

12

Управление групповыми политиками

Нам постоянно приходится сталкиваться с корпоративными политиками. Например, если припарковать автомобиль слишком близко к зданию, кто-то обязательно сделает замечание: “Эти места зарезервированы для сотрудников фирмы. Работающие по контракту должны парковаться вон там”. Или, если сделать предложение, которое слишком далеко выходит за пределы требований клиента, менеджер может показать на длинный список правил своей организации и объяснить, что “здесь так не принято”.

Я — дитя шестидесятых, поэтому мне очень тяжело быть связанным правилами и политиками, но я осознаю их необходимость. Любая организация, в которой работает больше двух человек, нуждается в политиках для определения ролей и описания поведения. Это в полной мере касается и компьютеров. Пользователи рассчитывают на возможности своих компьютеров, и персонал отдела информационных технологий не сможет удовлетворить их ожидания, если не постарается добиться определенного уровня равных возможностей на рабочих станциях и серверах.

Компания Microsoft осознала эту потребность и предложила реализовать управление рабочими станциями на основе политик. В операционной системе Windows 95 эта возможность называлась *системными политиками* (system policies). Эти политики представляли собой заранее заготовленные обновления системного реестра. Загрузка файла с обновлением выполнялась при регистрации клиента. После этого обновление вносилось в локальную копию системного реестра.

Классические системные политики были шагом в правильном направлении, но они обладали рядом серьезных ограничений.

- **Системные политики навсегда изменяют системный реестр на клиентском компьютере.** Компания Microsoft называла этот процесс *tattooing* (дословно — “татуировка”). Каждый, кто когда-либо ошибался в параметрах системной политики и рассылал файлы политики клиентам, знает, как сложно восстановить предыдущее состояние, поскольку изменения записываются непосредственно в системный реестр.
- **Системные политики позволяют управлять только ограниченным количеством процессов.** В стандартный набор системных политик входит очень небольшое количество записей системного реестра, и системные политики не могут использоваться для управления процессами, которые не используют записей системного реестра.

- **Системные политики могут распространяться только из одного файла.** В операционной системе Windows NT это файл `Ntconfig.pol`. В операционной системе Windows 9x это файл `Config.pol`. Требование по упаковке всех изменений в один файл делает системные политики очень негибкими и сложными в управлении. Существует возможность указать конкретную группу в файле с расширением `.pol`, но в таком случае получается большой файл, который сложно редактировать и долго загружать.

Начиная с операционной системы Windows 2000, компания Microsoft значительно изменила механизм управления на основе политик. Компания отказалась от статических системных политик на основе системного реестра и ввела новую возможность, которая называется *групповые политики* (group policies). В составе операционной системы Windows Server 2003 предоставляются все групповые политики, которые были доступны в операционной системе Windows 2000, а также дополнительные политики, которые позволяют использовать новые возможности операционных систем Windows Server 2003 и Windows XP.

В этой главе рассматриваются вопросы создания и распространения групповых политик, а также управление ими. Основное внимание уделяется вопросам реализации. Как работают групповые политики? Каковы требования к использованию групповых политик? Почему может нарушиться работа групповых политик в корпоративных сетях и как лучше восстановить их работу? Подробное описание групповых политик, включая большое количество примеров и рекомендаций по реализации отдельных политик приводится в книге *Windows 2000: Group Policy, Profiles, and IntelliMirror* Джереми Московица (Jeremy Moskowitz).

Новые возможности операционной системы Windows Server 2003

В составе операционной системы Windows Server 2003 компания Microsoft предоставила большое количество новых групповых политик, а также добавила новые возможности политик, которые помогают при устранении неисправностей и улучшают гибкость групповых политик. Рассмотрим эти усовершенствования.

- Свыше 160 новых групповых политик, которые позволяют управлять динамической регистрацией записей DNS, перемещаемыми профилями, серверами терминалов и работой Control Panel (Панель управления).
- Полностью интегрированная программа вычисления результирующего набора политик. Такая программа упрощает планирование и устранение неполадок в работе групповых политик в организациях с несколькими уровнями контейнеров и большим количеством политик, связанных с этими контейнерами. Расчет результирующего набора политик может осуществляться из командной строки или с помощью мастера.
- Полный журнал расчетов результирующего набора политик на каждом компьютере при регистрации пользователя. Этот журнал хранится в той же базе данных, в которой хранятся параметры работы аппаратных средств и параметры операционной системы, доступные с помощью инструментария управления WMI (Windows Management Instrumentation).
- Возможность фильтрации основанных на системном реестре политик, благодаря которой можно просмотреть только те политики, которые относятся к определенной версии Windows. Это позволяет упорядочить содержимое консоли управления и подобрать политики для соответствующих платформ.
- Новая утилита обновления групповых политик, которая называется `gpupdate` и заменяет собой непонятные переключатели утилиты `secedit`, использовавшейся в операционной системе Windows 2000. Теперь утилита `secedit` используется исключительно для применения содержимого базы данных системы безопасности и создания отчетов.

- Консоль Group Policy Management (Управление групповыми политиками), созданная в виде отдельной утилиты, предоставляет единый инструмент администрирования групповыми политиками.

Обзор функций групповых политик

Компьютерные политики имеют много общего с корпоративными политиками. Любой сотрудник отдела кадров может объяснить, что корпоративная политика может быть эффективной только в том случае, если она соответствует нескольким критериям.

- Политика должна быть изложена в ясной и простой форме.
- Пользователь должен иметь возможность выполнить действия, определенные политикой.
- Необходимо часто напоминать о политике, чтобы не допускать ее нарушения.

В следующих нескольких разделах рассматривается соответствие групповых политик Windows Server 2003 перечисленным критериям.

Назначение групповых политик

На самом простом уровне групповые политики предоставляют возможность эффективного управления большим количеством компьютеров. Иногда не удается дать точное определение термина "управлять". Например, в школах бизнеса учат, что людьми на самом деле нельзя "управлять". Люди могут разрешить, чтобы их направляли, подгоняли, заманивали или тащили по направлению к определенной цели, но они никогда не остаются без собственного мнения.

Компьютеры более податливы, чем люди, но принцип остается таким же. Компьютерами нельзя управлять насильно; они *позволяют*, чтобы ими управляли. Как будет показано далее, каждый клиент под управлением операционных систем Windows Server 2003, Windows 2000 и Windows XP имеет набор служб, которые знают, как обрабатывать инструкции, распространяемые в групповых политиках. От администратора зависит предоставление нужных инструкций нужным клиентам в нужные моменты времени.

В нескольких разделах будет рассказано, как создаются групповые политики, откуда клиенты знают, где получать групповые политики, как загружаются групповые политики и что происходит при обработке групповых политик. Вы узнаете, как реализовать каждый тип политики и устранить неполадки в работе групповых политик.

Компоненты групповых политик

Развертывание групповых политик в пределах предприятия быстро превращается в лабиринт узких проходов. Автору этой книги кажется, что компания Microsoft слишком усложнила эту операцию, связав с компонентами групповых политик перегруженную терминологию. Сначала вкратце будет описан каждый компонент, после чего компоненты будут рассмотрены более подробно.

- **Объект групповой политики (Group Policy Object — GPO).** Не пытайтесь искать в базе данных Active Directory такой объект. Компания Microsoft использует термин *объект групповой политики* в качестве синонима для идентификации двух компонентов групповой политики: *контейнера групповой политики (Group Policy Container)* и *шаблона групповой политики (Group Policy Template)*. Такие контейнеры Active Directory, как сайты, домены и организационные единицы, могут быть *связаны* (linked) с объектом групповой политики. При этом параметры объекта групповой политики применяются к объектам пользователей и компьютеров в соответствующем контейнере.

- **Шаблон групповой политики (Group Policy Template — GPT).** Шаблон групповой политики представляет собой набор инструкций, которые реализуют набор политик. Например, политики обновления системного реестра хранятся в файле шаблона групповой политики, который называется `Registry.pol`. Файлы шаблонов групповых политик хранятся в папках политик в каталоге `Sysvol` на каждом контроллере домена. Пример показан на рис. 12.1.
- **Контейнер групповой политики (Group Policy Container — GPC).** Контейнер групповой политики представляет собой объект Active Directory, в котором перечислены имена шаблонов групповой политики, связанных с определенным объектом групповой политики. Клиенты Windows используют информацию из контейнера групповой политики для определения загружаемых и обрабатываемых шаблонов групповой политики. (В документации от компании Microsoft термины *объект групповой политики* и *контейнер групповой политики* иногда заменяют друг друга.)
- **Расширение на стороне клиента (Client-Side Extension — CSE).** Групповые политики позволяют управлять различными функциями клиентов Windows. Для этих функций существуют службы, которые знают, как получать и обрабатывать предназначенные для них групповые политики. Такие службы называются расширениями на стороне клиента и предоставляются в виде динамически загружаемых библиотек DLL. Например, политики перенаправления папок обрабатываются расширением `Fdeploy.dll`.

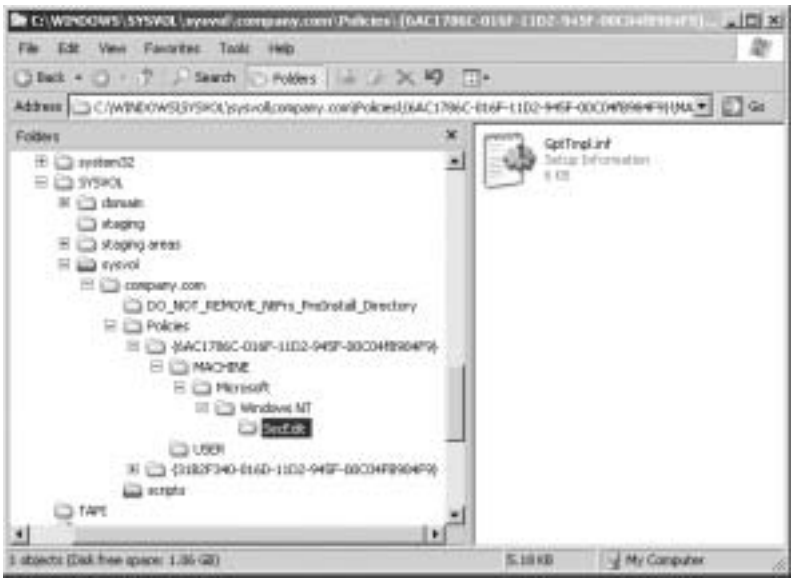


Рис. 12.1. Стандартный каталог `Sysvol`, в котором присутствуют каталоги групповых политик и файл шаблона групповой политики

- **Редактор групповой политики (Group Policy Editor — GPE).** Редактор представляет собой оснастку MMC, которая позволяет создавать объекты групповых политик и управлять ими. На рис. 12.2 показано редактирование групповой политики `Default Domain` (одного из двух объектов групповой политики, установленного в каждом домене).
- **Политики компьютеров** и **политики пользователей**. Параметры политик в объекте групповой политики могут относиться к объектам компьютеров или к объектам пользователей. Компьютеры загружают свои политики в процессе загрузки операционной системы.

Пользователи загружают свои политики при регистрации в домене. Двойственный характер объектов групповых политик является основным источником проблем при развертывании групповых политик.

- **Групповые политики** и **локальные политики**. Не все политики загружаются из домена. Каждый клиент имеет свой набор локальных политик, которые вступают в силу, если компьютер не является членом домена или регистрация пользователя выполняется с помощью локальной базы данных SAM, без регистрации в домене.

Теперь рассмотрим особенности совместного функционирования этих компонентов при создании, развертывании групповых политик и управлении ими.

Объекты групповых политик

Термин *объект групповой политики* (GPO) является общим и означает сразу две составляющие групповой политики: контейнер групповой политики (GPC) и шаблон групповой политики (GPT). Очень удобно воспринимать объект групповой политики как единый элемент, поскольку составляющие групповой политики всегда должны быть синхронизированы.

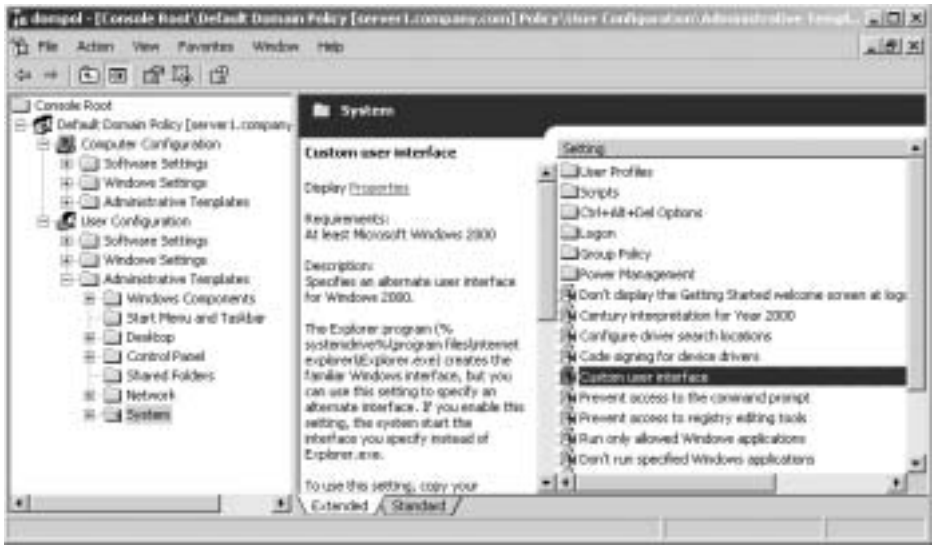


Рис. 12.2. Редактирование политики `Default Domain` *с помощью редактора групповых политик*

Просмотр и изменение объектов групповых политик

Для просмотра объектов групповых политик, связанных с определенными контейнерами Active Directory, откройте окно свойств контейнера на консоли Active Directory — Users and Computers (Active Directory — пользователи и компьютеры) или Active Directory — Sites and Services (Active Directory — сайты и службы), если речь идет о групповых политиках сайтов. Откройте вкладку Group Policy (Групповая политика). На рис. 12.3 показан пример набора групповых политик для организационной единицы.

В каждом домене Active Directory присутствуют как минимум два объекта групповых политик.

- **Default Domain.** Этот объект групповой политики содержит параметры безопасности, которые относятся ко всем компьютерам в пределах домена. Объект групповой политики связан с объектом `Domain`.

- **Default Domain Controller.** Этот объект групповой политики содержит параметры безопасности и параметры конфигурации, которые относятся ко всем контроллерам домена. Объект групповой политики связан с организационной единицей `Domain Controllers`.

Обычно групповые политики оказывают влияние только на объекты в связанных контейнерах (и на объекты в дочерних контейнерах при включении наследования). Политики объекта групповых политик `Default Domain Controller` работают немного по-другому. Этот объект групповой политики содержит множество критических параметров системы безопасности, которые важны для правильной работы контроллера домена. Таким образом, политики объекта групповой политики `Default Domain Controller` буквально отслеживают объекты контроллеров домена по всей базе данных Active Directory. Организационная единица `Domain Controller` выступает в роли якоря для объекта групповой политики.



Рис. 12.3. Окно свойств организационной единицы, в котором показан список групповых политик

Применение групповых политик с помощью утилиты `gpupdate`

Обычно новая групповая политика для пользователя не вступает в силу до завершения сеанса и повторной регистрации пользователя, а новая групповая политика для компьютера не вступает в силу до перезагрузки компьютера. Кроме этого, групповые политики периодически обновляются в результате работы фонового процесса.

Если новая групповая политика должна быть применена немедленно, можно воспользоваться утилитой `gpupdate`. Откройте приглашение командной строки и введите команду **gpupdate**. Утилита предоставлена вместо специальных параметров утилиты `Secedit`, которые использовались в операционной системе Windows 2000 для применения групповых политик. Параметр `/target` утилиты `gpupdate` позволяет указать политики для пользователей или компьютеров, например `gpupdate /target:user` или `gpupdate /target:computer`.

Если применяется пользовательская групповая политика, которая требует завершения сеанса пользователя и последующей регистрации, можно воспользоваться параметром `/logoff`, например `gpupdate /target:user /logoff`. Если политика, примененная таким образом, не оказывает влияния на расширения на стороне клиента, требующее завершения сеанса, то завершения сеанса не происходит.

Если применяется групповая политика для компьютеров, которая требует перезагрузки компьютеров для вступления в силу, можно воспользоваться параметром `/boot`, например `gpupdate /target:computer /boot`. Если такая политика не оказывает влияния на расширения на стороне клиента, требующие перезагрузки, перезагрузка не выполняется.

Обычно утилита `gpupdate` загружает и применяет только те групповые политики, которые изменились с момента последней загрузки групповых политик. Это позволяет сэкономить пропускную способность сети. Если необходимо загрузить и применить все политики, воспользуйтесь параметром `/force`, например `gpupdate /force`.

Номера версий объектов групповых политик

Система отслеживает изменения в групповых политиках, увеличивая атрибут *номера версии* при каждом изменении объекта групповой политики. Номер версии имеет интересный формат, так как система отслеживает обновления раздела Computer Configuration (Конфигурация компьютера) отдельно от изменений раздела User Configuration (Конфигурация пользователя) с тем же номером версии. Рассмотрим, как увеличивается номер версии объекта групповой политики.

- При внесении изменений в параметры политик в разделе Computer Configuration (Конфигурация компьютера) номер версии объекта групповой политики увеличивается на единицу.
- При внесении изменений в параметры политик в разделе User Configuration (Конфигурация пользователя) номер версии объекта групповой политики увеличивается на 65 536.

Система рассматривает два компонента номера версии объекта групповой политики как *номер редакции* (revision number) каждого компонента. Чтобы узнать номер версии объекта групповой политики, сначала номер версии нужно разделить на 65 536. Результат является номером редакции раздела `User`. Остаток является номером редакции раздела `Computer`. Например, номер версии объекта групповой политики 131 075 дает номер редакции `User`, равный 2, и номер редакции `Computer`, равный 3.

Номера редакций компонентов объекта групповой политики доступны в окне свойств объекта GPO (рис. 12.4).



Рис. 12.4. Окно свойств объекта GPO, в котором показаны номера редакции каждого компонента

Хранение номера версии объекта групповой политики

На самом деле отдельного объекта групповой политики не существует, поэтому номер версии должен храниться где-то в другом месте. Объект групповой политики состоит из контейнера групповой политики и шаблона групповой политики. Копия номера версии хранится в каждом компоненте следующим образом.

- Объект контейнера групповой политики в базе данных Active Directory хранит номер версии в атрибуте `VersionNumber`. Ниже приведен фрагмент списка атрибутов контейнера групповой политики:

```
versionNumber 65538
gPCFunctionalityVersion: 2;
gPCFileSysPath: \\company.com\SysVol\company.com\Policies\
 {5D769292-2424-4D93-ABBC-3EDD73BC58FB};
gPCMachineExtensionNames; [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
{0F6B957E-509E-11D1-A7CC-0000F87571E3}];
gPCWQLFilter: [company.com;{F76FB374-E3B3-434E-953D-0FDDFB634FCF};0];
```

- Номер версии контейнера групповой политики хранится в файле `Gpt.ini` в корневом каталоге политики в папке `Sysvol`:

```
[General]
Version=65538
displayName=TestGPO
```

Исправление ошибок при синхронизации объектов GPO

Номера версий контейнеров групповых политик (GPC) и шаблонов групповых политик (GPT) всегда должны совпадать в пределах одного объекта групповой политики (GPO). Содержимое двух компонентов GPO всегда должно совпадать на конкретном контроллере домена. Любое отличие на протяжении длительного периода времени означает, что произошла ошибка репликации.

Номера версий GPT и GPC могут различаться в течение коротких периодов времени из-за использования различных методов репликации для распространения изменений.

- Изменения в контейнере групповой политики распространяются с помощью механизма репликации Active Directory. Для распространения обновлений в пределах сайта требуется 15 минут. Для распространения обновления за пределами сайта требуется 3 часа.
- Изменения в шаблоне групповой политики, который расположен в каталоге `Sysvol`, реплицируются средствами службы репликации файлов. Служба репликации файлов работает значительно быстрее, чем репликация Active Directory. В большинстве случаев изменения в каталоге `Sysvol` реплицируются немедленно.

Во избежание проблем, связанных с более медленной репликацией GPC по сравнению с репликацией GPT, клиент загружает обновленный GPT, даже если номер версии не совпадает с номером версии соответствующего GPC. Это значит, что не существует явного метода определения различия в номерах версий шаблонов и контейнеров групповых политик. Придется периодически проверять номера версий.

Лучшей утилитой для отслеживания различий в номерах версий шаблонов и контейнеров групповых политик, а также различий в содержимом объектов групповых политик на разных контроллерах домена является `gpotool`, которая предоставляется в составе Resource Kit. Эта утилита должна запускаться каждый вечер с помощью Sheduler (Планировщик заданий). Результаты запуска утилиты должны быть сохранены в файле для просмотра администратором на следующее утро.

Для быстрой проверки совпадения номеров версий шаблонов и контейнеров групповых политик можно воспользоваться утилитой `Replmon` (монитор репликации), которая предоставля-

ется в составе Support Tools. Щелкните правой кнопкой мыши на пиктограмме сервера и выберите из контекстного меню команду Show Group Policy Object Status (Показать состояние объекта групповой политики). Пример использования этой утилиты показан на рис. 12.5.

Журнал диагностики службы репликации файлов

Если предполагается, что проблема несовпадения номеров версий шаблонов и контейнеров групповых политик на различных контроллерах домена связана с ошибками в работе службы репликации файлов, попытайтесь включить отладочный журнал службы. Для этого придется внести изменения в системный реестр. Добавьте следующую запись (значение записи `5` включает наиболее полную диагностику):

Раздел: `HKLM\System\CurrentControlSet\Services NtFrs\Parameters`

Запись: `DebugLogSeverity (REG_DWORD)`

Значение: `5`

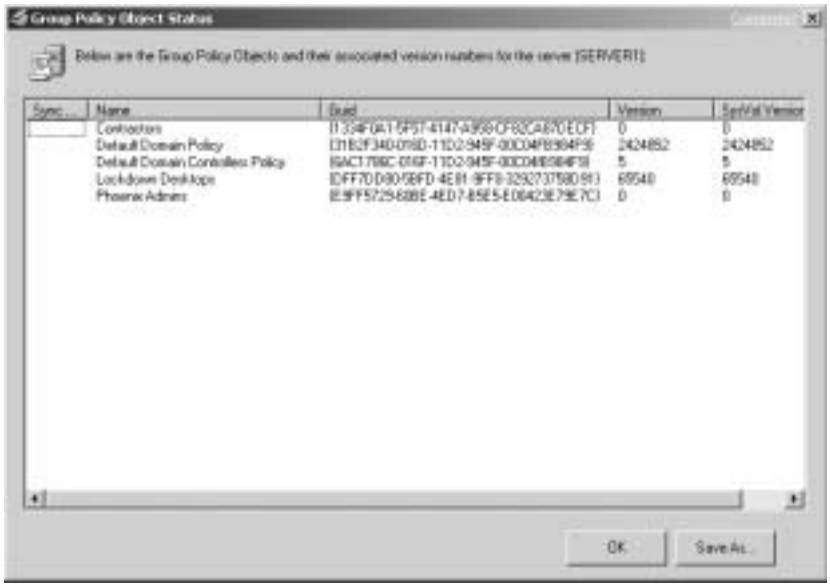


Рис. 12.5. В окне утилиты `Replmon` отображается состояние синхронизации объектов GPO

Расширения на стороне клиента

Если у вас есть дети, если вы сами росли в многодетной семье или знакомы с другими людьми, которые имеют детей (я никого не пропустил?), то вы отлично себе представляете принципы работы групповых политик.

Когда пятилетнему ребенку говорится “Не пачкай туфли в грязи”, родитель ожидает, что размазывание грязи по туфлям немедленно прекратится. Не нужно объяснять, как поднять ногу и как сохранять равновесие при разном расстоянии от ног до земли, так как ребенок уже обладает этими навыками. Короткая и простая директива должна побудить к правильному поведению. (В разделах, посвященным вопросам устранения неисправностей, на протяжении всей главы приводятся рекомендации на случай, если компьютер начнет себя вести, как *настоящий* пятилетний ребенок.)

Операционная система Windows Server 2003 предоставляет 11 функций, которые до определенной степени управляются групповыми политиками. За двумя исключениями (служба удаленной установки и программные ограничения) каждая из функций имеет службу, которая работает на клиенте и обрабатывает групповые политики. Эти службы называются расширениями на стороне клиента (Client-Side Extension — CSE). Каждое расширение работает, как часть динамически расширяемой библиотеки. В табл. 12.1 перечислены управляемые групповыми политиками функции и связанные с ними расширения на стороне клиента.

Таблица 12.1. Типы групповых политик и расширения на стороне клиента

Тип групповой политики	Библиотека реализации
`Administrative Templates` (Административные шаблоны (реестр))	`Userenv.dll`
`Folder Redirection` (Перенаправление папок)	`Fdeploy.dll`
`Scripts` (Сценарии загрузки/завершения работы)	`Gptext.dll`
`Security` (Параметры безопасности)	`Scecli.dll`
`Software Installation` (Установка программного обеспечения)	`Appmgmt.dll`
`Microsoft Disk Quota` (Квоты на пространство на диске)	`Dskquota.dll`
`EFS Recovery` (Восстановление зашифрованной файловой системы и инфраструктура открытого ключа PKI)	`Scecli.dll`
`Internet Explorer Branding` (Обслуживание Internet Explorer)	`Iedkcs32.dll`
`IP Security (IPSEC)`	`Gptext.dll`
`RIS` (Службы удаленной установки)	См. примечание 1
`QoS Packet Scheduling` (Составление расписания для пакетов QoS)	`Gptext.dll`
`Software Restrictions` (Программные ограничения)	См. примечание 2
`Wireless Networking` (Беспроводные сети)	`Gptext.dll`

Примечание 1. Политики служб удаленной установки (RIS) не используют расширения на стороне клиента. RIS-сервер получает содержимое политики при получении службой Binary Negotiation Layer (BINL) запроса на соединение от RIS-клиента. Политика определяет, какие файлы с расширением `.osc` сервер служб удаленной установки (RIS-сервер) будет использовать как часть мастера установки.

Примечание 2. Программные ограничения реализуются непосредственно операционной системой на основе записей системного реестра, добавленных политикой. Отдельное расширение на стороне клиента не используется.

Запоминать расширения на стороне клиента не обязательно, но желательно помнить, что каждое расширение использует специальные методы обработки для полученных групповых политик. Можно назвать такие методы специальной обработки.

- Фоновое обновление
- Синхронная обработка
- Обработка по низкоскоростному каналу
- Принудительные обновления
- Обработка сценариев

Ниже приводится подробная информация о специальных методах обработки и способах их настройки.

Совет по использованию системного реестра: список расширений на стороне клиента

Список расширений на стороне клиента доступен в разделе `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions`.
Для идентификации расширений на стороне клиента в списке используется идентификатор класса (ClassID — еще один термин для обозначения глобально уникального идентификатора). За одним исключением (`Default`) в записи для раздела расширения на стороне клиента указано легко понятное имя. Исключением является политика `Administrative Templates`, которая показана в списке полужирным шрифтом и не имеет значения (`Default`).

```
{25537BA6-77A8-11D2-9B6C-0000F8080861} = Folder Redirection
{35378EAC-683F-11D2-A89A-00C04FBBCFA2} = <Administrative Templates>
{3610eda5-77ef-11d2-8dc5-00c04fa31a66} = Microsoft Disk Quota
{426031c0-0b47-4852-b0ca-ac3d37bfcb39} = QoS Packet Scheduler
{42B5FAAE-6536-11d2-AE5A-0000F87571E3} = Scripts
{827D319E-6EAC-11D2-A4EA-00C04F79F83A} = Security
{A2E30F80-D7DE-11d2-BBDE-00C04F86AE3B} = Internet Explorer Branding
{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A} = EFS Recovery
{c6dc5466-785a-11d2-84d0-00c04fb169f7} = Software installation
{e437bc1c-aa7d-11d2-a382-00c04f991e27} = IP Security
{0ACDD40C-75AC-47ab-BAA0-BF6DE7E7FE63} = Wireless
```

Этот список можно использовать при включении отладки для отслеживания проблем в работе групповых политик. В некоторых журналах отладки расширения указываются с помощью идентификатора класса, а не дружественного имени.
При просмотре списка расширений в редакторе системного реестра можно обратить внимание, что четыре расширения на стороне клиента управляются одной библиотекой `Gptext.dll`, которая содержит функции для составления расписания для пакетов QoS, IPSec, беспроводной сети и сценариев. Это не оказывает влияния на работу системы, но может ввести в заблуждение при просмотре журналов отладки.

Фоновое обновление

Компьютерные политики применяются при загрузке компьютера. Пользовательские политики применяются при регистрации пользователя. Это кажется достаточно простым, но это не все. В течение дня политики могут меняться, а принудительное завершение пользовательских сеансов и перезагрузка компьютеров не всегда допустимы. По этой причине расширения на стороне клиента время от времени запрашивают обновления групповых политик.

По умолчанию контроллеры домена обновляют групповые политики каждые 5 минут, а обычные серверы и рабочие станции обновляют групповые политики от 90 до 120 минут. (Период выбирается случайным образом, чтобы предотвратить одновременное обращение клиентов к регистрационному серверу.) Два типа политик не поддерживают фоновое обновление, так как это приведет к нестабильности в работе.

- `Folder Redirection` (Перенаправление папок)
- `Software Distribution` (Распространение программного обеспечения)

Политики сценариев обрабатываются в процессе фонового обновления, но не вступают в силу, пока пользователь не завершит сеанс и не зарегистрируется в системе повторно (или, в случае компьютера, до перезагрузки).

Политики программных ограничений обновляются в фоновом режиме и вступают в силу немедленно. Но способ реализации программных ограничений может привести к странному "поведению" системы.

При запуске клиентского процесса программные ограничения читаются из системного реестра. Ограничения кэшируются для ускорения последующей обработки. Это значит, что работающий процесс не обнаружит новых ограничений до перезапуска процесса. Так как

большинство приложений запускается из Explorer, такая инициализация требует завершения сеанса. (Explorer можно остановить и перезапустить из Task Manager (Диспетчер задач), но обычные пользователи нечасто выполняют такие операции.)

Существует исключение из требования завершения сеанса при использовании политик программных ограничений. Консоль интерпретатора командной строки (`CMD`) работает независимо от Explorer, поэтому при получении новых программных ограничений они становятся доступными в командной строке, но никак не влияют на оболочку Explorer. Это может ввести пользователей в заблуждение, поэтому подготовьте службу поддержки к получению нескольких звонков от опытных пользователей после введения политик программных ограничений.

Синхронная обработка

Загрузка и обработка политик расширениями на стороне клиента требует некоторого времени. Для пользователей это выглядит, как задержка при утренней регистрации, а одной из главных целей проектирования Windows XP (и Windows Server 2003) считалась минимизация таких задержек при регистрации. Чтобы понять принципы минимизации задержек в результате обработки групповых политик, рассмотрим два варианта обработки.

- **Синхронный.** При такой обработке все расширения на стороне клиента должны завершить свою работу до передачи управления вызвавшему процессу. В случае компьютерных политик вызывающим процессом является `Winlogon`. В случае пользовательских политик вызывающим процессом является `Userenv`. Термин "синхронный" в данном случае не совсем корректен, поскольку под "синхронным" обычно подразумевается "одновременный" процесс. Здесь "синхронный" означает, что процессы выполняются последовательно.
- **Асинхронный.** Управление передается вызывающему процессу сразу после начала обработки расширением на стороне клиента.

Изменение интервала фонового обновления

Интервал фонового обновления можно изменить с помощью двух групповых политик, расположенных в разделе Computer Configuration⇨Administrative Templates⇨System⇨Group Policy (Конфигурация компьютера⇨Административные шаблоны⇨Система⇨Групповая политика).

- `Group Policy Refresh Interval for Computers` (Интервал обновления групповых политик для компьютеров)
- `Group Policy Refresh Interval for Domain Controllers` (Интервал обновления групповых политик для контроллеров домена)

Кроме стандартного интервала обновления от 90 до 120 минут, клиенты обновляют политики безопасности каждые 16 часов. В процессе обновления клиент загружает все политики безопасности, не обращая внимания на отсутствие изменений.

В отличие от интервалов фонового обновления, составляющих 5 и 90 минут, которые управляются значениями в разделе `Policies` в системном реестре, интервал обновления 16 часов (960 минут) жестко закодирован в системном реестре в разделе `Winlogon\Parameters`. Интервал контролируется следующей записью:

Раздел: `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{82...}`

Запись: `MaxNoGPOListChangesInterval`

Значение: `3c0 (960)`

При использовании синхронной обработки пользователю не предоставляется регистрационное окно до завершения обработки компьютерных политик и не предоставляется доступ к рабочему столу до завершения обработки пользовательских политик. В операционной сис-

теме Windows 2000 такой метод обработки принят по умолчанию, кроме обработки пользовательских регистрационных сценариев, которые обрабатываются асинхронно.

При использовании асинхронной обработки регистрационное окно предоставляется пользователю, когда компьютерные политики продолжают обрабатываться, а рабочий стол предоставляется, пока обрабатываются пользовательские политики. Это позволяет ускорить доступ к рабочему столу. По умолчанию в операционных системах Windows XP и Windows Server 2003 используется асинхронная обработка.

Асинхронная обработка может привести к нестабильной работе системы, если параметры компьютера или компоненты пользовательской среды зависят от параметров групповых политик. По этой причине два типа политик требуют специальной обработки: перенаправления папок и развертывания программного обеспечения. Если сценарии должны выполняться последовательно или завершаться до того, как пользователь получит доступ к рабочему столу, включите групповую политику, которая называется `Run Logon Script Synchronously` (Запускать регистрационные сценарии синхронно).

Тщательно проверьте сценарии перед включением этой политики. Если сценарий "зависнет", пользователь не сможет получить доступ к рабочей станции. Максимальное время на обработку каждого сценария составляет 10 минут. Все групповые политики должны быть обработаны в течение 60 минут. Это слишком долго, чтобы ждать завершения "зависшего" сценария.

Ограничение в 60 минут не может быть изменено с помощью групповой политики или записи в системном реестре. Время обработки отдельного сценария можно изменить с помощью групповой политики `Maximum Wait Time For Group Policy Scripts` (Максимальное время ожидания для сценария групповой политики). Политика хранится в разделе Computer Configuration⇨Administrative Templates⇨System⇨Scripts (Конфигурация компьютера⇨Административные шаблоны⇨Система⇨Сценарии).

Обработка по низкоскоростному каналу

Уже почти можно сделать вывод, что ничего сложного в развертывании групповых политик нет, но мы забыли рассмотреть клиенты, которые подключаются с использованием удаленного доступа по низкоскоростным коммутируемым каналам или линиям ISDN/DSL.

Обработка групповых политик и инициализация сети

Еще одной уловкой компании Microsoft для ускорения регистрации является предоставление пользователю рабочего стола до окончания инициализации сетевой подсистемы. Это позволяет значительно ускорить процесс регистрации, но "побочные эффекты" такого решения отражаются на групповых политиках.

Отложенная проверка сетевой инициализации заставляет выполнять две регистрации для реализации политики развертывания программного обеспечения. При первой регистрации политика устанавливается, а при второй регистрации загружается программный пакет.

Еще одним примером является использование расширенных возможностей в политике перенаправления папок для выбора определенной группы. В этом случае необходимы три регистрации: при первой устанавливается политика, при второй обнаруживается группа, а при третьей реализуется перенаправление папок.

Метод проверки сети можно вернуть в режим, использовавшийся в операционной системе Windows 2000. Для этого можно воспользоваться политикой `Always Wait For The Network At Computer Startup And Logon` (Всегда ожидать завершения инициализации сети при загрузке компьютера и регистрации). Эта политика хранится в разделе Computer Configuration⇨Administrative Templates⇨System⇨Logon (Конфигурация компьютера⇨Административные шаблоны⇨Система⇨Регистрация).

Каждое расширение на стороне клиента использует свой способ обработки политик при низкоскоростном подключении. Следующие типы политик всегда обрабатываются независимо от скорости подключения.

- Политики безопасности (включая политики шифрованной файловой системы и IPSec)
- Административные шаблоны (системный реестр)
- Программные ограничения

Следующие типы политик не обрабатываются при использовании низкоскоростного подключения, если их обработку не настроить специально.

- Параметры квот
- Перенаправление папок
- Регистрационные сценарии (загрузка/завершение работы)
- Обслуживание Internet Explorer
- Создание расписания для пакетов QoS
- Установка программного обеспечения

Для переопределения использования расширения через низкоскоростной канал можно воспользоваться параметром `Allow Processing Across A Slow Network Connection` (Разрешить обработку через низкоскоростное соединение) соответствующей политики в разделе Computer Configuration⇨Administrative Templates⇨System⇨Group Policy (Конфигурация компьютера⇨Административные шаблоны⇨Система⇨Групповая политика).

Принудительные обновления

По умолчанию клиент сохраняет пропускную способность сети и сокращает длительность регистрации, загружая только те групповые политики, которые изменились с момента последней загрузки.

Для проверки актуальности объекта групповой политики клиент проверяет номер версии, назначенный компонентам объекта групповой политики:

- номер версии в файле `Gpt.ini` в корневом каталоге политики в папке `Sysvol`;
- номер версии объекта GPC в базе данных Active Directory.

Изменение предельной скорости низкоскоростного соединения

Операционная система Windows Server 2003 определяет низкоскоростное подключение как подключение со скоростью передачи данных менее 500 Кбит/с. Система определяет скорость соединения с помощью отправки последовательности ICMP-запросов с заданной полезной нагрузкой и измерения времени до получения ответа.

Если некоторые пользователи подключаются к локальной сети офиса через виртуальную частную сеть по высокоскоростному соединению DSL или через кабельный модем, скорость соединения может превышать 500 Кбит/с и пользователи будут загружать групповые политики. По ряду причин эту возможность желательно отключить. Соединение со скоростью передачи данных 500 Кбит/с отлично подходит для работы в Интернет, но оказывается слишком медленным для загрузки программного обеспечения. Кроме этого, не стоит применять групповые политики на домашних компьютерах пользователей, на которых пользователи не имеют доступа к корпоративной службе поддержки.

Предельную скорость, согласно которой определяется низкоскоростной канал, можно изменить с помощью групповой политики `Group Policy Slow Link Detection` (Определение низкоскоростного соединения для групповых политик). Политика хранится в разделе Computer Configuratoin⇨Administrative Templates⇨System⇨Group Policy (Конфигурация компьютера⇨Административные шаблоны⇨Система⇨Групповая политика).

Каждый раз, когда клиент загружает содержимое объекта групповой политики, клиент сохраняет номер версии из контейнера групповой политики. Номер версии хранится в системном реестре в разделе `HKLM\Software\Microsoft\Windows\CurrentVersion\GroupPolicy\History`.

В следующий раз при сканировании объектов групповых политик клиент сравнивает номер версии в файле `Gpt.ini` и в контейнере групповой политики. Если номер любой из версий больше, чем номер версии, сохраненный в системном реестре, клиент обрабатывает групповую политику.

Можно заставить клиента игнорировать номера версий при обработке объектов групповых политик. В этом случае клиент загрузит все политики, даже если они не изменились. Для этого используется групповая политика `Process Even If The Group Policy Objects Have Not Changed` (Обрабатывать объекты групповых политик, даже если они не изменились). Эту политику необходимо указать для каждого расширения на стороне клиента. Политики для расширений на стороне клиента хранятся в разделе Computer Configuration⇨Administrative Templates⇨System⇨Group Policy (Конфигурация компьютера⇨Административные шаблоны⇨Система⇨Групповая политика).

Обработка сценариев

В операционной системе Windows 2000 пользовательские сценарии входа в систему запускаются асинхронно, даже если все остальные политики, включая сценарии загрузки компьютеров, запускаются синхронно. В операционных системах Windows Server 2003 и Windows XP все политики обрабатываются асинхронно. Если сценарии входа пользователей в систему должны быть завершены до предоставления доступа к рабочему столу, включите групповую политику, которая называется `Run Logon Script Synchronously` (Синхронно выполнять сценарии входа в систему). Политика расположена в разделе User Configuration⇨Administrative Templates⇨System⇨Scripts (Конфигурация пользователя⇨Административные шаблоны⇨Система⇨Сценарии).

Перед установкой этой политики тщательно проверьте сценарии. Если сценарий "зависнет", пользователь длительное время не сможет получить доступ к рабочему столу. Сценарию предоставляется 10 минут на завершение. Если сценарий все еще не завершил работу, система завершает его обработку и переходит к обработке следующего сценария. Если и следующий сценарий "зависнет", пользователю придется ждать еще 10 минут.

Обработка всех групповых политик должна завершиться в течение 60 минут. Это ограничение не может быть изменено с помощью групповой политики или записи системного реестра. Ограничение в 10 минут на обработку сценария можно изменить с помощью групповой политики `Maximum Wait Time For Group Policy Scripts` (Максимальное время завершения сценариев групповых политик). Политика хранится в разделе Computer Configuration⇨Administrative Templates⇨System⇨Scripts (Конфигурация компьютера⇨Административные шаблоны⇨Система⇨Сценарии).

Шаблоны групповых политик

Параметры, составляющие конкретную групповую политику, хранятся в одном или нескольких шаблонах групповых политик (Group Policy Template — GPT). Большинство групповых политик сохранено в виде файлов, которые загружаются и обрабатываются клиентами. Существует два исключения: политики инфраструктуры открытого ключа и политики IPSec. Они хранятся непосредственно в базе данных Active Directory. Файлы GPT хранятся в каталоге `Sysvol` на каждом контроллере домена.

> **Принудительная обработка политик из командной строки**
>
> Команда `gpupdate /force` заставляет клиент игнорировать номера версий и загружать все политики независимо от параметров расширений на стороне клиента.

За исключением двоичных файлов с расширениями .aas, которые используются при развертывании программного обеспечения, файлы шаблонов групповых политик являются текстовыми файлами. В них нет ничего сложного. Групповые политики не используют загадочные клиент/серверные операции. Клиент загружает текстовый файл и выполняет инструкции, описанные в этом файле.

В табл. 12.2 перечислены типы групповых политик и связанные с ними шаблоны GPT.

Таблица 12.2. Типы групповых политик и соответствующие файлы шаблонов

Тип групповой политики	Файл групповой политики
Системный реестр (административные шаблоны)	`Registry.pol`
Перенаправление папок	`Fdeploy.ini`
Регистрационные сценарии (загрузка/отключение)	`Script.ini` и сами файлы сценариев
Параметры безопасности	`Gpttmpl.inf`
Развертывание программного обеспечения	Файлы с расширением `.aas`
Дисковые квоты	`Registry.pol` (см. примечание 1)
Восстановление шифрованной файловой системы (EFS Recovery) и инфраструктура открытого ключа (PKI)	Сертификаты хранятся в базе данных Active Directory
IP Security	Политики хранятся в базе данных Active Directory
Обслуживание Internet Explorer	`Install.ins`
Службы удаленной установки	`Oscfilter.ini`
Составление расписания для пакетов QoS	Нет
Программные ограничения	`Registry.pol` (см. примечание 1)

> **Примечание 1.** Параметры квот и программных ограничений распространяются в файле `Registry.pol`, но обрабатываются раздельно

Создание шаблонов групповых политик

Рассмотрим пример использования редактора групповых политик для создания файлов GPT. Предположим, что создается объект групповой политики (GPO) под названием `Desktop Lockdown`, который связывается с организационной единицей `Phoenix`. В объекте групповой политики определяются три параметра.

- Параметр в системном реестре, который скрывает пиктограмму My Network Places (Мое сетевое окружение) на рабочем столе.
- Параметры безопасности, которые предоставляют аутентифицированным пользователям возможность устанавливать время на локальных рабочих станциях.
- Параметры перенаправления папок, которые перемещают папки My Documents (Мои документы) всех пользователей в папку с именем пользователя на совместно используемом ресурсе `\\Server\Docs`.

При создании такого GPO редактор создает объект GPC в базе данных Active Directory и папку политики в каталоге `Sysvol\<имя_домена>\Policies`. Контейнеру GPC и каталогу назначаются одинаковые имена. Имя создается с помощью того же алгоритма, который используется для создания глобально уникальных идентификаторов GUID. Это позволяет сохранять уникальность групповых политик даже в случае изменения дружественного имени. Дружественное имя является одним из атрибутов объекта GPC в базе данных Active Directory.

Папка политики в этом примере будет содержать три файла шаблона групповой политики.

- Файл `Registry.pol`, в котором хранится значение параметра `NoNetHood`.
- Файл `GptTempl.inf`, в котором содержится запись, предоставляющая привилегию `SeSystemTimePrivilege` идентификатору безопасности `S-1-5-11`.
- Файл `Fdeploy.ini`, в котором содержатся следующие строки:

```
[FolderStatus]
MyDocuments=11
[My Documents]
S-1-1-0=\\server1\docs\%username%\My Documents
```

Новая папка политики и файлы GPT реплицируются на другие контроллеры домена с помощью службы репликации файлов. Служба репликации файлов (FRS) распространяет изменения в каталоге `Sysvol` немедленно. Эта служба не подчиняется правилам пятиминутных уведомлений в пределах сайта и частоте опроса, заданной для связей сайтов между связующими серверами.

Контейнеры групповых политик

Контейнер групповой политики (Group Policy Container — GPC) является объектом в базе данных Active Directory. Для GPC созданы атрибуты, которые указывают на файлы шаблона GPT, связанного с определенной политикой и расширениями на стороне клиента, необходимыми для обработки GPT. Ниже приведен фрагмент списка атрибутов контейнера групповой политики `Default Domain`:

```
cn: {31B2F340-016D-11D2-945F-00C04FB984F9};
displayName: Default Domain Policy;
gPCFileSysPath: \\company.com\sysvol\company.com\Policies\
↪ {31B2F340-016D-11D2-945F-00C04FB984F9};
gPCFuntionalityVersion: 2;
gPCmachineExtensionNames: [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
↪{53D6AB1B-2488-11D1-A28C-00C04FB94F17}{53D6AB1D-2488-11D1-A28C-
↪ 00C004FB94F17}][{827D319E-6EAC-11D2A4EA-00C04F79F83A}
↪ {803E14A0-B4FB-11D0-A0D0-00A0C90F574B}][{B1BE8072-6EAC-11D2-A4EA-
↪ 00C04F79F83A}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}
↪ {53D6AB1D-2488-11D1-A28C-00C04FB94F17}];
gPCUserExtensionNames: [{3060E8D0-7020-11D2-842D-00C04FA372D4}
↪{3060E8CE-7020-11D2-842D-00C04FA372D4}];
gPCWQLFilter: [company.com;{F76FB374-E3B3-434E-953D-0FDDFB634FCF};0]; 1>
```

Ниже приводится описание атрибутов.

- Атрибут `GPCFileSysPath` указывает путь, по которому необходимо искать файлы GPT.
- Атрибут `GPCMachineExtensionNames` указывает идентификатор класса расширений на стороне клиента, которые клиент будет использовать для обработки файлов GPT для политик компьютера.
- Атрибут `GPCUserExtensionNames` указывает идентификатор класса расширений на стороне клиента, которые клиент будет использовать для обработки файлов шаблона групповой политики для пользовательской политики.
- Атрибут `GPCWQLFilter` содержит информацию о фильтрах WMI, которые применяются к объекту групповой политики.

Объекты GPC хранятся в контексте именования `Domain` в разделе `cn=Policies,cn=System,dc=`*<имя_домена>*`,dc=`*<корень>*. Важно помнить, что отдельные домены в пределах леса поддерживают собственные списки GPC. Контекст именования `Domain` не реплицируется на другие контроллеры домена (кроме серверов глобального каталога, но эти копии

предназначены только для чтения). Это налагает ограничения на связь групповых политик с контейнерами Active Directory.

- Избегайте связывания объекта групповой политики из одного домена с контейнером в другом домене.
- Избегайте создания политик сайтов в пределах леса, состоящего из нескольких доменов.

В следующих главах рассматриваются возможные последствия нарушения таких ограничений.

Связывание объектов GPO через границы доменов

Файлы GPT, связанные с объектом групповой политики (GPO), хранятся в каталоге `Sysvol` контроллеров того же домена, в котором хранится объект GPC.

Если связать объект групповой политики (GPO) из одного домена с контейнером в другом домене, клиенты, для которых назначена эта групповая политика, должны будут связываться с контроллерами другого домена для загрузки файлов GPT. Для этого требуется дополнительная аутентификация. Если контроллер домена доступен через внешнее соединение и находится в географически удаленном месте, то транзакция будет выполняться очень медленно.

Если используется лес из нескольких доменов и планируется развертывание целостного набора политик, создайте политики в каждом домене. Это повысит нагрузку на администратора, так как при каждом изменении политики в пределах предприятия придется редактировать несколько объектов групповой политики. Альтернативным решением является загрузка политик предприятия через внешнее соединение каждое утро при регистрации клиентов.

Политики сайтов в лесу из нескольких доменов

Информация о сайтах хранится в базе данных Active Directory в отдельном контексте именования `Configuration`, который реплицируется на все контроллеры доменов в пределах леса. С другой стороны, информация о доменах хранится в контексте именования `Domain`, который реплицируется только на контроллеры домена в пределах того же домена.

К сожалению, в контексте именования `Configuration` нет возможности для хранения информации о групповых политиках сайтов. Контейнер групповой политики (GPC) может храниться только в контексте именования `Domain`. Для этого есть ряд причин.

- В пределах любого сайта может присутствовать любое количество доменов конкретного леса, поэтому компания Microsoft приняла решение о хранении контейнеров групповых политик (GPC) для всех политик сайтов в одном контексте именования `Domain` (соответствующем корневому домену). Корневым является первый домен леса.
- Так как только контроллеры домена в корневом домене хранят контейнеры GPC для политик сайтов, соответствующие файлы GPT хранятся только в каталоге `Sysvol` на контроллерах домена в корневом домене.

Комбинация этих инженерных решений ограничивает функциональные возможности политик сайтов в лесу из нескольких доменов (рис. 12.6). На схеме показано, как будут назначаться политики в лесу, состоящем из нескольких доменов.

На рисунке показано два домена: `NA` и `PACRIM`. Контроллеры доменов и пользователи находятся в двух сайтах: `LA` и `Tokyo`. Для сайтов `LA` и `Tokyo` назначены групповые политики. Вспомните, что файлы GPT хранятся в каталоге `Sysvol` на контроллерах корневого домена леса независимо от расположения сайта и доменов, находящихся в пределах сайта.

Когда клиент из домена `NA` регистрируется в пределах сайта `LA`, он загружает файлы GPT для политик сайта `LA` с контроллера домена `NA`. Так как контроллер домена `NA` присутствует в пределах сайта `LA`, загрузка файлов шаблона групповой политики (GPT) выполняется достаточно быстро.

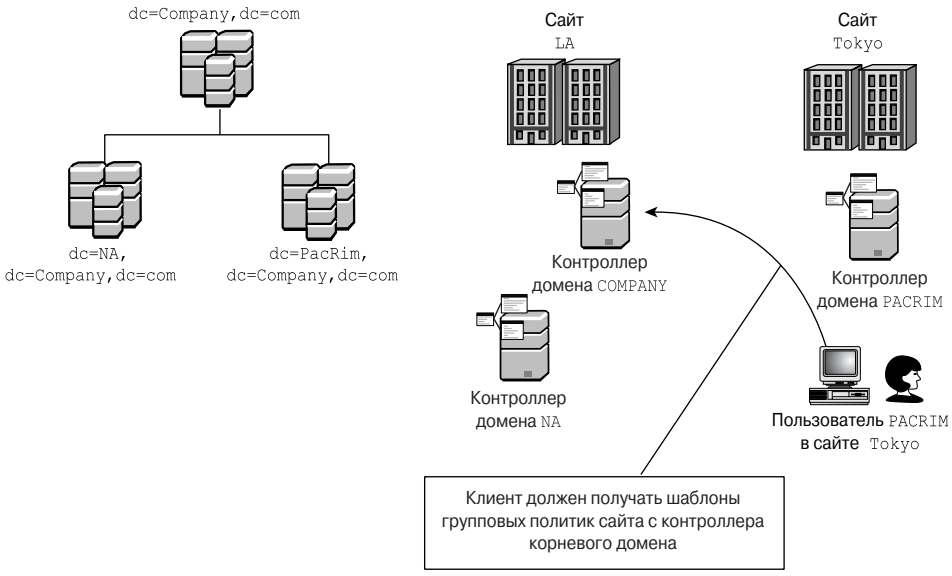


Рис. 12.6. Политики сайта в лесу, состоящем из нескольких доменов

Но у клиента домена `PacRim`, который регистрируется на сайте `Tokyo`, дела обстоят не так хорошо. Файлы GPT для сайта `Tokyo` хранятся на контроллере домена `NA`, корневого домена леса. Клиент из `Tokyo` должен использовать внешнее соединение для загрузки файлов GPT с контроллера домена `NA`, который находится в `LA`. Если в качестве внешнего соединения используется спутниковый канал со скоростью передачи данных 56 Кбайт/с, пользователи в `Tokyo` будут слишком долго ждать завершения регистрации.

Поэтому для реализации политик сайтов в лесу, состоящем из нескольких доменов, контроллеры корневого домена должны находиться в пределах каждого сайта, использующего политики сайта. Кроме этого, можно обеспечить быстрое внешнее соединение с ближайшим сайтом, в котором присутствует контроллер корневого домена. (Клиенты определяют ближайший сайт по ссылкам контроллера домена, который может проверять топологию сайта на основе IP-адресов, связанных с объектами IP Subnet, создаваемых для каждого сайта.)

Иерархия политик

Объекты групповых политик (GPO) *связаны* с объектами контейнеров в базе данных Active Directory. На основе таких связей клиенты определяют назначенные им политики. Объекты групповых политик можно связывать только с контейнерами трех типов.

- Сайты (site)
- Домены (domain)
- Организационные единицы (OU)

Связи политик в базе данных Active Directory отслеживаются с помощью атрибута `GPLink` объекта контейнера. Ниже приведен фрагмент списка атрибутов организационной единицы Phoenix, с которым связаны две групповые политики:

```
ou: OU=Poenix,DC=Company,DC=com
gPLink: [LDAP://CN={91c0a3bc-141e-49bf-ad38-2da7905dbf09},CN=Policies,
↪ CN=System,DC=Company,DC=com;0][LDAP://CN={205d4bee-acc2-465a-9aba-
↪ d84575d72523},CN=Policies,CN=System,DC=Company,DC=com;0];
gPOptions: 0;
```

- Атрибут `GPLink` содержит характерные имена всех контейнеров групповых политик (GPC), связанных с контейнером. Вспомните, что для обеспечения уникальности имен используется формат GUID. Контейнер может быть связан с несколькими объектами групповых политик, и объект групповой политики может быть связан с несколькими контейнерами.
- Атрибут `GPOptions` содержит значение параметра `Block Policy Inheritance` (Блокировать наследование политик), который рассматривается далее в этой главе. (Значение `0` отключает блокирование наследования. Значение `1` включает блокирование наследования для этого контейнера.)

Клиенты определяют список контейнеров по собственному характерному имени. Получив список контейнеров, клиент может запросить в базе данных Active Directory атрибуты `GPCLink` для каждого контейнера. Эта информация позволяет клиенту собрать параметры групповых политик из каждого объекта групповой политики в соответствии со следующими правилами приоритета (рис. 12.7).

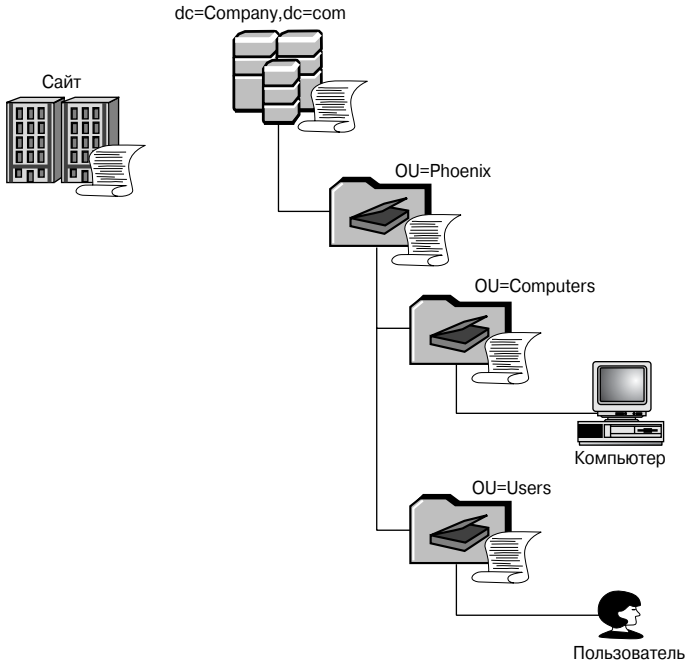


Рис. 12.7. Схема наследования политик

- Локальные политики (политики, определенные на локальном компьютере) имеют наименьший приоритет.
- Объекты групповой политики (GPO), связанные с контейнером сайта.
- Объекты групповой политики, связанные с контейнером домена.
- Объекты групповой политики, связанные с организационной единицей.
- Объекты групповой политики, связанные с ближайшей организационной единицей объекта пользователя или компьютера, имеют более высокий приоритет, чем объекты групповой политики, связанные с организационными единицами выше по дереву.

Последовательность символов LSDOU часто используется для представления этого порядка приоритетов. Порядок приоритетов реализует *иерархию наследования* (inheritance hierarchy). Эту иерархию можно переопределить двумя способами.

- Можно установить политику, которая противоречит такому же параметру в объекте групповой политики, связанном с организационной единицей выше по дереву.
- В базе данных Active Directory можно установить атрибут, который будет блокировать наследование всех объектов групповых политик, связанных выше по дереву.

Несложно догадаться, что оба варианта имеют свои преимущества. Рассмотрим их.

Отслеживание политики в системном реестре

Объект групповой политики, загруженный клиентом, хранится в локальном системном реестре в разделе `HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Shadow`. Каждой политике назначается последовательный номер, начиная с нуля. Эта последовательность определяется приоритетом объектов групповых политик. Больший номер имеет больший приоритет.

Записи всех загруженных клиентом групповых политик хранятся в разделе системного реестра `HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy` .

Переопределение наследования политик

Существует возможность переопределить наследование политик для определенной организационной единицы. После этого объекты в пределах организационной единицы (и всех дочерних организационных единиц) прекращают получать параметры политик из контейнеров выше по дереву.

Обратитесь к рис. 12.7 из предыдущего раздела. Предположим, что создан объект групповой политики и он связан с контейнером домена. В этом объекте групповой политики определена политика безопасности `Message Text For Users Attempting To Logon` (Текстовое сообщение для регистрирующихся пользователей). Эта политика выводит информационное сообщение при регистрации пользователей. В сообщении указывается, что все компьютерное оборудование принадлежит компании и компания оставляет за собой право просматривать все данные, хранящиеся на компьютерах.

Эта групповая политика связывается с контейнером домена, так как каждый пользователь в пределах организации должен видеть это сообщение при каждой регистрации, чтобы никто не мог заявить, что он ничего не знал об ограничениях.

Администраторы организационной единицы `Phoenix` устали от жалоб пользователей на это сообщение. Администраторы решили отказаться от вывода этого сообщения в пределах своей организационной единицы. Это очень просто сделать: достаточно открыть окно свойств организационной единицы на консоли Active Directory — Users and Computers (Active Directory — пользователи и компьютеры) и установить флажок Block Policy Inheritance (Блокировать наследование политик) в свойствах групповой политики (рис. 12.8).

После внесения изменений пользователи перестанут получать уведомление при регистрации. Это нравится пользователям, но не нравится аудиторам компании, которые нанесут визит на следующей неделе. Аудиторы сообщают о нарушениях руководству компании, и администратору верхнего уровня дается задание прекратить нарушение общей политики. Администратор использует свои права `Domain Administrator` (Администраторы домена) для сброса флажка Block Policy Inheritance (Блокировать наследование политики) в организационной единице `Phoenix`.

Через некоторое время, когда страсти улягутся, администраторы организационной единицы `Phoenix` опять устанавливают флажок Block Policy Inheritance (Блокировать наследование политик). Главный администратор замечает изменение и сбрасывает флажок. Они уста-

навливают. Это происходит некоторое время, после чего администраторы организационной единицы `Phoenix` сдаются. Они прекращают менять параметр Block Policy Inheritance (Блокировать наследование политики).

Внимательное изучение ситуации показывает, что администраторы организационной единицы `Phoenix` создали новый объект групповой политики, который связан с организационной единицей `Phoenix` и отключает параметр `Message Text For Users Attempting To Logon` (Текстовое сообщение для регистрирующихся пользователей). Так как объект групповой политики связан с ближайшей организационной единицей, он имеет больший приоритет и блокирует вывод уведомления.



Рис. 12.8. В свойствах организационной единицы можно установить флажок Block Policy Inheritance (Блокировать наследование политики)

Автор этой книги не знает, где ее будут читать, но в южном Нью-Мехико такое состязание имеет собственное название. Обычно вопрос решается с помощью шестизарядного револьвера в полдень перед салуном на главной улице. Жителей более мягких климатических зон может заинтересовать следующее, менее драматическое, решение.

Переопределение блокирования политики

Администратор домена или предприятия может установить параметр объекта групповой политики выше по дереву, который приведет к переопределению всех блокировок наследования. Установка этого параметра описывается в процедуре 12.1.

Процедура 12.1. Переопределение блокирования наследования

1. Откройте окно свойств контейнера верхнего уровня, например контейнера домена или организационной единицы.
2. Откройте вкладку Group Policy (Групповая политика).
3. Выделите объект групповой политики, для которого необходимо задать принудительное наследование.

4. Щелкните на кнопке Options (Параметры).
5. Выберите переключатель No Override (Не перекрывать), как показано на рис. 12.9.
6. Щелкните на кнопке OK для сохранения изменений.



Рис. 12.9. Окно параметров для контейнера организационной единицы с переключателем No Override (Не перекрывать) для выбранной групповой политики

Переключатель No Override (Не перекрывать), установленный в каждом объекте групповой политики, сделает все параметры политики, определенные в этом объекте, обязательными для компьютеров и пользователей ниже по дереву. Администраторы могут установить флажок Block Policy Inheritance (Блокировать наследование политики), но этот параметр будет проигнорирован. Если локальные администраторы попытаются переопределить конкретные параметры, они обнаружат, что различные параметры политики, определенные в объекте групповой политики более высокого уровня, неактивны и недоступны для изменения в редакторе групповых политик.

Определение результирующего набора политик

Объекты групповых политик (GPO) могут быть связаны, отфильтрованы, заблокированы и разблокированы тысячей способов. Компания Microsoft сделала большой шаг в сторону упрощения управления групповыми политиками, включив в состав операционной системы Windows Server 2003 программу, лицензированную у компании Full Armor Software (`www.fullarmor.com`). Программа называется FAZAM или Full Armor Zero Administration Management.

Как и в случае большинства технологий от сторонних производителей, лицензированных компанией Microsoft, возможности результирующего набора политик (Resultant Set of Policies — RSoP), предоставляемые Windows-версией программы FAZAM, являются только частью возможностей коммерческой версии программы FAZAM. Часть программы FAZAM, лицензированная компанией Microsoft, позволяет рассчитывать и протоколировать *результирующий набор политик* (RSoP) на основе расположения определенного пользователя или компьютера в базе данных Active Directory.

Определение результирующего набора политик можно использовать для проверки того, что произойдет, когда определенный пользователь зарегистрируется на определенном компьютере. При определении принимаются во внимание расположение объекта пользователя и объекта компьютера, имя узла и все фильтры, которые применяются на основе членства в группах и используемых аппаратных средств.

Кроме этого, в операционных системах Windows Server 2003 и Windows XP сохраняется журнал с отчетом о последнем определенном результирующем наборе политик для каждого регистрирующегося на компьютере клиента. Программу подсчета RSoP можно использовать для просмотра содержимого этого журнала для любого компьютера в пределах домена. Журнал расположен в хранилище Common Information Model (CIM). Дополнительная информация приводится в разделе “Фильтрация WMI”.

Планирование результирующего набора политик

Программа просмотра результирующего набора политик может быть запущена несколькими способами. Самый простой способ описан в процедуре 12.2.

Процедура 12.2. Запуск мастера результирующего набора политик в режиме планирования

1. Щелкните правой кнопкой мыши на объекте пользователя или компьютера на консоли Active Directory — Users and Computer (Active Directory — пользователи и компьютеры) и выберите из контекстного меню команду All Tasks⇨RSoP (Planning) (Все задачи⇨Результирующая политика (Планирование)). Запустится мастер результирующего набора политик, начиная с окна User and Computer Selection (Выбор компьютера и пользователя). Пример показан на рис. 12.10.

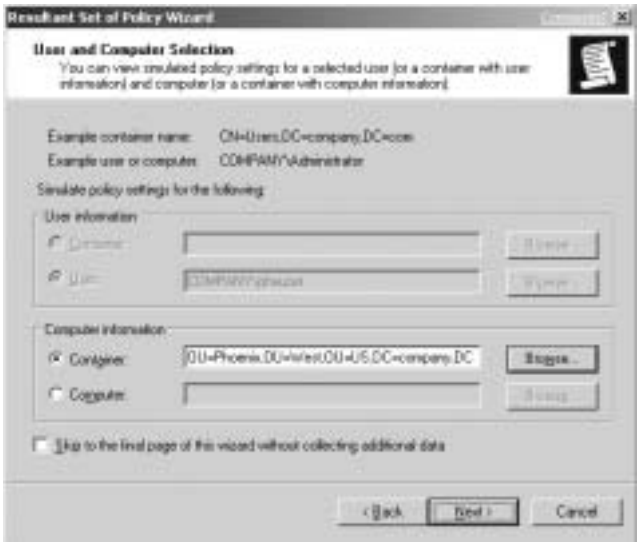


Рис. 12.10. Окно User and Computer Selection (Выбор компьютера и пользователя) мастера результирующего набора политик

2. В разделе Computer information (Сведения о компьютере) выберите переключатель Container (Контейнер), щелкните на кнопке Browse (Обзор) и выберите организационную единицу объекта пользователя.
3. На этом этапе мастер имеет достаточно информации для расчета результирующего набора политик, поэтому можно установить флажок Skip to the final page... (Перейти к последней странице, не собирая дополнительных данных) и щелкнуть на кнопке Next (Далее). Но мы рассмотрим дополнительные параметры, которые позволяют диагностировать потенциальные проблемы.
4. Щелкните на кнопке Next (Далее). Откроется окно Advanced Simulation Options (Дополнительные параметры эмуляции). В окне можно установить следующие параметры.
    - **Slow Network Connection (Низкоскоростное сетевое подключение).** В этом случае моделируется обработка объекта групповой политики по коммутируемому подключению, ISDN или подключению DSL.

- **Loopback Processing (Обработка по методу обратной петли).** Моделируется обмен данными между Computer Configuration и User Configuration, который возникает при использовании политики работы по методу обратной петли для объекта компьютера.
- **Site (Сайт).** Указывается сайт, в котором регистрируется пользователь.

5. Щелкните на кнопке Next (Далее). Откроется окно Alternate Active Directory Paths (Альтернативные пути Active Directory). Это позволит выбрать другую организационную единицу для учетных записей пользователя и компьютера.
6. Щелкните на кнопке Next (Далее). Откроется окно User Security Groups (Группы безопасности пользователя). В окне отображаются группы, в которые входит пользователь. Можно выбрать дополнительные группы или удалить существующие группы с целью планирования и устранения неисправностей.
7. Щелкните на кнопке Next (Далее). Откроется окно Computer Security Groups (Группы безопасности компьютера). В окне показаны группы, в которые входит компьютер. Можно выбрать дополнительные группы или удалить существующие группы с целью планирования и устранения неисправностей.
8. Щелкните на кнопке Next (Далее). Откроется окно WMI Filters for Users (Фильтры WMI для пользователей). В окне перечислены связанные фильтры WMI. С целью устранения неисправностей можно выбрать другие фильтры.
9. Щелкните на кнопке Next (Далее). Откроется окно WMI Filters for Computers (Фильтры WMI для компьютеров). В окне перечислены связанные с компьютером фильтры WMI. С целью устранения неисправностей можно выбрать другие фильтры.
10. Щелкните на кнопке Next (Далее). Откроется окно Summary of Selections (Выбранные параметры). Для изменения параметров щелкните на кнопке Back (Назад). Если необходимо сравнить результаты на различных контроллерах домена, можно выбрать другой контроллер домена, на котором будут обрабатываться выбранные параметры.
11. Щелкните на кнопке Next (Далее). После того как мастер завершит обработку, появится окно Finish (Готово). Щелкните на кнопке Finish (Готово), чтобы открыть окно с информацией о результирующем наборе политик.

Утилита просмотра результирующего набора политик напоминает стандартный редактор групповых политик, но он содержит только те параметры групповых политик, которые входят в объекты групповых политик, соответствующие указанным критериям. Еще одна утилита просмотра результирующего набора политик предоставляется в составе Help and Support Center. Эта утилита предоставляет список политик в формате XML. Список содержит всю информацию о групповых политиках, которые применяются на компьютере. Для запуска этой утилиты необходимы привилегии локального администратора на компьютере.

Утилита `gpresult`

Ели для просмотра результирующего набора политик предпочтительнее использовать утилиту с интерфейсом командной строки, воспользуйтесь утилитой `gpresult`. В отличие от утилиты `gpresult` из состава Windows 2000 Resource Kit, утилита из состава Windows Server 2003 выполняет те же расчеты, что и мастер результирующего набора политик. Кроме этого, утилиту `gpresult` можно использовать для просмотра журнала результирующего набора политик.

Отчет утилиты `gpresult` слишком велик для цитирования на страницах этой книги, но в него входит вся информация, необходимая для прослеживания каждого параметра политик к исходному объекту групповой политики и связанному с ним контейнеру. Утилиту `gpresult` можно запускать в режиме планирования и в режиме протоколирования.

Протоколирование результирующего набора политик

В утилите просмотра результирующего набора политик можно включить режим *протоколирования* (Logging), который позволяет просматривать результат определения результирующего набора политик для любого клиента на компьютере. Для просмотра журнала на компьютере необходимо иметь права администратора. Необходимая последовательность действий приведена в процедуре 12.3.

Процедура 12.3. Запуск мастера результирующего набора политик в режиме протоколирования

1. На консоли Active Directory — Users and Computers (Active Directory — пользователи и компьютеры) щелкните правой кнопкой мыши на объекте компьютера и выберите из контекстного меню команду Resultant Set Of Policy (Logging) (Результирующая политика (Протоколирование)). Запустится мастер результирующего набора политик и откроется окно Computer Selection (Выбор компьютера).
2. Щелкните на кнопке Next (Далее). Откроется окно User Selection (Выбор пользователя). Выделите имя пользователя, для которого необходимо просмотреть результаты работы мастера.
3. Щелкните на кнопке Next (Далее). Откроется окно Summary of Selections (Выбранные параметры).
4. Щелкните на кнопке Next (Далее). Мастер получит записи журнала пользователя с выбранного компьютера и выведет их на экран.

Сравнивая результаты работы мастера результирующего набора политик в режиме планирования и фактический результирующий набор политик, можно обнаружить различие и внести необходимые изменения.

Дополнительные утилиты диагностики

Если настроенные групповые политики работают не совсем так, как предполагалось, обратите внимание на следующие компоненты.

- **Event Viewer (Просмотр событий).** Обратитесь к журналу приложений и просмотрите записи службы `Userenv`. Предупреждения от этой службы указывают, что в процессе загрузки групповых политик что-то пошло не так.
- **Права доступа.** Одной из распространенных проблем в работе групповых политик являются неверно назначенные права доступа, связанные с системой безопасности. Всегда проверяйте, имеет ли пользователь права на политику, которую необходимо применить. Для этого откройте соответствующую консоль Active Directory, откройте окно свойств групповой политики для соответствующего контейнера и перейдите на вкладку Security (Безопасность). Пользователь должен являться членом группы с правами доступа `Read` (Чтение) и `Allow Group Policy` (Разрешить применение групповой политики).
- **Неправильные связи групповых политик.** Еще одной проблемой в работе групповых политик является неправильная настройка связей. Политику можно связать с одним контейнером, а проверку выполнять с помощью учетной записи пользователя из другого контейнера. Кроме этого, кто-то может разместить групповую политику в контейнере выше по дереву, которая перезаписывает параметры политики или полностью ее блокирует.
- **Утилита `gpotool`.** Как было показано в разделе о контейнерах групповых политик, утилита `gpotool` позволяет отследить несовпадения номеров версий шаблонов и контейнеров групповых политик, связанных с одним объектом групповой политики.

- **Проблемы в работе сети.** Удостоверьтесь, что клиент успешно устанавливает соединение с контроллером домена, сервером глобального каталога и сервером DNS. Невозможность подключения к одному из этих серверов приводит к проблемам в работе групповых политик. Для обнаружения ошибок можно воспользоваться утилитой `netdiag`.
- **Отладка службы Userenv.** Последней попыткой обнаружить проблему является включение журнала групповых политик. Добавьте следующую запись в раздел `Winlogon` системного реестра:

> Раздел: `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon`
> Запись: `UserEnvDebugLevel`
> Значение: `0x10002` (шестнадцатеричное), тип `REG_DWORD`

После добавления записи перезагрузите компьютер. Журнал сохраняется в файле `\Windows\Debug\Userenv.log`. Журнал большой, поэтому при его чтении стоит запастись чаем и пирожками.

Политики для компьютеров и политики для пользователей

Объекты групповых политик делятся на две части.

- В разделе `Computer Configuration` (Конфигурация компьютера) содержатся параметры политик для объектов компьютеров.
- В разделе `User Configuration` (Конфигурация пользователя) содержатся параметры политик для объектов пользователей.

В редакторе групповых политик эти разделы отображаются в вершине дерева разделов.

Некоторые параметры политик доступны в обоих разделах. Если возникает конфликт между параметрами в разных разделах, более высокий приоритет имеет раздел `Computer Configuration` (Конфигурация компьютера). Это справедливо, даже если параметры политик находятся в различных объектах групповых политик.

Рассмотрим пример, в котором организационная единица `Phoenix` содержит объекты пользователей и компьютеров. Существует два объекта групповой политики, которые связаны с организационной единицей `Phoenix`.

- Объект групповой политики `Phx-Computers`
- Объект групповой политики `Phx-Users`

Каждый объект групповой политики содержит политику в разделе `Task Scheduler` (Планировщик заданий), которая называется `Prohibit New Task Creation` (Запретить создание новых заданий). При включении этой политики в Control Panel (Панель управления) пиктограмма Add Scheduled Task (Добавить задание) не отображается в аплете Scheduled Tasks (Назначенные задания).

Объект групповой политики `Phx-Users` содержит политику в разделе `User Configuration` (Конфигурация пользователя), а объект `Phx-Computers` содержит политику в разделе `Computer Configuration` (Конфигурация компьютера). Рассмотрим, как обрабатывается эта политика.

- В объекте групповой политики `Phx-Users` политика отключена, а это значит, что можно создавать новые задания.
- В объекте групповой политики `Phx-Computers` политика включена, т.е. новые задания создавать невозможно.

При такой конфигурации пользователь из организационной единицы `Phoenix`, регистрирующийся на компьютере из организационной единицы `Phoenix`, не сможет получить доступ к пиктограмме Add Scheduled Task (Добавить задание), которая находится в аплете Scheduled Tasks (Назначенные задания). Создание новых запланированных заданий отклю-

чено, так как политика из раздела Computer Configuration (Конфигурация компьютера) имеет более высокий приоритет, чем политика из раздела User Configuration (Конфигурация пользователя).

Если администратор переключит политику в объекте групповой политики Phx-Computers из Disabled (Отключена) в Not Configured (Не задана), сразу же после обновления политик на рабочих станциях пользователи смогут получить доступ к пиктограмме Add Scheduled Task (Добавить задание).

Использование интерфейса обратной петли

В предыдущем разделе рассматривалась ситуация, когда параметры политики в разделе Computer Configuration (Конфигурация компьютера) переопределяют параметр политики из раздела User Configuration (Конфигурация пользователя). Существует еще одна ситуация, когда система должна определить приоритет политики на основании ее расположения.

Рассмотрим сценарий, похожий на последний пример, но в организационной единице Phoenix существуют еще две организационные единицы.

- В организационной единице Users хранятся объекты пользователей организационной единицы Phoenix. Эта организационная единица связана с объектом групповой политики Phx-Users.
- В организационной единице Computers хранятся объекты компьютеров организационной единицы Phoenix. Эта организационная единица связана с объектом групповой политики Phx-Computers.

Для объектов групповой политики (GPO) могут быть установлены различные параметры. Подробная информация о каждом параметре в данном случае не важна.

- Для объекта групповой политики Phx-Users заданы два параметра политик: политика безопасности в разделе Computer Configuration (Конфигурация компьютера) и политика распространения программного обеспечения в разделе User Configuration (Конфигурация пользователя).
- Для объекта групповой политики Phx-Computers заданы два параметра политик: политика аудита в разделе Computer Configuration (Конфигурация компьютера) и политика регистрационного сценария в разделе User Configuration (Конфигурация пользователя).

Как только пользователь из организационной единицы Users зарегистрируется на компьютере из организационной единицы Computers, результирующий набор политик будет содержать следующие политики.

- Политика распространения программного обеспечения из объекта групповой политики Phx-Users
- Политика аудита из объекта групповой политики Phx-Computers

В обычных условиях это вполне допустимо. Но иногда имеет смысл применять параметры раздела User Configuration (Конфигурация пользователя) из объектов групповой политики, связанных с контейнерами, в которых хранятся объекты компьютеров. Чаще всего такая ситуация возникает при использовании лабораторных компьютеров или серверов терминалов, на которых необходимо сохранять один и тот же внешний вид и одни и те же правила использования рабочего стола, а также поддерживать одинаковые наборы программного обеспечения независимо от зарегистрировавшегося пользователя.

В таких ситуациях систему можно настроить на применение параметров раздела User Configuration (Конфигурация пользователя) из объекта групповой политики, который связан с контейнером, содержащим объекты компьютеров. Этот метод называют *обработкой с использованием интерфейса обратной петли* (loopback processing).

Обработку с использованием интерфейса обратной петли можно включить с помощью групповой политики, которая называется `User Group Policy Loopback Processing Mode` (Режим обработки по методу обратной петли для пользовательской групповой политики). Эта политика хранится в разделе Computer Configuration⇨Administrative Templates⇨System⇨Group Policy (Конфигурация компьютера⇨Административные шаблоны⇨Система⇨Групповая политика).

Можно использовать два режима обработки по методу обратной петли.

- **Режим замены.** В этом режиме клиентский компьютер игнорирует политики из раздела `User Configuration` (Конфигурация пользователя), полученные из объекта групповой политики, связанного с пользовательским контейнером, и применяет групповые политики из раздела `User Configuration` (Конфигурация пользователя) из объекта групповой политики, связанного с контейнером компьютера.
- **Режим объединения.** В этом режиме клиентский компьютер сначала применяет политики из раздела `User Configuration` (Конфигурация пользователя) объекта групповой политики, связанного с контейнером компьютера. После этого применяются политики из раздела `User Configuration` (Конфигурация пользователя) объекта групповой политики, связанного с контейнером пользователя. Больший приоритет предоставляется параметрам политик пользователя.

Если обработка по методу обратной петли включена в режиме замены, клиент получит следующий результирующий набор политик.

- Политика аудита для организационной единицы `Phx-Computer`
- Политика регистрационного сценария для организационной единицы `Phx-Computer`

Политика из раздела `User Configuration` (Конфигурация пользователя) при обработке по методу обратной петли игнорируется. Политика из раздела `Computer Configuration` (Конфигурация компьютера) из пользовательского контейнера игнорируется независимо от режима обработки по методу обратной петли.

Если обработка по методу обратной петли включена в режиме объединения, клиент получит следующий результирующий набор политик.

- Политика аудита для организационной единицы `Phx-Computer`
- Политика регистрационного сценария для организационной единицы `Phx-Computer`
- Политика распространения программного обеспечения для организационной единицы `Phx-Users`

Политика из раздела `Computer Configuration` (Конфигурация компьютера) для пользовательского контейнера игнорируется независимо от режима обработки по методу обратной петли.

Следует избегать обработки по методу обратной петли во всех случаях, кроме случая создания специализированных сред. Обработка по методу обратной петли значительно усложняет диагностику групповых политик. Создавайте отдельные организационные единицы для хранения объектов компьютера. Иногда стоит физически идентифицировать компьютеры, для которых применяется обработка по методу обратной петли (например, с помощью пометки на мониторе), чтобы пользователи не удивлялись невозможности получить собственные параметры.

Редактор групповых политик

Содержимое объекта групповой политики (GPO) управляется с помощью редактора групповых политик (Group Policy Editor — GPE). Редактор является оснасткой MMC, доступной несколькими способами.

Чаще всего, чтобы получить доступ к редактору GPE, открывают окно свойств сайта, домена или организационной единицы, а затем переходят на вкладку Group Policy (Групповая политика).

Кроме этого, можно создать собственную консоль MMC и загрузить в нее оснастку GPE. При этом будет выдан запрос на выбор редактируемого объекта GPO. Щелкните на кнопке Browse (Обзор). Откроется окно Browse for a Group Policy Object (Поиск объекта групповой политики). Перейдите на вкладку All (Все), чтобы получить доступ к полному списку всех объектов групповой политики домена (рис. 12.11).

Оснастку GPE можно загружать несколько раз на одну и ту же консоль MMC. При каждой загрузке оснастки необходимо выбрать новый объект групповой политики. Это идеальный способ управления несколькими GPO из одного интерфейса.

Кроме этого, собственную консоль можно настроить на конкретную групповую политику или конкретный компьютер (или и то, и другое одновременно). В этих случаях используются параметры командной строки `/gpcomputer` и `/gpobject`. Именно так компания Microsoft создала специализированные консоли `Local Security Settings` и `Domain Security Policy`. Например, в ярлыке, загружающем консоль `Domain Security Policy`, в поле Target задано следующее значение:

```
C\WINDOWS\system32\dompol.msc /gpobject:"LDAP://CN={31b2f340-06d
↳ -11d2-945f-00c04fb984f9},CN=Policies,CN=System,DC=Company,DC=com"
```

Как будет показано в следующем разделе, консоль `Dompol.msc` использует возможность консоли MMC, которая позволяет загружать конкретные расширения редактора GPE.

Специальные конфигурации с использованием параметров командной строки

Если для управления консолью MMC необходимо использовать параметры командной строки `/gpcomputer` и `/gpobject`, то при загрузке объекта групповой политики на консоль с помощью окна Add/Remove Snap-in (Добавить/удалить оснастку) необходимо установить следующий параметр групповой политики:

Allow The Focus Of The Group Policy Snap-In To Be Changed When Launching From The Command Line (Разрешить изменять фокус оснастки групповой политики при запуске из командной строки).

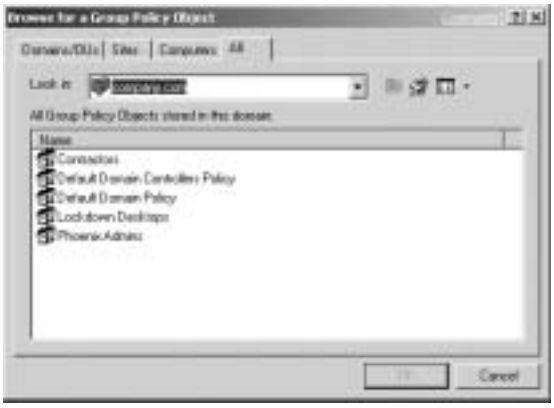


Рис. 12.11. Окно Browse for a Group Policy Object (Поиск объекта групповой политики), в котором показан список объектов групповой политики в домене `Company.com`

Выбор расширения редактора групповых политик

Редактор GPE зависит от нескольких файлов поддержки, которые предоставляют возможность редактирования различных типов политик. В табл. 12.3 перечислены файлы шаблонов групповых политик (GPT) и соответствующие расширения GPE. Если при открытии раздела в редакторе GPE выдается сообщение об ошибке, ищите проблему в работе соответствующего редактора или в файлах, которые он пытается открыть.

Таблица 12.3. Файлы шаблонов групповых политик и соответствующие расширения редактора GPE

Файл GPT	Расширение GPE
`Registry.pol`	`Gptext.dll`
`GptTmpl.inf`	`Wsecedit.dll`
`Script.ini`	`Gptext.dll`
`Fdeploy.ini`	`Fde.dll`
`*.aas` (развертывание программного обеспечения)	`Appmgr.dll`
`Install.ins`	`Ieaksie.dll`

При создании собственной консоли MMC для редактирования групповых политик можно указать отдельные расширения редактора. Для этого перейдите на вкладку Extensions (Расширения) в окне Add/Remove Snap-in (Добавить/удалить оснастку) и сбросьте флажки напротив всех расширений, которые загружать не нужно. На рис. 12.12 показан пример пользовательской консоли, на которой загружается только расширение Logon/Logoff Scripts (Сценарии входа/выхода из системы).

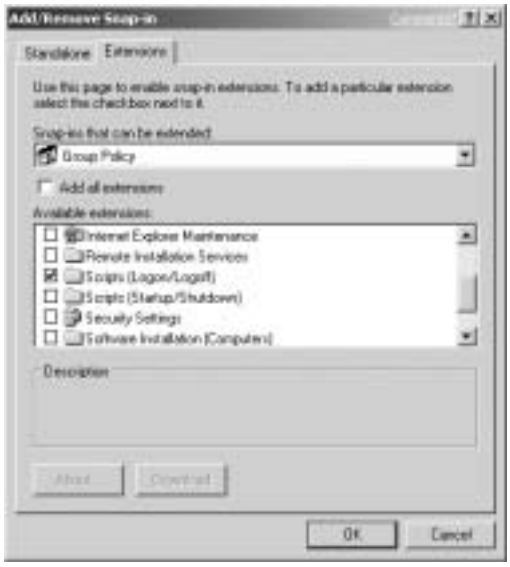


Рис. 12.12. Окно Add/Remove Snap-in (Добавить/удалить оснастку) для пользовательской консоли, в котором выбрано несколько расширений

PDC Emulator и редактор групповых политик

При редактировании объектов GPO редактор GPE читает контейнер GPC и шаблон GPT с определенного контроллера домена. По умолчанию выбирается контроллер домена, которому назначена роль PDC Emulator. Выбор контроллера домена не зависит от текущих настроек консоли Active Directory — Users and Computers (Active Directory — пользователи и компьютеры) или консоли Active Directory — Sites and Services (Active Directory — сайты и службы) на момент запуска редактора групповых политик.

Например, если консоль Active Directory — Users and Computers (Active Directory — пользователи и компьютеры) запускается на рабочей станции, использующей контроллер домена DC-37 в качестве регистрационного сервера, то консоль будет настроена на контроллер домена DC-37, но редактор GPE автоматически обратится за информацией на PDC Emulator, а не на контроллер домена DC-37.

На первый взгляд, редактирование групповых политик на единственном контроллере домена противоречит принципу репликации с несколькими хозяевами. В конце концов, изменения в любой копии базы данных Active Directory или каталога `Sysvol` будут реплицированы на все остальные контроллеры домена, не правда ли?

Использование единственного контроллера домена для редактирования групповых политик предотвращает возможность редактирования политик в объекте GPO двумя администраторами одновременно (в течение одного цикла репликации). Если это произойдет, внесенные одним администратором изменения будут перезаписаны изменениями, внесенными вторым администратором.

Если во время запуска редактора GPE недоступен сервер, выполняющий роль PDC Emulator, то будет выдан запрос следует ли выбрать другой контроллер домена или ожидать доступа к PDC Emulator. Ничего страшного в редактировании объекта GPO на другом контроллере домена нет, но необходимо убедиться, что этот объект групповой политики редактирует один администратор. В случае сомнений стоит подождать доступности PDC Emulator.

Изменение принятого по умолчанию контроллера домена

Если для изменения объектов GPO используется не PDC Emulator, а другой контроллер домена, для изменения критерия выбора контроллера домена можно установить соответствующую групповую политику. Политика называется `Group Policy Domain Controller Selection` (Выбор контроллера домена для групповых политик). Политика расположена в разделе User Configuration⇨Administrative Templates⇨System⇨Group Policy (Конфигурация пользователя⇨Административные шаблоны⇨Система⇨Групповая политика).

Эта политика имеет три параметра.

- **Use the Primary Domain Controller (Использовать основной контроллер домена).** Если политика не включена, этот параметр установлен по умолчанию.
- **Inherit From The Active Directory Snap-Ins (Унаследовать от оснасток Active Directory).** Это значение заставит редактор GPE выбирать контроллер домена, на который настроена консоль Active Directory — Users and Computers (Active Directory — пользователи и компьютеры) или консоль Active Directory — Sites and Services (Active Directory — сайты и службы), запустившая редактор групповых политик.
- **Use Any Available Domain Controller (Использовать любой доступный контроллер домена).** Это значение позволяет редактору использовать первый доступный контроллер домена. Обычно это сервер, на котором проходит регистрацию администратор, запускающий редактор GPE.

Можно обратить внимание на отсутствие одного очевидного варианта. Нельзя просто указать контроллер домена, который будут использовать все. Если все должны использовать определенный контроллер домена, просто передайте роль PDC Emulator этому серверу.

Групповые политики и локальные политики

Серверы под управлением операционной системы Windows Server 2003 и рабочие станции под управлением Windows XP не только загружают групповые политики с контроллера домена, но и используют политики из собственного локального хранилища политик в скрытом каталоге `\Windows\System32\GroupPolicy`. Кроме этого, на локальных компьютерах существуют хранилища данных, которые управляются групповыми политиками, а локальные изменения записываются в эти хранилища непосредственно.

Политики "накладываются" одна на другую в процессе применения. Наибольший приоритет получает последний набор политик. Локальные политики всегда применяются первыми, поэтому они чаще всего перекрываются групповыми политиками, загружаемыми с контроллера домена.

Если приходится управлять изолированной рабочей станцией или сервером, изменения в локальные политики можно внести с помощью консоли Local Policy Editor (Редактор локальной политики), `Gpedit.msc`. Файлы шаблонов групповой политики, созданные средствами консоли `Gpedit.msc`, хранятся в каталоге `\Windows\System32\GroupPolicy`.

Загруженные из домена групповые политики кэшируются локально. По этой причине пользователи портативных компьютеров, отключенных о сети, будут продолжать использование последнего набора групповых политик, загруженного с контроллера домена. Об этом важно помнить, так как некоторые групповые политики требуют кэшированной информации для нормального функционирования. В качестве примера можно привести шифрованную файловую систему, которая ищет кэшированную версию сертификата восстановления файлов от доменного агента восстановления данных (Data Recovery Agent — DRA) при шифровании файла пользователем. Если сертификат доменного агента восстановления данных недоступен, пользователю не удастся зашифровать файл.

Различные приоритеты групповых политик приводят к маскированию локальных политик. Иногда администраторы забывают об их существовании. Политики "тихо спят" в системном реестре или базе данных `Secedit` и никак себя не проявляют, пока компьютер не отключится от домена или пользователь не зарегистрируется с помощью локальной базы данных SAM вместо домена.

Цели групповых политик

В принятой по умолчанию конфигурации параметры из объекта групповой политики оказывают влияние на всех пользователей и все компьютеры, которые находятся в связанном контейнере. Если необходим более избирательный подход в назначении групповых политик, окажется полезной возможность фильтрации получателей политики. Операционная система Windows Server 2003 имеет два критерия фильтрации.

- Членство пользователя или компьютера в группе
- Аппаратная и программная конфигурация, доступная с помощью инструментария управления Windows (Windows Management Instrumentation — WMI)

Фильтрация групповых политик на основе групп безопасности

Одним из самых распространенных заблуждений является мнение о назначении групповых политик группам. Конечно же, это совершенно не соответствует истине. Групповые политики назначаются объектам пользователей и компьютеров на основе их положения в базе данных Active Directory. Группы для назначения групповых политик не используются.

Но существует возможность фильтрации объектов групповых политик таким образом, чтобы политика применялась только к объектам пользователей и компьютеров, которые являются членами определенной группы. Например, можно создать универсальный набор по-

литик настройки рабочих станций в объекте групповой политики, связанном с региональной организационной единицей, например `Phoenix`. Параметры этого объекта групповой политики подходят большинству пользователей, но руководитель отдела продаж требует ужесточения ограничений, чтобы обеспечить повышение производительности.

Можно переместить объекты пользователей из отдела продаж в отдельную организационную единицу в организационной единице `Phoenix` и создать новый объект групповой политики, связанный с этой организационной единицей, но иногда существуют ограничения, не позволяющие пойти на такой шаг. Например, предоставленные административные привилегии могут не позволять создавать новые организационные единицы. Или в организации принят проект развития домена Active Directory, который не допускает создания произвольных организационных единиц. Кроме этого, может потребоваться применение групповой политики к пользователям из различных организационных единиц.

В таких ситуациях можно создать новый объект групповой политики и включить фильтрацию, чтобы групповая политика применялась только к пользователям из группы `Sales`. Для этого необходимо изменить дескриптор безопасности контейнера групповой политики в базе данных Active Directory, чтобы только определенные группы могли читать и применять шаблоны GPT, определенные в контейнере GPC (рис. 12.13).



Рис. 12.13. Окно ACL Editor для групповой политики, в котором одной группе безопасности предоставлено разрешение `Apply Group Policy` *(Применение групповой политики)*

Самый простой способ изменения дескриптора безопасности контейнера групповой политики описан в процедуре 12.4.

Процедура 12.4. Настройка дескриптора безопасности GPO для фильтрации получателей политики

1. Щелкните правой кнопкой мыши на записи сайта, домена или организационной единицы, связанной с GPO. Из контекстного меню выберите команду Properties (Свойства).
2. Перейдите на вкладку Group Policy (Групповая политика).

3. Выделите групповую политику, для которой необходимо включить фильтрацию, и щелкните на кнопке Properties (Свойства). Откроется окно Properties (Свойства).
4. Перейдите на вкладку Security (Безопасность).
5. Измените список контроля доступа в соответствии с требованиями к фильтрации. Предоставьте разрешение `Apply Group Policy` (Применение групповой политики) всем группам, которые должны получать эту политику.
6. Щелкните на кнопке OK, чтобы сохранить изменения и закрыть окно редактора.

Если принято решение об использовании фильтрации для предоставления GPO только определенным группам или группе, помните, что фильтр применяется только в том случае, когда объекты пользователей в группе попадают в область действия GPO. Например, перемещение объекта пользователя отдела продаж из организационной единицы `Phoenix` в организационную единицу `Atlanta` приведет к тому, что пользователь перестанет получать групповую политику `Sales Lockdown`.

Фильтрация WMI

WMI (Windows Management Instrumentation), или инструментарий управления Windows, является реализацией инициативы *Web-Based Enterprise Management (WBEM)* от компании Microsoft. Инициатива предложена рабочей группой *Desktop Management Task Force (DMTF)*. На рис. 12.14 показана блок-схема компонентов WMI.

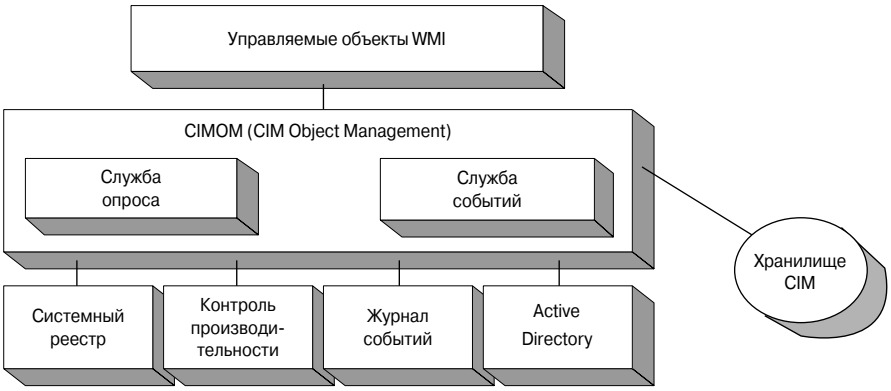


Рис. 12.14. Схема взаимосвязи компонентов WMI, которые используются при фильтрации WMI для групповых политик

Рассмотрим эти компоненты.

- **Управляемые объекты.** Инструментарий управления Windows собирает информацию от различных устройств и приложений. В качестве примера таких устройств можно привести жесткие диски, центральные процессоры, память и сетевые адаптеры. Эти объекты абстрагируются с помощью объектов COM, которые называются *провайдерами* (providers) и собирают информацию, предоставляемую управляемыми объектами.
- **Common Information Model (CIM).** Инструментарий управления Windows хранит полученную от провайдеров информацию об управляемых объектах в хранилище, которое называется *Common Information Model (CIM)*. Это хранилище больше похоже не на базу данных, а на аудиторию, в которой объекты выдают информацию при их вызове. Вершиной хранилища CIM является `\root\cimv2`.

- **Диспетчер объектов CIM.** Информация хранилища CIM предоставляется с помощью диспетчера объектов CIM (Common Information Model Object Manager — CIMOM). Диспетчер объектов отвечает за обработку входящей информации от провайдеров и связь с приложениями, которые нуждаются в информации из хранилища CIM.
- **Язык запросов инструментария управления Windows (WMI Query Language — WQL).** Поскольку WMI является реализацией инициативы WBEM от компании Microsoft, для доступа к информации, предоставляемой диспетчером объектов, используется созданный компанией Microsoft язык запросов инструментария управления Windows (WMI Query Language — WQL). Этот язык обеспечивает доступ с правом только для чтения к CIMOM. Обновления вносятся программными средствами с помощью провайдеров.
- **Триггеры событий.** Кроме пассивного ответа на запросы, CIMOM может активно отправлять сообщения и выполнять действия в ответ на события, возникающие в хранилище CIM. Групповые политики не используют события WMI.

Операционная система Windows Server 2003 использует WMI различными способами. В случае групповых политик WMI можно использовать для фильтрации объектов GPO, исходя из результатов запроса оператора на языке WQL.

Операторы языка WQL

Синтаксис языка WQL является подмножеством синтаксиса SQL с расширениями для специальных классов в хранилище CIM. Чаще всего в запросах к WMI используется оператор `Select` с модификаторами `Where`, которые определяют результирующее множество. Рассмотрим несколько примеров.

- Выдать перечень компьютеров, использующих процессор с частотой выше 600 МГц:

```
root\cinv2; SELECT * from Win32_Processor
↳ WHERE currentclockspeed < 600
```

- Выдать перечень компьютеров, которые работают под управлением операционной системы Windows 2000 Professional. Это необходимо для развертывания конкретных пакетов обновлений или утилит:

```
root\cinv2; SELECT * from Win32_OperatingSystem
↳ WHERE caption = ""Microsoft Windows 2000 Professional"
```

- Выдать перечень компьютеров, на которых установлен клиент для сетей Microsoft:

```
root\cinv2; SELECT * from Win32_NetworkClient
↳ WHERE name = ""Microsoft Windows Network"
```

Обратите внимание на использование двойных кавычек в операторе выбора. Двойные кавычки зарезервированы в языке WQL в качестве управляющего символа, поэтому их необходимо указывать дважды, чтобы они были переданы диспетчеру объектов CIM (CIMOM).

Вместо большого количества примеров рассмотрим замечательный способ поиска интересных классов WMI, что позволит создавать собственные операторы WQL.

Набор инструментальных средств разработки WMI (WMI SDK) предоставляется вместе с Web-ориентированным CIMOM-браузером *CIM Studio*. WMI SDK доступен на сайте компании Microsoft по адресу `msdn.microsoft.com/downloads`. Перейдите по дереву до раздела Windows Development⇨Windows Management Instrumentation.

Программа CIM Studio имеет интерфейс браузера (рис. 12.15). Этот браузер можно использовать для поиска интересующих классов. Для этого необходимо щелкнуть на кнопке Find (Найти) (пиктограмма бинокля над правой панелью) и ввести слово **network**. В результате будет выдан список всех классов, в названиях которых содержится слово **network**.

Классы, начинающиеся с `Win32_`, предоставляют доступ к провайдерам информации об операционной системе. Для просмотра информации о классе дважды щелкните левой кнопкой мыши в правой панели на одной из записей `Win32_*` в списке.

Чтобы просмотреть содержимое хранилища CIM для определенного класса, выберите класс и щелкните на кнопке Instances (Экземпляры) — четвертая кнопка справа над правой панелью. В панели будет отображен результат универсального запроса, который можно описать как “Покажи мне все экземпляры этого класса и все их атрибуты”. Заголовки столбцов можно использовать для создания собственного запроса.

Настройка фильтров WMI

Фильтры WMI не могут применяться к отдельным элементам GPO. Например, нельзя использовать фильтрацию только в разделе `Administrative Templates` (Административные шаблоны) объекта GPO. Это значит, что фильтры WMI управляются, как свойства самого GPO. Необходимая последовательность действий приводится в процедуре 12.5.

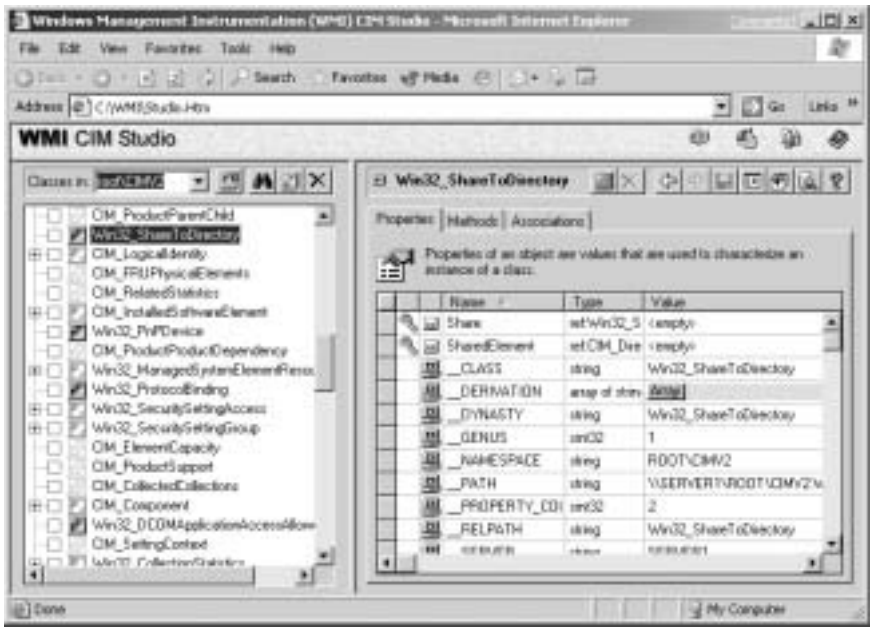


Рис. 12.15. Интерфейс CIM Studio

Процедура 12.5. Доступ к интерфейсу фильтров WMI

1. Откройте окно Properties (Свойства) интересующего GPO.
2. Перейдите на вкладку WMI Filter (Фильтр WMI), которая показана на рис. 12.16.
3. Выберите переключатель This Filter (Этот фильтр) и щелкните на кнопке Browse/Manage (Обзор и управление). Откроется окно Manage WMI Filters (Управление фильтрами WMI).
4. Щелкните на кнопке Advanced (Дополнительно). Откроется окно Edit Filter (Изменить фильтр), как показано на рис. 12.17.
5. Введите оператор WQL, чтобы определить перечень компьютеров или пользователей, для которых будут применяться параметры политики в объекте GPO.
6. Щелкните на кнопке Save (Сохранить) для сохранения оператора WQL и щелкните на кнопке OK для сохранения фильтра.
7. Проверьте работу фильтра, зарегистрировавшись с компьютера, соответствующего требованиям фильтра. Необходимо убедиться, что политика применяется на таком компьютере.



Рис. 12.16. Вкладка WMI Filter *(Фильтр WMI) свойств GPO*

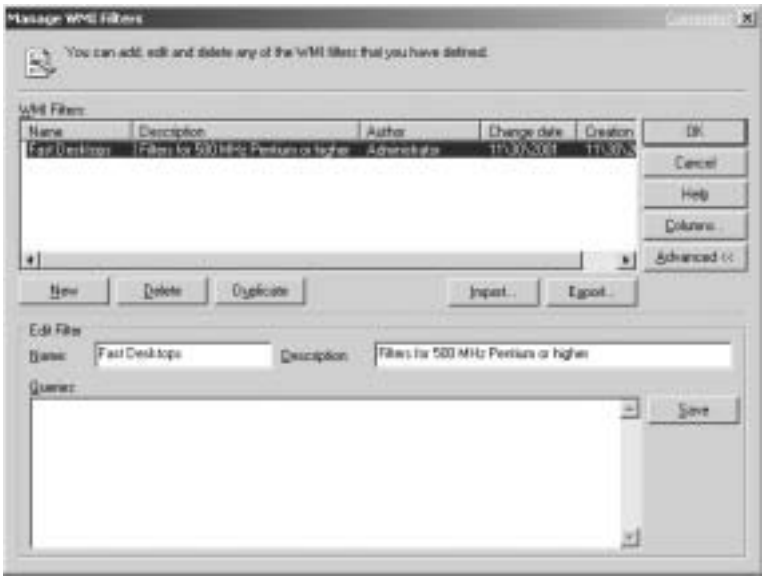


Рис. 12.17. В окне Edit Filter *(Изменить фильтр) отображаются дополнительные параметры для управления фильтром WMI*

Для произвольного GPO можно указать только один фильтр WMI. Фильтр может быть любой сложности, но помните, что клиент должен выполнить оператор до полного завершения. Добавление слишком большого количества критериев выбора в оператор может отрицательно сказаться на времени регистрации клиента.

Хранилище фильтров WMI

Фильтры WMI хранятся в базе данных Active Directory в виде объектов MS-WMI-SOM. Аббревиатура SOM расшифровывается как Scope of Management (Область действия обслуживания). Объекты фильтров хранятся в контейнере SOM с характерным именем `cn=SOM,cn=WMIPolicy,cn=System,dc=<имя_домена>,dc=<корень>`.

Ниже приведен фрагмент списка атрибутов объекта фильтра, в котором показаны атрибуты хранения и управления фильтром:

```
cn: {C3BB1D85-D674-4568-B3BD-BBD4C6EC5A4D};
msWMI-Author: Administrator;
msWMI-ID: {C3BB1D85-D674-4568-83BD-BBD4C6EC5A4D};
msWMI-Name: Phx-Filter-1;
smWMI-Parm1: Computers with CPUs faster than 600 MHz;
msWMI-Parm2: 1;3;10;60;WQL;root\cimv2;
↳ select * from Win32_Processor where currentclockspeed > 600;
```

Рассмотрим наиболее интересные элементы списка.

- В атрибуте `MSWMI-Author` хранится имя пользователя, который создал фильтр. Помните об этом, если не можете проанализировать фильтр и хотите понять, что имел в виду автор.
- В атрибуте `MSWMI-ID` хранится имя фильтра. Для обеспечения уникальности имен имя формируется с помощью алгоритма создания GUID.
- В атрибуте `MSWMI-Name` хранится дружественное имя фильтра.
- В атрибуте `MSWMI-Parm1` хранится описание фильтра.
- В атрибуте `MSWMI-Parm2` хранится оператор языка запросов для фильтра.

Делегирование управления политиками

Одной из ключевых особенностей Active Directory является возможность точной настройки административных прав. Например, можно создать организационную единицу для конкретного набора пользователей и групп и делегировать административные права для этой организационной единицы локальному администратору или опытному пользователю.

Делегирование возможности создания объектов групповых политик (GPO) и управления ими оказывается немного более сложным, чем делегирование возможности управления пользователями, компьютерами или совместно используемыми принтерами. Двойственный характер объекта GPO (состоящего из контейнера GPC и шаблона GPT) означает, что локальному администратору необходимо иметь две привилегии:

- привилегию создавать и изменять файлы в каталоге `Sysvol` на контроллере домена;
- возможность создавать новый объект групповой политики в базе данных Active Directory.

Эти привилегии по умолчанию пользователям не предоставляются. Их необходимо предоставлять отдельно.

Предоставление прав доступа к GPT

Шаблоны групповой политики (GPT) хранятся в файлах каталога политики в каталоге `Sysvol`. Предоставление прав доступа к этим файлам подразумевает установку разрешений NTFS для каталога `\Sysvol\Sysvol\<имя_домена>\Policies`.

На самом деле этот каталог является точкой функционального монтирования (reparse point), связанной с каталогом `\Sysvol\Domain\Policies`, поэтому разрешения можно устанавливать для любого из этих двух каталогов.

Начните с создания группы для локальных администраторов. Затем назначьте этой группе разрешения на чтение, запись, создание и изменение для каталога `Policies`.

С другой стороны, если локальным администраторам необходимо управлять существующими объектами GPO, но не требуется их создавать, можно сначала создать GPO, после чего предоставить доступ к каталогу политики.

Новые разрешения NTFS приводят к изменениям в каталогах, которые реплицируются на другие контроллеры домена средствами службы репликации файлов.

Предоставление прав доступа к GPC

После установки прав доступа к шаблонам групповых политик (GPT) предоставьте группе администраторов разрешения на создание GPO. Для этого добавьте администраторов в группу `Group Policy Creator Owners`. Эта группа имеет право создавать и изменять объекты в контейнере `Policies` в базе данных Active Directory: `cn=Policies,cn=System, dc=<имя_домена>,dc=<корень>`.

Если группе администраторов не был предоставлен полный доступ к организационной единице, придется делегировать группе разрешение `Create Link` (Создавать ссылку) для организационной единицы.

Управление отдельными типами групповых политик

Теперь, когда были показаны методы распространения различных групповых политик, а также методы их загрузки и применения, рассмотрим использование конкретных типов групповых политик.

В этом разделе рассматриваются механизмы реализации и устранения неисправностей в работе различных типов политик. Дополнительная информация приводится в следующих главах.

- Дополнительная информация о перенаправлении каталогов и управлении средой пользователя приводится в главе 19, “Управление операционной средой пользователя”.
- Дополнительную информацию об использовании политик безопасности можно получить в главе 11, “Безопасность доступа по сети и протокол Kerberos”.
- В главе 17, “Управление шифрованием файлов”, и главе 18, “Управление инфраструктурой открытого ключа”, содержится дополнительная информация о политиках шифрованной файловой системы, инфраструктуры открытого ключа и политиках IPSec.
- В главе 2, “Модернизация и автоматизированная установка”, подробно рассматривается использование политик служб удаленного доступа для управления мастером установки клиентов (Client Installation Master).

  Политики управления Internet Explorer в данной книге не рассматриваются.

Политики безопасности

Ранее в этой главе рассматривались особенности развертывания групповых политик безопасности в пределах домена. В этом разделе показано, как работает механизм развертывания групповых политик и как настраивать систему безопасности без использования групповых политик.

На компьютерах под управлением операционных систем Windows Server 2003, Windows XP и Windows 2000 параметры безопасности хранятся в локальной базе данных `Secedit.sdb`. Эта база данных находится в каталоге `\Windows\Security\Database`. Групповые политики безопасности реализовываются с помощью изменения значений в базе данных `Secedit.sdb`.

Кроме записей, в базе данных `Secedit.sdb` политики безопасности могут менять права доступа к файлам и каталогам файловой системы NTFS, разделам системного реестра и локальным службам.

Файлы шаблонов групповых политик безопасности

При создании параметра политики безопасности в GPO средствами редактора групповых политик (Group Policy Editor) редактор сохраняет параметры в файле шаблона групповой политики (GPT), `GptTmpl.inf`.

Клиенты, к которым относится GPO, загружают файл `GptTmpl.inf` и копируют его в локальный каталог `\Windows\Security\Templates\Policy`. Если на клиент оказывают действие несколько объектов GPO с параметрами безопасности, он копирует все файлы `GptTmpl.inf`, добавляя порядковые номера в имя файла с расширением `.inf`. Последовательность номеров совпадает с иерархией приоритета объекта групповой политики. Единственное исключение составляет политика `Default Domain`, которая получает специальное расширение `.dom`.

При регистрации пользователя процесс Winlogon извлекает содержимое файлов `.dom` и `.inf` и заносит полученные параметры в базу данных системы безопасности локального компьютера и в системный реестр. Результаты этой транзакции можно увидеть в файле `Winlogon.log` в каталоге `\Windows\Security\Log`. Политики безопасности вступают в силу сразу после загрузки.

Кроме этого, локальные клиенты загружают изменения политик безопасности при каждом обновлении групповых политик. Обновление выполняется с периодичностью от 90 до 120 минут для обычных компьютеров и каждые 5 минут для контроллеров домена. Дополнительное обновление политик безопасности выполняется каждые 16 часов. При стандартном фоновом обновлении загружаются только политики, в которые были внесены обновления. При обновлении каждые 16 часов загружаются все политики безопасности независимо от наличия изменений.

> ### Специальная обработка политик учетных записей
>
> Такие политики учетных записей, как политики паролей, политики блокирования учетных записей и политики Kerberos, могут устанавливаться только в объекте групповой политики `Default Domain`. Эти политики доступны и в других объектах групповых политик, но их установка ни на что не влияет.

Для просмотра политик безопасности, применяемых на локальном сервере, запустите консоль Local Security Settings (Локальная политика безопасности), воспользовавшись командой Start⇨Programs⇨Administrative Tools⇨Local Security Policy (Пуск⇨Программы⇨Администрирование⇨Локальная политика безопасности). На рис. 12.18 показан пример локальных политик безопасности для сервера, входящего в домен.

Просматривая параметры политики, можно обратить внимание, что для обозначения одних из них используется пиктограмма с небольшими синими символами, а для других — пиктограмма в виде изображения сервера с небольшим рулоном бумаги. Пиктограммы второго типа указывают, что параметр политики получен вместе с групповой политикой. Пиктограммы первого типа указывают, что параметр получен из локальной базы данных системы безопасности.

Принятые по умолчанию шаблоны безопасности

Групповые политики являются идеальным инструментом для управления параметрами безопасности на контроллерах домена и компьютерах, входящих в домен. Но параметры безопасности можно менять и непосредственно с помощью утилиты `Secedit`. Утилита `Secedit` исполь-

зует файл шаблона для предоставления параметров, заносимых в базу данных `Secedit.sdb`, и другие объекты системы безопасности.

Существует два набора шаблонов безопасности. Первый набор хранится в каталоге `\Windows\INF`. Система использует эти шаблоны для значительных изменений параметров безопасности при изменении роли сервера. Ниже перечислены эти шаблоны и их назначение.

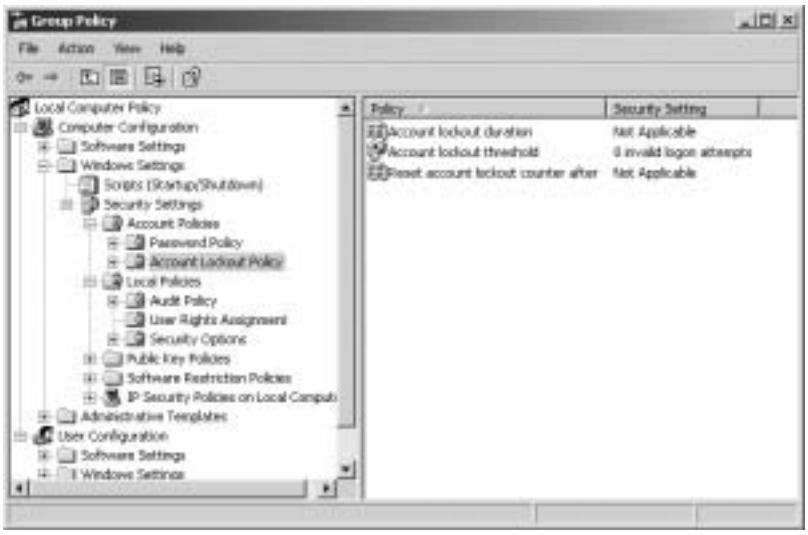


Рис. 12.18. Консоль Local Security Settings *(Локальная политика безопасности) для сервера в домене*

- **DEFLTSV.INF.** Применяется при первой установке сервера.
- **DEFLTDC.INF.** Применяется при повышении сервера до контроллера домена.
- **DSUP.INF.** Применяется при модернизации сервера с операционной системой Windows NT 4.0 или Windows 2000.
- **DCUP5.INF.** Применяется при модернизации контроллера домена под управлением операционной системы Windows 2000.
- **DSUPT.INF.** Применяется при модернизации сервера под управлением операционной системы Windows NT 4.0 Terminal Server или сервера под управлением операционной системы Windows 2000, работающего в режиме приложений.
- **DCFIRST.INF.** Применяется на сервере, который первым повышается до контроллера домена в пределах домена. В этом шаблоне присутствуют специальные политики Kerberos, политики учетных записей, группы с ограниченными привилегиями и информация о членстве в группах.

Специальные шаблоны безопасности

Кроме шаблонов безопасности, которые применяются во время процедуры установки и повышения до контроллера домена, существуют дополнительные шаблоны безопасности, которые хранятся в каталоге `\Windows\Security\Templates`. Эти шаблоны содержат предварительно созданные параметры простой, безопасной и "сверхбезопасной" конфигурации серверов, рабочих станций и контроллеров домена. Кроме этого, присутствует пакет для удаления группы `Terminal Server User` из разрешений файловой системы NTFS на сервере.

Совет по использованию системного реестра: текущий файл шаблона

Имя шаблона безопасности, который применяется программой установки или вручную добавляется в базу данных `Secedit`, хранится в записи системного реестра `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Secedit\TemplateUsed`.

Предварительно созданные шаблоны безопасности можно использовать для анализа параметров системы и модернизации системы с использованием новых параметров безопасности. Обычно это требуется только при управлении изолированным сервером. Контроллером домена необходимо управлять с использованием групповых политик.

Оснастка Security Configuration and Analysis (Анализ и настройка безопасности)

Эта оснастка MMC позволяет сравнить текущие локальные параметры безопасности с содержимым шаблона безопасности. Также эту оснастку можно использовать для применения параметров из шаблона безопасности.

Для использования оснастки необходимо создать собственную консоль MMC. После создания консоли необходимо загрузить шаблон безопасности и использовать его в качестве эталона для сравнения с текущими параметрами безопасности. Любое обнаруженное отличие должно привлечь внимание администратора и быть выделено большой пиктограммой красного цвета (рис. 12.19). Если параметры из шаблона безопасности вас полностью устраивают, их можно применить на данном компьютере. Необходимая последовательность действий приводится в процедуре 12.6.

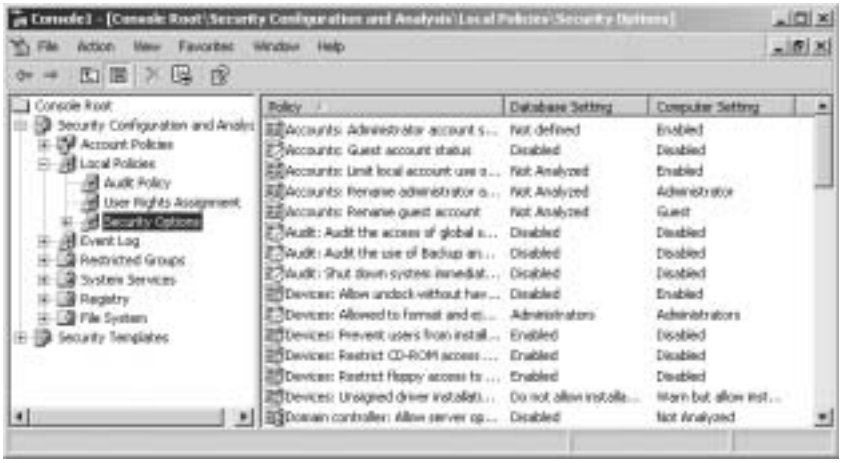


Рис. 12.19. Консоль Security Configuration and Analysis (Анализ и настройка безопасности), на которой выделены обнаруженные различия между конфигурацией в шаблоне безопасности и текущей конфигурацией компьютера

Процедура 12.6. Использование оснастки Security Configuration and Analysis (Анализ и настройка безопасности)

1. Откройте консоль MMC с помощью команды `mmc` в окне Run (Выполнить).
2. В меню консоли выберите Console⇨Add/Remove Snap-in (Консоль⇨Добавить/удалить оснастку). Откроется окно Add/Remove Snap-in (Добавить/удалить оснастку).

3. Щелкните на кнопке Add (Добавить). Откроется окно Add Standalone Snap-in (Добавить изолированную оснастку).
4. Выберите оснастки Security Configuration and Analysis (Анализ и настройка безопасности) и Security Templates (Шаблоны безопасности).
5. Закройте окно, чтобы вернуться в окно Add/Remove Snap-in (Добавить/удалить оснастку). В списке появятся две оснастки без расширений.
6. Щелкните на кнопке OK, чтобы сохранить выбранные элементы и вернуться на консоль MMC.
7. Выберите Console⇨Save As (Консоль⇨Сохранить как) и сохраните консоль под легко запоминаемым именем, например `Security Analysis.msc`.
8. Разверните дерево обеих оснасток. В разделе Security Templates (Шаблоны безопасности) будет отображен список шаблонов безопасности из каталога `\Windows\Security\Templates`. В разделе Security Configuration and Analysis (Анализ и настройка безопасности) будет отображен набор команд для выполнения анализа.
9. Раскройте раздел для одного из шаблонов и просмотрите параметры в разделах Account Policies (Политики учетных записей) и Local Policies (Локальные политики). Параметры шаблона можно изменить, чтобы они больше соответствовали реальной ситуации на локальном компьютере. Результат изменений лучше сохранить в виде нового шаблона.
10. Щелкните правой кнопкой мыши на пиктограмме Security Configuration and Analysis (Анализ и настройка безопасности) и выберите из контекстного меню команду Open Database (Открыть базу данных). Откроется окно Open Database (Открыть базу данных).
11. Введите имя базы данных, в которой будет храниться результат анализа. Не пытайтесь открыть существующую базу данных `Secedit.sdb`. Если попытаться это сделать, будет выдано сообщение об *отказе в доступе* (access denied).
12. Щелкните правой кнопкой мыши на пиктограмме Security Configuration and Analysis (Анализ и настройка безопасности) и выберите из контекстного меню команду Analyze Computer Now (Анализ компьютера). Откроется окно Perform Analysis (Выполнить анализ), в котором указан каталог для хранения журнала анализа.
13. Щелкните на кнопке OK. После завершения анализа раскройте раздел Security Configuration and Analysis (Анализ и настройка безопасности), чтобы просмотреть параметры безопасности. Каждое отличие между локальными параметрами и параметрами шаблона безопасности выделяется пиктограммой красного цвета.

Распространение шаблонов безопасности

Если используются изолированные серверы, например серверы в демилитаризованной зоне, серверы приложений, работающие за пределами домена, или серверы под управлением Windows Server 2003, входящие в состав домена Windows NT, обновления безопасности для этих компьютеров можно распространять с помощью шаблонов безопасности и утилиты `Secedit`.

Для утилиты `Secedit` предусмотрено четыре режима работы, каждый из которых включается с помощью соответствующего параметра командной строки.

- **Analyze (Анализ).** Утилита сравнивает существующие параметры безопасности с файлом шаблона и записывает результат в указанную базу данных SDB и файл журнала. Команда выглядит следующим образом:

```
secedit /analyze /db somename.sdb /cfg template.inf /log
↳ somename.log
```

- **Configure (Настройка).** Обновляет существующие параметры безопасности, используя содержимое файла шаблона безопасности. Можно выбрать определенные разделы шаблона вместо всего содержимого. Результат операции сохраняется в указанной базе данных.

Предупреждение. Применение шаблона безопасности может или снизить уровень безопасности до неприемлемого уровня, или заблокировать компьютер вплоть до полной невозможности получить доступ. Используйте этот параметр с осторожностью. Пример команды показан ниже:

```
secedit /configure /db somename.sdb /cfg template.inf /log
↳ somename.log /area area1 area2
```

- **Export (Экспорт).** Извлекает текущие параметры безопасности и записывает их в файл шаблона. Эта операция полезна при настройке группы серверов с одинаковыми параметрами безопасности. Настройте параметры одного компьютера и скопируйте параметры в шаблон безопасности для распространения шаблона с помощью утилиты `Secedit`. Команда выглядит следующим образом:

  ```
  secedit /export /cfg template.inf /log somename.log
  ```

- **Validate (Оценить).** Извлекает содержимое шаблона и проверяет правильность синтаксиса для импорта. Пример команды показан ниже:

  ```
  secedit /validate template.inf
  ```

Утилиту `Secedit` можно использовать для установки файлов шаблонов на компьютерах под управлением Windows Server 2003 в классическом домене Windows NT 4.0. Для этого файл `Secedit.exe` и шаблон безопасности необходимо разместить на общем ресурсе `Netlogon` каждого контроллера домена и добавить в регистрационный сценарий строку для применения шаблона безопасности. Удостоверьтесь, что регистрационный сценарий применяет шаблон безопасности только на серверах под управлением операционной системы Windows Server 2003. (Можно создать несколько шаблонов и при помощи ветвления в регистрационном сценарии выбирать подходящую платформу, но такую функциональную возможность достаточно сложно реализовать в стандартных файлах пакетной обработки.)

Резюме о политиках безопасности

Вот основные моменты применения политик безопасности на локальных компьютерах.

- Политики безопасности для локального компьютера хранятся в базе данных Security Editor, `\Windows\Security\Database\Secedit.sdb`.
- Групповые политики безопасности загружаются всегда, независимо от скорости соединения.
- Такие политики учетных записей, как история паролей, сложность пароля, политики блокирования и т.д., должны определяться в политике `Default Domain` и не могут быть изменены в других групповых политиках.
- Локальные политики безопасности применяются в процессе установки и в процессе повышения до контроллера домена. Для этого используются шаблоны безопасности из каталога `\Windows\INF`.
- Локальные политики безопасности могут быть изменены с помощью утилиты `Secedit` благодаря применению шаблонов безопасности из каталога `\Windows\Security\Templates`.

Политики административных шаблонов

Самым очевидным применением административных шаблонов является внесение изменений в системный реестр одновременно на сотнях и тысячах компьютеров. До этого уже было показано большинство механизмов создания и изменения политик административных шаблонов. Вот краткое описание принципов работы административных шаблонов.

- В редакторе групповой политики (GPE) параметры административных шаблонов выводятся на основе файлов шаблонов ADM. Файлы ADM хранятся в каталоге `\Windows\INF`.

- При включении или отключении политик административных шаблонов GPE создает запись в файле GPT, который называется `Registry.pol`. Этот файл хранится в каталоге политики в подкаталоге `Sysvol`. Для каждой политики существует два файла `Registry.pol`: один в каталоге `Machine`, где хранятся политики раздела `Computer Configuration` (Конфигурация компьютера), и один в каталоге `User`, где хранятся политики раздела `User Configuration` (Конфигурация пользователя).
- Клиенты, связанные с объектом групповой политики, который содержит административные шаблоны, загружают файлы `Registry.pol` и вносят их содержимое в специальные разделы системного реестра `Policies`.
- Настроенные на поиск параметров в разделах `Policies` приложения в своей работе зависят от содержимого групповой политики.

Рассмотрим эти процессы более подробно. Желательно полностью понять принципы обработки административных шаблонов. Большинство возможностей распределенного управления в операционной системе Windows Server 2003 в том или ином виде основано на политиках системного реестра.

Специальные разделы системного реестра для использования политик

Политики административных шаблонов в файле `Registry.pol` записываются в специальные разделы системного реестра, предназначенные для хранения временных записей групповых политик. Такие политики хранятся в четырех разделах. Политики из раздела `Computer Configuration` (Конфигурация компьютера) записываются в раздел системного реестра `HKLM`, а политики из раздела `User Configuration` (Конфигурация пользователя) записываются в раздел `HKCU`.

- `HKLM\Software\Policies`
- `HKLM\Software\Microsoft\Windows\CurrentVersion\Policies`
- `HKCU\Software\Policies`
- `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies`

Записи в этих разделах обновляются каждый раз при загрузке компьютера или при регистрации пользователя. Если из объекта групповой политики (GPO) удалить административный шаблон или разорвать связь с GPO, содержащим административные шаблоны, записи будут удалены из локального системного реестра клиента. Это позволяет устранить недостаток, характерный для классических системных политик Windows NT, когда в системном реестре навсегда сохранялись внесенные изменения.

Постоянное хранение внесенных изменений и классические системные политики

Рассмотрим пример постоянного хранения изменений. При использовании классических системных политик Windows NT можно определить фоновое изображение рабочего стола для группы пользователей. Если внести пользователя в такую группу, политика будет внесена в раздел системного реестра `HKCU` и выбор фонового изображения вступит в силу.

Если удалить пользователя из такой группы, выбор фонового изображения останется в силе на рабочей станции пользователя. Для удаления фонового изображения придется вручную внести изменения на рабочей станции или определить другую группу с системной политикой, удаляющей фоновое изображение. Во втором случае пользователя придется включить в новую группу.

При использовании групповых политик такая ситуация решается значительно проще. Сначала определяется политика для фонового изображения. С этой целью создается объект группо-

вой политики с политикой административного шаблона, который называется `Active Desktop Wallpaper`, в разделе User Configuration⇨Administrative Templates⇨Desktop⇨Active Desktop (Конфигурация пользователя⇨Административные шаблоны⇨Рабочий стол⇨Active Desktop). Этот GPO необходимо связать с организационной единицей, в которую входят учетные записи пользователей. После этого все пользователи получат одинаковое фоновое изображение на рабочем столе.

При удалении пользователя из организационной единицы параметр политики удаляется и используется оригинальное фоновое изображение, которое использовалось до назначения групповой политики ("статус-кво", как говорят в Вашингтоне).

Политики и предпочтения

Гибкость и непостоянство основанных на системном реестре групповых политик делают их привлекательным инструментом, но есть одна особенность, которую стоит запомнить. Такие политики работают только в том случае, если приложения запрограммированы на использование соответствующих записей в системном реестре. Другими словами, управление приложением XYZ с помощью групповых политик невозможно, если приложение XYZ не знает, что нужно просматривать один из разделов `Policies` в системном реестре для получения параметров.

Групповые политики можно использовать для изменения параметров в системном реестре за пределами разделов `Policies`. В таком случае будут внесены постоянные изменения, как при использовании классических системных политик Windows NT. Компания Microsoft называет такие постоянные изменения системного реестра *предпочтениями* (preferences). Они отличаются от *политик* (policies), которые могут свободно добавляться в системный реестр и удаляться из него.

Политики оказываются намного гибче и проще в управлении, чем предпочтения, но если нужно управлять устаревшими приложениями, изменения в системный реестр приходится вносить с помощью предпочтений. Далее будет показано, как создавать предпочтения, но сначала рассмотрим, как с помощью редактора групповых политик создавать стандартные политики.

Файлы шаблонов ADM

Политики административных шаблонов получили такое название из-за того, что параметры извлекаются из текстовых файлов шаблонов ADM. Это напоминает классические системные политики Windows NT, но структура файлов ADM и их использование значительно отличаются.

Файлы шаблонов ADM хранятся в каталоге `\Windows\INF`. Редактор групповых политик по умолчанию загружает четыре таких файла.

- **System.adm.** В этом файле содержится полный список параметров политик для управления большинством возможностей Explorer (Проводник).
- **Inetres.adm.** Политики Internet Explorer, которые оказывают влияние на такие компоненты, как Internet Explorer, Control Panel (Панель управления), автономные страницы, меню браузера, Persistence Behavior и `Administrator Approved Controls`.
- **Conf.adm.** Политики NetMeeting.
- **Wmplayer.adm.** Политики Windows Media Player.

Устаревшие шаблоны

Кроме стандартных шаблонов ADM, в составе операционной системы Windows Server 2003 предоставляются дополнительные шаблоны для обратной совместимости с классическими системными политиками Windows NT. За одним исключением такие шаблоны ADM не могут

загружаться в редактор групповых политик. Для доступа к таким шаблонам (кроме шаблона `Inetset.adm`) необходимо воспользоваться *редактором системных политик* (System Policy Editor или Poledit). Ниже перечислены доступные шаблоны для обратной совместимости.

- **Inetset.adm.** В этом шаблоне содержатся предпочтения для управления параметрами Internet Explorer (дополнительную информацию о предпочтениях можно получить в предыдущем разделе).
- **Inetcorp.adm.** В этом файле содержатся системные политики, которые управляют языками Internet Explorer, ограничениями коммутируемого доступа и кэшированием.
- **Winnt.adm.** Системные политики для операционной системы Windows NT 4.0.
- **Windows.amd.** Системные политики для операционных систем Windows 9x.
- **Common.adm.** Системные политики, общие для параметров операционных систем Windows NT 4.0 и Windows 9x.

Загрузка дополнительных шаблонов ADM

Купив приложение, в котором используются временные групповые политики, например Office 2003 или Office XP, в редактор групповых политик можно загружать шаблоны ADM, как описано в процедуре 12.7.

Процедура 12.7. Загрузка шаблонов ADM в редактор групповых политик

1. Откройте редактор групповых политик для объекта групповой политики, в который следует добавить дополнительные шаблоны.
2. Раскройте подраздел `Administrative Templates` (Административные шаблоны) в разделе `Computer Configuration` (Конфигурация компьютера) или в разделе `User Configuration` (Конфигурация пользователя) — разница не существенна.
3. Щелкните правой кнопкой мыши на пиктограмме Administrative Templates (Административные шаблоны) и выберите из контекстного меню команду Add/Remove Templates (Добавление и удаление шаблонов).
4. Щелкните на кнопке Add (Добавить). Откроется список шаблонов, хранящихся в каталоге `\Windows\INF`.
5. Найдите каталог, в котором хранятся нужные шаблоны, и выберите интересующий шаблон.
6. Закройте окно Add/Remove Templates (Добавление/удаление шаблонов), чтобы загрузить выбранный шаблон. (Выбор шаблона сохраняется в параметрах консоли MMC, поэтому шаблон будет открыт при следующем запуске консоли.)
7. Убедитесь, что политики загруженного шаблона доступны для просмотра. Если используется некорректный формат шаблона, то в процессе загрузки будет выдано сообщение об ошибке.
8. Если шаблон содержит только классические системные политики без инструкций по обработке, он будет расположен в разделе внешних политик и содержимое политик окажется недоступным.

> **Редактор системных политик Poledit и операционная система Windows Server 2003**
>
> В составе операционной системы Windows Server 2003 предоставляется редактор системных политик `Poledit`, который можно использовать для создания файлов `Config.pol` и `Ntconfig.pol` для клиентов более старых версий Windows и управления ими.

Сохраните файлы с расширением .pol в каталоге \Windows\Sysvol\Sysvol\<*имя_домена*>\Scripts. Этот каталог предоставляется для совместного доступа под именем Netlogon.

Современные клиенты Windows (Windows Server 2003, Windows XP и Windows 2000), входящие в домен Windows NT 4.0, будут загружать и применять системные политики. Как только домен будет модернизирован до Windows Server 2003 или Windows 2000, все современные клиенты Windows прекратят использование системных политик и перейдут к использованию групповых политик.

Групповые и системные политики

Пользователи и компьютеры под управлением операционной системы Windows Server 2003 обрабатывают классические системные политики только в том случае, если групповые политики Active Directory недоступны. Рассмотрим несколько примеров.

- Пользователь в домене Active Directory регистрируется на компьютере под управлением Windows Server 2003, который также входит в домен Active Directory. Системные политики не обрабатываются.
- Пользователь в домене Active Directory регистрируется на компьютере под управлением Windows Server 2003, который входит в домен Windows NT 4.0: система обрабатывает политики компьютера из файла Ntconfig.pol.
- Пользователь в домене Windows NT 4.0 регистрируется на компьютере Windows Server 2003, который входит в домен Active Directory: система обрабатывает политики пользователя из файла Ntconfig.pol.

Файлы Registry.pol

После того, как администратор включает параметры политик административных шаблонов в редакторе групповых политик (GPE), редактор GPE извлекает параметры политик из шаблона ADM и использует их для создания записей в файле Registry.pol. Это текстовый файл в кодировке Unicode.

Редактор групповой политики предоставляет три альтернативных значения групповой политики: Enabled (Включена), Disabled (Отключена) и Not Configured (Не установлена). Вот что редактор групповой политики записывает в файл Registry.pol в зависимости от значения политики.

- **Enabled (Включена).** Редактор групповых политик (GPE) извлекает содержимое соответствующего файла шаблона .adm и на его основе создает запись в файле Registry.pol. Например, при включении политики Hide My Network Places (Скрывать Мое сетевое окружение) GPE добавляет следующую запись в файл Registry.pol:

```
[Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
↪ ;NoNetHood ; ; ;]
```

- **Disabled (Отключена).** Редактор GPE добавляет в файл Registry.pol запись, которая отключает фрагмент файла ADM. Например, при отключении политики Hide My Network Places (Скрывать Мое сетевое окружение) редактор добавляет следующую запись в файл Registry.pol:

```
[Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
↪ ;**del.NoNetHood ; ; ;]
```

- **Not Configured (Не установлена).** Редактор GPE удаляет из файла Registry.pol все записи, связанные с листингом. Это не оказывает влияния на другие файлы Registry.pol, поэтому, если запись внесена в другой объект групповой политики, политика будет применяться.

При загрузке клиентом файла Registry.pol записи вносятся во временный раздел Policies, указанный в шаблоне. Эта операция выполняется расширением на стороне клиента Userenv.dll и не требует вмешательства администратора.

Подробное описание записей в файлах ADM

Листинги групповых политик ADM предназначены для занесения во временные разделы системного реестра Policies. Рассмотрим фрагмент файла System.adm, чтобы продемонстрировать, как это работает:

```
CLASS USER
CATEGORY !!Desktop
    KEYNAME "Software\Microsoft\Windows\CurrentVersion\Policies\
↳ Explorer"
    POLICY !!NoNetHood
        #if version >= 4
            SUPPORTED !!SUPPORTED_Win2k
        #endif

        EXPLAIN !!NoNetHood_Help
        VALUENAME "NoNetHood"
    END POLICY
END CATEGORY

[strings]
Desktop="Desktop"
NoNetHood="Hide My Network Places icon on desktop"
NoNetHood_Help="removes the My Network Places icon from the desktop.
↳ \n\n Этот параметр влияет только на пиктограмму. Он не позволяет
↳ заблокировать пользователям доступ в сеть или доступ к совместно
↳ используемым сетевым ресурсам."
SUPPORTED_Win2k="At least Microsoft Windows 2000"
```

Чтобы упростить чтение шаблонов ADM, компания Microsoft активно использует ярлыки строк (string token). Если возле слова присутствует строка из двух восклицательных знаков (!!), можно сделать вывод, что это ярлык строки. В каждом файле ADM присутствует список ярлыков строк и полных версий этих строк, для которых созданы ярлыки.

Ниже приведено краткое описание различных элементов содержимого файла ADM.

- **CLASS USER.** Указывает на фрагменты кода, которые отображаются как подразделы в разделе User Configuration (Конфигурация пользователя) в редакторе групповой политики.
- **CATEGORY.** Указывает на фрагменты кода, которые отображаются как подразделы раздела, обозначенного ярлыком строки. В этом случае ярлык !!Desktop "разворачивается" в слово Desktop.
- **KEYNAME.** Указывает на фрагменты кода, которые превращаются в одноименные записи системного реестра. Отдельные листинги могут переопределять принятую по умолчанию запись KEYNAME. Обратите внимание, что в этом примере показана запись в одном из временных разделов системного реестра, Software\Microsoft\Windows\CurrentVersion\Policies.
- **POLICY.** Этот фрагмент кода отображается в редакторе групповых политик в разделе, идентифицированном ярлыком строки !!NoNetHood. Этот ярлык строки "разворачивается" в имя Hide My Network Places icon on desktop.
- **SUPPORTED.** Это новое ключевое слово Windows Server 2003, которое идентифицирует платформу, поддерживающую политику. Это ключевое слово используется фильтром GPE для отображения подмножества политик.

- **EXPLAIN.** Этот ярлык содержит справочное сообщение, которое отображается вместе с политикой в редакторе групповой политики. Текст выводится на вкладке Explain (Описание) в окне политики и на панели консоли MMC в режиме Web-обозревателя. Ярлык строки `!!NoNetHood_Help` "разворачивается" в полный текст описания.
- **VALUENAME.** Этот ярлык содержит точное значение, которое будет записано в файл `Registry.pol` при активизации этого фрагмента кода. По умолчанию используется тип значения `REG_SZ`. Параметр `NUMERIC=` позволяет указать тип значения `REG_DWORD` или `REG_BINARY`.

При загрузке файла `Registry.pol` с этими записями расширение на стороне клиента запишет в системный реестр следующее:

> Раздел: `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`
> Запись: `NoNetHood`

После этого файла ADM пиктограмма My Network Places (Мое сетевое окружение) исчезнет с рабочего стола в операционной системе Windows Server 2003) и меню Start (Пуск) исчезнет в операционной системе Windows XP. Помните, что это работает только из-за того, что программа Explorer запрограммирована на получение конкретной записи системного реестра при создании рабочего стола для пользователя. Explorer использует сотни записей в системном реестре, но с помощью политик можно установить всего несколько десятков таких записей.

Политики и предпочтения

Существует возможность создания собственных шаблонов `ADM`, которые будут записывать значения за пределами временных разделов `Policies`. Эти записи будут обработаны расширениями на стороне клиента точно так же, как обычные групповые политики, но результатом обработки станет запись в системном реестре.

Компания Microsoft использует термин *предпочтение* (preference) для описания групповой политики, которая вносит запись в системный реестр за пределами временных разделов `Policies`. В редакторе GPE предпочтение обозначается красной точкой на пиктограмме. Стандартные групповые политики обозначаются синей точкой.

Для просмотра предпочтений удобно загрузить шаблон `Inetres.adm`. Этот шаблон содержит записи, которые вносятся за пределами временных разделов `Policies`. Содержимое шаблона отображается, как предпочтения с красной точкой на пиктограмме.

Иногда стандартные политики называют *управляемыми* (managed) политиками. По умолчанию редактор групповых политик отображает информацию только об управляемых политиках. Для отображения предпочтений щелкните правой кнопкой мыши на пиктограмме Administrative Templates (Административные шаблоны) и выберите из контекстного меню команду Filtering (Фильтрация). В окне Filtering (Фильтрация) сбросьте флажок Only Show Policy Settings That Can Be Fully Managed (Показывать только управляемые параметры политик) и сохраните внесенное изменение.

После этого можно будет просматривать предпочтения из шаблона `Inetres.adm`. Будут доступны следующие варианты.

- Если активизировать (Enable) предпочтение, запись в файле `Registry.pol` содержит полный путь в системном реестре. Расширение на стороне клиента внесет запись непосредственно в системный реестр.
- Если отключить (Disabled) предпочтение, запись в файле `Registry.pol` меняется, и к названию записи добавляется префикс `**del`. Расширение на стороне клиента удалит запись из системного реестра.
- Если переключить предпочтение в состояние Not Configured (Не определено), в силе останется последняя запись, которая была добавлена в системный реестр.

Для удаления предпочтения его сначала нужно отключить, подождать, пока клиенты загрузят политику, после чего установить для предпочтения значение Not Configured (Не определено).

Создание собственного шаблона ADM

С помощью копирования существующего шаблона можно создавать собственные шаблоны `ADM`. Перед этим убедитесь, что политики уже не существует. Утилита Help and Support (Справка и поддержка) позволяет просмотреть все политики. В составе Resource Kit предоставляется файл справки по групповым политикам (`Gp.chm`), в котором политики перечислены в более удобной форме.

Помните, что создание шаблона, который добавляет запись в раздел `Policies`, оказывает влияние только на те приложения, которые запрограммированы на поиск параметров в этих разделах. В большинстве случаев все эти записи уже описаны в шаблонах `ADM`. Если создать шаблон, который добавляет запись за пределы временных разделов `Policies`, GPE создаст предпочтение с красной точкой на пиктограмме.

Политики распространения программного обеспечения

Если верить шумихе торговой прессы, то XXI век является веком расцвета инструментария Application Service Provider (ASP). Даже если это правда, пройдет еще очень много времени, пока все приложения вашего предприятия станут использовать интерфейсы браузера. До этого момента возможность предоставления необходимого программного обеспечения, предназначенного для конкретного пользователя на конкретном компьютере и настроенного соответствующим образом сразу после запуска, остается мечтой системных администраторов.

Развертывание программного обеспечения в операционной системе Windows Server 2003 не совсем похоже на мечту, но эта технология все-таки лучше, чем хождение от одного рабочего места к другому с пачкой компакт-дисков. В этом разделе рассматриваются механизмы развертывания программного обеспечения в операционной системе Windows Server 2003, а также требования к пакетам, предназначенным для развертывания.

Шаблоны ADM могут быть неожиданно перезаписаны

Каждый раз, когда редактор GPE открывает политику, он обновляет собственную локальную копию шаблонов `ADM`, используя главные шаблоны из каталога `\Windows\INF`. По этой причине стоит избегать модификации существующих шаблонов. Вместо этого создавайте новые шаблоны `ADM` и храните их в центральном хранилище, где к ним может получить доступ любой администратор, который вносит изменения в объекты групповых политик.

Альтернативные инструменты развертывания программного обеспечения

Программное обеспечение на основе политик хорошо справляется с распространением файлов, но не более того. При наличии сложных требований к развертыванию или необходимости мониторинга и создания отчетов рекомендуется воспользоваться другими инструментами. Ниже перечислены возможные решения.

- System Management Server (SMS) от компании Microsoft
- Tivoli от компании IBM
- ShipIT от компании Computer Associates
- Программные решения для развертывания предприятия InstallShield
- Mobile Automation

Развертывание программного обеспечения

Как и большинство возможностей на основе политик, развертывание программного обеспечения зависит от целого ряда компонентов.

- **Служба Windows Installer.** Эта служба распространяет содержимое пакета приложения и вносит в системный реестр соответствующие записи, необходимые для установки. Доступны версии службы для операционных систем Windows NT 4.0, Windows 9x и Windows ME, но для развертывания программного обеспечения на основе политик в операционной системе Windows Server 2003 необходимы клиенты, способные взаимодействовать с Active Directory. Развертывание программного обеспечения на клиентах более старых версий, например Windows 9x и Windows NT, не поддерживается.
- **Пакет установки Microsoft (Microsoft installer package — MSI).** Установочный пакет, который состоит из файлов приложения, каталога файлов и инструкций, которые описывают процедуру установки для операционной системы Windows.
- **Пакет развертывания программного обеспечения (Software deployment package — AAS).** Файл шаблона групповой политики, в котором указано расположение файла MSI и инструкции по его развертыванию. Объект `Class Store` в базе данных Active Directory содержит информацию о программном пакете.
- **Сервер развертывания.** Это сервер, на котором хранятся пакеты MSI. Сервер не обязательно должен работать под управлением операционной системы Windows Server 2003 или другой операционной системы Windows, но на нем должен храниться совместно используемый каталог, к которому могут получать доступ клиенты, получающие политики развертывания программного обеспечения.

Кроме этого, развертываемое приложение должно предоставляться в виде файла MSI. (Устаревшее приложение можно упаковать в файл ZAP, который представляет собой пакетный файл, запускающий программу установки приложения.)

Служба Windows Installer

Служба Windows Installer выполняет следующие функции.

- Проверяет версию каждого файла и подсчитывает ссылки на каждый файл, чтобы минимизировать проблемы, возникающие при перезаписи одной версии другой версией. Служба Installer работает совместно с функцией Side-by-Side (SxS) операционной системы Windows Server 2003.
- Выполняет отложенную установку, ожидая, пока пользователь выберет приложение из меню Start (Пуск) или выполнит двойной щелчок на файле данных, связанном с приложением.
- Поддерживает журнал транзакций установки, чтобы была возможность продолжить установку с момента останова. Также поддерживается возможность возврата к предыдущему состоянию даже в процессе процедуры установки.
- Поддерживает каталог установленных компонентов и изменений системного реестра, которые могут быть удалены вместе с приложением. Эта возможность поддерживает параметр групповой политики, который позволяет удалить приложение при удалении пользователя из области действия GPO с политикой распространения программного обеспечения.
- Поддерживает самовосстанавливающиеся приложения, автоматически загружая компоненты, которые были случайно удалены или перезаписаны.
- Может устанавливать приложения, используя расширенные права доступа. Это позволяет пользователям устанавливать приложения без привилегий локального администратора. (Мне показалось, или читатели вскричали “Слава Богу!”?)

Пакеты MSI

Основанное на политиках развертывание программного обеспечения зависит от службы Windows Installer, а служба Windows Installer требует упаковки приложений в файлы MSI.

Не обязательно интегрировать в файл MSI все компоненты приложения, но они должны быть доступны в хранилище, к которому служба Windows Installer может получить доступ, следуя инструкциям из файла MSI. Обычно это означает, что файлы и каталоги в пакете MSI должны находиться в стандартной конфигурации.

Часто установку пакетов MSI можно настраивать с помощью файлов Microsoft Transform (MST). Эти файлы предоставляют сценарии установки (scripted installation) базового пакета MSI. Например, Office Resource Kit (ORK) предоставляет утилиты для отображения окон процесса установки Office 2000 и Office XP и сохранения выбранных параметров в файле MST.

Создание собственных пакетов для развертывания программного обеспечения

Любое приложение, получившее логотип Windows 2000 и Windows Server 2003, должно распространяться в пакете MSI. Этому требованию не соответствует большое количество приложений. Если необходимо развернуть 32-разрядное приложение Windows, которое не имеет пакета MSI, пакет можно создать самостоятельно с помощью нескольких утилит. Ниже показан список доступных утилит (в порядке возрастания стоимости, но не обязательно доступных возможностей).

- **WinInstall 2000.** От компании Veritas, `www.veritas.com`. На установочном компакт-диске операционной системы Windows Server 2003 предоставляется урезанная версия программы WinInstall.
- **Wise Installer.** От компании Wise Solutions, `www.wisesolutions.com`.
- **InstallShield Professional (Installer Edition).** От компании InstallShield, `www.installshield.com`.

Расширение привилегий при установке программного обеспечения

Возможность службы Windows Installer устанавливать пакет MSI, используя расширение привилегий, решает основной вопрос, по которому пользователи обращаются в службу поддержки рабочих станций.

По умолчанию установка с расширением привилегий разрешена только при развертывании приложений с помощью групповых политик. Можно установить групповую политику, которая позволяет службе Windows Installer устанавливать все пакеты MSI с расширением привилегий. Это дает возможность использовать утилиты от сторонних производителей и даже вложения сообщений электронной почты для распространения программного обеспечения, которое будет установлено обычными пользователями.

Политика называется `Always Install With Elevated Privileges` (Всегда устанавливать с расширением привилегий) и хранится в разделе Computer Configuration⇨Administrative Templates⇨Windows Components⇨Windows Installer (Конфигурация компьютера⇨Административные шаблоны⇨Компоненты Windows⇨Windows Installer).

Расширенные права доступа получает только поток процесса, который устанавливает программное обеспечение, поэтому не стоит беспокоиться, что пользователь получит дополнительные привилегии, "вломившись" в процедуру установки. Но включение этой политики действительно приводит к возможности установки "троянской" программы, которая маскируется под пакет MSI и пытается получить расширенные привилегии. Не активизируйте эту политику, не защитив все уязвимые места системы.

Пакет развертывания программного обеспечения

Файл шаблона групповой политики для пакета развертывания программного обеспечения предоставляется в виде двоичного файла и имеет расширение `.aas`. Этот файл хранится в каталоге политики, связанном с объектом групповой политики, в каталоге `Sysvol`.

Пакет развертывания сообщает расширению на стороне клиента, где можно найти пакет MSI (обычно пакет доступен на сетевом ресурсе, указанном с помощью пути UNC), и предоставляет инструкции по специальной обработке пакета. Существует два способа развертывания пакета.

- **Публикация.** Приложение становится доступным в меню аплета Add/Remove Programs (Установка и удаление программ) в Control Panel (Панель управления). Пользователю достаточно дважды щелкнуть на интересующем приложении, и служба Windows Installer установит приложение из пакета MSI, хранящегося на сервере распространения.

  Если публикуется множество приложений, для упрощения выбора интересующего приложения можно присвоить приложениям категории. Для установки категорий для опубликованных приложений откройте окно Properties (Свойства) для пиктограммы Software Distribution (Распространение программного обеспечения) и перейдите на вкладку Categories (Категории).

- **Назначение.** Пакет установки добавляет соответствующие ярлыки в меню Start (Пуск) и регистрирует приложение в системном реестре, как будто приложение уже установлено. При выборе соответствующего пункта в меню Start (Пуск) или двойном щелчке на файле данных, связанном с приложением, служба Windows Installer перехватывает управление и устанавливает пакет MSI с сервера распространения.

В любом случае приложение устанавливается таким образом, чтобы сервер распространения не оказался под пиковой нагрузкой в часы массовой регистрации пользователей. Можно открыть окно с дополнительными параметрами политики развертывания программного обеспечения и установить параметр для принудительной установки назначенного пакета при регистрации пользователя. Это бывает полезно, когда необходимо обеспечить актуальность версии клиентского программного обеспечения при изменении серверной части приложения.

Кроме этого, доступны следующие дополнительные возможности (параметр `Advanced`).

- Поддержка адреса URL для опубликованных приложений, щелчок на котором приводит к предоставлению дополнительной информации о приложении.
- Возможность удаления приложения, если объект пользователя перемещается за пределы контейнера, связанного с объектом групповой политики.
- Возможность удаления существующих копий приложений, которые устанавливались без помощи групповых политик.
- Инструкции по модернизации существующих копий приложения.
- Возможность назначения файлов MST (Microsoft Transform) или другие изменения к основному пакету MSI.

Устранение неисправностей при развертывании программного обеспечения

Если при попытке обеспечить работоспособность пакета программного обеспечения возникают проблемы, начните с проверки применения всех остальных политик из объекта групповой политики. Если остальные политики успешно применяются, проверьте возможность доступа к файлу MSI со стороны клиента и возможность получения пакета для своего пользовательского объекта, помещенного в связанный с объектом групповой политики контейнер.

Если все проверки завершились удачно, придется применять тяжелую артиллерию: журнал диагностики и утилиту addiag.

Журнал диагностики управления приложениями

Расширение на стороне клиента Appmgmt отвечает за загрузку и обработку пакетов развертывания .aas. Существует возможность включения журнала диагностики для расширения Appmgmt. Это позволит проследить за работой расширения и обнаружить все ошибки и проблемы.

Включение журнала диагностики требует внесения изменений в системный реестр. Создайте следующую запись в системном реестре.

> Раздел: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics
> Запись: AppMgmtDebugLevel (REG_DWORD)
> Значение: 4b

Внесение этой записи приведет к созданию журнала Appmgmt.log в каталоге \Windows\Debug\Usermode.

Журнал диагностики службы Windows Installer

После загрузки и обработки пакета .aas расширением Appmgmt служба Windows Installer перехватывает управление и переходит к обработке пакета MSI. Включение журнала диагностики для службы Windows Installer позволяет определить, что делает служба для установки приложения, и увидеть все сообщения об ошибках. Для включения этого журнала также требуется внесение записи в системный реестр.

> Раздел: HKLM\Software\Policies\Microsoft\Windows\Installer
> Запись: Logging (REG_SZ)
> Значение: voicewarmup

Важна каждая буква в значении записи. Порядок может быть произвольным. Ниже расшифровано значение каждой буквы.

- i — сообщения о состоянии
- w — некритические предупреждения
- e — все сообщения об ошибках
- a — начало операций
- r — записи, характерные для операций
- u — пользовательские запросы
- c — начальные параметры пользовательского интерфейса
- m — недостаток памяти или информация о фатальном завершении
- o — сообщения о недостатке дискового пространства
- p — свойства терминала
- v — подробный отчет
- + — добавить к существующему файлу
- ! — заносить в журнал каждую строку
- * — использовать все параметры, кроме v
- l*v — шаблон с подробным отчетом

Эта запись приводит к созданию журнала в каталоге %TEMP%. Имя журнала начинается строкой MSI, после чего указывается последовательность цифр и расширение .log.

Утилита addiag

Утилита addiag входит в состав Support Tools. Утилита предоставляет информацию об установленных пакетах MSI и источнике этих пакетов. Ниже показан листинг, в котором расшифрованы разделы отчета, выдаваемого утилитой addiag.

```
<Info> — отображает общую информацию
<TS> — отображает информацию о службах терминалов
<LocalApps> — отображает список локальных управляемых приложений
<ServerApps> — отображает список приложений, развернутых сервером
<MSIApps> — отображает список локальных приложений MSI
<GPOList> — отображает список локальных объектов групповой политики
<ScriptList> — отображает список сценариев локальных приложений
<ADHistory> — отображает историю локальных политик Active Directory
<MSIFeatures> — отображает список локальных возможностей MSI
<EventDump> — отображает события приложений для журнала
<Check> — отображает проверку целостности Active Directory
```

Рассмотрим пример отчета утилиты addiag:

```
Z:\Program Files\Support Tools>addiag /v

Microsoft (R) Software Installation Diagnostics. Version 1.00
Copyright (C) Microsoft Corp 1998-1999. All rights reserved.
Collecting info...
Initializing Remote DS Data...
Initializing Local AppMgmt Registry Data...
Initializing Local AppMgmt File Data...
Initializing Local Windows Installer Data...
Initializing Local Shell Data...
Initializing Local Event Data...

========================= General Info ==============================

User — NameSamCompatible: COMPANY\phxuser1
User — NameFullyQualifiedDN: CN=phxuser1,OU=Phoenix,DC=company,DC=com
User — Logon Server: \\SERVER1
User — SID: S-1-5-21-2000478354-746137067-1957994488-1117
User — Profile Type: LOCAL
User — Locale: 1033
Processor Architecture: x86
System Locale: 1033

========================= TS Info ========================

Not running TS

========================= Managed Apps (Local List) =================

No Managed applications were found.

========================= Managed Applications (Server)
=========================

User dump for COMPANY.COM
Dumping GPO list (1 items)...
        GPO GUID:{B672BEFE-7815-44C4-9F28-E482AEC2CBAD}
        Name:Distro1
               Administration Tools Pack
                  Object GUID:{D34A6C2A-5D4D-4005-85F6-CBDBB5136C57}
                  Package Flags:
                          Published
                          PostBeta3
```

```
                        UserInstall
                        OnDemandInstall
                        OrphanOnPolicyRemoval
                ProductCode:{5E076CF2-EFED-43A2-A623-13E0D62EC7E0}
                UI Level:Full.

======================== Windows Installer Apps ==================

Found 2 MSI application(s)
Easy CD Creator 5 Platinum
WebFldrs


======================== Local AD History ========================

Found 1 Applied GPO(s)in the history
Distro1
        GPO GUID:{B672BEFE-7815-44C4-9F28-E482AEC2CBAD}
        Version:0xf000f

======================== Application log events ====================

EventID:  1004
Type: WARN
Date: 20:32:41.0000 - 2/02/2002
User: N/A
Computer: PRO10
Source: MsiInstaller
Description: Product: Detection of product '{5E076CF2-EFED-43A2-A623
↳ -13E0D62EC7E0}',feature 'FeDNSConsole ',component
↳ '{455FE9A8-07D6-11D3-9C52-00A0C9F14522}' failed..
The resource 'D:\Windows \System32 \dnsmgmt.msc ' does not exist..
Data:.
```

Политики перенаправления каталогов

При сохранении файлов пользователем приложение обычно предлагает сохранение в принятом по умолчанию каталоге. Если приложение имеет логотип Windows 98, Windows 2000, Windows XP или Windows Server 2003, по умолчанию предлагается каталог My Documents (Мои документы). Такая стандартизация помогает управлять нагромождением файлов на рабочей станции пользователя, но дополнительных действий по копированию файлов на сервер для последующего резервного копирования и сканирования на предмет наличия вирусов не выполняется.

Это касается и других каталогов в профиле пользователя. Например, в каталоге Desktop (Рабочий стол) хранятся файлы и ярлыки, которые будут потеряны, если откажет локальный жесткий диск. В каталоге Application Data хранится информация о конфигурации программ, загруженных на рабочей станции, а также другие важные данные, например открытые ключи. Меню Start (Пуск) содержит ярлыки для всех приложений, установленных на компьютере.

Переместив критические компоненты Explorer, можно добиться централизации хранения и управления. Наиболее простая реализация предоставляется политиками перенаправления каталогов.

Политика перенаправления каталогов реализована в виде файла `Fdeploy.ini`, который указывает имя UNC ресурса, на котором должен находиться системный каталог. Расширение на стороне клиента `fde.dll` обрабатывает этот файл, внося изменения в разделы системного реестра, связанные с каталогами Explorer. При этом меняется пространство имен объектов, используемых Explorer и другими компонентами в операционной системе Windows.

С точки зрения пользователей, перенаправление оказывается совершенно незаметным. Единственный момент, когда пользователь может догадаться об удаленном хранении файлов, возникает при разрыве сетевого соединения. С этим часто сталкиваются пользователи портативных компьютеров. В этом случае стоит обратить внимание на автономные каталоги, в которых можно хранить локальные копии файлов из перенаправленных каталогов.

Политики сценариев

В классической операционной системе Windows NT предоставлялся только один способ доставки сценария пользователю. Сценарий размещался в сетевом каталоге `Netlogon` на каждом контроллере домена. После этого в профиле пользователя указывалась ссылка на этот сценарий. Предоставлялась возможность запуска только одного сценария, и сценарий не мог находиться в другом месте.

В современных операционных системах Windows ситуация со сценариями заметно изменилась. Политики сценариев позволяют запускать несколько сценариев из любого места. Кроме этого, предоставляется возможность запуска сценариев во время завершения сеанса пользователя и запуска сценариев при загрузке и завершении работы компьютера.

Операционная система все еще поддерживает классические сценарии для клиентов более старых версий. В Active Directory предоставляется атрибут объекта пользователя, в котором можно указать регистрационный сценарий. Клиенты более старых версий получают имя сценария при регистрации. Контроллер домена продолжает поддерживать ресурс `Netlogon` для хранения классических сценариев. Но расположение этого ресурса изменилось. В современных операционных системах Windows ресурс `Netlogon` связан с каталогом `\Windows\Sysvol\Sysvol\`*<имя_домена>*`\Scripts`. В классической операционной системе Windows NT для совместного доступа предоставляется каталог `\WINNT\System32\Repl\Import\Scripts`.

Классическая репликация сценариев

Все, что хранится в каталоге `Sysvol`, реплицируется на все контроллеры в пределах домена, и сценарии не являются исключением. Но если домен работает в режиме Windows 2000 Mixed и использует резервные контроллеры домена под управлением операционной системы Windows более старой версии, могут возникнуть проблемы.

В классической операционной системе Windows NT содержимое ресурса `Netlogon` синхронизировалось между контроллерами домена средствами службы LanMan Replication (LMRepl). Служба LMRepl реплицировала содержимое каталога `\WINNT\System32\Repl\Export` на основном контроллере домена в каталог `Import` на резервных контроллерах домена. Именно этот каталог предоставлялся для совместного доступа как ресурс `Netlogon`.

В операционной системе Windows Server 2003 служба LMRepl не поддерживается. Для синхронизации сценариев придется настроить классический резервный контроллер домена в качестве сервера экспорта LMRepl вместо основного контроллера домена. (В режиме Windows Mixed контроллер домена, которому предоставлена роль PDC Emulator, должен работать под управлением операционной системы Windows Server 2003.)

После этого необходимо использовать какой-либо метод копирования содержимого каталога `Scripts` с контроллера домена под управлением Windows Server 2003, выполняющего роль PDC Emulator, на классический резервный контроллер домена, который выступает в роли сервера экспорта. Можно воспользоваться Task Scheduler (Планировщик заданий) для запуска утилиты `xcopy`, одной из утилит массового копирования из состава Resource Kit или утилитой от стороннего производителя. Утилита `LMBridge` из состава Resource Kit успешно справляется с этой задачей.

Типы сценариев

Сценарии могут иметь любой формат, который может интерпретироваться клиентом. Это могут быть файлы пакетной обработки (`.bat`) или командные файлы (`.cmd`), а также сценарии на более сложных языках сценариев.

Операционные системы Windows Server 2003 и Windows XP поддерживают языки VBScript и JavaScript как часть стандартной инфраструктуры Windows Script Host (WSH). Кроме этого, можно использовать другие языки сценариев, например Perl и Python. Для этого на рабочих станциях необходимо установить соответствующие интерпретаторы команд. (Самые актуальные версии интерпретаторов ActivePerl и ActivePython предоставляются в виде пакетов MSI для обеспечения простой процедуры установки. Ознакомительные копии интерпретаторов команд доступны по адресу `www.activestate.com`.)

Язык VBScript и компьютерные вирусы

Известно, что многие компьютерные вирусы используют распространенную поддержку языка VBScript в операционной системе Windows для запуска вредоносного кода. Вирусы I-Love-You и AnnaKornikova являются примерами таких вредоносных программ. Если честно, то это уязвимое место не является неотъемлемым свойством языка VBScript. Если бы компания Microsoft приняла решение распространять вместе с операционной системой Windows интерпретатор ActivePerl, то вредоносный код писали бы на языке Perl.

В операционной системе Windows Server 2003 можно установить групповые политики, которые запрещают запускать вложения VBScript из сообщений электронной почты, но это не блокирует другие уязвимые места. Еще одним решением, предложенным Джейсоном Фоссеном (Jason Fossen) из компании SANS, является привязка расширения файлов `.vbs` к редактору Notepad (Блокнот) вместо механизма выполнения сценариев Cscript/Wscript.

В последнем случае все еще можно использовать язык VBScript для создания регистрационных сценариев. Для этого имя сценария необходимо указать в качестве параметра выполняемого файла Cscript. На рис. 12.20 показано, как это будет выглядеть в окне Edit Script (Изменить сценарий) редактора групповой политики.



Рис. 12.20. Окно Edit Script редактора GPE. Имя сценария VBScript указывается в качестве параметра приложения `Cscript.exe`

Развертывание сценариев

Политики сценариев состоят из двух компонентов.

- Файл `Script.ini`, в которомперечисляются сценарии и указывается их расположение для клиента.
- Собственно сценарий. Всегда храните сценарии в каталогах политик, чтобы они реплицировались на все контроллеры домена. Это предотвращает обращение клиентов через внешние соединения для загрузки необходимых сценариев.

Для развертывания сценариев необходимо создать файл `Script.ini` в редакторе групповых политик. Для этого откройте окно свойств интересующего сценария (рис. 12.21).

Возможность Show Files (Показать файлы) позволяет просмотреть файлы в каталоге `Scripts`. Это простой способ копирования сценариев в необходимый каталог политики. В противном случае пришлось бы просматривать каталог `Sysvol` и угадывать, какая из папок с именем в виде глобально уникального идентификатора соответствует обновляемой политике.

После размещения файла сценария в каталоге `Policies` воспользуйтесь кнопкой Add (Добавить), чтобы добавить сценарий в файл `Script.ini`.

Клиенты загружают файл `Script.ini` и передают его расширению на стороне клиента `Gptext`. После этого расширение загружает сам сценарий, который запускается под управлением соответствующего интерпретатора.

Если клиент загружает сценарии из различных объектов групповых политик, сценарии запускаются одновременно. По этой причине не стоит вставлять в один сценарий операции, которые зависят от операций в других сценариях.



Рис. 12.21. В окне Logon Properties отображается список выбранных сценариев

Кроме этого, пользователи получают доступ к рабочему столу, когда регистрационные сценарии еще выполняются. Это значит, что не стоит создавать ярлыки и параметры оболочки Explorer, которые зависят от действий регистрационных сценариев.

Многие организации используют многоуровневые регистрационные сценарии. Например, администраторы домена верхнего уровня могут создать сценарий, который устанавливает стандартные параметры настольного компьютера, например подключает сетевые диски и запускает стандартные приложения. Администраторы организационной единицы хотели бы дополнить такой регистрационный сценарий, но они не могут предполагать, что во время запуска их собственного регистрационного сценария уже подключены сетевые диски.

Чтобы использовать многоуровневые регистрационные сценарии или блокировать доступ к рабочему столу до завершения выполнения всех сценариев, необходимо настроить систему на синхронный запуск регистрационных сценариев (дополнительную информацию по этому вопросу можно получить в разделе “Синхронная обработка” ранее в этой главе.)

Консоль управления групповыми политиками

Консоль управления групповыми политиками (Group Policy Management Console — GPMC) является альтернативой механизму управления объектами групповых политик на основе контейнеров, который реализован на консоли Active Directory — Users and Computers (Active Directory — пользователи и компьютеры).

Консоль управления групповыми политиками предоставляет многие из возможностей программы Fazam2000 от компании Full Armor, например моделирование и резервное копирование политик. Кроме этого, устанавливается новый объект автоматизации, `Gpmgmt`, который предоставляет большое количество операций для использования в сценариях.

- Поиск объектов групповых политик
- Создание и удаление объектов групповых политик
- Резервное копирование и восстановление объектов групповых политик
- Импорт и экспорт
- Копирование объектов групповых политик
- Связывание объектов групповых политик с контейнерами
- Изменение фильтров WMI
- Делегирование прав доступа для объектов групповых политик
- Создание собственных отчетов для объектов групповых политик, включая результирующий набор политик

Компания Microsoft выпускает консоль управления групповыми политиками (GPMC) отдельно от операционной системы Windows Server 2003. Консоль может быть загружена с сайта Microsoft и установлена на любой компьютер под управлением операционной системы Windows Server 2003 или Windows XP SP1. Для установки консоли на операционную систему Windows XP требуется установка исправления (hotfix), предоставленного вместе с установочным пакетом.

В следующей главе

На этом этапе развертывания операционной системы Windows Server 2003 в пределах предприятия система способна принимать входящие соединения пользователей. Перед тем как распахивать двери, рассмотрим настройку хранилища данных, чтобы предоставить безопасный и надежный способ хранения пользовательских данных.