14. Лекция: Вопросы безопасности Windows Server

В лекции рассмотрены вопросы безопасности в ОС Windows, поиск вторжений в данную ОС.

Аудит системы

Все системы Windows должны подвергаться аудиту. Политика аудита в системе настраивается в утилите Local Security Settings (Локальные параметры безопасности) (см. рис. 14.1). Выберите событие, аудит которого следует производить, и дважды щелкните на нем, чтобы отобразить окно конфигурации.

Политика аудита должна настраиваться в соответствии с политикой безопасности организации. Как правило, рекомендуется фиксировать следующие события:

- аудит событий входа через учетные записи, успех или неудача;
- аудит управления учетными записями, успех или неудача;
- аудит событий входа, успех или неудача;
- аудит доступа к объектам, неудача;
- аудит изменения политики, успех или неудача;
- аудит использования привилегий, неудача;
- аудит системных событий, успех или неудача.

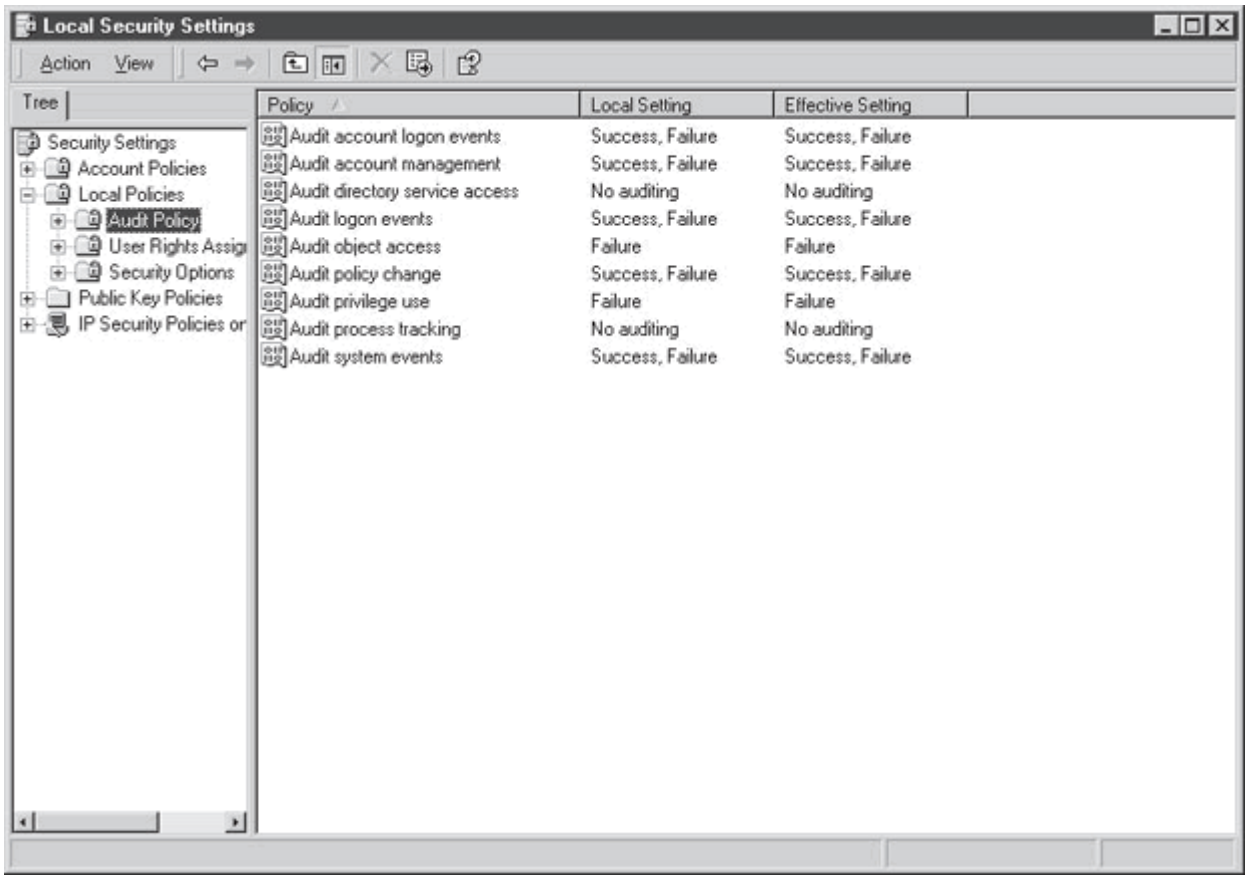

Рис. 14.1. Настройка политики аудита в системе Windows

Внимание!

При аудите доступа к объектам может генерироваться достаточно большое число записей журнала, даже если включена только опция записи неудачных событий. Тщательно отслеживайте новую систему и убедитесь, что по этой причине не происходит переполнение файлов журналов.

Файлы журнала

Записи журнала аудита в системе Windows создаются в журнале событий безопасности, который расположен в папке \%systemroot%\system32\ config. Разрешения журнала событий безопасности предоставляют доступ только администраторам. Администраторы должны регулярно проверять файлы журналов. Так как записи файлов журналов являются самым лучшим средством выявления неполадок в системе или несанкционированных действий пользователей, то, если администраторы не будут просматривать файлы журналов, смысл фиксирования информации сведется к нулю (см. раздел "Поиск подозрительных признаков", в котором рассказывается о признаках подозрительной активности).

Если регулярно производится резервное копирование системы, файлы журнала также должны резервироваться. Если журналы событий нужно сохранять на более длительные периоды времени, рекомендуется периодически перемещать файлы журналов с системы. Файлы можно сохранять в виде текстовых файлов или файлов с разделителями-запятыми посредством команды Save As (Сохранить как) в меню Action (Действие) в программе Event Viewer (Просмотр событий).

Поиск подозрительных признаков

Существует несколько признаков того, что в системе Windows 2000 что-то идет не так, как нужно, и что кто-то пытается выполнить запрещенные действия.

Попытки атак с использованием "грубой силы"

Если кто-либо пытается угадать пароли учетных записей (вручную или с привлечением автоматизированной программы), в журнал событий будут занесены записи, отображающие неудачные попытки входа в систему. Кроме того, если система настроена на блокировку учетных записей после определенного числа попыток входа, будет присутствовать набор заблокированных учетных записей. Сообщения о неудачных попытках входа в журнале событий безопасности содержат имя рабочей станции, с которой

осуществлялась каждая попытка. С этой рабочей станции и следует начать выяснение причины неудачных попыток входа в систему. Метод выяснения зависит от источника попыток. Если источник внутренний, следует найти сотрудника, работающего за данной рабочей станцией, и поговорить с ним. Если источник внешний, следует заблокировать на межсетевом экране доступ с IP-адреса источника.

Ошибки доступа

Ошибки доступа могут означать, что доступ к секретным файлам пытается получить авторизованный пользователь. Единичные ошибки считаются в порядке вещей. Однако если обнаружится пользователь, совершивший неудачные попытки входа в большое число файлов или каталогов, то у вас появятся все основания для выяснения причин неудачных попыток.

Примечание

Информация в журнале событий безопасности содержит перечень неудачных попыток входа. Она не представляет собой доказательства того, что конкретный сотрудник пытался получить несанкционированный доступ к информации. Эти сообщения журнала могут генерироваться процессами, пытающимися осуществить доступ без ведома пользователя; также причиной возникновения этих записей является использование кем-либо учетной записи данного пользователя или его системы. Ни в коем случае не следует считать, что записи в журнале являются достаточным доказательством для того, чтобы обвинить сотрудника в совершении противоправных действий.

Отсутствие файлов журналов или пробелы в них

В работающей системе Windows с включенным аудитом файлы журналов никогда не бывают пусты. Многие злоумышленники очищают файлы журналов сразу после входа в систему в надежде скрыть факт своего присутствия. Если вы обнаружили пустой файл журнала, это говорит о том, что с системой что-то не в порядке, и следует немедленно начать выяснение причин отсутствия в журналах данных. Может оказаться, что другой администратор указал опцию очистки файлов журналов, так как они имели очень большой размер. Однако может выясниться, что в систему кто-то проник несанкционированно.

Не так давно начали выходить в свет утилиты, помогающие злоумышленникам изменять отдельные записи в файлах журналов. В результате этого действия в файле журнала может оказаться пробел. Чтобы обнаружить пробел, просмотрите содержимое файла и выясните, присутствуют ли в нем пропуски, большие, чем обычные. Если обнаружатся значительные пробелы в содержимом файла, следует выяснить причину их появления. Имейте в виду, что система не создает записи в журнале, когда

она отключена. В данном случае в содержимом файла перед и после каждого пробела будут присутствовать записи отключения и запуска системы.

Неизвестные процессы

В системах Windows выполняется множество процессов. Некоторые из них обнаружить легко, другие - сложнее. Если посмотреть в окно программы Task Manager (Диспетчер задач) (см. рис. 14.2), то можно увидеть процессы, выполняющиеся в данный момент в системе, а также процент использования процессора и объем используемой процессами памяти.

Системные администраторы должны периодически открывать Диспетчер задач и выяснять, не выполняются ли в системе какие-либо неизвестные процессы. Например, рекомендуется всегда искать процессы CMD. Процесс CMD является сеансом командной строки или окном DOS. Если он работает, то на экране должно отображаться соответствующее окно. В некоторых случаях злоумышленники запускают процесс CMD для выполнения операций в системе. Это явный признак того, что в системе происходит что-то необычное.

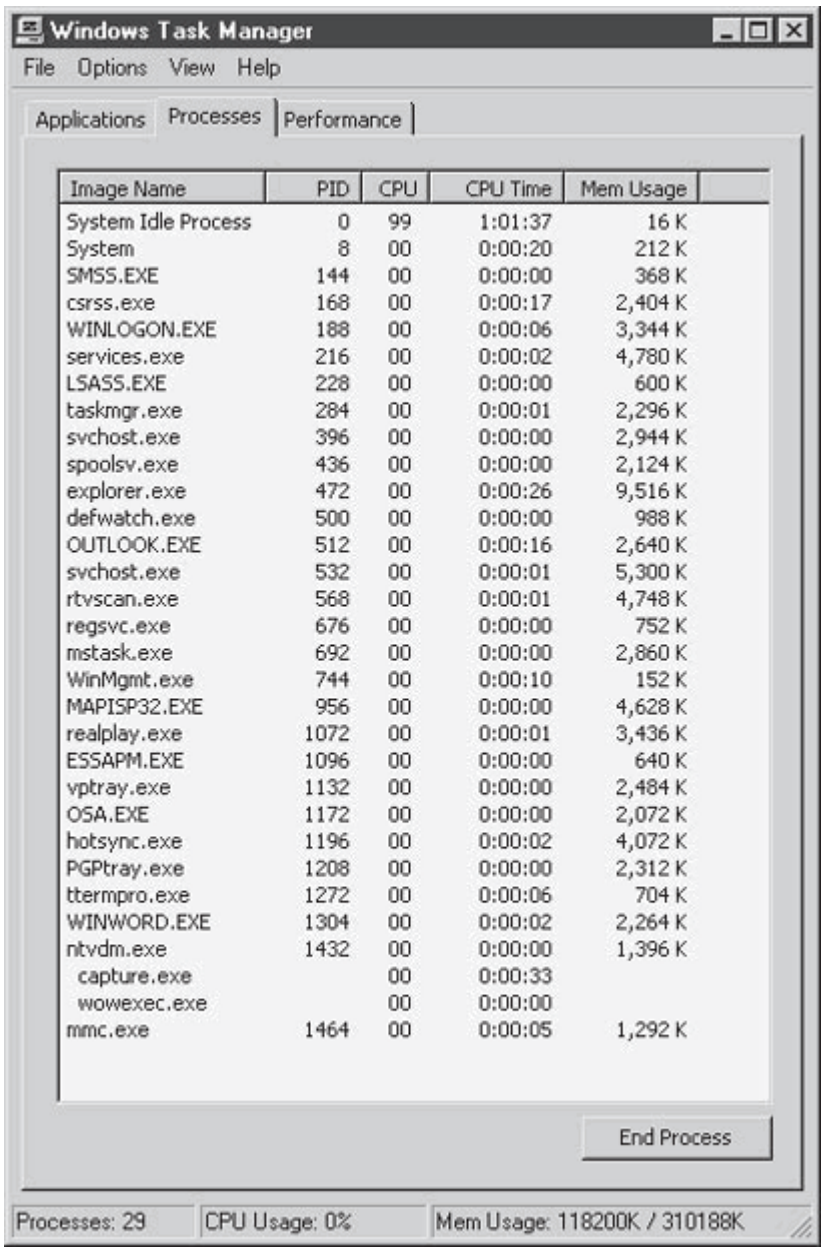

Рис. 14.2. Диспетчер задач Windows

Использование Active Directory

Центральным элементом системы безопасности Windows является Active Directory (AD). AD - это служба каталогов, разработанная и внедренная в последние версии операционной системы Windows. Она является попыткой Microsoft создания масштабируемой структуры домена, взамен старой модели домена Windows NT.

Примечание

Основным различием Windows Server является гибкость и управляемость AD. Самое значительное изменение, связанное с безопасностью, связано с доверием между лесами.

AD может состоять из одного или более доменов, причем каждый домен имеет свои политики безопасности и безопасные (т. е. доверенные) взаимоотношения с другими доменами. Пространство имен домена соответствует домену DNS, а домен Root - это первый домен, создаваемый в AD. Все домены в AD совместно используют одну и ту же конфигурацию, схему и глобальный каталог. Ключевыми компонентами AD и их функциями являются следующие элементы.

- Global Catalog (GC, Глобальный каталог). Серверы GC содержат частичные реплики всех доменов в AD, а также полную реплику схемы и именования конфигурации, поэтому эти системы являются носителями секретной информации и должны соответствующим образом защищаться.
- Схема. Схема определяет, какие объекты и атрибуты могут храниться в AD. Она поддерживает все классы объектов и атрибуты, содержащиеся в AD. Для каждого класса объектов схема определяет место в AD для создания класса объекта, а также список атрибутов, которые должен содержать класс. Это ключевой компонент AD, и очень важно обеспечить его безопасность
- Домен. Домен - это группа компьютеров, объединенных для формирования административной ограниченной области пользователей, групп, компьютеров и организационных единиц.
- Организационная единица (OU) - это тип объектов каталога, с которыми можно связать групповые политики и таким образом определять в них ограничения безопасности. Это наименьшие административные единицы в AD, формирующие границы защищаемой области. По умолчанию, так как домен является ограниченной областью администрирования, и OU существует только внутри домена, домен является наиболее внешней организационной единицей.
- Групповые политики. Объект домена, обеспечивающий возможность группирования параметров безопасности и конфигурации в шаблоны, которые могут применяться к отдельным системам, доменам или организационным единицам.
- Доверительные взаимоотношения. Доверительные взаимоотношения позволяют использовать информацию из одного домена, такую как идентификаторы безопасности пользователей, в другом домене. По умолчанию в AD имеется двустороннее транзитивное доверие. Домены с двусторонним доверием полностью доверяют друг другу. Транзитивное доверие означает, что если домен A доверяет домену B, а домен B доверяет домену C, то домен A доверяет домену C. Можно сравнить этот принцип с доверием в Windows NT, где оно было однонаправленным (поэтому приходилось настраивать доверие в отдельном порядке) и не транзитивным, т. е. доверие имело место

только по отношению к тем доменам, с которыми были установлены непосредственные доверительные отношения.

Безопасная установка и настройка

При настройке AD наиболее важным моментом, связанным с безопасностью, является выбор опции Permissions Compatible with Pre-Windows Server (Разрешения совместимы с версиями Windows, предшествующими Windows Server). Эта опция делает группу Everyone (Все) членом встроенной группы Pre-Windows Compatible Permissions (Разрешения, совместимые с операционными системами, предшествующими Windows). Это позволяет устанавливать анонимные соединения с AD (т. е. предоставляются анонимные полномочия на чтение всем важным пользовательским и групповым атрибутам домена). Если поддержка систем, предшествующих Windows 2000, не требуется, не следует включать эту опцию.

На данном этапе (если вы не упустили какие-либо разрешения) AD должна быть достаточно защищена. Единственное, что осталось сделать, - убедиться, что пользователи используют надежные пароли, и что системы защищены от сетей без доверия (таких как интернет).

Администрирование

Ниже приведен перечень основных средств, используемых для управления AD, с кратким описанием каждой утилиты.

- Active Directory Domains and Trusts. Эта утилита используется для запуска программы Domain Manager (Диспетчер домена), управления доверительными взаимоотношениями, установки режима функционирования и определения альтернативных суффиксов UPN (User Principal Name).
- Active Directory Sites and Services. Эта утилита используется для администрирования топологии репликации, добавления и удаления сайтов, переноса компьютеров в сайт, добавления в сайт подсети, связывания сайта с подсетью и создания связи сайта.
- Active Directory Users and Computers. Эта утилита используется для управления объектами в домене. С ее помощью осуществляется добавление, перенос, удаление и изменение атрибутов таких объектов AD, как пользователи, группы, компьютеры и общие папки.
- ADSIEdit. Эта оснастка позволяет выполнять LDAP-операции по отношению к любым разделам каталога (домен, конфигурация или схема). ADSIEdit осуществляет доступ к AD через ADSI и позволяет добавлять, удалять и перемещать объекты внутри AD. Также с ее помощью можно просматривать, изменять и удалять атрибуты.

Групповая политика и безопасность

Групповые политики (GP) представляют собой основной метод обеспечения централизованного управления конфигурацией безопасности в Windows. Они могут применяться на уровне сайта, домена и OU, а также могут применяться к пользователям и компьютерам (Users and Computers) в Active Directory. GP используются для выполнения следующих действий.

- Блокировка рабочих столов пользователей.
- Применение параметров безопасности.
- Ограничение доступа к приложениям.
- Установка разрешения реестра и файловой системы.
- Настройка конфигурации беспроводной сети.

Совет

Настоятельно рекомендуется использовать утилиту Group Policies вместо Local System Policies, если это возможно.

Параметры конфигурации

Утилита Group Policies разделена на две области - User (Пользователь) и Computer (Компьютер). Область настройки пользователя User Configuration содержит такие элементы, как параметры рабочего стола, параметры безопасности и сценарии входа и выхода их системы. Эти элементы определены под деревом User Configuration и применяются при входе в систему или обновлении групповой политики. Computer Configuration используется для настройки работающей системной среды (а не пользовательской оболочки), включая параметры служб, параметры безопасности и сценарии загрузки/отключения. Эти элементы определены в дереве Computer Configuration и применяются при загрузке и обновлении Group Policy.

По умолчанию GP применяются в зависимости от расположения настраиваемого объекта. Пользовательские GP зависят от того, в каком сайте, домене и организационной единице находится объект "пользователь". То же самое относится и к компьютеру. GP применяются к компьютерам в зависимости от расположения объекта "компьютер" (сайт, домен и организационная единица, в которой находится компьютер). Это означает, что если GP применяется к объекту User (Пользователь), то используется конфигурация пользователя, а конфигурация компьютера групповой политики игнорируется. И наоборот, если GP применяется к объекту Computer (Компьютер), используется конфигурация компьютера, а конфигурация пользователя игнорируется.

Групповые политики по умолчанию

Имеются две групповые политики, установленные по умолчанию, создаваемые при создании домена: Default Domain Policy (Политика домена по умолчанию) и Default Domain Controller Policy (Политика контроллера домена по умолчанию). Политика домена по умолчанию применяется к контейнеру домена. Она может быть применена ко всем компьютерам в домене по умолчанию. Политика контроллера домена по умолчанию применяется к "специальному" контейнеру контроллера домена в домене и, кроме того, применима только к контроллерам домена.

Параметры конфигурации в групповой политике

Так как мы не можем рассказать подробно о групповых политиках, уложившись в одну лекцию, то обсудим наиболее важные элементы, связанные с безопасностью, которые могут (и должны) быть применены через групповую политику. Как уже говорилось ранее, каждая групповая политика имеет два основных дерева данных конфигурации: Computer Configuration (Конфигурация компьютера) и Users Configuration (Конфигурация пользователей). Эти области отображаются в виде двух раздельных секций в окне Group Policy Object Editor (Редактор объекта групповой политики) (см. рис. 14.3).

Конфигурация компьютера:

- Account Policies: Password Policy (Политики учетных записей: политика паролей). Позволяет настраивать историю, требования к возрасту, длине и сложности паролей.
- Account Policies: Account Lockout Policy (Политики учетных записей: политика блокировки учетных записей). Позволяет настраивать число попыток, длительность и сброс.
- Local Policies: Audit Policies (Локальные политики: политики аудита). Позволяет включать аудит в системах.

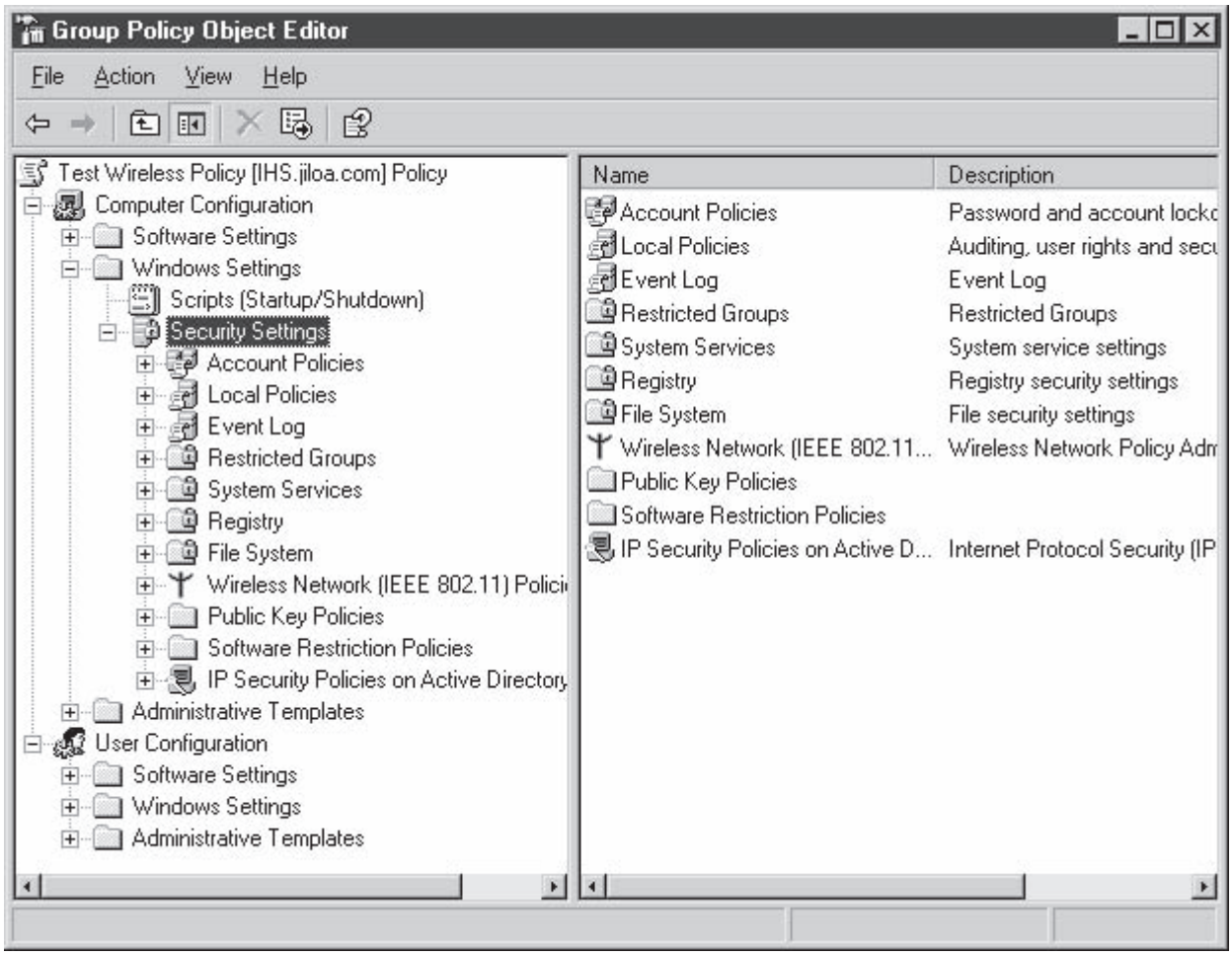

Рис. 14.3. Редактор объекта групповой политики

- Local Policies: User Rights Assignment (Локальные политики: присвоение прав пользователей). Позволяет присваивать пользовательские права пользователям и группам.
- Local Policies: Security Options (Локальные политики: параметры безопасности). Позволяет настраивать политики, связанные с безопасностью, включая подписи SMB, ограничения безопасности каналов, автоматический выход, уровень аутентификации LAN Manager, текстовое сообщение входа и примечание, а также множество других элементов (40 по умолчанию).
- Event Log: Settings for Event Logs (Журнал событий: параметры журналов событий). Позволяет настраивать объем журнала, ограничения доступа, параметры сохранения, а также необходимость отключения системы по заполнении журналов.
- Restricted Groups: Members of Restricted Group (Ограниченные группы: члены ограниченной группы). Предписывает членство в группе. Если пользователь или группа входят в список членов ограниченной группы, но не находятся в группе, происходит добавление в группу этого пользователя или группы. Если пользователь или группа является

членом группы, но отсутствует в списке членов ограниченной группы, то этот пользователь или группа удаляется.

- Restricted Groups: Restricted Group Is Member Of (Ограниченные группы: ограниченная группа входит в). Если ограниченная группа не входит в группу, которой она должна принадлежать, она добавляется в нее. В отличие от предписания членства в группе, описанного выше, если ограниченная группа принадлежит группе, которая здесь отсутствует, то эта ограниченная группа не удаляется.
- IP Security Policies (Политики безопасности IP). Позволяет настраивать списки и действия фильтров, правила политик, методы защиты и аутентификации, типы соединений и ключевые параметры и методы обмена.

Конфигурация пользователя:

- Windows Settings: Internet Explorer Maintenance: Security (Настройки Windows: обслуживание Internet Explorer: безопасность). Позволяет настраивать особые зоны безопасности, оценку содержимого и параметры аутентификации.
- Windows Settings: Scripts (Настройки Windows: сценарии). Позволяет указывать сценарии входа и выхода из системы.
- Administrative Templates: Windows Components: Windows Explorer (Шаблоны администрирования: компоненты Windows: Проводник Windows). Позволяет настраивать пользовательские параметры для Проводника Windows. Среди этих параметров следует отметить удаление меню File (Файл), опций Map Network Drive (Подключить сетевой диск) и Disconnect Network Drive (Отключить сетевой диск), скрытие вкладки Hardware (Оборудование), запрос аутентификационных данных для сетевых инсталляций и многое другое.
- Administrative Templates: Windows Components: Windows Installer (Шаблоны администрирования: компоненты Windows: программа установки Windows Installer). Позволяет запретить пользователям производить установку со съемных носителей, а также вносить другие изменения в конфигурацию.
- Administrative Templates: Start Menu and Taskbar (Шаблоны администрирования: меню Пуск и панель задач). Позволяет удалять папки пользователя из меню Start (Пуск), отключать и удалять ссылки на Windows Update, отключать опцию Log Off (Выход из системы) в меню Start (Пуск), отключать и удалять команду Shut Down (Завершение работы), удалять отдельные меню и др.
- Administrative Templates: Desktop (Шаблоны администрирования: Рабочий стол). Используется для скрытия всех значков Рабочего стола, запрета на изменение пользователями пути к папке My Documents (Мои документы), необходимости сохранения параметров при выходе

и др. Также позволяет настраивать элементы, связанные с Active Desktop, и взаимодействие пользователей с Active Directory.
- System: Group Policy (Система: групповая политика). Позволяет настраивать пользовательские параметры, такие как интервал обновления пользователей, выбор контроллера домена, автоматическое обновление файлов ADM и др.

Выше приведены наиболее важные компоненты оснастки Group Policies с указанием того, каким образом они связаны с безопасностью. Это лишь очень общее описание рассматриваемой области, а не полноценный обзор. Обязательно ознакомьтесь с более детальной информацией по данной теме перед тем, как вплотную заняться работой с оснасткой Group Policies.

Дополнения групповой политики в Windows

В Windows в групповую политику добавлены два отдельных элемента, связанных с безопасностью систем в AD. Этими элементами являются Software Restriction Policies (Политики ограничения программного обеспечения) (о них уже говорилось выше) и Wireless Network (IEEE 802.11) Policies (Политики беспроводных сетей [IEEE 802.11]).

Политики ограничения программного обеспечения. Функции оснастки Group Policy такие же, как у оснастки Local Security Policy (Локальная политика безопасности), однако эту оснастку можно применить к домену или OU. Параметры, связанные с безопасностью, настраиваемые с помощью данной групповой политики, включают в себя следующие настройки.

- Тип беспроводной сети, к которой могут осуществлять доступ клиенты: Ad Hoc (Точка доступа), Infrastructure (Инфраструктура) или Any (Любая).
- Возможность запрета на использование беспроводными клиентами Windows локальных параметров Windows для настройки их параметров беспроводных сетевых соединений.
- Возможность разрешить пользователям подключаться только к предпочитаемым сетям.
- Возможность требовать аутентификацию 802.1X при каждом подключении к беспроводным сетям 802.11 (см. рис. 14.4).
- Указание типа EAP: Smart Card or other certificate (Смарт-карта или другой сертификат) или Protected EAP (PEAP) (Защищенный EAP).
- Выбор метода аутентификации для использования в PEAP: Secured password (EAP-MSCHAP v2) (Защищенный пароль EAP-MSCHAP v2) или Smart Card or other certificate (Смарт-карта или другой сертификат).

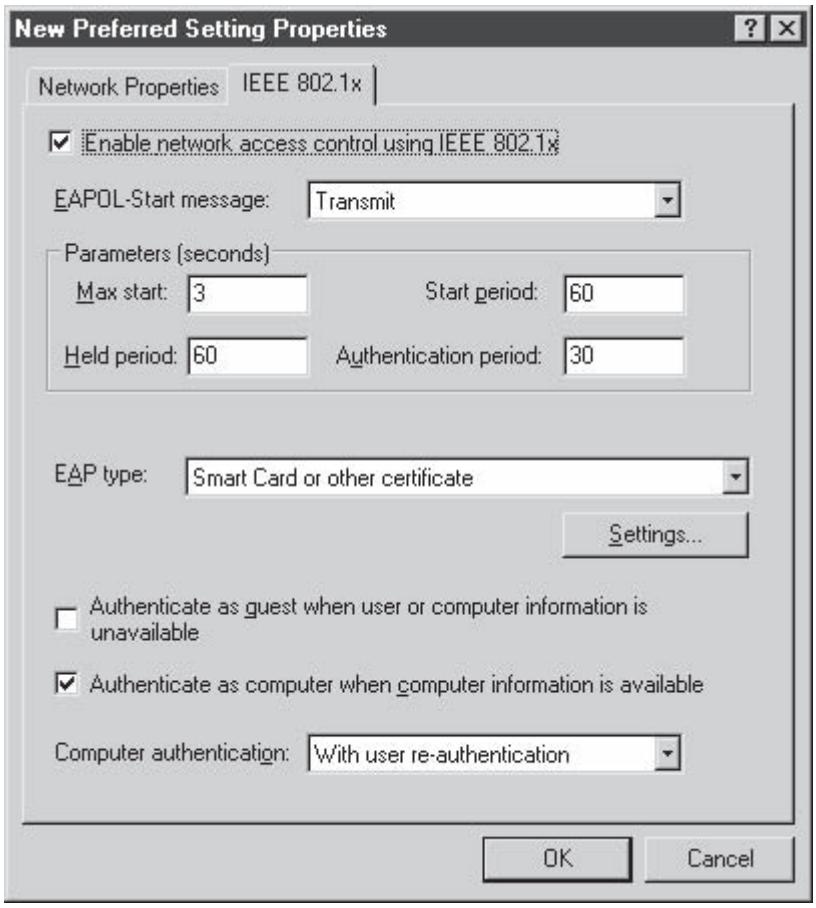

Рис. 14.4. Свойства IEEE 802.1x

Старшинство

Ниже приведены шаги, автоматически выполняемые системой при оценке/применении Group Policy.

При загрузке системы:

1. Область Computer Configuration (Конфигурация компьютера) оснастки Local Security Policy (Локальная политика безопасности).
2. Область Computer Configuration (Конфигурация компьютера) оснастки Group Policies (Групповые политики), связанной с сайтом (в порядке предпочтения - от наименее до наиболее предпочтительного).
3. Область Computer Configuration (Конфигурация компьютера) оснастки Group Policies (Групповые политики), связанной с доменом.
4. Область Computer Configuration (Конфигурация компьютера) оснастки Group Policies (Групповые политики), связанной с OU, в порядке предпочтения - от самой внешней организационной единицы до самой внутренней, и внутри OU - с самого низкого уровня до самого высокого.

При входе пользователя:

1. Области User Configuration (Конфигурация пользователя) оснастки Local Security Policy (Локальная политика безопасности).
2. Области User Configuration (Конфигурация пользователя) оснастки Site Group Policies (Групповые политики сайта) в порядке предпочтения.
3. Области User Configuration (Конфигурация пользователя) оснастки Domain Group Policies (Групповые политики домена) в порядке предпочтения.
4. Области User Configuration (Конфигурация пользователя) оснастки OU Group Policies (Групповые политики организационного подразделения) в порядке предпочтения.

Замыкание на себя

Ранее мы говорили о том, что по умолчанию GP применяются в зависимости от расположения настраиваемого объекта. Чтобы обойти эту возможность для пользователей, компания Microsoft реализовала замыкание на себя (loopback). Эта возможность используется для конфигурации пользователя групповых политик, а также конфигурации компьютера, в зависимости от расположения объекта "компьютер" (не пользователь) при входе пользователя в систему. Таким образом, каждый пользователь, осуществляющий вход в систему компьютера, получает конфигурацию пользователя (User Configuration) из групповых политик этого компьютера. При включении опции можно также указать функцию Merge (Слияние) (объединение конфигурации из всех групповых политик) или Replace (Замещение) (только применение конфигураций пользователей в зависимости от расположения объекта "компьютер").

Наследование

Во многом аналогично наследованию списков ACL, параметры GP передаются от самых дальних к самым ближним, причем ближние/низшие имеют большее старшинство. Порядок оценки таков: Local Security Policy (Локальная политика безопасности), Site Group Policies (Групповые политики сайта), Domain Group Policies (Групповые политики домена) и OU Group Policies (Групповые политики организационного подразделения). Существует возможность блокировки наследования политики, если не требуется наследовать параметры. Это позволит блокировать групповые политики, связанные с сайтами, доменами или организационными единицами высших уровней от применения их к текущему сайту, домену или организационному подразделению и к их дочерним объектам. Как администратору верхнего уровня вам может понадобиться включение принудительного использования некоторых политик верхнего уровня (например, минимальная длина пароля); для этого существует опция No Override (Игнорирование невозможно). Эту опцию можно включить для того, чтобы предотвратить обход (включая блокировку) политики любым дочерним объектом.

Примечание

По большому счету, между сайтами и доменами в действительности нет никакого "наследования". Будет происходить оценка только тех групповых политик, связанных с конкретным сайтом или доменом, в котором находится пользователь или компьютер. Организационная единица является единственным контейнером, для которого действительно наблюдается наследование при проходе вниз по дереву элементов.

Средства управления групповой политикой

Следующие утилиты весьма полезны для управления групповыми политиками и просмотра результатов их работы.

Group Policy Management Console. Утилита Group Policy Management Console (Консоль управления групповой политикой) представляет собой оснастку MMC и набор сценариев, предоставляющих единый интерфейс управления групповой политикой на предприятии. Интерфейс показан на рисунке 14.5 с отображением части политики домена по умолчанию (Default Domain Policy) для домена jiloa.com.

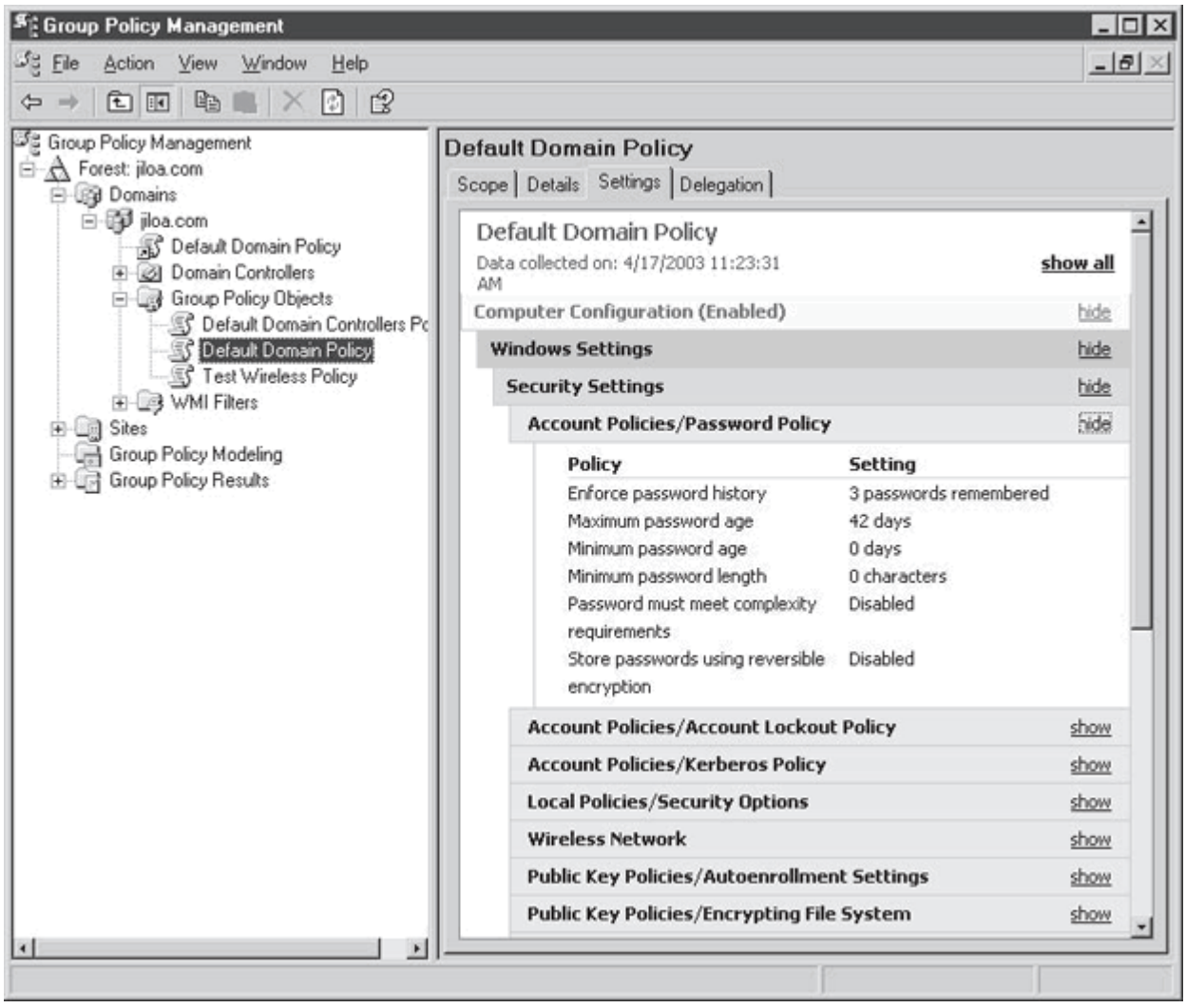

Рис. 14.5. Консоль управления групповой политикой

Group Policy Results. Консоль управления групповой политикой предоставляет средство для определения результирующей политики для данного пользователя и/или системы. (Этот метод отличается от средства Resultant Set of Policy, обсуждаемого ниже.) Чтобы сгенерировать запрос Group Policy Results (Результаты групповой политики) для пользователя/компьютера, нужно открыть лес, щелкнуть правой кнопкой мыши на пункте Group Policy Results (Результаты групповой политики) и затем выбрать Group Policy Results Wizard (Мастер результатов групповой политики). Выполните предписания мастера и введите соответствующую информацию в окнах ввода данных. На рисунке 14.6 показаны результаты запроса Group Policy Results для администратора в IHS в домене jiloa.com.

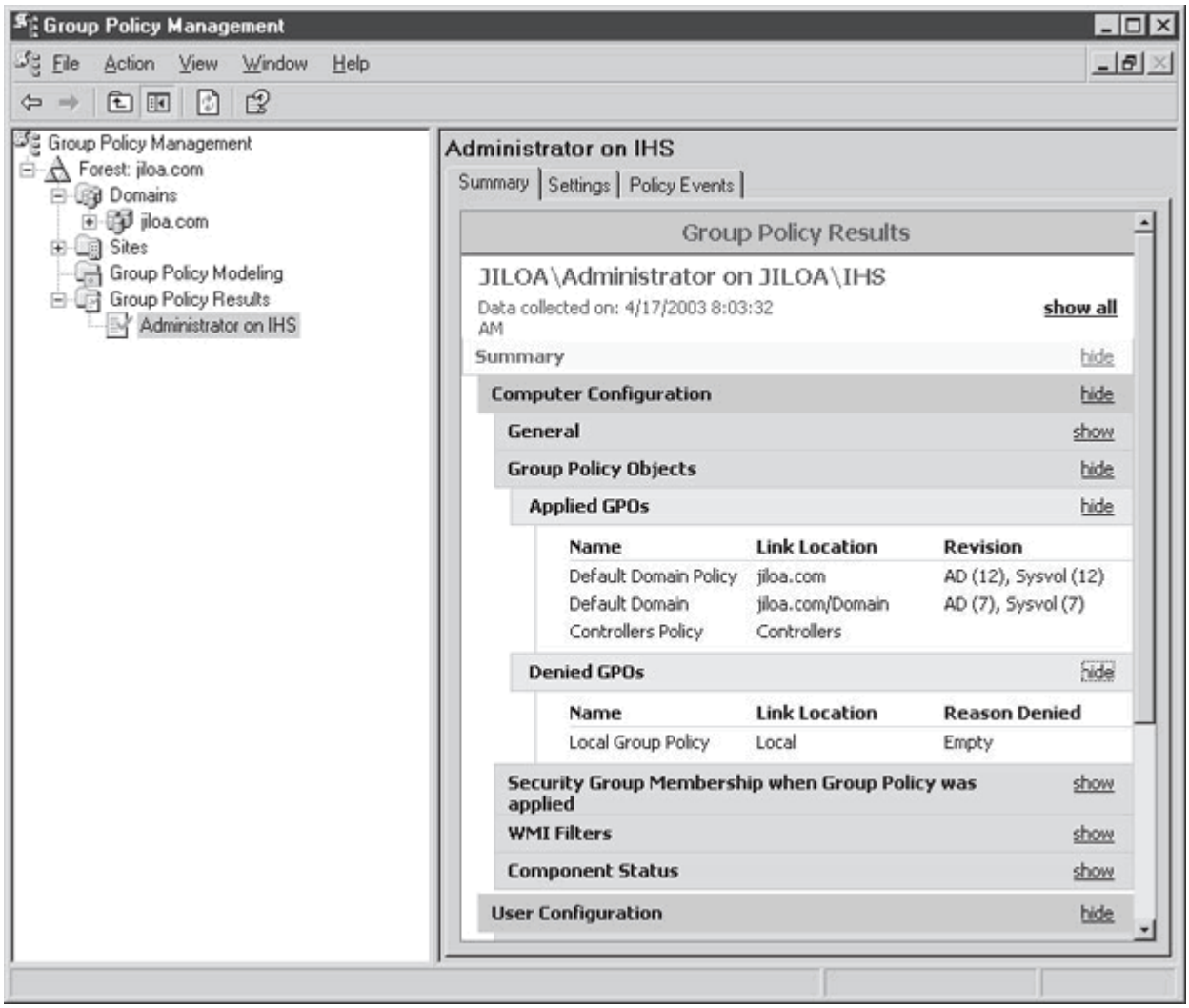

Рис. 14.6. Результаты групповой политики для администратора в IHS

Resultant Set of Policy (RSoP). Утилита предназначена для облегчения процессов применения политик и устранения неполадок в них. Она

предоставляет детальные сведения обо всех сконфигурированных параметрах политики и может помочь определить набор примененных политик и порядок, в котором они применяются. Это очень полезно, когда несколько политик применяются на различных уровнях, таких как сайт, домен и организационное подразделение (единица).

Эта утилита используется для симуляции результатов применения параметров политики, которые вы собираетесь применить к компьютеру или пользователю, а также для определения параметров текущей политики для пользователя, находящегося в данный момент в системе компьютера. На рисунке 14.7 приведен пример RSoP для политики аудита системы IHS. RSoP находится в оснастке MMC и открывается в консоли управления Microsoft (MMC), оснастке Active Directory Users and Computers (Пользователи и компьютеры Active Directory) или оснастке Active Directory Sites and Services (Сайты и службы Active Directory).

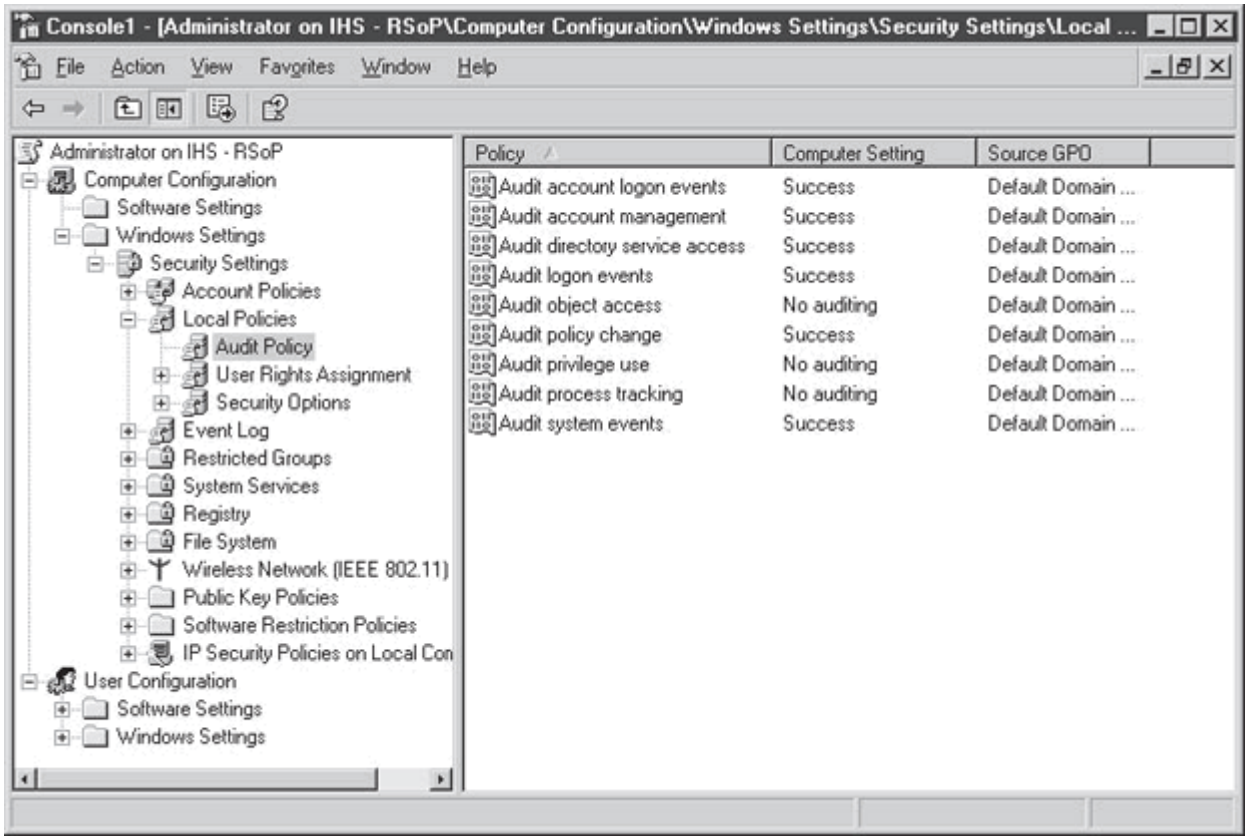

Рис. 14.7. RSoP для политики аудита на IHS

Управление пользователями и группами AD

Необходимо обеспечить правильность настроек безопасности для всех учетных записей. Это можно сделать двумя способами: посредством политики учетной записи через групповую политику в домене с рассматриваемой учетной записью или посредством отдельных ограничений в свойствах пользовательской учетной записи для конкретного объекта User

(Пользователь). Политики учетных записей применяются через оснастку Local Security Policy (Локальная политика безопасности) (об этом рассказывалось выше) или через механизм Group Policy (Групповые политики) в домене, в котором находится учетная запись. Свойства учетной записи пользователя устанавливаются для пользователей в индивидуальном порядке. Так как эти параметры специфичны для каждого пользователя, у них нет ничего общего с групповой политикой или локальными параметрами безопасности; они являются атрибутами объекта User. С помощью оснастки Active Directory Users and Computers (Пользователи и компьютеры Active Directory) можно осуществлять администрирование пользователей домена, а посредством оснастки Local Users and Groups (Локальные пользователи и группы) - администрирование локальных пользователей.

Оснастка Active Directory Users and Computers (Пользователи и компьютеры Active Directory)

При создании учетных записей пользователей основной используемой утилитой администрирования является оснастка Active Directory Users and Computers (Пользователи и компьютеры Active Directory), предназначенная для администрирования учетных записей в рамках домена Active Directory. Оснастка Active Directory Users and Computers (Пользователи и компьютеры Active Directory) (см. рис. 14.8) используется для управления пользователями, группами и другими элементами, такими как организационные единицы для доменов в лесу. По умолчанию оснастка запускается из меню Start/Programs/Administrative Tools (Пуск/Программы/Администрирование) на каждом контроллере домена. Эту оснастку также можно добавить в любую консоль MMC.

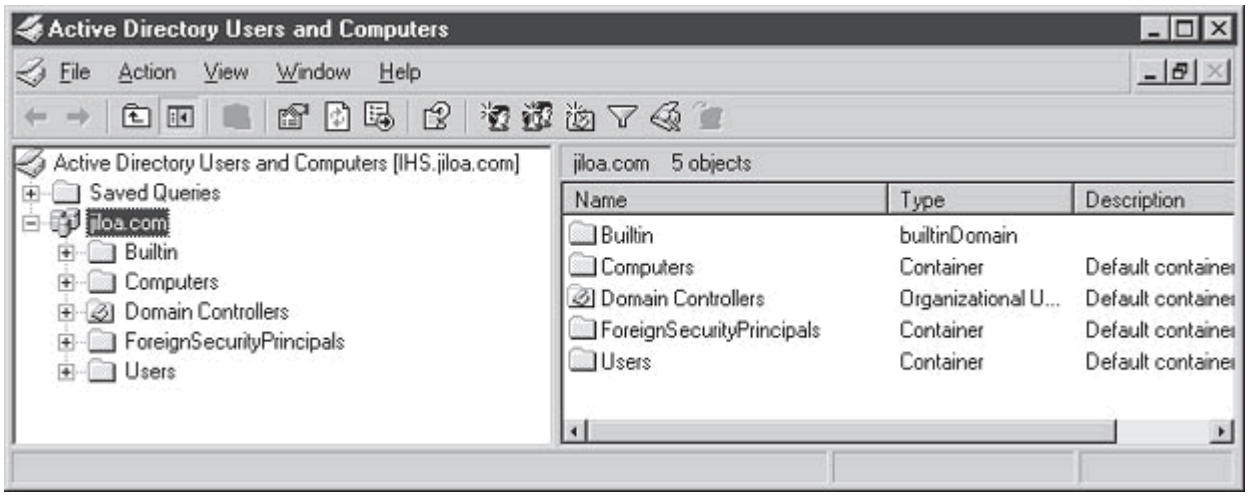

Рис. 14.8. Утилита Active Directory Users and Computers (Пользователи и компьютеры Active Directory)

Использование команды secedit для управления параметрами безопасности в Windows

Данный проект предназначен для того, чтобы продемонстрировать управление большим числом параметров безопасности системы.

Шаг за шагом

1. Начните с системы Windows, к которой у вас есть доступ с правами администратора и на которой можно вносить изменения без влияния на рабочие приложения.
2. Запустите графический пользовательский интерфейс Local Security Policy (Локальная политика безопасности) и внесите нужные изменения в параметры безопасности системы.
3. Внесите изменения в политику паролей согласно нуждам организации.
4. Проделайте то же самое для конфигурации аудита.
5. По окончании настройки конфигурации используйте команду secedit для экспортирования политики безопасности в виде файла шаблона.
6. Теперь используйте этот шаблон для анализа политики безопасности, используемой на другой системе. Проверьте результаты и выясните, можете ли вы выявить какие-либо угрозы, обусловленные изменениями, внесенными в политику.
7. Если существует возможность внести изменения во вторую систему без влияния на рабочие приложения, используйте команду secedit для конфигурации политики безопасности на этой системе.

Выводы

Утилита secedit применяется для управления параметрами безопасности набора систем. Так как это средство позволяет автоматически замещать конфигурацию любой системы, можно сконструировать сценарий, выполняемый при запуске системы или через определенные промежутки времени и обновляющий конфигурацию системы. Аналогичным образом изменения могут вноситься в конфигурацию посредством обновления шаблона.

Контрольные вопросы

1. Какая команда может использоваться для управления конфигурацией безопасности системы Windows?
2. Какие два признака могут быть обнаружены в случае проявления атаки "грубой силы", направленной на пароль?
3. Признаком какой активности является большое число неудачных попыток доступа к файлам?
4. Каков наиболее защищенный уровень шифрования для службы Terminal Services?
5. Для чего используются политики ограничения программного обеспечения?

6. Каким образом можно настроить политики ограничения программного обеспечения?
7. Каково назначение групповой политики?
8. Расскажите о доверительных взаимоотношениях в Active Directory.