольких объектов.

▶ **Импорт шаблонов безопасности в локальные и нелокальные ОГП**

1. В консоли, предназначенной для управления локальными и нелокальными параметрами групповой политики, выберите нужный ОГП,
2. В дереве консоли щелкните узел Security Settings (Параметры безопасности) правой кнопкой мыши и выберите команду Import Policy (Импорт политики).
3. В диалоговом окне Import Policy From (рис. 13-14) выберите шаблон безопасности, который хотите импортировать, и щелкните кнопку Open (Открыть).

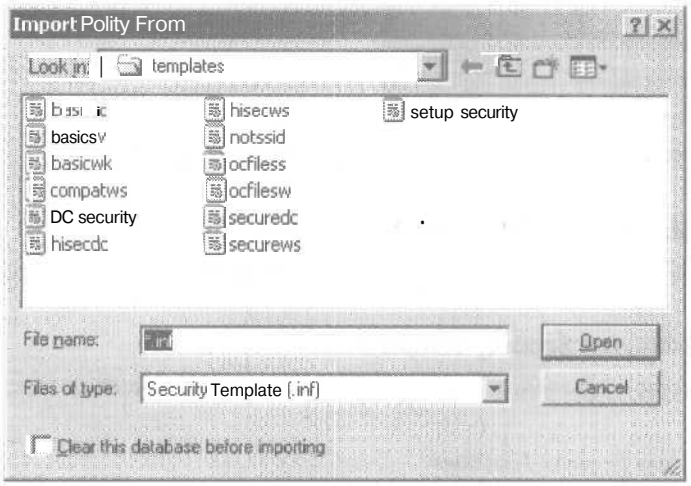


Рис. 13-14. Диалоговое окно Import Policy From (Импорт политики из)

4. Изменения вступят в силу только при следующем применении политики. Чтобы принудительно применить политику, выполните одно из следующих действий:
   - в командной строке наберите **secedit /refreshpolicy machine_policy** и нажмите Enter;
   - перезагрузите компьютер;
   - дождитесь автоматического применения политики. Период применения политики настраивается, по умолчанию он равен 8 часам.

Экспорт параметров в шаблон безопасности

В шаблон безопасности можно экспортировать локальные и действующие параметры безопасности. Экспорт локальных параметров позволяет сохранить первоначальную конфигурацию системы. ОГП домена имеют приоритет над локальными ОГП, поэтому при необходимости удастся восстановить локальные параметры безопасности. Экспорт действующих параметров в шаблон безопасности позволяет впоследствии импортировать их в базу данных безопасности (см. занятие 6), применять новые шаблоны и анализировать возможные противоречия.

▶ **Экспорт параметров в шаблон безопасности**

1. Раскройте меню Start\Programs\Administrative Tools и выберите команду Local Security Policy (Локальная политика безопасности).

2. В дереве консоли щелкните узел Security Settings (Параметры безопасности) правой кнопкой мыши, в контекстном меню выберите Export Policy (Экспорт политики), а затем — команду Local Policy (Локальная политика) или Effective Policy (Текущая политика).
3. В диалоговом окне Export Policy To (Экспорт политики в) выберите имя нужного шаблона безопасности и щелкните кнопку Save (рис. 13-15).

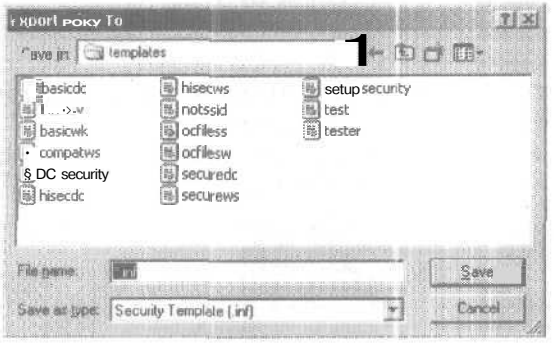


Рис. 13-15. Диалоговое окно Export Policy To (Экспорт политики в)

Практикум: управление шаблонами безопасности

Вызовите консоль Security Templates и настройте стандартный шаблон безопасности.

Упражнение 1: вызов консоли Security Templates

Вызовите основное средство управления шаблонами безопасности — консоль Security Templates.

► **Задание: вызовите консоль Security Templates**

1. В меню Start выберите команду Run, в командной строке наберите mmc и щелкните (Ж.
2. В меню Console выберите команду Add/Remove Snap-In и щелкните кнопку Add.
3. В диалоговом окне Add Standalone Snap-In выберите Security Templates, щелкните кнопку Add, затем — Close, затем — OK.
4. В меню Console выберите команду Save.
5. В качестве имени консоли наберите **Security Templates** и щелкните Save. Ярлык новой консоли появится в меню Administrative Tools.

Упражнение 2: настройка стандартного шаблона безопасности

Настройте стандартный шаблон безопасности. Для этого сохраните его под другим именем (чтобы сохранить исходный шаблон), а затем измените конфигурацию безопасности согласно вашим требованиям.

► **Задание: настройте стандартный шаблон безопасности**

1. В консоли Security Templates дважды щелкните узел Security Templates (Шаблоны безопасности).
2. Дважды щелкните стандартную папку *systemroot*\Security\Templates, щелкните шаблон basicdc правой кнопкой мыши и выберите команду Save As.
3. В диалоговом окне Save As в поле File Name наберите **new template** и щелкните кнопку Save.

4. В дереве консоли щелкните шаблон New Template правой кнопкой мыши и выберите команду Set Description.
5. В диалоговом окне Security Template Description введите описание **Новый шаблон безопасности контроллера домена** и щелкните OK.
6. В дереве консоли дважды щелкните шаблон New Template.
7. Дважды щелкните Account Policies, выберите политику Password Policy и дважды щелкните параметр Minimum Password Length.
8. В диалоговом окне Template Security Policy Setting отметьте флажок Define This Policy Setting In The Template и задайте минимальную длину пароля равной 10 символам.
9. Щелкните OK.
10. Закройте консоль Security Templates и сохраните изменения.
11. В открывшемся окне щелкните Yes, чтобы сохранить шаблон безопасности в файле NEW TEMPLATE.INF.

Резюме

Под шаблоном безопасности понимается физическое представление конфигурации безопасности, то есть отдельный файл, в котором хранятся параметры безопасности. Хранение всех параметров безопасности в одном месте упрощает администрирование.

К задачам управления шаблонами безопасности относится вызов консоли Security Templates, настройка стандартных шаблонов безопасности, создание новых шаблонов безопасности, импорт шаблонов безопасности в локальные и нелокальные ОГП, экспорт параметров в шаблоны безопасности.

Выполняя практическую часть занятия, вы научились вызывать основное средство управления шаблонами безопасности консоль Security Templates и настраивать стандартные шаблоны безопасности.

Занятие 6, Консоль Security Configuration and Analysis

Консоль Security Configuration and Analysis (Анализ и настройка безопасности) представляет собой основное средство настройки и анализа безопасности, просмотра результатов и исправления несоответствий, обнаруженных в процессе анализа. Мы расскажем, как использовать консоль Security Configuration and Analysis.

Изучив материал этого занятия, вы сможете:

- ✓ объяснить принцип работы консоли Security Configuration and Analysis;
- ✓ использовать консоль Security Configuration and Analysis для решения задач, связанных с конфигурацией и анализом безопасности.

Продолжительность занятия — около 25 минут.

Принципы работы консоли Security Configuration and Analysis

Для настройки и анализа безопасности консоль Security Configuration and Analysis использует специальную базу данных. Эта база данных представляет собой хранилище данных о компьютере. Ее архитектура позволяет использовать персональные базы данных, импортировать и экспортировать шаблоны безопасности, создавать составной шаблон на основе нескольких других и применять его для анализа и настройки безопасности системы. Добавляемые в базу данных шаблоны безопасности формируют составной шаблон либо заменяют имеющийся шаблон безопасности. Шаблоны безопасности каждого пользователя хранятся в персональной базе данных.

Конфигурация безопасности

Консоль Security Configuration and Analysis применяется для настройки безопасности локального компьютера. Консоль использует персональную базу данных, куда можно импортировать шаблоны безопасности, созданные с помощью консоли Security Templates (Шаблоны безопасности), и применить их к ОГП локального компьютера. В этом случае система немедленно будет настроена согласно конфигурации из шаблона.

Анализ безопасности

Операционная система и работающие в ней приложения находятся в динамичном взаимодействии. Например, для неотложного решения неполадок сети или вопросов администрирования уровень безопасности системы можно временно снизить. Если после этого систему не вернуть в прежнее состояние, ее защита не будет удовлетворять требованиям безопасности.

Консоль Security Configuration and Analysis позволяет администратору быстро проанализировать параметры безопасности. В результате анализа формируются рекомендации к текущим параметрам системы. Для обозначения несоответствий между текущими и предполагаемыми параметрами используются значки или примечания. Консоль Security Configuration and Analysis позволяет исправить любые несоответствия, выявленные в процессе анализа.

Регулярный анализ обеспечивает нужный уровень безопасности каждого компьютера, В результате анализа администратору предоставляется полная информация обо всех пара-

метрах системы, связанных с защитой, что позволяет обеспечить требуемый уровень безопасности и, что более важно, обнаружить любые ее нарушения.

Использование консоли Security Configuration and Analysis

Настройка и анализ безопасности состоит из нескольких операций.

1. Вызов консоли Security Configuration and Analysis.
2. Создание рабочей базы данных.
3. Импорт шаблонов безопасности в базу данных.
4. Анализ безопасности системы.
5. Просмотр результатов анализа.
6. Настройка безопасности системы.
7. Экспорт параметров из базы данных в шаблон безопасности.

Вызов консоли Security Configuration and Analysis

Консоль Security Configuration and Analysis является основным средством настройки и анализа безопасности.

▶ Вызов консоли Security Configuration and Analysis

1. Выберите один из вариантов:
   - чтобы создать новую консоль, в меню Start (Пуск) выберите команду Run (Выполнить), введите mmc и щелкните OK;
   - чтобы добавить консоль Security Configuration and Analysis к существующей консоли, сразу выполняйте пункт 2,
2. В меню Console выберите команду Add/Remove Snap-In и щелкните кнопку Add.
3. В диалоговом окне Add Standalone Snap-In выберите Security Configuration and Analysis (Анализ и настройка безопасности) и щелкните кнопку Add.
4. Щелкните кнопку Close, затем — OK.
5. В меню Console выберите команду Save.
6. Введите имя новой консоли и щелкните кнопку Save.

   Новая консоль появится в меню Administrative Tools.

Создание рабочей базы данных

Для настройки и анализа безопасности системы консоль Security Configuration and Analysis использует специальную базу данных. В первую очередь, для работы с консолью необходимо установить рабочую базу данных.

▶ **Выбор рабочей базы данных**

1. Откройте консоль Security Configuration and Analysis (рис. 13-16) и щелкните одноименный узел правой кнопкой мыши.
2. В контекстном меню выберите команду Open Database (Открыть базу данных).
3. В одноименном диалоговом окне укажите существующую персональную базу данных или введите имя для ее создания и щелкните кнопку Open (Открыть).

   В первом случае выбранная база данных становится рабочей; во втором случае откроется диалоговое окно Import Template (Импортировать шаблон).
4. Выберите шаблон безопасности и щелкните кнопку Open (Открыть), чтобы импортировать его базу данных.

   Рабочая база данных создана.

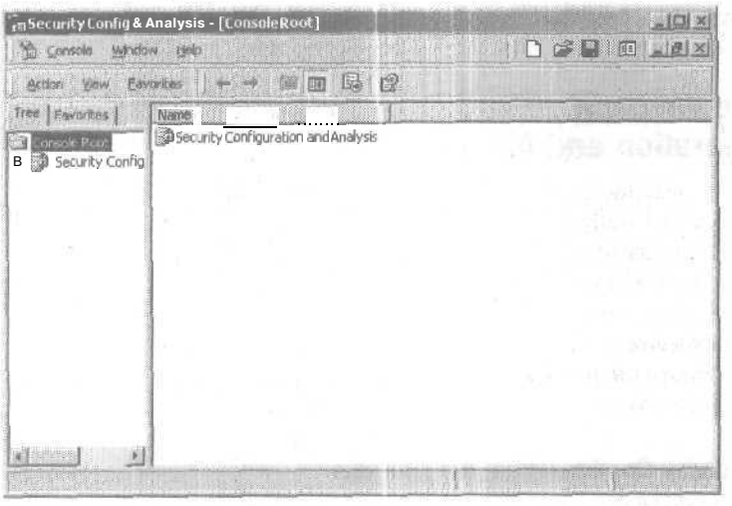


Рис. 13-16. Консоль Security Configuration and Analysis

Импорт шаблонов безопасности в базу данных

На занятии *5* вы узнали, как импортировать шаблон безопасности в ОГП. Здесь вы научитесь импортировать шаблоны в базу данных безопасности, с которой работает консоль Security Configuration and Analysis.

При импорте шаблонов в рабочую базу данных разрешается объединить их в один составной шаблон и затем использовать его для настройки и анализа безопасности системы. Противоречия, возникающие в процессе создания составного шаблона, решаются в процессе импорта, то есть шаблон, импортированный последним, имеет приоритет над другимишаблонами.

После импорта шаблона в базу данных можно выполнять настройку и анализ безопасности системы.

▶ **Импорт шаблонов в базу данных безопасности**

1. В консоли Security Configuration and Analysis щелкните одноименный узел правой кнопкой мыши.
2. Откройте или создайте рабочую базу данных.
3. Щелкните узел Security Configuration and Analysis правой кнопкой мыши и выберите команду Import Template (Импорт шаблона).
4. Выберите файл шаблона безопасности и щелкните кнопку Open.
5. Повторите предыдущие пункты для каждого шаблона, который нужно объединить с шаблонами, хранящимися в базе данных.

Примечание Если вы хотите не объединить, а заменить шаблон, хранящийся в базе данных, в диалоговом окне Import Template отметьте флажок Clear This Database Before Importing (Очистить эту базу данных перед импортом).

Анализ безопасности системы

В ходе анализа консоль Security Configuration and Analysis сравнивает текущее состояние безопасности системы с шаблоном безопасности, который импортирован в персональную базу данных. Этот шаблон называется конфигурацией базы данных и содержит рекомендуемые для данной системы значения параметров безопасности.

Консоль Security Configuration and Analysis запрашивает параметры каждой области безопасности системы. Собранные значения сравниваются с конфигурацией базы данных. Правильными считаются значения, совпадающие со значениями, хранящимися в базе данных. При несоответствии параметров политика считается потенциальным источником проблем и требует анализа.

► **Анализ безопасности системы**

1. В консоли Security Configuration and Analysis установите рабочую базу данных (если она еще не установлена).
2. Щелкните Security Configuration And Analysis правой кнопкой мыши и выберите команду Analyze Computer Now (Анализ компьютера).
3. В диалоговом окне Perform Analysis (Анализ) укажите путь к файлу журнала и щелкните OK.

   Во время анализа будут отображаться разные области безопасности. По его завершении вы можете просмотреть журнал.

Примечание Чтобы просмотреть журнал, щелкните узел Security Configuration And Analysis правой кнопкой мыши и выберите команду View Log File (Просмотр файла журнала).

Просмотр результатов анализа безопасности

Для каждой области безопасности консоль Security Configuration and Analysis оформляет результаты анализа в виде визуальных флагов, указывающих на наличие проблем. Консоль показывает текущую конфигурацию базы данных и компьютера для всех политик безопасности каждой области безопасности.

► **Просмотр результатов анализа**

1. В консоли Security Configuration and Analysis щелкните одноименный узел.
2. Дважды щелкните любую область безопасности, например Account Policies (Политики учетных записей), а затем щелкните политику безопасности, например Password Policy (Политика паролей).
3. В столбце Policy (Политика) в правой панели (рис. 13-17) перечислены политики, в столбце Database Setting (Параметр базы данных) — значения параметра безопасности из шаблона, а в столбце Computer Setting (Параметр компьютера) — текущий уровень безопасности системы.

   Красный значок с крестиком указывает на различие с конфигурацией базы данных; зеленая галочка — на соответствие с конфигурацией базы данных; отсутствие значка — на то, что политика безопасности не включена в шаблон и поэтому не анализировались.

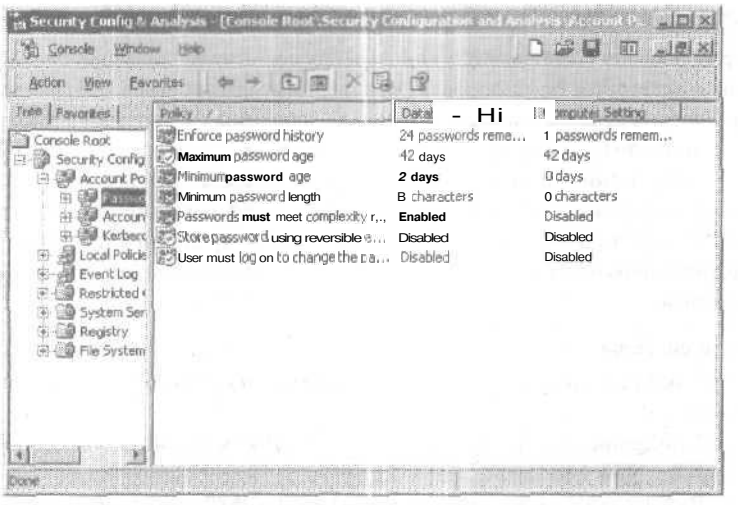


Рис. 13-17. Анализ результатов политики Password Policy (Политика паролей)

Настройка безопасности системы

Консоль Security Configuration and Analysis позволяет исправить несоответствия, выявленные в процессе анализа:

- принять или изменить любые значения параметров, которые не соответствуют уровню безопасности данной роли компьютера;
- применить конфигурацию базы данных, если текущие параметры системы не соответствуют требуемому уровню безопасности;
- импортировать в базу данных более подходящий для данной роли компьютера шаблон безопасности и применить его к системе,

Импортируя шаблоны в рабочую базу данных, можно объединить их в один составной шаблон и затем использовать его для настройки и анализа безопасности системы. Противоречия, возникающие в процессе создания составного шаблона, решаются в порядке импорта, то есть шаблон, импортированный последним, имеет приоритет над другими шаблонами. После импорта шаблона в базу данных воспользуйтесь командой Configure System Now (Настроить компьютер), чтобы применить конфигурацию базы данных к системе.

Внимание! Все коррективы касаются не исходного шаблона, а того, который хранится в базе данных безопасности. Исходный файл шаблона изменится, только если вы отредактируете его в консоли Security Templates (Шаблоны безопасности) или экспортируете в него конфигурацию базы данных.

Консоль Security Configuration and Analysis не рекомендуется применять для анализа безопасности клиентов домена, так как вам придется работать индивидуально с каждым клиентом. В этом случае стоит вернуться в консоль Security Templates, изменить шаблон, а затем заново применить его к соответствующему ОГП.

► **Настройка безопасности системы**

1. В консоли Security Configuration and Analysis установите рабочую базу данных (если она еще не установлена).

2. Щелкните узел Security Configuration And Analysis правой кнопкой мыши и выберите команду Configure Computer Now (Настроить компьютер).
3. В диалоговом окне Configure System (Настройка системы) введите новое имя журнала анализа или просто щелкните OK, чтобы использовать стандартный журнал.

   В ходе настройки будут отображаться различные области безопасности. По ее завершении вы можете просмотреть журнал или проанализировать безопасность системы.

▶ **Редактирование конфигурации базы данных**

1. В консоли Security Configuration and Analysis щелкните одноименный узел,
2. Дважды щелкните любую область безопасности, например Account Policies, затем щелкните политику безопасности, например Password Policy.
3. В правой панели дважды щелкните любой параметр безопасности.
4. Отметьте флажок Define This Policy In The Database (Определить следующую политику в базе данных), чтобы разрешить редактирование.
5. Введите новое значение параметра и щелкните OK.
6. Выполните эти действия для каждого параметра, который необходимо изменить.

▶ **Просмотр результатов настройки безопасности**

1. В консоли, предназначенной для управления групповой политикой, дважды щелкните ОГП.
2. В дереве консоли щелкните узел Security Settings.
3. Дважды щелкните любую область безопасности, например Account Policies, затем щелкните политику безопасности, например Password Policy.
4. Дважды щелкните любой параметр, например Minimum Password Length (Мин. длина пароля).

Экспорт шаблонов безопасности

Конфигурацию безопасности разрешается экспортировать из базы данных в шаблон безопасности. Новый шаблон безопасности, в свою очередь, можно импортировать в другие базы данных, использовать для анализа и настройки системы или даже переопределить средствами консоли Security Templates.

▶ **Экспорт параметров из базы данных в шаблон безопасности**

1. Если вы хотите сохранить в отдельном файле составной шаблон, который хранится в базе, в консоли Security Configuration and Analysis щелкните одноименный узел правой кнопкой мыши и выберите команду Export Template (Экспорт шаблона).
2. Откроется диалоговое окне Export Template To (Экспорт шаблона в). В поле File Name введите имя файла, в списке Save As Type тип файла и щелкните кнопку Save.

Практикум: использование консоли Security Configuration and Analysis

Вызовите консоль Security Configuration and Analysis, установите рабочую базу данных, выполните анализ безопасности системы и просмотрите его результаты.

Упражнение 1: вызов консоли Security Configuration and Analysis Console

Вызовите консоль Security Configuration and Analysis.

► **Задание: вызовите консоль Security Configuration and Analysis**

1. В меню Start выберите команду Run, в командной строке введите тшс и щелкните OK.
2. В меню Console выберите команду Add/Remove Snap-In и щелкните кнопку Add.
3. В диалоговом окне Add Standalone Snap-In выберите Security Configuration And Analysis и щелкните кнопку Add.
4. Щелкните Close, затем — OK.
5. В меню Console выберите команду Save.
6. В поле File Name введите имя консоли security **config** & **analysis** и щелкните кнопку Save.

   Новая консоль появится в меню Administrative Tools.

Упражнение 2: установка рабочей базы данных

Установите рабочую базу данных.

► **Задание: установите рабочую базу данных**

1. В консоли Security Configuration and Analysis щелкните одноименный узел правой кнопкой мыши.
2. В контекстном меню выберите команду Open Database (Открыть базу данных).
3. В одноименном диалоговом окне в поле File Name введите new и щелкните кнопку Open, чтобы создать новую персональную базу данных.
4. В диалоговом окне Import Template (Импортировать шаблон), выберите шаблон securedc и щелкните кнопку Open, чтобы импортировать шаблон в новую базу данных безопасности.

   База new стала рабочей базой данных. Новая рабочая база данных содержит шаблон securedc.

Упражнение 3: анализ безопасности системы

Выполните анализ безопасности системы и сравните параметры шаблона securedc с текущими параметрами безопасности системы.

► **Задание: проанализируйте безопасность системы**

1- Щелкните узел Security Configuration And Analysis правой кнопкой мыши и выберите команду Analyze Computer Now (Анализ компьютер).
2. В диалоговом окне Perform Analysis (Анализ) укажите путь к файлу журнала и щелкните OK.

   Появятся результаты анализа по каждой области безопасности.

Упражнение 4: просмотр результатов анализа безопасности

Просмотрите результаты анализа безопасности.

► **Задание; просмотрите результаты анализа безопасности**

1. В консоли Security Configuration and Analysis щелкните одноименный узел.
2. Дважды щелкните узел Account Policies и выберите политику Password Policy.

   Что показывают поля Policy, Database Setting и Computer Setting в правой панели?

   Что означают красный значок с крестиком и зеленая галочка в поле Policy?

Резюме

Для настройки и анализа безопасности системы консоль Security Configuration and Analysis обращается к специальной базе данных.

При настройке безопасности системы с помощью консоли Security Configuration and Analysis все изменения касаются не исходного шаблона, а того, который хранится в базе данных безопасности. Исходный файл шаблона изменится, только если вы отредактируете его в консоли Security Templates или экспортируете в него конфигурацию базы данных.

В процессе анализа безопасности консоль Security Configuration and Analysis сравнивает текущее состояние безопасности системы с шаблоном безопасности, который был импортирован в персональную базу данных. Этот шаблон называется конфигурацией базы данных и содержит рекомендуемые для данной системы значения параметры безопасности.

Выполняя практикум, вы научились вызывать консоль Security Configuration and Analysis, устанавливать рабочую базу данных, анализировать систему безопасности и просматривать результаты анализа.

Занятие 7. Решение проблем с конфигурацией безопасности

Здесь описаны проблемы, связанные с конфигурацией безопасности.

Изучив материал этого занятия, вы сможете:

- ✓ решить проблемы с конфигурацией безопасности.

Продолжительность занятия — около 5 минут.

Проблемы с конфигурацией безопасности

В табл. 13-15 перечислены ситуации, когда возможны проблемы, связанные с конфигурацией безопасности.

Табл. 13-15. Решение проблем с конфигурацией безопасности

Появление сообщения об ошибке: Event message: **Event ID 1202, Event source:** scecli, Warning **(0x%x) occurs to apply security policies (ошибка с кодом 1202)**

Причина	Решение
Групповая политика не обновляется после изменения	Обновите групповую политику с помощью программы Secedit, которая запускается из командной строки

Появление сообщения об ошибке: Failed to open the Group Policy Object (невозможно открыть ОГП)

Причина	Решение
В большинстве случаев связанно с конфигурацией сети	Проверьте конфигурацию DNS. Убедитесь, что в базе данных DNS нет устаревших записей. Исправьте записи локального DNS-сервера и DNS-сервера *поставщика услуг Интернета* (Internet service provider, ISP). Допустим, параметры локального сетевого адаптера указывают на два DNS-сервера: локальный DNS-сервер (возможно, тот же самый компьютер) и DNS-сервер ISP. При попытке сделать тестовый опрос вашего домена с помощью утилиты ping появится сообщение, что узел не найден. Даже если все записи в локальной базе данных корректны, DNS-сервер ISP не сможет определить ваш домен, так как их базы данных отличаются друг от друга. Чтобы решить эту проблему, добавьте *IP-адрес* DNS-сервера ISP в число перенаправлителей на локальном DNS-сервере

Изменение параметров безопасности не вступает в силу

Причина	Решение
Политика домена имеет приоритет над любой локальной политикой. То, что изменения локальных параметров не вступили в силу, может означать их игнорирование политикой домена	Иногда причина в том, что политика просто не успела обновиться. Обновите политику вручную. Для этого в командной строке наберите seccdit / **refreshpolicy machine_policy**

Табл. 13-15. Решение проблем с конфигурацией безопасности *(окончание)*

Политики не сохраняются при переходе с Windows NT 4.0 на Windows 2000

Причина	Решение
Политики Windows NT 4.0 нельзя перенести в *Windows* 2000. В Windows NT 4.0 системные политики хранились вместе с информацией о группах в одном файле с расширением .pol. Windows 2000 не поддерживает передачу этих данных в структуру Active Directory. Управление группами в Windows 2000 осуществляется совершенно по-другому	При обращении клиентов Windows NT 4.0 к компьютеру Windows 2000 Server и клиентов Windows 2000 Professional к компьютеру Windows NT 4.0 Server используется общий ресурс Netlogon (модель Windows NT 4.0). При обновлении клиента Windows NT 4.0 до Windows 2000 применяются только групповые политики Active Directory, старые политики Windows NT 4.0 не сохраняются. Хотя политики Windows NT 4.0 можно активизировать (с помощью параметров групповой политики), делать это не рекомендуется. Политики Windows NT 4.0 действуют только в процессе входа в систему. Это значит, что обрабатываются параметры и компьютера, и пользователя. Такое поведение нельзя назвать оптимальным по следующим причинам: параметры компьютера Windows NT 4.0 перекроют групповую политику, заданную в процессе загрузки. Во время обновления параметров групповой политики все противоречия сохранятся. Это создаст неопределенную ситуацию. Политики Windows NT 4.0 необратимо меняют параметры реестра.

Политики не сохраняются при переходе с Windows NT 4.0 на Windows 2000

Причина	Решение
	Помните также, что сервер терминалов не позволит задавать параметры компьютера в зависимости от вошедшего в систему пользователя

Резюме

Здесь вы познакомились с проблемами конфигурации безопасности и их решением.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении А «Вопросы и ответы» в конце книги.

1. Необходимо осуществить аудит доступа к папке, расположенной на рядовом сервере домена. На каком компьютере следует настроить политику аудита?

2. В чем разница между параметрами политики аудита, которые отслеживают доступ к службе каталогов и доступ к объектам?

3. Как при просмотре журнала безопасности определить успешность или неудачу события?

4. Чем права пользователя отличаются от разрешений?

5. Что такое шаблон безопасности и для чего он используется?

6. Где консоль Security Configuration and Analysis хранит информацию, необходимую для настройки конфигурации и анализа?

ГЛАВА 14

Управление производительностью Active Directory

В этой главе

Здесь рассказывается об управлении производительностью Active Directory посредством мониторинга и диагностики, а также при помощи контроля доступа к общим папкам.

Прежде всего

Для изучения материалов этой главы необходимо:

- настроить компьютер в соответствии с инструкциями вводной главы;
- изучить материалы о настройке консолей управления;
- настроить компьютер в качестве контроллера домена.

Занятие 1. Средства мониторинга производительности Active Directory

Мониторинг производительности Active Directory — важная функция поддержки и администрирования Microsoft Windows 2000. Данные о производительности Active Directory позволяют:

- оценить производительность Active Directory и ее влияние на ресурсы системы;
- наблюдать за изменениями и тенденциями производительности и использованием ресурсов и соответствующим образом планировать модернизацию парка компьютеров;
- тестировать изменения конфигурации или параметры настройки системы посредством мониторинга результатов;
- диагностировать проблемы, а также компоненты или процессы, требующие оптимизации.

На этом занятии рассматриваются средства мониторинга производительности Active Directory, а также обсуждаются этапы настройки мониторинга производительности службы каталогов Active Directory.

Изучив материал этого занятия, вы сможете:

- ✓ описать назначение консоли Event Viewer (Просмотр событий);
- ✓ просмотреть журналы событий с помощью консоли Event Viewer;
- ✓ описать компоненты консоли Performance (Производительность);
- ✓ описать назначение оснастки System Monitor (Системный монитор);
- ✓ выполнить мониторинг счетчиков производительности с помощью System Monitor;
- ✓ описать назначение оповещений, журналов счетчиков и трассировочных отчетов;
- ✓ создавать оповещения, журналы счетчиков и трассировочные отчеты с помощью оснастки Performance Logs and Alerts (Оповещения и журналы производительности).

Продолжительность занятия — около 50 минут.

В Windows 2000 имеется несколько средств мониторинга производительности Active Directory. Консоль Event Viewer (Просмотр событий), доступная в программной группе Administrative Tools (Администрирование), позволяет просматривать файлы журналов и сообщения об ошибках, передаваемые приложениями. Консоль Performance (Производительность) предназначена для просмотра сведений о производительности Active Directory в графическом виде в соответствии с выбранными вами счетчиками. Кроме того, данная консоль позволяет регистрировать активность системы или отсылать предупреждения, а также распечатывать журналы событий или просматривать их на экране компьютера.

Консоль Event Viewer

Предназначена для просмотра регистрируемых в журналах глобальных событий Windows, например событий приложений, системы и безопасности, а также событий, генерируемых отдельными службами, например событий службы каталогов. Так, чтобы получить подробную информацию о времени репликации разделов каталогов, можно из консоли Event Viewer просмотреть журнал File Replication Service (Служба репликации файлов).

Кроме того, при возникновении проблем в работе службы Active Directory для определения их источника *в первую очередь* рекомендуется просмотреть журналы службы каталогов. Информация журнала событий поможет вам глубже понять последовательность и типы событий, вызвавших конкретную проблему производительности.

В предыдущей главе вы научились использовать консоль Event Viewer для просмотра, поиска, фильтрования и архивирования информации журналов безопасности Windows 2000, а также для настройки этих журналов. Для журналов событий, применяемых при мониторинге производительности Active Directory, указанные задачи выполняются аналогичным образом. Журналы событий описаны в табл. 14-1.

Табл. 14-1. Журналы событий, используемые при мониторинге производительности Active Directory

Журнал	Описание
Application Log (Журнал приложений)	Содержит **ошибки, информацию** или предупреждения, генерируемые приложениями, **например, сервером БД** или программой **для работы** с электронной **почтой**
Directory Service	**Содержит ошибки, информацию и** предупреждения, **генерируемые** службой Active **Directory (рис.** 14-1)
File Replication Service **(Служба** репликации **файлов)**	**Содержит ошибки, информацию и предупреждения,** генерируемые службой **File Replication Service**
System **Log** (Журнал **системы)**	**Содержит ошибки, информацию и предупреждения,** генерируемые непосредственно Windows 2000. **Регистрируемые** события **определяются Windows** 2000

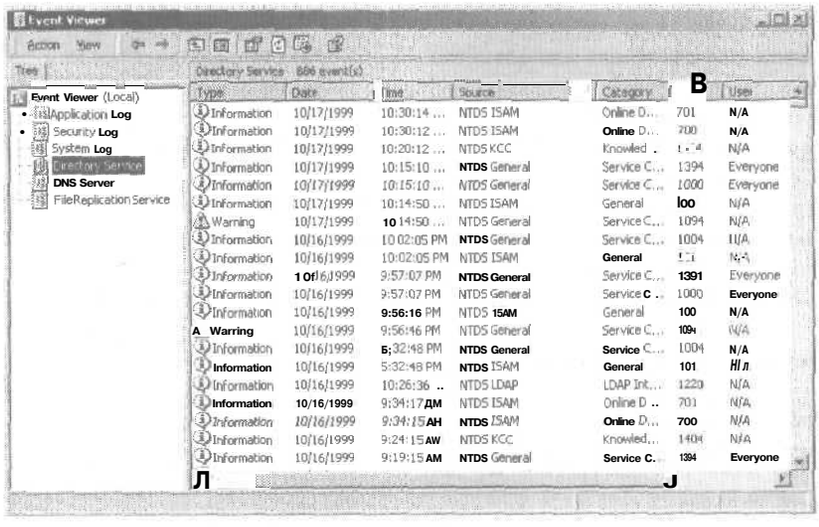


Рис. 14-1. Журнал Directory Service

Консоль Performance

Позволяет выполнять мониторинг состояния локальных и удаленных компьютеров сети, а также создавать отчет о производительности через заданный интервал времени. В консоли Performance имеются различные счетчики для мониторинга использования ресурсов в реальном времени. Консоль позволяет выводить результаты в файл, **благодаря** чему **вы можете просматривать и диагностировать проблемы производительности за нужный** пе-

риод. При наличии соответствующих разрешений можно отслеживать использование ресурсов других компьютеров сети, на которых запущены службы сервера, Кроме того, консоль Performance предназначена для сбора данных об эталонном уровне производительности и последующей отправке оповещений о несоответствии текущей производительности эталонному уровню службе Event Log (Журнал событий) или какому-либо другому объекту.

Консоль Performance включает оснастки System Monitor (ActiveX-элемент) и Performance Logs and Alerts.

Оснастка System Monitor

Позволяет оценивать производительность Active Directory на вашем и других компьютерах сети. Посредством System Monitor можно:

- собирать в реальном времени и просматривать данные о производительности локального и удаленных компьютеров;
- просматривать текущие или старые данные, хранящиеся в журнале счетчика;
- просматривать данные в виде графика, гистограммы или отчета;
- активизировать функции System Monitor в Microsoft Word и другие приложения пакета Microsoft Office при помощи Автоматизации (Automation);
- создавать HTML-страницы из представлений данных о производительности;
- создавать конфигурации для мониторинга, которые можно установить на другие компьютеры, использующие MMC.

Пример оснастки System Monitor приведен на рис. 14-2.

Для отбора отображаемых данных предназначены несколько параметров.

- Тип данных. Чтобы ограничить диапазон регистрируемых данных, укажите один или несколько экземпляров счетчиков или объектов мониторинга производительности.
- Источник данных. System Monitor позволяет собирать сведения о локальном компьютере или о других компьютерах в сети, к которым вы имеете доступ (по умолчанию требуются полномочия администратора). Кроме того, можно включить любые данные, собираемые в реальном времени, или данные, хранящиеся в журналах.
- Способ выборки. System Monitor поддерживает ручную выборку, автоматическую выборку с заданным интервалом и выборку до запросу. При просмотре журнала для отбора интересующих вас данных можно указать требуемый временной интервал.

Кроме того, System Monitor предоставляет возможности для настройки вида представлений.

- Тип отображения. System Monitor представляет данные в виде графика, гистограммы или отчета.
- **Параметры отображения.** Для любого из вышеперечисленных видов отображения вы можете определить параметры, цвета и шрифты.

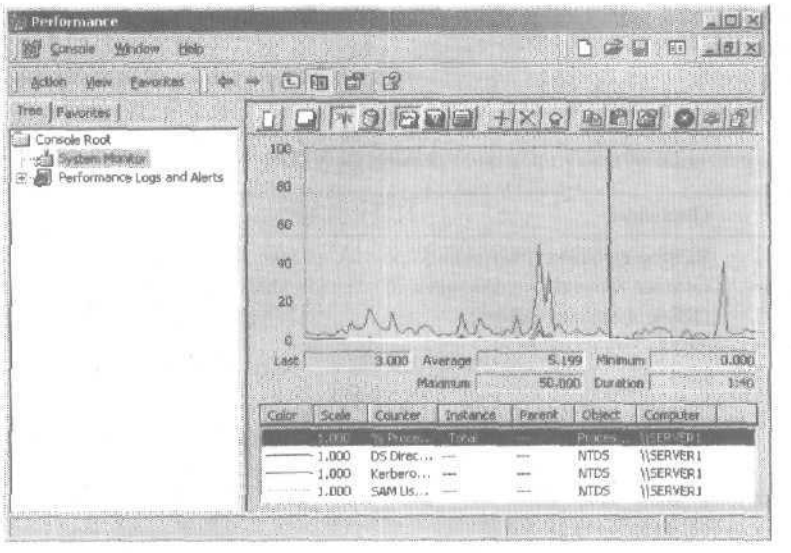


Рис. 14-2. Оснастка System Monitor

Отбор наблюдаемых данных

Для мониторинга данных вы указываете объекты и счетчики производительности. *Объект производительности* (performance object) — логическое объединение счетчиков, связанное с ресурсом или службой. Для мониторинга Active Directory следует контролировать активность объекта производительности NTDS (NT Directory Service). System Monitor фиксирует активность объектов производительности с помощью счетчиков. *Счетчики производительности* (performance counter) — условия, относящиеся к объектам производительности. Например, если вам нужно узнать текущее число клиентских сеансов по протоколу Lightweight Directory Access Protocol (LDAP), выберите в объекте производительности NTDS счетчик LDAP Client Sessions и просмотрите его текущую активность с помощью System Monitor.

Счетчики производительности объекта NTDS

Объект производительности NTDS включает множество счетчиков, предоставляющих статистические данные о производительности Active Directory. После отбора наблюдаемой статистической информации необходимо найти соответствующие счетчики производительности.

Счетчики производительности предоставляют базовую информацию для анализа, что позволяет планировать емкость и производительность. Обычно в имени счетчиков, используемых для планирования емкости, присутствует слово «total». Такие счетчики делятся на статистические, относительные и кумулятивные. *Статистические счетчики* (statistic counter) отображают общее число событий в секунду; например счетчик DRA (Directory Replication Agent) Inbound Properties Total/Sec отображает общее число свойств объектов полученных от партнеров по входящей репликации. *Относительные счетчики* (ratio counter) отображают отношение числа конкретных событий к суммарному числу событий в данной категории. Например, счетчик DS (Directory Service) % Writes From LDAP отображает процент операций записи в каталог, генерируемых LDAP-запросом. *Кумулятивные счетчики* (accumulative counter) показывают общее число событий с момента последнего запуска Active Directory. Например, счетчик DRA Inbound Bytes Total Since Boot отображает

общее число полученных в ходе репликации байт — сумму несжатых (никогда не сжимавшихся) и сжатых данных (в байтах).

Для каждого счетчика имеются правила использования и ограничения. Наиболее интересны счетчики, описанные в табл. 14-2.

Табл. 14-2. Основные счетчики объекта производительности NTDS

Счетчик	Описание
DRA Inbound Bytes Compressed (Between Sites, After Compression)/Sec [Входящих сжатых байт DRA (между сайтами, после сжатия)/сек]	Размер (в байтах) входящих сжатых данных репликации [размер сжатых данных, полученных от агентов Directory System Agent (DSA) в других сайтах]
DRA Inbound **Bytes** Compressed **(Between Sites, Before** Compression)/ Sec [Входящих сжатых **байт DRA** (между сайтами, до сжатия)/сек]	Исходный размер (в байтах) входящих сжатых данных репликации (размер до сжатия данных, полученных от агентов DSA в других сай гах)
DRA Inbound Bytes Not Compressed (Within Site)/ Sec [Входящих несжатых байт DRA (внутри сайта)/ сек]	Количество байт репликации, которые не были сжаты на источнике (например, от DSA в этом же сайте), в секунду.
DRA Inbound Bytes Total/Sec (Всего входящих байт DRA/сек)	Общее количество входящих байт репликации. Равно сумме несжатых (никогда не сжимавшихся) байт и сжатых байт (после сжатия)
DRA Inbound Full Sync Objects Remaining (Осталось объектов входящей полной синхронизации DRA)	Число объектов, которое необходимо обработать до завершения полного процесса синхронизации
DRA Inbound Objects/Sec (Входящих объектов DRA/сек)	Обшее количество объектов, получаемых в секунду от партнеров в процессе входящей репликации
DRA Inbound Objects Applied/Sec (Применено входящих объектов DRA/сек)	Частота, с которой получаемые от партнеров обновления репликации применяются локальной службой каталогов. Этот счетчик не включает изменения, которые получены, но не применены (например, когда такое изменение уже было сделано раньше). Показывает интенсивность обновлений репликации на сервере в результате изменений, сгенерированных на других серверах
DRA Inbound **Objects** Filtered/Sec **(Отфильтровано входящих объектов DRA/сек)**	Число объектов в секунду, получаемых от партнеров по входящей репликации, которые не содержат подлежащих применению обновлений

Табл. **14-2. Основные счетчики объекта производительности NTDS** *(продолжение)*

Счетчик	Описание
DRA Inbound Object Updates Remaining in Packet (Оставшихся в пакете входящих обновлений объектов DRA)	Количество обновлений объектов, полученных в текущем пакете обновления репликации каталога, которые еще не применены на локальном сервере. Значение счетчика позволяет оценить, сколько времени уходит у наблюдаемого сервера для регистрации принимаемых изменений в БД
DRA Inbound Properties Applied/Sec (Применено входящих свойств DRA/сек)	Количество свойств, обновленных посредством входящей репликации в результате того, что входящее свойство выигрывает при применении логики согласования
DRA Inbound Properties Filtered/Sec (Отфильтровано входящих свойств DRA/сек)	Количество изменений свойств, полученных во время репликации, которые уже поступали ранее
DRA Inbound Properties Total/Sec (Всего входящих свойств DRA/сек)	Общее количество свойств объектов, получаемых в секунду от партнеров по входящей репликации
DRA Inbound Values (DNs Only)/Sec [Входящих значений DRA (только DN)/сек]	Количество получаемых в секунду от партнеров по входящей репликации значений свойств объектов; эти значения представляют собой составное имя, например ссылки на другие объекты. Значения составных имен, например составы групп или списков распространения, требуют больше затрат на регистрацию по сравнению с другими типами значений. Это связано с тем, что объекты групп или списков распространения могут включать сотни и тысячи членов, и, как следствие, они гораздо больше простых объектов с одним или двумя атрибутами. Этот счетчик помогает выяснить причину долгой регистрации входящих изменений в БД
DRA Inbound Values Total/Sec (Всего входящих значений DRA/сек)	Общее количество значений свойств объектов, полученных в секунду от партнеров по входящей репликации. Каждый входящий объект обладает одним или несколькими свойствами, и каждое свойство может иметь от нуля до нескольких значений. Отсутствие значений указывает на удаление свойства
DRA Outbound Bytes Compressed (Between Sites, After Compression) /Sec [Исходящих сжатых байт DRA (между сайтами, после сжатия)/сек]	Сжатый размер (в байтах) исходящих сжатых байт репликации (размер после сжатия, от DSA в других сайтах)
DRA Outbound Bytes Compressed (Between Sites, Before Compression) /Sec [Исходящих сжатых байт DRA (между сайтами, до сжатия)/сек]	Исходный размер (в байтах) исходящих сжатых байт репликации (размер до сжатия, от DSA в других сайтах)

Табл. 14-2. Основные счетчики объекта производительности NTDS *(продолжение)*

Счетчик	Описание
DRA Outbound Bytes Not Compressed (Within Site) /Sec [Исходящих несжатых байт DRA (внутри сайта)/сек]	Количество исходящих байт репликации, которые не были сжаты (например, от DSA в этом же сайте)
DRA Outbound Bytes Total/Sec (Всего исходящих байт DRA/сек)	Общее количество исходящих байт репликации. Равно сумме количества несжатых байт (никогда не сжимаемых) и количества сжатых байт (после сжатия)
DRA Outbound Objects/ Sec (Исходящих объектов DRA/сек)	Количество реплицируемых объектов в секунду
DRA Outbound Objects Filtered/Sec (Отфильтровано исходящих объектов DRA/сек)	Количество объектов, просматриваемых при исходящей репликации и не содержащих обновлений, которых еще не было у партнера по исходящей репликации
DRA Outbound Properties/Sec (Исходящих свойств DRA/сек)	Количество реплицируемых свойств в секунду. Значение счетчика показывает, возвращает ли сервер-источник объекты или нет
DRA Outbound Values (DNs Only)/Sec [Исходящих значений DRA (только DN)/сек]	Количество значений свойств объектов, содержащих составные имена (DN) и отправленных партнерам по исходящей репликации. DN-значения, такие, как группа или список распространения, обычно требуют больших затрат на чтение, чем другие виды значений. Это связано с тем, что объекты групп или списков распространения могут включать сотни и тысячи членов, и, как следствие, они гораздо больше простых объектов с одним или двумя атрибутами
DRA Outbound Values Total/Sec (Всего исходящих значений DRA/сек)	Общее количество значений свойств объектов, отправляемых в секунду партнерам по исходящей репликации
DRA Pending Replication Synchronizations (Ожидающих синхронизации репликации DRA)	Количество необработанных синхронизации каталогов, находящихся в очереди данного сервера. Значение счетчика позволяет определить объем невыполненной репликации. Чем больше значение, тем больше данных осталось реплицировать
DRA Sync Requests Made (Запросов синхронизации DRA)	Количество запросов синхронизации, переданных партнерам по репликации
DS Directory Reads/Sec (Операций чтения в каталоге DS/сек)	Количество операций чтения в каталоге в секунду
DS Directory Writes/Sec (Операций записи в каталог DS/сек)	Количество операций записи в каталог в секунду
DS Security Descriptor Suboperations/Sec (Подопераций дескриптора безопасности DS/сек)	Частота выполнения подопераций распространения дескрипторов безопасности (Security Descriptor Propagation). Одна операция распространения состоит из нескольких подопераций. Подоперация примерно соответствует проверке одного объекта

Табл. 14-2. Основные счетчики объекта производительности NTDS *(окончание)*

Счетчик	Описание
DS Security Descriptor Propagations Events (Событий распространения дескриптора безопасности DS/сек)	Количество событий распространения дескриптора безопасности, которые поставлены в очередь, но еще не обработаны
DS Threads in Use (Используется потоков DS)	Текущее количество потоков, используемых службой каталогов (отличающееся от числа потоков процесса службы каталогов). Этот счетчик учитывает потоки, в данный момент обслуживающие вызовы клиентских API, и позволяет определить, будет ли выгодно использование дополнительных процессоров
Kerberos Authentications/Sec (Проверок подлинности Kerberos/сек)	Показывает, сколько раз в секунду клиенты используют билет на этот контроллер домена для проверки подлинности данного контроллера домена
LDAP Bind Time (Время привязки LDAP)	Время (в миллисекундах), потребовавшееся на выполнение последней успешной привязки LDAP
LDAP Client Sessions (Сеансов LDAP-клиентов)	Количество подключенных сеансов LDAP-клиентов
LDAP Searches/Sec (Поисков LDAP/сек)	Частота, с которой LDAP-клиенты выполняют операции поиска
LDAP Successful Binds/Sec (Успешных привязок LDAP/сек)	Количество успешных привязок LDAP в секунду
NTLM Authentications (Проверок подлинности NTLM)	Количество аутентификаций NT LAN Manager (NTLM) в секунду, выполняемых данным контроллером домена
XDS Client Sessions (Сеансов XDS-клиентов)	Количество подключенных клиентских сеансов расширенной службы каталогов. Указывает количество подключений от других служб Windows NT и программы Windows NT Administrator

Мониторинг счетчиков производительности

Вы можете отобрать наблюдаемые счетчики производительности и затем средствами System Monitor просмотреть их данные в виде графика, гистограммы или файла журнала.

► **Мониторинг счетчиков производительности Active Directory**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Performance (Системный монитор).
2. Щелкните в дереве консоли System Monitor (Системный монитор), а затем на правой панели щелкните кнопку со значком «+» — Add (Добавить).
3. В открывшемся диалоговом окне Add Counters (Добавить счетчики) (рис. 14-3к
   - для мониторинга локального компьютера, на котором запущена консоль, щелкните переключатель Use Local Computer Counters (Использовать локальные счетчики);
   - для мониторинга определенного компьютера, независимо от того, где запущена консоль, щелкните переключатель Select Counters From Computer (Выбрать счетчи-

ки с компьютера) и выберите из списка имя наблюдаемого компьютера (по умолчанию выбрано имя локального компьютера).

4. В списке Performance Object (Объект) щелкните объект производительности NTDS.

Примечание Для просмотра описания выберите счетчик в списке (рис. 14-3) и щелкните кнопку Explain (Объяснение).

5. Укажите требуемые счетчики.
   - для мониторинга всех счетчиков объекта производительности NTDS щелкните переключатель All Counters (Все счетчики);

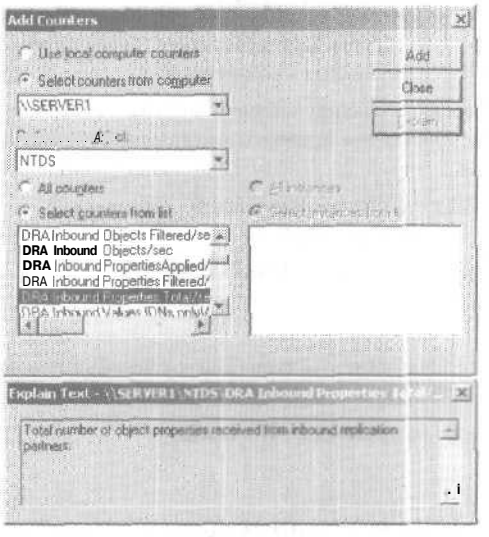


Рис. 14-3. Диалоговое окно Add Counters (Добавить счетчики)

Примечание Наблюдение за большим количеством счетчиков серьезно увеличит нагрузку на систему.

   - для мониторинга отдельных счетчиков щелкните переключатель Select Counters From List и выберите требуемые счетчики из списка. Чтобы указать несколько счетчиков, щелкая их названия, удерживайте нажатой клавишу Ctrl.
6. Щелкните кнопку Add (Добавить).
7. Закончив добавление счетчиков, щелкните кнопку Close (Закрыть).

Выбранные счетчики отображаются в нижней части экрана, причем каждый — собственным цветом. Укажите тип представления (график, гистограмма или отчет), щелкнув соответствующую кнопку на панели инструментов.

Примечание При создании оснастки System Monitor для экспорта убедитесь, что в диалоговом окне Select Counters (Выбор счетчиков) вы щелкнули переключатель Use Local Computer Counters (Использовать локальные счетчики). Иначе System Monitor будет получать данные от компьютера, указанного в текстовом поле, независимо от того, где установлена оснастка.

Оснастка Performance Logs and Alerts

Позволяет автоматически создавать оповещения, журналы счетчиков и трассировочные отчеты на локальных и удаленных компьютерах.

Журналы счетчиков

Как и System Monitor, журналы счетчиков позволяют выбирать объекты и счетчики производительности, а также задавать интервал выборки для мониторинга аппаратных ресурсов и системных служб. Сведения о производительности регистрируются в журналах счетчиков с разделением запятыми или символами табуляции, что упрощает импорт информации в программы для работы с электронными таблицами или БД. Для просмотра информации из журналов счетчиков можно воспользоваться System Monitor или экспортировать данные в файл для дальнейшего анализа и создания отчета.

Трассировочные отчеты

Используя системный поставщик данных по умолчанию или какой-либо другой поставщик, трассировочные отчеты фиксируют данные при выполнении системой определенных действий, например при операциях дискового ввода-вывода иди при ошибках памяти. При наступлении события поставщик отправляет данные службе Performance Logs And Alerts. Такая запись и пересылка данных отличается от работы счетчиков журналов, при которой служба получает данные от системы по истечении интервала обновления, а не при наступлении определенного события.

Active Directory включает *поставщики* данных для служб NetLogon, Kerberos, Security Accounts Manager (SAM) и Windows NT Active Directory Service. Эти компоненты доступа генерируют файлы трассировочных отчетов, включающие сообщения, предназначенные для контроля за выполнением операции.

При работе с выводом трассировочного журнала вам потребуется синтаксический анализатор. Для его создания программисты могут воспользоваться API-интерфейсами, доступными на Web-узле компании Microsoft по адресу http://msdn.microsoft.com/.

Параметры регистрации

Для журналов счетчиков и трассировочных отчетов можно:

- определить время начала и завершения регистрации, а также имена, типы и размеры файлов и прочие параметры автоматического создания журналов. Кроме того, вы можете управлять несколькими сеансами регистрации из одного окна консоли;
- запускать и останавливать регистрацию вручную или автоматически, по заданному пользователем расписанию;
- настраивать дополнительные параметры автоматического ведения журнала, в том числе автоматическое переименование файлов, а также задавать время запуска/останова журнала на основе прошедшего с начала его записи времени или размера его файла;
- выбрать программу, запускаемую после останова ведения журнала;
- просматривать журналы в процессе или после сбора данных. Поскольку процесс регистрации выполняется как служба, данные собираются независимо от того, какой пользователь работает в настоящий момент за наблюдаемым компьютером.

Требования к созданию журналов счетчиков и трассировочных отчетов

Для создания или изменения журнала вы должны обладать разрешением доступа Full Control к разделу реестра, управляющему службой Performance Logs and Alerts:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SysmonLog\Log Queries

Обычно администраторы обладают этим разрешением по умолчанию. Чтобы предоставить это разрешение доступа пользователю, в меню Security (Безопасность) утилиты Regedt32.exe выберите команду Permissions (Разрешения).

Для запуска службы Performance Logs and Alerts (которая при настойке журналов выполняется в фоновом режиме) вам необходимо обладать разрешением на запуск или настойку служб системы. Администраторы обладают таким разрешением по умолчанию и вправе предоставлять его пользователям посредством групповой политики. Для регистрации данных удаленного компьютера службу Performance Logs and Alerts должен запустить пользователь, который обладает доступом к удаленной системе.

Создание журнала счетчиков

Прежде чем создать журнал, определите, мониторинг каких счетчиков вы собираетесь выполнить, и задайте параметры файла журнала и расписания.

▶ **Создание журнала счетчиков**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Performance (Системный монитор).
2. Дважды щелкните узел Performance Logs And Alerts (Оповещения и журналы производительности), затем щелкните папку Counter Logs (Журналы счетчиков).

   В правой панели отобразятся несколько журналов. Зеленый значок указывает, что журнал в настоящий момент регистрирует данные; красный — что регистрация данных приостановлена.
3. Щелкните в пустом месте правой панели правой кнопкой и выберите команду New Log Settings (Новые параметры журнала).
4. В одноименном окне в поле Name (Имя) введите имя журнала и щелкните **OK.**
5. На вкладке General (Общие) окна свойств журнала счетчиков в поле Current Log File Name (Текущий файл журнала) отобразится полное имя файла журнала. Шелкните кнопку Add (Добавить).
6. В окне Select Counters (Выбор счетчиков) выберите компьютер, для которого собираетесь регистрировать показания счетчиков.
   - Для регистрации значений счетчиков компьютера, на котором будет запущена служба Performance Logs and Alerts (Оповещения и журналы производительности), щелкните переключатель Use Local Computer Counters (Использовать локальные счетчики).
   - Длярегистрации значений счетчиков конкретного компьютера, независимо от того, где будет выполняться служба Performance Logs and Alerts, щелкните переключатель Select Counters From Computer (Выбрать счетчики с компьютера) и выберите из списка имя наблюдаемого компьютера.
7. В списке Performance Object (Объект) выберите объект, значения счетчиков которого собираетесь регистрировать.
8. Укажите требуемые счетчики из списка и щелкните кнопку Add (Добавить).
9. Завершив отбор счетчиков, щелкните кнопку Close (Закрыть).
10. На вкладке Log Files (Файлы журналов) диалогового окна журнала счетчиков задайте параметры, руководствуясь данными рис. 14-4 и табл. 14-3.

Табл. 14-3. Параметры вкладки Log Files (Файлы журналов)

Параметр	Описание
Location (*Размещение*)	Имя папки, где будет создан файла журнала. Для выбора нужной папки можно также щелкнуть кнопку Browse (Обзор)
File Name (Имя файла)	Неполное или базовое имя файла журнала. При необходимости этот параметр можно использовать совместно с параметром End File Names With. Это имя отображается в правой панели оснастки Performance Logs and Alerts
End File Names With (Дописывать к имени)	Суффикс имени файла; выбирается из списка. Позволяет различать отдельные файлы журналов с одинаковыми именами в автоматически созданной группе журналов
Start Numbering At (Начать нумерацию с)	Начальное число, используемое для автоматической нумерации файлов, если в списке End File Names With выбран пункт nnnnnn
Log File Type (Тип журнала)	Формат файла журнала: *Text File — CSV* (Текстовый файл — CSV) — файл журнала с разделением запятыми (файлу присваивается расширение .csv). Этот формат используется для экспорта данных из журнала в программы обработки электронных таблиц; *Text File — TSV* (Текстовый файл — TSV) — файл журнала с разделением символами табуляции (файлу присваивается расширение tsv). Этот формат используется для экспорта данных из журнала в программы обработки электронных таблиц; *Binary File* (Двоичный файл) — последовательный двоичный файл с расширением .blg. Этот формат используется, если требуется обеспечить запись непоследовательных экземпляров данных; то есть останавливаемых и запускаемых после запуска журнала. Файлы журналов в недвоичном формате не могут включать непостоянные экземпляры; *Binary Circular File* (Двоичный циклический файл) — двоичный циклический файл. Данный формат файла позволяет использовать один журнал, перезаписывая новые данные поверх старых
Comment (Комментарий)	Комментарий или описание файла журнала. Отображается в правой панели оснастки Performance Logs and Alerts
Log File Size (Размер файла журнала)	*Maximum Limit* (Максимально возможный) — данные записываются в файл журнала до тех пор, пока он не достигнет размеров, заданных дисковой квотой или операционной системой; *Limit Of* (Не более) — максимальный размер файла журнала (указывается в килобайтах; не может превышать 2 Гб). Выберите этот параметр, если хотите использовать циклические файлы журнала

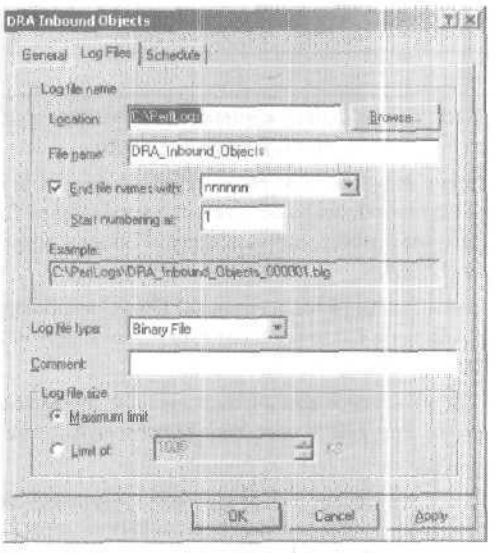


Рис. 14-4. Вкладка Log Files (Файлы журналов) окна свойств журнала счетчиков

11. На вкладке Schedule (Расписание) окна свойств журнала счетчиков задайте параметры, руководствуясь данными рис. 14-5 и табл. 14-4.

Табл. 14-4. Параметры вкладки Schedule (Расписание)

Параметр	Описание
Start Log (Запуск журнала)	*Manually* (Вручную) — регистрация данных запускается вручную; *At* (Время) — регистрация данных запускается в заданное вами время
Stop Log (Остановка журнала)	*Manually* (Вручную) — регистрация данных прекращается вручную; *After* (Через) — регистрация данных прекращается по прошествии заданного вами временного интервала; *At* Время) — регистрация данных прекращается в заданное вами время; *When The Log File Is Full* (Когда файл журнала заполнен) —регистрация данных прекращается по достижении максимального размера файла журнала
When A Log File Closes (Когда файл журнала будет закрыт)	*Start A New Log File* (Начать новый файл журнала) — после прекращения записи в текущий файл создается новый файл журнала, и регистрация данных продолжается; *Run This Command* (Выполнить команду) — при закрытии текущего файла журнала будет выполнена указанная вами команда

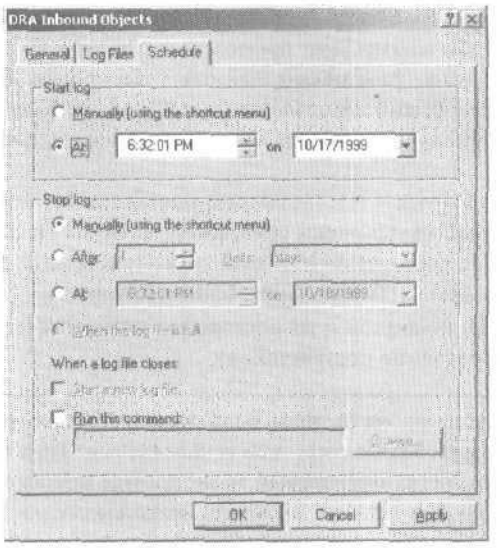


Рис. 14-5. Вкладка Schedule **(Расписание) диалогового окна журнала счетчиков**

12. Щелкните OK.

Примечание При создании оснастки Performance Logs and Alerts для экспорта убедитесь, что в диалоговом окне Select Counters вы щелкнули переключатель Use Local Computer Counters. Иначе System Monitor будет получать данные от компьютера, указанного в текстовом поле, независимо от того, где установлена оснастка.

Создание трассировочного отчета

Перед созданием трассировочного отчета определите, как будут регистрироваться события, и задайте параметры расписаниям и файлам журнала,

▶ **Создание трассировочного отчета**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Performance.
2. Дважды щелкните узел Performance Logs And Alerts, затем щелкните папку Trace Logs (Журналы трассировки).

   В правой панели отобразятся несколько журналов, Зеленый значок указывает, что журнал в настоящий момент регистрирует данные; красный — что регистрация данных приостановлена.
3. Щелкните в пустом месте правой панели правой кнопкой и выберите команду New Log Settings (Новые параметры журнала).
4. В одноименном окне в поле Name (Имя) введите имя журнала и щелкните OK.

   На вкладке General (Общие) окна свойств журнала трассировки в поле Current Log File Name (Текущий файл журнала) указан путь и имя файла журнала. По умолчанию файл журнала создается в папке PerfLogs корневого каталога. К введенному вами имени файла добавляется порядковый номер; тип файла определен как «sequental» (последовательный, расширение .etl).
5. Выберите события, которые требуется регистрировать.

- Щелкните переключатель Events Logged By System Provider (События, протоколируемые системным поставщиком), чтобы мониторинг процессов, потоков и др. выполнял поставщик данных по умолчанию (поставщик данных трассировки ядра Windows). Для отбора регистрируемых событий пометьте соответствующие флажки. Применение поставщика данных по умолчанию иногда несколько снижает производительность системы.
- Щелкните переключатель Nonsystem Providers (Несистемные поставщики), чтобы выбрать сторонние поставщики данных трассировки (например, если вы создали собственные поставщики данных). Для добавления или удаления несистемных поставщиков воспользуйтесь кнопками Add (Добавить) или Remove (Удалить).

Для просмотра списка установленных поставщиков и их состояния (активен/отключен) щелкните кнопку Provider Status (Состояние поставщиков).

Примечание Компьютер может одновременно вести лишь один журнал трассировки, использующий системный поставщик данных. Кроме того, нельзя параллельно запустить несколько журналов трассировки, использующих одинаковый несистемный поставщик. Если системный поставщик данных трассировки активен, включить несистемные поставщики нельзя, и наоборот. Тем не менее вы можете одновременно активировать несколько несистемных поставщиков данных.

---

6. На вкладке Log Files (Файлы журналов) окна свойств журнала трассировки задайте параметры. Это делается, как и для журналов счетчиков, за исключением параметров, перечисленных в табл. 14-5.

Табл. 14-5. Особые параметры вкладки Log Files для журналов трассировки

Параметр	Описание
Log File Type	Формат файла журнала: *Circular Trace File* (Файл циклической трассировки) — циклический файл журнала с расширением .etl. Данный формат файла позволяет использовать один журнал, так как старые данные перезаписываются новыми; *Sequential Trace File* (Файл последовательной трассировки) — последовательный файла журнала с расширением .etl. По достижении заданного пользователем максимального размера текущий файл журнала закрывается, и регистрация данных продолжается в новом файле
Log File Size	*Maximum Limit* (Максимально возможный) — данные записываются в файл журнала до тех пор, пока он не достигнет размеров, заданных дисковой квотой или операционной системой; *Limit Of* (Не более) — максимальный размер файла журнала (в мегабайтах). Выберите этот параметр, если хотите использовать циклические файлы журнала

7. На вкладке Schedule (Расписание) окна свойств журнала трассировки задайте параметры аналогично тому, как для журналов счетчиков.
8. Щелкните OK.

Примечание При трассировке подробных сведений о файлах или ошибок страниц регистрируются данные очень больших объемов. Рекомендуется ограничить время регистрации сведений о файлах и ошибках страниц двумя часами.

Оповещение

Как System Monitor и журналы счетчиков, оповещения позволяют выбирать объекты и счетчики производительности, а также задавать интервал выборки для мониторинга аппаратных ресурсов и системных служб. На основе полученных данных можно создать для счетчика оповещение, которое при превышении показаний счетчика порогового значения заносит соответствующую запись в журнал событий приложения, отсылает компьютеру сетевое сообщение, начинает регистрацию данных производительности или запускает приложение.

Сканирование оповещений запускают или останавливают как вручную, так и автоматически, по заданному пользователем расписанию.

Создание оповещения

Прежде чем создавать оповещение, определите счетчики, значения которых требуется отслеживать, и затем задайте параметры срабатывания оповещения и параметры расписания.

▶ **Создание оповещения**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Performance.
2. Дважды щелкните узел Performance Logs And Alerts, затем щелкните папку Alerts.
   В правой панели отобразятся настроенные оповещения. Зеленый значок указывает, что оповещение в настоящий момент активно; красный — что оповещение было отключено.
3. Щелкните в пустом месте правой панели правой кнопкой и выберите в контекстном меню команду New Alert Settings.
4. В поле Name (Имя) диалогового окна New Alert Settings (Новые параметры оповещений) введите имя оповещения и щелкните OK.
5. В поле Comment (Комментарий) диалогового окна свойств оповещения введите описание оповещения и щелкните кнопку Add (Добавить).
6. В диалоговом окне Select Counters (Выбор счетчиков) выберите компьютер, для которого создается оповещение.
   - Чтобы создать оповещение на компьютере, где будет запущена служба Performance Logs and Alerts, щелкните переключатель Use Local Computer Counters (Использовать локальные счетчики).
   - Чтобы создатьоповещение на определенном компьютере, независимо от того, где будет запущена служба Performance Logs and Alerts, щелкните переключатель Select Counters From Computer (Выбрать счетчики с компьютера) и выберите имя компьютера из списка.
7. В списке Performance Object (Объект) укажите объект мониторинга.
8. Выберите из списка требуемые счетчики и щелкните кнопку Add.
9. Закончив отбор счетчиков, щелкните кнопку Close.
10. В списке Alert When The Value Is (Оповещение, когда значение) выберите Under (Меньше) или Over (Больше), а в поле Limit (Порог) введите значение, при котором сработает оповещение.
11. В разделе Sample Data Every (Сжимать показания каждые) укажите значение и единицу измерения интервала обновления.
12. На вкладке Action (Действие) задайте параметры запуска оповещения, руководствуясь рис. 14-6 и табл. 14-6.

Табл. 14-6. Параметры вкладки Action (Действие)

Параметр	Описание
Log An Entry **In The** Application Event Log (Сделать запись в журнале событий **приложений)**	Создает запись, отображаемую в консоли Event Viewer (Просмотр событий)
Send A Network Message To (Послать сетевое сообщение)	Приказывает службе сообщений отослать сообщение определенному компьютеру
Start Performance Data Log (Запустить журнал производительности)	При срабатывании оповещения начинает указанный журнал счетчиков
Run This Program (Запустить программу)	Приказывает службе при срабатывании оповещения создать процесс и запустить указанную программу
Command Line Arguments (Аргументы командной строки)	Приказывает службе в случае использования параметра Run This Program скопировать заданные аргументы командной строки

13. На вкладке Schedule диалогового окна оповещения задайте параметры аналогично тому, как для журналов счетчиков.
14. Щелкните OK.

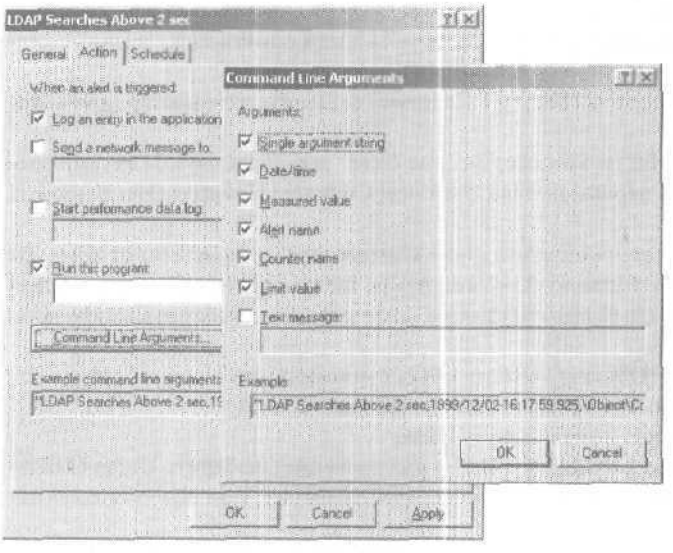


Рис. 14-6. **Вкладка Action (Действие)** окна **свойств оповещения и диалоговое окно Command Line Arguments (Аргументы командной строки)**

Практикум: использование System Monitor

Вы выполните мониторинг определенных счетчиков производительности с помощью System Monitor. Затем, посредством консоли Performance Logs and Alerts вы создадите журнал счетчиков и оповещение для счетчика LDAP Searches/Sec (Поисков LDAP/сек).

▶ Задание 1: пронаблюдайте счетчики производительности Active Directory

Вы отберете для просмотра некоторые счетчики производительности и затем с помощью System Monitor просмотрите их данные в виде графика, гистограммы или файла журнала.

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Performance (Системный монитор).
2. В дереве консоли щелкните System Monitor (Системный монитор).
3. Щелкните в правой панели правой кнопкой и выберите команду Add Counters (Добавить счетчики).
4. Щелкните переключатель Select Counters From Computer (Выбрать счетчики с компьютера) и убедитесь, что выбрано имя локального компьютера.
5. В списке Performance Object (Объект) укажите объект производительности NTDS.
6. Щелкните переключатель Select Counters From List (Выбрать счетчики из списка) и выберите из списка счетчик DRA Pending Replication Synchronizations (Ожидающих синхронизации репликации DRA). Затем щелкните кнопку Add (Добавить).
7. Выберите счетчик LDAP Searches/Sec (Поисков LDAP/сек) и щелкните кнопку Add.
8. Щелкните кнопку Close (Закрыть).

   Выбранные счетчики отобразятся в нижней части экрана; каждый из счетчиков представлен собственным цветом. Выберите тип представления (график, гистограмма или отчет), щелкнув соответствующую кнопку на панели инструментов.

▶ Задание 2: создайте журнал счетчиков

Вы создадите журнал счетчиков: сначала определите регистрируемые счетчики, а затем зададите параметры файла журнала и расписания.

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Performance.
2. Дважды щелкните узел Performance Logs And Alerts, затем щелкните папку Counter Logs (Журналы счетчиков).
3. Щелкните в пустом месте правой панели правой кнопкой и выберите команду New Log Settings.
4. В окне New Log Settings в поле Name введите LDAP Searches Per Sec и щелкните OK.
5. Удостоверьтесь, что на вкладке General (Общие) окна LDAP Searches Per Sec в поле Current Log File Name (Текущий файл журнала) указано имя файла журнала и путь по умолчанию. После этого щелкните кнопку Add.
6. В диалоговом окне Select Counters (выбор счетчиков) щелкните переключатель Select Counters From Computer (Выбрать счетчики с компьютера) и удостоверьтесь, что указано имя локального компьютера.
7. В списке Performance Object (Объект) выберите объект производительности NTDS.
8. Выберите счетчик LDAP Searches/Sec и щелкните кнопку Add. Затем — кнопку Close.
9. На вкладке Log Files (Файлы журналов) задайте следующие параметры:
   - Location (Размещение): C:\PerfLogs (здесь C:\ — имя системного диска);
   - File Name (Имя файла): LDAP_Searches_Per_Sec;
   - End File Names With (Дописывать к имени): nnnnnn;
   - Stan Numbering At (Начать нумерацию с): 1;

- Log File Type (Тип журнала): Text File—CSV;
- Log File Size (Размер файла журнала): Maximum Limit.

10. На вкладке Schedule (Расписание) задайте следующие параметры:
    - Start Log (Запуск журнала) At (Время): через 3 минуты, считая с настоящего момента;
    - Stop Log (Остановка журнала) After (Через): через 2 минуты.
11. Щелкните кнопку OK.
12. Когда по прошествии 3 минут начнется запись данных в журнал, откройте консоль Active Directory Users and Computers (Active Directory — пользователи и компьютеры), попробуйте открыть и закрыть различные ОП и объекты и затем закройте консоль.
13. Когда ведение журнала будет остановлено, вы сможете просмотреть его содержание, открыв файл \PERFLOGS\LDAP_SEARCHES_PER_ SEC_000001.CSV с помощью программы для работы с электронными таблицами, например Microsoft Excel.

▶ Задание 3: создайте оповещение

Вы создадите оповещение: сначала определите регистрируемые счетчики и затем зададите параметры срабатывания оповещения и параметры расписания.

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Performance.
2. Дважды щелкните узел Performance Logs And Alerts, затем щелкните папку Alerts (Оповещения).
3. Щелкните в пустом месте правой панели правой кнопкой и выберите команду New Alert Settings (Новые параметры оповещений).
4. В поле Name окна New Alert Settings введите **LDAP Searches Above 5 Sec** и щелкните OK.
5. В поле Comment окна свойств оповещения введите **Alerts when LDAP Searches are more than 5 per second** и щелкните кнопку Add.
6. В диалоговом окне Select Counters щелкните переключатель Select Counters From Computer и удостоверьтесь, что выбрано имя локального компьютера.
7. В списке Performance Object выберите объект NTDS.
8. Выберите из списка счетчик LDAP Searches/Sec и щелкните кнопку Add. После этого щелкните кнопку Close.
9. В списке Alert When The Value Is (Оповещать, когда значение) выберите Over (Больше), а в поле Limit (Порог) введите 5.
10. В области Sample Data Every (Сжимать данные каждые) задайте интервал обновления, равный, 3 секундам.
11. На вкладке Action (Действие) пометьте флажок Log An Entry In The Application Event Log (Сделать запись в журнале событий приложений).
12. На вкладке Schedule (Расписание) задайте следующие параметры:
    - Start Scan (Запуск наблюдения) At (Время): через 3 минуты, считая с настоящего момента;
    - Stop Scan (Остановка наблюдения) After (Через): через 2 минуты.
13. Щелкните OK.
14. Когда, по прошествии 3 минут, начнется запись данных в журнал, откройте консоль Active Directory Users and Computers, попробуйте открыть и закрыть различные ОП и объекты, а затем закройте консоль.
15. Когда ведение журнала будет прекращено, вы сможете просмотреть оповещения в журнале Application Log (Журнал приложений) с помощью консоли Event Viewer (Просмотр событий). Чтобы просмотреть информацию об оповещении, дважды щелкните соответствующую запись журнала.

Резюме

Мы рассказали о средствах наблюдения за производительностью Active Directory — консолях Event Viewer и Performance.

Консоль Event Viewer позволяет просматривать такие события, как ошибки приложений или успешный запуск службы. В случае возникновения проблем в работе службы Active Directory для определения их источника в первую очередь рекомендуется просмотреть журналы службы каталогов.

Консоль Performance позволяет выполнять мониторинг состояния локальных и удаленных компьютеров сети, а также создавать отчет о производительности через заданный интервал времени. Консоль Performance включает оснастки System Monitor (ActiveX-элемент) и Performance Logs and Alerts. Оснастка Performance Logs and Alerts позволяет автоматически создавать оповещения, журналы счетчиков и трассировочные отчеты на локальных и удаленных компьютерах.

Выполняя практическую часть занятия, вы научились проводить мониторинг отдельных счетчиков производительности с помощью оснастки System Monitor, а также создали средствами оснастки Performance Logs and Alerts журнал счетчиков и оповещение для счетчика LDAP Searches/Sec.

Занятие 2» Средства поддержки Active Directory

Некоторые из утилит пакета Windows 2000 Support Tools на компакт-диске Windows 2000, упрощают мониторинг, поддержку и устранение неполадок Active Directory. Здесь рассказывается об утилитах пакета Windows 2000 Support Tools, используемых для поддержки Active Directory-

Изучив материал этого занятия, вы сможете:

- ✓ установить Windows 2000 Support Tools;
- ✓ описать утилиты пакета Windows 2000 Support Tools, применяемые для поддержки Active Directory.

Продолжительность занятия - около 10 минут.

Пакет служебных программ Windows 2000 Support Tools, записанный на компакт-диск Windows 2000, упрощает диагностику и устранение неполадок компьютера.

Примечание Инструкции по установке пакета Windows 2000 Support Tools см. в главе 3.

Для поддержки Active Directory доступны следующие средства:

- LDP.EXE — утилита администрирования Active Directory;
- REPLMON.EXE — монитор репликации Active Directory;
- REPADMIN.EXE — утилита диагностикирепликации *;
- DSASTAT.EXE — утилита диагностики Active Directory *;
- SDCHECK.EXE — утилита проверки дескриптора безопасности *;
- NLTEST.EXE *;
- ACLDIAG.EXE — утилита диагностики списковACL *;
- DSACLS.EXE *.

* утилита командной строки.

Утилита LDP

Позволяет выполнять с LDAP-совместимым каталогом, например с Active Directory, различные LDAP-операции — подключение, привязку, поиск, изменение, добавление и удаление. LDAP — стандартный протокол связи Интернета, применяемый службой Active Directory. Утилита LDP — графическое средство поддержки, доступное из меню Windows 2000 Support Tools\Tools.

При устранении неполадок утилита LDP позволяет администраторам просматривать объекты каталога Active Directory вместе с их метаданными, например дескрипторами безопасности и метаданными репликации.

Утилита REPLMON

Позволяет администраторам просматривать состояние репликации Active Directory на низком уровне, принудительно синхронизировать контроллеры доменов, просматривать топологию в графическом виде, а также выполнять мониторинг состояния и производительности репликации контроллера домена с помощью графического интерфейса. Утилита REPLMON — графическое средство поддержки, доступное из меню Windows 2000 Support Tools\Tools.

Ниже перечислены ключевые возможности утилиты REPLMON.

- **Графическое отображение.** REPLMON показывает, является ли наблюдаемый сервер сервером глобального каталога, автоматически обнаруживает разделы наблюдаемого сервера, графически отображает их и показывает партнеры по входящей репликации для каждого раздела. В пользовательском интерфейсе Replication Monitor по-разному отображает прямые партнеры репликации, транзитивные партнеры репликации, серверы-плацдармы и серверы, удаленные из сети. Сбои, вызываемые определенным партнером, обозначаются изменениями представляющего его значка.
- **Журнал состояния репликации.** Для каждого раздела каталога и партнера репликации создается четкая хронология репликации между двумя контроллерами домена. Журнал можно просмотреть в пользовательском интерфейсе Replication Monitor, а также в автономном режиме или на удаленном компьютере при помощи текстового редактора.
- **Страницы свойств.** Набор страниц свойств для каждого из прямых партнеров репликации отображает имя контроллера домена, его GUID, раздел каталога, который он: реплицирует наблюдаемому серверу, используемый протокол (RPC или SMTP; при применении RPC различаются межсайтовая и внутрисайтовая репликации), время последнего успешного и предпринятого события репликации, значения USN-номеров и другие специальные свойства соединения двух серверов.
- **Создание отчетов о состоянии.** Администраторы могут создавать отчет о состоянии наблюдаемого сервера, включающий перечень разделов каталогов сервера, сведения о состоянии всех партнеров репликации (прямых и транзитивных) для каждого раздела каталога, перечень контроллеров домена, извещаемых наблюдаемым сервером в случае записи изменений, сведения о состоянии всех объектов групповой политики (ОГП), перечень контроллеров доменов выполняющих роли *одиночных хозяев операций* (Flexible Single Master Operations, FSMO), снимок счетчиков производительности компьютера и конфигурацию реестра сервера [в том числе параметры для Knowledge Consistency Checker (KCC), Active Directory, БД Jet и LDAP]. Кроме того, администратор может включить в отчет сведения о конфигурации сети предприятия — сайте, связи сайтов, мосте связи сайтов, подсети, контроллере домена (независимо от домена) и свойствах каждого из упомянутых типов объектов. Например, для контроллера домена в отчете появятся сведения о GUID, составляющем используемую при репликации запись DNS, о размещении учетной записи компьютера в Active Directory, межсайтовом почтовом адресе, имени узла данного компьютера и всех специальных флагах сервера (независимо от того, является ли он сервером глобального каталога или нет). Такая информация очень полезна при устранении неполадок репликации Active Directory.
- **Мастер Server Wizard.** Позволяет администратору выбрать наблюдаемый сервер или явно зарегистрироваться на нем. Администратор может также создать файл .ini,, предопределяющий имена наблюдаемых серверов. Затем этот файл загружается утилитой REPLMON для заполнения пользовательского интерфейса.
- **Графическая топология сайтов.** REPLMON отображает внутрисайтовую топологию в графическом представлении и позволяет администраторам с помощью контекстного меню контроллера домена быстро выделять свойства, а также все межсайтовые и внутрисайтовые подключения сервера.
- **Отображение свойств.** Администратор может просматривать свойства наблюдаемого сервера, в том числе имя сервера, DNS-имя узла компьютера, расположение учетной записи компьютера в Active Directory, состояние основного сервера-плацдарма, все специальные флаги сервера (например, является ли он эмулятором основного контроллера для своего домена или нет), какие компьютеры с его точки зрения выполняют роли FSMO, подключения репликации (Replication Monitor различает объекты подключения, сгенерированные автоматически и созданные администратором), причины, по

которым эти подключения созданы, а также конфигурацию протокола IP для наблюдаемого сервера.

- **Статистика и опрос состояния репликации.** В режиме Automatic Update утилита REPLMON опрашивает сервер с интервалом, заданным администратором, для получения текущей статистики и состояния репликации. Данная функция генерирует журнал изменений для каждого наблюдаемого сервера и его партнеров репликации и позволяет администратору наблюдать изменения топологии на этом сервере. В данном режиме REPLMON ведет мониторинг числа неудачных попыток репликации для каждого из партнеров репликации. Если полученное число равняется или превышает заданное администратором значение, REPLMON заносит соответствующую запись в журнал событий и отсылает администратору уведомление по электронной почте.
- **Инициирование репликации.** Администраторы могут активировать на сервере репликацию с определенным партнером репликации, со всеми другими контроллерами доменов сайта или со всеми другими контроллерами доменов вне и внутри сайта.
- **Активация KCC.** Администраторы могут активировать KCC на наблюдаемом сервере, чтобы перестроить топологию репликации.
- **Отображение нереплицированных изменений.** При необходимости администраторы могут просматривать изменения Active Directory, еще не реплицированные с партнера репликации.

Утилита REPADMIN

Утилита командной строки, упрощающая диагностику неполадок репликации между контроллерами домена Windows 2000.

В ходе нормальной работы KCC автоматически управляет топологией репликации для каждого контекста именования, содержащегося на контроллерах доменов.

REPADMIN позволяет администратору просматривать топологию репликации с точки зрения каждого контроллера домена. Кроме того, утилита REPADMIN позволяет вручную создать топологию репликации (обычно это не требуется), принудительно генерировать события репликации между контроллерами домена, а также просматривать метаданные репликации и векторы актуальности.

Примечание Обычно создавать топологию репликации вручную не требуется. Некорректное использование REPADMIN может оказать на топологию репликации негативное влияние. Данная утилита применяется в основном для мониторинга репликации и выявления разного рода проблем — наличия отключившихся от сети серверов или недоступных ЛВС/ГВС-подключений.

Утилита DSASTAT

Утилита командной строки, предназначенная для сравнения и выявления различий между контекстами именования на контроллерах доменов.

Утилита DSASTAT позволяет сравнивать два дерева каталогов между репликами одного или, для глобального каталога, разных доменов. DSASTAT получает статистические сведения о емкости (Мб/сервер, количество объектов на сервере, Мб/класс объектов и т. д.) и сравнивает атрибуты реплицированных объектов.

Конечные контроллеры доменов и дополнительные параметры работы указываются в командной строке или в файле инициализации. DSASTAT определяет, имеется ли у контроллеров согласованный и точный образ их домена. В случае с глобальным каталогом

DSASTAT проверяет, есть ли у него согласованный с контроллерами образ домена. Утилита DSASTAT дополняет утилиты мониторинга репликации REPADMIN.EXE и REPLMON.EXE и гарантирует, что на каждом из контроллеров содержится обновленная информация о других контроллерах домена.

Утилита SDCHECK

Утилита командной строки SDCHECK отображает дескрипторы безопасности всех объектов, хранящихся в каталоге Active Directory. Дескриптор безопасности содержит списки ACL, которые определяют права пользователей в отношении объектов из хранилища в Active Directory.

Чтобы администратор мог определить действующие разрешения доступа к объекту, SDCHECK также отображает иерархию объектов и все наследуемые объектом списки ACL.

Все изменения в списках ACL объекта или родительского объекта автоматически распространяются службой Active Directory. Утилита SDCHECK отображает метаданные распространения дескрипторов безопасности, что позволяет администраторам отслеживать эти изменения с учетом распространения наследуемых списков ACL, а также репликации списков ACL с других контроллеров доменов. Утилита SDCHECK дополняет утилиты мониторинга репликации REPADMIN.EXE и REPLMON.EXE и гарантирует, что на каждом из контроллеров содержится обновленная информация о других контроллерах домена.

Утилита NLTEST

Утилита командной строки NLTEST упрощает выполнение таких задач администрирования сети, как:

- проверка доверительных отношений и состояния репликации контроллера домена в домене Windows;
- опрос и проверка состояния доверия;
- принудительное выключение;
- получение списка основных контроллеров домена;
- принудительная синхронизация БД учетных записей пользователей с контроллерами доменов Microsoft Windows NT 4.0 или более ранних версий (для поддержки учетных записей пользователей контроллеры доменов Windows 2000 применяют совершенно иной механизм).

NLTEST.EXE работает только на компьютерах семейства x86 (Intel).

Утилита ACLDIAG

Утилита командной строки ACLDIAG упрощает диагностику и устранение проблем с разрешениями на объекты Active Directory. ACLDIAG считывает атрибуты из списков ACL и выводит информацию в удобочитаемом виде или в файл, разделенный символами табуляции. Этот файл можно открыть в текстовом редакторе для поиска конкретных разрешений, пользователей или групп либо в программе для работы с электронными таблицами или БД для составления отчетов. Кроме того, утилита ACLDIAG предоставляет некоторые простые функции очистки.

Средства ACLDIAG позволяют:

- сравнивать список ACL объекта служб каталогов с разрешениями, определенными в схеме по умолчанию;
- проверять или исправлять стандартные делегирования, выполненные с использованием шаблонов мастера Delegation of Control (Мастер делегирования управления) консоли Active Directory Users and Computers;

- просматривать действующие права, предоставленные определенному пользователю, группе или всем пользователям и группам из списка ACL.

ACLD1AG отображает разрешения только тех объектов, правами на просмотр которых обладает пользователь. Поскольку ОГП — виртуальный объект и не имеет составного имени, утилита ACLDIAG не может работать с ним.

Для создания отчетов общего плана, а также для изменения параметров ACL из командной строки можно воспользоваться утилитой DSACLS.

Утилита DSACLS

Утилита командной строки DSACLS упрощает управление списками ACL для служб каталогов. DSACLS позволяет запрашивать атрибуты безопасности объектов Active Directory и управлять ими, и представляет собой эквивалент вкладки Security (Безопасность) разных оснасток Active Directory, работающий из командной строки.

Средствами утилит ACLDIAG и DSACLS можно конфигурировать и диагностировать безопасность объектов Active Directory из командной строки.

Резюме

На этом занятии вы познакомились с утилитами пакета Windows 2000 Support Tools, используемыми для поддержки Active Directory.

Занятие 3. Мониторинг доступа к общим папкам

В Microsoft Windows 2000 имеется оснастка Shared Folders (Общие папки), упрощающая контроль доступа к сетевым ресурсам и отправку административных сообщений пользователям. Мониторинг доступа к сетевым ресурсам позволяет оценить и управлять текущим использованием серверов сети.

Изучив материал этого занятия, вы сможете:

- ✓ описать средство Windows 2000 лля контроля доступа к сетевым ресурсам и рассылки административных сообщений пользователям;
- ✓ рассказать, кто имеет право выполнять мониторинг доступа к сетевым ресурсам;
- ✓ создать общие папки на компьютере;
- ✓ выполнять мониторинг общих папок;
- ✓ выполнять мониторинг открытых файлов;
- ✓ отключать пользователей от одного или всех открытых файлов.

Продолжительность занятия — около 20 минут.

Назначение мониторинга сетевых ресурсов

Вот некоторые причины необходимости наблюдения за сетевыми ресурсами.

- **Обслуживание.** Прежде чем сделать ресурс временно или постоянно недоступным, вы можете определить, какие пользователи в настоящий момент работают с ним, и оповестить их.
- **Безопасность.** Мониторинг доступа к конфиденциальным или нуждающимся в защите ресурсам позволяет гарантировать, что к ним смогут обратиться лишь полномочные лица.
- **Планирование.** Вы можете определить, с какими ресурсами и насколько интенсивно работают пользователи. Это позволит вам спланировать будущие потребности системы.

В Microsoft Windows 2000 имеется оснастка Shared Folders, упрощающая контроль доступа к сетевым ресурсам и отправку административных сообщений пользователям. Она доступна в консоли Computer Management (Управление компьютером) и позволяет выполнять мониторинг ресурсов локального компьютера. Добавляя оснастку Shared Folders в консоль MMC, вы можете указать, мониторинг ресурсов какого компьютера требуется — локального или удаленного.

Требования к мониторингу сетевых ресурсов

Не все пользователи имеют право контролировать доступ к сетевым ресурсам. В табл. 14-7 перечислены группы, полномочные наблюдать за сетевыми ресурсами.

Табл. 14-7. Группы, обладающие правами мониторинга сетевых ресурсов

Члены группы	Имеет право на мониторинг
Administrators (Администраторы) или Server Operators (Операторы сервера) домена	Всех компьютеров домена
Administrators или Power Users (Опытные пользователи) рядового сервера, изолированного сервера или компьютера Microsoft Windows 2000 Workstation	Локального компьютера

Мониторинг доступа к общим папкам

Для просмотра списка общих папок компьютера и определения числа подключенных к ним пользователей применяется папка Shares (Ресурсы) оснастки Shared Folders (Общие папки). На рис. 14-7 папка Shares выделена в дереве консоли Computer Management, и в правой панели отображаются все общие папки данного компьютера.

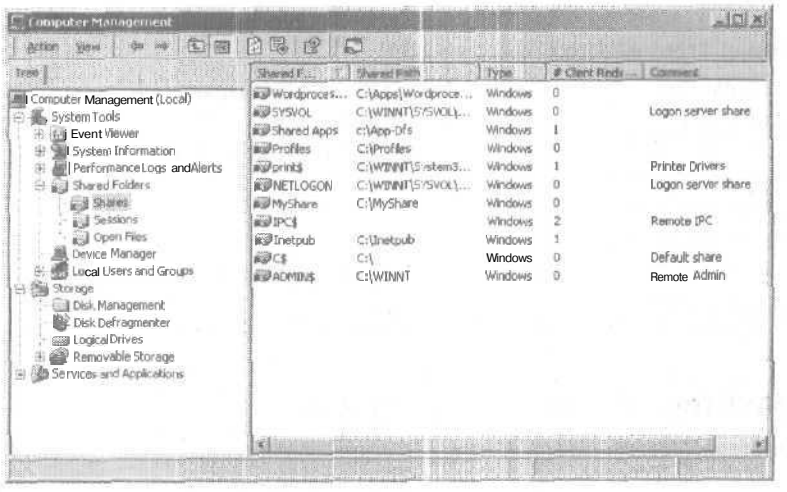


Рис. 14-7. Папка Shares (Ресурсы) в оснастке Shared Folders

В табл. 14-8 описывается содержание правой панели папки Shares (рис. 14-7).

Табл. 14-8. Поля правой панели папки Shares

Поле	Описание
Shared Folder (Общая папка)	Имена общих папок компьютера
Shared Path (Общий путь)	**Путь к общей папке**
Type (Тип)	Тип операционной системы, под управлением которой должен работать компьютер для доступа к общей папке
# Client Redirections (Клиентских перенаправлений)	Число клиентов, удаленно подключенных к общей папке
Comment (Комментарий)	Описания папки. Вы задали этот комментарий, когда создавали общую папку

Примечание Windows 2000 не обновляет список общих папок, открытых файлов и пользовательских сеансов автоматически. Чтобы обновить его, в меню Action (Действие) выберите команду Refresh (Обновить).

Определение максимально допустимого числа одновременных подключений к общей папке

Оснастка Shared Folders позволяет определить максимально допустимое число одновременных подключений к общей папке. В правой панели Shared Folders щелкните папку,

для которой требуется задать максимальное число подключений, и в меню Action выберите команду Properties. Откроется диалоговое окно свойств общей папки. Максимальное число подключений отображается на вкладке General (Общие).

Кроме того, средствами оснастки Shared Folders можно определить, достигнуто ли максимально допустимое число подключений к папке. Это весьма упрощает устранение неполадок подключений. Предположим, пользователь не может подключиться к общему ресурсу. Проверьте число подключений к этой папке и сравните его с максимально допустимым. Если максимально допустимое число подключений достигнуто, пользователю не удастся подключиться к ресурсу.

Изменение свойств общей папки

Папка Shares позволяет изменять существующие общие папки, в том числе и модифицировать их разрешения. Для изменения свойств щелкните папку и выберите в меню Action команду Properties. На вкладке General открывшегося окна свойств отображается имя общей папки, путь к ней и комментарий. Кроме того, здесь можно узнать и задать ограничения на число пользователей для доступа к папке. Вкладка Security (Безопасность) позволяет просматривать и изменять разрешения общей папки.

Мониторинг открытых файлов

Папка Open Files (Открытые файлы) оснастки Shared Folder (рис. 14-8) позволяет просматривать список открытых файлов общих папок и подключенных к этим файлам пользователей. Эта информация пригодится, если вам требуется оповестить подключенных пользователей об остановке системы. Кроме того, вы можете выявить пользователей, у которых открыты подключения к файлу, чтобы известить их о том, что к занятому им файлу пытаются обратиться другие люди.

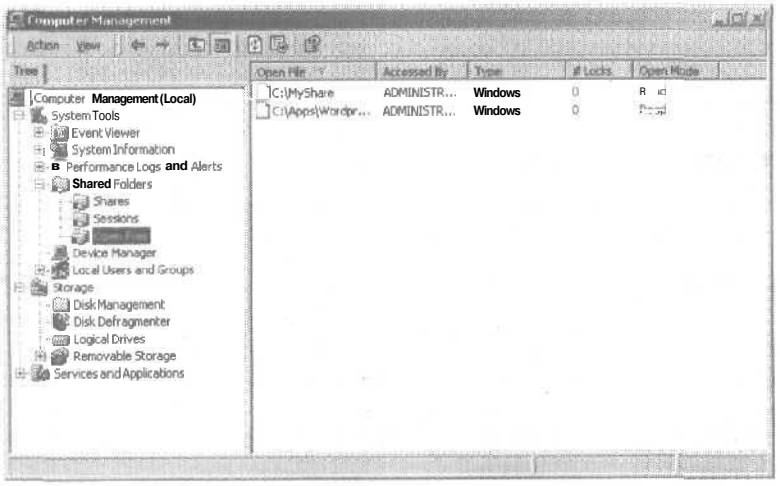


Рис. 14-8. Палка Open Files **(Открытые файлы) оснастки Shared Folders**

В табл. 14-9 описано содержимое папки Open **Files.**

Табл. 14-9. Поля папки Open Files

Поле	Описание
Open File (Открытый файл)	Имена открытых файлов
Accessed By (Пользователь)	Регистрационные имена пользователей, открывших файлы
Type (Тип)	Операционная система компьютера пользователя
# Locks (Блокир.)	Число блокировок файла. Некоторые программы требуют от ОС блокировать файл для монопольного доступа и не допускать его изменение другими программами
Open Mode (Режим открытия)	Тип доступа, запрошенный пользовательским приложением при открытии файла (Read или Write)

Отключение пользователей от открытых файлов

Вы можете отключать пользователей как от одного, так и от всех открытых файлов. Изменения разрешений в файловой системе NTFS на доступ к файлу, открытому на данный момент каким-либо пользователем, не будут известны пользователю до тех пор, пока он заново не откроет файл.

Чтобы эти изменения вступили в силу незамедлительно, можно:

- отключить всех пользователей от всех открытых файлов. Для этого в дереве оснастки Shared Folders щелкните папку Open Files и выберите в меню Action команду Disconnect All Open Files (Отключить все открытые файлы);
- отключить всех пользователей от одного открытого файла. Для этого в дереве оснастки Shared Folders щелкните папку Open Files и выберите в меню Action команду Close Open File (Закрыть файл).

Внимание! Отключение пользователей от открытых файлов может привести к потере данных.

Отправка консольных сообщений

Для предотвращения потери данных вы можете послать сообщение нескольким или всем пользователям, подключенным к общим папкам.

► **Отправка консольного сообщения подключенному пользователю**

1. Щелкните оснастку Shared Folders (Общие папки) и выберите в меню Action (Действие) команду All Tasks\Send Console Message (Все задачи\Отправка сообщения консоли).
2. В одноименном окне в поле Message (Сообщение) введите текст отправляемого сообщения.
3. Выберите в поле Recipients (Получатели) имя компьютера, которому отправляете сообщение, и щелкните кнопку Send (Отправить).

   Если пользователь зарегистрирован на нескольких компьютерах, сообщение получат лишь компьютеры, указанные в списке получателей.

   Если какие-либо адресаты не получили данное сообщение, вы вернетесь в диалоговое окно Send Console Message. Адресаты, не получившие данное сообщение, останутся в списке получателей. Проверьте правильность указания имен и доступность компьютеров.

Практикум: управление общими папками

Вы просмотрите общие папки и открытые файлы сервера с помощью оснастки Shared Folders и затем отключите всех пользователей от всех открытых файлов.

▶ **Задание 1: просмотрите общие папки компьютера**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Computer Management (Управление компьютером).
2. В дереве консоли Computer Management раскройте папку System Tools (Служебные программы), а затем — папку Shared Folders (Общие папки).
3. В дереве консоли щелкните подпапку Shares.

   Заметьте, что в правой панели отображается список всех общих папок компьютера,

▶ **Задание 2: просмотрите открытые файлы компьютера**

1, В дереве консоли щелкните подпапку Open Files (Открытые файлы) ниже узла Shared Folders.

   Если вы работаете на компьютере, не подключенном к сети, открытых файлов не будет — в папке Open Files отображаются лишь подключения удаленных компьютеров к общим ресурсам вашей системы,

▶ **Задание 3: отключите всех пользователей от файлов, открытых на вашем компьютере**

1. В дереве консоли щелкните подпапку Open Files и выберите в меню Action команду Disconnect All Open Files (Отключить все открытые файлы).

   Если вы не подключены к сети, открытых файлов для отключения не будет.
2. Закройте консоль Computer Management.

Резюме

Оснастка Shared Folders в Microsoft Windows 2000 упрощает контроль доступа к сетевым ресурсам и отправку административных сообщений пользователям. Она позволяет выполнять мониторинг ресурсов локального компьютера. Добавляя оснастку Shared Folders в консоль MMC, вы можете указать, наблюдать ресурсы какого компьютера требуется — локального или удаленного.

Для просмотра списка общих папок компьютера и определения числа подключенных к ним пользователей применяется папка Shares оснастки Shared Folders. На вкладке General окна свойств общего ресурса можно задать максимально допустимое число подключений к папке. Папка Open Files оснастки Shared Folders позволяет просматривать список открытых файлов общих папок и подключенных к этим файлам пользователей.

Выполняя практикум, вы просмотрели общие папки и открытые файлы своего компьютера и отключили всех пользователей от всех открытых файлов.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении А «Вопросы и ответы» в конце книги.

1. Что рекомендуется предпринять в первую очередь при неполадках в работе Active Directory?

2. Чем различаются объект и счетчик производительности?

3. Чем различаются журнал счетчиков и трассировочный отчет?

4. Какие действия может вызывать оповещение?

5. Какие возможности предоставляет администратору утилита LDP и как ее запустить?

6. Как узнать, какие файлы общей папки открыты и кто к ним подключен?

ГЛАВА 15

Установка Windows 2000 с использованием RIS

В этой главе

Службы удаленной установки (Remote Installation Services, RIS) позволяют настроить компьютеры-клиенты удаленно, то есть не покидая своего рабочего места. Вы можете установить операционные системы на компьютеры, поддерживающие удаленную загрузку. Для этого надо подключиться к компьютеру по сети, запустить компьютер-клиент и войти в систему с учетной записью пользователя. В этой главе речь пойдет о службах удаленной установки. Выполняя практикум, вы научитесь внедрять и администрировать RIS. Кроме того, вы изучите особенности работы службы RIS, а также методы устранения проблем.

Прежде всего

Для изучения материалов этой главы вам не нужны никакие специальные знания.

Занятие 1. Знакомство со службой RIS

На этом занятии мы опишем архитектуру и компоненты RIS, а также служб Microsoft Windows 2000, необходимых для удаленной установки ОС. На этом занятии также обсуждаются компоненты и службы, необходимые для удаленной установки ОС на клиентском компьютере.

Изучив материал этого занятия, Вы сможете:

- ✓ перечислить службы и компоненты, необходимые для удаленной установки ОС;
- ✓ описать ход процесса удаленной установки ОС;
- ✓ перечислить **требования к клиентам** и серверам RIS;
- ✓ перечислить сетевые платы, поддерживаемые загрузочным диском RIS.

Продолжительность занятия — около 20 минут.

Удаленная установка ОС

На рис. 15-1 показаны службы и компоненты удаленной установки ОС.

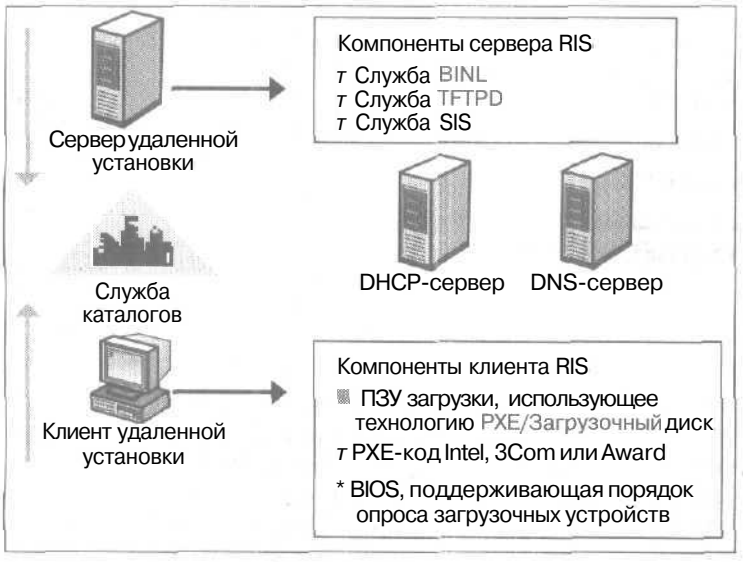


Рис. 15-1. Удаленная установка ОС

Для удаленной установки ОС требуются некоторые специальные службы. Возможно, некоторые уже установлены и работают н вашей сети, а другие — нет. К ним относятся Active Directory, обновленный DHCP-сервер и совместимая версия DNS.

Компоненты сервера удаленной установки

При установке службы RIS на сервер добавляются компоненты, перечисленные ниже.

- **Уровень согласования информации загрузки (Boot Information Negotiation Layer, BINL).** Служба BINL добавляется в процессе установки RIS и позволяет управлять всей средой служб удаленной установки. Эта служба реагирует на запросы клиентов на сетевое обслуживание, запрашивает Active Directory от имени клиентских систем и обеспечи-

вает применение правильных политик и параметров в процессе установки ОС на клиентском компьютере. Служба BINL гарантирует, что клиенту переданы верные файлы и в случае предварительной настройки клиента гарантирует, что он обслуживается гем сервером служб удаленной установки, которым нужно. Если компьютер-клиент предварительно не настроен, служба BINL создает объект учетной записи компьютера-клиента в Active Directory.

- **Упрощенный FTP-демон (Trivial File Transfer** Protocol Daemon, **TFTPD).** Сервер служб удаленной установки использует эту службу для загрузки файлов, необходимых для начала удаленной установки. Служба TFTPD применяется для загрузки мастера Client Installation (Мастер установки клиентов) и всех его диалоговых окон для текущего сеанса,
- **Хранилище единственных копий (Single Instance Store, SIS).** Это способ уменьшения полного объема хранилища, требуемого на томе служб удаленной установки. Служба S1S прикрепляет себя к тому RIS и ищет идентичные файлы. Для дубликатов файлов SIS создает ярлыки, в результате чего службам удаленной установки требуется меньше места на серверном диске.

Компоненты клиента удаленной установки

Существует два типа удаленных компьютеров-клиентов, поддерживающих удаленную загрузку:

- компьютеры с основанным на DHCP загрузочным ПЗУ, использующим технологию PXE (Pre-Boot execution Environment);
- компьютеры с сетевыми платами, поддерживаемыми загрузочным диском служб удаленной установки.

Технология удаленной загрузки **PXE**

Удаленная установка ОС использует протокол DHCP, соответствующий архитектуре PXE, для установки ОС из удаленного источника на жесткий диск клиентской системы. Удаленный источник (сервер, поддерживающий RIS) предоставляет сетевой эквивалент установки Windows 2000 с компакт-диска или предварительно сконфигурированный RIPrep-образ. На данный момент операционная система Windows 2000 Professional — единственная ОС, поддерживаемая службой удаленной установки. Возможны разные варианты установки.

- **Установка с компакт-диска.** Аналогична установке непосредственно с компакт-диска Windows 2000 Professional. Исходные файлы хранятся в сети на серверах RIS;
- **Форматирование с записью RIPrep-образа.** Позволяет сетевому администратору копировать стандартную конфигурацию офисного компьютера, дополненную параметрами ОС, рабочего стола и приложениями, установленными локально. Установив ОС Windows 2000 Professional на первый компьютер и настроив ее службы и любые стандартные приложения, сетевой администратор запускает мастер, который подготавливает и реплицирует образ установки на доступный RIS-сервер. Затем с этого сервера ОС устанавливают на другие компьютеры.
- После размещения образа на RIS-сервер (ах) конечные пользователи удаленных систем с основанным на PXE загрузочным ПЗУ могут начать установку ОС с любого из доступных в сети RIS-серверов. Так как пользователь справляется с установкой ОС без помощи администратора, последний может потратить свое время для решения других задач. Таким образом, уменьшается время и снижаются расходы на установку ОС.

Как работает технология удаленной загрузки PXE

PXE (Pre-Boot execution Environment) — новая технология удаленной загрузки, разработанная столпами компьютерной индустрии. Она позволяет компаниям использовать для поиска RIS-серверов в сети существующую сетевую инфраструктуру TCP/IP, основанную на DHCP. Компьютеры, совместимые со стандартом Net PC/PC98, могут применять технологию удаленной загрузки, встроенную в операционную систему Windows 2000. Net PC/PC98 — ежегодные рекомендации для разработчиков оборудования, издаваемые совместно Microsoft и Intel при сотрудничестве Compaq и других крупных компаний. PC98 — стандарт разработки оборудования, расширяющий возможности аппаратной платформы и позволяющий Microsoft включать в Windows дополнительные функции, такие, как служба удаленной установки.

На рис. 15-2 иллюстрируется порядок запросов к службе DHCP, выполняемых загрузочным ПЗУ PXE-совместимого сетевого адаптера.

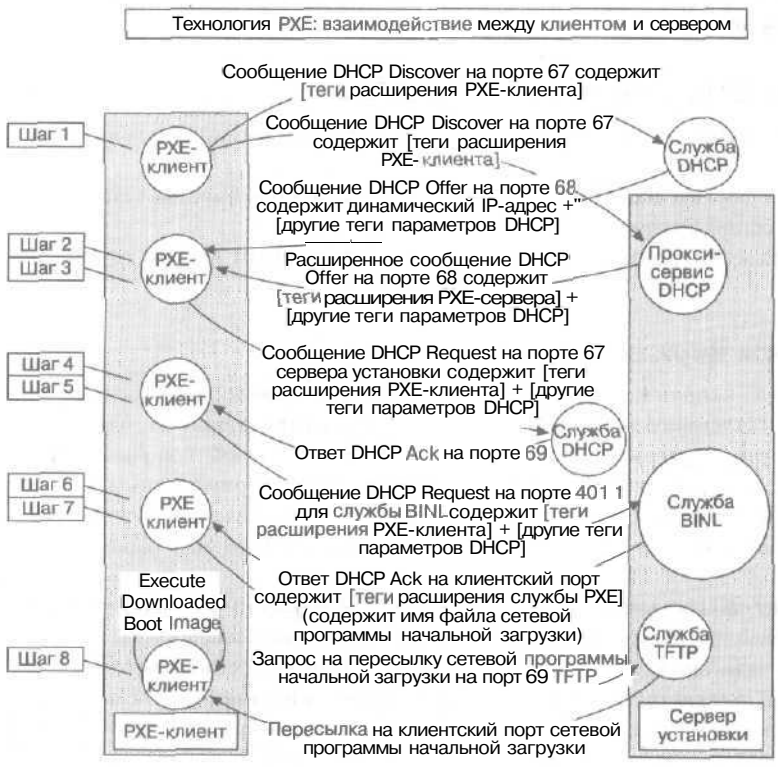


Рис. 15-2. Процесс загрузки ПЗУ, использующего технологию PXE

Когда первый раз запускается новый компьютер-клиент, для которого разрешена удаленная загрузка PXE, клиент запрашивает IP-адрес через протокол DHCP. В начале запроса компьютер-клиент сообщает доступным в сети RIS-серверам, что он поддерживает PXE и его необходимо обслужить. На это извещение может ответить любой доступный RIS-сервер, сообщив клиенту свой IP-адрес и имя загрузочного файла, который надо запросить для дальнейшего обслуживания. Если клиентский компьютер отвечает серверу, что нуждается в обслуживании со стороны последнего, служба DHCP подтверждает свою готовность. Клиент должен также запросить готовность службы BINL, которая передает

клиенту файл начальной загрузки и гарантирует, что прошедшие предварительную настройку клиенты обслуживаются соответствующим RIS-сервером.

После того как служба BINL скопирует на клиентский компьютер программу начальной сетевой загрузки, пользователь действует в зависимости от поставщика сервера удаленной установки, ответившего на клиентский запрос на обслуживание. Далее мы подробно рассмотрим работу службы удаленной установки, встроенной в ОС Windows 2000 Server.

Загрузочный диск служб удаленной установки

Применяется на компьютерах-клиентах, которые не имеют ПЗУ удаленной загрузки и поддерживает разные сетевые PCI-платы. Использование загрузочного диска служб RIS позволяет не оснащать существующие компьютеры-клиенты новыми сетевыми платами с ПЗУ удаленной загрузки на основе PXE. Загрузочный диск имитирует процесс загрузки PXE для компьютеров без ПЗУ удаленной загрузки.

Реализация удаленной установки

Удаленная установка проиллюстрирована на рис. 15-3. Для загрузочного ПЗУ на основе PXE и загрузочного диска служб RIS удаленная установка выполняется аналогично. Далее подробно описан каждый из этапов этого процесса.

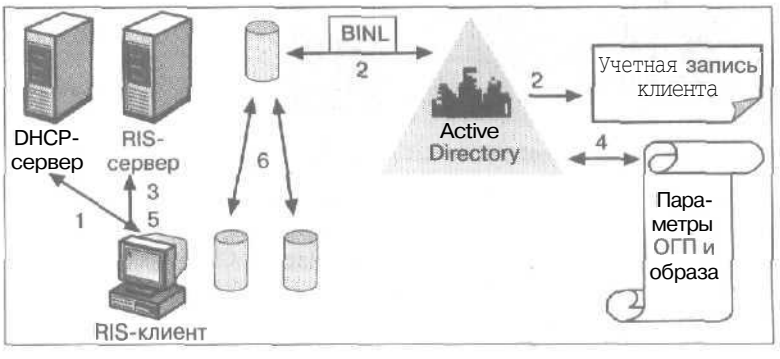


Рис. 15-3. Архитектура RIS

Подключение к RIS-серверу и выбор образа ОС осуществляется в несколько этапов: вход клиентского компьютера с поддержкой PXE в сеть и обслуживание этого компьютера RIS-сервером.

Процесс удаленной установки операционной системы

1. Подключенный к сети компьютер-клиент загружается и посылает запрос на обслуживание. Как часть запроса на сетевое обслуживание, в сеть передается пакет DHCPDISCOVER, запрашивающий у ближайшего DHCP-сервера IP-адрес доступного RIS-сервера. В составе запроса клиент передает собственный глобально уникальный идентификатор (GUID). GUID указан в BIOS PC98/Net PC-совместимых компьютеров-клиентов. DHCP-сервер отвечает на запрос, отсылая клиенту IP-адрес RIS-сервера. Любой доступный RIS-сервер может сообщить свой IP-адрес и имя загрузочного файла, который клиенту надо запросить для дальнейшего обслуживания. Чтобы начать обслуживание, вам придется нажать клавишу F12, о чем вы будете проинформированы соответствующим сообщением.

1. RIS-сервер (с помощью службы BINL) проверяет, имеется ли в каталоге Active Directory предопределенная учетная запись, соответствующая этому компьютеру-клиенту. Для проверки BINL запрашивает в Active Directory компьютер-клиент с GUID, переданным на первом этапе.
3. По завершении проверки на компьютер-клиент загружается *мастер установки клиента* (Client Installation Wizard, CIW), который предлагает пользователю зарегистрироваться в сети.
4. После входа пользователя в сеть RIS-сервер ищет в Active Directory его учетную запись, проверяя пароль. Затем RIS проверяет параметры настройки политики групп и определяет, доступом к каким параметрам установки обладает пользователь. Кроме того, RIS определяет, какие образы ОС будут предложены конкретному пользователю. Мастер CIW предоставляет эти параметры клиенту (рис. 15-4).

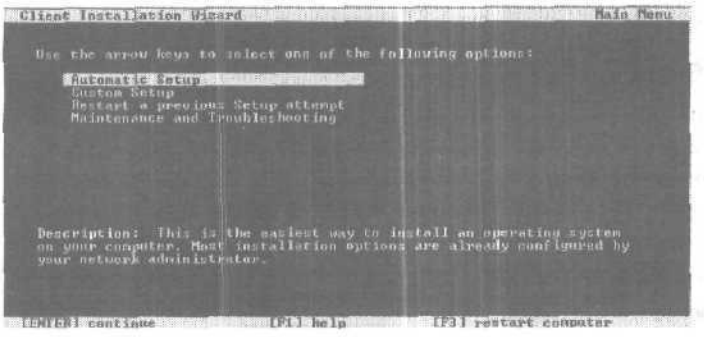


Рис. 15-4. Параметры установки, предоставляемые мастером CIW

5. Если пользователю доступны лишь один вариант установки и один образ ОС, ему не предлагается выбирать что-либо. Если же пользователю доступны несколько вариантов установки и образов ОС, отображается их список. Мастер CIW предупреждает пользователя, что в процессе установки его жесткий диск будет отформатирован и вся информация на нем будет удалена. Затем пользователю предлагается запустить удаленную установку.

Примечание Подробнее о настройке параметров установки, предоставляемых мастером CIW, — на занятии *1*.

6. После того как пользователь подтверждает в окне обобщения выбранные параметры, начинается установка операционной системы. Если на данном этапе учетная запись компьютера-клиента отсутствует в каталоге Active Directory, служба BINL создает ее, автоматически генерируя имя компьютера. ОС устанавливается локально, то есть в процессе установки конечному пользователю не предлагается выбирать какие-либо параметры.

Внимание! Поскольку мастер CIW работает в среде PXE, он не поддерживает символы из расширенного набора ни в отображаемом тексте, ни в полях ввода (имя пользователя, пароль, домен и любые другие параметры, указываемые пользователем). Необходимо внимательно проанализировать создаваемые имена пользователей и доменов, так как имена с символами из расширенного набора в RIS применять нельзя.

С точки зрения конечного пользователя процесс удаленной установки ОС прямолинеен. Администратор может помогать пользователю во время установки ОС, предопределив доступные тому параметры установки. Кроме того, администратор также имеет право ограничить количество доступных пользователю образов ОС, гарантируя тем самым корректный тип установки ОС и ее успешное завершение.

Требования к серверу и клиенту RIS

Требования к аппаратному обеспечению сервера

- Персональный компьютер с процессором Pentium или Pentium II с тактовой частотой не ниже 166 МГц (рекомендуется процессор с тактовой частотой 200 МГц или более быстрый).
- 64 Мб ОЗУ (96—128 Мб ОЗУ, если установлены дополнительные службы, такие, как Active Directory, DHCP или DNS).
- Жесткий диск или раздел диска, предназначенный для дерева каталогов RIS, объемом не менее 2 Гб. RIS требует значительного объема свободного пространства на жестком диске.
- Сетевой адаптер со скоростью 10 или 100 Мб/сек (рекомендуется 100 Мб/сек).

Внимание! Устанавливать RIS следует на раздел жесткого диска, отличный от загрузочного. RIS нельзя установить на один диск с системным томом. Том, выбранный для установки RIS, должен быть отформатирован с файловой системой Windows NT (NTFS).

Требования к программному обеспечению сервера

Следующие службы необходимо установить либо на отдельные серверы, либо на один общий сервер, чтобы они были активны и доступны:

- DNS;
- DHCP;
- Active Directory.

Примечание Подробнее об установке и настройке DHCP — в приложении Б.

Требования к аппаратному обеспечению клиента

- Net PC-совместимый компьютер с процессором Pentium 166 МГц или более быстрым.
- Не менее 32 Мб ОЗУ (рекомендуется 64 Мб).
- Жесткий диск объемом не менее 800 Мб.
- Поддерживаемая сетевая PCI-плата стандарта Plug and Play.
- Дополнительно: ПЗУ удаленной загрузки на основе PXE версии .99c или более поздней.

Сетевые платы, поддерживаемые загрузочным диском RIS

Далее перечислены сетевые платы, поддерживаемые загрузочным диском RIS. Для просмотра списка поддерживаемых сетевых плат можно также запустить в командной строке утилиту RBFG и выбрать Adapter List.

Сетевые платы 3Com:

- 3C900 (Combo и TP0);

- 3C900B (Combo, FL, TPC, TPO);
- 3C905 (T4 и TX);
- 3C905B (Combo, TX, **FX);**
- 3C905C (TX).

Сетевые платы AMD:

- AMD PCNet и Fast PCNet.

Сетевые платы Compaq:

- Netflex 100 (NetIntelligent II);
- Netflex 110 (NetIntelligent III);
- Netflex 3.

Сетевые платы Digital Equipment Corp (DEC):

- DE 450;
- DE 500.

Сетевые платы Hewlett-Packard:

- HP Deskdirect 10/100 TX.

Сетевые платы Intel Corporation:

- Intel Pro 10+;
- Intel Pro 100+;
- Intel Pro 100B (включая серию E100).

Сетевые платы SMC:

- SMC 8432;
- SMC 9332;
- SMC 9432.

Примечание Программа создания загрузочного диска RIS поддерживает только PCI-платы. Платы ISA, EISA и Token ring не поддерживаются.

Резюме

Здесь описана архитектура RIS и службы Windows 2000, необходимые для удаленной установки ОС, а также компоненты и службы сервера и клиента, требуемые для реализации удаленной установки ОС в вашей организации.

Занятие 2. Особенности реализации RIS

Здесь обсуждаются установка и настройка RIS, создание образа RIPrep, создание загрузочного диска RIS и проверку конфигурации RIS.

Изучив материал этого занятия, Вы сможете:

- ✓ установить и настроить RIS;
- ✓ создать образ RIPrep;
- ✓ создать загрузочный диск RIS;
- ✓ проверить конфигурацию RIS.

Продолжительность занятия - около 30 минут.

Установка RIS

Осуществляется в два этапа — добавление компонента RIS и установка RIS.

Внимание! Перед установкой RIS обязательно изучите раздел «Требования к серверу и клиенту RIS» занятия 1.

Добавление компонента RIS

Первый этап установки RIS: добавление служб удаленной установки — дополнительного компонента Windows 2000. На этом этапе необходимые для установки файлы копируются на жесткий диск сервера. Компонент RIS можно добавить как в процессе, так и после установки Windows 2000 Server с помощью программы Add/Remove Programs (Установка и удаление программ) из панели управления Windows.

► **Добавление компонента RIS**

1. Запустите мастер Windows Components (Мастер компонентов Windows) одним из следующих способов:
   - во время установки Windows 2000 Server;
   - раскройте меню Start\Settings (Пуск\Программы) и щелкните Control Panel (Панель управления); в панели управления дважды щелкните значок Add/Remove Programs (Установка и удаление программ). В открывшемся окне щелкните кнопку Add/Remove Windows Components (Добавление и удаление компонентов Windows).
2. В диалоговом окне мастера (рис. 15-5) пометьте флажок Remote Installation Services (Службы удаленной установки) и щелкните Next.
3. По запросу системы вставьте в привод установочный компакт-диск Windows 2000 Server.
4. В окне Completing The Windows Components Wizard (Завершение работы мастера установки Windows) щелкните кнопку Finish (Готово).
5. В окне сообщения System Settings Change (Изменение параметров системы) щелкните кнопку Yes для перезагрузки сервера перед установкой RIS.

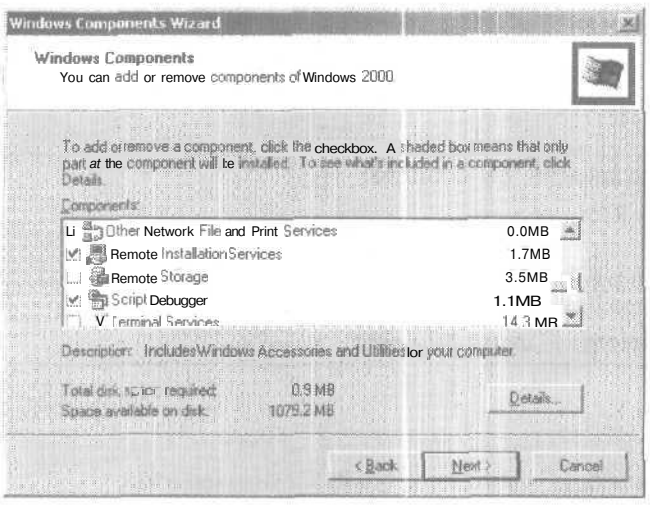


Рис. 15-5. Диалоговое окно мастера компонентов Windows

Установка RIS

Второй этап настройки RIS — установка RIS на сервер.

▶ **Установка RIS**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Configure Your Server (Настройка сервера).
2. В диалоговом окне Configure Your Server (Настройка сервера Windows 2000) щелкните ссылку Finish Setup (Завершение установки).
3. На вкладке Configure Remote Installation Services (Настройка служб удаленного доступа) диалогового окна Add/Remove Programs шелкните кнопку Configure (Настроить), чтобы запустить мастер установки с.]ужб RIS.
4. В первом окне мастера щелкните Next.
5. Продолжайте установку, отвечая на вопросы мастера. Вам придется выбрать:
   - место в файловой системе сервера, где следует создать структуру установочных папок;
   - должен ли сервер RIS начать обслуживание клиентов сразу по окончании установки;
   - путь к установочному компакт-диску Windows 2000 Professional или место в сети, где находятся установочные файлы этой ОС;
   - имя папки образа установки на сервере;
   - понятное описание и справочный текст, описывающий пользователям этот образ установки.

   По завершении работы мастера в зависимости от выбранных параметров сервер RIS либо начинает обслуживать запросы клиентских компьютеров, либо ожидает, пока вы зададите параметры RIS. В следующем разделе описываются конфигурационные параметры, доступные администратору RIS.

Настройка RIS для обслуживания клиентов

В режиме по умолчанию по завершении установки сервер RIS не начинает сразу же обслуживать компьютеры-клиенты. Чтобы настроить RIS для обслуживания клиентов, необходимо:

- авторизовать RIS-сервер;
- задать свойства RIS-сервера;
- задать параметры установки RIS-клиентов;
- настроить права доступа к образам RIPrep.

Авторизация серверов RIS

Предотвращает добавление неавторизованных серверов RIS и гарантирует, что обслуживать клиентов будут только RIS-серверы, авторизированные администратором. При попытке подключить к сети неавторизованный RIS-сервер он автоматически выключается и не может обслуживать клиентов. Для обслуживания клиентов любой RIS-сервер должен пройти авторизацию.

▶ **Авторизация сервера RIS**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните DHCP.
2. В дереве консоли DHCP щелкните узел DHCP.
3. В меню Action (Действие) выберите команду Manage Authorized Servers (Список авторизованных серверов).
4. В диалоговом окне Manage Authorized Servers (Управление авторизованными серверами) щелкните кнопку Authorize (Авторизовать).
5. В диалоговом окне Authorize DHCP Server (Авторизация DHCP-сервера) введите имя или IP-адрес аутентифицируемого сервера и затем щелкните OK.
6. В окне сообщения DHCP щелкните кнопку Yes.
7. В диалоговом окне Manage Authorized Servers выберите компьютер и щелкните OK. Аутентифицированный RIS-сервер теперь отображается в узле DHCP.

Настройка свойств RIS-сервера

Позволяет управлять тем, как сервер обрабатывает запросы клиентов на обслуживание.

▶ **Настройка свойств RIS-сервера**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers (Active Directory — пользователи и компьютеры).
2. В дереве консоли выберите папку с компьютером, конфигурацию которого требуется проверить, например папку Computers или Domain Controllers,
3. В правой панели щелкните правой кнопкой мыши соответствующий RIS-сервер и выберите команду Properties (Свойства).
4. В диалоговом окне свойств перейдите на вкладку Remote Install (Удаленная установка).
5. На вкладке Remote Install (рис. 15-6) окна свойств задайте параметры, описанные в табл. 15-1.

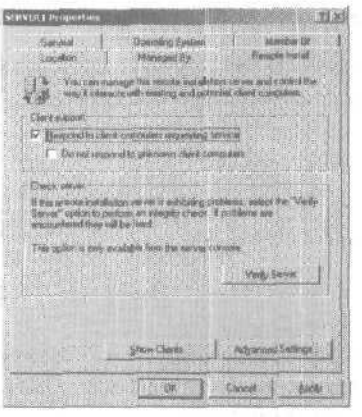


Рис. 15-6. Вкладка Remote Install (Удаленная установка) окна свойств RIS-сервера

Табл. 15-1. Параметры вкладки Remote Install

Параметр	Описание
Respond To Client Computers Requesting Service (Отвечать клиентским компьютерам, запрашивающим обслуживание)	Сервер RIS отвечает всем клиентским компьютерам, запрашивающим обслуживание
Do Not Respond To Unknown Client Computers (Не отвечать неизвестным клиентским компьютерам)	Сервер RIS не отвечает на запросы неизвестных клиентских компьютеров. Этот параметр доступен, только если помечен флажок Respond To Client Computers Requesting Service

6. На вкладке Remote Install щелкните кнопку Advanced Settings (Дополнительные параметры).
7. На вкладке New Clients (Новые клиенты) диалогового окна свойств службы удаленной установки (рис. 15-7) задайте параметры, описанные в табл. 15-2.

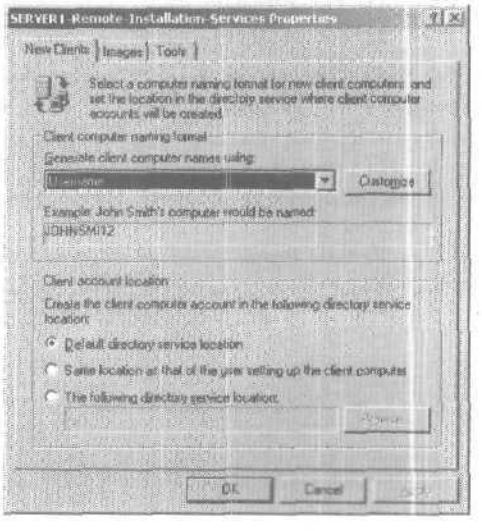


Рис. 15-7. Вкладка New Clients (Новые клиенты) окна свойств RIS-сервера

Табл. 15-2. Параметры вкладки New Clients

Параметр	Описание
Generate Client Computer Names Using (Создавать имена с помощью)	Данный список задает формат автоматически генерируемого имени клиентского компьютера. В процессе установки ОС он предоставляет расширенные возможности именования новых компьютеров-клиентов без вмешательства конечного пользователя или администратора
Customize (Настройка)	Эта кнопка открывает диалоговое окно Computer Account Generation (Генерация учетных записей компьютеров), где можно создать образец формата имени клиентского компьютера
Client Account Location (Размещение учетной записи компьютера-клиента)	Размещение учетной записи клиентского компьютера в службе каталогов: *Default Directory Service Location* (Размещение в домене по умолчанию) — указывает, что учетная запись клиентского компьютера будет создана в разделе Active Directory, где по умолчанию генерируются все учетные записи компьютеров во время объединения доменов; *Same Location As That Of The User Setting Up The Client Computer* (Там же, где находится устанавливающий пользователь) – указывает, что учетная запись клиентского компьютера будет создана в том же контейнере Active Directory, где хранится информация о пользователе, настраивающем компьютер; *Use The Following Directory Service Location* (В указанном размещении службы каталогов) — позволяет администратору указать специальный контейнер Active Directory, где будут храниться учетные записи клиентских компьютеров, устанавливаемых с этого сервера. Подразумевается, что большинство администраторов выберут этот параметр и укажут специальный контейнер для хранения учетных записей всех клиентов удаленной установки

8. На вкладке Images (Образы) диалогового окна свойств служб RIS (рис. 15-8) перечислены имеющиеся на RIS-сервере образы. Ознакомьтесь с ними. Щелкните кнопку Add (Добавить) и следуйте инструкциям мастера для установки дополнительных образов на сервер RIS. Более подробно об этом рассказано на занятии 3.
9. На вкладке Tools (Сервис) диалогового окна свойств службы RIS (рис. 15-9) отображаются имеющиеся на RIS-сервере утилиты поддержки системы и устранения проблем.
10. В диалоговом окне свойств RIS-сервера щелкните OK.
11. В следующем диалоговом окне снова щелкните OK.

Администраторы, которым требуется удаленно управлять серверами с рабочих станций Windows 2000 Professional, могут воспользоваться административными утилитами, установив пакет Windows 2000 Administration Tools (Администрирование) с компакт-диска Windows 2000 Server.

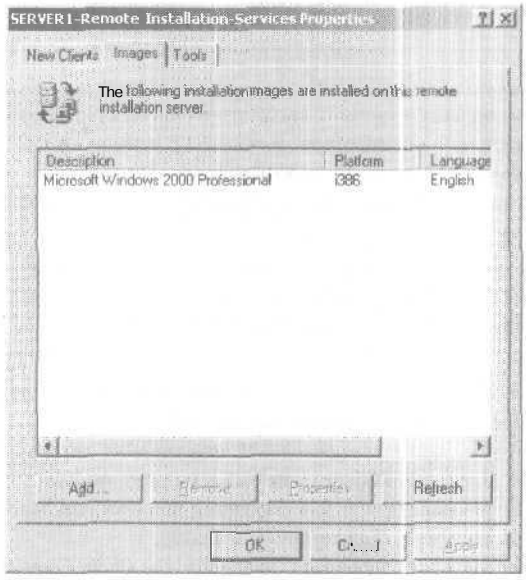


Рис. 15-8. Вкладка Images (Образы) диалогового окна свойств RIS-сервера

Примечание При использовании пакета Windows 2000 Administration Tools на системе, отличной от RIS-сервера, администратор не может добавлять дополнительные образы ОС и проверять целостность RIS-сервера. Все другие параметры конфигурации доступны.

Рис. 15-9. Вкладка Tools (Сервис) диалогового окна свойств RIS-сервера

Параметры установки клиентов RIS

Позволяют управлять параметрами, доступными различным группам пользователей в мастере **CIW.** Имеется четыре параметра установки (рис. 15-4):

- Automatic Setup (Автоматическая установка);
- Custom Setup (Выборочная установка);
- Restart A Previous Setup Attempt (Перезапуск предыдущей попытки установки);
- Maintenance And Troubleshooting (Обслуживание и устранение неполадок).

Automatic Setup

Доступом к этому параметру установки обладают все пользователи службы RIS. Automatic Setup позволяет задать параметры установки ОС таким образом, что пользователь будет обычным порядком регистрироваться в системе и запускать установку. Пользователю не придется выбирать какие-либо параметры, что упростит процесс и сократит затраты на поддержку.

Возможен и другой вариант: администратор разрешает пользователям выбирать устанавливаемый образ ОС. Служба RIS позволяет задать сопровождающий текст, описывающий параметры ОС. поэтому конечному пользователю не составит труда выбрать наиболее подходящий для него образ ОС.

Задавая конфигурационные параметры службы удаленной установки, администратор предопределяет формат автоматического именования компьютеров и место в Active Directory, где будут создаваться учетные записи компьютеров-клиентов.

Custom Setup

Параметр Custom Setup во многом аналогичен параметру Automatic Setup, он позволяет настроить компьютер для другого пользователя. Вы сможете полностью настроить компьютер-клиент, и подготовить клиентскую систему, создав соответствующую учетную запись компьютера в службе Active Directory.

Параметр Custom Setup позволяет переопределить формат автоматического именования компьютеров и место в Active Directory, где будут создаваться учетные записи компьютеров. По умолчанию RIS-сервер генерирует имя компьютера, согласно формату, определенному администратором службы удаленной установки ОС. Вы можете также указывать, где в службе Active Directory во время процесса установки будет создана *учетная запись клиентского компьютера* (client computer account object, CAO). По умолчанию политика автоматического именования компьютеров генерирует имя системы на основе имени пользователя, работающего с мастером CIW.

Restart A Previous Setup Attempt

Повторяет установку ОС, если процедура не была завершена из-за сбоя. Мастер CIW можно настроить так, что он задаст пользователю ряд вопросов о конкретной устанавливаемой ОС. При продолжении прерванной установки эти вопросы он не повторяет — программа установки уже обладает всей необходимой информацией; она просто возобновит копирование файлов и завершит установку ОС.

Maintenance And Troubleshooting

Обеспечивает доступ к программам обслуживания и устранения неполадок компьютеров-клиентов. Примеры содержат программы поиска вирусов в памяти, обновление Flash BIOS системы и программы диагностики компьютера. Эти средства доступны еще перед установкой и запуском ОС на клиентском компьютере.

Когда пользователю доступен параметр Maintenance And Troubleshooting, управление доступом к образам отдельных утилит осуществляется аналогично управлению доступом к параметрам ОС — администратор должен задать соответствующие разрешения для файла настройки автоматической установки (.sif), связанного с данной утилитой. Например, он может предоставить конечным пользователям доступ лишь к одной диагностической утилите, а специалистам службы технической поддержки — ко всем имеющимся диагностическим средствам. Когда пользователь обращается к специалисту за помощью, тот объясняет, как, применив доступную утилиту, собрать необходимую для диагностики проблемы информацию. Если же специалист службы поддержки выезжает к пользователю для решения проблемы, он регистрируется в мастере CIW и по своим реквизитам получает доступ к необходимым для устранения проблемы утилитам.

► **Выбор параметров установки клиентов**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers.
2. В дереве консоли щелкните правой кнопкой мыши соответствующее **ОП,** например Computers или Domain Controllers, и выберите команду Properties. Затем перейдите на вкладку Group Policy (Групповая политика).
3. В диалоговом окне свойств групповой политики щелкните объект групповой политики (ОГП). Затем щелкните кнопку Edit (Изменить), чтобы открыть консоль групповой политики.
4. В дереве консоли групповой политики раскройте узел User Configuration\Windows Settings (Конфигурация пользователя\Конфигурация Windows) и щелкните Remote Installation Services (Службы удаленной установки).
5. На правой панели дважды щелкните значок Choice Options (Параметры выбора).

   Параметры диалогового окна Choice Options Properties (Свойства: Параметры выбора) определяют вид мастера CIW для пользователя (рис. 15-10):
   - Automatic Setup (Автоматическая установка);
   - Custom Setup (Выборочная установка);
   - Restart Setup (Перезапуск установки);
   - Tools (Сервис).
6. Для каждого параметра установки щелкните один из следующих переключателей:
   - **Allow (Разрешить)** — параметр установки будет доступен пользователям, на которых распространяется действие политики;
   - **Don't Care (Не важно)** — будут применены параметры политики родительского контейнера. Например, если администратор домена задал особую для RIS групповую политику, а администратор данного контейнера щелкнул переключатель Don't Care, политика, определенная для домена, применяется ко всем пользователям этого домена. Переключатель Don't Care выбран по умолчанию;
   - **Deny (Запретить)** — параметр установки будет недоступен пользователям, на которых распространяется действие политики.
7. В диалоговом окне Choice Options Properties щелкните **OK.**
8. Закройте оснастку Group Policy и затем в окне свойств групповой политики щелкните OK.

Изменения политики RIS вступают и силу только после того, как политика будет передана (распространена) на ваш компьютер, и поэтому для получения политики вам необходимо предпринять одно из следующих действий: наберите в командной строке **secedit /refreshpolicy user_policy** и нажмите клавишу Enter; перезагрузите компьютер; дождитесь автоматического применения политики — это происходит через определенные интервалы време-

ни, которые вы можете задать самостоятельно. По умолчанию политика применяется каждые 8 часов.

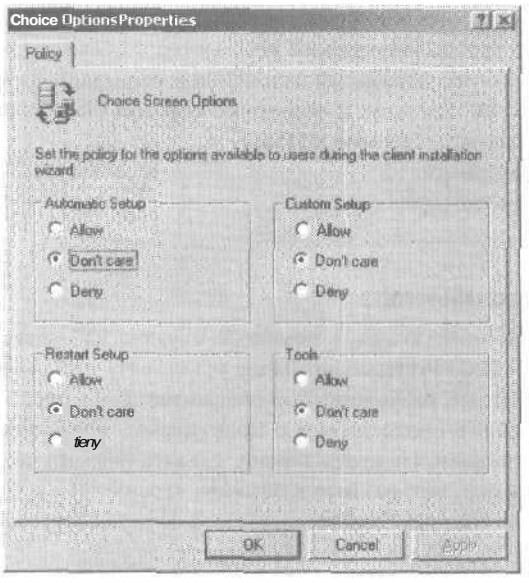


Рис. 15-10. Диалоговое окно Choice Options Properties (Свойства: Параметры выбора)

Задание разрешений на доступ к образу RIPrep

Определяя пользователей и группы, обладающие доступом к имеющимся на RIS-сервере образам установки RIPrep, вы помогаете пользователям выбрать правильный вариант необслуживаемой установки ОС, соответствующий их роли в компании. По умолчанию после добавления на RIS-сервер образ доступен всем пользователям, обслуживаемым данным сервером.

▶ **Задание разрешений доступа к образу RIPrep**

1. Раскройте меню Start\Programs\Accessories (Пуск\Программы\Стандартные) и щелкните Windows Explorer (Проводник).
2. В папке \RemoteInstall\Setup*соответствующий_язык*\Images*имя_ соответствующего_образа*\i386\templates (или папке сервера, в которую вы будете копировать установочные файлы образа) щелкните нужный файл .sifправой кнопкой и выберите команду Properties,
3. В окне свойств данного файла перейдите на вкладку Security (Безопасность).
4. Задайте необходимые разрешения, чтобы предоставить пользователям доступ к образам ОС, и затем щелкните OK.

Примечание Чтобы немного освободить администратора от назначения разрешений на доступ к образам, там, где это допустимо, задавайте разрешения не для отдельных .sif файлов, а для папки Templates. Предоставляйте или запрещайте доступ группам, а не отдельным пользователям.

Создание образа RIPrep

Для репликации конфигурации большинства офисных компьютеров многие организации используют программное обеспечение для создания образов или клонирования содержимого диска. Эти утилиты позволяют настроить клиентский компьютер в соответствии с вашими потребностями и затем сделать копию образа для дальнейшей установки на компьютерах-клиентах сети. В службе RIS для создания и установки образов стандартного офисного компьютера можно воспользоваться образами RIPrep.

Перед созданием образа RIPrep необходимо:

- создатьконфигурацию исходного компьютера;
- настроить рабочую станцию.

Создание конфигурации исходного компьютера

Чтобы создать конфигурацию исходного компьютера, с помощью службы RIS удаленно установите базовую версию ОС Windows 2000 Professional. Далее установите приложения или пакеты приложений, включая программы, разработанные специалистами вашей компании. Затем настройте рабочую станцию в соответствии с политиками, принятыми в компании. Например, можно задать определенные цвета экрана, сделать логотип компании рисунком рабочего стола, удалить игры, встроенные в базовую версию ОС, а также настроить параметры прокси-сервера для Internet Explorer.

Настройка рабочей станции

Во время создания образов RIPrep важно понимать, как связаны профили пользователей, коррективы, вносимые на исходном компьютере RIPrep, и желаемый результат для пользователей, которые регистрируются на компьютерах, настроенных с помошью образа RIPrep. Приложения с логотипом «Certified for Windows» корректно разделяют конфигурационные параметры компьютера и пользовательские параметры и данные, что позволяет делать такие программы при установке на компьютеры фирмы доступными всем пользователям. Эти приложения смогут также применять все пользователи систем, настроенных в соответствии с исходным образом RIPrep. Несовместимые с Windows 2000 приложения могут задавать и/или полагаться на пользовательские параметры, характерные не для всех пользователей системы, но для профиля конкретного пользователя, который устанавливает приложение перед запуском RIPrep (обычно это локальный администратор). Эти параметры так и остаются уникальными для профиля пользователя. В результате приложение или параметры становятся недоступными для пользователей компьютеров, установленных с образа RIPrep, или неправильно работают на них. Кроме того, некоторые изменения параметров, не связанные с приложениями, например рисунок рабочего стола пользователя, по умолчанию распространяются только на профиль текущего пользователя и не применяются к пользователям или системам, установленным с образа RIPrep.

Тщательно проверьте все приложения и конфигурационные параметры, которые вы собираетесь использовать в составе образа RIPrep, чтобы гарантировать их корректную работу при текущей схеме пользовательских профилей, принятой в вашей организации. Для проверки внесите какие-либо изменения, зарегистрировавшись как один из пользователей (например, как локальный администратор компьютера). Завершите сеанс работы и зарегистрируйтесь в системе по учетной записи другого сотрудника. Если сделанные вами изменения распространяются и на него, они будут также действительны и для пользователей, регистрирующихся в системах, настроенных с помощью включающего эти изменения образа RIPrep. Для завершения проверки создайте образ RIPrep, восстановите его

на другом компьютере и зарегистрируйтесь в качестве третьего сотрудника. Убедитесь, что все изменения корректно распространяются на систему.

Некоторые конфигурационные параметры копируются из профиля пользователя, на который они распространялись (в предыдущем примере это профиль локального администратора), непосредственно в профиль All Users. К таким параметрам относится, например, рисунок рабочего стола, некоторые параметры меню Start и ярлыки. Тем не менее все подобные коррективы необходимо тщательно протестировать и убедиться, что их функциональность не нарушается собственными параметрами пользователей.

Создание образа RIPrep

После настройки рабочей станции в соответствии с вашими требованиями можно создавать образ RIPrep.

▶ **Создание образа RIPrep**

1. На компьютере-клиенте в меню Start выберите команду Run (Выполнить). В поле Open введите UNC-путь к утилите RIPrep и щелкните OK. Например: *сервер**общий_ресурс*\RemoteInstall\Admin\I386\RIPREP.EXE
2. В первом окне мастера подготовки удаленной установки щелкните Next.
3. Продолжайте установку, отвечая на сообщения мастера Remote Installation Preparation. Вам будет предложено указать;
   - Server Name **(Имя сервера)** — имя сервера, на который будет скопирован дисковый образ. По умолчанию это сервер, где запущен мастер Remote Installation Preparation Wizard;
   - **Folder Name (Имя папки)** — имя папки на RIS-сервере, в которую будет скопирован образ установки;
   - **Friendly Description And Help Text (Понятное описание и текст справки)** — понятное описание и текст справки, отображаемые для данного образа мастером CIW.
4. Прежде чем продолжить, закройте на исходном компьютере все программы и службы. Просмотрите список выполняющихся программ и служб, закройте все запущенные в настоящий момент приложения и щелкните Next.
5. Просмотрите отчет о выбранных вами параметрах и щелкните Next.
6. Просмотрите сводку параметров и щелкните Finish, чтобы реплицировать образ установки исходного компьютера на RIS-сервер.

Примечание Если на исходном компьютере установлен жесткий диск объемом 1 Гб, а на конечной системе — жесткий диск емкостью 2 Гб, по умолчанию RIS отформатирует диск конечного компьютера как раздел объемом 2 Гб с той же файловой системой, которая использовалась на исходном компьютере при создании образа.

Получив ответы на базовые вопросы об образе, мастер приводит рабочую станцию в стандартное состояние, удаляя все уникальные параметры клиента — уникальный *идентификатор безопасности компьютера* (security identifier, SID), имя компьютера и уникальные параметры реестра. По окончании фазы подготовки образ автоматически реплицируется на указанный RIS-сервер. По окончании репликации он добавляется в список доступных параметров установки ОС, отображающихся мастером CIW. Теперь любой компьютер-клиент с поддержкой удаленной загрузки или компьютер, поддерживающий технологии удаленной загрузки на основе PXE, может установить созданный образ.

7. По завершении репликации образа исходный компьютер выключается. При перезагрузке компьютера автоматически запускается сокращенная программа установки. Завершите процесс установки, чтобы воспользоваться данным компьютером-клиентом для создания других образов установки.

Требования RIPrep

- Аппаратное обеспечение конечного компьютера (компьютера, который устанавливает образ, хранимый на RIS-сервере) не обязательно должно точно совпадать с аппаратным обеспечением исходного компьютера, использовавшегося для создания образа, Для выявления различий в оборудовании конечного и исходного компьютеров с Windows 2000 Professional в процессе установки образа мастер RIPrep использует технологию Plug and Play. Тем не менее драйверы *уровня абстрагирования оборудования* (hardware abstraction layer, HAL) должны совпадать для исходного и всех конечных компьютеров, которые будут устанавливать образ (например, оба драйвера должны либо поддерживать интерфейс ACPI, либо не поддерживать его). В большинстве случаев рабочим станциям не требуются уникальные драйверы HAL, необходимые серверам.
- Необходимо, чтобы емкость жесткого диска конечного компьютера равнялась или превышала емкость жесткого диска исходного компьютера.
- Все копии программного обеспечения корпорации Microsoft, изготовленные или установленные с помощью служб удаленной установки должны быть лицензированы. Это же касается и всех копий программного обеспечения, изготовленных или установленных с помощью служб удаленной установки. В обязанности получателя лицензии входит проверка лицензий на изготовление таких копий.

Ограничения RIPrep

- Мастер подготовки удаленной установки в настоящее время поддерживает репликацию одного диска или одного загрузочного раздела установки Windows 2000 Professional на отдельный сервер удаленной установки. Для этого необходимо, чтобы операционная система Windows 2000 Professional и все приложения, которые образуют стандартный образ установки, размещались на одном разделе исходного компьютера-клиента.
- Мастер позволяет репликацию исходного образа только на доступные серверы удаленной установки. В настоящее время репликация на альтернативные диски или другие типы носителя не поддерживается.
- Репликация шифрованных файлов не поддерживается.
- Изменения, внесенные в реестр исходного компьютера до запуска мастера подготовки удаленной установки, не сохраняются в образе установки.
- Изменения реплицированных образов установки не поддерживаются.

Источники образа установки

Если мастер подготовки удаленной установки используется для создания образа установки компьютера-клиента, который первоначально установлен с помощью розничной версии Windows 2000 Professional, файл ответов автоматической установки служб удаленной установки (riprep.sif) должен быть дополнен *регистрационным номером продукта* (product ID, PID). PID — уникальный идентификационный номер, присвоенный каждой копии Windows 2000. PID позволяет идентифицировать установку ОС и контролировать число копий, установленных в организации.

Примечание Если PID не указан в файле riprep.sif, установка будет остановлена и пользователю будет предложено ввести регистрационный номер во время установки этого образа RIPrep.

▶ **Добавление PID в файл RIPREP.SIF**

1. Откройте файл RIPREP.SIF (\RemoteInstall\Setup*соответствующий_язык*\Images\-*имя_соответствующего_образа*\I386\Templates\RIPREP.SIF).
2. В разделе [UserData] файла RIPREP.SIF наберите **ProductID = «xxxxx-xxx-xxxxxxx-xxxxx»** (включая все тире и кавычки). Здесь x — это PID розничной версии Windows 2000 Professional.

   Для каждого процесса установки клиента PID генерируется случайным образом на основе PID, указанного в файле RIPREP.SIF.

   Если на исходном компьютере была установлена OEM-версия Windows 2000 Professional, изменять PID в файле RIPREP.SIF не надо.

Создание загрузочного диска RIS

Загрузочный диск удаленной установки используется на компьютерах-клиентах, у которых нет ПЗУ удаленной загрузки, но на которых установлен поддерживаемый RIS сетевой адаптер. Процесс работы с диском загрузки напоминает процесс загрузки с использованием ПЗУ — вы включаете компьютер, загружаетесь с диска RIS и нажимаете клавишу F12 для загрузки сетевой службы, после чего на компьютер загружается и запускается мастер CIW. Далее процесс удаленной загрузки совпадает для всех вариантов независимо от того, загрузился ли клиент с диска RIS или с помощью загрузочного ПЗУ на основе PXE,

▶ **Создание загрузочного лиска RIS**

1. В меню Start выберите команду Run (Выполнить). В поле Open введите UNC-путь к утилите RBFG и щелкните OK. Например; *сервер\общий_ресурс*\RemoteInstall\Admin\I386\RBFG.EXE
2. Вставьте в дисковод отформатированную дискету.
3. В диалоговом окне Windows 2000 Remote Boot Disk Generator (Дискета удаленной загрузки для Windows 2000) щелкните подходящее имя дисковода (диск A или диск B) и затем — кнопку Create Disk (Создать диск) (рис. 15-11).

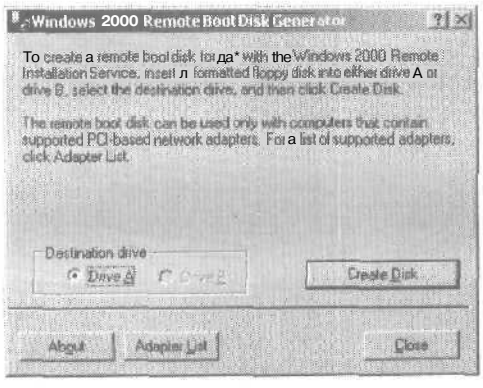


Рис. 15-11. Диалоговое окно Windows 2000 Remote Boot Disk Generator

4. Когда диск будет готов, щелкните кнопку Close (Закрыть) и достаньте дискету из дисковода.

Примечание Загрузочный диск можно использовать только на компьютерах с поддерживаемыми RIS типами сетевых PCI-адаптеров. Чтобы просмотреть список поддерживаемых адаптеров, щелкните в диалоговом окне Windows 2000 Remote Boot Disk Generator кнопку Adapter List (Список адаптеров).

Проверка конфигурации RIS

Службы удаленной установки позволяют проверять целостность RIS-серверов. При подозрении на отказ сервера, явном несогласованном поведении системы или при необходимости восстановить из резервной копии том RIS можно проверить конфигурацию RIS. В этом вам поможет мастер Check Server (Мастер проверки сервера).

▶ **Проверка конфигурации RIS**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers.
2. В дереве консоли щелкните папку, содержащую компьютер, конфигурацию которого необходимо изменить, например Computers или Domain Controllers.
3. В правой панели щелкните правой кнопкой соответствующий RIS-сервер и выберите в контекстном меню команду Properties.
4. В диалоговом окне свойств сервера на вкладке Remote Install щелкните кнопку Verify Server (Проверить сервер), чтобы запустить мастер Check Server (Мастер проверки сервера).
5. В первом окне мастера щелкните Next.
6. Просмотрите отчет в окне Remote Installation Services Verification Complete (Проверка служб удаленной установки завершена) и щелкните кнопку Finish (Готово).

Примечание Если вы проверяете конфигурацию сервера для восстановления тома RIS из архива, эту операцию следует выполнять перед восстановлением.

Резюме

Вы узнали о задачах по внедрению служб удаленной установки, в том числе об установке и настройке RIS, создании образа RIPrep, создании загрузочного диска RIS и проверке конфигурации RIS.

Занятие 3. Администрирование RIS

Здесь обсуждаются задачи по администрированию **RIS,** включая управление образами установки, компьютерами-клиентами RIS и безопасностью **RIS.**

Изучив материал этого занятия, вы сможете:

- ✓ **управлять образами установки** клиентов **RIS;**
- ✓ **управлять компьютерами-клиентами RIS;**
- ✓ **управлять безопасностью RIS.**

Продолжительность занятия — около 20 минут.

Администрирование RIS

Подразумевает управление:

- образами установки клиентов RIS;
- компьютерами-клиентами RIS;
- безопасностью RIS.

Управление образами установки клиентов RIS

Оно требует от администратора навыков:

- добавления новых образов установки ОС;
- привязки файлов **ответов автоматической установки.**

▶ **Добавление нового образа установки ОС**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Active Directory Users And Computers (Active Directory — пользователи и компьютеры).
2. В дереве консоли щелкните правой кнопкой мыши соответствующий RIS-сервер и выберите команду Properties.
3. В диалоговом окне свойств сервера перейдите на вкладку Remote Install (Удаленная установка) и щелкните кнопку Advanced Settings (Дополнительные параметры).
4. В окне свойств перейдите на вкладку Images (Образы).
5. Щелкните кнопку Add, чтобы запустить мастер добавления образа.
6. В окне New Answer File Or Installation Image (Новый файл ответов или образ установки) щелкните переключатель Add A New Installation Image (Добавить новый образ установки) и затем — Next, чтобы запустить мастер Add Installation Image (Мастер добавления образа установки).
7. В первом окне мастера щелкните Next.
8. В окне Installation Source Files Location (Местонахождение установочных файлов) введите путь к установочным файлам Windows 2000 Professional (на компакт-диске или на сетевом диске) и щелкните Next.
9. В окне Windows Installation Image Folder Name (Имя папки образа установки Windows) наберите имя образа установки Windows и щелкните Next.
10. В окне Friendly Description And Help Text (Понятное описание и текст справки) введите понятное описание и справочный текст для образа установки. Затем щелкните Next.
11. Если предыдущие окна мастера CIW отображались, откроется окно Previous Client Installation Screens Found (Найдены прежние экраны мастера установки клиентов).

Выберите набор экранов мастера CIW, который следует использовать для данного образа, и щелкните Next.

12. Просмотрите отчет на странице Review Settings (Просмотр параметров) и щелкните кнопку Finish (Готово).

Мастер Remote Installation Setup завершит добавление нового образа установки клиента.

▶ **Привязка файла ответов**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers.
2. В дереве консоли щелкните правой кнопкой мыши соответствующий RIS-сервер и выберите в контекстном меню команду Properties.
3. В диалоговом окне свойств сервера перейдите на вкладку Remote install и щелкните Advanced Settings.
4. В окне свойств перейдите на вкладку Images (Образы).
5. Щелкните кнопку Add, чтобы запустить мастер добавления образа.
6. В окне New Answer File Or Installation Image (Новый файл ответов или образ установки) щелкните переключатель Associate A New Answer File To An Existing Image (Сопоставить новый файл ответов существующему образу) и затем — Next.
7. В окне Unattended Setup Answer File Source (Источник файла ответов для автоматической установки) щелкните один из следующих переключателей, чтобы указать источник файла автоматической установки:
   - Windows Image Sample Files (Образцы файлов образа Windows);
   - Another Remote Installation Server (Другой сервер удаленной установки);
   - An Alternate Location (Иное место).
8. Щелкните Next.
9. В окне Select An Installation Image (Выбор образа установки) укажите дисковый образ, которому будет сопоставлен файл автоматической установки, и щелкните Next.
10. В окне Select A Sample Answer File (Выбор образца файла ответов) укажите образец файла ответов и щелкните Next.
11. В окне Friendly Description And Help Text (Понятное описание и текст справки) введите понятное описание и справочный текст для образа. Затем щелкните Next.
12. Просмотрите отчет в окне Review Settings (Просмотр параметров) и щелкните кнопку Finish (Готово).

Управление компьютерами-клиентами RIS

Оно подразумевает:

- предварительную настройку компьютеров-клиентов RIS;
- просмотр компьютеров-клиентов RIS.

Предварительная настройка компьютеров-клиентов RIS

Означает создание действительной *учетной записи компьютера-клиента* (client computer account object, CAO) в хранилище Active Directory. Это позволит настроить RIS-серверы для ответа исключительно на запросы предварительно подготовленных клиентских компьютеров. Таким образом, вы гарантируете, что установить ОС с RIS-сервера смогут лишь клиенты, предварительно настроенные в качестве авторизованных пользователей. Предварительная настройка экономит время и деньги, зачастую устраняя необходимость полной предварительной установки компьютера.

В процессе предварительной настройки компьютера-клиента можно задать индивидуальное имя компьютера и, при желании, указать RIS-сервер, обслуживающий данный компьютер. Эта информация используется для идентификации и маршрутизации компьютеров-клиентов при запросе на загрузку сетевой службы. Убедитесь, что пользователям предварительно настроенных компьютеров-клиентов назначены соответствующие разрешения доступа. При предварительной настройке клиентского компьютера в домене с несколькими контроллерами задержка репликации информации о клиентском CAO иногда приводит к тому, что компьютер-клиент начинает обслуживать другой RIS-сервер.

▶ **Предварительная настройка компьютера-клиента**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers.
2. В дереве консоли щелкните правой кнопкой мыши ОП, где будет располагаться новый клиентский компьютер, и выберите в контекстном меню команду New\Computer (Создать\Компьютер).
3. В диалоговом окне New Object — Computer (Новый объект — Компьютер) введите имя компьютера-клиента, назначьте права присоединения к домену для пользователя или группы, которая содержит пользователя, которому принадлежит представленный данной учетной записью компьютер. Затем щелкните Next.

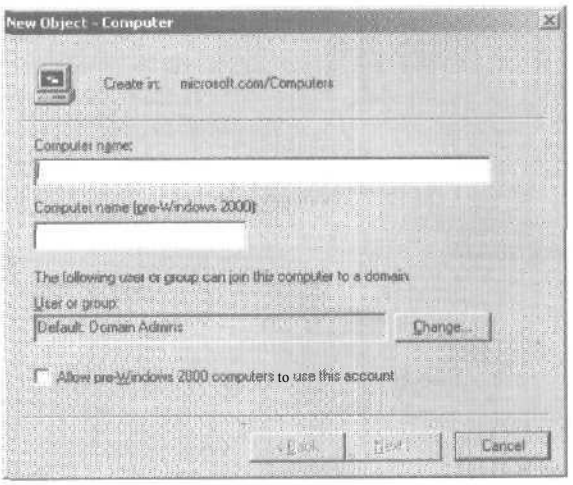


Рис. 15-12. Диалоговое окно New Object — Computer (Новый объект — Компьютер)

4. В диалоговом окне Managed (Управляемый) пометьте флажок This Is A Managed Computer (Это управляемый компьютер), введите GUID клиентского компьютера и щелкните Next (рис. 15-13). Подробности см. в разделе «Поиск GUTD для компьютеров-клиентов» этого занятия.
5. В диалоговом окне Host Server (рис. 15-14) щелкните один из следующих переключателей, чтобы указать сервер, обслуживающий данный клиентский компьютер:
   - **Any Available Remote Installation Server** — компьютер-клиент может обслуживаться любым RIS-сервером;
   - **The Following Remote Installation Server** — компьютер-клиент будет обслуживаться указанным вами RIS-сервером;

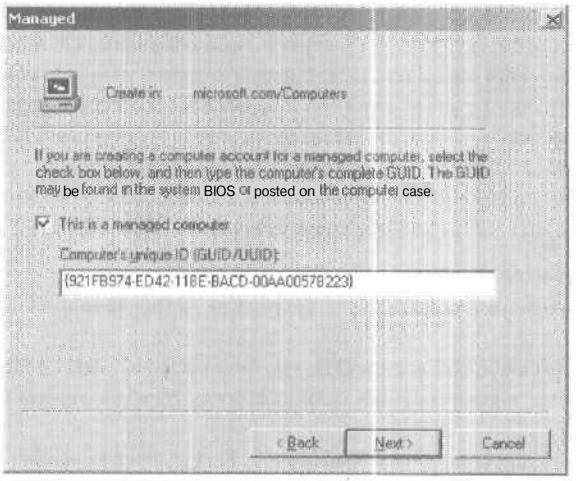


Рис. 15-13. Диалоговое окно Managed (Управляемый)

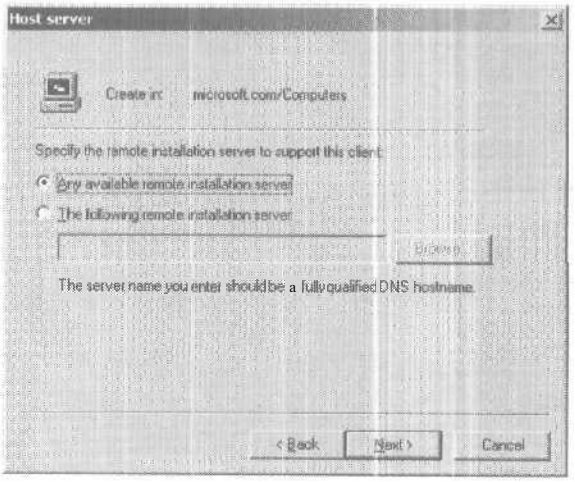


Рис. 15-14. Диалоговое окно Host Server

Параметры диалогового окна Host Server (Хост-сервер) позволяют вручную распределить клиентов между доступными в сети вашей организации RIS-серверами, а также, если вам известно физическое размещение каждого **RIS** сервера и место, куда будет установлен компьютер-клиент, сегментировать сетевой трафик. Например, если RIS-сервер расположен на пятом этаже здания и новые компьютеры также устанавливаются на пятом этаже, можно привязать их к RIS-серверу пятого этажа.

6. Щелкните Next.
7. Просмотрите сводные параметры в окне New Object — Computer и щелкните кнопку Finish (Готово).

Просмотр компьютеров-клиентов RIS

Для поиска учетных записей компьютеров-клиентов RIS в Active Directory можно указать имя или GUID компьютера. Функция Show Clients ищет все компьютеры-клиенты, предваритель-

но настроенные для данного RIS-сервера. Поиск можно задать во всем хранилище Active Directory или только в отдельном домене. Служба поиска возвращает список компьютеров-клиентов, отсортированный по имени или GUID.

Служба Show Clients допускает использование в имени RIS-сервера метасимволов. Например, если RIS-сервер называется RISsvr1, служба Show Clients выполнит поиск по имени сервера RISsvrl*. При поиске средствами службы Show Clients в среде с несколькими RIS-серверами результаты могут включать компьютеры-клиенты с нескольких серверов. Например, если у вас есть RIS-серверы с именами RISsvr1, RISsvr10, и RISsvr100, служба поиска возвратит для каждого сервера сведения о клиентских компьютерах, имя которых начинается с одинаковой комбинации символов.

Поиск GUID для компьютеров-клиентов

GUID компьютера:

- записан на наклейке на боковой стороне корпуса компьютера;
- записан на наклейке внутри корпуса компьютера;
- отображается в BIOS компьютера.

GUID компьютера указывает изготовитель в форме {*dddddddd-dddd-dddd-dddd-dddddddddddd*}, где *d* — шестнадцатеричная цифра. Например: 8 шестнадцатеричных цифр, затем 4, еще 4, еще 4, затем 12 цифр, как в этом примере: {921FB974-ED42-11BE-BACD-00AA0057B223}

GUID компьютера-клиента может содержать следующие шестнадцатеричные цифры и символы:

0 1 2 3 4 5 6 7 8 9 a b c d e f - A B C D E F

Тире не обязательны, пробелы игнорируются. GUID необходимо заключить в фигурные скобки {}.

▶ Поиск компьютера-клиента RIS

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers.
2. В дереве консоли щелкните правой кнопкой мыши требуемый RIS-сервер и выберите команду Properties.
3. В диалоговом окне свойств сервера перейдите на вкладку Remote Install.
4. На вкладке Remote Install щелкните кнопку Show Clients (Просмотр клиентов).
5. В поле GUID (Код GUID) диалогового окна Find Remote Installation Clients (рис. 15-15) введите GUID компьютера и щелкните Find Now (Найти).

Примечание Чтобы ограничить область поиска компьютера-клиента конкретным RIS-сервером, укажите имя этого сервера в поле RI server (Сервер удаленной установки).

6. В нижней части диалогового окна Find Remote Installation Clients отобразится список компьютеров-клиентов RIS, содержащий колонки Name и GUID.
7. Закройте диалоговое окно Find Remote Installation Clients.
8. Закройте диалоговое окно свойств сервера.

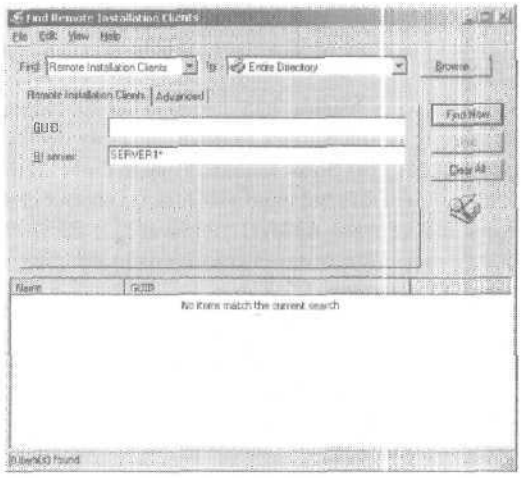


Рис. 15-15. Диалоговое окно Find Remote Installation Clients (Поиск; Клиенты удаленной установки)

Управление безопасностью RIS

Оно подразумевает:

- определение разрешений доступа для создания учетных записей предварительно настроенных компьютеров, а также учетных записей компьютеров, настроенных пользователем;
- определение разрешений для присоединения компьютеров, созданных в контейнере Computers и в ОП, к домену.

Определение разрешений доступа для создания учетных записей компьютеров

Для создания учетных записей компьютеров в Active Directory пользователи должны обладать соответствующими разрешениями и правами доступа. Вам необходимо определить пользователей, которым позволено создавать новые учетные записи компьютеров, и соответствующим образом изменить их разрешения и права доступа.

▶ **Определение разрешений доступа для создания учетных записей предварительно настроенных компьютеров**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers.
2. В меню View выберите команды Users, Groups And Computers As Containers (Пользователи, группы и компьютеры как контейнеры) и Advanced Features (Дополнительные функции).
3. В дереве консоли щелкните правой кнопкой мыши соответствующую учетную запись компьютера и выберите команду Properties.
4. В окне свойств перейдите на вкладку Security (Безопасность) и щелкните кнопку Add (Добавить).
5. В окне Select Users, Computers, Or Groups (Выбор: Пользователи, Компьютеры или Группы) выберите из списка пользователя или группу, щелкните кнопку Add и затем — OK.
6. В окне свойств выберите добавленного пользователя или группу.

7. В окне Permissions пометьте разрешения Read (Чтение), Write (Запись), Change Password (Смена пароля) и Reset Password (Сброс пароля) и затем щелкните OK.

   Если эти разрешения вы назначаете группе, не забудьте объединить в нее пользователей.

   Для учетных записей компьютеров-клиентов, предварительно настроенных в другой папке Active Directory, откройте консоль Active Directory Users and Computer и выберите соответствующую учетную запись компьютера.

► **Определение разрешений доступа для создания учетных записей компьютеров, настраиваемых пользователем**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers.
2. В дереве консоли щелкните правой кнопкой мыши соответствующий домен и выберите команду Delegate Control (Делегирование управления), чтобы запустить мастер Delegation Of Control (Мастер делегирования управления).
3. В первом окне мастера щелкните Next.
4. В окне Users Or Groups (Пользователи или группы) щелкните кнопку Add.
5. В диалоговом окне Select Users, Computers, Or Groups выберите учетную запись пользователя или группы (рекомендуется), куда входят пользователи, для которых настраиваются разрешения. Затем щелкните кнопки Add и OK.
6. В окне Users Or Groups щелкните Next.
7. В окне Tasks To Delegate (Делегируемые задачи) выберите Delegate The Following Common Tasks (Делегировать следующие обычные задачи), щелкните Join A Computer To The Domain (Присоединение компьютера к домену) и затем — Next,
8. Изучите параметры и щелкните кнопку Finish (Готово).

Определение разрешений для присоединения компьютеров к домену

Для добавления новых учетных записей компьютеров в домен пользователи должны обладать определенными правами и разрешениями. Вам необходимо определить пользователей, которые будут добавлять в домен новые учетные записи компьютеров, и соответствующим образом изменить разрешения и права доступа этих пользователей.

► **Определение разрешений для присоединения объектов компьютеров, созданных в контейнере Computers, к домену**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers.
2. В дереве консоли щелкните правой кнопкой мыши соответствующий домен и выберите в контекстном меню команду Delegate Control, чтобы запустить мастер Delegation Of Control.
3. В первом окне мастера щелкните Next.
4. В окне Users Or Groups щелкните кнопку Add.
5. В диалоговом окне Select Users, Computers, Or Groups выберите учетную запись пользователя или группу (рекомендуется), включающую пользователей, которые будут добавлять компьютеры в домен. Затем щелкните кнопки Add и OK.
6. В окне Users Or Groups щелкните Next.
7. В окне Tasks To Delegate выберите Delegate The Following Common Tasks, затем — Join A Computer To The Domain и щелкните Next.
8. Просмотрите отчет и щелкните Finish.

Определение разрешений для присоединения объектов компьютеров, созданных в ОП, к домену

1. Раскройте меню Start\Programs\Administrative Tools и щелкните Active Directory Users And Computers.
2. В дереве консоли щелкните правой кнопкой мыши соответствующее ОП и выберите команду Properties.
3. В диалоговом окне свойств ОП, на вкладке Group Policy выберите в поле Group Policy Object Links (Ссылки на объекты групповой политики) требуемый ОГП и щелкните кнопку Edit.
4. В оснастке Group Policy (Групповая политика) раскройте узел Computer Configuration \Windows Settings\Security Settings\Local Policies (Конфигурация компьютера\Конфигурация Windows\ Параметры безопасности\Локальные политики) и затем щелкните User Rights Assignment (Назначение прав пользователя).
5. Дважды щелкните Add Workstations To Domain.
6. В диалоговом окне Security Policy Setting (Параметр политики безопасности) щелкните кнопку Add.
7. В поле User And Group Names (Имена пользователей и групп) диалогового окна Add User Or Group (Добавление пользователя или группы) введите имена учетных записей или групп безопасности (рекомендуется), включающих пользователей, правомочных добавлять компьютеры в домен. Затем щелкните OK.
8. В диалоговом окне Security Policy Setting щелкните OK.
9. Закройте оснастку Group Policy.
10. В диалоговом окне свойств ОП щелкните OK.

Изменения политики RIS вступают в силу только после того, как политика будет передана (распространена) на ваш компьютер. Поэтому для получения обновленной политики вам необходимо предпринять одно из следующих действий: наберите в командной строке secedit /refreshpolicy **user_policy** и нажмите клавишу Enter; перезагрузите компьютер; дождитесь автоматического применения политики — оно выполняется через определенные интервалы времени, которые вы можете определить сами. По умолчанию применение политики происходит каждые 8 часов.

Резюме

Здесь описаны задачи по администрированию RIS, включая управление образами установки, компьютерами-клиентами RIS и безопасностью RIS.

Занятие 4. Ответы на часто задаваемые вопросы о службах RIS и устранение неполадок RIS

Здесь приведены ответы на часто задаваемые вопросы о службах удаленной установки, а также обсуждаются некоторые проблемы и методы их устранения.

Изучив материал этого занятия, Вы сможете:

- ✓ устранять неполадки RIS.

Продолжительность занятия — около 15 минут.

Ответы на часто задаваемые вопросы о RIS

Вопрос 1. Нет уверенности в правильности версии ПЗУ PXE.

Ответ. При запуске компьютера Net PC или компьютера-клиента, имеющего ПЗУ удаленной загрузки, версия ПЗУ PXE отображается на экране. Службы удаленной установки поддерживают версии ПЗУ PXE .99c и последующие всегда, за исключением некоторых ситуаций, требующих только .99L. Если возникают сложности при работе с установленной на компьютере-клиенте версией ПЗУ, обратитесь к изготовителю компьютера за более новой версией программы для ПЗУ PXE.

Вопрос 2. Нет уверенности в том, что компьютер-клиент получил IP-адрес и установил связь с сервером служб удаленной установки.

Ответ. При загрузке компьютера-клиента можно увидеть начало загрузки и инициализацию ПЗУ загрузки PXE. Для большинства компьютеров PC9S и Net PC, компьютеров с ПЗУ PXE и компьютеров, использующих загрузочный диск служб удаленной установки, выполняется описанная ниже последовательность действий.

▶ **Последовательность загрузки ПЗУ удаленной загрузки**

Действие 1. На компьютере-клиенте выводится сообщение «DHCP», которое показывает, что клиент запрашивает IP-адрес у DHCP-сервера. Это также может означать, что клиент получил IP-адрес от службы DHCP и ожидает ответа от сервера удаленной установки. Чтобы удостовериться, что клиент получает IP-адрес, проверьте арендованные IP-адреса, предоставленные DHCP-сервером.

Устранение неполадок. Если клиент не получил сообщения, IP-адрес не может быть получен или сервер BINL не отвечает. Постарайтесь получить ответы на следующие вопросы.

- Доступен ли DHCP-сервер и запущена ли служба? Серверы DHCP и удаленной установки должны быть авторизованы в Active Directory, чтобы иметь возможность запускать свои службы. Убедитесь, что служба запущена и что другие клиенты, для которых не разрешена удаленная загрузка, получают IP-адреса в этом сегменте.
- Определена ли область IP-адресов для DHCP-сервера и активизирована ли она?
- Не расположен ли между клиентом и DHCP-сервером маршрутизатор, который не пропускает DHCP-пакеты?
- Нет ли в журнале событий сообщений об ошибках, связанных со службой DHCP?
- Могут ли другие компьютеры-клиенты, для которых не разрешена удаленная загрузка, получать IP-адреса в этом сегменте сети?

Действие 2. Когда клиент получает IP-адрес от DHCP-сервера, сообщение может измениться на «BINL», Это свидетельство того, что клиент успешно арендовал IP-адрес и теперь ожидает подключения к серверу удаленной установки. Клиент в конечном счете ожидает определенное время и отправляет сообщение об ошибке «No Bootfile received from DHCP, BINL, or Bootp» (Файл загрузки не получен от DHCP, BINL или Bootp).

Устранение неполадок. Если клиент не получил сообщения службы BINL, значит, клиент не получил ответа от сервера удаленной установки. Постарайтесь получить ответы на следующие вопросы.

- Доступен ли сервер удаленной установки и запушены ли службы удаленной установки? Серверы удаленной установки должны быть авторизованы, чтобы они могли запускать свои службы. Используйте оснастку «DHCP» для авторизации DHCP-серверов и серверов удаленной установки в Active Directory.
- Получают ли другие клиенты, имеющие возможность удаленной загрузки, сведения от мастера установки клиентов? Если получают, то этот компьютер-клиент или не поддерживается, или у него возникли неполадки, связанные с ПЗУ удаленной загрузки. Проверьте версию ПЗУ PXE на компьютере-клиенте. Также проверьте в Active Directory, не настроил ли администратор предварительно этот компьютер-клиент на сервер удаленной установки, который отключен или недоступен компьютеру-клиенту.
- Не расположен ли между клиентом и сервером удаленной установки маршрутизатор, который не пропускает запросы и ответы службы DHCP? Сервер RIS на начальном этапе согласования взаимодействует с клиентом путем передачи пакетов DHCP При необходимости настройте маршрутизатор для перенаправления пакетов DHCP.
- Нет ли в журнале событий системы или приложений сообщений об ошибках, связанных со службами удаленной установки (BINLSVC), DNS или Active Directory?

Действие 3. Затем клиент переключается на TFTP или предлагает пользователю нажать клавишу F12. Это означает, что клиент подключился к серверу служб удаленной установки и ожидает получения первого файла образа. На некоторых компьютерах сообщения BINL и TFTP не выводятся, поскольку последовательность выполняется очень быстро.

Устранение неполадок. Если компьютер-клиент не получил ответ от сервера удаленной установки, клиент ожидает определенное время и отправляет сообщение об ошибке о том, что им не получен файл от DHCP, BINL или TFTP. Если сервер RIS не ответил компьютеру-клиенту, выполните следующие действия.

1. Остановите и перезапустите службу BINLSVC, раскрыв меню Start (Пуск) и выбрав команду Run (Выполнить).
2. В диалоговом окне Run (Запуск программы) введите в текстовое поле Net Stop BINLSVC Net Start BINLSVC и щелкните OK.
3. Проверьте свойства сервера RIS и убедитесь, что флажок Respond To Client Computers Requesting Service (Отвечать клиентским компьютерам, запрашивающим обслуживание) помечен, а флажок Do Not Respond To Unknown Client Computers (Не отвечать неизвестным клиентам) снят, если только компьютер-клиент не был предварительно настроен в Active Directory.
4. Проверьте в журнале событий наличие сообщений об ошибках, относящихся к DHCP, DNS, BINLSVC или Active Directory.

Действие 4. На компьютер-клиент надо загрузить мастер установки клиентов, далее появляется экран с приветствием пользователя.

Вопрос 3. Является ли безопасной часть программы ПЗУ PXE удаленной загрузки, выполняющаяся до загрузки?

Ответ. Нет. Все операции, необходимые для загрузки через ПЗУ и установки ОС или процесса репликации, не являются безопасными с точки зрения шифрования типа пакета, нарушения подлинности клиента/сервера или механизмов прослушивания сети, использующих средства анализа пакетов. Поэтому следует с осторожностью применять службы удаленной установки в корпоративной сети. Убедитесь, что в сети разрешены только авторизованные серверы RIS и контролируется число администраторов, которым разрешено устанавливать или настраивать серверы RIS.

Вопрос 4. Сохраняют ли службы удаленной установки атрибуты файлов и параметры безопасности, заданные для исходного компьютера при использовании образа в формате RIPrep?

Ответ. Да. Атрибуты файлов и параметры безопасности, определенные для исходного компьютера, сохраняются на конечном компьютере, на который устанавливается образ. Однако RIPrep не поддерживает шифрованную файловую систему, включенную и использованную на исходном компьютере-клиенте.

Вопрос 5. Как реплицировать образы установки ОС, расположенные в настоящее время на сервере RIS, на другие серверы RIS в сети для согласования параметров ОС на всех компьютерах-клиентах?

Ответ. В настоящее время службы удаленной установки не обеспечивают механизм репликации образов ОС с одного сервера RIS на другой, но известны способы, которые позволяют решить эту задачу, Используйте мощные возможности репликации в Systems Management Server. Этот продукт обеспечивает планируемую репликацию, сжатие и возможность работы по медленным подключениям. Для репликации образа ОС также применяют решения других поставщиков программного обеспечения. Удостоверьтесь, что выбранный механизм репликации сохраняет атрибуты файлов и параметры безопасности исходных образов.

Вопрос 6. Можно ли установить в сети одновременно сервер RIS и сервер удаленной загрузки от другого поставщика программного обеспечения? Если да, то каковы последствия?

Ответ. Да, в одной физической сети могут находиться серверы удаленной загрузки или установки от различных поставщиков. Важно понимать, что программа ПЗУ удаленной загрузки PXE не делает различий между серверами удаленной загрузки или установки. Поэтому, когда компьютер-клиент, для которого разрешена удаленная загрузка, запускается и запрашивает IP-адрес сервера удаленной загрузки или установки, клиенту ответят все доступные серверы. Таким образом, клиент не может убедиться в том, что он обслуживается конкретным сервером.

Службы удаленной установки позволяют администратору предварительно настроить компьютеры-клиенты в Active Directory и указать сервер RIS, предназначенный для обслуживания компьютера-клиента. Настроив сервер RIS на ответ только известным компьютерам-клиентам (предварительно настроенным), администратор гарантирует, что клиента будет обслуживать требуемый сервер RIS.

Не во всех серверах удаленной загрузки или установки реализована возможность игнорирования запросов обслуживания. Иногда требуется изолировать в сети серверы определенных изготовителей, чтобы клиенты не получали ответы от этих серверов.

Вопрос 7. Можно ли добавить сетевые адаптеры на загрузочный диск служб удаленной установки?

Ответ. Нет. **В** текущей версии служб удаленной установки служебную программу Rbfg.exe нельзя изменить для учета новых поддерживаемых сетевых адаптеров. Корпорация Microsoft предполагает в недалеком будущем добавлять сведения о новых поддержи-

ваемых RIS сетевых адаптерах и предлагать обновленную программу Rbfg.exe через обычные каналы распространения, например Интернет, или включить ее в обновления Windows.
Вопрос 8. Можно ли использовать атрибуты объекта Active Directory при создании формата имени для автоматического присвоения имен компьютерам в ходе удаленной установки?

Ответ. Нет. В настоящий момент существующие атрибуты, поддерживаемые автоматическим присвоением имен, используют Active Directory. Однако сейчас поддерживаются не все атрибуты объектов Active Directory.

Устранение неполадок RIS

Ниже описаны некоторые проблемы, возникающие при использовании служб удаленной установки, а также возможные способы их устранения.

Табл. 15-3. Устранение неполадок RIS

Симптом: Параметры команд не обрабатываются при автоматической установке

Причина	Решение
При использовании параметра «OemPreinstall = yes» в файле .sif требуются правильные сведения о каталогах	Измените параметры каталога на \\RemoteInstall\Setup*требуемый_язык*\Images*соответствующее_имя*\oem

Возможности выбора языка не отображаются во время сеанса работы мастера установки клиентов

Причина	Решение
По умолчанию службы удаленной установки для управления выбором клиентом образа установкл используют файл Welcome.osc. Для выбора образов установки с несколькими языками необходимо заменить файл по умолчанию Welcome.osc на файл Multilng.osc	Для управления возможностью выбора образа, устанавливаемого клиентом, мастер CIW использует файл Welcome.osc, расположенный в папке \RemoteInstall\OSChooser. Когда удаляется файл Welcome.osc file и файл Multilng.osc переименовывается в Welcome.osc, мастер установки клиентов предлагает пользователю нескольких языков на иыбор. Файл Welcome.osc разрешается редактировать для создания особых параметров языка

Компьютер-клиент настроен на сервер RIS, но его обслуживает другой сервер

Причина	Решение
Когда компьютер-клиент предварительно настраивается в домене с несколькими контроллерами домена, из-за задержки репликации сведений САО к обслуживанию клиента может приступить другой сервер RIS	Можно подождать, пока сведения об учетной записи клиента не будут переданы в течение следующего сеанса репликации или изменить частоту репликации между контроллерами домена

Табл. 15-3. Устранение неполадок RIS *(окончание)*

После восстановления тома служб удаленной установки из резервной копии эти службы работают неправильно

Причина	Решение
Программа архивирования восстановила том без каталога хранилища единственных копий (SIS)	Проверьте настройку тома служб удаленной установки и снова восстановите том

Резюме

Вы ознакомились с наиболее распространенными вопросами о RIS и ответами на них. Вы также узнали о некоторых проблемах, возникающих при использовании служб удаленной установки, а также о возможных способах их устранения.

Закрепление материала

Приведенные ниже вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении А «Вопросы и ответы* в конце книги.

1. Что такое службы удаленной установки? Какие типы удаленной загрузки поддерживает **RIS?**

2. Что обеспечивает технология удаленной загрузки PXE?

3. Что такое загрузочный диск служб удаленной установки?

4. Что такое образ RIPrep?

5. Что представляет собой мастер установки клиентов?

Приложение А

Вопросы и ответы

Глава 1 Знакомство с Microsoft Windows 2000

стр. 32

Закрепление материала

1. Каково основное различие между Windows 2000 Professional и Windows 2000 Server?

   Windows 2000 Professional предназначена главным образом для использования в качестве самостоятельной рабочей станции (компьютера в одноранговой сети) либо **как рабочей станции в иомене Windows 2000** Server. **Windows 2000 Server предназначена для использования в качестве** сервера **файлов, печати и приложений, а также как платформа для Web-сервера.**

2. В чем состоит главное различие между рабочей группой и доменом?

   Основное различие между рабочей группой и доменом заключается в том, **где** располагается информация об **учетной записи** пользователя для входа. В рабочей группе **информация** об учетной **записи пользователя располагается** в локальной **защищенной базе данных на каждом компьютере рабочей группы. В домене информация об учетной записи хранится в базе данных Active** Directory.

3. Какие из встроенных подсистем отвечают за работу Active Directory?

   Подсистема безопасности.

4. Каково назначение Active Directory?

   Active Directory — это служба каталогов, поставляемая с Windows 2000 Server. **Active Directory хранит** информацию **об объектах сети и предоставляет эту информацию пользователям** и **системным администраторам. Active Directory позволяет пользователям** сети обращаться **к общим** ресурсам, **единожды введя имя и** пароль. **Active Directory представляет** сеть в интуитивно понятном **иерархическом виде и позволяет централизованно управлять всеми объектами сети.**

5. Что происходит при входе пользователя в домен?

   Windows 2000 **посылает учетную информацию контроллеру домена, который сравнивает** ее с **информацией пользователя в каталоге. Если данные** совпадают, **контроллер домена аутентифицирует пользователя и** отправляет **ему маркер доступа.**

6. Как пользоваться диалоговым окном Windows Security (Безопасность Windows)?

   Диалоговое окно Windows Security предоставляет простой доступ **к важным параметрам безопасности,** в том **числе к возможности заблокировать** компьютер, **сменить** пароль, **остановить программы, не отвечающие на системные запросы, завершить рабочий сеанс** либо **выключить компьютер. В** этом **окне вы** также **можете указать домен и учетную информацию для подключения** к нему.

Глава 2 Введение в Active Directory

стр. 52

Закрепление материала

1. Что такое схема Active Directory?

   Схема содержит формальное описание содержания и структуры Active Directory, в том числе все атрибуты, классы и свойства классов.

2. Каково назначение организационного подразделения (ОП)?

   ОП — это контейнер, используемый для организации объектов в домене в логические административные группы, которые отражают функциональную или бизнес-структуру вашей организации. ОП может содержать такие объекты, как учетные записи пользователей, контакты, группы, компьютеры, принтеры, приложения, общие файлы и другие ОП того же домена.

3. Что такое сайты и домены и чем они отличаются?

   Сайт — это комбинация одной или более IP-подсетей, которые должны быть соединены высокоскоростным каналом связи. Домен — это логическое объединение серверов и других сетевых ресурсов, собранных под одним именем. Сайт — это компонент физической структуры Active Directory, тогда как домен — компонент логической структуры.

4. Чем отличаются неявные двусторонние транзитивные доверительные отношения и явные односторонние нетранзитивные отношения?

   Неявное двустороннее доверие — это доверительное отношение между доменами, которые являются частью масштабируемого пространства имен Windows 2000, например между родительским и дочерним доменами в пределах дерева либо между доменами верхнего уровня в лесу. Такие доверительные отношения делают все объекты во всех доменах доступными для всех других доменов в дереве.

   Явное одностороннее доверие — это отношение между доменами, которые не являются частями одного дерева. Односторонние доверительные отношения поддерживают подключения к существующим не-Windows 2000 доменам для настройки доверительных отношений с доменами в других деревьях,

Глава 3 Задачи и средства администрирования Active Directory

Занятие 3. Консоли управления

стр. 67

▶ Задание: задействуйте стандартную консоль MMC

2. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Event Viewer (Просмотр событий).

   Откроется консоль управления Event Viewer, отображающая содержимое журналов событий. Event Viewer применяется для контроля работы различного программного обеспечения и аппаратных средств.

   Какие три журнала перечислены в дереве консоли?

   Журнал приложений, Журнал безопасности, Журнал системы.

   Можете ли вы добавить оснастки в консоль?

   Нет. Это стандартная консоль, она сохранена в пользовательском режиме. Консоли, сохраненные в пользовательском режиме, изменять нельзя.

стр. 68

▶ Задание 1: создайте пользовательскую консоль MMC

5. Для просмотра текущей конфигурации консоли в меню Console (Консоль) выберите команду Options (Параметры).

Откроется окно **Options** (Параметры) с вкладкой Console (Консоль), где можно задать режим **консоли.**

Чем отличается консоль, сохраненная в пользовательском режиме, от консоли, сохраненной Б авторском режиме?

Вы можете изменять консоли, которые сохранены в авторском, но не пользовательском режиме. Разные уровни пользовательского режима по-своему ограничивают возможности пользователей модифицировать консоль.

стр. 70

▶ Задание 5: удалите расширения из оснастки

12. Щелкните Computer Management (Local) и перейдите на вкладку Extensions (Расширения).

Появится список расширений для оснастки Computer Management.

Какой фактор определяет набор расширений, перечисленных в этом окне?

Доступные расширения зависят от оснастки, которую вы выбрали.

15. Раскройте узлы Computer Management (Управление компьютером) и System Tools (Служебные программы), чтобы убедиться, что расширения System Information и Device Manager удалены.

Когда нужно удалять расширения из консоли?

При настройке консоли для решения узких задач администрирования. Это позволит вам включать только те расширения, которые относятся к администрируемому вами компьютеру. Следует также удалить расширения из консолей, предназначенных администраторам, *отвечающим* за *ограниченный* участок работы.

стр. 76

Закрепление материала

1. Какие функции выполняют консоли управления Active Directory Domains and Trusts, Active Directory Sites and Services и Active Directory Users and Computers?

Консоль Active Directory Domains and Trusts управляет доверительными отношениями между доменами. Консоль Active Directory Sites and Services создает сайты для управления репликацией информации Active Directory. Консоль Active Directory Users and Computers управляет пользователями, компьютерами, группами безопасности и другими объектами Active Directory.

2. Для чего создаются пользовательские консоли управления MMC?

Собственные консоли создаются для решения специализированных административных задач. Например, вы можете для удобства объединить оснастки, которые вы наиболее часто используете, в одну консоль. Вам не придется переключаться между несколькими программами или окнами MMC, поскольку все оснастки, которые вам нужны, будут «под рукой».

3. Когда и почему целесообразно использовать расширение?

Когда в конкретную оснастку надо добавить дополнительные *функции*. Расширения — это оснастки, которые предоставляют дополнительные административные функции для другой оснастки. Изолированная оснастка предоставляет одну функцию или связанный набор функций.

4. Вам необходимо создать пользовательскую консоль для администратора, которому требуются **лишь** консоли Computer **Management** и Active **Directory** Users and Computers. Причем администратор:

   - не должен иметь возможность добавлять какие-либо дополнительные консоли или оснастки;
   - должен иметь полный доступ к обеим **консолям;**
   - должен иметь возможность управлять **обеими** консолями.

Какой режим консоли следует использовать для конфигурирования данной пользовательской консоли?

Пользовательский режим, полный доступ.

5. Что необходимо **сделать** для удаленного **администрирования** компьютера с Windows 2000 Server с компьютера, на котором установлена Windows 2000 Professional?

Windows 2000 **Professional не содержит все оснастки, которые поставляются вместе с Windows 2000** Server. **Для решения задачи нужно добавить требуемые оснастки в** Windows **2000 Professional, запустив файл** *systemroot*\system32\adminpak.msi, **находящийся на Windows 2000 Server, из окна My Network** Places с **рабочего стола** Windows 2000 **Professional.**

6. Вам необходимо автоматически запускать служебную программу на компьютере с Windows 2000 Server один раз в неделю. Как это сделать?

   Следует настроить расписание выполнения служебной программы средствами Task Scheduler.

Глава 4 Внедрение Active Directory

Занятие 2. Установка Active Directory

стр. 93

► Задание 1: установите службу Active Directory на изолированный сервер

11. Убедитесь, что для размещения SYSVOL указан путь *systemroot*\ SYSVOL (если Windows 2000 установлена не в каталоге WINNT, общий системный том будет находиться в подпапке SYSVOL папки, где установлена Windows 2000).

    Каково требование к размещению SYSVOL?

    Sysvol должен находиться на разделе Windows **2000, отформатированном под NTFS** 5.0.

    Каковоназначение SYSVOL?

    Sysvol — **это системный том на контроллере домена** Windows **2000. Он хранит сценарии и часть объектов групповой политики текущего домена и предприятия в целом. В папке** *systemroot*\SYSVOL\SYSVOL **хранятся общедоступные файлы домена.**

стр. 94

► Задание 2: просмотрите домен из окна My Network Places

3. Дважды щелкните значок My Network Places (Мое сетевое окружение).

   Откроется одноименное окно.

   Какие параметры отображаются?

   Add Network Place (Новое место в сетевом окружении) и Entire Network (Вся сеть),

4. Дважды щелкните значок Entire Network (Вся сеть), затем дважды щелкните значок Microsoft Windows Network (сеть Microsoft Windows).

   Что вы видите?

   Ответ зависит от имени вашего домена (в предыдущем упражнении мы назвали его microsoft).

стр. 94

► Задание 3: просмотрите домен с помощью Active Directory Users And Computers

2. В дереве консоли дважды щелкните microsoft.com (или имя вашего домена).

   Что содержит узел microsoft?

   Папки Builtin, Computers, Domain Controllers и Users.

Занятие 4. Внедрение структуры ОП

стр. 105

► Задание: создайте ОП

3. Раскройте домен microsoft.com (или заданный вами домен).

ОП отображаются в списке домена в виде папок со значком книги каталога. Папки без значков — это специализированные контейнеры.

Какие ОП заданы в вашем домене по умолчанию?

Domain Controllers. Папки Builtin, Computers и Users — это объекты-контейнеры.

стр. 107

Закрепление материала

1. Каковы причины создания нескольких доменов?

   Вот некоторые из причин: распределенное администрирование сети, управление репликацией, разные требования к паролям в разных организациях, большое число объектов, разные имена доменов Интернета, региональные требования и требования внутренней политики.

2. Для вашей организации внешнее пространство имен Интернета зарезервировано регистрационной организацией DNS. При планировании внедрения Active Directory вы рекомендуете расширить это пространство имен для внутренней сети. Какие это дает преимущества?

   Расширение существующего пространства имен обеспечивает согласованность имен в рамках дерева для внутренних и внешних ресурсов. Кроме того, этот план позволяет вашей организации использовать одинаковые имена входа и имена учетных записей для внутренних и внешних ресурсов. Наконец, вам не придется резервировать дополнительное пространство имен DNS.

3. Как настройка сайтов отражается на работе Windows 2000?

   Вход и идентификация на рабочей станции. Когда пользователь входит в систему, Windows 2000 **пытается найти контроллер домена в том же сайте, что и компьютер пользователя, для обеспечения запроса пользователя на вход и последующих запросов сетевой информации.**

   Репликация каталога. Вы можете настроить расписание и путь для репликации каталога домена по-разному для репликаций внутри сайта и вне него. Как правило, следует выполнять репликацию между сайтами реже, чем внутри сайта.

4. Что такое общий системный том, каково его назначение, где он расположен и как называется?

   Общий системный том — это дерево каталогов, существующее на всех контроллерах доменов Windows 2000. Он хранит сценарии и некоторые объекты групповой политики для текущего домена и предприятия в целом. Стандартное местоположение и имя общего системного тома — *systemroot*\Sysvol. **Общий системный том может располагаться только на томе, отформатированном под NTFS 5.0.**

5. Каково назначение ролей хозяина операций?

   Поскольку непрактично вносить в каталог некоторые изменения из нескольких точек, один или несколько контроллеров домена могут быть назначены для выполнения операций, которые требуют централизованного выполнения (одного хозяина). Для выполнения операций с одним хозяином контроллерам доменов назначаются соответствующие роли хозяина операций.

6. Какое средство применяется для создания ОП?

   Для создания ОП служит консоль Active Directory Users and Computers.

Глава 5 Взаимодействие DNS и Active Directory

Занятие 2. Зоны

стр. 122

▶ Задание 4: добавьте запись ресурса

2. Щелкните имя ранее созданной тестовой зоны.

   Какие записи ресурсов уже существуют в зоне?

Start of Authority и Name Server.

стр. 132

Закрепление материала

1. С какой целью применяются запросы прямого поиска? Запросы обратного поиска?

   Запрос прямого поиска преобразует имя к IP-адрес. Запрос обратного поиска преобразует IP-адрес в имя.

2. Каковы преимущества использования зоны, встроенной в Active Directory?

   Возможность выполнять обновления с несколькими хозяевами и высокая безопасность, Зоны реплицируются и синхронизируются с новыми контроллерами домена автоматически, как только новая зона добавляется в домен Active Directory. Вы можете упростить планирование и администрирование DNS и Active Directory путем интегрирования хранилища вашего пространства имен DNS в Active Directory. Репликация каталогов работает быстрее и эффективнее, чем стандартная репликация DNS.

3. Для чего нужна запись ресурса SOA?

   Запись ресурса SOA указывает полномочный сервер имен в данном домене. Первой записью в базе данных зоны должна быть запись SOA. Эта запись также хранит такие свойства, как информацию о версии и временные интервалы обновления и устаревания базы данных зоны. Эти свойства регулируют частоту зонных передач между полномочными серверами зоны.

4. Что нужно сделать для делегирования ноны?

   Когда вы делегируете зону в рамках пространства имен, вы должны создать запись SOA, ссылающуюся на полномочный DNS-сервер новой зоны, и обеспечить корректность ссылок на другие DNS-серверы, полномочные для данной зоны.

5. Почему добавочная зонная передача эффективнее полной?

   Запрос IFXR позволяет дополнительному серверу получать только те изменения в зонах, которые требуются для синхронизации своей копии зоны с ее исходным вариантом, либо с первичной или вторичной копией зоны, хранимой на другом DNS-сервере. Запрос AXFR обеспечивает полную передачу всей информации о зоне.

Глава 6 Настройка сайтов

Занятие 1. Настройка параметров сайта

стр. 139

► Задание 1: переименуйте сайт

2. Щелкните папку Sites.

   Какие объекты отображаются в правой панели?

   Default-First-Site-Name (стандартный сайт, созданный мастером установки Active Directory), контейнер Inter-Site Transports и контейнер Subnets.

стр. 140

► Задание 5: создайте связь сайтов

1. Откройте папку Inter-Site Transports и щелкните папку IP.

   Какой объект отображается в правой панели?

   DEFAULTIPSITELINK, стандартная связь сайтов, созданная мастером установки Active Directory.

стр. 153

Закрепление материала

1. Назовите четыре этапа настройки сайта.

   Создание сайта, сопоставление подсети сайту, подключение сайта с использованием связей сайта и выбор лицензирующего компьютера для сайта.

2. Назовите два конфигурационных объекта сайта, которые мастер установки Active Directory создает автоматически.

   Мастер установки Active Directory автоматически создает объект с именем Default-First-Site-Name в контейнере Sites и объект с именем DEFAULTIPSITELINK в контейнере IP.

3. Какой протокол использует удаленные вызовы процедур для межсайтовой и внутрисайтовой репликации?

   Протокол репликации IP.

4. Назовите три этапа настройки репликации между сайтами.

   Создание связи сайта, настройка атрибутов связей сайта (такие, как стоимость связи сайта, частота репликации и возможность репликации) и создание мостов связей сайта.

5. В чем отличие частоты и доступности репликации?

   Частота репликации — это интервал между репликациями через связь сайтов. Доступность репликации подразумевает, что связь сайта доступна для репликации информации каталогов.

6. Для чего предназначен сервер-плацдарм?

   Сервер-плацдарм упорядочивает выбор контроллера домена — основного приемника межсайтовой репликации. Сервер-плацдарм затем распространяет информацию каталога путем межсайтовой репликации.

Глава 7 Управление учетными записями пользователей

Занятие 2. Планирование новых учетных записей

стр. 162

Определение правил именования

Заполните табл. 7-3, **используя** информацию **из разделов** «Сценарий», «Условия» **и** «Список новых сотрудников», **чтобы** определить правила именования для **новых** служащих.

Ответы могут меняться. Например, можно скомбинировать полное имя с именем подразделения для повторяющихся имен или взять за основу регистрационного имени пользователя его имя и первую букву фамилии плюс дополнительные символы из фамилии для повторяющихся имен. Все регистрационные имена пользователей и полные имена должны быть уникальными.

Заполните табл. 7-4, **используя** информацию **из разделов** «Сценарий», «Условия» и «Список **новых** сотрудников», **чтобы** определить часы входа в систему для новых служащих и компьютеры, с которых они **могут** это сделать.

Штатные сотрудники могут входить в сеть 24 часа в сутки, семь дней в неделю с любого компьютера в сети. Временные сотрудники совместно используют учетные записи Tempi и Temp2. Только два временных работника могут регистрироваться одновременно в течение смены, поэтому вы должны определить график работы 4-х сотрудников на 2-х компьютерах.

Выберите в табл. 7-5 **подходящие** параметры **смены паролей для каждого пользователя, чтобы определить, кто контролирует пароль пользователя.**

Временным сотрудникам не разрешается менять свои пароли. Постоянные сотрудники могут менять свои пароли, более того, они обязаны сделать это при следующем входе в систему.

Занятие 3. Создание учетной записи

стр. 169

► Задание: создайте доменную учетную запись

3. Раскройте узел microsoft.com (если вы используете другое имя домена, раскройте свой домен) и дважды щелкните папку Users.

   Какие учетные записи мастер установки Active Directory создал по умолчанию?

   Administrator, Cert **Publishers, DHCP Administrators, DHCP Users, DnsAdmins, DnsUpdateProxy, Domain Admins, Domain Computers, Domain Controllers, Domain Guests, Domain Users, Enterprise Admins, Group Policy Creator Owners, Guest, IUSR_SERVER1, IWAM_ SERVER1, krbtgt, RAS and IAS Servers, SchemaAdmins и TsInternet User. (Ответы могут варьироваться.)**

4. Щелкните правой кнопкой мыши папку Users и выберите в контекстном меню команду New\User (Создать\Пользователь).

   Откроется окно New Object — User.

   Где в Active Directory будет создана новая учетная запись?

   microsoft.com/Users (Ответ может меняться, если имя вашего домена — не **microsoft.com)**

8. В списке справа от окна User Logon выберите @microsoft.com (имя домена может отличаться, если вы не использовали microsoft.com в качестве доменного имени DNS).

   Имя входа пользователя в сочетании с доменным именем, появляющимся в окне справа от окна User Logon Name, — это полное имя входа пользователя в Интернете. Это имя уникально определяет пользователя в каталоге (например, user1@microsoft.com).

   Заметьте: поле имени входа для предыдущих версий Windows заполняется автоматически.

   В каких случаях используется имя входа предыдущих версий Windows?

   Имя входа для пользователя пред-Windows 2000 применяется для регистрации в домене Windows **2000 с** компьютера **под управлением предыдущих версий Microsoft Windows.**

11. Определите, может ли пользователь изменять свой пароль.

    Каковы результаты одновременного применения флажков User Must Change Password At Next Logon и User Cannot Change Password? Поясните ответ.

    Появится следующее сообщение, что нельзя одновременно отметить оба этих флажка для одного пользователя.

    Когда пользователь в следующий раз попытается войти в систему, ему будет предложено **сменить пароль (иначе он не сможет войти в систему). Тем не менее Windows** 2000 **не позволит пользователю ни сменить пароль, ни войти в систему.**

    В каком случае следует выбрать флажок Account is Disabled при создании новой учетной записи?

    Некоторые возможные ответы: если это учетная запись пользователя, который еще не начал работать в компании; если пользователь временно отсутствует.

стр. 177

► Задание 1: определите время входа

2. На правой панели щелкните правой кнопкой параметр User Three и выберите в контекстном меню команду Properties (Свойства).

   Откроется окно User Three Properties (Свойства: User Three), вкладка General (Общие).

   Какую информацию, кроме имени и фамилии, можно задать для учетной записи на вкладке General? Для чего нужна эта информация?

   Отображаемое имя, описание, кабинет, номер телефона, адрес электронной почты и персональная Web-страница. Active Directory способна хранить сведения о пользователе, которые иначе пришлось сохранять средствами отдельного приложения. Кроме того, введенная информация о пользователе помогает найти его в Active Directory.

3. На вкладке Account (Учетная запись) щелкните кнопку Logon Hours (Время входа). Откроется окно Logon Hours For User Three (Время входа для User Three).

   В какое время пользователю User Three разрешается войти в систему?

   По умолчанию вход разрешен в любое время во все дни недели.

стр. 177

▶ Задание 2: задайте срок действия учетной записи

3. Щелкните вкладку Account (Учетная запись).

   Когда окончится срок действия учетной записи?

   Никогда.

стр. 178

▶ Задание 1: протестируйте возможности входа в систему под каждой учетной записью

3. Щелкните OK, чтобы закрыть окно *сообщения*.

   Удалось ли вам войти в систему? Почему?

   Нет. По умолчанию администраторы имеют право на регистрацию на контроллере домена, а простые **пользователи — нет.**

стр. 178

▶ Задание 3: протестируйте параметры времени входа

1. Попытайтесь войти в систему как User1 с паролем student.

   Удалось ли вам войти в систему? Почему?

   Да, поскольку Userl имеет доступ в сеть 24 часа в сутки семь дней в неделю, а теперь он получил право и на интерактивную регистрацию.

3. В открывшемся окне измените пароль на **student.**

   Удалось ли вам войти в систему? Почему?

   Нет, поскольку User3 имеет право на вход в систему только с 18:00 до **6:00. (Ответ «Да , если пользователь входит в систему** с **18:00 до** 6:00).

стр. 178

▶ Задание 4: протестируйте параметры пароля

1. Попытайтесь войти в систему как User7 без пароля.

   Удалось ли вам войти в систему? Почему?

   Нет, поскольку пользователю User7 пароль был задан при создании учетных записей.

3. В открывшемся окне измените пароль на student.

   Удалось ли вам войти в систему? Почему?

   Да, поскольку User7 — верный пароль для учетной записи User7.

5. Попытайтесь войти в систему как User9 с паролем User9.

   Удалось ли вам войти в систему? Почему?

   Да, поскольку User9 — верный пароль для учетной записи User9.

стр. 179

▶ Задание 5: протестируйте параметры пароля, попытавшись изменить его

3. В поле Old Password (Старый пароль) введите пароль для учетной записи User9, а в полях New Password (Новый пароль) и Confirm New Password (Подтверждение) введите **student** и щелкните OK.

   Удалось ли вам изменить пароль? Почему?

   Нет, поскольку пользователю User9 не разрешено менять пароль.

стр. 179

► Задание 6: протестируйте срок действия учетной записи

2. В появившемся окне измените пароль **на student.**

Удалось ли вам войти в систему? Почему?

Да, поскольку срок действия учетной записи User5 истечет в конце сегодняшнего дня.

Занятие 4. Создание профиля пользователя

стр. 187

► **Задание** 3: просмотрите **существующие** профили

3. **Перейдите** на вкладку User Profiles (Профили пользователей).

Какие профили пользователей **хранятся** на вашем компьютере?

MICROSOFT\administrator, MICROSOFT\puser и пользователи, которые когда-либо входили в систему данного компьютера.

стр. 187

► Задание 4: определите и протестируйте локальный профиль

5. **Выйдите** *из* системы и вновь **войдите как** puser.

Сохранились ли цвета экрана? Почему?

Да, поскольку цветовая палитра экрана хранится в профиле puser.

стр. 190

► Задание 6: протестируйте перемещаемый профиль

1. Выйдите из системы и войдите как User2.

Совпадают **ли или** отличаются **цвета** экрана и рабочий стол от **заданных в Profile** Template? Почему?

Цветовая палитра та же, что задана в шаблоне профиля, поскольку перемещаемый профиль для учетной записи User2 был загружен из общей папки на сервере сети и применен к тому компьютеру, на котором зарегистрировался пользователь User2.

стр. 190

► Задание 7: определите тип профиля, **назначенного пользователю**

2. Дважды щелкните строку System (Система) **и перейдите на** вкладку User **Profiles (Профили** пользователей).

Какие типы профиля перечислены для учетной записи User2?

Перемещаемый профиль пользователя.

Занятие 6. Изменение учетных записей

стр. 196

► Задание 1: отключите учетную запись

6. На правой панели **консоли** Active Directory Users and **Computers** щелкните **правой** кнопкой **мыши** учетную **запись** пользователя, **которую** только **что отключили, чтобы** появилось **контекстное меню.**

Как определить, что учетная **запись** отключена?

В контекстном меню присутствует команда Enable Account, и значок учетной записи пользователя на правой панели помечен красным крестом.

8. Попытайтесь войти в систему как puser.

   Удалась ли эта попытка? Почему?

   Нет, поскольку учетная запись заблокирована.

стр. 196

▶ Задание 2: включите учетную запись

6. На правой панели консоли Active Directory Users and Computers щелкните правой кнопкой мыши учетную запись пользователя, которую только что включили, чтобы появилось контекстное меню. Как определить, что учетная запись включена?

   В контекстном меню присутствует команда Disable Account, и значок учетной записи пользователя на правой панели не помечен красным крестом.

стр. 197

▶ Задание 3: протестируйте включение учетной записи и измените ее пароль

1. Войдите в систему как puser.

   Удалось ли это? Почему?

   Да, поскольку учетная запись разблокирована.

стр. 197

▶ Задание 2: протестируйте смену пароля

1. Войдите в систему как puser с паролем password.

   Удалось ли это? Почему?

   Не сразу. Поскольку выбран параметр User Must Change Password At Next Logon, появится сообщение о входе л систему, показывающее, что пароль устарел, и его надо сменить. Затем откроется диалоговое окно Change Password, где надо ввести и подтвердить новый пароль, известный только пользователю. Только после этого пользователь сможет войти в систему.

стр. 198

Закрепление материала

1. Какие возможности предоставляют пользователям локальные и доменные учетные записи?

   Локальная учетная запись разрешает пользователю войти в систему и получить доступ к ресурсам только на том компьютере, на котором вы создали эту запись. Доменная учетная запись позволяет пользователю входить в домен с любого компьютера в сети и получать доступ к ресурсам всего домена, к которым этому пользователю разрешен доступ.

2. На что следует обратить внимание при планировании новых учетных записей?
   - Правила именования, которые обеспечат уникальные, но понятные имена учетных записей.
   - Кто будет определять пароль — вы или пользователь.
   - Часы, в которые пользователю разрешено или запрещено входить в сеть.
   - Надо ли блокировать учетную запись.
   - Тип профиля пользователя.
   - Где хранить документы пользователя — в локальной папке My Documents или в домашней папка на сервере.

3. Какая информация требуется для создания доменной учетной записи?

   Имя или фамилия, имя для входа, а также имя для входа с устаревших версий Windows.

4. Пользователю нужен доступ к сетевым ресурсам из дома, но он не хочет оплачивать расходы на телефонную связь. Как следует настроить учетную запись?

   В окне свойств учетной записи на вкладке Dial-In щелкните Set By Caller (Routing and Remote Access Service Only), чтобы сервер RAS выполнил обратный вызов пользователя по указанному им номеру. Вы также можете выбрать параметр Always Callback To, чтобы сервер RAS задействовал указанный номер телефона для обратного вызова. В таком случае пользователь должен находиться по указанному номеру телефона для установления соединения с сервером.

5. В чем разница между локальным и перемещаемым профилями пользователя?

   Локальный профиль пользователя хранится на компьютере, где регистрируется пользователь. Перемешаемый профиль хранится на сервере домена и копируется на клиентский компьютер, с которого пользователь входит в систему.

6. Как убедиться, что пользователь на клиентском компьютере с Windows 2000 имеет перемешаемый профиль?

   Сначала создайте общую папку на сервере **сети. Затем для каждой учетной записи в** диалоговом окне **свойств укажите путь к этому общему** каталогу **на сервере. В следующий раз, когда пользователь** войдет **в сеть, будет создан перемещаемый профиль пользователя.**

7. Как убедиться, что пользователь имеет хранящуюся централизованно домашнюю папку?

   Сначала создайте родительскую папку на сервере и откройте к ней доступ. Затем предоставьте группе Users разрешение Full Control для этой папки. После **этого укажите путь к общей папке, включая имя домашней папки конкретного пользователя** (*\\имя_сервера\имя_общей_папки\имя_входа_пользователя).*

8. Почему следует переименовывать учетную запись?

   Переименуйте учетную запись, если вы хотите, чтобы новый пользователь получил все свойства прежнего, включая права, параметры рабочего стола и членство в группах. Преимущество переименования учетной записи в том, что вам не придется задавать все свойства, как для нового пользователя.

Глава 8 Управление учетными записями групп

Занятие 2. Стратегия формирования группы

стр. 208

Заполнение тетради «Планирование групп»

Название группы	Тип и область действия	Состав
Testers глобальная	Группа безопасности —	Все контролеры ОТК
Customer Reps	Группа безопасности — глобальная	Все представители отдела по обслуживанию клиентов
Maint Workers	Группа безопасности — глобальная	Все сотрудники службы поддержки
Managers	Группа безопасности — глобальная	Все управляющие
Sales Reps	Группа безопасности — глобальная	Все представители отдела сбыта
Network Admin	Группа безопасности — глобальная	Все сетевые администраторы
All Employees	Группа безопасности — глобальная	Все сотрудники
Topics Employees	Группа безопасности — глобальная	Сотрудники, занимающиеся производством
Customerdatabase	Группа безопасности — локальная доменная	Представители отдела по обслуживанию клиентов, управляющие, представители отдела сбыта

Заполнение тетради «Планирование групп» *(окончание)*

Название группы	Тип и область действия	Состав
Company policies	Группа безопасности — локальная доменная	Все сотрудники
Microsoft Office	Группа безопасности — локальная доменная	Контролеры ОТК, представители отдела по обслуживанию клиентов, управляющие, представители отдела сбыта, сетевые администраторы
Sales reports	Группа безопасности — локальная доменная	Представители отдела сбыта
E-mail announcements	Группа распространения — локальная доменная	Все сотрудники
E-mail manufacturing topics	Группа распространения — локальная доменная	Определенные категории сотрудников

1. Необходимы ли в вашей сети локальные группы?

   Нет. Из сценария ясно, что создавать локальные группы, которые вы можете использовать только на одном компьютере, не требуется.
2. Необходимы ли в вашей сети универсальные группы?

   Нет. Из сценария ясно, что создавать универсальные группы не потребуется. В вашем домене **нет групп, которым нужен доступ к ресурсам в нескольких доменах или в которые могут входить пользователи из нескольких доменов.**
3. Торговые представители вашей компании часто посещают штаб-квартиру и другие подразделения. Следовательно, придется создать для них учетные записи в других доменах с теми же правами доступа к ресурсам, какими обладают учетные записи торговых представителей в вашем домене. Вам также следует упростить процедуру предоставления администраторами других доменов доступа к ресурсам вашего домена. Как это осуществить?

   Нужно создать глобальные группы для представителей отдела сбыта ко всех других доменах. Добавьте **эти глобальные группы в соответствующие доменные локальные группы в вашем домене. Сообщите администраторам других доменов о глобальной группе, где собраны сотрудники отдела сбыта в вашем домене. Проследите, чтобы эти администраторы добавили группу сотрудников** отдела **сбыта из вашего домена в соответствующие доменные локальные группы в их доменах.**

стр. 226

Закрепление материала

1. Зачем нужны группы?

   Группы упрощают администрирование, так как позволяют задавать права и разрешения о ин раз для группы, а не для каждого пользователя.
2. Какова цель добавления одних групп в другие?

   Добавляя группы в другие группы (вложение), вы можете создать объединенную группу, что позволит вам реже задавать разрешения.
3. Почему следует использовать не группы распространения, а группы безопасности?

   Группы безопасности применяются для назначения разрешений, а группы распространения — когда **основная функция группы не относится к безопасности, например, если для списка распространения почты. Нельзя применять группы распространения для назначения разрешений.**
4. Какую стратегию необходимо выбрать при использовании глобальных и локальных групп домена?

Следует включить учетные записи пользователей в глобальные группы, глобальные группы — в доменные локальные группы, а затем назначить разрешения для доменных локальных групп.

5. Почему не следует применять локальные группы на компьютере, который был присоединен к домену?

   Локальные группы не появляются в Active Directory: вам придется администрировать их отдельно на каждом компьютере.

6. Опишите простейший способ предоставить пользователю права управления всеми компьютерами в домене.

   Добавьте его учетную запись в стандартную глобальную группу Domain Admins. После чего он сможет выполнять все административные задачи на всех компьютерах домена и в Active Directory. Пользователь получает права администратора, поскольку Windows 2000 включает стандартную глобальную группу Domain Admins во встроенную доменную локальную группу Administrators, а также во встроенную локальную группу Administrators на каждом рядовом сервере домена и компьютере с Windows 2000 Professional. Встроенная доменная локальная группа Administrators имеет все полномочия для всех контроллеров домена и Active Directory. Каждая встроенная локальная группа Administrators имеет полный контроль над компьютером, на котором она существует.

7. Почему не следует работать на компьютере с полномочиями администратора? Что рекомендуется предпринять вместо этого?

   Работа под Windows 2000 с правами администратора делает систему уязвимой для атак «троянских коней» и др. Для большинства работ, выполняемых на компьютере, достаточно полномочий групп Users или Power Users. Для выполнения административных задач вы сможете войти в систему как администратор, выполнить требуемые действии и выйти из системы. Если вам часто приходится выполнять такие задачи, вы можете командой Run As запускать программу с полномочиями администратора.

8. Предположим, что штаб-квартира упоминавшейся здесь производственной компании имеет единственный домен в Париже. Менеджерам компании для выполнения своих задач требуется доступ к инвентаризационной БД. Как предоставить менеджерам доступ к этой БД?

   Объедините всех менеджеров в глобальную группу. Создайте локальную доменную группу, обладающую полномочиями доступа к инвентарной базе, и добавьте глобальную группу менеджеров в эту локальную доменную группу.

9. Предположим, что в этой же компании используется среда с тремя доменами. Корневой домен находится в Париже, а другие домены — в Австралии и Северной Америке. Менеджерам из всех трех доменов для выполнения задач требуется доступ к расположенной в Париже инвентаризационной БД. Как предоставить менеджерам доступ к этой БД?

   В каждом домене создайте глобальную группу и добавьте учетные записи менеджеров в этом домене в эту глобальную группу. Создайте локальную доменную группу для доступа к инвентарной базе данных в домене, где располагается эта БД (в Париже). Добавьте глобальную группу для доступа к базе данных инвентаря в домен, в котором находится база данных (Париж). Добавьте глобальные группы менеджеров из каждого домена в локальную доменную группу базы данных. Затем предоставьте права доступа к инвентарной БД локальной доменной группе.

Глава 9 Безопасность сетевых ресурсов

Занятие 2. Назначение разрешений NTFS

стр. 236

Упражнение 1: планирование разрешений NTFS

Какое разрешение NTFS по умолчанию следует удалить при назначении пользовательских разрешений файлу или папке?

Разрешение Full Control для группы Everyone на уровне тома.

Заполните табл. 9-5, чтобы спланировать и записать разрешения.

Табл. 9-5. Планирование разрешений для упражнения 1

Путь	Учетная запись или группы	Разрешения NTFS	Блокирование наследования (да\нет)
Apps	Administrators	Full Control	Нет
Apps\WordProc	Users	Read & Execute	Нет
Apps\Spreadsh	Accounting Managers Executives	Read & Execute Read & Execute Read & Execute	Нет
Apps\Database	Accounting Managers Executives	Read & Execute Read & Execute Read & Execute	Нет
Public	Administrators Creator Owner Users	Full Control Full Control Write	Нет
Public\Library	Administrators Users	Full Control Read & Execute	Да
Public\Manuals	Administrators Users User81	Full Control Read & Execute Full Control	Да

стр. 238

▶ Задание 1: удалите разрешения для группы Everyone (Все)

4. Перейдите на вкладку Security (Безопасность), чтобы просмотреть разрешения на доступ к папке Data.

   Перечислите имеющиеся разрешения на доступ к папке Data.

   Группа Everyone имеет разрешение Full **Control.**

5. В списке Name (Имя) выберите группу Everyone (Все) и щелкните кнопку Remove (Удалить).

   Что вы видите?

   Появится сообщение, **что папка наследует** права **для** группы Everyone **от своей родительской** папки. **Для изменения разрешений для** Everyone надо сначала отключить наследование.

8. Щелкните кнопку Remove (Удалить).

   Перечислите имеющиеся разрешения доступа к папке Data.

   Пока не назначено никаких разрешений.

стр. 238

▶ Задание 2: назначьте группе Users (Пользователи) разрешение на доступ к папке Data

4. Щелкните OK, чтобы вернуться в диалоговое окно свойств папки Data.

   Перечислите имеющиеся разрешения на доступ к папке.

   Группа Users имеет следующие **разрешения: Read & Execute, List Folder Contents и Read. Это разрешения по умолчанию, которые Windows 2000 назначает,** когда вы **добавляете учетную** запись или группу **в список разрешений.**

стр. 239

▶ Задание 3: назначьте группе CREATOR OWNER (Создатель-владелец) разрешения на доступ к папке Data

4. Щелкните OK. чтобы вернуться в окно свойств папки Data.

   Перечислите существующие разрешения папки.

Группа Users имеет следующие разрешения: Read & Execute, List Folder Contents, Read и Write. Группа Creator Owner не имеет разрешений.

5. Убедитесь, что выбрана группа CREATOR OWNER (Создатель-владелец), и пометьте флажок Allow (Разрешить) у разрешения Full Control. Затем щелкните кнопку Apply (Применить), чтобы сохранить внесенные изменения.

   Что вы видите?

   Для группы Creator Owner не отмечен ни один из флажков Allow ни для каких разрешений. Рядом с кнопкой Advanced появляется примечание, что существуют дополнительные разрешения, которые здесь не отображаются. Щелкните кнопку Advanced для их просмотра.

7. Под полем Name (Имя) выберите CREATOR OWNER (Создатель-владелец).

   Какие разрешения назначены группе CREATOR OWNER (Создатель-владелец) и на какие файлы и папки они распространяются?

   Группа Creator Owner имеет разрешение Full Control. Эти разрешения применяются только к подпапкам и файлам. Разрешения, назначенные группе Creator Owner, не применимы к данной папке, но только к файлам и подпапкам, которые будут создаваться в данной папке. Пользователь, создающий новый файл или папку, получает права, назначенные группе Creator Owner для родительской папки каталога, и должен принадлежать к другим группам, которые имеют права записи в новые файлы **и папки.**

стр. 239

▶ Задание 4: проверьте разрешения, назначенные папке Data

3. В папке Data попробуйте создать текстовый файл с именем user81.

   Удалось ли это сделать? Почему?

   Да, поскольку группа Users (в которой состоит User81) имеет разрешение Write для **папки Data.**

стр. 241

▶ Задание 1: проверьте разрешения на доступ к папке Reports пользователя User81

3. Попробуйте создать файл в папке Reports.

   Удалось ли это? Почему?

   Нет, поскольку только User82 и члены групп Managers и Administrators имеют право создавать и изменять файлы в папке Reports.

стр. 241

▶ Задание 2: проверьте разрешение на доступ к папке Reports пользователя User82

3. Попробуйте создать файл в папке Reports.

   Удалось ли это? Почему?

   Да, поскольку User82 имеет разрешение Modify для данной папки.

стр. 241

▶ Задание 3: проверьте разрешение на доступ к папке Sales пользователя Administrator

3. Попробуйте создать файл в папке Sales.

   Удалось ли это? Почему?

   Да, поскольку группа Administrators имеет разрешение Full Control для папки Sales.

стр. 241

▶ Задание 4: проверьте разрешение на доступ к папке Sales пользователя User81

3. Попробуйте создать файл в папке Sales.

   Удалось ли это? Почему?

   Нет, поскольку только группа Sales имеет разрешение NTFS на создание и изменение файлов в папке Sales. **User81 не входит в эту группу.**

стр. 241

▶ Задание 5: проверьте разрешения на доступ к папке Sales пользователя User82

3. Попробуйте создать файл в папке Sales.
   Удалось ли это? Почему?

   Да, поскольку User82 является членом группы Sales, которой было назначено разрешение Modify для папки Sales.

Занятие 3. Специальные разрешения

стр. 248

▶ Задание 1: определите разрешения для файла

4. Перейдите на вкладку Security (Безопасность), чтобы увидеть разрешения для файла OWNER.TXT.
   Каковы текущие разрешения для OWNER.TXT?

   Группа Administrators имеет разрешение Full Control. Группа **Users имеет разрешение Read & Execute.**

6. Перейдите на вкладку Owner (Владелец).
   Кто является текущим владельцем файла OWNER.TXT?

   Группа Administrators.

стр. 249

▶ Задание 3: станьте владельцем файла

6. Щелкните кнопку Advanced (Дополнительно), чтобы открыть диалоговое окно Access Control Settings For OWNER.TXT (Параметры управления доступом для OWNER.TXT), и перейдите на вкладку Owner (Владелец).
   Кто на данный момент владеет файлом OWNER.TXT?

   Группа Administrators.

7. В списке Name (Имя) выберите User83 и щелкните кнопку Apply (Применить).
   Назовите текущего владельца файла OWNER.TXT.

   User83.

Занятие 4. Копирование и перемещение файлов и папок

стр. 253

▶ Задание 1: создайте папку, зарегистрировавшись в системе как пользователь

1. Зарегистрируйтесь в системе как User83. В Windows Explorer (Проводник) создайте на диске C: папку с именем Tempi.
   Перечислите разрешения, назначенные этой папке.

   Группа **Everyone имеет разрешение Full** Control.

   Кто является ее владельцем? Почему?

   User83, поскольку тот, кто создал папку или файл, и является его владельцем.

стр. 253

▶ Задание 2: создайте папку, зарегистрировавшись как Administrator

2. На диске C: создайте папки Temp2 и Temp3.
   Перечислите назначенные им разрешения.

Группа Everyone имеет разрешение Full Control.

Кто является владельцем папок Temp2 и Тетр3? Почему?

Группа Administrators, поскольку эти каталоги создал член группы Administrators.

стр. 253

► **Задание** 3: скопируйте **папку** в другую папку в пределах **тома NTFS**

2. Сравните разрешения и владельцев папок C:\Temp1\Temp2 и C:\Temp2.

Кто является владельцем папки C:\Temp1\Temp2 и каковы разрешения, назначенные ей? **Почему?**

Владельцем по-прежнему является группа Administrators, поскольку вы вошли в систему как Administrator. Когда папка или файл копируется в пределах тома NTFS, тот, кто копирует эту папку или файл, становится его владельцем.

Группа Everyone имеет разрешение Full Control, поскольку, когда папка или файл копируется в пределах тома NTFS, эта папка или файл наследует разрешения от папки, в которую он был скопирован.

стр. 253

► **Задание** 4: переместите папку в пределах тома **NTFS**

2. Выберите папку C:\Temp3 и переместите ее в **папку** C:\Temp1.

Что произошло с разрешениями и кто теперь **является** владельцем папки C:\Temp1\Тетр3?

Папка C:\Temp1\Temp3 сохраняет те же разрешения и владельца (группу Administrators), что и C:\Temp3. Это происходит потому, что, когда каталог или файл перемещается в пределах тома NTFS, он сохраняет свои исходные разрешения и владельца.

Занятие 5. Устранение неполадок при задании разрешений

стр. 257

► Задание 3: протестируйте применение разрешения Full **Control**

1. В Windows Explorer (Проводник) дважды щелкните файл NOACCESS.TXT **в папке** C:\Fullaccess, чтобы открыть его.

Удалось ли вам это? Почему?

Нет. Для группы Everyone было отменено разрешение Full Control для файла C:\Futlaccess\noaccess.txt. Учетная запись Administrator входит в группу Everyone.

4. Удалите NOACCESS.TXT, набрав **del noaccess.txt.**

Удалось ли вам **это?** Почему?

Да, поскольку разрешение Full Control включает специальное разрешение Delete Subfolders and Files для совместимости с POSIX-приложениями. Это специальное разрешение позволяет пользователю удалять файлы в корне каталога, для которого пользователь имеет разрешение Full Control. Это разрешение перекрывает разрешения для файлов.

Как пользователю с разрешением Full Control для папки запретить удалять файл в этой **палке?**

Предоставьте пользователям все индивидуальные разрешения, а затем отмените для них специальное разрешение Delete Subfolders and Files.

стр. 258

Закрепление материала

1. Какое разрешение **задано** по умолчанию, когда том отформатирован под NTFS? Кто имеет доступ к тому?

Разрешением по умолчанию — Full Control. Группа Everyone имеет доступ к тому.

2. **Какими** разрешениями обладает пользователь, имеющий разрешение **Write для папки и являющийся** также членом группы с разрешением **Read** для **той** же папки?

Пользователь имеет разрешения Read и Write для данной папки, поскольку разрешения NTFS суммируются.

3. **Пользователь** имеет **разрешение** Modify для папки и разрешение **Read для файла. Файл** копируется **в** эту папку. Какое **разрешение для** файла **имеет** пользователь?

   Пользователь может изменять файл, поскольку файл наследует разрешение Modify от папки.

4. Что происходит с **разрешениями,** назначенными для **файла,** когда **файл** перемещается из одной **папки** в другую на **том же** томе **NTFS? Что происходит,** когда файл перемещается в папку на другом **томе NTFS?**

   Когда файл перемещается из одной папки в другую в рамках тома NTFS, он сохраняет свои разрешения. Когда файл перемещается в папку на другом томе NTFS, он наследует разрешения от папки назначения.

5. Как передать файлы и папки уволившегося сотрудника во владение другому сотруднику?

   Вы должны войти в систему как Administrator, чтобы стать владельцем файлов или папок сотрудника. Предоставьте специальное разрешение Take Ownership другому сотруднику, чтобы тот мог стать владельцем папок и файлов. Сообщите сотруднику, которому вы предоставили разрешение Take Ownership, чтобы тот принял во владение требуемые файлы и папки.

6. Какие **три параметра** следует проверить, когда пользователь не может получить **доступ** к ресурсу?

   Проверьте разрешения, назначенные учетной записи пользователя и группам, к которым он относится.

   Проверьте, не запрещен ли для учетной записи пользователя или группы, к которой он относится, доступ к нужному файлу или папке.

   Проверьте, не была **ли папка (файл)** переименована **или перемещена на другой том.** Если так, разрешения могли **измениться.**

Глава 10 Администрирование общих папок

Занятие 1. Общие папки

стр. 262

Практикум; назначение разрешений

1. User1 — член **групп** Group1, Group2 **и Group3. Для папки FolderA** у Group1 **есть** разрешение **Read, у** Group3 **— Full Control (Полный** доступ), а группе Group2 для этой папки **разрешений не** назначено. **Какие** результирующие разрешения будет иметь **Userl для FolderA?**

   Поскольку Userl имеет разрешения всех групп, то у Userl для папки FolderA есть разрешение Full Control, которое также включает все возможности разрешения Read.

2. Userl также является членом группы Sales, которой **назначено разрешение Read** (Чтение) **для FolderB.** Для User1, **как отдельного** пользователя, отменено разрешение Full **Control** (Полный доступ) для FolderB. **Какие** результирующие **разрешения** будет **иметь** UserlOl для **FolderB?**

   Userl не имеет доступа к папке FolderB. Даже если Userl — член группы Sales, которая имеет разрешение Read для папки Sales, для Userl отменено разрешение Full Control для папки FolderB. Запрет разрешения всегда имеет высший приоритет.

Занятие 4. Сочетание разрешений на доступ к общей папке и разрешений NTFS

стр. 274

Упражнение 1: сочетание разрешений

1. **В первом случае** открыт доступ к папке **Data. Группа Sales имеет для нее разрешение Read,** а для вложенной в нее папки Sales — NTFS-разрешение Full **Control.**

Каким будет результирующее разрешение группы Sales для доступа к папке SaJes при подключении по **сети к** папке **Data?**

Группа Sales имеет разрешение Read для подпапки Sales, поскольку, когда разрешения общих папок комбинируются с разрешениями NTFS, **применяются более жесткие ограничения.**

2. Во втором случае **папка** Users содержит **личные папки** пользователей. Каждая личная папка содержит данные, **доступные только** пользователю, именем которого она названа. **Папка** Users доступна группе Users с разрешением Full Control. User1 и User2 имеют разрешения **NTFS Full** Control только для своих личных папок и **никаких разрешений NTFS для остальных.** Эти пользователи — члены **группы Users.**

Какими разрешениями доступа к папке User1 обладает **Userl при подключении к общей** папке Users? Каковы его разрешения для папки User2?

Userl имеет разрешение Fall Control для полпапки Userl, поскольку и разрешения общих папок, и разрешения NTFS предоставляют полный доступ. Userl не может получить доступ к подпапке User2, поскольку не имеет разрешений NTFS для доступа к ней. Очень часто личные файлы централизованно хранятся на файловом сервере.

стр. 275

Упражнение 2: планирование общих папок

Возможны два варианта. Вы можете целиком полагаться на разрешения NTFS и назначить разрешение Full Control для всех **общих** папок группе Everyone, либо вы можете **использовать** разрешения **общих папок.** Ниже перечислены предполагаемые **общие** папки и соответствующие им разрешения доступа, если вы решили назначать разрешения общих папок.

Откройте общий доступ к папке **Management** Guidelines с именем ресурса **MgmtGd.** Предоставьте разрешение Full Control группе Managers.

Откройте общий доступ к папке Data с именем ресурса Data. Предоставьте разрешение Full Control встроенной группе Administrators.

Откройте общий доступ к папке Data\Customer Service с именем ресурса **CustServ.** Предоставьте **разрешение** Change группе Customer Service.

Откройте общий доступ к папке **Data\Public** с именем ресурса Public. Предоставьте разрешение Change встроенной группе Users и **разрешение** Full Control — встроенной группе **Administrators.**

Откройте **общий** доступ к папке Applications с именем ресурса Apps. Предоставьте разрешение Read встроенной группе Users и разрешение **Full** Control — встроенной группе Administrators.

Откройте общий доступ к папке Project Management с именем ресурса ProjMan. Предоставьте разрешение Change группе Managers и разрешение Full Control — встроенной группе Administrators.

Откройте общий доступ к папке **Database\Customers** с **именем** ресурса CustDB. Предоставьте разрешение Change группе CustomerDBFull, разрешение Read — группе **CustomerDB-**Read и разрешение Full Control — встроенной группе Administrators.

Откройте общий доступ к папке Users с именем ресурса Users. Создайте под**папки** для каждого сотрудника. Предоставьте каждому сотруднику разрешение Full Control **для** его каталога. Лучше, если вы позволите **Windows** 2000 создавать и назначать разрешения для этих папок автоматически при создании учетной записи пользователя.

стр. 276

► Задание: предоставьте доступ **к папкам**

6. В поле Comment (Комментарий) введите **shared productivity applications и** щелкните кнопку OK. Как Windows Explorer **изменит значок** папки Apps, иллюстрируя, что к папке **открыт доступ?**

Windows Explorer отображает значок руки, держащей папку Apps. Это означает, что к данной папке открыт совместный доступ.

стр. 276

▶ Задание 1: определите текущие разрешения для общей папки Apps

1. В окне свойств папки Apps щелкните вкладку Sharing (Доступ) и затем — кнопку Permissions (Разрешения).

   Каковы разрешения по умолчанию для этой папки?

   Группа Everyone имеет разрешение Full Control.

стр. 277

▶ Задание 3: назначьте разрешение Full Control группе Administrators

3. Щелкните кнопку OK.

   Группа Administrators добавится в список групп, имеющих разрешения.

   Какой вид доступа будет назначен группе Administrators по умолчанию?

   Разрешение Read.

4. В столбце Allow (Разрешить) окна Permissions (Разрешения) установите флажок Full Control (Полный доступ).

   Почему также стало действующим разрешение Change (Изменение)?

   Разрешение Full Control включает в себя все остальные разрешения.

стр. 277

▶ Задание 1: подключите сетевой диск с помощью команды Run

3. В поле Open (Открыть) наберите \\SERVER1 (если у контроллера вашего домена другое имя, используйте его здесь и далее) и щелкните кнопку OK.

   Откроется окно SERVER1. Пользователям сети видны только общие папки.

   Какие папки доступны в данный момент?

   Помимо папок, к которым вы открыли общий доступ на вашем **контроллере** домена, доступны следующие: **Printers,** Scheduled **Tasks, NETLOGON и SYSVOL. Все принтеры, к** которым вы открыли доступ, также **появятся в списке.**

стр. 277

▶ Задание 2: подключите общую папку как сетевой диск командой Map Network Drive

7. Чтобы проверить, что сетевой диск успешно подключен, дважды щелкните значок My Computer (Мой компьютер) на рабочем столе — вы увидите, что появился новый логический диск P: Apps On Server1.

   Как Windows Explorer обозначает, что этот диск соответствует удаленной общей папке?

   Windows Explorer помечает диск значком с изображением сетевого кабеля, подключенного к диску.

стр. 278

▶ Задание 4: попытайтесь подключиться к общей папке на контроллере домена

3. В поле Open (Открыть) наберите \\SERVER1 (если у контроллера вашего домена другое имя, далее используйте именно его) и щелкните кнопку OK.

   Появится сообщение, что доступ закрыт. Почему?

   Потому что User81, учетная запись, которую вы использовали для входа в систему, не имеет требуемых **разрешений для доступа к обшей** папке. **Только группа Administrators может** получить доступ **к общей папке Apps.**

стр. 278

▶ Задание 5: подключитесь к общей папке от имени другого пользователя

4. Щелкните ссылку Connect Using A Different User Name (Подключение под другим именем).

8 окне Connect As (Подключиться как) задаются **параметры учетной записи** для подключения **к общей** папке, **в** том **числе** для подключения к другим доменам (в **ранних** версиях Windows). Когда следует использовать **этот режим?**

Если учетная запись, которую вы в данный момент используете, не обладает полномочиями для общей папки и у вас есть другая учетная запись, полномочная, подключитесь под этой записью. При этом вам не придется выходить из системы и повторно входить для получения доступа к общей лапке.

7. Удостоверьтесь, **что флажок** Reconnect At Logon (Восстанавливать при входе в систему) сброшен, **и шелкните Finish (Готово).**

   Можете ли **вы получить** доступ к диску J средствами Windows **Explorer? Почему?**

   Да, потому что учетная запись администратора имеет необходимые разрешения для доступа к общей палке.

стр. 280

▶ Задание 1: **проверьте разрешения** для папки Manuals при **локальном входе в** систему под именем User82

3. В папке Manuals попытайтесь создать какой-либо файл.

   Удалось ли вам **это? Почему?**

   Нет. Только группа Administrators и User83 имеют разрешение NTFS на создание и изменение файлов в папке Manuals.

стр. 280

▶ Задание 2: **проверьте разрешения для** папки Manuals при подключении к ней по сети

5. Попробуйте создать в ней какой-либо файл.

   Удалось ли вам это? **Почему?**

   Нет. Хотя группа Users имеет разрешение общего доступа Full Control для \\server1\public, только группа Administrators и User83 имеют разрешение NTFS на создание и изменение файлов в папке Manuals.

стр. 280

▶ **Задание 3: проверьте разрешения для папки** Manuals при локальном доступе

3. **В папке** Manuals **попытайтесь** создать какой-либо файл.

   Удалось ли вам это? **Почему?**

   Да. User83 **имеет NTFS-разрешение Full Control для этой папки.**

Занятие 5. Настройка DFS

стр. 289

▶ Задание 6: получите доступ к корню DFS

2. Дважды щелкните компьютер SERVER1.

   Windows Explorer выведет список всех общих папок на **контроллере** вашего домена. **Одна из них — Shared Apps,** созданный вами **корень DFS.**

   Обозначает ли как-либо Windows 2000, что Shared **Apps не является обычной** общей папкой?

   Windows 2000 не показывает, что этот ресурс — корень Dfs.

3. **Для просмотра** DFS-ссылок **дважды** щелкните папку **Shared Apps.**

   Windows Explorer откроет окно Shared Apps On Server1 со списком **всех** ссылок **этого корня.**

   Обозначает ли как-либо Windows 200l), что DFS-ссылки в **Shared Apps не** являются **обычными общими папками?**

   Windows 2000 не показывает, что эти папки являются ссылками Dfs.

стр. 290

Закрепление материала

1. Общая папка расположена на томе FAT, и пользователь имеет для нее **разрешение** Full Control. К каким объектам в этой папке получит **доступ** пользователь?

   Все папки и файлы в общей папке.

2. Назовите разрешения доступа к общей **папке.**

   Full Control, Change и Read.

3. Какие **разрешения** назначаются общей папке по умолчанию?

   Группа Everyone имеет разрешение Full Control.

4. Общая папка расположена **на томе NTFS,** и пользователь **имеет для нее разрешение** Full Control, **К каким** объектам **в** этой папке получит доступ пользователь?

   Только к папке и не обязательно к ее содержимому. Пользователь также должен иметь разрешения NTFS для каждого файла и подпапки в общей папке для получения доступа к этим файлам и подпапкам.

5. Почему рекомендуется централизованно хранить общие папки данных?

   Централизованное хранение данных упрощает их резервное копирование.

6. Каков наилучший способ защиты общих **файлов** и папок на томе NTFS?

   Следует поместить файлы, которые вы хотите использовать совместно, в общую папку и сохранить назначенные по умолчанию разрешения (группа Everyone имеет разрешение Full Control для тики). Назначьте разрешения NTFS пользователям и группам для управления доступом ко всему содержимому папки или к отдельным файлам.

7. Как система DFS облегчает навигацию пользователей по сети?

   Пользователю, работающему с общей папкой, управляемой DFS, не нужно знать имя сервера, на котором в действительности находится эта папка. После подключения к корню DFS пользователь может просматривать и получать доступ ко всем ресурсам, которые содержатся в каждой ссылке, вне зависимости от расположения сервера, на котором хранится данный ресурс.

Глава 11 Администрирование Active Directory

Занятие 1. Поиск объектов Active Directory

стр. 295

► **Задание 2: найдите** учетную запись пользователя **в домене**

1. В дереве консоли щелкните свой **домен правой** кнопкой и выберите **команду** Find (Найти).

   Откроется диалоговое **окно Find** (Поиск).

   Какие типы объектов доступны для поиска?

   Пользователи, контакты и группы; компьютеры; принтеры; общие папки; подразделения; особый поиск и клиенты удаленной установки (если установлены службы RIS).

2. **Убедитесь,** что **в** поле Find выбран элемент Users, Contacts, And **Groups (Пользователи,** контакты и группы), и щелкните кнопку Find Now (Найти). Что вы увидите?

   Список пользователей и групп в домене.

Занятие 2. Управление доступом к объектам Active Directory

стр. 302

► Задание 2: **просмотрите** разрешения, заданные Active Directory по умолчанию **для ОП**

4. **Запишите** в **приведенную** ниже **таблицу группы,** обладающие разрешениями **доступа к ОП** Security1. Эта информация понадобится на занятии 5.

Табл. 11-5. Группы, обладающие разрешениями доступа к ОП Security1

Учетная запись или группа	Установленные разрешения
Account Operators	Специальные разрешения
Administrators"	Наследуют разрешения Read, Write и Create All Child Objects, а также имеют специальные разрешения
Authenticated Users	Read
Domain Admins	Full Control
Enterprise Admins	Наследует Full Control
Pre-Windows 2000 Compatible Access	Специальные разрешения
Print Operators	Специальные разрешения
SYSTEM	Full Control

Как узнать, не наследуются ли какие-либо разрешения от домена (родительского объекта)?

Разрешения, которые предоставлены группе Administrators, наследуются от родительского объекта. **Флажки для наследованных разрешений выделяются серым цветом.**

стр. 302

► Задание 3: просмотрите специальные разрешения ОП

2. Чтобы просмотреть специальные разрешения группы Account Operators (Операторы учета), в списке Permission Entries (Элементы разрешении) выделите каждый элемент, относящийся к данной группе, и затем щелкните кнопку View/Edit (Показать/Изменить).

   Откроется окно Permission Entry For Security1 (Элемент разрешения для Security1).

   Какие разрешения объекта назначены группе Account Operators? Какие действия могут выполнять члены группы Account Operators в данном ОП? (Совет: проверьте в поле Permission Entries каждую запись разрешения, относящуюся *к* группе Account Operators).

   Разрешения, назначенные группе Account **Operators,** таковы: **Create User Objects, Delete User** Objects, **Create Group** Objects, **Delete** Group **Objects, Create Computer Objects и Delete Computer** Objects. **Операторы** учета **могут** только создавать и удалять **учетные записи пользователей, группы и компьютеры.**

   Все ли объекты данного ОП наследуют разрешения, назначенные для группы Account Operators? Почему?

   Нет. Объекты в ОП не наследуют **этих разрешений. Колонка Apply To в списке Permission Entries диалогового** окна Access **Control Settings For Securityl показывает, что разрешения, данные группе Account** Operators, **применяются только к этому объекту** (This **Object Only).**

стр. 303

► Задание 4: просмотрите разрешения, назначаемые Active Directory по умолчанию для объекта-пользователя

4. Запишите в приведенную ниже таблицу группы, обладающие разрешениями доступа к учетной записи Secretary1. Эта информация понадобится вам на занятии 5. Если в диалоговом окне для какой-либо группы отображаются специальные разрешения, не включайте в список разрешения, для просмотра которых необходимо щелкнуть кнопку Advanced.

Табл. 11-6. Разрешения для объекта Security1

Группа	Установленные разрешения
Account Operators (Операторы учета)	Full Control (Полный доступ)
Administrators	Наследует все разрешения, кроме Full Control и Delete All Chile Objects (Удаление всех дочерних объектов), также имеет специальные разрешения
Authenticated Users	Разрешение Read для общей, личной и Web-информации
Cert Publishers	Специальные разрешения
Domain Admins	Full Control
Enterprise Admins	Наследует Full Control
Everyone	Change Password
Pre-Windows 2000 Compatible Access	Наследует разрешения Read (Чтение), Read Phone and Mail Options (Чтение Телефонные и почтовые параметры), Read General Information (Чтение Общие сведения), Read Group Membership (Чтение Членство в группах), Read Personal Information (Чтение Личная информация), Read Public Information (Чтение Публичная информация), Read Remote Access Information (Чтение Информация удаленного доступа), Read Information Logon (Чтение Информации о входе), Read Web Information (Чтение Информация о вебе) и Read Account Restrictions (Чтение Ограничения учетной записи)
RAS and IAS Servers	Разрешение Read Group Membership, Read Remote Access Information, Read Account Restrictions и Read Logon Information
SELF	Read, Change Password (Смена пароля), Receive As (Получить как), Send As (Отправить как), Read Phone and Mail Options, Read General Information, Read Group Membership, Read Personal Information, Read Public Information, Read Remote Access Information, Read Account Restrictions, Read Logon Information, Read Web Information; Write Phone and Mail Options, Write Personal Information и Write Web Information
SYSTEM	Full Control

Одинаковы ли обычные разрешения для объекта-пользователя и объекта-ОП? Почему?

Нет. Стандартные разрешения для каждого типа объектов разные. Причина этих различий в том, что разные типы объектов используются для разных задач, и поэтому требования безопасности для каждого типа объектов различаются.

Унаследованы ли какие-нибудь разрешения от родительского объекта Security1? Как это узнать?

От родительского объекта наследуются только стандартные разрешения, назначенные группам Administrators и Enterprise Admins. Флажки для унаследованных разрешений затенены.

Какими правами обладают члены группы Account Operators в отношении объекта-пользователя?

Группа Account Operators имеет разрешение Full Control. Член группы может совершать любые действия над объектом пользователя, включая его удаление.

Занятие 4. Перемещение объектов Active Directory

стр. 313

▶ Задание 2: зарегистрируйтесь в системе как пользователь, состоящий в нестандартном ОП

1. Зарегистрируйтесь в системе как User21.

Потребовала ли Windows 2000 указать ОП, к которому относится данная учетная запись? Почему?

Нет. Windows 2000 автоматически находит объект пользователя в Active Directory, вне зависимости от его расположения в иерархии каталога.

Занятие 5. Делегирование управления объектами Active Directory

стр. 316

▶ Задание 1: проверьте текущие разрешения

3. В дереве консоли раскройте свой домен и щелкните Securityl.

Какие объекты-пользователи отображаются в ОП Securityl?

Учетные записи Secretary1 и Assistant1 а также User20, User21 и User22.

Какие разрешения позволяют вам видеть эти объекты? (Совет: см. таблицы, заполненные вами на занятии 2.)

Учетная запись Assistant1 автоматически принадлежит встроенной группе Authenticated Users, которая имеет разрешение Read для данного ОП.

Для учетной записи Secretaryl измените время входа в систему. Удалось ли вам это? Почему?

Нет. Учетная запись Assistantl не имеет разрешение Write для объекта Secretaryl.

Измените время входа в систему для учетной записи Assistantl. Удалось ли вам это? Почему?

Нет. Учетная запись Assistantl не имеет разрешения Write для объекта Assistantl.

стр. **317**

▶ Задание 3: проверьте делегированные разрешения

4. Попытайтесь изменить время входа в систему для учетных записей из ОП Securityl.

Удалось ли вам это? Почему?

Да. Учетной записи Assistantl назначено разрешение Full Control для всех объектов в ОП, включая разрешение для настройки времени входа.

5. Попытайтесь изменить время входа в систему для учетной записи из контейнера Users.

Удалось ли вам это? Почему?

Нет. Учетная запись Assistantl не имеет никаких разрешений для контейнера Users.

стр. 333

Закрепление материала

1. Как глобальный каталог помогает пользователям искать объекты Active Directory?

Глобальный каталог содержит частичную копию всего каталога, поэтому он хранит информацию о каждом объекте в дереве доменов или лесе. Поскольку глобальный каталог содержит информацию о каждом объекте, пользователь может найти информацию вне зависимости от того, в каком домене, дереве или лесе содержатся данные. Active Directory автоматически генерирует содержимое глобального каталога из доменов, которые составляют каталог,

2. Вы хотите разрешить руководителю отдела продаж создавать, изменять и удалять учетные записи для подчиненных ему сотрудников. Как это сделать?

Поместите все учетные записи этого отдела в ОП, а затем делегируйте управление организационным подразделением руководителю отдела.

3. Что происходит с разрешениями объекта при перемещении его из одного ОП в другой?

Разрешения, назначенные непосредственно объекту, остаются теми же. Объект также наследует разрешения от нового ОП. Любые разрешения, ранее унаследованные от старого ОП, больше не влияют на объект.

4. На каком уровне позволяет настраивать административный контроль мастер Delegation Of Control?

   На уровне ОП или контейнера.

5. Какие данные надо архивировать для восстановления Active Directory? Что относится к этим данным?

   Необходимо *архивировать данные состояния* системы. Для Windows 2000 Server эти данные включают реестр, базу данных регистрации COM+, системные загрузочные файлы и базу данных служб сертификации (если этот сервер служб сертификации). Если сервер является контроллером домена, Active Directory и каталог SYSVOL также содержатся в данных состояния системы.

6. Как надо зарегистрироваться в системе при ее перезагрузке в режиме восстановления служб каталога? Почему?

   При перезагрузке компьютера в режиме восстановления служб каталогов надо войти в систему как Administrator, используя правильные имя и пароль учетной записи Security Accounts Manager SAM), но *не* учетную запись администратора Active Directory, так как службы Active Directory отключены, и нельзя их средствами проверить подлинность учетной записи. Для этого применяется база данных учетных записей SAM. Пароль учетной записи SAM задается в *процессе* установки Active Directory.

Глава 12 Администрирование групповой политики

Занятие 3. Внедрение групповой политики

стр. 363

▶ Задание: делегируйте управление ОГП

2. Щелкните корневой узел (Dispatch Policy [server1.microsoft.com] Policy) консоли правой кнопкой мыши, выберите команду Properties и перейдите на вкладку Security (Безопасность).

   Откроется диалоговое окно свойств для ОГП DispathPolicy.

   Какие группы безопасности обладают административными полномочиями в отношении ОГП DispatchPolicy?

   Domain Admins, Enterprise Admins и SYSTEM.

стр. 363

▶ Задание: настройте параметры групповой политики для ОГП

3. Щелкните элемент Start Menu & Task Bar (Панель задач и меню «Пуск»).

   Что отображается в правой панели?

   Политики, доступные в категории Start Menu & Task Bar.

5. Щелкните переключатель Enabled (Включена), затем — OK.

   Как быстро определить, что этот параметр включен?

   Параметр отображается как включенный в правой панели.

стр. 365

▶ Задание: проверьте ОГП DispatchPolicy

2. Нажмите комбинацию клавиш Ctrl+Alt+Delete.

   Откроется диалоговое окно Windows Security (Безопасность Windows).

   Можете ли вы заблокировать рабочую станцию? Почему?

   Нет, кнопка Lock Computer недоступна. Assistant1 не может блокировать рабочую станцию, поскольку в упражнении 8 вы создали привязку ОГП DispatchPolicy к ОП Security1.

3- Щелкните кнопку Cancel (Отмена) и раскройте меню Start.
Отображаются ли в меню Start команды Search (Найти) и Run (Выполнить)?

Нет.

7. Нажмите комбинацию клавиш Ctrl+Alt+Delete.
Можете ли вы заблокировать рабочую станцию? Почему?

Да, поскольку кнопка Lock Computer доступна. **Assistant I может блокировать компьютер, поскольку** группа **Sales была** отфильтрована из области **действия ОГП Dispatch** Policy **в упражнении 7.**

стр. 395

Закрепление материала

1. Что такое ОГП?
ОГП — это объект **групповой политики, где хранятся параметры конфигурации групповой политики.** Каждый **компьютер с** Windows 2000 **имеет** один **локальный ОГП и на него может распространяться действие любого числа нелокальных ОГП (хранимых в Active Directory).**

Один локальный ОГП хранится на каждом **компьютере вне зависимости от того, является ли компьютер частью среды Active Directory или сетевой среды. Локальные параметры ОГП могут перекрываться нелокальными ОГП.**

Нелокальные ОГП сопоставляются **объектам Active** Directory **(сайтам, доменам или ОП) и могут** быть применены **как** к **пользователям, так** и к компьютерам. **Для использования нелокальных ОГП** необходим **контроллер домена Windows** 2000. **Следуя свойствам Active Directory, нелокальные ОГП** применяются **иерархически,** от сайтов к **ОП; их** параметры **суммируются по аналогии с наследованием** разрешений.

2- Назовите два вида параметров групповой политики и расскажите, как они используются.
Это параметры конфигурации **компьютера и параметры конфигурации пользователя. Первые служат для настройки** групповых политик, **применяемых к компьютерам, вне зависимости от того,** кто **на нем** работает. **Вторые реализуются при старте** операционной **системы для** применения **групповых политик** пользователя **вне зависимости от того, на каком компьютере он работает,**

3. Опишите порядок применения групповой политики в структуре Active Directory.
Групповая **политика** применяется в следующем **порядке: сайт, домен, затем ОП.**

4. Перечислите задачи по внедрению групповой политики,
К ним относится: создание ОГП, создание оснастки **для ОГП, делегирование административного** управления ОГП, настройка параметров групповой **политики для ОГП, запрещение неиспользуемых параметров групповой** политики, отображение **любых исключительных ситуаций при обработке ОГП, фильтрование области действия ОГП и привязка ОГП к сайту, домену или ОП.**

5. В чем отличие параметров Block Policy Inheritance и No Override?
Параметр **Block** Policy **Inheritance применяется непосредственно к сайту, домену нли ОП. Он не применяется к ссылкам ОГП и отклоняет** *все* **параметры групповой политики, которые применяются к сайту,** домену **или ОП по иерархии, вне зависимости от того, от какого ОГП эти параметры** были **получены. Ссылки ОГП,** для которых **задано No Override, применяются** всегда и не могут **быть заблокированы параметром Block** Policy **Inheritance.**

Для любого **ОГП, связанного с сайтом, доменом или ОП (нелокальный), разрешается задать параметр** No Override **в отношении данного сайта, домена или ОП, чтобы никакие его политики не перекрывались. Если** параметр **No Override задан для нескольких ОГП в иерархии, приоритет отдается наивысшему в иерархии Active Directory (либо наивысшему в иерархии, заданной администратором на каждом фиксированном** уровне **Acitve Directory). Параметр No Override применяется к** ссылке **на ОГП.**

6. Чем отличается публикация приложения от его назначения?
Приложение назначается, если его надо установить на компьютерах всех пользователей. Приложение можно опубликовать как для **компьютеров,** так и для **пользователей.**

Приложение публикуется, чтобы сделать его доступным пользователям соответствующего ОГП, затребовавшим приложение. При публикации приложения каждый человек сам решает, устанавливать его или нет. Приложение можно публиковать только для пользователей.

7. Какие **папки** можно перенаправлять?

   Application Data, Desktop, My Documents, My Pictures и Start Menu.

Глава 13 Администрирование конфигурации безопасности

Занятие 2. Аудит

стр. 415

Упражнение 1: проектирование политики аудита домена

Принятые решения запишите в таблицу (табл. 13-7).

Ответы могут варьироваться. Возможны следующие ответы: Account logon events: Неудача (для аудита попыток входа в сеть); Account management: Успех (для аудита административных действий); Directory service access: Неудача (для аудита неавторизованного доступа); Logon events: Неудача (для аудита попыток входа в сеть); Object access: Успех (для аудита использования принтера) и Неудача (для аудита неавторизованного доступа); Policy change: Успех (для аудита административных действий); Privilege use: Успех (для аудита административных действий и процедур резервного копирования); Process tracking: не выполнять аудит (главным образом для разработчиков); System events: Успех и Неудача (для аудита попыток взлома сервера).

стр. 417

▶ Задание: проверьте аудит **объекта Active Directory**

6. В диалоговом окне Access **Control** Settings For Users перейдите на вкладку Auditing и дважды щелкните группу Everyone.

   Откроется диалоговое окно Auditing Entry For Users.

   Просмотрите стандартные параметры аудита доступа к объекту для группы Everyone. Чем отличаются виды доступа, для **которых** выполняется аудит, от тех, для которых он не выполняется?

   Выполняется аудит всех типов доступа, которые способны изменить объект; типы доступа, которые не приводят к изменению объекта, не отслеживаются.

7. Щелкайте OK, **чтобы закрыть** окна Auditing Entry For **Users,** Access Control Settings **For** Users и Users Properties.

   На каких компьютерах будет **регистрироваться** доступ к объекту Active **Directory?** Сможете ли вы просмотреть журнал?

   Windows 2000 записывает отслеживаемые события доступа к Active Directory на контроллерах домена, на уровне ОП. Поскольку вы настроили аудит контроллера домена, вы сможете просматривать события доступа в Active Directory. Если вы настроили аудит для локального компьютера или для политики домена но умолчанию, вы не сможете просматривать события доступа в Active Directory.

стр. 450

Закрепление материала

1. Необходимо осуществить аудит доступа к папке, расположенной на рядовом сервере домена. **На каком** компьютере следует настроить **политику** аудита?

   Надо настроить политику аудита на рядовом сервере, так как это делается на том компьютере, где расположена папка.

2. В чем разница между параметрами политики аудита, которые отслеживают доступ к службе каталогов и доступ *к* объектам?

   Первая отслеживает, когда пользователь получает доступ к объекту Active Directory, а вторая — когда пользователь получает доступ к файлу, папке или принтеру.

3. Как при просмотре журнала безопасности определить успешность или неудачу события?

   Успешные события отображаются **со значком ключа, а неуспешные — со значком замка.**

4. Чем права пользователя отличаются от разрешений?

   Права пользователей применяются к их учетным записям, а разрешения — к объектам.

5. Что такое шаблон безопасности и для чего он используется?

   Шаблон безопасности - это физическое представление конфигурации безопасности, одиночный файл, в котором записан набор параметров безопасности. Хранение всех параметров безопасности в одном месте упрощает администрирование.

6. Где консоль Security Configuration and Analysis хранит информацию, необходимую для настройки конфигурации и анализа?

   В специальной базе данных.

Глава 14 Управление производительностью Active Directory

стр. 482

Закрепление материала

1. Что рекомендуется предпринять в первую очередь при неполадках в работе Active Directory?

   Вы должны проверить журнал событий службы каталогов в Event Viewer.

2. Чем различаются объект и счетчик производительности?

   Объект производительности — это логическое объединение счетчиков производительности, ассоциированных с наблюдаемым ресурсом или службой. Счетчик производительности — это условие, которое применяется к объекту производительности.

3. Чем различаются журнал счетчиков и трассировочный отчет?

   Журналы счетчиков собирают данные счетчиков производительности в указанном интервале. Журналы трассировки записывают данные, собираемые поставщиком операционной системы или несистемными поставщиками, когда происходят определенные действия, например операции дискового ввода-вывода или ошибки страниц. При использовании журналов счетчиков служба Performance Logs and Alerts получает данные от системы по истечении интервала обновления, вместо того чтобы ждать конкретного события, как в случае с журналами трассировки.

4. Какие действия может вызывать оповещение?

   Оповещения выводят записи в журнал событий приложений, отправляют компьютеру сообщения по сети, запускают журнал данных производительности или программу, когда значение счетчика предупреждений выходит из указанного интервала.

5. Какие возможности предоставляет администратору утилита LDP и как ее запустить?

   Утилита Active Directory Replication Monitor позволяет администраторам просматривать низкоуровневый статус репликации Active Directory, принудительно запускать синхронизацию между контроллерами домена, просматривать топологию и отслеживать состояние и производительность репликации контроллеров домена в графическом виде. Active Directory Replication Monitor — это графическая утилита, доступная из программной группы Windows 2000 Support Tools.

6. Как узнать, какие файлы общей папки открыты и кто к ним подключен?

   Надо раскрыть меню Start\Programs\Administrative Tools и щелкнуть Computer Management. В дереве консоли под Shared Folders нужно щелкнуть Open Files.

Глава 15 Установка Windows 2000 с использованием RIS

стр. 518

Закрепление материала

1. Что такое службы удаленной установки? Какие типы удаленной загрузки поддерживает RIS?

   Службы удаленной установки (Remote Installation Services, RIS) — это программные службы, позволяющие администратору настраивать новые клиентские компьютеры удаленно со своего рабочего места. Клиенты должны поддерживать удаленную загрузку. Существуют два типа клиентов с возможностью удаленной загрузки: компьютеры с ПЗУ, поддерживающим среду PXE и функции DHCP, и компьютеры с сетевыми адаптерами, поддерживаемыми загрузочным диском RIS.

2. Что предоставляет технология удаленной загрузки PXE?

   PXE — это новая форма технологии удаленной загрузки. PXE позволяет использовать существующую инфраструктуру TCP/IP с серверами DHCP для обнаружения в сети серверов RIS. Системы, совместимые с Net PC/PC98, могут использовать преимущества удаленной загрузки, реализованной в Windows 2000, Net PC/PC98 — это ежегодное руководство для изготовителей оборудования, разработанное Microsoft и Intel с уметом предложений Compaq и других изготовителей устройств. PC9S предлагается как стандарт для разработки оборудования и позволяет Microsoft включать расширенные возможности, подобные RIS. в платформу Windows.

3. Что такое загрузочный диск служб удаленной установки?

   Для удаленноu загрузки компьютеров с ПЗУ, не поддерживающим PXE, в Windows 2000 предусмотрено средство создания специального загрузочного диска. Диск удаленной загрузки RIS может использоваться с множеством сетевых адаптеров на шине PCI. Использование загрузочного диска RIS устраняет необходимость переоснащения клиентских компьютеров новыми сетевыми адаптерами с PXE-совместимым ПЗУ. Загрузочный диск RIS имитирует последовательность удаленной загрузки PXE и поддерживает наиболее распространенные сетевые адаптеры.

4. Что такое образ RIPrep?

   Программа RIPrep позволяет сетевому администратору копировать стандартную корпоративную конфигурацию компьютера, дополненную конфигурациями ОС, рабочего стола и локально установленными приложениями. После первой установки и настройки ОС Windows 2000 Professional, ее служб и любых стандартных приложений на компьютер сетевой администратор запускает мастер, который создает образ установки н копирует его на доступный в сети сервер RIS для установки на клиенты.

   Что представляет собой мастер установки клиентов?

   Мастер установки клиента (Client Installation Wizard, CIW) позволяет клиентам выбирать параметры установки, операционную систему и средства устранения неполадок. Мастер предлагает пользователю ввести имя, пароль и имя домена. Подтвердив личность пользователя, мастер отображает доступные пользователю параметры установки. После того, как пользователь задаст параметры, указанный установочный образ ОС копируется на локальный жесткий диск клиентского компьютера.

Приложение Б

Установка и настройка службы DHCP

Для использования *служб удаленной установки* (Remote Installation Services, RIS) требуется установить и настроить службы DHCP на индивидуальных серверах или на том же сервере, что и RIS.

Примечание Данное приложение содержит только основные инструкции по установке и настойке службы DHCP. Подробнее эта тема изложена в учебном курсе MCSE — «Администрирование сети на основе Windows 2000» («Русская Редакция», 2001).

Установка службы DHCP

Первый этап внедрения DHCP — установка службы DHCP, Прежде всего, для привязанной к TCP/IP сетевой платы сервера необходимо указать статический IP-адрес, маску подсети и шлюз по умолчанию.

► **Установка службы DHCP**

1. Раскройте меню Start\Settings (Пуск\Настройки), щелкните ярлык Control Panel (Панель управления) и в окне окно Add/Remove Programs (Установка и удаление программ) щелкните кнопку Add/Remove Windows Components (Добавление и удаление компонентов Windows).
2. В окне мастера компонентов Windows выберите Networking Services (Сетевые службы) и щелкните кнопку Details (Состав).
3. В перечне компонентов сетевых служб пометьте флажок Dynamic Host Configuration Protocol (DHCP) и шелкните OK.
4. Щелкните Next для установки выбранных компонентов.
5. Когда появится соответствующее предложение, вставьте установочный компакт-диск Windows 2000 Server.
6. В окне мастера Completing The Windows Components Wizard (Завершение работы мастера компонентов Windows) шелкните кнопку Finish (Готово).
7. Закройте диалоговое окно Add/Remove Programs (Установка и удаление программ).
8. Закройте окно Control Panel и выньте из дисковода установочный компакт-диск Windows 2000 Server.

Примечание Служба DHCP автоматически активизируется во время установки; для обеспечения связи с клиентами DHCP она должна быть запущена.

Настройка службы DHCP

Основные задачи настройки службы DHCP — создание и настройка области DHCP, а также настройка резервирования IP-адресов.

Создание области DHCP

Прежде чем сервер DHCP сможет предоставить клиентам IP-адреса, необходимо создать *область* (scope) DHCP — пул действительных IP-адресов, предназначенных для клиентов DHCP. Создание области DHCP — следующий шаг после установки и запуска службы DHCP.

Создавая область DHCP, помните:

- для каждого сервера DHCP необходимо определить минимум одну область;
- исключите из области статические IP-адреса;
- для централизации администрирования и выделения IP-адресов, характерных для подсети, на сервере DHCP можно определить несколько областей; конкретной подсети разрешается задать лишь одну область;
- информация об областях не является общей для серверов DHCP, поэтому при создании областей на нескольких серверах убедитесь, что в них нет одинаковых IP-адресов — это поможе г избежать проблем с идентичными IP-адресами.

▶ **Создание области DHCP**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование), затем щелкните DHCP.
2. В дереве консоли щелкните правой кнопкой узел сервера DHCP и выберите команду New Scope (Создать область) для запуска мастера создания области.
3. Щелкните Next.
4. В поле Name (Имя) окна Scope Name (Имя области) задайте имя создаваемой области. В поле Description (Описание) можно ввести ее описание. Затем щелкните Next.
5. В окне IP Address Range (Диапазон адресов) определите диапазон IP-адресов, включенных в область. Маску подсети определяют по длине или как IP-адрес. Затем щелкните кнопку Next.
6. В окне Add Exclusions (Добавление исключений) определите любые адреса, которые будут исключены из области, затем щелкните Next.

Примечание Исключение — это адрес или диапазон адресов, которые сервер не выделяет. Можно исключить несколько диапазонов адресов.

---

7. В окне Lease Duration (Срок действия аренды адреса) определите продолжительность использования клиентом IP-адреса из данной области сервера DHCP, затем щелкните Next.
8. В окне Configure DHCP Options (Настройка параметров DHCP) определите, хотите вы настроить основные параметры DHCP сейчас или сделаете это позже, затем шелкните Next,
9. Если вы решили настраивать основные параметры DHCP позже, перейдите к пункту 12.
10. Если вы решили настраивать основные параметры DHCP сейчас, то выполните следующие действия:
    - в окне Router (Default Gateway) [Маршрутизатор (основной шлюз)] задайте IP-адреса маршрутизаторов или шлюзов по умолчанию, распределяемых данной областью, затем шелкните Next;
    - в окне Domain Name And DNS Servers (Имя домена и DNS-серверы) укажите имя родительского домена, которое будет использоваться клиентскими компьютерами для разрешения имен средствами DHCP. Если вы хотите, чтобы клиенты области использовали DNS-серверы, введите имена и IP-адреса этих серверов. Затем щелкните Next;
    - в окне WINS Servers (WINS-серверы) определите имена и IP-адреса серверов, чтобы позволить клиентам запрашивать WINS до того, как они смогут пользоваться широковещательными сообщениями для регистрации и разрешения имен NetBIOS. Затем щелкните Next.
11. В окне Activate Scope (Активизировать область) определите, будете вы активизировать область сейчас или сделаете это позже, затем шелкните Next.

Примечание При создании область необходимо активизировать, чтобы она стала доступной для распределения аренды.

12. В окне Completing The New Scope Wizard (Завершение работы мастера создания области) щелкните кнопку Finish (Готово).

Внимание! Для создания новой маски или диапазона IP-адресов область необходимо удалить и повторно создать.

Настройка области DHCP

Создав область, настройте параметры клиентов DHCP. Есть два главных уровня параметров области — сервера и области.

Параметры сервера

Доступны всем клиентам DHCP. Их применяют, если всем клиентам во всех подсетях нужна одинаковая информация о параметрах. Например, чтобы все клиенты использовали один WINS-сервер. Параметры сервера всегда применяются, если не заданы параметры области или клиента.

► **Настройка параметров сервера DHCP**

1. В оснастке DHCP щелкните правой кнопкой папку Server Options (Параметры сервера) и выберите команду Configure Options (Настроить параметры).
2. Выберите в списке параметр DHCP, который необходимо настроить, введите в поле Data Entry (Запись данных) соответствующее значение и щелкните OK.

Параметры области

Доступны только клиентам, арендующим адреса из определенной области. Например, если для каждой подсети вы определили разные области, для них разрешается задать и уникальные адреса шлюзов по умолчанию. Параметры области перенастраивают параметры сервера.

► Настройка **параметров области DHCP**

1. В оснастке DHCP раскройте узел области.
2. Щелкните правой кнопкой значок Scope Options (Параметры области) и выберите команду Configure Options (Настроить параметры).
3. Выберите в списке параметр DHCP, который хотите настроить, введите в поле Data Entry соответствующее значение и щелкните OK.

Настройка резервирования IP-адреса

Для некоторых клиентов DHCP важно, чтобы по окончании срока аренды им был выделен тот же самый IP-адрес. Для них можно зарезервировать IP-адрес. Тогда служба DHCP всегда будет присваивать им один и тот же IP-адрес. Например, если сервер SRV187 находится в сети, клиентов которой не поддерживает WINS, для SRV187 необходимо настроить резервирование IP-адреса. После этого он всегда будет получать с сервера DHCP один и тот же IP-адрес. Клиенты этой сети без поддержки WINS для разрешения NetBIOS-имен компьютеров используют файл LMHOSTS. Поскольку это статический файл, содержащий привязку NetBIOS-имени к IP-адресу, в случае смены IP-адреса сервера SRV187 при разрешении имен с помощью файла LMHOSTS произойдет ошибка.

► **Настройка резервирования IP-адреса**

1. В оснастке DHCP раскройте узел области, щелкните правой кнопкой узел Reservations (Резервирование) и выберите команду New Reservation (Создать резервирование).

2. В поле Reservation Name (Имя клиента) введите имя для идентификации клиента. Для идентификации клиента консоль DHCP использует имя, связанное с аппаратным адресом сетевого адаптера.
3. В поле IP Address (IP-адрес) введите IP-адрес, который вы хотите зарезервировать для конкретного клиента.
4. В поле MAC Address (MAC-адрес) введите аппаратный адрес сетевого адаптера клиента. Дефисы вводить не надо.

Внимание! Неверно введенный MAC-адрес не будет соответствовать значению, посылаемому клиентом DHCP, и служба DHCP вместо зарезервированного IP-адреса выделит данному клиенту один из доступных адресов.

5. В поле Description (Описание) введите описание клиента.
6. В группе Supported Types (Поддерживаемые типы) укажите, для каких клиентов разрешено резервирование:
   - Both (Оба) — резервирование IP-адреса разрешено и клиентам DHCP, и клиентам BOOTP.
   - DHCP Only (Только DHCP) — резервирование IP-адреса разрешено только клиентам DHCP.
   - BOOTP Only (Только BOOTP) — резервирование IP-адреса разрешено только клиентам BOOTP.
7. Щелкните кнопку Add (Добавить), чтобы добавить это резервирование в базу данных области.

Предметный указатель

B

C

D

M

N

O

P

T

U

V

W

Z

А

Б

В

Г

Д

Ж

З

И

К

P

Ф

Х

Ц

Ш

Э

Microsoft Corporation

Microsoft Windows 2000 Active Directory Services

Учебный курс MCSE

3-е издание, исправленное

Перевод с английского под общей редакцией А. **И. Иванова**

Переводчики **А. В. Иванов, А. П. Харламов**

Редактор **Ю. П. Леонова**

Технический редактор **Н. Г. Тимченко**

Корректор Л. **А. Панчук**

Компьютерный дизайн и подготовка иллюстраций
Д. **В. Петухов, Е. В. Козлова**

Дизайнер обложки **Е. В. Козлова**

Оригинал-макет выполнен с использованием
издательской системы Adobe PageMaker 6.0

Para(-)Type

TypeMarketFontLibrary
легальный пользователь

Главный редактор **А. И. Козлов**

Подготовлено к печати издательством «Русская Редакция»
121087, Москва, ул. Антонова-Овсеенко, *д.* 13
тел.: (095) 256-5120, тел./факс: (095) 256-4541
e-mail: info@rusedit.ru, http:// www.rusedit.ru

РУССКАЯ РЕДАКЦИЯ

Подписано в печать 16.02.2004 г. Тираж 2000 экз.
Формат 70x100¹/16. Физ. п.л, 38

Отпечатано в ОАО «Типография "Новости"»
107005, Москва, ул. Фр. Энгельса, 46

Хотите сэкономить на обучении до $1000?

Издательство «Русская Редакция» и учебный центр компании «Инвента» проводят конкурс «Читатель месяца» и будут ежемесячно выбирать двух самых активных читателей книг серии «Учебный курс».

Просто вырежьте купон из книги, помеченной на обложке специальным значком «Читатель месяца», и пришлите нам по адресу: **123317, Россия, г. Москва, ул. Антонова-Овсеенко, д. 13. Издательство «Русская Редакция».**

Лотерея определит победителей месяца. Один купон — один голос!
Чем больше купонов вы пришлете, тем больше у вас шансов выиграть!

Призы победителям — бесплатное обучение в учебном центре «Инвента» в Москве!

Но это не все! Помимо выбранного вами курса по программе сертификации Microsoft, победителей ждут и другие призы — скидка на дальнейшее обучение в учебном центре и подарок от "Русской Редакции».

Подробности конкурса — на сайте издательства «Русская Редакция» (*www.rusedit.ru/bonus*) и на сайте компании «Инвента» (*www.inventa.ru*). Там же все новости о конкурсе и о победителях. Телефон для справок (095) 775-8777

КОНКУРС

Купон участника конкурса «Читатель месяца»

И РУССКАЯ РЕДАКЦИЯ

ИНВЕНТА

Ф. И. О.:

E-mail:

Телефон:

Род занятий:

ВНИМАНИЕ! Незаполненные купоны не принимаются.

Конкурс проводится исключительно за счет устроителей и данный купон не может рассматриваться как коммерческое предложение.

Купон из книги **Microsoft Windows 2000 Active Directory Services. Учебный курс** MCSE.
Экз. № 70-217. ISBN 5-7502-0247-X