13. Лекция: Вопросы безопасности Windows Server

В лекции рассмотрены вопросы безопасности в ОС Windows, настройка данной ОС, управление пользователями и системой.

В системе Microsoft Windows были, по большей части, заменены внутренние и внешние настройки, присутствовавшие в Windows NT. Без сомнения, Windows является одной из наиболее передовых операционной системой в отношении интернета. Также очевиден тот факт, что в Windows сохранены традиционные возможности, такие как серверы файлов, печати и баз данных для внутреннего пользования, а также веб-серверы и серверы приложений для работы с интернетом. Дополнительные возможности, такие как сервер telnet, позволяют выполнять в Windows те функции, которые зарезервированы для систем Unix. Несмотря на то, что эти функции могут использоваться, совершенно понятно, что в Windows будет храниться и осуществляться работа с секретной информацией. Windows (ранее Windows.NET) призвана вывести операционную систему на новый уровень с замещением общих для предыдущих версий установок, имеющихся в Windows. Windows специально разрабатывалась как сервер (у нее нет версии для рабочих станций) и, как и предполагалось, начала быстро внедряться в организации.

Мы будем обсуждать основные этапы настройки имеющейся системы, а также то, как правильно осуществлять управление пользователями в домене Windows. Мы обсудим вопросы управления системой с точки зрения безопасности. В последнем разделе этой лекции мы попытается определить ключевые признаки вторжений, на которые должны обращать внимание администраторы во время своей работы.

Настройка системы

В Windows добавлены серьезные функции безопасности к тем возможностям, которые имели место в Windows NT. Как вы увидите в следующих разделах, польза от этих новых возможностей довольно ощутима. К сожалению, их использование требует гомогенной среды Windows. При использовании в смешанных средах Windows и Windows NT в системе должны быть установлены самые "слабые" настройки Windows NT для обеспечения взаимодействия.

Windows не является защищенной системой сразу после установки (хотя уровень ее защиты по умолчанию выше, чем у Windows NT). Имея это в виду, необходимо произвести настройку некоторых параметров для повышения уровня безопасности, прежде чем система будет готова к работе. Параметры конфигурации подразделяются на параметры локальной политики безопасности и параметры конфигурации системы.

Параметры локальной политики безопасности

В Windows появилось новое средство - графический пользовательский интерфейс редактирования локальной политики. Чтобы запустить эту утилиту, откройте Control Panel/Administrative Tools/Local Security Policy (Панель управления/Администрирование/Локальная политика безопасности) (см. рис. 13.1). Это средство позволяет настраивать политики учетных записей и локальные политики безопасности. Позже мы обсудим конфигурирование учетной записи. Сейчас давайте сконцентрируем внимание на локальных политиках безопасности.

Графический пользовательский интерфейс локальных политик безопасности в действительности является лишь внешней оболочкой процесса внесения изменений в реестр. Следовательно, для внесения изменений в общие параметры реестра больше не требуется использовать программы regedit или regedit32 - лучше использовать утилиту, чем открывать реестр и вносить изменения собственноручно.

На рисунке 13.2 показаны элементы политики безопасности, которые можно настраивать через графический пользовательский интерфейс локальных политик безопасности. В следующих разделах более подробно обсуждаются рекомендуемые изменения для внесения в политику безопасности.

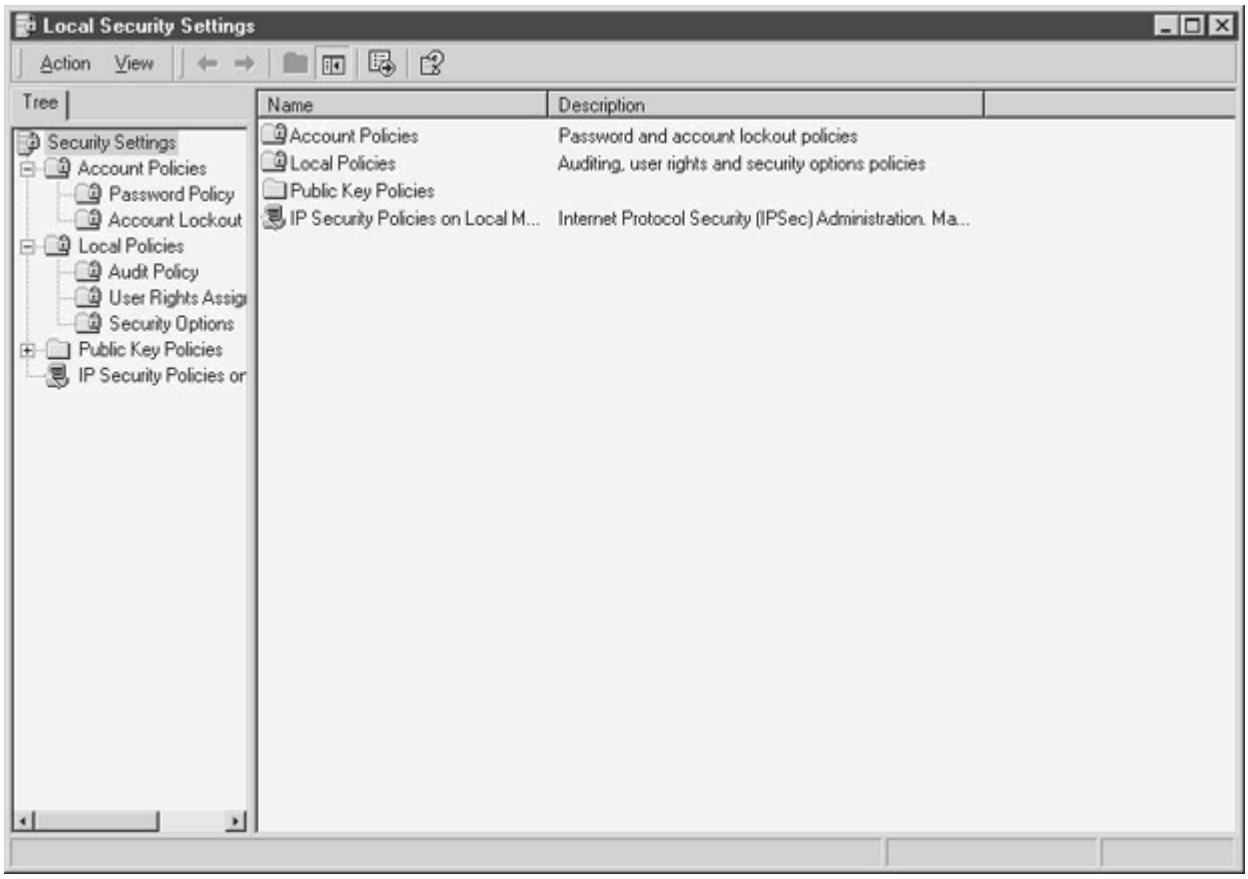

Рис. 13.1. Графический пользовательский интерфейс управления локальными политиками безопасности

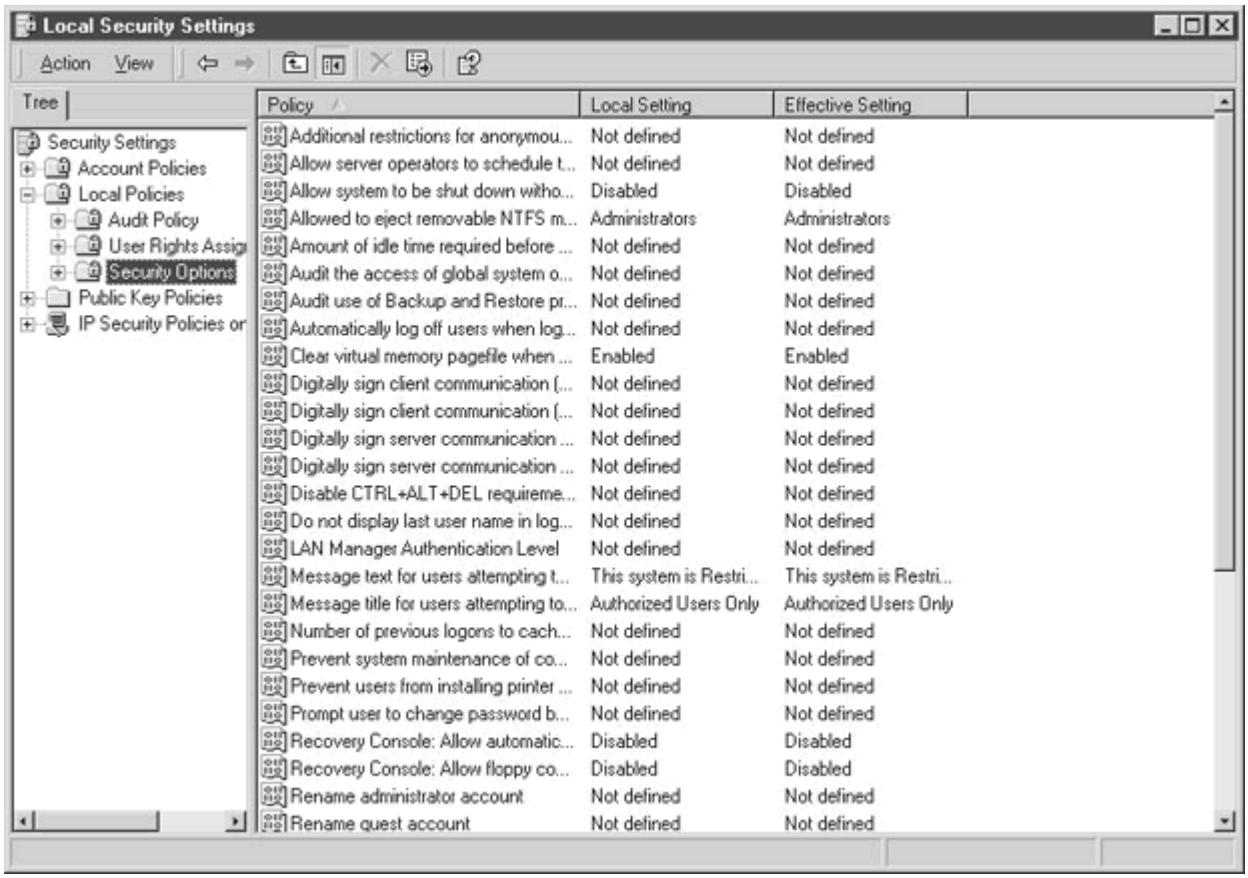

Рис. 13.2. Настраиваемые элементы локальной политики безопасности

Примечание

Windows содержит набор шаблонов, которые используются для конфигурации системы, настройки локальной политики безопасности и параметров управления пользователями в системе. Если вы будете использовать один из этих шаблонов, убедитесь, что вам понятны изменения, которые будут внесены в систему.

Сообщение входа

В Windows имеются два параметра, настраивающие сообщение входа, отображаемое пользователям:

- Message Text for Users Attempting to Log On (Текст сообщения для пользователей, пытающихся осуществить вход);
- Message Title for Users Attempting to Log On (Название сообщения для пользователей, пытающихся осуществить вход);

Очистка файла виртуальной памяти при отключении системы

Страничный файл виртуальной памяти содержит важную системную информацию во время работы системы, такую как ключи шифрования или пароли. Чтобы Windows очищала системный страничный файл при отключении системы, включите параметр Clear Virtual Memory Pagefile When System Shuts Down (Очистить файл подкачки при отключении системы).

Разрешить отключение системы без осуществления входа

Пользователи не должны иметь возможность отключать системы, если они не могут осуществлять вход. Следовательно, опция Allow System to Be Shut Down Without Having to Log On (Разрешить отключение системы без входа) должна быть отключена.

Уровень аутентификации LAN Manager

Аутентификация LAN Manager - это система аутентификации, позволяющая серверам Windows работать с клиентами Windows. Схемы аутентификации LAN Manager значительно более слабы, нежели система аутентификации NT или Windows (которая называется NTLM v2) и, таким образом, могут позволить злоумышленнику произвести атаку грубой силой на зашифрованные пароли с использованием гораздо меньших вычислительных мощностей. Чтобы в принудительном порядке использовать аутентификацию NTLM v2, примените следующие параметры.

1. Выберите параметр политики LAN Manager Authentication Level (Уровень аутентификации LAN Manager).
2. Выберите соответствующий уровень в ниспадающем меню.

Устанавливаемое значение зависит от рассматриваемой среды. Существуют шесть уровней:

- Send LM and NTLM Responses (Отправлять ответы LM и NTLM). Это уровень по умолчанию. Происходит отправка обоих ответов - LAN Manager и NTLM. В системе никогда не будет использоваться защита сеанса NTLM v2;
- Send LM и NTLM, Use NTLM v2 If Negotiated (Отправка LM и NTLM, использование NTLM v2 при согласии);
- Send NTLM Response Only (Отправлять только ответ NTLM);
- Send NTLM v2 Response Only (Отправлять только ответ NTLM v2);
- Send NTLM v2 Response Only, Refuse LM (Отправка только ответа NTLM v2, отклонение LM);
- Send NTLM v2 Response Only, Refuse LM and NTLM (Отправка только ответа NTLM v2, отклонение LM и NTLM).

Дополнительные ограничения для анонимных соединений

Этот параметр политики позволяет администратору определить, какие действия разрешены для выполнения через анонимное соединение. Он имеет три опции:

- None, Rely On Default Permissions (Нет ограничений, использовать разрешения по умолчанию);
- Do Not Allow Enumeration of SAM Accounts and Shares (Запретить перечисление учетных записей и общих местоположений в SAM);
- No Access Without Explicit Anonymous Permissions (Запретить доступ без отдельных разрешений на анонимный доступ).

Эти параметры могут предотвратить получение доступа к информации о пользователях системы при работе в недействительных пользователей через недействительные сеансы.

Дополнительные параметры локальной политики безопасности в Windows Единственным отличием локальных политик безопасности Windows Server и Windows являются политики ограничения программного обеспечения (Software Restriction Policies) (см. рис. 13.3). Политики ограничения программного обеспечения позволяют осуществлять контроль над тем, какие программы могут выполняться на данном локальном компьютере. Преимуществом этой возможности является то, что администратор может указывать, выполнение каких программ разрешено в системе, и, таким образом, предотвращать выполнение программ, не пользующихся доверием.

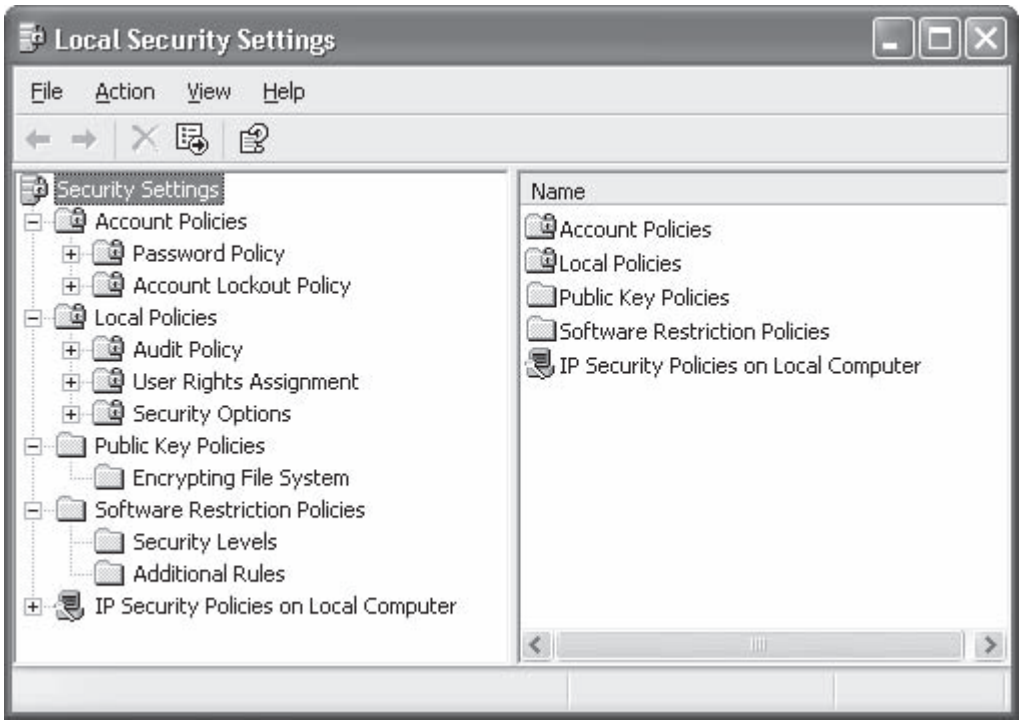

Рис. 13.3. Политика ограничения программного обеспечения для локальной системы

Вы можете определить уровень безопасности по умолчанию Unrestricted (Без ограничений) (разрешить все, что не запрещено) или Disallowed (Запрещено) (Запретить все, что не разрешено). Последний вариант лучше с точки зрения безопасности, однако при его использовании могут возникнуть проблемы из-за того, что этот уровень окажется слишком ограничительным. Настоятельно рекомендуется потратить время на то, чтобы проверить эти настройки на тестовой системе, перед тем как применять их на работающих системах.

После установки уровня по умолчанию можно указать исключения в данном уровне безопасности посредством создания правил политики ограничения программного обеспечения для конкретных программ. Исключения могут быть указаны на основе программного обеспечения:

- хеши;
- сертификаты;
- пути (включая путь реестра);
- зоны интернета.

Некоторые примеры действий, которые можно реализовать посредством политик ограничения программ:

- запрет на запуск определенных типов файлов в каталоге вложений электронной почты используемой почтовой программы;
- ограничение того, какие программы могут запускаться пользователями на серверах терминала.

Примечание

Политики ограничения программ не должны использоваться вместо антивирусного программного обеспечения.

Конфигурация системы

Существует несколько различий между Windows и Windows NT в плане конфигурации системы. В Windows включены новые функции безопасности, однако следует понимать, в чем заключаются преимущества и недостатки каждой новой возможности. В следующих разделах мы будем обсуждать четыре основные темы:

- файловые системы;
- параметры сети;
- параметры учетных записей;

- сервис-пакеты и "горячие" обновления.

Политика безопасности организации в обязательном порядке должна предусматривать определенные параметры и требования к конфигурации системы.

Файловые системы

Все файловые системы в Windows должны быть преобразованы в NTFS. Так как файловые системы FAT не позволяют использовать разрешения файлов, NTFS лучше с точки зрения безопасности. Если какая-либо из имеющихся файловых систем является системой FAT, можно использовать программу CONVERT, чтобы сменить их на NTFS. Эта программа требует перезагрузки, однако ее можно выполнить с уже имеющейся информацией на диске.

Также следует заметить, что Windows поставляется с новой версией NTFS - NTFS-5. NTFS-5 содержит новый набор индивидуальных разрешений:

- проход по папке/выполнение файла;
- просмотр папки/чтение данных;
- чтение атрибутов;
- чтение расширенных атрибутов;
- создание файлов/запись данных;
- создание папок/присоединение данных;
- запись атрибутов;
- запись расширенных атрибутов;
- удаление подпапок и файлов;
- удаление;
- чтение разрешений;
- изменение разрешений;
- присвоение прав владения.

Перед тем как включать Windows в работу, администраторы и сотрудники отдела безопасности должны разобраться в новых разрешениях и просмотреть структуру разрешений для файлов и каталогов.

Шифрующая файловая система. Одним из недостатков файловой системы NTFS является то, что она защищает файлы только тогда, когда используется с Windows NT или Windows. Если злоумышленник загрузит систему с использованием другой операционной системы (например, DOS), он сможет использовать программу (такую как NTFSDOS) для чтения файлов и, таким образом, обойдет элементы управления доступом NTFS. В Windows введена файловая система Encrypting File System (EFS) для защиты секретных файлов от атак данного типа.

EFS реализована таким образом, чтобы быть незаметной для пользователя. Следовательно, пользователю не требуется инициировать дешифрование или шифрование файла (после применения EFS для файла или каталога). Чтобы активизировать EFS, выберите файл или каталог, который нужно защищать, щелкните правой кнопкой на этом элементе и выберите Properties (Свойства). Нажмите кнопку Advanced (Дополнительно) в окне General (Общие) и выберите Encrypt Contents to Secure Data (Шифровать содержимое для защиты данных).

Когда для файла назначено шифрование, система выбирает ключ для использования в алгоритме симметричного шифрования и шифрует данный файл. После этого ключ шифруется с использованием открытого ключа одного или нескольких пользователей, которые будут иметь доступ к файлу. Здесь следует заметить, что EFS имеет встроенный механизм, позволяющий осуществлять восстановление зашифрованной информации. По умолчанию из локальной учетной записи администратора всегда можно расшифровать любые файлы EFS.

В зависимости от способа взаимодействия EFS с пользователем и операционными системами некоторые команды будут приводить к расшифровыванию файлов, а другие - нет. Например, команда Ntbackup копирует зашифрованный файл в том виде, в каком он есть. Однако если пользователь выполнит команду Copy, файл будет расшифрован и перезаписан на диск. Если конечным расположением файла является раздел, отличный от NTFS 5.0, или гибкий диск, то файл не будет шифроваться при записи. Кроме того, если файл копируется на другой компьютер, он будет шифроваться заново с использованием другого ключа симметричного алгоритма. Два файла будут выглядеть различным образом на двух компьютерах, даже если их содержимое идентично.

Общие местоположения Как и Windows NT, Windows создает административные общие местоположения при загрузке. Ими являются C$, D$, IPC$, ADMIN$ и NETLOGON (имеются только на контроллерах доменов). Полный список текущих общих местоположений можно просмотреть в утилите Computer Management (Управление компьютером), выбрав в панели управления значок Administrative Tools (Администрирование) (см. рис. 13.4). Несмотря на то, что эти общие местоположения могут использоваться злоумышленниками для осуществления попыток раскрытия пароля администратора посредством грубой силы, отключать какие-либо из них не рекомендуется.

Сеть

Работа в сети с использованием Windows значительно изменилась по сравнению с Windows NT. В дополнение к стандартным портам Windows

(135, 137 и 139) в Windows используется порт 88 для Kerberos, порт 445 для SMB через IP, порт 464 для Kerberos kpasswd и порт 500 (только UDP) для Internet Key Exchange (IKE). Это означает, что если требуется удалить NetBIOS из системы Windows, то вам потребуется отключить опцию File and Print Sharing for Microsoft Networks (Совместный доступ к файлам и принтерам в сетях Microsoft) в данном конкретном интерфейсе. Это можно сделать в окне Network and Dial-up Connections (Сеть и удаленный доступ). Выберите меню Advanced (Дополнительно) и затем выберите Advanced Settings (Дополнительные параметры), чтобы открыть вкладку Adapters and Bindings (Адаптеры и компоненты) (см. рис. 13.5).

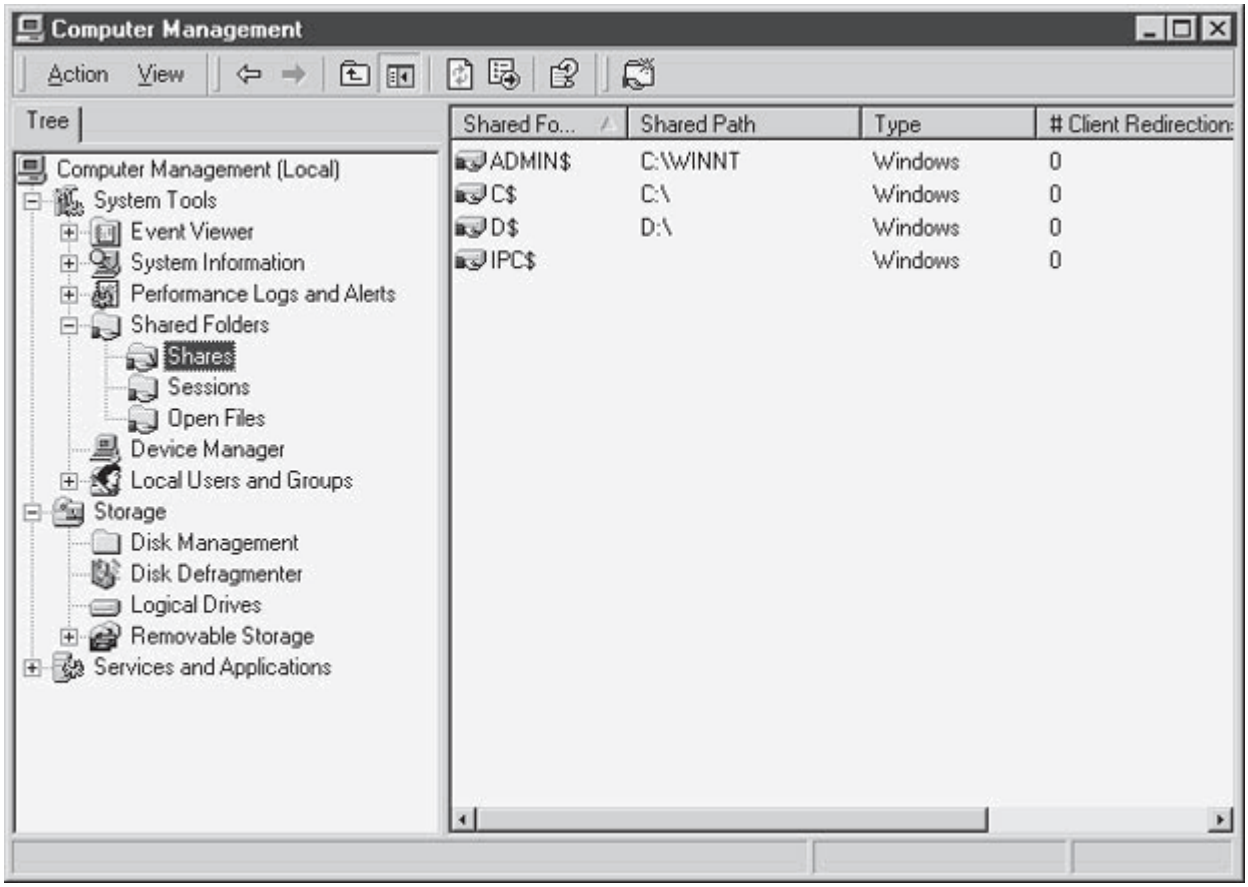

Рис. 13.4. Имеющиеся общие местоположения, отображаемые в оснастке Computer Management (Управление компьютером)

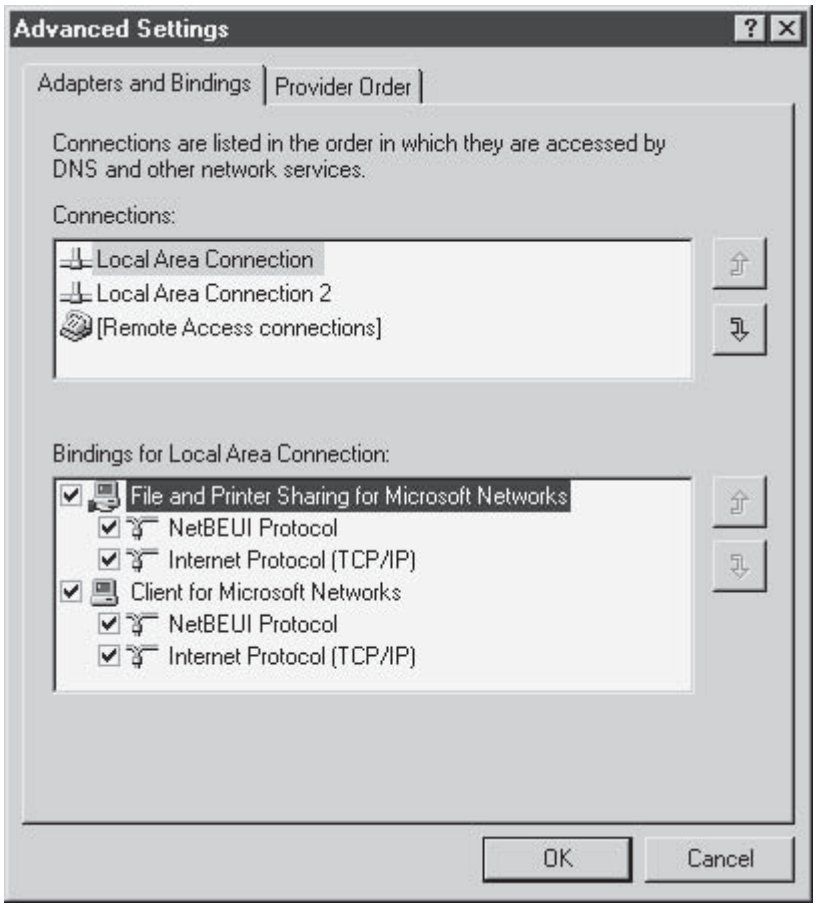

Рис. 13.5. Удаление компонентов для NetBIOS

Сеть по-прежнему является ключевой частью Windows. Домены Windows 2000 исключают концепцию PDC и BDC. Теперь имеют место только лишь контроллеры доменов (DC). Домены Windows 2000 по-прежнему поддерживают централизованное управление пользовательской базой данных. Однако структура Active Directory не позволяет использовать иерархическую концепцию. Это означает, что группы могут создаваться над или под другими группами, и домен может быть поделен на организационные единицы с локальным управлением. Более детальное обсуждение Active Directory приведено далее в лекции.

Примечание

Перед развертыванием Windows в организации необходимо четко спланировать структуру доменов. Нельзя просто перенести имеющуюся структуру доменов из Windows NT в Windows, т. к. это может привести к возникновению проблем.

Параметры учетных записей

В Windows имеются две учетные записи по умолчанию: Administrator (Администратор) и Guest (Гость). Обе учетные записи можно переименовать

с помощью утилиты Local Security Settings (Локальные параметры безопасности). Выберите элементы политики Rename Administrator Account (Переименование учетной записи администратора) и Rename Guest Account (Переименование гостевой учетной записи), чтобы внести изменения. Гостевая учетная запись также должна быть отключена. На всякий случай рекомендуется сменить пароль гостевой учетной записи, указав очень длинный пароль со случайным набором символов.

Каждая рабочая станция и сервер Windows в организации будут содержать учетную запись Administrator (Администратор), являющуюся локальной по отношению к данному компьютеру и требующую соответствующей защиты. Для защиты этих учетных записей необходимо разработать процедуру создания очень надежного пароля. Пароль должен быть записан, заклеен в конверт и положен на хранение в запираемом кабинете.

Примечание

Политики паролей и блокировки, описываемые в следующих разделах, могут быть применены посредством оснастки Group Policies (Групповые политики) и Active Directory, о чем будет рассказано далее в лекции.

Политика паролей. Политика системных паролей определяется с помощью средства Local Security Settings (Локальные параметры безопасности) (см. рис. 13.6). В этом окне настраиваются параметры паролей и требования к их надежности. Как в случае с любой компьютерной системой, эти параметры должны настраиваться в соответствии с политикой безопасности организации.

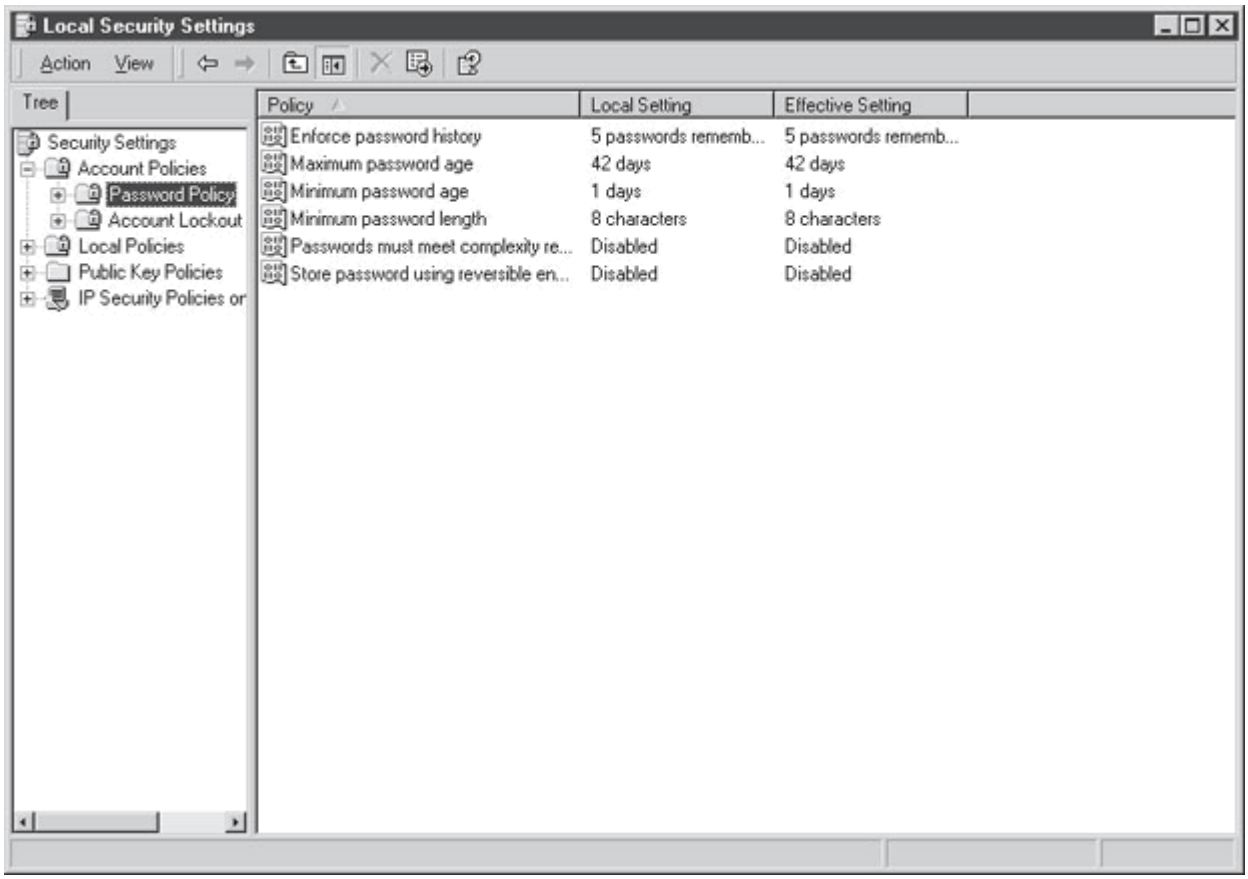

Рис. 13.6. Использование средства Local Security Settings (Локальные параметры безопасности) для настройки политики паролей

Если включить параметр Passwords Must Meet Complexity Requirements (Пароли должны отвечать требованиям сложности), то будет применен фильтр паролей, установленный по умолчанию (PASSFILT.DLL). Этот фильтр требует, чтобы длина всех паролей составляла не менее шести символов, чтобы пароли не содержали частей имени пользователя и содержали, по крайней мере, какие-либо из следующих элементов: цифры, символы, строчные или прописные буквы.

За исключением случая крайней необходимости не следует включать параметр Store Passwords Using Reversible Encryption (Сохранять пароли с использованием обратимого шифрования).

Политика блокировки учетных записей. Политика блокировки учетных записей также настраивается с использованием средства Local Security Settings (Локальные параметры безопасности) (см. рис. 13.7). Эти параметры должны настраиваться в соответствии с политикой безопасности организации.

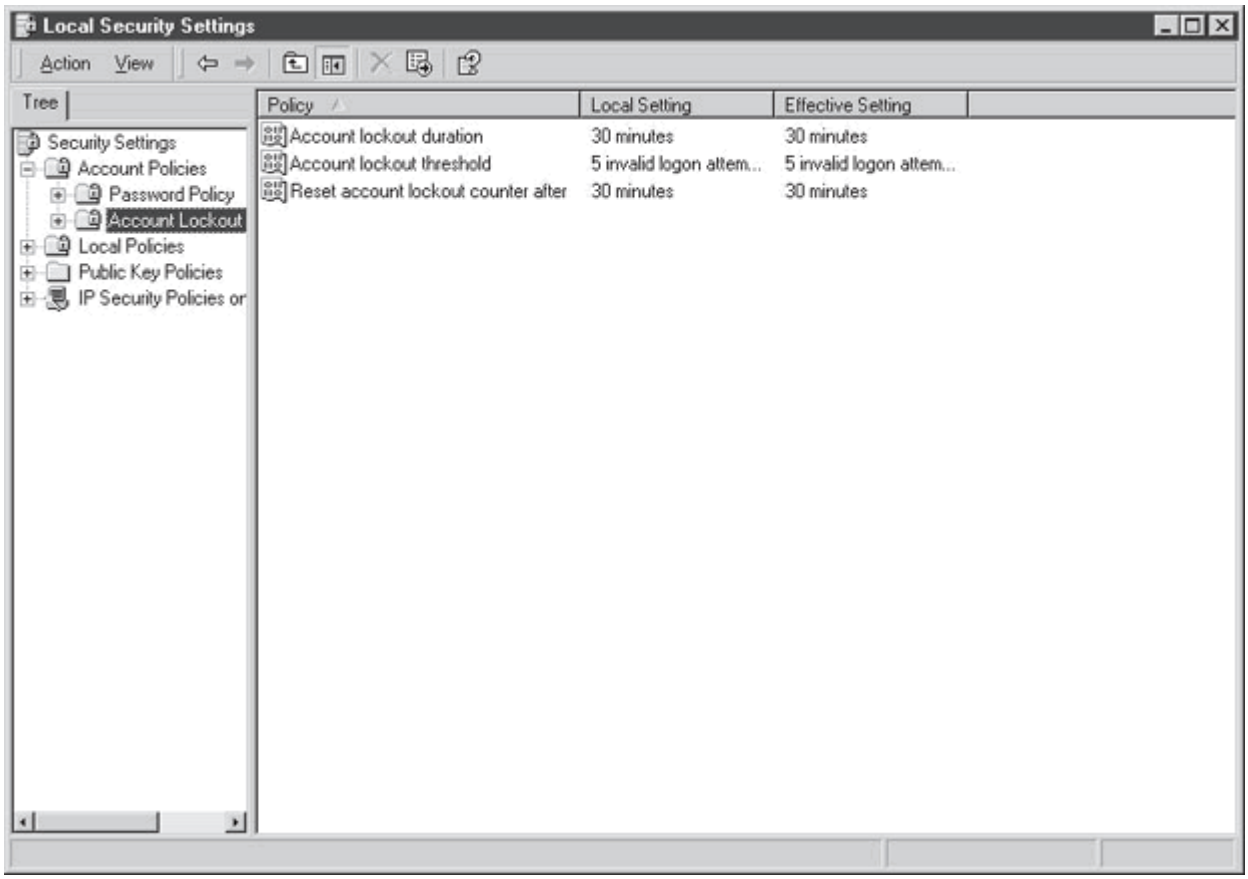

Рис. 13.7. Использование средства Local Security Settings (Локальные параметры безопасности) для настройки политики блокировки

Внимание!

Политика блокировки учетных записей предназначена для предотвращения атак "грубой силы", направленных на угадывание паролей. Данная возможность также используется для создания условия отказа в обслуживании по отношению ко всему сообществу пользователей. Следовательно, следует принимать во внимания возможные последствия продолжительных блокировок пользователей при настройке данной политики.

Блокировка не распространяется в принудительном порядке на учетную запись администратора. Учетная запись Administrator (Администратор) всегда доступна для входа в систему из системной консоли.

Сервис-пакеты и "горячие" обновления

На момент написания этой книги для Windows существует три сервис-пакета. С течением времени будут появляться новые сервис-пакеты и обновления. Как и в случае с обновлениями Windows NT, сервис-пакеты и горячие

обновления должны устанавливаться в сети организации после соответствующего тестирования.

Особенности конфигурации Windows

Изначально процесс установки системы идентичен установке Windows. Однако имеются три задачи по настройке, которые необходимо правильно выполнить после установки системы:

- служба Terminal Services;
- ограничения на программное обеспечение;
- настройка Framework .NET

Службы терминала (Terminal Services)

По умолчанию система Windows Server содержит функцию Remote Desktop for Administration (Удаленный рабочий стол для администрирования) (Terminal Services в режиме Remote Administration [удаленное администрирование] в Windows). Она позволяет создавать до двух удаленных сеансов плюс сеанс консоли. Так как эта возможность разрешает пользователям удаленно управлять серверами с любого клиента сети, необходимо обеспечить ее защиту от несанкционированного использования. Чтобы обеспечить максимальный уровень безопасности, необходимо убедиться в наличии следующих параметров, настраиваемых с помощью опции Properties (Свойства) для конкретного соединения в оснастке Terminal Services Configuration (Настройка службы терминала) (см. рис. 13.8).

- Уровень шифрования. В параметре Encryption Level (Уровень шифрования) приводится перечень доступных уровней, используемых для защиты данных, передаваемых между клиентом и сервером. Здесь имеются четыре опции:
- Low (Низкий). Данные шифруются с использованием 56-битного ключа.
- Client Compatible (Совместимый с клиентом). Данные шифруются с использованием ключа максимальной длины, поддерживаемого клиентом.
- High (Высокий). Данные шифруются с использованием 128-битного шифрования. Клиенты, не поддерживающие этот уровень шифрования, не будут иметь возможность подключения (рекомендуется использовать эту опцию).
- FIPS Compliant (Соответствие FIPS). Данные шифруются в соответствии со стандартом Federal Information Processing Standard 140-1, определяющим соответствующие методы шифрования.
- Logon Settings (Параметры входа в систему). Здесь можно указать аутентификационные данные для использования по умолчанию при подключении клиентов к серверу терминала (см. рис. 13.9). По

умолчанию используются аутентификационные данные, предоставляемые клиентом. Другая опция позволяет использовать одну учетную запись пользователя для всех соединений. Последняя опция требует от пользователя ввода пароля, даже если предоставлены аутентификационные данные.

- Network Adapter settings (Параметры сетевого адаптера). С помощью этой опции можно определить, какие сетевые адаптеры будет использовать служба. Это относится только к системам с несколькими сетевыми адаптерами.

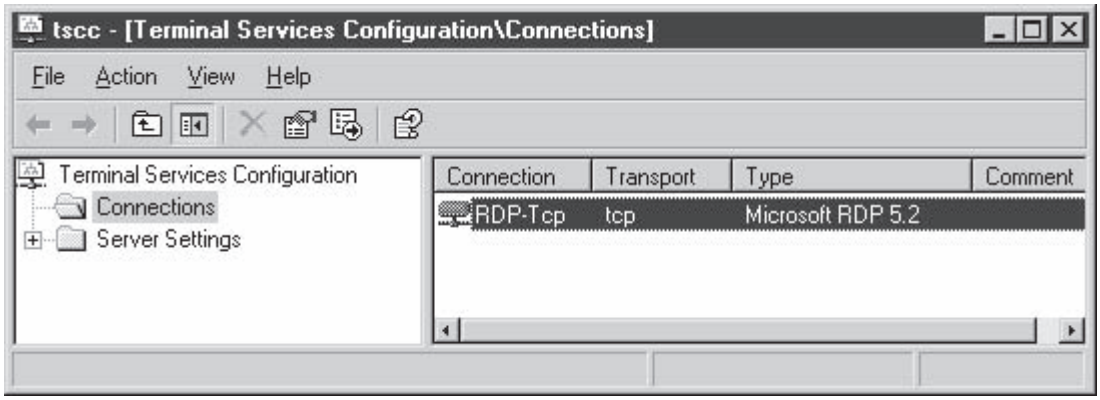

Рис. 13.8. Настройка службы Terminal Services

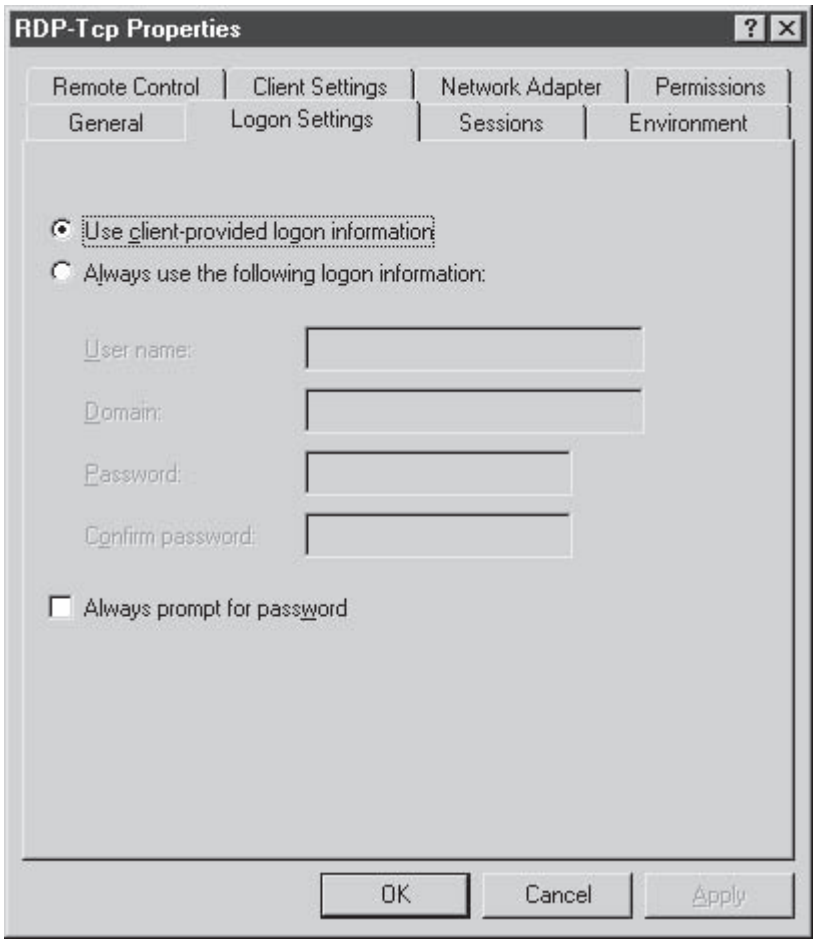

Рис. 13.9. Вкладка Logon Settings (Параметры входа в систему).

Вот так. При правильном администрировании учетных записей пользователей (посредством надежных паролей, блокировки и т. д.) и правильной защите системы (с использованием межсетевых экранов) данная служба будет относительно защищена.

Настройка Framework .NET 1.1

Средство .NET Framework Configuration (см. рис. 13.10) позволяет настраивать политику безопасности доступа к коду специально для версии 1.1 Framework .NET. В данной утилите есть возможность обеспечения защиты и/или удаления управляемых компонентов, установленных на рассматриваемом компьютере. С точки зрения безопасности данное средство может использоваться для контроля за доступом приложений к защищенным ресурсам. Система безопасности использует три уровня политики: Enterprise (Предприятие), Machine (Компьютер) и User (Пользователь) -для определения набора разрешений.

- Enterprise (Предприятие). Политика безопасности для предприятия в целом. Следует иметь в виду, что нет четких границ между данным уровнем и политикой Machine (Компьютер), так как обе эти политики применяются к каждому компьютеру.
- Machine (Компьютер). Применяется ко всем программам, выполняемым на данном компьютере.
- User (Пользователь). Применяется к пользователю, работающему в системе в данный момент.

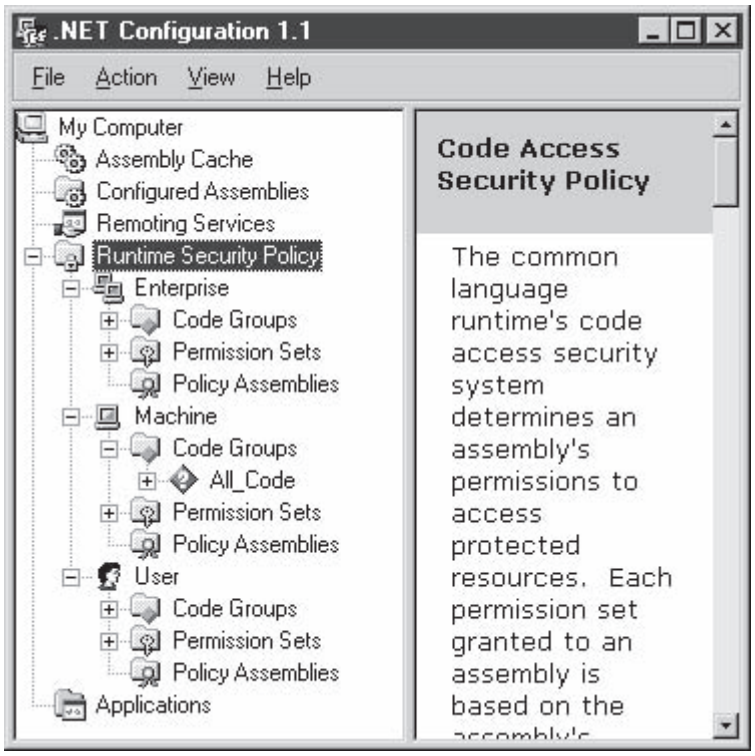

Рис. 13.10. Утилита настройки .NET

Оценка политик осуществляется в отдельном порядке, и программам предоставляется минимальный набор разрешений, обуславливаемый комбинацией политик. Любой "запрет" имеет преимущество перед "разрешением".

Примечание

Для получения более подробной информации о модели безопасности программного доступа, обратитесь к документации Microsoft .NET Framework SDK.

Вопросы для самопроверки

1. Новым интерфейсом управления безопасностью в системе Windows является _____.
2. _____ - это дополнение к NTFS, которое позволяет обеспечить дополнительный уровень конфиденциальности файлов.

Управление пользователями

Управление пользователями в системе Windows 2000 является очень важным аспектом безопасности системы и организации в целом. В организации необходимо наличие корректных процедур по определению полномочий каждого нового пользователя. При увольнении сотрудника из организации

также необходимо применять соответствующие процедуры, чтобы обеспечить запрет доступа увольняемого сотрудника к системам организации.

Добавление пользователей в систему

При добавлении новых пользователей в систему необходимо следовать процедурам управления пользователями. Эти процедуры должны определять, кто может запрашивать новые учетные записи, и кто может одобрять эти запросы. Новые пользователи добавляются в систему или домен через оснастку Computer Management (Управление компьютером). Выберите элемент Users (Пользователи) из Local Users and Groups (Локальные пользователи и группы). Затем выберите New User (Новый пользователь) из меню Action (Действие) (см. рис. 13.11). Как и в Windows, каждый пользователь должен иметь уникальный пользовательский идентификатор и свою собственную учетную запись. Если двум пользователям требуется доступ одинакового уровня, следует создать две учетные записи и разместить их в одной группе. Ни при каких обстоятельствах нельзя присваивать нескольким пользователям один и тот же идентификатор.

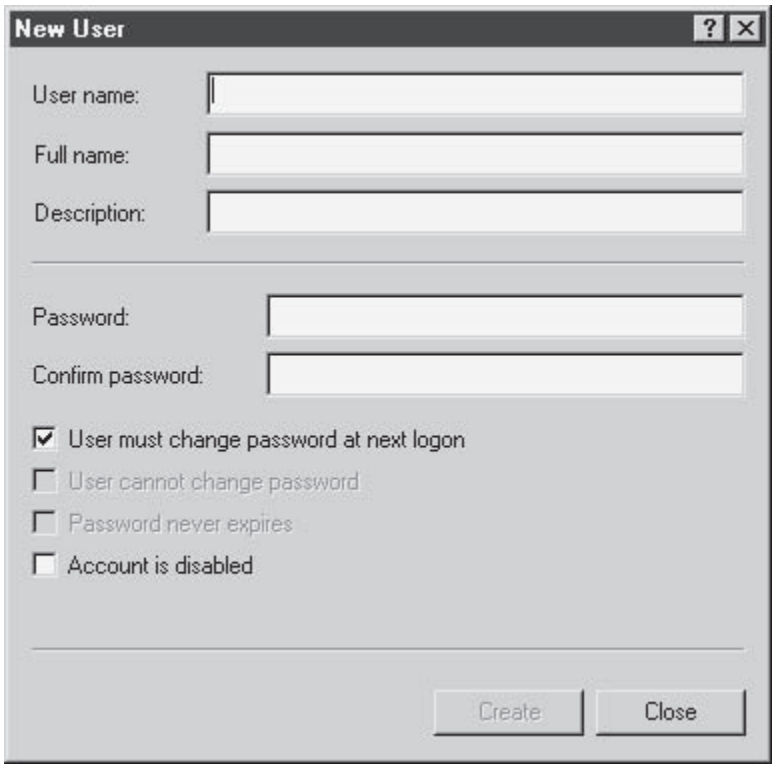

Рис. 13.11. Окно New User (Новый пользователь)

Для каждого идентификатора нового пользователя следует назначить начальный пароль, а также отметить опцию User Must Change Password (Пользователь должен изменить пароль). Это потребует от пользователя

смены пароля при первом входе в систему. Ни в коем случае не отмечайте опцию Password Never Expires (Срок действия пароля не ограничен).

Примечание

В организациях не должен использоваться один и тот же пароль для каждой новой учетной записи. Несмотря на то, что таким образом упрощается задача создания новых учетных записей, это обуславливает потенциальную уязвимость систем. Если новая учетная запись создается перед тем, как сотрудник будет принят на работу в организацию, эта запись будет доступна для использования неавторизованными лицами. Все, что им понадобится для доступа - это стандартный пароль новых пользователей. Рекомендуется использовать надежные и уникальные пароли новых пользователей.

Сразу после создания учетной записи ее следует добавить в соответствующие группы. Это можно сделать следующим образом: перейдите к каждой группе по отдельности, дважды щелкните на ней и нажмите кнопку Add (Добавить) (см. рис. 13.12). В качестве альтернативы щелкните правой кнопкой мыши на вновь созданном пользователе и выберите Properties (Свойства). Откройте вкладку Member Of (Член группы) и добавьте в список соответствующие группы (см. рис. 13.13). Стандартные пользовательские учетные записи не должны входить в состав группы Administrator (Администратор).

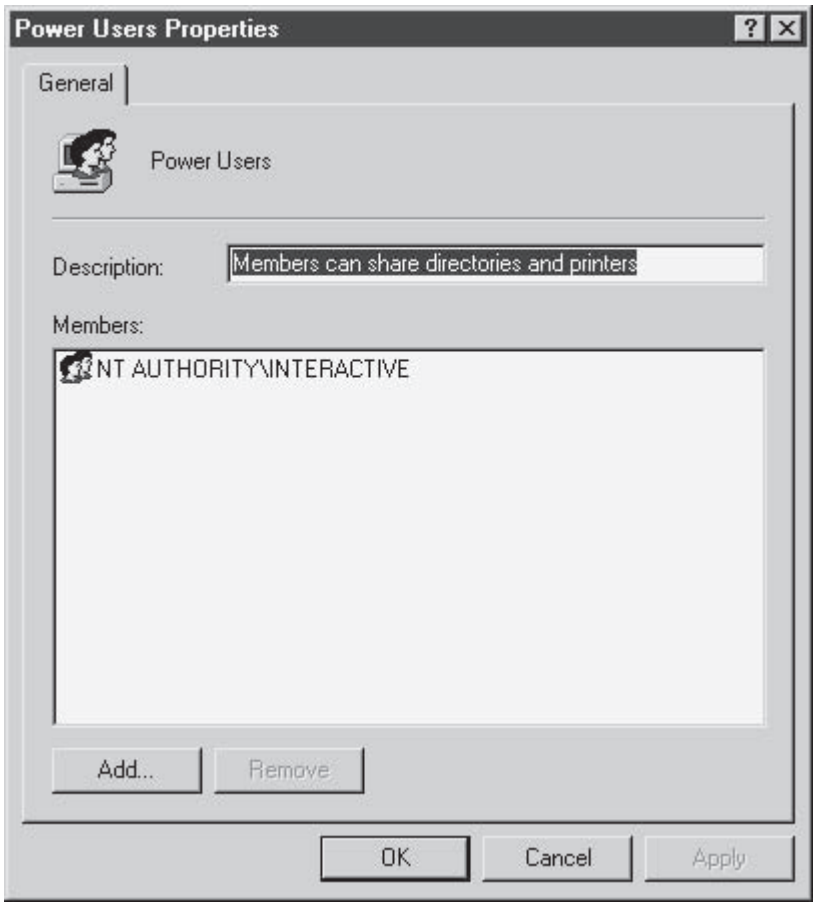

Рис. 13.12. Добавление пользователей в группу с помощью списка групп

Настройка файловых разрешений

Для настройки разрешений файлов и общих местоположений следует использовать группы. Это позволит облегчить управление файловыми разрешениями (в отличие от предоставления отдельным пользователям полномочий на доступ к файлам и общим местоположениям). Убедитесь, что членом группы Guests (Гости) является только учетная запись Guest (Гость), и что учетная запись Guest (Гость) отсутствует во всех остальных группах.

Удаление пользователей из системы

Как и при добавлении пользователей в систему, администраторам необходимо выполнять процедуры по управлению пользователями при удалении пользователей. Когда пользователь покидает организацию, его учетная запись должна немедленно отключаться с помощью утилиты Computer Management (Управление компьютером). Выберите нужного пользователя, щелкните на нем правой кнопкой мыши и выберите Properties (Свойства). Появившееся окно позволит отключить учетную запись. В то же время необходимо изменить пароль на произвольную случайную комбинацию символов. Это предотвратит использование учетной записи пользователем или кем бы то ни было еще.

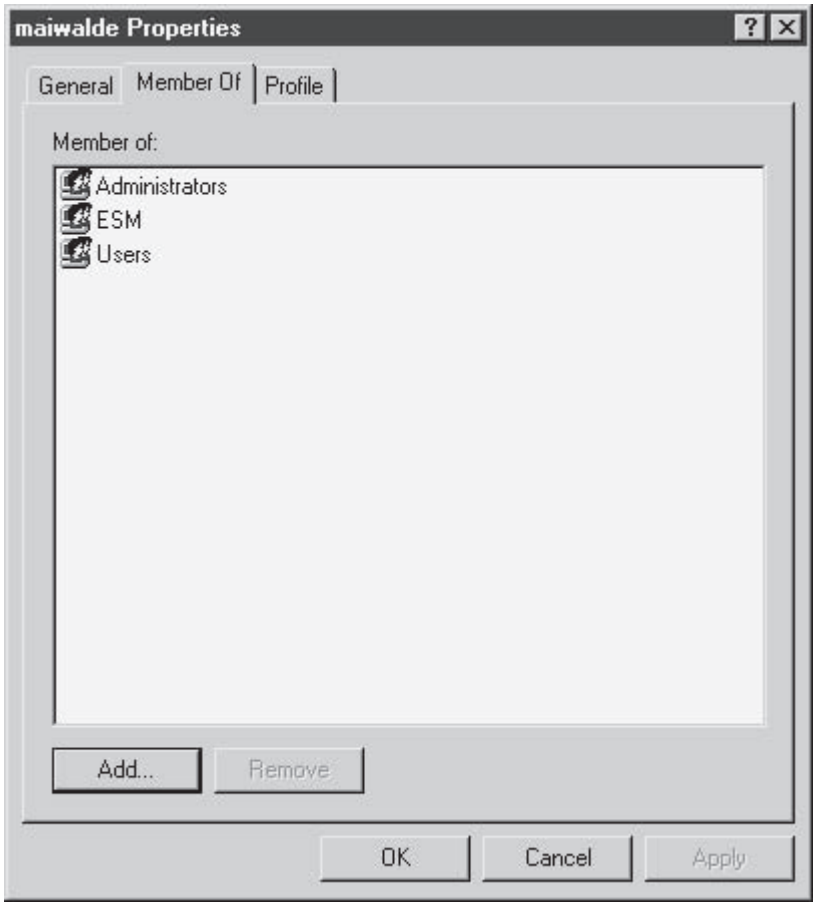

Рис. 13.13. Добавление пользователей в группы в окне свойств

Бывает так, что рассматриваемый пользователь имел файлы или полномочия, необходимые организации; его учетная запись должна оставаться отключенной в течение некоторого времени (как правило, 30 дней), чтобы начальник пользователя смог получить доступ к этим файлам и скопировать нужные материалы. Если пользователь использовал файловую систему EFS, то для доступа к файлам можно применять локальную учетную запись Administrator (Администратор). По прошествии 30 дней учетная запись должна быть удалена из системы вместе со всеми файлами и каталогами, принадлежащими учетной записи.

Примечание

В некоторых организациях учетные записи не удаляются и находятся в отключенном состоянии, чтобы выяснить, будет ли кто-нибудь пытаться использовать старую учетную запись. Действия, производимые с учетной записью, обусловливаются процедурами управления пользователями, утвержденными в организации.

Управление системой

Безопасность необходимо обеспечивать не только при установке и настройке системы, о ней следует помнить и при выполнении ежедневных операций. Возможно, наилучшим образом это сможет делать администратор, внимательно следящий за своими системами. Имея это в виду, следует упомянуть о некоторых действиях, которые можно выполнять в системе Windows для повышения вероятности обнаружения администратором потенциальных проблем, связанных с безопасностью.

Команда secedit

Windows содержит утилиту secedit.exe, которая используется для управления политикой безопасности при большом количестве систем. Secedit предоставляет следующие возможности.

- Анализ. Политика рассматриваемой системы анализируется и сопоставляется с предоставленной политикой.
- Конфигурация. Политика рассматриваемой системы изменяется для соответствия предоставленной политике.
- Утверждение. Файл конфигурации безопасности может быть утвержден.
- Обновление. Политика заново применяется к системе.
- Экспорт. Сохраненный шаблон из базы данных безопасности системы экспортируется в виду файла шаблона безопасности.

В следующих разделах будет рассмотрено, как эти возможности используются для управления безопасностью систем Windows.

Анализ

С помощью secedit можно сопоставлять имеющуюся политику в системе с Windows с политикой, соответствующей данной системе. Для этого нужно ввести в командной строке следующую команду:

Secedit /analyze [/DB имя файла базы данных]

[/CFG имя файла конфигурации]

[/log имя файла журнала] [/verbose] [/quiet]

В команде можно указывать следующие параметры:

- /DB имя файла базы данных. Указывает путь к файлу базы данных, который содержит сохраненную конфигурацию для анализа. Если имя файла указывает на новый файл, также необходимо использовать параметр /CFG.
- /CFG имя файла конфигурации. Указывает путь к шаблону безопасности, который будет импортирован в базу данных. При отсутствии этого параметра будет использоваться конфигурация, сохраненная в базе данных.
- /log имя файла журнала. Указывает путь к файлу журнала, который будет создан в результате выполнения команды. Файл журнала содержит всю информацию, полученную в ходе анализа.
- /verbose. Этот параметр обеспечивает отображение детальной информации при выполнении команды.
- /quiet. Отключает вывод данных на экран в процессе выполнения.

После выполнения команды файл журнала можно проанализировать для определения того, соответствует ли система политике организации.

Конфигурация

Secedit также позволяет конфигурировать систему. Синтаксис команды для выполнения этой операции выглядит следующим образом.

Secedit /configure [/DB имя файла базы данных] [/CFG имя файла конфигурации] [/overwrite] [/areas area1 area2:] [/log имя файла журнала]

[/verbose] [/quiet

В команде можно указывать следующие параметры:

- /DB имя файла базы данных. Указывает путь к базе данных, содержащей необходимый для использования шаблон.
- /CFG имя файла конфигурации. Указывает путь к шаблону безопасности, который можно импортировать в базу данных и затем установить в системе.
- /overwrite. Указывает необходимость перезаписи политики в шаблоне безопасности, определенном командой /CFG, поверх политики в базе данных.
- /areas. Указывает области безопасности шаблона, которые следует применить к системе. Этими областями являются: Securitypolicy, Group_mgmt, User_rights, Regkeys, Filestore, Services. Если ни одна область не указана, то по умолчанию используются все области.
- /log имя файла журнала. Указывает путь к файлу журнала, который будет создан в результате выполнения команды.
- /verbose. Сообщает команде secedit о том, что необходимо отображать детальные сведения во время выполнения.
- /quiet. Отключает вывод данных на экран в процессе выполнения.

Данная команда может использоваться для принудительного применения конкретной конфигурации безопасности в системе.

Утверждение

Secedit может использоваться для утверждения файла конфигурации. При этом происходит проверка корректности синтаксиса файла. Для выполнения этой операции необходимо выполнить следующую команду:

Secedit /validate имя_файла

Обновление

Опция обновления команды secedit представляет собой механизм обновления политики безопасности организации. Эта команда заново применяет политику безопасности к локальному компьютеру. Синтаксис этой команды таков:

Secedit: /refreshpolicy [machine_policy или user_policy] [/enforce]

Здесь могут использоваться следующие параметры:

- Machine_policy. Указывает, что необходимо обновить политику безопасности для локального компьютера.
- User_policy. Указывает, что необходимо обновить параметры безопасности локального пользователя, который в данный момент находится в системе.

- /enforce. Указывает, что политика должна быть обновлена, даже если в нее не внесено никаких изменений.

Эта команда обеспечивает тот факт, что в системе действует нужная политика безопасности.

Экспорт

Secedit применяется также для экспорта конфигурации из базы данных безопасности в шаблон безопасности, что позволяет использовать шаблон безопасности на других компьютерах. Соответствующая команда имеет вид:

Secedit /export [/MergedPolicy] [/DB имя файла базы данных]

[/CFG имя файла конфигурации]

[/areas area1 area2:] [/log имя файла журнала]

[/verbose] [/quiet].

В данной команде могут использоваться следующие параметры:

- MergedPolicy. Указывает, что secedit должна экспортировать как доменную, так и локальную политику.
- /DB имя файла базы данных. Указывает путь к базе данных, содержащей конфигурацию, которую необходимо экспортировать.
- /CFG имя файла конфигурации. Указывает путь сохранения шаблона безопасности.
- /areas. Указывает области безопасности шаблона, которые должны быть применены к системе. Этими областями являются: Securitypolicy, Group_mgmt, User_rights, Regkeys, Filestore, Services. Если ни одна область не указана, то по умолчанию используются все области.
- /log имя файла журнала. Указывает путь к файлу журнала, который будет создан в результате выполнения команды.
- /verbose. Сообщает команде secedit о том, что необходимо отображать детальные сведения во время выполнения.
- /quiet. Отключает вывод данных на экран в процессе выполнения.

Результаты выполнения этой команды можно сравнить с результатами выполнения других команд, чтобы обеспечить действие одной и той же политики по всему домену.

Вопрос к эксперту

Вопрос. Можно ли использовать secedit для управления большим числом систем?

Ответ. Конечно. Ее можно использовать для разработки корректной конфигурации системными администраторами на тестовой системе. Эту конфигурацию затем можно экспортировать и использовать для утверждения конфигурации для каждой рабочей станции и сервера. Secedit используется во время выполнения сценариев загрузки для проверки текущей конфигурации и для ее обновления в случае внесения локальным администратором или пользователем каких-либо изменений.

Контрольные вопросы

1. Каковы различия в параметрах безопасности систем Windows и Windows NT, если они работают в одной и той же сети?
2. Для чего нужен графический пользовательский интерфейс Local Security Policy (Локальная политика безопасности)?
3. При каких условиях файл, защищенный EFS, будет записываться на диск в незашифрованном виде?
4. К файлам, защищенным EFS, всегда имеют доступ, по крайней мере, два пользователя. Кто эти пользователи?
5. Какие два изменения внесены в Windows в функционирование доверительных взаимоотношений?
6. Если в конфигурации безопасности используется параметр Passwords Must Meet Complexity Requirements (Пароли должны соответствовать требованиям сложности), какие требования предъявляются ко всем паролям?
7. Членом какой группы или групп должна являться учетная запись Guest (Гость)?