bhv

АЛЕКСАНДР КЕНИН

Практическое руководство системного администратора

2-е издание

- Задачи системного администратора
- Эксплуатация сети передачи данных
- Решения на основе технологий Windows и Linux
- Рекомендации по установке, настройке и оптимизации основных служб
- Секреты оптимальной и безопасной работы в Интернете
- Обеспечение работы мобильных пользователей
- Защита информации и отказоустойчивость
- Мониторинг информационных систем

СИСАДМИН
СИСТЕМНЫЙ АДМИНИСТРАТОР

Александр Кенин

Практическое руководство системного администратора

2-е издание

Санкт-Петербург
«БХВ-Петербург»
2013

УДК 004
ББК 32.973.26-018.2
К33

Кенин А. М.

К33 Практическое руководство системного администратора. — 2-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2013. — 544 с.: ил. — (Системный администратор)

ISBN 978-5-9775-0874-2

Практическое руководство к действию для системных администраторов, создающих и эксплуатирующих информационные системы офиса. Параллельно рассмотрены решения на основе технологий Windows и Linux. Приведены рекомендации по установке, настройке и оптимизации основных служб информационной системы, организации работы системного администратора, развертыванию операционных систем Windows и Linux (Ubuntu), программ корпоративной работы, мониторинга состояния серверов. Особое внимание уделено вопросам обеспечения безопасности и надежности. Даны конкретные советы по настройке основных сетевых служб, обеспечению распределенной работы в Интернете. Описана технология разрешения проблем в работе операционной системы и прикладных программ и их совместная тонкая настройка.

Второе издание доработано с учетом выхода новых версий ПО и появления новых технологий.

Для системных администраторов

УДК 004
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Екатерина Капалыгина*
Редактор	*Анна Кузьмина*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Марины Дамбиевой*

Подписано в печать 30.04.13.
Формат $70\times100^{1}/_{16}$. Печать офсетная. Усл. печ. л. 43,86.
Тираж 1500 экз. Заказ №
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Первая Академическая типография "Наука"
199034, Санкт-Петербург, 9 линия, 12/28

ISBN 978-5-9775-0874-2

Оглавление

Предисловие

Эта книга написана для всех тех, кто занимается эксплуатацией и развитием информационных систем. Вы держите в руках уже второе издание, которое существенно доработано и дополнено по отношению к предыдущим выпускам.

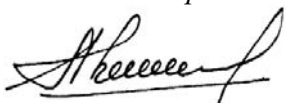
В каждой информационной системе есть компоненты, работа которых обеспечивает стабильность всех приложений. Администратору важно правильно настроить и сопровождать функционирование базовых служб. В этой книге мы рассмотрим вопросы, связанные с установкой, настройкой и обслуживанием системы передачи данных, базовых сетевых сервисов (DHCP, DNS и др.), систем обеспечения совместной работы пользователей (электронная почта, порталы) и контроля состояния информационной системы. Все то, с чем каждодневно приходится сталкиваться администратору. Учитывая, что современные информационные системы интегрируют как Windows-, так и Linux-компьютеры, я постарался привести параллельные рекомендации.

В силу ограниченности ресурсов сопровождением информационных систем в малых и средних организациях часто занимаются специалисты, вынужденные одновременно работать в нескольких структурах. Часто им просто не хватает времени, чтобы изучить функции того или иного продукта, иногда внедрение и поддержка нового функционала просто расценивается как излишняя, неоплачиваемая нагрузка. Поэтому я постарался показать, как те или иные возможности современного программного обеспечения позволяют обеспечить более комфортную работу.

Настоящая книга предназначена в помощь тем системным администраторам, которые хотят наиболее эффективно задействовать возможности современных технологий. В ней я постарался изложить практические рекомендации по администрированию информационных систем, уделяя основное внимание конкретным советам по настройке применяемых продуктов.

В информационных технологиях очень важен показатель удовлетворенности клиента. Также и автору хотелось бы получить ваши отзывы, замечания, предложения, которые могли бы улучшить эту книгу, сделать ее более полезной на практике. Их можно отправить на адрес издательства или мне по электронной почте на **kenin@hotbox.ru**.

Ваш Александр Кенин



ГЛАВА 1

Системный администратор

Не подлежит сомнению, что ведущая роль в управлении информационной системой принадлежит системным администраторам. При том, что в нашей стране часто не формализованы требования к этой профессии.

Квалификационные требования к системным администраторам

Каждая организация имеет свою уникальную информационную систему и предъявляет к соискателям на должность системного администратора различные требования. Тем не менее можно выделить некоторые типовые параметры.

Во-первых, информационные системы бывают различной сложности. Принято классифицировать их по размеру — по числу компьютеров. В малых организациях число компьютеров составляет не более 10—15 единиц, в больших — более сотни. Понятно, что уровень требований к системному администратору будет разным в случае большой или средней организации.

> ***Примечание***
>
> Критерии размеров организаций различны для реалий нашей страны и западных компаний. Обычно размер компании в нашей стране, определяемый по числу компьютерных систем, соответствует меньшему уровню западной фирмы. Это следует учитывать, например, оценивая рекомендации по выбору программного обеспечения и т. п.

Во-вторых, по степени подготовленности можно выделить несколько уровней системных администраторов.

Начинающий системный администратор

Обычно от такого специалиста требуется точное выполнение указаний руководителя (опытного администратора). Большей частью начинающему системному администратору поручается взаимодействие с конечными пользователями.

Поэтому требования к нему могут быть сформулированы так:

- умение взаимодействовать с пользователями;
- углубленное знание операционной системы рабочей станции (настройка прав пользователя, знание особенностей структуры домашних папок, умение вылечить систему от последствий вирусной атаки и аналогичные компетенции).

"Младший" системный администратор

Будем называть такого специалиста *младшим* администратором только для того, чтобы отличать его от начинающего системного администратора. В принципе, этот уровень соответствует начальной степени подготовки администратора, которую он может приобрести примерно за 2—3 года работы.

Такой администратор может сопровождать небольшую информационную систему либо работать в качестве помощника администратора крупной организации.

В дополнение к требованиям, изложенным для начинающего администратора, для этого уровня добавляются следующие критерии:

- понимание особенностей функционирования сетевой инфраструктуры (знание основ маршрутизации, умение добавлять станции в домен, предоставлять в пользование и подключаться к общим ресурсам, диагностировать сетевые проблемы и т. д.);
- фундаментальные знания операционной системы и практические навыки работы (обслуживание баз, разбиение дисков, создание и мониторинг логических массивов, резервное копирование и восстановление операционных систем и прикладного ПО и т. п.);
- умение составлять сценарии управления на одном из языков программирования.

Системный администратор

Этот "базовый" уровень должен соответствовать следующим требованиям:

- умение самостоятельно организовывать свой рабочий день;
- качественное сопровождение пользователей (умение общаться, решать проблемы и т. п.);
- умение проводить обучение сотрудников, готовить необходимые презентации;
- практический опыт настройки основных программных систем (почтовой системы, межсетевого экрана, параметров безопасности, различных вариантов разворачивания систем и т. п.);
- фундаментальное знание операционной системы;
- умение устранять сбои в работе системы (выявлять узкие места, производить отладку в случае необходимости, пользоваться снифферами и т. п.);
- умение составлять и отлаживать сценарии на основных языках. Умение модифицировать (приспосабливать) сценарии управления к потребностям собственной системы.

Опытный системный администратор

Администратор данного уровня должен:

- ❒ уметь общаться с сотрудниками, с представителями смежных организаций, с вендорами, уметь готовить презентации;
- ❒ быстро и полностью решать проблемы в информационной системе;
- ❒ уметь выделять задания, выполнение которых можно автоматизировать, и реализовывать соответствующие алгоритмы;
- ❒ глубоко понимать операционную систему и принципы сетевого взаимодействия;
- ❒ программировать на основных языках управления, иметь опыт составления собственных программ.

Опытный системный администратор должен уметь управлять сложной информационной системой (в том числе распределенной, с большим числом мобильных пользователей). Он должен быть способен выполнять роль технического руководителя для других системных администраторов, программистов и т. д.

Как правило, для такого специалиста требуется не менее чем 5-летний опыт работы в области системного администрирования.

Дополнительные требования

Вы не могли не заметить, что в качестве требований были указаны, в общем-то, общие характеристики, предъявляемые к должности. Понятно, что в каждой организации требования к вакансии системного администратора обычно конкретизируются по следующим позициям.

- ❒ **Знание конкретных операционных систем.** Это могут быть различные выпуски Windows, клоны Linux, операционные системы Oracle Solaris, HP AIX, Red Hat и пр., которые эксплуатируются в организации. Часто от претендентов при приеме на работу требуются только базовые навыки с последующей обязанностью досконального изучения в ходе эксплуатации.
- ❒ **Умение специального программирования.** Например, от администратора может потребоваться умение устранить ошибку (или отладить сценарий) в 1С.
- ❒ **Опыт сетевого администрирования.** Может потребоваться знание сетей Novell, умение настройки протоколов маршрутизации (OSPF, BGP и т. п.), наличие опыта работы с протоколом PPP и т. п.
- ❒ **Особые требования по информационной безопасности.** Например, настройка межсетевых экранов конкретных вендоров, умение разворачивать систему PKI, опыт настройки аутентификации по смарт-картам, знание основ шифрования данных и цифровой защиты документов и т. п.
- ❒ **Требования по умению документировать.** От администратора может потребоваться умение описывать информационную систему, составлять инструкции для пользователей и т. п.

- **Опыт работы с базами данных.** Часто от администратора требуются навыки администрирования баз данных (резервное копирование и восстановление данных, экспорт информации, управление пользователями, назначение прав, настройка параметров производительности и т. д.).
- **Знание оборудования.** Как правило, от администратора требуется знание оборудования (опыт работы с ним), которое эксплуатируется в конкретной организации (например, конкретной линейки серверов, источников аварийного питания, модемов, маршрутизаторов и т. д.).

Сертификация системных администраторов

Подтверждением профессионализма администратора являются *сертификаты*, которые он может получить от тех или иных организаций. Для получения сертификата обычно требуется сдача некоторого числа экзаменов и наличие опыта работы по данному направлению. Хотя формально опыт работы и не проверяется, но, не имея его, сдать экзамен достаточно сложно.

Сертификаты бывают различными. Имеются сертификаты от вендоров (Sun/Oracle, Red Hat, Microsoft, Hewlett-Packard и др.), от организаций (например, от сообщества системных администраторов — SAGE) и др.

Традиционно наличие сертификата рассматривается кадровыми службами как дополнительный аргумент в пользу соискателя. Хотя в последнее время — по данным анализа зарубежных организаций — большинство сертификатов начинает терять свою значимость для технических руководителей. Не в малой степени этому способствуют такие случаи, когда сертификат системного инженера одного из ведущих вендоров получают 13-летние подростки, подготовленные только к ответам на тестовые вопросы.

Планирование рабочего дня

Рабочее время администратора расходуется на три основные группы задач:

- анализ состояния информационной системы;
- реагирование на события системы и обращения пользователей;
- плановые работы (расширение сети, установка новых служб, обновление программных комплексов и т. п.).

Выделяйте время на перспективные проекты

Реализация проектов требует вдумчивости и сосредоточения. Оперативная работа отвлекает от проектов, поэтому необходимо найти способ выделить время на решение стратегических задач. Если функции системного администратора возложены на нескольких специалистов, то можно так распределить обязанности, что один администратор будет заниматься обслуживанием пользователей, а другой — работать над проектом. Потом можно поменяться функциями.

Если численность специалистов не позволяет выделить специалиста для проектов, то нужно постараться так организовать работу с обращениями, чтобы высвободить хотя бы несколько часов. Для этого можно, например, предусмотреть для системного администратора "творческое время", в течение которого его можно отвлекать только для решения критических проблем, а остальные обращения будут поставлены в очередь и т. п.

Периодически анализируйте распределение своего времени. Например, если вы заметите, что значительная часть времени расходуется на поддержание функционирующего оборудования, то не лучше ли выйти к руководству с предложением об обновлении, которое будет обосновано реальными цифрами расхода времени?

Работа с пользователями

По тому, как системный администратор общается с пользователями, во многом оценивается его работа со стороны, в том числе и руководителями предприятия. По решению проблем пользователя судят о работе администратора со стороны. Пользователь не может, например, знать, что в этот момент есть другие важные проблемы, также требующие срочного разрешения. Пользователь должен ощутить внимание со стороны администратора к своему вопросу и остаться уверенным в том, что для решения его проблемы будут "брошены все силы".

Ни в коем случае нельзя разговаривать с пользователем так, чтобы акцентировать внимание на его незнании компьютера и простейших операций. Кроме сиюминутного чувства вашего превосходства такой способ общения существенно усложнит взаимодействие и только затянет решение проблемы.

Обучение системного администратора

Основную часть информации системный администратор сегодня черпает из Интернета, на специализированных форумах, в онлайновой базе знаний. Однако не следует пренебрегать и традиционными формами обучения, которые часто проводятся как подготовка по тому или иному курсу вендора.

Такие очные формы обучения полезны тем, что дают более общий взгляд на продукт, позволяют ознакомиться со всеми функциями программного обеспечения, а не только с теми, которые используются на практике в данной организации. Кроме того, преподаватели часто рассказывают об особенностях продукта, ошибках и ограничениях, о которых не пишут в рекламных документах и не сообщают на бесплатных презентациях. На таких курсах традиционно развернуты полигоны, где можно протестировать различные возможности программного обеспечения или оборудования.

Конечно, такой курс будет и не лишним с точки наличия соответствующей строчки в резюме.

Реализация изменений в информационной системе

Информационная система не может быть застывшей. Изменения в нее вносятся как по результатам исправления ошибок, так и в процессе планового развития. Традиционно процесс изменений включает в себя:

- ❒ планирование изменений;
- ❒ тестирование (если возможно);
- ❒ их реализацию;
- ❒ работу с изменениями, сбор информации о поведении системы;
- ❒ анализ информации, поиск и устранение ошибок в случае нестабильной работы.

Планирование изменений

Идеальным случаем является ситуация, когда изменения в системе являются штатными: они планируются заранее, тестируются по возможности и только после этого внедряются.

Если изменения касаются большинства систем, то их можно охарактеризовать уже как *критические*, поскольку их реализация может существенно осложнить функционирование бизнес-процессов.

Весь процесс изменений должен тщательно протоколироваться: от составления плана до фиксации всех операций. Часто бывает, что в случае возникновения проблем в работе администраторы предпринимают различные шаги по исправлению ошибок. Если к успеху не приводят одни настройки, то осуществляют другие и т. д. Выполненные настройки по исправлению забываются, считается, что они не повлияли на работу; ищутся новые исправления. В результате через некоторое время уже невозможно определить, какие операции повлияли на результат, и не удается полностью отказаться от промежуточных настроек системы.

Поэтому надо взять за правило документировать каждый свой шаг: что сделано, почему, записать ссылки на использованные статьи базы знаний и т. п.

Другой важный совет: не менять сразу много за один раз. Лучше провести несколько операций изменения, чем совместить их все. Это может не только много раз сэкономить время администратора, но и когда-нибудь нарушить работу системы на длительный срок.

Конечно, план внедрения специфичен для каждой организации. Но можно отметить необходимость следующих позиций:

- ❒ организация тестирования изменений на полигоне (провести обновления и проверить корректность работы всей системы);
- ❒ подготовка плана отмены изменений;
- ❒ выбор времени для изменений;
- ❒ организация оповещения пользователей;
- ❒ отключение пользователей;

- ❒ осуществление обновлений;
- ❒ проверка корректности работы;
- ❒ подключение пользователей;
- ❒ проверка корректности работы;
- ❒ документирование проведенных операций, доработка шаблона плана внедрения изменений по выявленным проблемам.

Обратите внимание, что после внедрения изменений на следующий день администратор обязательно с самого утра должен быть доступен для пользователей, поскольку не исключена возможность выявления ошибок на этапе начала работы в системе. Кроме того, недоступность администратора в такой ситуации косвенно будет характеризовать его заинтересованность в успешном функционировании информационной системы.

Планирование момента изменений и продолжительности операций

Реализуемые изменения не должны помешать работе организации в случае возникновения проблем. В зависимости от критичности планируемых изменений время их внедрения может выбираться во время обеда, перед началом рабочего дня, в ночное время или выходные дни. При этом любые изменения системы должны быть исключены в периоды плановых отчетов, на время проведения (и подготовки) серьезных совещаний и т. п.

О планируемых изменениях пользователи должны быть предупреждены заблаговременно. Можно озвучить планируемые операции на совещаниях у руководителей подразделений, оповестить конечных пользователей по электронной почте и т. п. Не следует относиться к оформлению оповещений формально: например, если изменения проводятся часто, то сотрудники вряд ли будут читать сам текст письма, они обратят внимание только на его тему. Поэтому уже по ней должно быть понятно, кого коснутся изменения. А в самом тексте следует объяснять, зачем проводятся эти изменения и кого и как предупредить о возражениях (например, если у подразделения на этот период запланированы важные мероприятия).

Планируя внедрение изменений, обязательно нужно готовить планы откатов изменений. Следует учитывать, что ошибки могут быть замечены и через некоторое время. Например, если планируется внесение изменения в бухгалтерскую программу, то ошибки в формировании квартальных отчетов могут быть обнаружены в худшем случае через три месяца. И вам необходимо иметь возможность восстановить исходный вариант отчетов и внести в него все операции за эти три месяца.

Время на реализацию изменений должно быть запланировано (запрошено) с запасом и включать в себя не только время на непосредственное изменение, но и запас на откат в случае неудачи, некоторый период на анализ ситуации и т. п.

При оценке периода операции следует учесть все факторы. Например, если обновление требует перезагрузки сервера, то следует предусмотреть время для штатного закрытия программ, сохранения данных, для периода тестирования оборудования

при старте системы и т. п. Если обновление предполагается установить на все системы с последующей перезагрузкой, то должна быть учтена и последовательная очередность выключения и включения систем (сначала должны выключаться файловые серверы, в последнюю очередь — серверы аутентификации и оборудование, обеспечивающее подключение к другим сетям, включение следует выполнять в обратной последовательности). Возможны и другие ситуации, которые нужно учитывать. Например, включение системы хранения данных (СХД) с одновременной раскруткой большого количества жестких дисков приводит к большой нагрузке на источники питания. А это может вызвать просадку напряжения и, возможно, сбои в работе другого оборудования. Поэтому резонно выделить некоторый период времени на включение СХД, во время которого не включать никакого другого оборудования.

Системный администратор как продавец ИТ-технологий

Системный администратор не является лицом, распределяющим финансовые ресурсы. Обычно на предприятиях подобные решения принимаются ИТ-директорами, в подчинении у которых находятся системные администраторы. Объективно как финансовые руководители, так и ИТ-директора не разбираются в тонкостях информационной системы и часто основывают свои решения на советах тех людей, которым они доверяют, например, сына, любящего посещать компьютерные клубы, или друга, которого считают специалистом ИТ. Или, что еще хуже, с позиций поддержки фирм, в которых работают родственники и знакомые. Без реального представления проблем, которые решаются при работе информационных систем.

Системным администраторам нужно приспосабливаться к такой ситуации. Без поддержки финансовых руководителей, ИТ-директоров, без нахождения компромиссов развитие ИТ-структуры будет неоптимальным. Системные администраторы должны поддерживать руководителей, обучать их, чаще посвящать в свои проблемы. Пытаться донести проблемы до руководителя в понятных ему терминах.

Системное администрирование обычно рассматривается только с точки зрения расходования бюджета. Но в тот момент, когда руководитель начинает понимать эффективность своих решений на практике и может оценить экономический эффект от работы системного администратора, а это происходит в случае ухудшения показателей основного бизнеса из-за проблем с работой инфраструктуры, служб и т. п., работа системных администраторов уже развалена, и службу приходится воссоздавать заново.

Чтобы не доводить информационную систему до критических показателей, системному администратору надо становиться *продавцом информационных технологий*. Он должен искать аргументы для обоснования выделения средств на поддержание и развитие системы. Желательно при этом опираться на независимые цифры. Например, на стоимость внешних контрактов, на количество обращений, зафикси-

рованных службой поддержки, на планы роста числа пользователей, отраженные в бизнес-планах предприятия, и т. д. Для этого нужно знать и свою статистику (например, количество предотвращенных сетевых атак), и тенденции в мире, решения у конкурентов... Если говорить коротко, то нужно показать, что конкретное вложение средств в ИТ-структуру отвечает *интересам руководителя*.

На практике используются два варианта финансирования: централизованное (содержание группы администраторов) и финансирование за счет отдельных проектов. Каждый вариант имеет свои преимущества и недостатки, но в любом случае требуются тщательно проработанные уровни обслуживания и контроль качества (чтобы при лучшем обслуживании группе системных администраторов выделялось больше средств, а руководители бизнеса в случае дополнительного финансирования могли ожидать улучшения качества обслуживания).

Учитывать человеческие особенности

Деятельность администратора по управлению системой не должна ухудшать комфортность работы пользователей. Поверьте, что через некоторое время пользователи все равно найдут способ, как обойти введенные администратором ограничения. А поскольку такие обходные пути менее безопасны и потенциально более рискованны, то они могут привести и к более серьезным отказам. Формально нарушение в таких случаях будет сделано самими пользователями, но первопричиной его фактически явится ваша политика.

Поэтому лучше так регулировать правила и ограничения, чтобы обеспечить необходимый уровень безопасности и надежности без существенных изменений принятой практики (если, конечно, такое возможно).

Быть в курсе

Системный администратор (руководитель группы администраторов) не должен замыкаться в проблемах информационной системы. Он должен знать приоритеты бизнеса и соответствующим образом планировать свою работу, в том числе заранее вносить предложения по изменению структуры (по созданию новых рабочих мест, в части организации работы сотрудников на дому, подключения филиалов и т. п.). Должны быть налажены отношения со специалистами юридической и кадровой служб предприятия.

Следует выделять время на участие в конференциях и семинарах. Обязательно подписаться на различные специализированные рассылки. И, естественно, не забывать и о самообразовании.

И не заблуждайтесь, считая, что все знают, например, о ваших планах модернизации информационной системы. Или о планируемых настройках. Чаще рассказывайте людям о своих намерениях, пытайтесь сделать пользователей своими сторонниками. Ну а если не можете перебороть себя, то хотя бы публикуйте минимальный объем информации на корпоративном сайте.

Ошибки администратора

От ошибок никто не застрахован. Не нужно скрывать их, как и не стоит наказывать подчиненных администраторов за неверные действия. Жестко придерживайтесь только одного правила: о возникновении проблемы должны быть оперативно проинформированы заинтересованные лица.

Чаще советуйтесь. Мнение собеседника, даже если он не является специалистом по данной проблеме, может подтолкнуть вас к решению совершенно с неожиданной стороны.

Старайтесь фиксировать все свои действия по настройке системы и соответствующие указания начальников. Если сомневаетесь в чем-то (например, в каком-то указании начальника), попытайтесь получить письменное подтверждение (по электронной почте и т. п.).

Инструкции и контрольные листы

Инструкции позволяют описать последовательность выполнения операций (например, по установке операционной системы в конфигурации конкретного отдела) и добиться идентичности результатов работы для различных специалистов. Удобно, если инструкции будут снабжены контрольными листами (обычно их принято называть *check*-листами), в которых будут последовательно перечислены все необходимые шаги. После изучения инструкции даже не совсем опытному администратору для выполнения операций достаточно будет только использовать контрольные листы, чтобы не пропустить какой-либо важный шаг в настройке системы.

Кроме того, заполненный контрольный лист является хорошим вариантом отчетности о выполненной работе. Особенно использование контрольных листов важно при выполнении серьезных изменений. Сам факт наличия контрольного листа уже будет свидетельствовать о том, что к предстоящим операциям была проведена серьезная подготовка.

Полномочия системного администратора

Фиксация полномочий и обязанностей системного администратора поможет снять многие претензии и оговорить условия выполнения специальных работ.

Так, желательно зафиксировать в соответствующих документах следующие параметры:

- четко определить обязанности, например, указать, что администраторы не поддерживают чужое ПО, самостоятельно установленное пользователем;
- распределить обязанности (если поддержку системы выполняют несколько специалистов): кто отвечает за установку ПО, кто решает проблемы сети, кто поддерживает пользователей данного подразделения и т. п.;
- определить особенности поддержки мобильных пользователей, работ на выставках, организуемых предприятием, и т. п.;

- ❒ зафиксировать временные рамки: в какое время можно обращаться пользователям, кто осуществляет поддержку после окончания рабочего времени и в выходные дни;
- ❒ выделить временные диапазоны на решение проблем (понятно, что длительность решения будет зависеть от категории проблемы, серьезности сбоя). Обязательно письменно определить экстренную ситуацию, при возникновении которой администратор имеет право самостоятельно прервать работы над некритичными проблемами;
- ❒ должны быть описаны процессы действий по инциденту (какая информация и как должна быть собрана, к кому обратиться, например, для вскрытия помещения в выходной день, как и в какие сроки проблема должна быть эскалирована, если ее не удается решить собственными силами).

Если в организации внедряется новая система

Если руководство внедряет новую информационную систему, то администратор обязан не только содействовать этому процессу, но и фактически принять на себя руководство всеми проблемами интеграции нового продукта:

- ❒ оценить простоту продукта, достаточность его функциональности (при этом и не должно быть избыточности);
- ❒ оценить открытость кода: что сделано специально для организации, передан ли этот код вам, уточнить права на него, возможность доработки кода, если организация откажется от услуг поставщика (или он прекратит существование, как часто это бывает);
- ❒ оценить процессы: что надо дополнительно сделать в уже существующем процессе, как, надо ли докупать лицензии и т. д.;
- ❒ определить, как будет организована связь с поставщиком, как он будет реагировать на ошибки, на просьбы доработки (кто и как должен сообщать об ошибках, в какие сроки должны быть проведены доработки, на каких условиях и т. п.);
- ❒ установить, как будет взаимодействовать новый продукт с существующей системой аутентификации и авторизации;
- ❒ оценить, как будет загружена сеть после его внедрения;
- ❒ установить, какие службы системы будут использованы или необходимо их установить дополнительно;
- ❒ если будет работать межсетевой экран, то поддерживают ли установленные в организации версии соответствующие протоколы;
- ❒ уточнить, использует ли продукт собственные протоколы (например, свой протокол поверх HTTP) — это усложнит настройку;
- ❒ разобраться, как будут протоколироваться операции, как можно подключить журналирование системы к существующей системе мониторинга;
- ❒ понять, работает ли продукт (есть ли его версии) под теми версиями операционных систем, которые изучены и используются на предприятии;

- оценить расходы на обучение: нужно ли готовить дополнительно специалистов поддержки;
- выяснить надежность продукта и его перспективы: как долго существует решение, какова надежность поставщика (не исчезнет ли);
- дополните существующие инструкции и правила, внесите в них, например, периодические проверки конфигурации нового проекта.

Особенности организации рабочего места администратора

Оснащенность рабочего места системного администратора существенно зависит от специфики выполняемых работ. Мы все же попытаемся кратко описать наиболее общие требования к оснащению рабочего места системного администратора.

- **Персональный компьютер.** Комплектация персонального компьютера системного администратора должна быть лучше типовой конфигурации компьютеров организации. Во-первых, его желательно оснастить двумя мониторами, чтобы администратор мог одновременно держать под контролем много информации. Во-вторых, системный блок должен позволять запускать (в качестве виртуальных машин) как аналоги эксплуатируемых систем, так и программное обеспечение, только планируемое к размещению. Это налагает ограничения на тип материнской платы (64 бит, возможно, наличие EFI и т. д.), на процессор (состав поддерживаемых функций виртуализации, параметры производительности и т. д.), объем памяти (достаточность для запуска в виртуальной среде нескольких серверов), на интерфейсы (возможность чтения карт памяти различных форматов) и т. д.
- **Ноутбук.** Это, в первую очередь, инструмент для настройки оборудования. Поэтому особых требований к его производительности не предъявляется, главное, чтобы аккумулятор находился в рабочем состоянии (мог обеспечить автономную работу не менее чем на 1—1,5 часа) и чтобы в ноутбуке присутствовали необходимые интерфейсы. Это COM-порт (требуется для настройки оборудования; различные переходники USB—COM на практике на части оборудования работают, на другой — нет), Wi-Fi-адаптер (для подключения к беспроводной сети внутри предприятия), 3G-модем или другое средство беспроводного подключения к Интернету (для оперативного доступа к базам знаний, обновлениям и т. п.).

  Обычно на ноутбук следует поставить сниффер, клиент SSH/Telnet, возможно, TFTP-сервер (для сохранения и загрузки конфигураций и прошивок активного оборудования).
- **Сменные носители информации.** Во-первых, нужно иметь флешку, позволяющую разместить на ней загрузочный (установочный) образ системы. Как правило, объем такого устройства должен быть 4 Гбайт и более. Конечно, лучше

подготовить несколько флеш-карт (для различных операционных систем), но можно обойтись и одной.

Во-вторых, нужен сменный жесткий диск (если потребуется установить программное обеспечение на автономный компьютер или скопировать с такой системы данные). В продаже они сейчас представлены USB-устройствами объемом 300 Гбайт и более, такого объема достаточно для текущего обслуживания систем.

- **Средства связи.** Системный администратор всегда должен быть на связи. Хорошо, если его телефон оснащен фотокамерой, которая может понадобиться, например, чтобы сфотографировать наклейки оборудования (не переписывать серийные номера в полевых условиях) или зафиксировать состояние устройств (их повреждения и т. п.).

  У администратора должны быть "под рукой" прямые контакты руководителей предприятия, лиц, ответственных за режим предприятия, и т. п., которыми ему, возможно, придется воспользоваться в особых ситуациях.

- **Инструменты.** Лучше, конечно, приобрести специализированный комплект инструментов, но начать можно со шлицевых и крестообразных отверток различных размеров, обжимных щипцов для RJ11/RJ45-разъемов, плоскогубцев, кусачек. По мере приобретения оборудования комплект инструментов будет пополняться специализированными ключами, поставляемыми производителями вместе с устройствами.

- **Приборы.** Обязательно приобретите кабельный тестер, хотя бы самого стартового уровня. Неплохо иметь универсальный тестер (для замеров напряжения, сопротивления).

- **Запасные части.** У администратора должен быть комплект различных деталей для оперативной замены в случае неисправности. В том числе:

  - несколько силовых кабелей (для подключения в розетку 220 В и для подключения к аварийному источнику питания);
  - несколько патч-кордов различной длины (в том числе и оптические со всеми вариантами сочетаний используемых типов разъемов, если в организации есть оптические каналы связи);
  - Ethernet-кабель (витая пара) длиной около 50—100 м и разъемы RJ45 (RJ11) — для организации временных подключений оборудования;
  - несколько клавиатур, мышей, сетевых карт;
  - самые ненадежные узлы компьютеров: блоки питания, жесткие диски (соответствующие по параметрам, используемым в организации);
  - набор различного крепежа (часто можно скомплектовать из запасных частей, поставляемых вместе с оборудованием, шкафами и т. п.).

- **Библиотека.** Во-первых, системный администратор постоянно нуждается в получении новых знаний. Чем больше литературы он изучает (как в электронном виде, так и в бумажном), тем легче ему справиться с обязанностями.

Во-вторых, в библиотеке должна быть представлена документация с описанием информационной системы (проекты, схемы сети, результаты тестирования, данные о ремонтах, спецификации оборудования с серийными номерами и т. п.).

В-третьих, администратор должен иметь копии организационно-распорядительных документов, на базе которых он должен строить свою деятельность. Это и различные положения (о коммерческой тайне на предприятии, матрица прав доступа и т. д.), инструкции (инструкция пользователя, инструкция по парольной защите и др.), регламенты (проведения технического обслуживания серверов, резервного копирования и т. д.) и т. п.

Для хранения и предоставления документов удобнее использовать ресурсы вебсервера (порталы). Существует много бесплатных шаблонов, которые помогут организовать, например, собственный Wiki-ресурс. Только на сайте WikiMatrix (**http://www.wikimatrix.org/**) представлено для сравнения по функционалу почти полторы сотни Wiki-продуктов, большая часть из которых бесплатна для использования. Размещение на общедоступных ресурсах подробных руководств по основным операциям (например, как удаленно подключиться к ресурсам организации или оформить документы на командировку) помогут существенно снизить нагрузку на администратора.

- **Аптечка.** Если к аптечке предприятия у администратора нет доступа в любой момент времени (например, она недоступна в выходные дни), то на его рабочем месте должен быть представлен минимальный комплект медицинских средств (перевязочные средства, основные лекарства и т. п.), которым, не дай Бог, придется воспользоваться во время обслуживания или восстановления системы.

Программное оснащение рабочего места администратора

Системному администратору необходимо иметь ряд программных инструментов, помогающих в управлении информационной системой. Понятно, что выбор их индивидуален, а мы только попытаемся частично проиллюстрировать возможные варианты.

Загрузочный диск

Загрузочный диск позволяет получить доступ к данным неработающего компьютера, выполнить тестирование и ремонт, восстановить работу операционной системы.

Существуют различные сборки подобных дисков, которые несложно найти в Интернете или в сетях провайдеров. Типовой состав такого диска включает в себя:

- утилиты управления (восстановления) таблицами разбиения дисков;
- утилиты восстановления данных с диска;
- редакторы реестра Windows (в оффлайн-режиме);
- средства сброса пароля администратора системы;

- ❒ сетевые утилиты (обеспечивающие возможность выполнения сетевых операций копирования);
- ❒ средства проверки наличия вирусов, руткитов и т. п.;
- ❒ другие утилиты, например, средства записи на CD и т. д.

Комплект переносных утилит

Администратору периодически приходится сталкиваться с обслуживанием автономного компьютера. Например, у которого не функционирует подключение к сети или расположенного за пределами предприятия. В таких случаях поможет комплект утилит, сохраненный на сменный носитель.

На такой носитель необходимо, во-первых, установить *переносные приложения*. Переносными приложениями (portable application) называются программы, которые не производят изменений в системе при установке (не изменяют реестр, не производят запись в папки Program Files, Windows и т. д.) и не создают никаких файлов на дисках (кроме папки своего размещения).

В Интернете легко можно найти желаемые программы, разработанные для переносного использования. Существует специальная оболочка, облегчающая поиск, загрузку и управления такими программами. Она доступна к бесплатной загрузке с сайта **http://portableapps.com**. На этом же сайте можно найти и подборку бесплатных переносных программ.

После загрузки программы ее необходимо установить на сменное устройство. Запущенная программа помещает свой значок в область уведомлений (системный трей). В его меню — запуск переносных программ, опции их установки (в том числе возможность загрузки с сайта программы) и т. д. (рис. 1.1).

Принято добавлять в конец имени установочного пакета переносной программы символы *paf*. Если вы видите в названии файла такие символы, то установку его желательно запускать из-под данной оболочки. В таком случае программа будет автоматически установлена в папку сменного носителя и появится в списке программ. Конечно, можно установить приложение в любую папку и запускать его из нее выбором исполняемого файла, но использовать оболочку намного удобнее.

Переносные программы широко представлены в Сети. Их можно загружать не только с указанного сайта, но и с таких популярных ресурсов, как Cnet (**http://download.cnet.com/3055-18512_4-75182000.html**), Portable4pro (**http://portable4pro.ru/**) и др. Практически любую типовую задачу можно решить, имея подобранный набор переносных программ. На рис. 1.2 представлено окно переносной программы очистки диска, с помощью которой был проведен поиск файлов дампов памяти системы с последующей очисткой.

Во-вторых, на сменный носитель следует записать сценарии, которые вы используете при управлении системой.

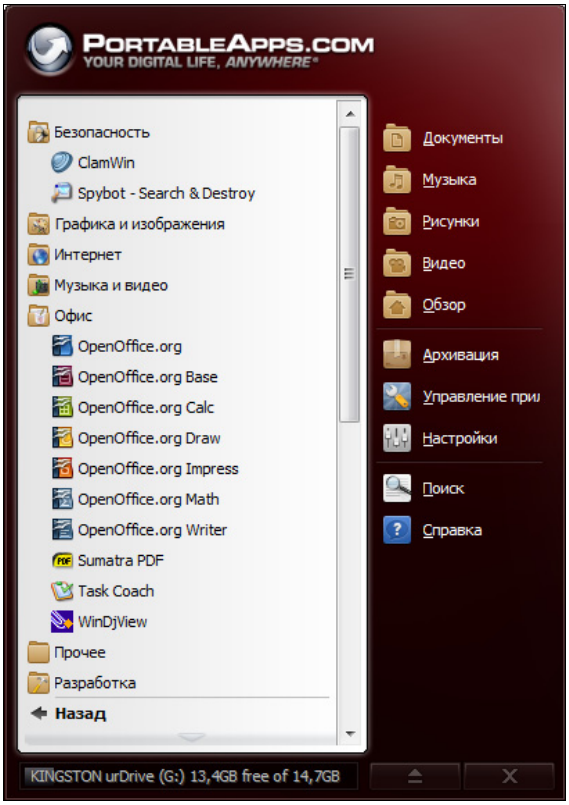


Рис. 1.1. Оболочка управления переносными программами

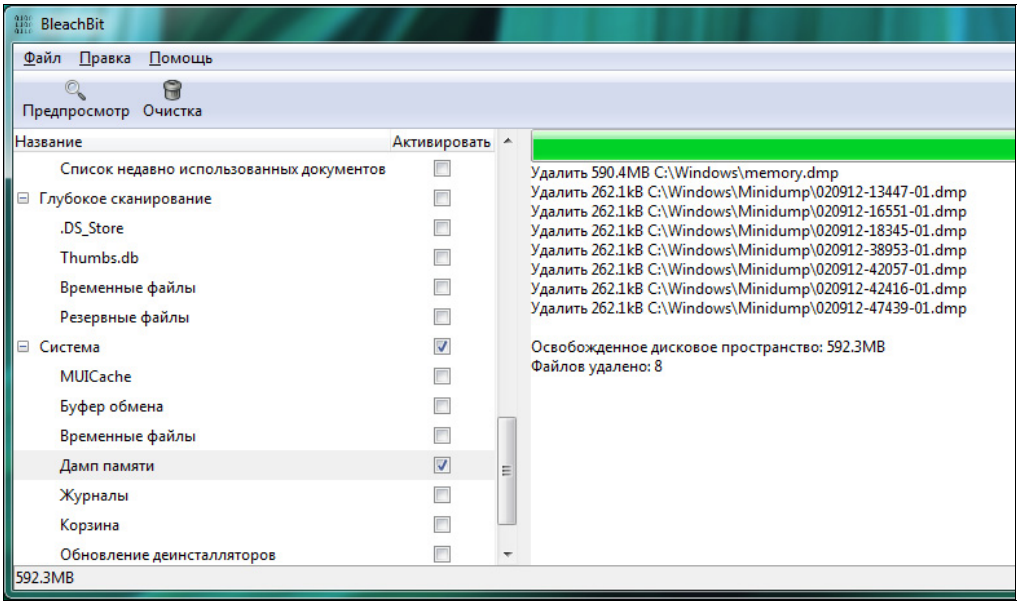


Рис. 1.2. Окно переносной программы очистки диска

Отдельные утилиты

Cain&Abel

Вообще-то данное средство предназначено для сбора и дешифрования паролей, но знакомство с ним полезно в целях создания собственного представления о качестве программ, используемых в целях взлома.

Nmap

Свободно распространяемая утилита Nmap (**http://nmap.org/**) предназначена для исследования безопасности сети, но ее с успехом можно применять для обнаружения устройств в локальной сети, проверки функционирования служб (межсетевого экрана, сетевых служб), опроса состояния систем и т. п. В Windows-варианте программа поставляется вместе с графическим интерфейсом — Zenmap, позволяющим настраивать запуск проверки и отображать результаты работы в удобном виде, просматривать данные отдельных систем, фильтровать хосты и т. п. (рис. 1.3).

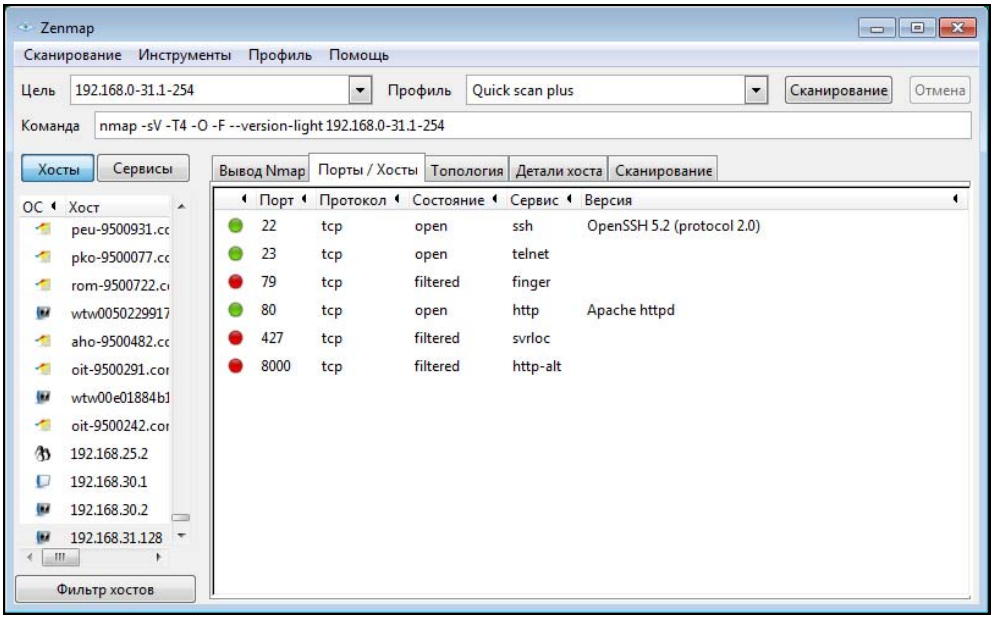


Рис. 1.3. Окно оболочки Zenmap

Результаты работы программа сохраняет в XML-файле, для обработки которого удобно использовать сценарий PowerShell — Parse-Nmap.ps1, доступный к загрузке со страницы **http://www.sans.org/windows-security/downloads/** (сценарий также доступен из репозитория по ссылке **http://poshcode.org/1179**). Сценарий формирует из отчета список хостов, который можно фильтровать по отдельным параметрам, используя возможности PowerShell. Например, чтобы найти в сети работающие веб-службы, достаточно выполнить следующую команду:

```
parse-nmap.ps1 <файл отчета nmap> | where {($_.Ports -match "open: TCP:80")} |
ft hostname, ipv4
```

(Команда выведет на экран имена компьютеров, у которых открыты порты веб-сервера, и их IP-адреса.)

> ***Примечание***
>
> Следует учитывать, что хотя сканирование портов не запрещено стандартами Интернета, но программы защиты хоста часто детектируют этот процесс компьютера как атаку на систему.

Сниффер

Администратор должен уметь анализировать сетевой трафик. Существуют бесплатные анализаторы сетевого трафика, функциональности которых достаточно для проверки сети организации. Наиболее известен пакет Wireshark (**http://www.wireshark.org/**). Программа доступна для загрузки в различных версиях, в том числе есть и portable-сборка.

На рис. 1.4 показано окно программы в режиме сбора пакетов. Программа снабжена простым анализатором, который может собрать поток пакетов (например, восстановить звонок IP-телефонии или отобразить связанные пакеты). В большинстве случаев возможностей программы более чем достаточно для анализа.

Программа для мониторинга сети из состава Windows (Network Monitor), которую можно бесплатно загрузить с сайта разработчика, также позволяет перехватывать пакеты, передаваемые по сети, но лично автору кажется менее удобной, чем Wireshark. С особенностями использования Network Monitor можно при желании познакомиться в блоге **http://blogs.technet.com/netmon**.

> ***Примечание***
>
> Отметим такую особенность Network Monitor, как возможность перехватывать трафик виртуальной частной сети системы и туннелей за счет подключения к соответствующим интерфейсам Windows.

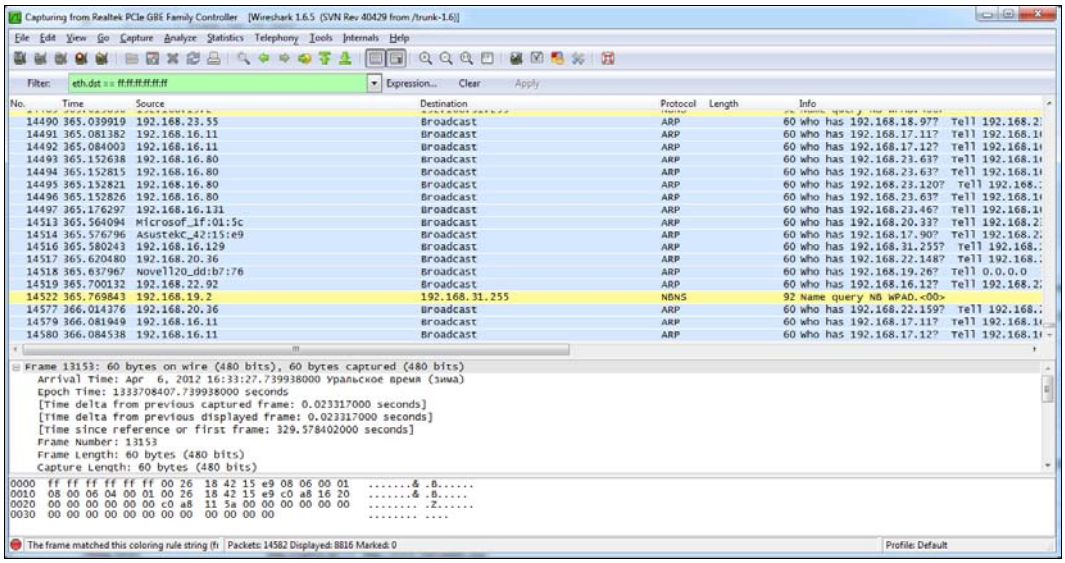


Рис. 1.4. Окно программы Wireshark (с активной фильтрацией отображения)

JXplorer

Администратору приходится часто работать с данными из службы каталогов. Поэтому инструмент, позволяющий выполнить поиск по структуре каталога, скопировать целиком дерево каталога, поддерживающий последние стандарты и т. п., крайне необходим. Одним из наиболее функциональных бесплатных продуктов является JXplorer (**http://jxplorer.org/**) — рис. 1.5.

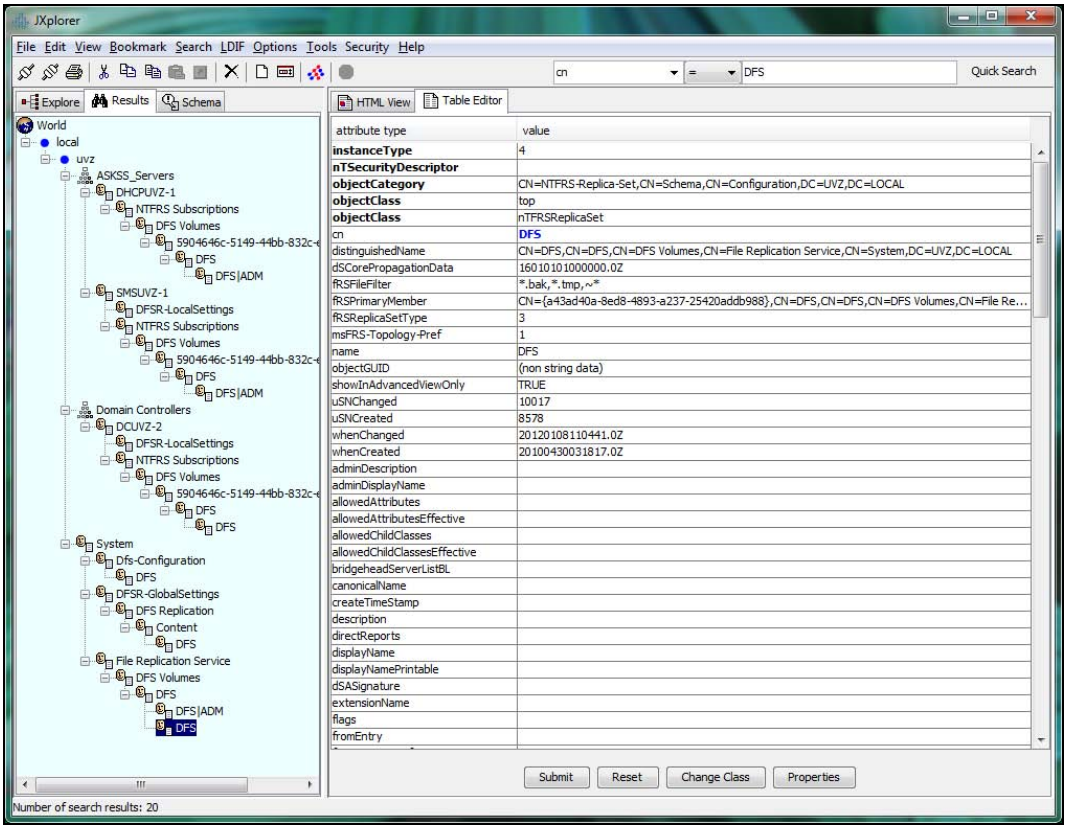


Рис. 1.5. Программа JXplorer (отображены результаты поиска по каталогу)

Friendly Pinger

Программу Friendly Pinger (**http://www.kilievich.com/rus/fpinger/**) мы упомянем за простоту и функциональность. Она позволяет в реальном режиме времени отображать сведения о том, какие компьютеры включены, а какие — нет, оповещать администраторов в случае остановки сервисов, проводить инвентаризацию оборудования и программного обеспечения, отображать активность на компьютере (кем открыты файлы) и т. п.

Эта программа является хорошим стартом для контроля небольшой сети, который может быть осуществлен без значительных усилий.

Утилиты от Sysinternals

По адресу **http://www.sysinternals.com/** (компания вошла в состав Microsoft и эти утилиты стали частью технической библиотеки — **http://technet.microsoft.com/ru-ru/sysinternals**) находится список нескольких бесплатных утилит, весьма необходимых администратору.

Прежде всего, отметим утилиту FileMon (**http://technet.microsoft.com/ru-ru/sysinternals/bb896642**), которая позволяет отследить все файловые операции, совершаемые в системе. Утилита показывает, какие файлы создаются в системе, какие программы и к каким файлам обращаются за чтением данных или для их записи, успешны ли эти операции или завершены с ошибкой.

Аналогичная утилита следит за любыми обращениями к реестру системы и помогает узнать, какая программа и как запрашивает информацию. Существует программа, отображающая все запущенные в системе процессы с указанием их иерархии. А утилита DiskView (**http://technet.microsoft.com/ru-ru/sysinternals/bb896650**) позволяет увидеть, какой сектор занят заданным файлом (удобно для получения информации о поврежденном файле в случае появления сбойных секторов).

В состав продуктов компании Sysinternals входят утилиты мониторинга системы, инструменты анализа безопасности ресурсов, программы настройки ресурсов компьютера и т. п. Список утилит достаточно велик, поэтому просто порекомендую посетить упомянутый сайт и загрузить необходимые программы.

Некоторые административные утилиты

В завершение упомянем несколько утилит, предназначенных для администрирования организации. Это коммерческие продукты. Обычно из их функциональности администраторы используют возможности подключения к удаленному рабочему столу и создания базы инвентаризации оборудования и программного обеспечения.

- **DameWare NT Utilities.** Комплект утилит (**http://www.dameware.ru/**), предназначенных для управления объектами службы каталогов. Позволяет управлять на удаленных системах различными ресурсами (службами, процессами, реестром, принтерами и т. д.). Включает средство наблюдения за рабочим столом.
- **Ideal Administrator.** Еще один набор утилит (**www.pointdev.com**), весьма любимых системными администраторами. Включает множество функций, весьма прост в использовании.
- **Hyena.** Популярный пакет (**http://www.systemtools.com/hyena/index.html**) для каждодневного администрирования Windows-систем.

ГЛАВА 2

Готовим компьютер к эксплуатации

После появления нового компьютера перед системным администратором встает задача ввода его в эксплуатацию. В зависимости от целей приобретения системы — под новую задачу, в качестве дополнительного типового рабочего места или взамен вышедшей из строя системы — возможны различные варианты подготовки компьютера, часть из которых мы попытаемся описать в этой главе.

Паспорт компьютера

Одно из главных требований при вводе в эксплуатацию новой системы — наличие на нее паспорта. Неважно, в какой форме будут храниться данные — в электронном ли виде или на бумаге, на бланке или просто написанные от руки, главное, чтобы конфигурация компьютера была описана, а вы и другие администраторы, которые будут работать после вас, знали, каковы параметры настройки компонентов системы, какие версии драйверов установлены.

Если даже вы настроили оборудование просто с установками по умолчанию, то отметьте и этот факт. Чтобы специалист, которому, например, через два года придется восстанавливать вышедший из строя RAID-массив, знал, что был выбран тип 5 с размером сектора в 64 Кбайт, а не какая-либо иная конфигурация. Поверьте, подобная информация очень дорого стоит для обслуживающего персонала.

Типовая информация о конфигурации системы должна содержать параметры, перечисленные в табл. 2.1.

Таблица 2.1. *Параметры паспорта оборудования*

№	Название	Описание
1	Назначение	Описание назначения системы, например, сервер баз данных отдела 123
2	Host name	DNS-имя системы
3	Отдел	В каком подразделении установлена система
4	Изготовитель	Изготовитель оборудования, например, Hewlett-Packard, Oracle и т. д.

Таблица 2.1 *(окончание)*

№	Название	Описание
5	Модель	Модель оборудования, например, HP ProLiant DL580 G7
6	Статус	Состояние оборудования: эксплуатируется, на складе и готово к эксплуатации, для списания, только для полигона и т. д.
7	Категория оборудования	Например, сервер, рабочая станция, аппаратный межсетевой экран, коммутатор, точка беспроводного доступа и т. д.
8	Серийный номер	Серийный номер от производителя
9	Part Number	Номер по каталогу изготовителя. Необходим при поиске, например, совместимых элементов и т. д.
10	Service TAG	Гарантийный номер. Часто указывается дополнительно к серийному номеру. Нужен в случаях обращения в службу технической поддержки
11	Учетный номер на предприятии	Номер, который присвоен оборудованию в учетных документах предприятия
12	Находится...	Необходимо указать точное место расположения. Это может быть комната, номер шкафа, номер позиции в шкафе и т. д. (зависит от конкретного типа оборудования и особенностей предприятия)
13	IP-адрес	IP-адрес устройства (если несколько адресов, то указать все, в том числе адрес out-of-band-управления)
14	Сетевые карты	В случае наличия нескольких сетевых карт нужно перечислить их все и указать соответствующие параметры
15	Порты коммутатора	Указать порты коммутатора, в которые подключена каждая сетевая карта
16	Чем контролируется	Например, мониторится в Nagios
17	Системы хранения	Указать подключения к СХД предприятия по FC или iSCSI (если есть): к каким системам, номера LUN и т. д. Указать количество и тип встроенных жестких дисков
18	Операционная система	Указать тип и версию операционной системы. Например, Windows Server 2008 R2 или Ubuntu 11.10
19	Дата начала гарантии	Указать дату
20	Дата окончания гарантии	Параметр указан отдельным полем для удобства работы в случае, если гарантия продлевалась дополнительными соглашениями
21	Дата запуска в эксплуатацию	Указать дату
22	Дополнительная информация	Зависит от оборудования. Например, если это веб-сервер, то может быть указан его внешний IP-адрес, адреса сайтов, которые размещены на нем, и т. д.

Установка операционной системы

Для большинства вновь приобретенных серверов администратору необходимо выполнить на них установку программного обеспечения. Споры о выборе операционной системы, что лучше — Windows или Linux, постепенно уходят в прошлое. Реальная информационная система включает в себя как Linux-серверы, так и Windows-системы, беря от них лучшие черты: надежность и производительность Linux, знание интерфейса Windows и т. д. Системный администратор должен уметь управлять любой операционной системой.

Live-версии операционных систем

Операционную систему не всегда нужно устанавливать на жесткий диск. Широко распространены так называемые Live-версии (например, LiveCD и т. п.), представляющие собой полнофункциональные системы, не требующие установки и запускаемые со сменных носителей.

Такие версии позволяют, во-первых, выполнять некоторую работу (например, многие версии Linux-систем комплектуются программами офиса), а во-вторых, познакомиться со средой до ее установки на компьютер.

Live-версии Windows

Windows не предназначена[1] для запуска с CD или другого сменного носителя. Тем не менее, существуют различные неофициальные сборки, которые легко найти в Интернете (см., например, **http://www.trickspedia.com/tips/how-to-run-windows-xp-from-a-usb-stick/**) и применить на практике.

Так, упомянутая ранее сборка "весит" всего 58 Мбайт и может быть установлена на флешку объемом от 256 Мбайт. Все инструкции, как выполнить разворачивание данного образа, можно найти в файле загрузки.

Понятно, что в таких объемах возможности операционной системы существенно урезаны, но вполне могут быть достаточными в конкретных ситуациях. Еще раз повторим, что такие сборки не являются официальными.

> ***Примечание***
>
> Live-сборки Windows характеризуются отказом от ряда компонентов и такой настройкой системы, при которой отпадает необходимость в виртуальной памяти и до минимума снижается потребность в операциях ввода-вывода на носитель. Кроме того, обычно загрузчик Windows заменяется загрузчиком от Linux, который обеспечивает более стабильную работу.

[1] Объявлено, что корпоративная версия Windows 8 будет включать возможность работы со сменного носителя с подключением к корпоративному профилю.

Live-версии Linux-систем

Live-версии Linux-систем официально подготавливаются соответствующими разработчиками. В большинстве случаев сами дистрибутивы Linux уже являются LiveCD.

В состав Live-версий входит не только собственно операционная система, но и ряд прикладных программ (офис, браузеры Интернета, медиапроигрыватели и т. п.). Такая версия может как использоваться в работе без установки на компьютер (единственное неудобство состоит в меньшей скорости работы нежели с нежестких дисков), так и с нее можно развернуть данную операционную систему на жесткий диск компьютера.

Для создания LiveCD достаточно загрузить файл его образа и записать на болванку при помощи любой соответствующей программы. Чтобы создать загрузочную флешку, можно использовать одну из многочисленных программ, например рекомендуемый разработчиками Ubuntu инсталлятор, который доступен по ссылке **http://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/**.

Установка Windows

В зависимости от объемов установки новых систем администратор может воспользоваться различными способами оптимизации своей работы.

Автоматизация установки

Windows 7/Server 2008, как и предыдущие версии, можно установить в автоматическом режиме, когда все ответы на запросы мастера установки подготовлены и сохранены заранее. Честно говоря, использовать данный вариант установки имеет смысл только при большом объеме операций.

Для подготовки автоматического развертывания нужно установить на имеющуюся систему пакет Windows Automated Installation Kit (AIK), который бесплатно доступен с сайта разработчика. Пакет объемный (суммарный объем загрузки порядка полутора гигабайт). Собственно файл ответов создается компонентом этого пакета — диспетчером установки Windows (Windows SIM). Вам нужно запустить эту программу и правильно указать соответствующие опции установки.

Основное назначение WAIK — это создание индивидуальных образов установки, которые будут включать только те компоненты, которые необходимы в вашей организации. В том числе и прикладные программы. К сожалению, WAIK достаточно трудоемок в настройке и требует специальной подготовки администратора. Кроме того, он мало подходит для работы с предыдущими версиями Windows. Поэтому на практике более распространен вариант клонирования систем через дублирование жесткого диска с использованием продуктов третьих фирм. Интересующихся читателей мы отошлем к оригинальному документу разработчика — "Пошаговому руководству построения стандартного образа Windows 7" (**http://technet.microsoft.com/ru-ru/library/ee523217%28v=ws.10%29.aspx**).

Установка с USB-носителя

Традиционный способ установки операционной системы с CD/DVD-диска не всегда удобен. Во-первых, скорость чтения с USB-носителей существенно выше, поэтому операции могут быть выполнены быстрее. Во-вторых, часть устройств просто не имеет соответствующих дисководов (нетбуки и т. д.). А вариант установки по сети обычно используется только в крупных организациях, поскольку требует наличия подготовленной инфраструктуры и администраторов.

Для разворачивания системы с USB необходимо, во-первых, чтобы компьютер мог загружаться с USB, во-вторых, подготовить загрузочный флеш-диск.

В Windows 7 подготовить загрузочный флеш-диск можно встроенными командами, однако только для установки ОС той же разрядности (например, на компьютерах *x*64 — только для установки 64-разрядной операционной системы). Поэтому целесообразнее воспользоваться специализированными утилитами.

Как всегда, доступны различные средства. Например, для подготовки дисков для Windows 7/8 можно загрузить утилиту от Microsoft — Windows 7 USB/DVD tool (**http://www.microsoftstore.com/store/msstore/html/pbPage.Help_Win7_usbdvd_dwnTool**). С ее помощью можно подготавливать диски как на системах с Windows 7/8, так и на компьютерах Windows XP. Правда, для использования ее на Windows XP требуется наличие некоторых компонентов (они описаны на странице загрузки).

Также можно использовать программу UltraISO (это коммерческий продукт, но нужная опция доступна в триальной версии). Для подготовки загрузочного флеш-диска в этой программе нужно открыть образ диска и выполнить команду **Самозагрузка | Записать образ жесткого диска** (рис. 2.1).

При этом необходимо выбрать вариант метода записи **USB-HDD+** (выделено на рисунке).

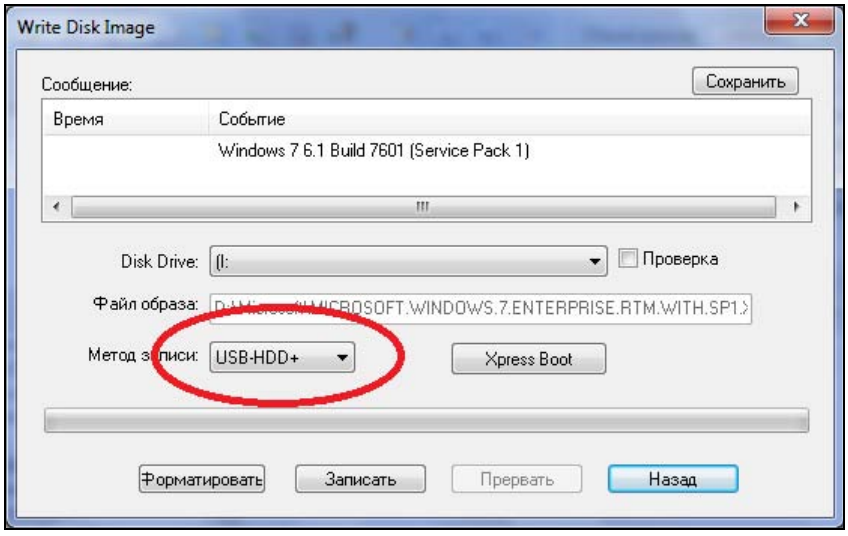


Рис. 2.1. Подготовка загрузочного флеш-диска

В Интернете легко можно найти и другие специализированные утилиты, например WinToFlash (**http://wintoflash.com/**). Преимущество их состоит в том, что они позволяют сделать загрузочный диск Windows не только для Windows 7/8, но и для Windows XP (вариант, официально не поддерживаемый).

После подготовки загрузочного носителя необходимо включить в BIOS поддержку загрузки с USB-устройств, поставить его первым в списке загрузки и выполнить установку операционной системы.

Режим Windows Core

Для повышения надежности работы сервера Microsoft подготовила специальный вариант установки — режим Core, в котором отсутствуют некоторые компоненты операционной системы. За счет этого уменьшаются возможности атак на такую систему, снижается количество необнаруженных ошибок и т. п.

Режим Core — это не полнофункциональный сервер Windows. В этом режиме, например, не могут быть реализованы все роли. Список доступных ролей таков:

- Active Directory (AD);
- Active Directory Certificate Services;
- Active Directory Lightweight Directory Services (AD LDS);
- DHCP Server;
- DNS Server;
- File Services;
- Hyper-V;
- Print Services;
- Streaming Media Services;
- Web Server (IIS).

После установки в режиме Core необходимые операции управления можно производить как в графическом интерфейсе (вариант псевдографики показан на рис. 2.2, это окно настройки вызывается командой `sconfig`), при помощи удаленного управления стандартными утилитами Windows (для этого сначала необходимо разрешить удаленное управление) или с использованием сценариев PowerShell.

При помощи команды `sconfig` выполняются базовые настройки: задаются сетевые параметры, регулируется членство сервера в домене или рабочей группе, разрешается удаленное управление и т. п. Не все настройки доступны через данную утилиту. Например, часто необходимо настроить параметры межсетевого экрана для обеспечения доступа к серверу. Сделать это придется командой `netsh`. Так, для разрешения удаленного подключения к серверу следует выполнить команду

```
netsh advfirewall set currentprofile settings remotemanagement enable
```

Примечание

В режиме Core по умолчанию при включенном контроле учетных записей пользователей может выполняться установка только тех программ, которые не требуют админи-

стративных полномочий. В противном случае вы получите сообщение об ошибке. Для устранения этой проблемы в ключе

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` установите значение параметра `EnableLUA` в 0.

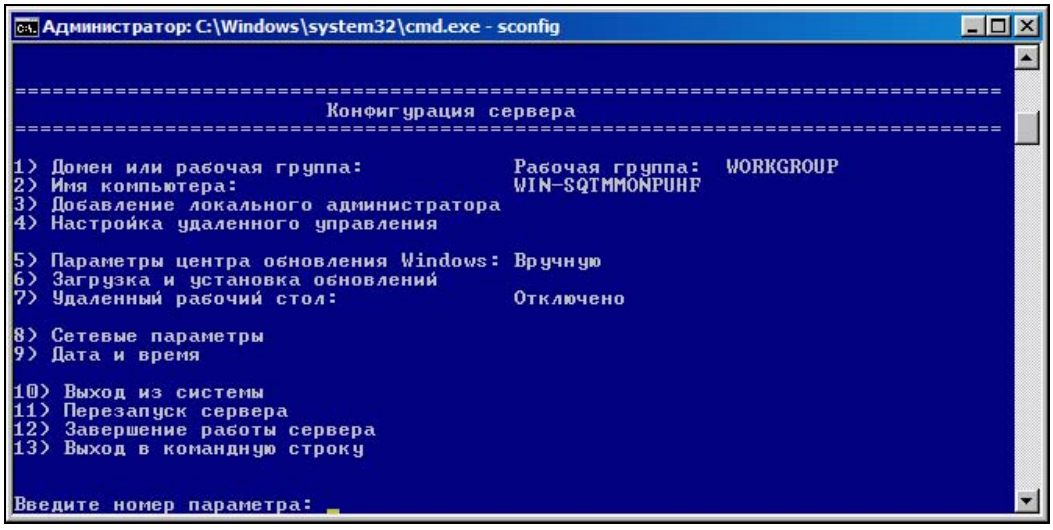


Рис. 2.2. Псевдографический режим управления Core

Для облегчения административных функций можно найти много свободно распространяемых утилит, реализующих возможности управления серверов в графическом режиме. Например, Core Configurator (**http://coreconfig.codeplex.com/releases/view/36678**), Core Configurator от Smart-X (**http://www.smart-x.com/downloads/**), Visual Core Configurator (**http://ctxadmtools.musumeci.com.ar/VisualCore2008/VisualCore11_on_R2.html**) и др.

В качестве примера рассмотрим Core Configurator 2.0. Эта бесплатная программа (а точнее, набор PowerShell-сценариев) позволяет выполнить следующие операции:

- активировать продукт;
- настроить сетевые параметры, в том числе параметры прокси-сервера, параметры межсетевого экрана;
- вызвать операцию подключения к домену;
- настроить параметры iSCSI;
- настроить роли и компоненты сервера, разрешить удаленное управление сервером;
- настроить права пользователей и групп;
- управлять общим доступом к ресурсам сервера;
- управлять службами, устанавливать и удалять программы

и т. п.

На рис. 2.3 показан пример одного из интерфейсов настроек, выполненный в традиционном Windows-стиле.

Продукт доступен как в виде ISO-образа для использования в виртуальных средах, так и ZIP-файла, который можно скопировать на физический сервер с помощью USB-носителя.

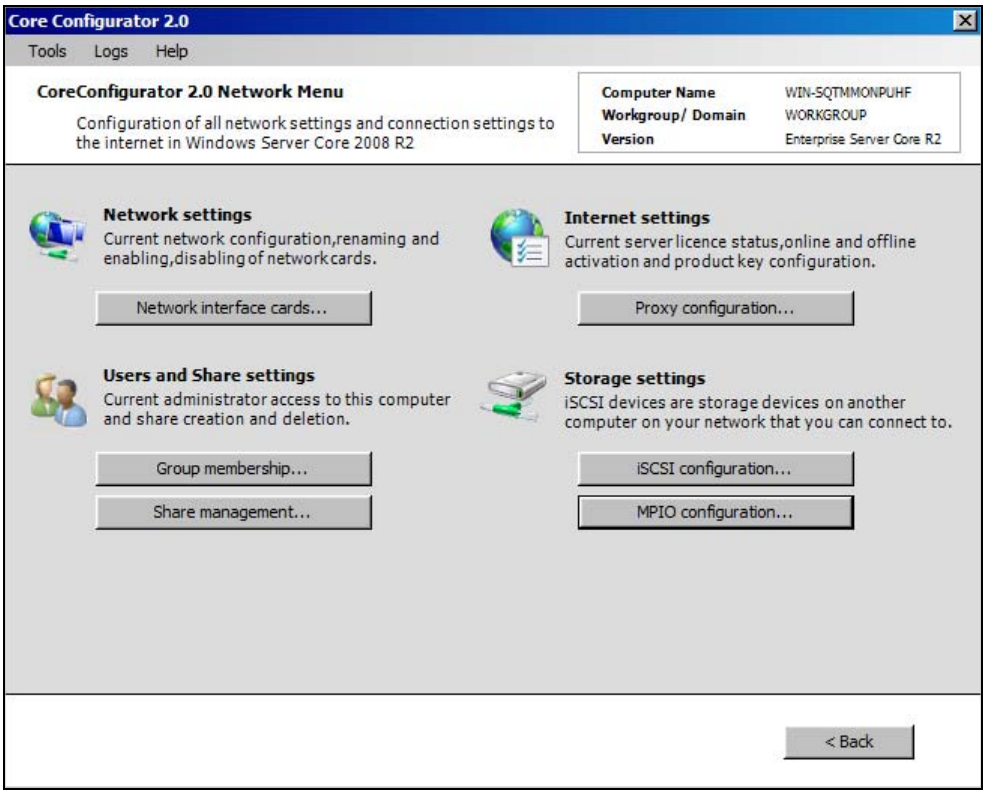


Рис. 2.3. Программа Core Configurator 2.0

Для использования данной программы необходимо включить компонент Microsoft PowerShell, который по умолчанию отключен. Сделать это можно разными способами, например, командами `ocsetup` (`start /w ocsetup` *компонент*) или DISM (`DISM /Online /Enable-Feature /FeatureName:`*название*). Лично мне больше нравится второй вариант, поскольку он сопровождается более подробной информацией по результатам работы команды.

Чтобы включить PowerShell, необходимо сначала активизировать его родительский компонент (NetFx2-ServerCore), а потом и его самого следующими командами:

```
DISM /Online /Enable-Feature /FeatureName: NetFx2-ServerCore
DISM /Online /Enable-Feature /FeatureName: MicrosoftWindowsPowerShell
```

После чего запуск утилиты управления можно осуществить вызовом сценария Start_Coreconfig.wsf.

Установка Linux-систем

Существует несколько клонов Linux, которые активно развиваются. В качестве примера в данном издании мы будем использовать Ubuntu — популярный клон на основе Debian, который поддерживается многими вендорами. Причем существует как бесплатная гарантированная на длительный срок поддержка (выпуск обновлений), так и возможность заключения контракта на коммерческое обслуживание системы.

Установка Ubuntu начинается с загрузки с компакт-диска дистрибутива. Все операции выполняются по шагам, под руководством мастера операций. Так что никаких сложностей данный процесс не вызывает. Длительность установки обычно в несколько раз меньше соответствующих операций в случае Windows-сервера.

На первом этапе установки следует выбрать русский язык, после чего практически все диалоги программы не потребуют знания английского (рис. 2.4).

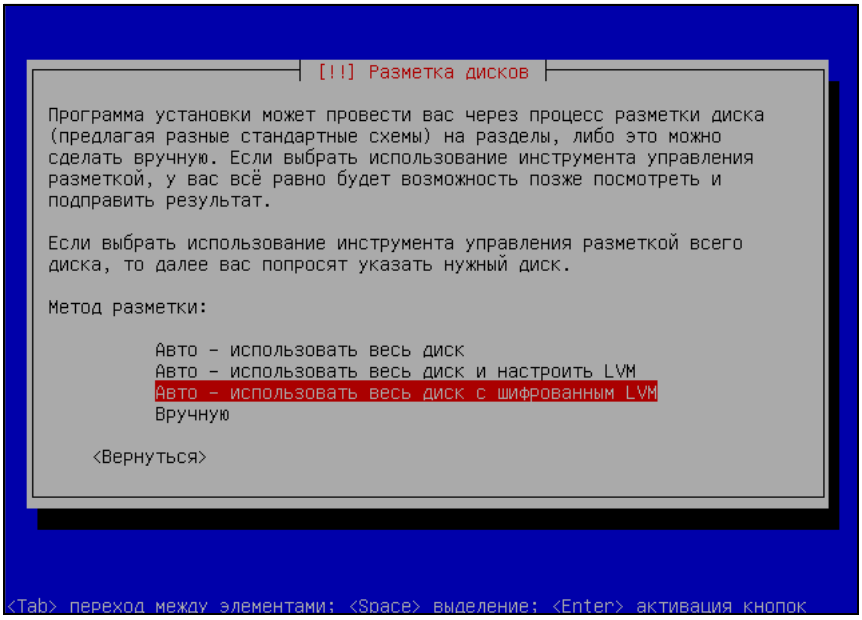


Рис. 2.4. Один из экранов установки Ubuntu

На определенном этапе мастер установки попросит определить список устанавливаемого прикладного программного обеспечения. Состав устанавливаемых программ обычно выбирается исходя из будущих задач сервера. Но в любом случае следует установить пакет SSH для обеспечения удаленного доступа к серверу. Даже если вы не выберете никакой программы, то после установки сервера соответствующий компонент легко добавить как путем индивидуальной установки, так и запуском программы установки комплектов ПО (запускается командой `tasksel`).

После установки сервера желательно выполнить несколько дополнительных настроек.

Настройка локализованной консоли

Несмотря на выбор русского языка в опциях программы, после установки консоль неверно отображает русские символы. Для исправления достаточно выполнить переконфигурацию консоли при помощи команды:

```
sudo dpkg-reconfigure console-setup
```

На первые запросы программы следует согласиться с предложениями по умолчанию (если вы только не хотите выбрать иные сочетания клавиш переключения) и дойти до запроса о выборе поддерживаемых наборов символов. Этот запрос выводится следующим после запроса варианта раскладки, который хорошо "читается", поскольку отображен латинскими символами (по умолчанию выбран вариант UTF-8). В окне поддерживаемых наборов символов следует перейти на строчку, в которой есть сочетания KOI-8R и KOI8-U. Далее выберите любой вариант шрифта (Terminus, VGA и т. д. через запрос программы, на который нужно просто нажать кнопку **OK**) и завершите настройку консоли.

Настройка сетевых параметров

Если во время установки программного обеспечения сервера последний был подключен к сети с работающей службой DHCP, то параметры сетевого интерфейса останутся настроенными на автоматический режим. Это не лучший вариант для сервера.

Назначение параметров сетевого интерфейса осуществляется в файле конфигурации, который расположен по пути /etc/network/interfaces с последующим указанием параметров DNS-сервера в файле /etc/resolv.conf.

Для редактирования можно воспользоваться программами vi, nano или другими — в зависимости от личных предпочтений. Откройте файл конфигурации сетевого интерфейса, например, так:

```
sudo vi /etc/network/interfaces
```

Найдите блок параметров (начинается со строки `# The primary network interface`) и замените строки после `auto eth0` (начинаются с `iface eth0 inet dhcp`) текстом листинга 2.1 (естественно, указав свои значения настроек).

Листинг 2.1

```
iface eth0 inet static
address 192.168.0.2
netmask 255.255.255.0
network 192.168.0.0
broadcast 192.168.0.255
gateway 192.168.0.1
```

Откройте файл resolv.conf (например, `sudo vi /etc/resolv.conf`) и внесите изменения в параметры сервера DNS. Содержимое файла должно выглядеть примерно следующим образом:

```
search суффикс
nameserver ip_адрес
nameserver ip_адрес
```

Где *суффикс* — суффикс, который будет добавляться к имени системы при поиске полного DNS-имени (FDQN), а *ip_адрес* — IP-адреса серверов DNS.

Проверьте содержимое файла /etc/hosts. Для нормальной работы почтовой системы и других служб необходимо, чтобы он включал в себя как полное доменное имя системы, так и краткое.

Чтобы внесенные изменения вступили в силу, перезапустите сеть командой

```
sudo /etc/init.d/networking restart
```

В завершение проверьте действующие параметры сетевого интерфейса командой

```
ifconfig -a
```

Примерный текст команды иллюстрирует листинг 2.2. Обратите внимание, что для настраиваемого интерфейса в его свойствах должны отображаться состояния UP и RUNNING.

Листинг 2.2

```
ubuntu:~$ ifconfig –a
ethl Link encap: Ethernet HWaddr 00:0c:29:14:4d: d5
inet addr:192.168.0.2 Bcast:192.168.0.255 Mask:255.255.252
inet6 addr: fe80::20c:29ff: fel4:4dd5/64 Scope: Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1438 errors:0 dropped:0 overruns:0 frame:0
TX packets:461 errors:0 dropped:0 overruns:© carrier:0
collisions:0 txqueuelen:1000
RX bytes:168370 (168.3 KB) TX bytes:84826 (84.8 KB)
Interrupt:18 Base address:0x2000
lo Link encap: Local Loopback
inet addr:127.0.0.1 Nask:255.0.0.0
inet6 addr:::1/128 Scope: Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:54 errors:0 dropped:0 overruns:0 frame:0
TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23153 (23.1 KB) TX bytes:23153 (23.1 KB)
```

Настройка синхронизации времени

При использовании строгих технологий аутентификации существенно точное значение текущего времени систем. В процессе установки Ubuntu производится первичная синхронизация времени компьютера с одним из серверов Интернета. Поскольку спешка или отставание локальных часов компьютера неизбежны, следует настроить систему на автоматическую синхронизацию.

Самый простой способ решения заключается в настройке автоматического ежедневного исполнения команды синхронизации времени. Для этого в папке /etc/cron.daily/ создайте файл, например, с именем ntpdate, который должен содержать следующую строку:

```
ntpdate 1.ru.pool.ntp.org
```

Не забудьте, что этот файл должен быть исполняемым, поэтому дайте разрешения на его исполнение:

```
sudo chmod +x /etc/cron.daily/ntpdate
```

Файл /etc/cron.daily/ntpdate будет ежедневно исполняться планировщиком системы. При этом будет запускаться команда синхронизации времени `ntpdate`, которой в качестве параметра передается имя сервера времени (**1.ru.pool.ntp.org**). **1.ru.pool.ntp.org** — это имя сервера (можно указать также серверы **2.ru.pool.ntp.org**, **3.ru.pool.ntp.org** и т. д.) в проекте виртуальных кластеров серверов времени (**http://www.pool.ntp.org/**). Данный проект обеспечивает предоставление IP-адреса реально работающего сервера времени. Этот IP-адрес может случайным образом меняться в зависимости от проверки работоспособности участвующих в проекте серверов времени.

Многовариантная загрузка

Под многовариантной загрузкой понимается установка на один компьютер нескольких операционных систем, выбор которых происходит при включении системы.

Потребность в наличии на компьютере одновременно нескольких операционных систем существенно снизилась с развитием технологий виртуализации, но не исключена полностью. Например, необходимость во второй операционной системе может быть оправдана желанием использовать оборудование, которое не поддерживается по тем или иным причинам в "основной" ОС.

Требования к сосуществованию двух ОС

Для установки второй ОС на компьютере должен существовать раздел (логический диск), на который предполагается выполнить установку. Этот раздел не должен совпадать с тем, на котором находится существующая операционная система, а его размер — соответствовать требованиям для установки (например, не менее 10 Гбайт при установке Ubuntu в качестве второй ОС).

Сжатие существующего раздела

В большинстве компьютеров на всем жестком диске обычно создан только один[1] логический диск. В этом случае для создания нового раздела необходимо сначала *сжать* существующий.

---

[1] В современных системах часто имеется раздел *восстановления* (System Restore), являющийся загрузочным и хранящий информацию для восстановления системы в первоначальное состояние. Размер этого раздела (обычно порядка 100 Мбайт) не позволяет использовать его для установки второй ОС, поэтому необходимость сжатия раздела для освобождения места для установки сохраняется.

Сжатие раздела может быть произведено штатными средствами Windows 7/Server 2008 или при помощи утилит третьих фирм в случае добавления новой ОС к Windows XP. При сжатии диска данные, содержащиеся на нем, сохраняются.

Возможность сжатия раздела Windows включена в установку Linux-систем. Вам нужно просто выбрать вариант установки новой ОС параллельно с существующей установкой Windows, и мастер операций предложит выполнить необходимые шаги по созданию раздела для установки новой системы.

> ***Примечание***
>
> До начала операции сжатия раздела настоятельно рекомендуем провести дефрагментацию диска и проверку его на отсутствие ошибок (командой `chkdsk`). Кроме того, настоятельно советуем выполнить резервное копирование данных, особенно если вы не являетесь опытным пользователем, способным справиться с неожиданно возникшей проблемой.

Для сжатия раздела в Windows 7/Server 2008 откройте консоль управления компьютером и перейдите к опции управления дисками. Отметьте тот диск, который вы хотите сжать, и выберите из его контекстного меню пункт **Сжать том** (рис. 2.5).

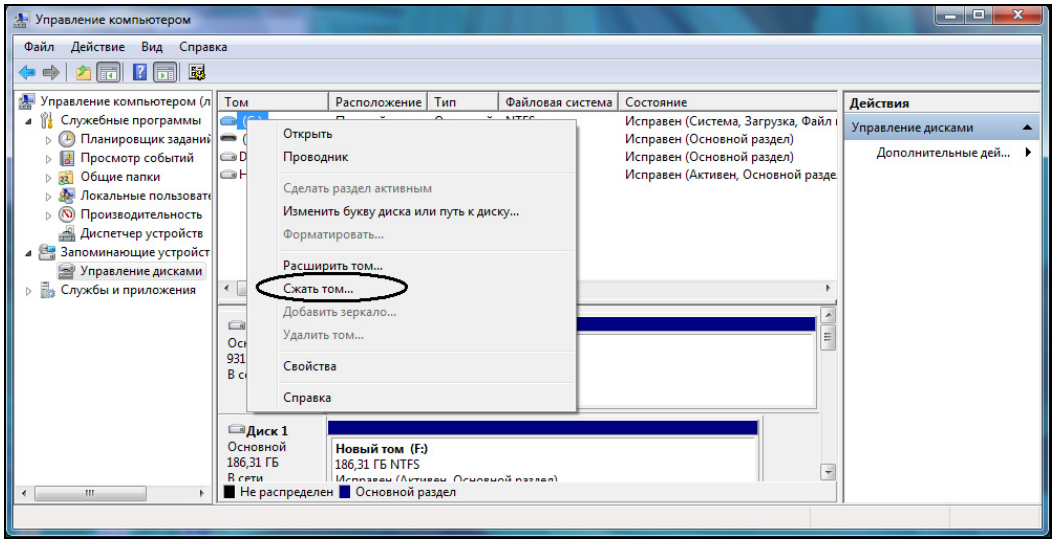


Рис. 2.5. Опция **Сжать том...** в разделе **Управление дисками**

После этого программа начнет подсчет пространства, которое может быть высвобождено на диске. Этот процесс может выполняться достаточно длительное время, после чего будет предложен вариант сжатия с максимальным высвобождением пространства (рис. 2.6).

Как правило, следует уменьшить размер сжимаемого пространства, чтобы сохранить возможность работы в текущей операционной системе. Достаточно указать в качестве параметра операции такой размер, чтобы на этом месте можно было установить новую ОС. Если доступного для сжатия пространства не хватает, то необходимо вручную провести очистку диска и полную дефрагментацию.

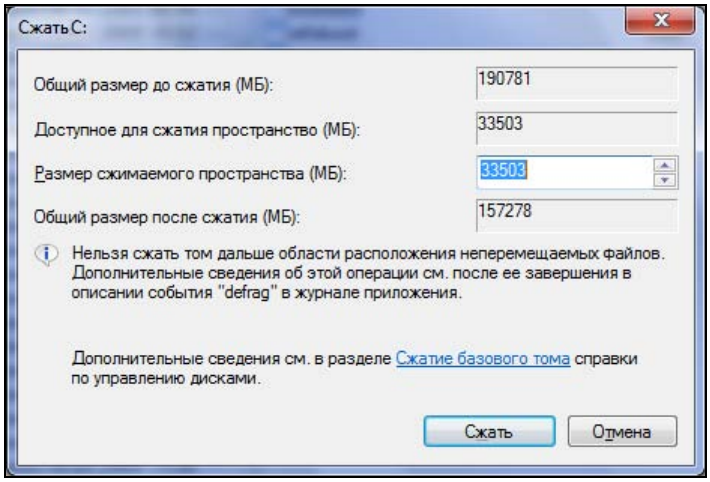


Рис. 2.6. Параметры операции сжатия раздела

Примечание

Если на диске есть свободное место, но программа отказывается сжимать раздел, то это свидетельствует о "неудачном" расположении неперемещаемых файлов. В таком случае помочь могут утилиты дефрагментации диска, имеющие возможность оффлайнового (при перезагрузке системы) перемещения специальных файлов.

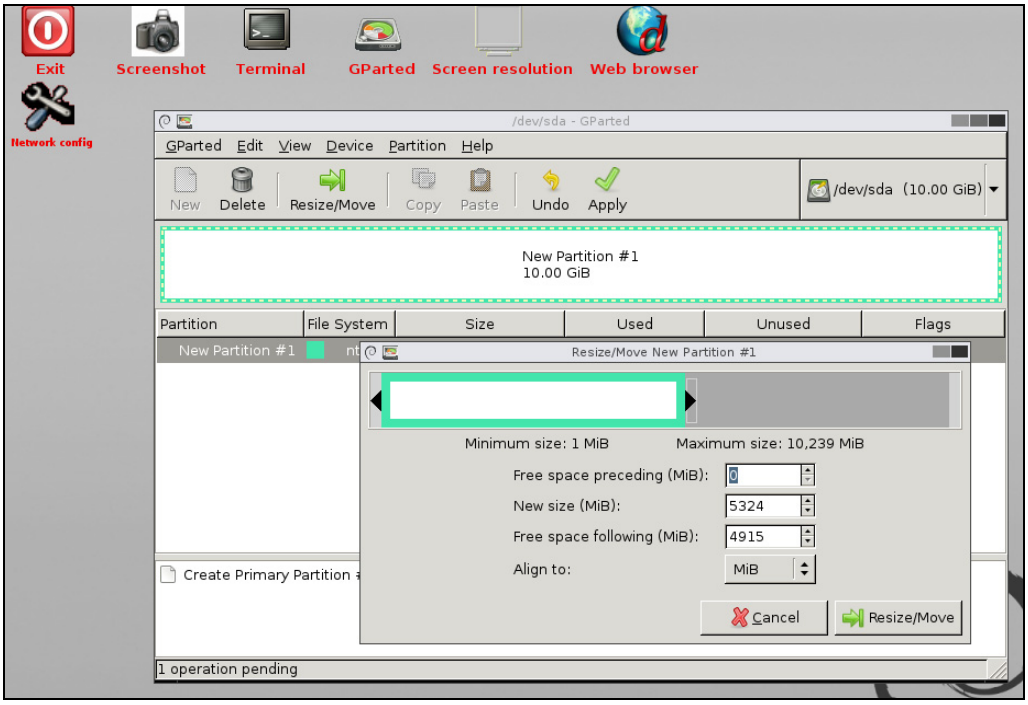


Рис. 2.7. Экран программы GParted, запущенной с LiveCD (производится выбор опций изменения размера раздела)

Если необходимо сжать раздел на Windows XP, то придется прибегнуть к утилитам сторонних разработчиков. Доступны как коммерческие решения, так и бесплатные варианты. Одним из наиболее популярных бесплатных решений является GParted. Для его использования необходимо скачать образ загрузочного диска с **http://gparted.sourceforge.net/livecd.php**, записать на соответствующее устройство (можно выбрать варианты CD, USB Flash, размещения на PXE-сервере) и загрузиться с него (на запросы в процессе старта — выбора варианта загрузки, используемого языка и т. д. — достаточно просто нажимать клавишу <Enter>, соглашаясь с вариантами по умолчанию). После появления окна GParted нужно выбрать раздел для операции, выполнить для него команду **Resize/Move** и ввести параметры (на сколько сжать раздел, можно использовать и графический режим — перемещать границу раздела — рис. 2.7).

Другая популярная утилита — EaseUs Partition Master Home Edition (**http://www.partition-tool.com/personal.htm**). Эта утилита может быть использована как на 32-разрядных ОС, так и на 64-разрядных, в том числе, "понимает" логические диски, собранные в RAID-массив.

Установка двух ОС на один компьютер

Загрузчик от Windows некорректно ведет себя по отношению к другим системам, заменяя собой существующие версии. Поэтому загрузчик Linux желательно ставить на раздел с Linux, чтобы Windows не произвела модификацию при последующих обновлениях системы. Предпочтительным вариантом является использование для старта компьютера именно загрузчика от последней версии Windows, в который в качестве опций добавлены варианты запуска других ОС. Такая конфигурация создается автоматически, если:

- Windows более новой версии устанавливается на компьютер с предыдущей версией, например, Windows 7 на компьютер с Windows XP;
- Linux ставится второй ОС на компьютер с Windows.

При такой последовательности установки при старте компьютера появится возможность выбора операционной системы для загрузки.

Восстановление двойной загрузки в Windows

Если попытаться выполнить установку Windows XP на компьютер с Windows 7, то после завершения операций опция загрузки Windows 7 будет недоступна при включении компьютера. Происходит это потому, что программа установки "не знает" о новом загрузчике и устанавливает собственные настройки.

Опция выбора вариантов загрузки может "потеряться" и в случае восстановления ОС (например, если потребовалось восстановить или переустановить Windows XP) либо — принципиально — после установки пакетов обновлений.

Чтобы восстановить возможность двойной загрузки, необходимо:

- восстановить загрузочную запись диска;
- скопировать на диск загрузочные файлы как Windows 7, так и Windows XP;
- восстановить записи о вариантах загрузки.

Ручное восстановление двойной загрузки в Windows 7

Для восстановления загрузочной записи диска используется утилита `bootsect`. Она находится на установочном диске Windows 7 (в папке Boot) и должна быть запущена следующим образом:

```
bootsect /nt60 All
```

Другой способ, более простой, но не столь быстрый, — использовать средства восстановления Windows 7, для чего загрузиться с установочного диска и выбрать опцию восстановления операционной системы.

Загрузочные файлы Windows 7 — это файл bootmgr и папка Boot (папка скрытая), для Windows XP — это файлы ntldr, ntdetect.com, boot.ini (в случае локализованной версии еще и файл Bootfont.bin). Загрузочные файлы Windows 7 можно сохранить в виде резервной копии (командой `bcdedit /export <путь>`), но можно и восстановить с использованием варианта восстановления операционной системы. Загрузочные файлы Windows XP необходимо перенести вручную с установочного диска.

Для управления загрузочными записями используется команда `bcdedit`. Команда требует некоторого предварительного изучения, поэтому мы отошлем читателя к специальному документу, который описывает синтаксис этой утилиты, иллюстрирует ее использование на примерах и т. п. и может быть загружен по ссылке **http://go.microsoft.com/fwlink/?LinkId=69448**.

Восстановление двойной загрузки с использованием EasyBCD

Для работы с загрузочными записями разработана специальная утилита — EasyBCD, которая бесплатно доступна для некоммерческого использования (ссылка для загрузки — **http://neosmart.net/dl.php?id=1**).

С помощью этой утилиты можно восстановить загрузочную запись диска (записать MBR на любой диск компьютера), добавить варианты второй загрузки для Windows XP, Mac OS X, Linux, настроить загрузку со сменного носителя, по сети, установить очередность загрузки и т. п.

Утилита предназначена для запуска в Windows 7, поэтому желательно сначала восстановить возможность загрузки компьютера в этой операционной системе, а потом добавить опцию запуска второй операционной системы. Хотя опытные пользователи смогут только при помощи EasyBCD восстановить MBR и создать базу загрузки на основе данных реестра системы.

Для того чтобы с помощью EasyBCD добавить опцию загрузки новой операционной системы, достаточно нажать кнопку **Add New Entry** в окне программы (рис. 2.8). После этого нужно выбрать операционную систему, которая должна быть запущена по данной опции.

Пусть в нашем случае это будет Windows XP. EasyBCD может автоматически определить диск с установленной ОС, для этого достаточно установить флажок **Automatically detect correct drive**. Поэтому указывать самостоятельно диск с установленной Windows XP не нужно. Для завершения операции достаточно нажать кнопку **Add Entry**, и новый вариант загрузки будет добавлен в настройки. Обрати-

те внимание, что необходимые загрузочные файлы Windows XP будут автоматически скопированы утилитой EasyBCD на диск.

Примечание

Строго говоря, EasyBCD копирует собственные варианты загрузочных файлов, позволяющие создать несколько загрузок различных экземпляров Windows XP. За уточнениями можно обратиться к онлайновой документации.

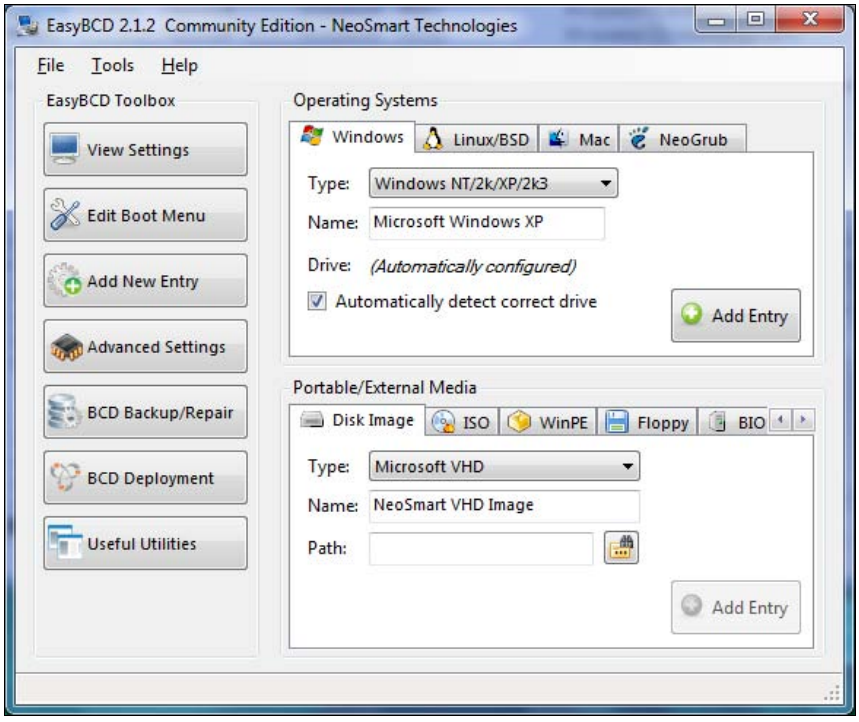


Рис. 2.8. Создание опции загрузки второй ОС с помощью EasyBCD

Для регулировки порядка загрузки и других параметров можно воспользоваться командой **Edit Boot Menu**.

Кроссплатформенный доступ

Часто возникает необходимость выполнить какую-либо операцию удаленно. Существуют различные способы выполнения команд на Linux-системах с Windows-компьютера и наоборот.

Удаленный доступ к Linux

В Linux существует несколько команд, обеспечивающих выполнение операций на удаленном компьютере, например `rlogin`, `rsh` и др. При возможности выбора следует остановиться на технологии SSH (Secure SHell, безопасная оболочка) для выполнения заданий на удаленной системе.

Для использования SSH необходимо на управляемом сервере установить пакет OpenSSH. Лучше всего это сделать в момент установки операционной системы, поскольку потребность в этом пакете возникает практически с первого момента работы с сервером.

Работа в Linux-системе с другого Linux-компьютера

Традиционно для управления Linux-системой администраторы используют режим командной строки. В этом режиме можно выполнить любые операции управления. Синтаксис операции удаленного выполнения команды следующий:

```
ssh имя@сервер команда
```

Без указания команды вы просто подключитесь к консоли удаленной системы и будете выполнять команды так же, как будто сидите за клавиатурой другого компьютера.

После запуска подключения по SSH система запросит пароль указанного в параметрах пользователя и при удачном подключении выведет на локальный экран итоги исполнения команды на удаленном компьютере. Например, `ssh имя@сервер pwd` позволит сменить пароль учетной записи *имя* на системе *сервер*. А команда `ssh имя@сервер ls ~ -la` отобразит подробное содержимое папки профиля пользователя.

Для копирования файлов между компьютерами удобна команда `scp`, входящая в состав пакета SSH:

```
scp имя1@host1:file1 имя2@host2:file2
```

В этом примере команда скопирует файл *file1*, находящийся на компьютере *host1*, к которому мы подключимся с использованием учетной записи *имя1*, на компьютер *host2* в файл *file2* при подключении с именем *имя2*.

> ***Примечание***
>
> В команде можно не вводить пароли, а использовать ключи аутентификации. Такой вариант запуска удобен для пакетного выполнения заданий (например, по расписанию). Более подробно о ключах команды можно прочесть в ее справочной документации.

Подключение к Linux с компьютеров под управлением Windows

Для работы с компьютерами с операционной системой Linux из-под Windows созданы многочисленные как коммерческие утилиты, так и бесплатные программы. Самой большой популярностью пользуется бесплатный SSH-клиент Putty, доступный к загрузке с многих серверов Сети (страница создателя программы **http://www.chiark.greenend.org.uk/~sgtatham/putty/**; последняя версия имеет номер beta 0.60, это стабильно работающая версия, и не стоит обращать внимание на слово beta).

Эта утилита не требует установки. После запуска достаточно ввести имя удаленной системы, выбрать команду подключения, чтобы достаточно быстро появилось окно с приглашением ввода параметров учетной записи. При работе с несколькими сер-

верами параметры подключения и настройки клиента можно сохранить в конфигурационном файле.

> ***Примечание***
>
> Putty также позволяет использовать ключи аутентификации для доступа к удаленным системам. Чтобы сгенерировать ключи, необходимо загрузить соответствующие утилиты с сайта разработчика (или найти версию программы, включающую эти утилиты комплектом).

Для подключения к системам Ubuntu в настройки сессии необходимо внести только одно изменение — указать использование кодировки UTF-8. Это можно сделать уже на подключенной сессии (щелкнуть правой кнопкой мыши по значку программы в окне сессии и выбрать команду **Change Settings...**; изменения наступят после обновления окна — при отображении результатов следующей команды), так и сохранить в параметрах сессии по умолчанию, если вы подключаетесь ко многим системам (в блоке **Category** выбрать пункт **Window | Translation** и указать в правой части окна кодировку UTF-8 для параметра **Received data assumed to be in which character set**).

Putty хорошо работает с Midnight Commander, понимает его функциональные клавиши (<F5>, <F8> и т. п.). С помощью Putty легко организовывать SSH-туннели к другим компьютерам в удаленной сети. Предположим, что в удаленной сети есть компьютеры с операционной системой Windows, и вы хотите подключиться к рабочему столу одного из таких компьютеров. Для этого достаточно создать туннель, соединяющий какой-либо порт локального компьютера и порт 3389 соответствующей станции в удаленной сети. Введите эти параметры в опции сессии (это можно сделать уже для подключенной сессии, не забудьте только после ввода параметров нажать кнопку **Apply**). На локальном компьютере откройте программу подключения к удаленному рабочему столу и введите в строке адреса 127.0.0.1:81 (81 — номер локального порта, который вы указали в настройках туннеля — рис. 2.9). Вы увидите, как быстро компьютер подключится к удаленному рабочему столу, время подключения будет существенно ниже, чем в случае подключения с использованием клиента VPN.

Вторая операция, которая часто необходима при работе с Windows, — это копирование файлов из Windows в Linux и наоборот. Для этих целей можно использовать бесплатную утилиту WinSCP (**http://winscp.net**, рис. 2.10). Интерфейс программы создан по типу Norton Commander, на одной панели которого отображаются локальные данные, а на вторую выводятся папки подключенной системы. Выполняются операции так же, как и в любых других файловых менеджерах для Windows.

Акцентируем внимание читателя только на двух моментах. Поскольку к Ubuntu по умолчанию невозможно подключиться с правами суперпользователя, то при файловых операциях вы будете ограничены правами той учетной записи, которая использована для подключения. Если необходимо скопировать файлы, для которых требуются права суперпользователя, то лучше всего подключиться к системе при помощи Putty, далее командой `sudo` предоставить необходимые права (например, сначала скопировать файл в папку пользователя, а потом назначить на него полные права) и уже после этого выполнить файловую операцию в WinSCP.

Второй момент, на который обычно не обращают внимания, — это наличие опции, включающей доступ к дополнительным параметрам (**Advanced Options**). Дополнительные настройки позволяют использовать WinSCP при доступе в Интернет через прокси-сервер, а также подключаться по SSH-туннелям.

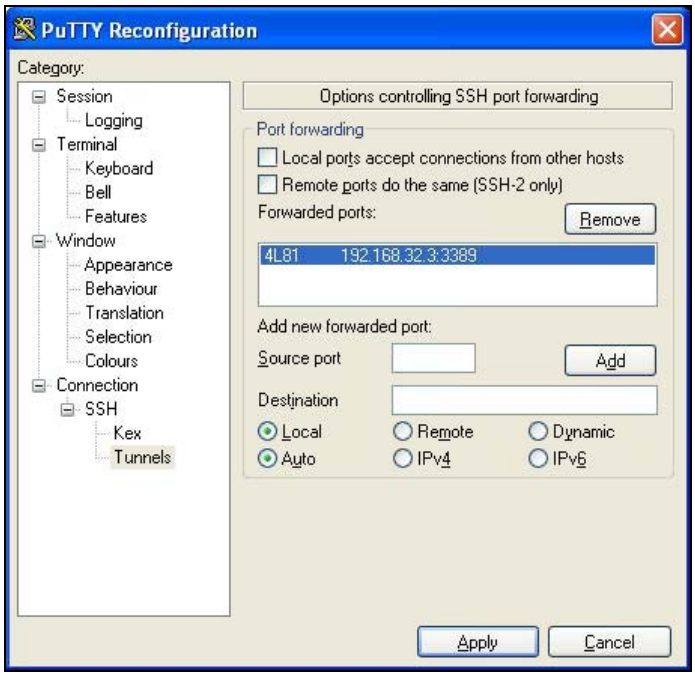


Рис. 2.9. Создание туннеля средствами Putty

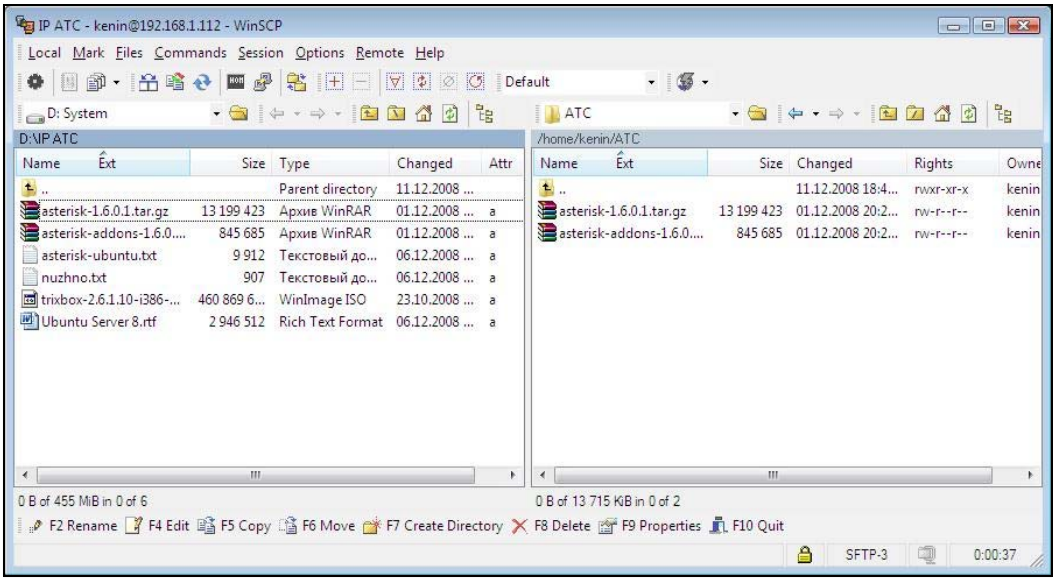


Рис. 2.10. Программа WinSCP

Перенаправление графического вывода с Linux-систем

Графическое отображение в Linux выполнено по технологии клиент-сервер, что легко позволяет перенаправлять графический вывод программ на любую удаленную консоль.

Чтобы вывести на локальный экран в Windows графические данные программы из Linux (например, вы можете запустить текстовый редактор на компьютере с Linux, а работать с ним — видеть текст, редактировать и т. д. — за экраном и с клавиатуры Windows), нужно:

1. Перенаправить графический вывод программы с удаленного компьютера на локальный.
2. Установить на локальной системе программное обеспечение для отрисовки графики (его называют еще X-сервером).

Перенаправление графического вывода позволяет делать, в том числе, утилита Putty. Для этого достаточно в ее настройках указать **SSH | Tunnels | Enable X11 forwarding**. Сделать это нужно до подключения, поскольку после подключения коррекция этой опции недоступна.

X-серверы существуют как в коммерческих версиях (например, Xmanager Enterprise — **http://www.netsarang.com/products/xme_overview.html**), так и в OpenSource-вариантах. Наиболее известные бесплатные пакеты — это X-Ming (**http://sourceforge.net/projects/xming/**) и Cygwin (**http://x.cygwin.com/**).

Для перенаправления графического вывода необходимо сначала запустить X-сервер на Windows, потом подключиться к Linux-системе клиентом SSH с установленной опцией туннелирования графического интерфейса и запустить соответствующую графическую программу в Linux.

Подключение к рабочему столу Linux

К Linux-системе, если на ней установлена графическая подсистема, можно подключиться так же, как к терминальному серверу Windows. Наиболее распространенным средством такого подключения является применение кроссплатформенного пакета VNC (бесплатное решение), который позволяет использовать в качестве сервера и клиента операционные системы Windows и Linux в любом сочетании (можно подключаться к Linux, работая в Windows, и наоборот).

Существует большое количество как различных бесплатных реализаций VNC, так и коммерческих продуктов, созданных на его базе. Обычно для каждой версии Linux имеются соответствующие пакеты VNC, бесплатно доступные из репозиториев. Для других платформ (например, Windows) читатель без труда найдет наиболее привлекательный для себя вариант, отметим только одну из самых популярных бесплатных сборок — UltraVNC (**http://www.uvnc.com/**).

Для обеспечения возможности подключения к Linux с использованием VNC вы должны проверить, что соответствующий пакет серверного программного обеспечения установлен и включена его автоматическая загрузка. Кроме того, следует на-

строить конфигурацию сервера VNC, определить допустимое число сессий, пароли и т. д. Эти действия выполняются в соответствии с описаниями справочной системы.

Помимо VNC существуют и другие варианты бесплатного подключения к рабочему столу Linux. Так, для случая не более двух одновременных подключений можно использовать программу NoMachine NX (**http://www.nomachine.com/**).

Коммерческие продукты обычно предоставляют больше удобств при подключениях, например, упоминавшийся ранее Xmanager Enterprise позволяет подключиться к рабочему столу Linux без необходимости проведения дополнительных настроек на последнем (рис. 2.11).

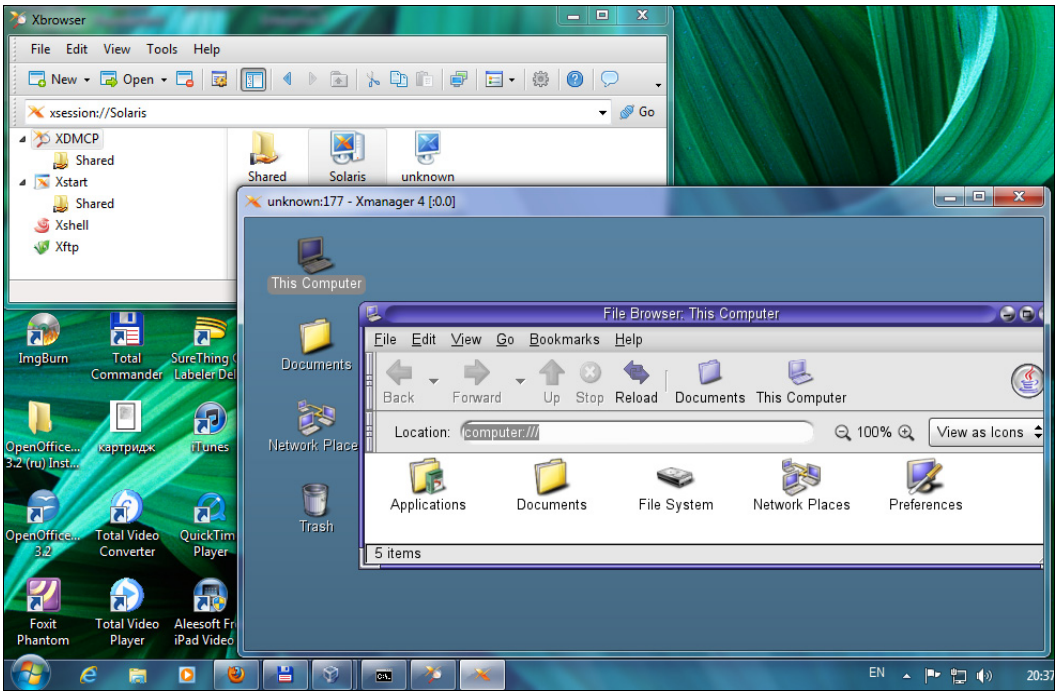


Рис. 2.11. Подключение к рабочему столу Solaris из Windows 7

Запуск Windows-программ на Linux

Существует несколько технологий, обеспечивающих запуск Windows-приложений на Linux. Однако все эти проекты сталкиваются с большими трудностями вследствие неполноты или отсутствия документации по многим элементам Windows.

Наиболее известным проектом является Wine. Wine воспринимает системные вызовы Windows-приложений к операционной системе и подменяет их своими. Для работы Wine не требует наличия установленной ОС Windows, хотя может использовать ее библиотеки.

В Wine не удается запустить все приложения Windows. Полноценно работают под Wine те приложения, которые не используют недокументированные возможности

Windows. В качестве примера отметим, что до появления версии 1С, специально созданной для Linux, энтузиасты добились стабильной работы этой программы в среде Wine.

Настройка Wine не тривиальна. Поэтому интересующихся читателей отошлем к официальному сайту продукта — **http://www.winehq.com/**, а также к FAQ продукта — **http://ru.wikibooks.org/wiki/LOR-FAQ-Wine**, которое фактически является руководством по установке и использованию.

Клонирование систем

Сэкономить свое время при вводе новой системы можно, если выполнить *клонирование* жесткого диска.

Клонирование представляет собой процесс воспроизведения данной системы на другом рабочем месте. Клонированная станция будет иметь аналогичную версию операционной системы, те же установленные (и соответствующим образом настроенные) прикладные программы пользователей и т. п. К клонированию обычно прибегают при обновлении аппаратной части рабочего места (новый системный блок), при восстановлении "упавшего" компьютера, при создании типовых рабочих мест и т. д.

Учитывайте уникальные параметры системы

Главный подводный камень операции клонирования — необходимость изменения *всех* уникальных параметров для новой операционной системы. Так, следует сменить в ОС сетевое имя на уникальное, настроить новые параметры сетевых интерфейсов. Кроме указанных очевидных настроек необходимо сменить и другие уникальные характеристики, присущие системам. Например, уникальный идентификатор безопасности для ОС Windows. Именно его наличие не дает возможность запуска sysprep на членах домена. Конечно, существует утилита NewSID (**http://technet.microsoft.com/ru-ru/sysinternals/bb897418**), позволяющая установить новый идентификатор безопасности (если вы сдублировали диск без предварительного запуска sysprep) и выполнить связанные с этим настройки доступа. В большинстве случаев после ее использования вы получите полностью работоспособную систему, хотя в некоторых редких ситуациях можно встретиться после генерации нового идентификатора и с ошибками в прикладном ПО.

> ***Примечание***
>
> Некоторые коммерческие программы дублирования позволяют создавать копии дисков компьютеров — членов домена. На самом деле такая операция проводится в несколько этапов: используя параметры заданной учетной записи, такая программа выполняет операцию включения нового компьютера в домен.

Кроме указанного идентификатора безопасности, некоторые программы могут записывать на компьютеры и собственные, также уникальные метки. Например, программы мониторинга и сетевого управления. Составить исчерпывающий перечень подобных программ невозможно. Поэтому системному администратору следует

предугадывать подобные варианты при планировании клонирования или же устранять конфликты уже после начала работ с новой системой.

Дублирование жесткого диска

Наиболее простой вариант создания копии системы заключается в дублировании жесткого диска. Существует несколько программ, с помощью которых можно выполнить подобную операцию. Наиболее популярна программа GHost от Symantec, часто применяют утилиты от Acronis (**http://www.acronis.ru/**).

Структуру жесткого диска можно копировать непосредственно с диска на диск как на одном компьютере, так и на различных системах при подключении через COM-, LPT-, USB-порты или сеть. Можно сохранить образ диска в виде файла и на его основе создать последующие копии дисков. Последний вариант наиболее удобен в практике администрирования, поскольку подготовить инфраструктуру для восстановления в такой конфигурации не представляет особого труда.

> ***Примечание***
>
> Поскольку при шифровании данных применяется уникальный идентификатор безопасности, который заменяется программами дублирования диска, то для сохранности информации *все зашифрованные файлы необходимо расшифровать перед клонированием*.

Утилита *sysprep*

Поскольку клонированный диск вряд ли будет ставиться на идентичную аппаратную платформу, то необходимо обеспечить обнаружение нового оборудования и установку драйверов при первом включении в новой системе. Для этого используется утилита `sysprep`, которая "возвращает" систему на этап обнаружения оборудования: при включении выполняются завершающие этапы конфигурирования операционной системы.

Учтите, что версии утилиты отличаются для различных операционных систем. При возможности следует всегда использовать наиболее свежие версии, предназначенные для вашей версии Windows. В Windows Server 2008 утилита находится в папке Windows, в других версиях ее нужно искать в Support\Tools\ установочного компакт-диска системы в архиве deploy.cab.

При использовании sysprep допустимо применять все возможности автоматизации инсталляции: создать файл ответов, добавить новые, отсутствующие в дистрибутиве драйверы устройств, выполнить после завершения процесса определенные программы и т. д.

Особенностью использования программы является то, что установленные на исходном компьютере прикладные программы остаются работоспособными после операции клонирования. То есть вы можете полностью "укомплектовать" компьютер, установить все прикладные программы, а затем быстро создать новые компьютеры "по образцу".

Модификация образов диска

Вместо дублирования подготовленного диска можно создать его *образ* и сохранить такой файл на сервере. Практически все программы клонирования дисков позволяют сформировать новый диск из такого файла.

Данный способ, во-первых, упрощает хранение образов. А во-вторых, позволяет добавлять в образы новые файлы, программы и т. д. Поскольку `sysprep` обеспечивает настройку системы путем выполнения сценариев при первом включении, то легко можно добавить в файл образа необходимые дополнительные компоненты (например, новые драйверы или автоматический запуск установки дополнительного продукта). Описание соответствующих правил добавления автозапускаемых сценариев можно найти в справке утилиты `sysprep`.

Установка виртуальных систем

Установка операционной системы на виртуальную машину имеет некоторые особенности. Существует несколько способов создания новой виртуальной машины:

- путем "чистой" установки операционной системы *(clean install)*;
- клонированием существующей виртуальной машины;
- снятием образа системы с физического сервера на виртуальный жесткий диск.

Создание виртуальной машины путем чистой установки операционной системы

Это самый простой способ создания новой виртуальной машины. Установка ОС выполняется так же, как и на "чистый" компьютер, разве только вместо реальных CD/DVD можно использовать файлы их образов, да и параметры сетевого подключения гостевой ОС следует сначала определить в настройках гипервизора.

Собственно установка гостевой ОС на современных системах происходит достаточно быстро, обычно порядка 10 минут. После установки ОС в виртуальной машине необходимо проинсталлировать расширения, предлагаемые соответствующим гипервизором.

Хотя в качестве гостевых ОС можно использовать "обычные" версии ПО, лучше воспользоваться специальными облегченными дистрибутивами. В случае ОС Windows таковыми являются:

- для Windows XP — Windows Fundamentals for Legacy PCs;
- для Windows 7 — Windows Thin PC.

Данные версии имеют некоторые ограничения (например, в Windows Thin PC не поддерживается .NET Framework, нельзя добавлять компоненты и т. д. — полный перечень ограничений необходимо уточнить по сопроводительной документации), но в подавляющем большинстве случаев функциональности этих версий достаточно для полноценной работы, а их "облегченность" сводит к минимуму нерациональное использование ресурсов компьютера.

Например, Windows Fundamentals for Legacy PCs предъявляет следующие минимальные требования к аппаратной составляющей:

- процессор от Pentium 233 и выше;
- память от 64 Мбайт (после установки операционной системы компьютер может работать с памятью объемом 32 Мбайт);
- жесткий диск от 500 Мбайт;
- видеоадаптер и монитор с разрешением 800×600;
- сетевая карта от 10 Мбит/с.

Это существенно ниже требований к базовой системе.

Клонирование виртуальной машины

Клонирование — самый быстрый способ создания виртуальной машины, заключающийся в копировании уже существующего образа. Обычно создается несколько *шаблонов* — файлов образов жесткого диска с различными наборами установленного программного обеспечения, которые используются для создания новой виртуальной машины.

Снятие образа физического сервера

При внедрении виртуализации часто приходится переводить уже существующие физические серверы под управление гипервизора. Для этой цели вендорами разработаны специальные решения. Например, компания VMware предлагает бесплатный VMware vCenter Converter (**http://www.vmware.com/products/converter/**). Microsoft включила данную функциональность в состав Hyper-V (**http://technet.microsoft.com/en-us/magazine/ff458344.aspx**, только для диска данных), Microsoft Deployment Toolkit 2010 и т. д. Можно использовать и возможности утилит, предназначенных для работы с жесткими дисками (например, WinImage, Ghost и др.). Данная функциональность входит в состав коммерческих средств управления виртуальными системами (например, System Center Virtual Machine Manager и др.).

Но, на взгляд автора, очень удобно использовать небольшую утилиту от Windows Sysinternals — Disk2vhd (**http://download.sysinternals.com/Files/Disk2vhd.zip**). Эту программу можно запустить на работающем сервере и создать VHD-файл — копию реального диска. Утилита Disk2vhd использует теневые снимки жесткого диска, поэтому возможные причины ошибки ее запуска связаны с проблемами службы теневого копирования (Volume Shadow Copy Service), которые устраняются соответствующими пакетами обновлений (см., например, **http://support.microsoft.com/Default.aspx?kbid=940349**).

Другая причина возможных ошибок при использовании утилиты Disk2vhd заключается в отсутствии драйверов контроллеров IDE и соответствующих записей в реестре, если для загрузочных устройств сервера, клонирование которого необходимо выполнить, применены драйверы вендора. В этом случае при загрузке виртуальной машины с vhd-диска, сформированного утилитой Disk2vhd, вы получите

"голубой экран смерти" — Stop 0x0000007B. Исправить ситуацию можно, если сначала применить к работающему серверу рекомендации, изложенные в документе KB314082 (при необходимости скопировать указанные драйверы и добавить записи в реестр системы; данная операция не требует перезагрузки сервера), и только после этого сделать копию диска (см. **http://support.microsoft.com/kb/314082**).

Следует учесть, что виртуальные машины, сформированные описанным способом, содержат в себе избыточные драйверы оборудования, которые использовались на физическом сервере. Это программное обеспечение, в общем случае, увеличивает риск возникновения ошибок в работе операционной системы. Поэтому желательно удалить ненужные компоненты из системы.

Миграция между решениями различных вендоров

На практике часто бывает необходимо подключить виртуальную машину, подготовленную в ПО одного вендора, к гипервизору другого разработчика. Например, протестировать на развернутом гипервизоре демо-предложение, присланное в виде виртуальной машины.

Подобный перенос предполагает решение двух проблем: копирование настроек виртуальной машины и преобразование файла виртуального жесткого диска в формат, поддерживаемый установленным гипервизором.

Хотя настройки виртуальной машины и представлены обычно в виде текстового файла, часто достаточно определить их заново в мастере операций. Для преобразования форматов файлов виртуальных дисков нужно использовать специальные программы. Как правило, найти подобные утилиты преобразования виртуальных машин, созданных в одном гипервизоре, в другую среду не представляет особого труда. В частности, автор предпочитает использовать бесплатные средства из состава Oracle VirtualBox. Эти утилиты находятся в папке установки пакета (они не отображаются в графическом меню) и запускаются в режиме командной строки. Необходимая информация по их применению (ключи запуска) доступна по онлайновой справке.

Использование неизменной конфигурации системы

Одним из способов обеспечения стабильной работы системы является запрет на внесение изменений на локальный диск. Традиционный совет для тех, кто не хочет "подхватить" что-то в Интернете, заключается в работе в системе, запущенной с LiveCD.

Кроме того, есть специальные решения по обеспечению неизменности конфигурации. Так, Microsoft подготовила специальную модификацию для Windows XP, предназначенную для интернет-кафе и игровых клубов, которая возвращает состояние системы к начальному после каждой перезагрузки.

Аналогичные решения присутствуют и среди бесплатных продуктов. Например, по адресу **http://www.bitdisk.ru/** доступна программа BitDisk, которая также может

контролировать запись изменений во время работы системы. Бесплатная версия программы после перезагрузки системы возвращает состояние к тому моменту, на котором эта функция была включена (платная версия позволяет переключаться между режимами без перезагрузки и управлять возможностью сохранения изменений на локальный диск).

Для Windows 7 о подобных решениях от вендора автору неизвестно. Официальная рекомендация состоит в использовании настроек, которые в своей совокупности создают практически неизменяемую систему. Соответствующие рекомендации описаны в документе "Creating a Steady State by Using Microsoft Technologies", доступном к загрузке по ссылке **http://go.microsoft.com/fwlink/?LinkID=201413**.

В условиях домена неизменность конфигурации можно обеспечить также соответствующей настройкой групповых политик. Рекомендации по особенностям настройки политик для сохранения неизменности конфигурации можно загрузить по ссылке **http://go.microsoft.com/fwlink/?LinkId=201798**.

Настройка серверов

Типовая конфигурация операционной системы (после стандартной установки "из коробки") предназначена для обеспечения универсальной работоспособности компьютера, чтобы установленная система сразу была пригодна для производственной деятельности.

Необходимо выполнить ряд настроек, которые во многом индивидуальны для каждого компьютера. Поэтому привести универсальные рекомендации в данной книге не представляется возможным.

Отмечу только, что администратору системы следует оптимизировать *каждый* сервер под те задачи, которые он решает. Необходимые рекомендации легко можно найти на сайтах разработчиков программного обеспечения по ключевым словам *"hardening"* или *"security guide"*. В подобных документах обычно достаточно подробно описываются параметры, влияющие на уровень безопасности системы, и возможные последствия в функционировании информационной структуры при их изменении. Администратору следует внимательно проанализировать каждый параметр и оценить целесообразность предполагаемых изменений.

Security Configuration Manager

В составе Windows Server присутствует программа Security Configuration Manager (SCM). Как видно по названию, SCM предназначена для настройки параметров безопасности сервера. Практически программа предлагает применить к системе один из шаблонов безопасности, выбрав ту или иную роль данного сервера.

SCM привлекательна тем, что предлагает применить *комплексно* все те рекомендации, которые содержатся в объемных руководствах по безопасности. Однако в реальных системах редко можно найти серверы с "чистой" ролью: обычно присутствуют те или иные модификации, заставляющие администратора тщательно ревизо-

вать предлагаемые к назначению настройки. Поэтому данный мастер следует рассматривать только как первый шаг настройки сервера.

Security Compliance Manager

Microsoft разработала специальное средство для анализа и разворачивания в организации групповых политик безопасности — Microsoft Security Compliance Manager. Утилита доступна к бесплатной загрузке со страницы **http://go.microsoft.com/fwlink/?LinkId=182512**. Установить ее можно на системы под управлением Windows Vista/7/Server 2008; продукт требует сервера базы данных (бесплатная версия может быть загружена и настроена в процессе установки утилиты).

Microsoft подготовила шаблоны рекомендуемых параметров настроек безопасности для систем Windows XP/Vista/7/Server 2003/Server 2008, предназначенных для эксплуатации в типовых условиях, в условиях предприятия и для организаций с повышенным уровнем безопасности. Обычно в конкретных условиях применить все рекомендации невозможно: например, какие-то компоненты, рекомендуемые для отключения, предполагается использовать. Утилита Security Compliance Manager и предназначена для того, чтобы сравнить текущие параметры групповой политики с рекомендациями, отредактировать их и применить групповую политику в организации.

Установка обновлений прошивок оборудования

Ряд элементов системного блока компьютера имеет обновляемое ПО, которое часто называют *прошивками*. Это могут быть и новые версии BIOS, и программное обеспечение, контролирующее работу узлов серверной платы (Baseboard Management Controller, BMC), различные обновления firmware и т. п. Качество данного ПО существенно влияет на стабильность работы прикладного программного обеспечения. Кроме того, это направление стало приобретать популярность у злоумышленников, пытающихся получить несанкционированный доступ к системе. На практике ведь часто забывают о необходимости такого обновления, и серверы работают по много лет с неизменяемым кодом.

Поэтому крайне важно установить последнюю версию таких прошивок до передачи системы в эксплуатацию. Чтобы получить новые версии, необходимо посетить сайт изготовителя. При этом нужно быть особо внимательным к описаниям, сопровождающим различные версии ПО. Часто установка того или иного обновления допустима только на определенные серийные номера оборудования или может зависеть от установки другого компонента.

Установка обновлений безопасности

Установку обновлений безопасности необходимо обеспечивать в течение всего периода эксплуатации сервера или рабочей станции. Если в системе будет сохраняться уязвимость, то это означает, что злоумышленник в любой момент может получить управление над нею. Строгая настройка межсетевого экрана снижает риск

атаки, но оставляет "двери" в систему в виде портов, открытых для каких-либо приложений.

Если говорить об обновлениях для операционных систем Windows, то они выпускаются регулярно, обычно раз в месяц. Естественно, что при обнаружении критической уязвимости соответствующая заплатка выпускается вне графика. Для того чтобы быть в курсе выпускаемых обновлений безопасности, следует подписаться на соответствующие рассылки вендоров. На странице **http://technet.microsoft.com/ru-ru/security/dd252948.aspx** можно подписаться на наиболее удобный для вас вид оповещений о выпуске обновлений безопасности для систем Windows (возможны варианты по электронной почте, по каналам RSS, Windows Live Alert и т. д.). Для операционной системы Ubuntu получение оповещений доступно на основе RSS-подписки (**http://www.ubuntu.com/usn/rss.xml**), а перечень выпущенных обновлений публикуется на странице **http://www.ubuntu.com/usn**.

Когда устанавливать обновления

Установка обновлений безопасности — это модификация операционной системы. В общем случае, перед установкой каждое обновление нужно протестировать в условиях, приближенных к реальной эксплуатации в данной организации. Было много случаев, когда установка вроде безобидного патча приводила, например, к ошибкам печати на сетевой принтер или отказу какого-либо эксплуатируемого приложения и т. п. Конечно, в средних и небольших организациях такие проверки выполнить очень сложно. Поэтому отключите автоматическое обновление, по крайней мере, серверов и настройте график установки заплаток так, чтобы в эти моменты вы могли быстро вмешаться и восстановить работу информационной системы.

> ***Совет***
>
> Автор советовал бы до установки обновлений изучить их описания, для чего они предназначены и т. п. Часто установка обновлений на конкретную систему нецелесообразна в силу специфики данного конкретного рабочего места.

Кроме того, нелишне убедиться, что до начала установки обновлений у вас есть актуальная копия данных, которая позволит восстановить работу при катастрофическом отказе системы в результате процесса обновления.

Для большинства пользовательских компьютеров обычно не критично, если они будут выведены из строя на достаточно существенный промежуток времени. Поэтому на таких рабочих местах можно включить режим автоматической загрузки и установки обновлений.

В Windows XP/Server 2003 режим установки обновлений настраивался через вызов свойств задачи Мой компьютер, в Windows Vista/7/Server 2008 необходимые параметры назначают в задаче **Панель управления | Центр обновлений | Изменить параметры**. Обратите внимание, что в этом окне (рис. 2.12) можно включить поиск и установку обновлений не только для самой операционной системы, но и для тех приложений Microsoft, которые обслуживаются Windows Update (программы Microsoft Office, SQL Server и т. п.). Для этого необходимо включить опцию использования Windows Update.

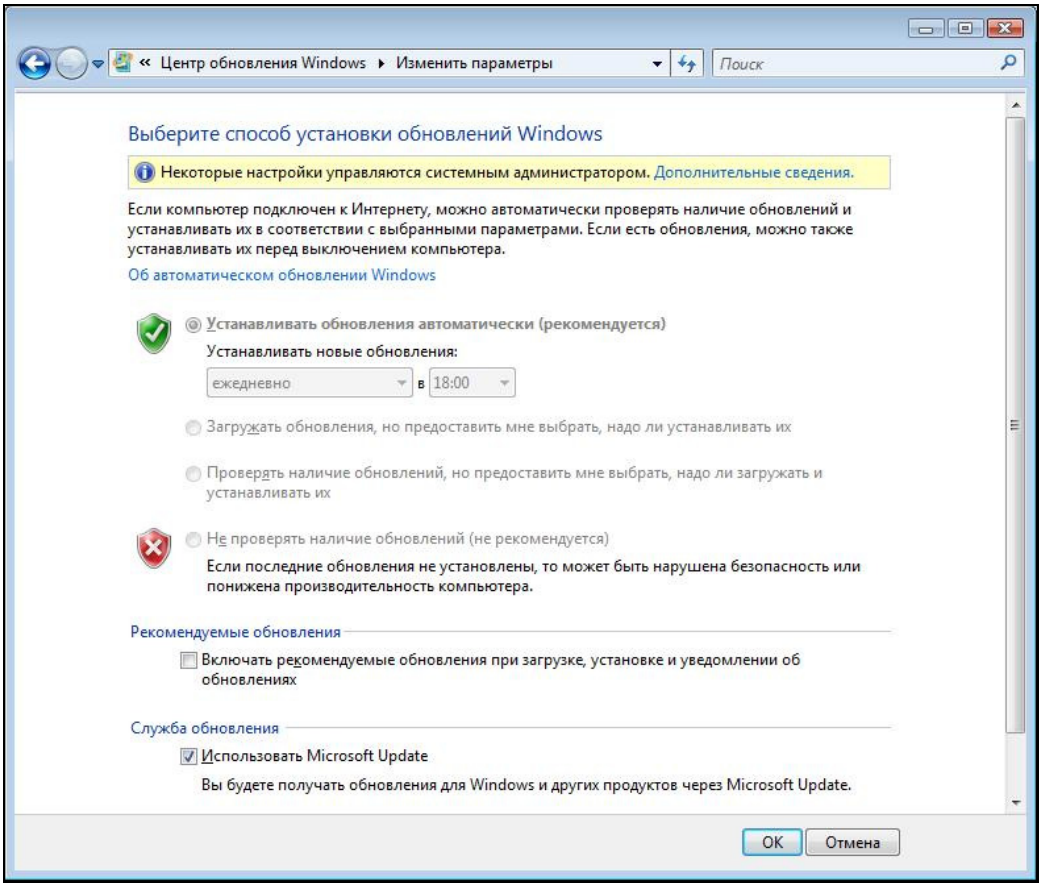


Рис. 2.12. Настройка режима обновления операционной системы Windows

Нужно ли устанавливать все обновления?

Обновления принято подразделять на критические, рекомендуемые и обновления драйверов (программного обеспечения видеоадаптеров, материнских плат и т. п.). Общая рекомендация заключается в обязательной установке всех критических и рекомендуемых обновлений. Однако если вы обладаете некоторым опытом администрирования систем, то можете сделать осознанный выбор. Установка каждого обновления — это риск нарушить работу системы. Например, стоит ли устанавливать обновление безопасности, основная цель которого — исключить возможность пиратской активации? Или обновить медиапроигрыватель, которым вы точно не будете пользоваться?

Каждое обновление сопровождается соответствующим бюллетенем безопасности, в котором описаны устраняемые уязвимости. Достаточно внимательно прочитать этот документ, чтобы принять верное решение. Для отключения установки обновления в Windows при использовании технологии Windows Update достаточно просто скрыть его, для установки скрытого обновления — отобразить список скрытых обновлений и подтвердить необходимость установки (рис. 2.13).

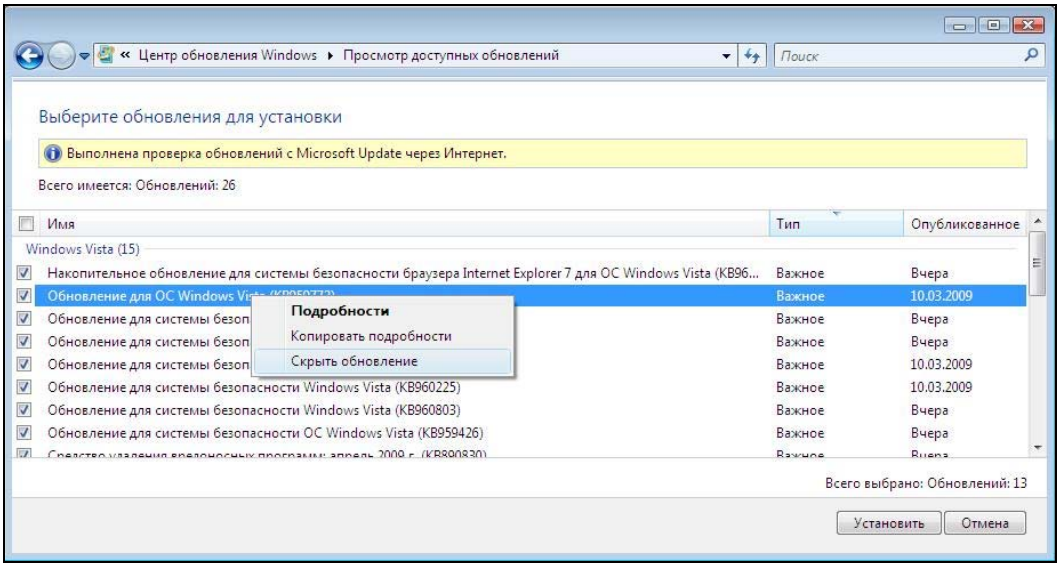


Рис. 2.13. Скрытие и отображение обновлений Windows

Настройка установки обновлений с сервера интрасети

Microsoft выпустила бесплатный пакет установки сервера обновлений — WSUS, позволяющий создать в интрасети сервер обновлений. Этот сервер фактически является прокси-сервером для обновлений с сайта Microsoft.

> ***Примечание***
>
> Не забудьте, что на системы Windows 2000 и Windows XP без пакетов обновлений необходимо предварительно установить пакет автоматического обновления, который нужно загрузить с сайта Microsoft.

Устанавливать WSUS в небольшой сети не имеет смысла, поскольку экономия на трафике будет не столь существенной, по сравнению с затратами на поддержание сервера в работоспособном состоянии и периодический контроль результатов операций для локальных систем. Однако серверы WSUS часто устанавливают интернет-провайдеры и разрешают использование их для обновлений систем из обслуживаемых диапазонов. При этом трафик с такого сервера, как правило, тарифицируется как бесплатный.

Для реализации локального сервера обновлений необходимо выполнить настройку систем. Сделать это предпочтительно через настройку групповой политики (запустить оснастку следует командой `gpedit.msc` — рис. 2.14).

Параметры настройки сервера обновления расположены по пути **Конфигурация компьютера | Административные шаблоны | Компоненты Windows | Центр обновления Windows**. Минимально необходимо определить адрес сервера, другие параметры (время обновления и т. п.) уточняются при необходимости.

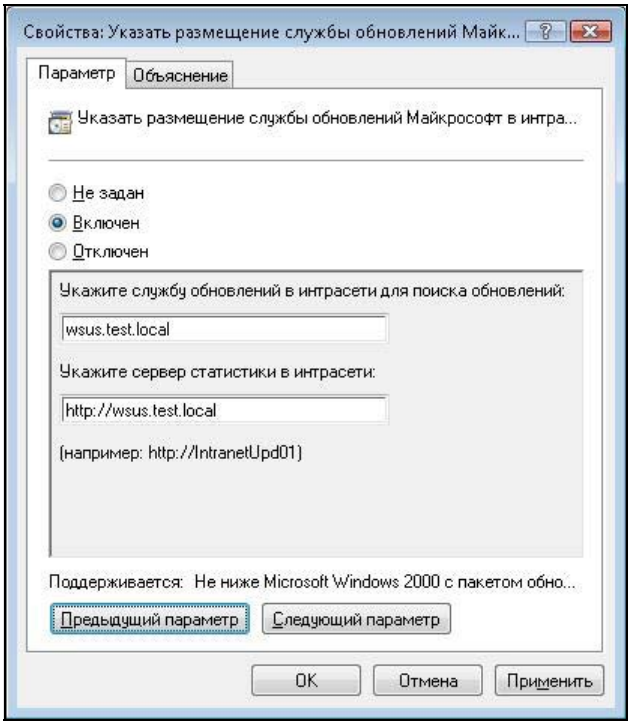


Рис. 2.14. Настройка параметров сервера обновления

Другой способ заключается в непосредственном указании в реестре систем по ключу `HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate` адреса сервера обновлений:

```
WUServer=http://адрес
WUStatusServer=http://адрес
```

Локальные системы загружают обновления с помощью службы HTTP, которая не применяет настройки доступа в Интернет из обозревателя. Это может осложнить процесс обновлений при наличии в локальной сети прокси-сервера. В этом случае необходимо воспользоваться утилитой `proxycfg`, включенной в состав Windows XP, начиная со второго обновления. Ключи утилиты описаны в библиотеке Microsoft (**http://msdn.microsoft.com/en-us/library/aa384069%28VS.85%29.aspx**), обычно достаточно выполнить команду

```
proxycfg -p адрес:порт
```

Примечание

Некоторые клонированные системы не могут использовать сервер обновлений до тех пор, пока вручную не будет выполнен ряд настроек. Подробности операций описаны на странице **http://support.microsoft.com/Default.aspx?id=903262**.

Установка обновлений в Linux

Установка обновлений в Linux не представляет никакой сложности. Сами обновления имеют малый объем загрузки (несколько десятков килобайт), могут быть установлены на сервер без прекращения обслуживания.

Для установки в Ubuntu используются заранее подготовленные пакеты программ, хранимые на специальных серверах — *репозиториях*. Список репозиториев представлен в файле /etc/apt/sources.list. При установке операционной системы в этот файл заносятся параметры серверов, оптимизированные для района эксплуатации. При этом по умолчанию настройки обеспечивают доступ к сертифицированным для данного выпуска пакетам. Вы можете несколько расширить перечень доступных к установке пакетов, если раскомментировать соответствующие строки в этом файле.

Перед установкой любого пакета (или обновлением сервера) необходимо синхронизовать информацию сервера с данными репозиториев. Для этого достаточно выполнить команду

```
sudo apt-get update
```

Вы должны увидеть в консоли информацию об успешной загрузке нужных файлов. После чего необходимо выполнить команду

```
sudo apt-get upgrade
```

которая обновит все установленные на компьютере программы.

Пакеты обновлений безопасности можно устанавливать в автоматическом режиме. В этих целях используется пакет unattended-upgrades. Он должен быть установлен командой `apt-get install` и является, по сути, сценарием для этой утилиты. Загрузка и установка обновлений прописываются в ежедневно выполняемый сценарий (/etc/cron.daily/apt). Обратите внимание, что устанавливаться будут только те обновления, которые находятся в сконфигурированных репозиториях.

Настройка обновлений системы через прокси-сервер

Если доступ в Интернет осуществляется через прокси-сервер, то его настройки достаточно прописать в файле конфигурации apt — /etc/apt/apt.config.d/proxy[1]:

```
Acquire:: http:: Proxy "http://пользователь:пароль@адрес_прокси:порт/";
Acquire:: ftp:: Proxy "ftp://пользователь:пароль@адрес_прокси:порт/";
```

Такая настройка обеспечивает работу через профессиональные прокси-серверы. Однако при работе через прокси от Microsoft подобных настроек недостаточно. Проблема заключается в особенностях авторизации NTLM от Microsoft.

---

[1] Вы можете увидеть в Сети отличающиеся рекомендации. Есть несколько файлов настройки, в которых можно определить данные параметры. Кроме того, возможен и иной вариант синтаксиса (приведен вариант написания доменной учетной записи и многострочная запись):

```
ACQUIRE
{
http::Proxy "http://DOMAIN\пользователь:пароль@прокси:порт"
}
```

Существует несколько способов решения проблемы. Самый простой вариант — установить дополнительный прокси-сервер, который будет осуществлять NTLM-аутентификацию на сервере Windows. Например, с сайта **http://cntlm.sourceforge.net/**.

В конфигурационный файл данного прокси (/etc/cntlm.conf) нужно внести параметры учетной записи пользователя, имеющего право доступа в Интернет, перестартовать этот прокси. А затем указать в параметрах конфигурации apt данные локального сервера (адрес 127.0.0.1 и порт, выбранный при установке).

Обновление версии сервера

Описанная ранее процедура обновляет установленные программы, но делает это в пределах текущей версии сервера. Если в Сети доступны новые версии Ubuntu, то для перехода на них необходимо выполнить команду

```
sudo do-release-upgrade
```

> ***Примечание***
>
> Обновление на новую версию можно выполнить и командой `apt-get dist-upgrade`, но разработчик рекомендует осуществлять эту операцию с использованием `do-release-upgrade`.

На практике обновление версии сервера является достаточно критичной операцией, после выполнения которой могут возникнуть проблемы в работе прикладных приложений. Поэтому такой переход требует предварительного тестирования и не выполняется без подготовки на рабочих серверах.

Ускорение запуска программ

В операционных системах часто реализуют технологию кэширования данных, которая позволяет ускорить повторный запуск приложения. В Windows данная технология встроена (prefetch) и на практике обычно не нуждается в настройках со стороны администратора.

Для того чтобы реализовать аналогичную технологию для Ubuntu (обеспечить предварительную загрузку в память наиболее часто используемых данных), достаточно установить пакет preload:

```
apt-get install preload
```

Этот пакет анализирует статистику запуска программ и на основе этих данных обеспечивает загрузку необходимых компонентов в память системы. Настройки по умолчанию (/etc/preload.conf) обеспечивают достаточный уровень оптимизации, но желающие могут попытаться подрегулировать их, используя описания справочной подсистемы.

Регулировка приоритетов приложения

В Windows регулировка приоритета запущенного приложения (иными словами, регулировка использования ресурсов приложением) доступна через **Диспетчер за-**

дач регулировкой приоритета процесса. При этом вас сразу предупреждают о возможных проблемах в работе такого приложения. Если администратор уже до запуска приложения хочет использовать для него другой приоритет, то можно стартовать приложение с использованием команды `start` с одним из ключей: `/LOW`, `/NORMAL`, `/HIGH`, `/REALTIME`, `/ABOVENORMAL`, `/BELOWNORMAL`.

Для серверных платформ Windows регулировка предоставления ресурсов приложению возможна также посредством **Диспетчера системных ресурсов** (этот компонент по умолчанию не установлен, его следует включить в **Диспетчере сервера**). Используя **Диспетчер системных ресурсов**, можно регулировать выделение ресурсов процессора и памяти конкретному приложению, задавать приоритеты предоставления ресурсов и т. д.

При этом следует учесть, что практически **Диспетчер системных ресурсов** не будет оказывать влияния, если загрузка процессора приложением составляет менее 70%. Иными словами, применять диспетчер следует только для лимитирования приложений, генерирующих высокую нагрузку системы.

Использование данного ресурса не представляет особой сложности: вам необходимо выбрать приложение и указать для него все параметры политики регулирования ресурсов.

В случае Linux возможности регулировки предоставления ресурсов приложениям существенно выше. Во-первых, упомянем о команде `nice`, которая позволяет запускать приложения с тонкой настройкой приоритетов: от –20 (самый приоритетный процесс) до 19 (самый низкоприоритетный). Например:

```
nice -n 19 приложение
```

Для уже запущенного приложения приоритет можно изменить командной `renice`:

```
renice 19 -p 1234
```

где 1234 — PID соответствующего процесса (можно уточнить командой `ps`). Это вполне безопасное изменение приоритета, которое не приведет к ошибкам приложения.

Помимо регулирования выделения процессорных ресурсов, можно использовать средство управления операциями ввода-вывода `ionice`, которое позволяет планировать запускаемый процесс в нескольких классах (1 — режим реального времени, 2 — нормальный режим, 3 — только в режиме простоя) и использовать несколько приоритетов. Например, так можно запустить процесс резервного копирования с низким влиянием на полезную производительность системы:

```
ionice -c2 -n7 backup.sh
```

> ***Примечание***
>
> В данной утилите возможны приоритеты только с 0 до 7, для режима простоя возможность указания приоритетов отсутствует.

Проблемы совместимости ПО разных версий Windows

Новые версии операционных систем неизбежно имеют особенности, препятствующие запуску в них версий программного обеспечения, разработанных для предыдущих выпусков. Только промышленная операционная система Solaris может "похвастаться" тем, что официально поддерживает работоспособность программ, выпущенных ранее (начиная с версии 2), в новых выпусках (текущая версия Solaris — 11).

Проблемы совместимости обострились с выходом Windows 7/Server 2008, в которой присутствует ряд серьезных модификаций кода. Прежде всего, это новые требования безопасности (контроль учетных записей пользователей, новая библиотека аутентификации, запрет использования сеанса "0" для пользователя системы и т. п.).

При обнаружении известных проблем совместимости в операционной системе автоматически запускается мастер, который пытается внести некоторые настройки в окружение ПО и добиться его работы. Его можно запустить вручную, если выделить файл приложения и открыть его меню свойств (щелкнуть правой кнопкой мыши). После этого появится окно мастера операций, который проведет вас через несколько шагов и попытается настроить запуск программ. Встроенный в Windows 7 мастер совместимости обладает весьма скромными возможностями, например, даже не позволяет задействовать режим совместимости с Windows XP.

Более расширенной функциональностью обладают специализированные продукты. Выпущены различные инструменты для разработчиков (от Microsoft — Application Compatibility Toolkit, **http://www.microsoft.com/download/en/details.aspx?id=7352**, пример решения другого вендора — AdminStudio Application Compatibility Pack и т. д.). Эти продукты позволяют протестировать пакеты на наличие проблем совместимости и выдать рекомендации по их исправлению. Например, Application Compatibility Toolkit может провести анализ работы программного обеспечения и подготовить — если это оказывается возможным — пакет исправлений, обеспечивающий использование купленного программного обеспечения в новых версиях Windows. Эти исправления могут быть распространены через сценарий входа в систему или групповые политики. Соответствующие файлы также готовятся данным пакетом.

Однако использование этих инструментов не может гарантировать возможность нормальной работы программного обеспечения. Если ваша программа работала в Windows XP или предыдущих версиях и не доступна в Windows 7/Server 2008, то практически единственным способом решения является запуск ее в виртуальной машине, в которой операционной системой установлена соответствующая версия Windows.

Владельцам Windows 7 бесплатно доступен так называемый режим Windows XP (XP Mode). Но файлы установки не входят в состав дистрибутива Windows 7, их нужно загрузить с сайта Microsoft. Практически вы должны установить у себя Virtual PC и подключить к ней образ Windows XP, загруженный с сайта Microsoft.

Подробности можно прочитать по ссылке **http://windows.microsoft.com/ru-RU/windows7/install-and-use-windows-xp-mode-in-windows-7**.

Поскольку автор предпочитает виртуальную машину Virtual Box, как более функциональную и менее требовательную к ресурсам, то осмелюсь посоветовать после загрузки файлов не выполнять установку, а разархивировать их на диск и подключить файл образа диска к Virtual Box. Обратите внимание, что в архиве файл образа диска не имеет расширения имени vhd, но его легко определить по объему и подключить в качестве существующего диска гостевой системы. После этого вы сможете запускать необходимые приложения и обмениваться данными с основной системой, например, используя общие папки виртуальной машины.

Установка программ Windows из сети

В Windows предусмотрен вариант централизованной установки программ из сети с использованием групповых политик.

Особенности установки через групповые политики

Какие особенности данного решения стоит отметить? Во-первых, с использованием групповых политик практически невозможно планировать его установку. При использовании групповой политики установить или деинсталлировать приложение можно только при следующей загрузке системы. Поэтому практически невозможно организовать массовое обновление приложения, например, в ночное время, когда нагрузка на сеть минимальная. В таких ситуациях необходимо применять коммерческие решения.

Во-вторых, поддерживаются только MSI- и ZAP-установщики. Поскольку не все программы используют эти установщики, то соответствующие продукты не смогут быть установлены через групповые политики.

В-третьих, администратор практически не имеет возможности управления порядком установки приложения. При добавлении нового приложения в объект групповой политики, оно устанавливается последним.

В-четвертых, сам процесс установки приложений невозможно контролировать. У администратора нет штатного механизма получения сообщений о возможных неисправностях в процессе установки приложения.

Публикация и назначение приложений

Другая особенность использования групповой политики касается режимов установки: *публикация* или *назначение*. *Опубликованные* программы по умолчанию просто появляются в перечне задач, которые можно установить через задачу **Установка/удаление программ** в Панели управления. В случае использования *назначенных программ* в системе в меню **Пуск** появляется ярлык к ним, при первом вызове программы через который осуществляется установка соответствующего программного обеспечения.

Установка на компьютер и для пользователя

Установка программ может быть включена в политику как в раздел **Компьютер**, так и **Пользователь**. В первом случае установка программ будет проведена на систему, они будут доступны для любого пользователя.

Обратите внимание, что программы, установленные в режиме *для пользователя*, обычно не могут быть обновлены с помощью средств автоматического обновления программного обеспечения. Также следует учитывать возможность работы подобного пользователя на терминальном сервере. В этом случае администратору следует либо дорабатывать политику ограничений для терминального сервера, либо включать опцию `lookback` для того, чтобы исключить установку программ на терминале.

> ***Примечание***
>
> Если политика предусматривает установку программного обеспечения *для компьютера* из общей сетевой папки, то доступ к такой папке будет осуществляться от имени компьютера. При назначении прав доступа обратите внимание, что учетные записи компьютеров не входят в группу пользователей домена, а являются только членами группы компьютеров домена. Поэтому следует разрешить доступ к подобным общим папкам, по крайней мере, учетным записям, прошедшим проверку (аутентифицированным пользователям).

Подготовка ZAP-файла

ZAP-формат используется для продуктов третьих фирм и является текстовым файлом с описанием особенностей предполагаемой установки. Формат файла приведен в документе KB231747. Мы просто процитируем часть данной статьи с рекомендациями по созданию соответствующих строк. По приведенному образцу читатель легко сможет создать ZAP-файл для любой программы.

```
[Application]
; .
; Обязательны только параметры FriendlyName и SetupCommand,
; остальные — опциональны

; FriendlyName — имя, которое будет отображаться
; в списке установленных программ
FriendlyName = "Microsoft Excel 97"

;
; SetupCommand — командная строка установки с параметрами
; Длинные пути должны заключаться в кавычки
SetupCommand = "\\server\share\long _folder\setup.exe" /unattend
; Версия программы (опционально)
DisplayVersion = 8.0
; Разработчик программы (опционально)
Publisher = Microsoft
```

Установка программ в Linux

Новые программы в Ubuntu можно устанавливать как из исходных файлов, так и из специально подготовленных пакетов.

Установка приложений из репозиториев

Подготовленный пакет не потребует от пользователя никаких дополнительных операций: достаточно просто получить на локальный диск системы нужный файл и запустить его установку. Дополнительные программы загружаются из Интернета с официальных сайтов, которые прописаны в настройках программы. В некоторых случаях от вас может потребоваться откорректировать этот список или же явно выполнить загрузку файла.

Установка новых пакетов и удаление ненужных выполняется при помощи команд `apt-get` и `aptitude` (далее приведено их описание). Для установки новой программы следует выполнить

```
apt-get install <имя_программы>
```

Для удаления пакета нужно использовать команду

```
apt-get remove <имя_программы>
```

> ***Примечание***
>
> Команда `apt-get` фактически является надстройкой над утилитой управления пакетами `dpkg`. При помощи `dpkg` вы можете получить существенно больше информации по конкретному пакету при необходимости. Например, `dpkg -s apache2` выведет на экран полную версию об установленном в системе веб-сервере.

Если инсталлируемый пакет требует предварительной установки других программ, то `apt-get` выведет соответствующее сообщение и загрузит все дополнительные пакеты.

В качестве источника пакетов обычно выбирается Интернет, тем более что объем пакетов установки невелик — обычно несколько сотен килобайт. Но если вы хотите установить программу с компакт-диска, то для этого необходимо включить данный диск в число источников пакетов командой

```
sudo apt-cdrom add
```

Перечень узлов, с которых система загружает обновления, содержится в файле /etc/apt/sources.list. Обычно менять его не следует, но иногда может потребоваться добавление новых путей. Например, чтобы иметь возможность автоматически устанавливать пакеты, подготовленные фирмой Oracle, следует в этот файл добавить такую строчку:

```
deb http://oss.oracle.com/debian unstable main non-free
```

Описание подобных изменений и дополнительных действий обычно доступно в соответствующих руководствах.

Примечание

Например, при добавлении в репозитории сайта Oracle рекомендуется скопировать на систему параметры его цифровой подписи, чтобы контролировать идентичность загружаемого файла:

```
wget http://oss.oracle.com/el4/RPM-GPG-KEY-oracle -O | sudo apt-key add.
```

После добавления ссылки на новый репозиторий необходимо обновить данные командой

```
apt-get update
```

Многие пакеты содержат в своем названии номер версии. Поскольку это значение обычно заранее не известно и правильно указать имя пакета в командной строке программы `apt-get` не удается, то для получения точного названия следует воспользоваться поиском. Сделать это можно как в программе `aptitude`, так и простой операцией поиска по кэшу пакетов:

```
apt-cache search <ключевое_слово>
```

В качестве параметров команды установки можно указать сразу несколько пакетов, все они будут последовательно загружены из сети и установлены в систему:

```
sudo apt-get install build-essential linux-headers-2.6.24-19-server
libncurses5-dev
```

В Ubuntu существует и другая команда для установки программного обеспечения, отличающаяся от `apt-get` наличием псевдографического интерфейса (в режиме консоли). Это `aptitude` (рис. 2.15). Кроме удобного представления пакетов (в древовидной форме) программа позволяет легко осуществить поиск пакета, увидеть

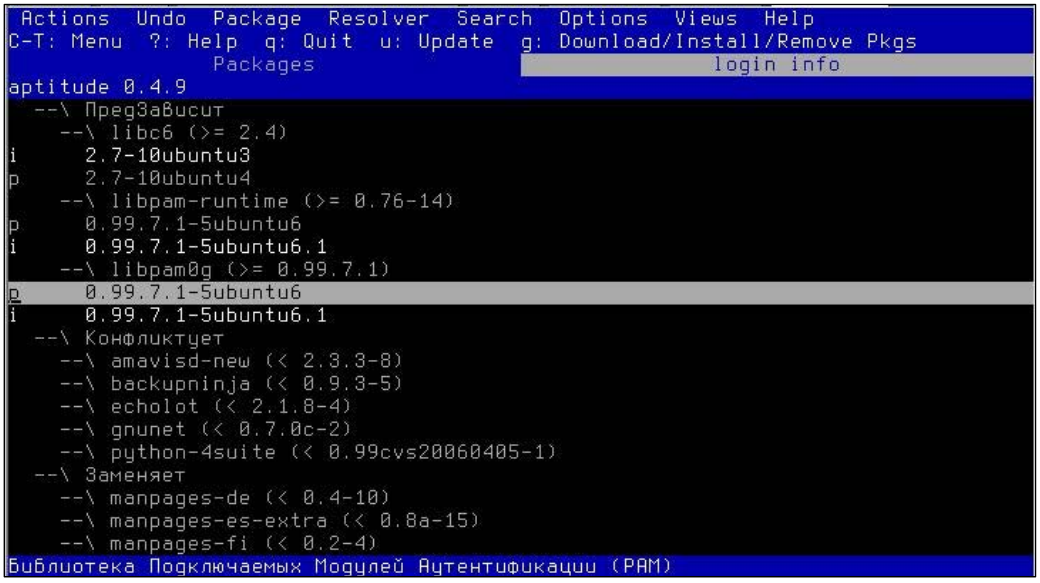


Рис. 2.15. Утилита `aptitude`

в этом же окне зависимости пакета и названия пакетов, с которым конфликтует данное программное обеспечение, и т. д.

Выбор той или иной команды для установки определяется только предпочтениями пользователя.

Программы `apt-get` и `aptitude` устанавливают пакеты с возможностью загрузки их из Сети. Если пакет уже скопирован на диск системы, то для его установки следует использовать команду `dpkg`:

```
dpkg -i <имя_пакета>
```

Эта команда позволяет также отобразить на экране список установленных пакетов — достаточно выполнить команду

```
dpkg --get-selections
```

В качестве параметров можно указать шаблоны для отображения только определенных пакетов.

> ***Примечание***
>
> Список всех установленных пакетов можно вывести командой `dpkg -l`, но вывод этой команды весьма объемен, поэтому лучше провести поиск указанным способом. Заметьте также, что если сохранить вывод этой команды в файл, то потом можно перенести список установленных пакетов на новую систему командой `dpkg --set-selections`, после чего установка пакетов должна быть произведена командой `dselect` (сам пакет dselect необходимо сначала установить).

Переконвертация пакетов

Бывает, что нужно установить пакет, подготовленный для другого клона Linux. Например, много пакетов подготовлено в формате RPM (для Red Hat Linux). Существуют технологии *переконвертации* установочного пакета из одного формата в другой. В Ubuntu для этого используется программа `alien` (`apt-get install alien`). Установка потребует загрузки ряда дополнительных пакетов (например, у автора объем загрузки был около 18 Мбайт). После установки конвертация осуществляется следующим образом:

```
alien -d <имя_пакета.rpm>
```

После выполнения этой команды на диске появится пакет в формате Debian, который можно будет установить командой `dpkg`. Установку пакета можно провести за один шаг вместе с конвертацией, если указать ключ `-i`. Однако автор предпочитает разбивать подобные операции на несколько шагов для удобства работы с ошибками.

Установка программ Linux из исходных кодов

В "нормальных условиях" следует стремиться к установке программ из специально подготовленных пакетов. Однако в некоторых случаях может возникнуть ситуация, когда программу необходимо будет собрать из исходных кодов. В этом случае на компьютере предварительно следует установить компилятор. Целесообразно ин-

сталлировать не только сам компилятор, а сразу весь комплект утилит *build-essential*:

```
sudo apt-get install build-essential
```

Прикладные программы, которые вы захотите установить, могут потребовать наличия связанных пакетов.

Установка программ из исходных кодов выполняется в несколько этапов:

1. Загрузка исходных кодов с сайта и разархивирование их.
2. Запуск программы конфигурирования.
3. Компиляция пакета командой `make`.
4. Установка программы командой `make install`.

Для загрузки кода обычно используется команда `wget`:

```
wget путь_к_файлу_на_сайте
```

Обычно для хранения исходных кодов в Ubuntu применяется папка /usr/src; именно в нее следует сохранять загруженные файлы. Поскольку для записи в нее необходимы права суперпользователя, то в дальнейших примерах мы будем считать, что работа происходит с правами root (например, открыта сессия командой `sudo -s`).

Загруженный файл разархивируется такой командой:

```
tar zxvf программа.tar.gz
```

> ***Примечание***
>
> Перед установкой можно выполнить проверку командой `make check`.

Перед началом установки обязательно следует ознакомиться с файлами README и INSTALL, которые включаются в папку с кодами. В этих файлах описываются особенности установки данного конкретного пакета.

Все последующие команды следует запускать из папки, в которой расположены исходные коды программы. Переходим в папку программы и запускаем ее конфигурирование:

```
cd программа/
./configure
```

На экран будет выведено достаточно много строк. Самое главное, что в итоге вы не должны увидеть сообщений об ошибках, только сообщение примерно такого содержания:

```
configure: Package configured for:
configure: OS type: linux-gnu
configure: Host CPU: i686
```

Если программа сообщит об ошибках, то необходимо устранить вызвавшие их причины.

Примечание

До компиляции пакета в некоторых случаях можно установить опции запуском команды `make menuselect`. В результате выполнения этой команды на экране появится набор опций; выбирая пункты меню, можно устанавливать те или иные параметры.

Для компиляции и установки программы последовательно выполните команды

```
make
make install
```

В итоге их работы программа будет установлена, о чем вы получите соответствующие сообщения в конце работы этих команд.

Если приходится повторно устанавливать программу (например, в случае возникновения ошибок и попыток их устранения), то перед конфигурированием программы следует очистить предыдущие настройки командой

```
make clean
```

Иногда при конфигурировании необходимо задать дополнительные параметры. Такие ситуации разрешаются путем изучения документации и поиска в Сети.

Для некоторых пакетов могут потребоваться дополнительные опции установки. Например, при установке пакета NRPE (из состава пакета Nagios — *см. гл. 11*) требуются дополнительные шаги (`make install-plugin`, `make install-daemon`, `make install-daemon-config`). Необходимость в подобных шагах также уточняется по документации к программе.

Виртуализация приложений

Для использования приложения его совсем не обязательно устанавливать на локальную систему. В настоящее время идет развитие технологии *виртуализации приложений*, которая позволяет запустить программу без установки.

Идея подобного решения заключается в том, что программа запускается в особом окружении. При этом все попытки обращения программы к реестру системы, к ini-файлам, к программным библиотекам перехватываются специальным компонентом и обрабатываются внутри некоего контейнера программы.

Подобный подход имеет многие преимущества. Во-первых, в локальную систему не надо вносить никаких изменений, ставить дополнительные пакеты и т. п. В результате, например, можно запускать одновременно различные версии программы, что часто бывает нужно на практике. Во-вторых, виртуализированные приложения управляются централизованно, а значит, существенно облегчаются проблемы обновления, установки заплат и сервис-паков, контроля лицензий и т. п.

Существует несколько реализаций виртуализации приложений. Если говорить о собственных решениях Microsoft, то это Microsoft Application Virtualization, или App-V, которое доступно для корпоративных подписчиков (входит в состав Microsoft Desktop Optimization Pack). Другие решения — VMware ThinApp, Citrix XenApp, Symantec Workspace Streaming, Novell ZENworks Application Virtualization

и т. п. Подробности использования технологии представлены в Интернете, например, App-V можно начать изучать со ссылки

http://social.technet.microsoft.com/wiki/contents/articles/what-is-microsoft-application-virtualization-app-v.aspx.

Следует заметить, что не каждое приложение может быть виртуализировано. За подробностями следует обратиться к соответствующей технической документации разработчика.

Использование опубликованных приложений. RemoteApp

Другой вариант использования программы без установки на локальную систему заключается в запуске ее на терминальном сервере. Подключение к терминальному серверу можно настроить таким образом, что при открытии сессии автоматически будет запускаться нужная программа, а при ее закрытии будет происходить отключение от терминального сервера. Подобную настройку администраторы обычно использовали для таких пользователей, как бухгалтеры: подключение к терминальному серверу для них воспринималось просто как запуск программы 1С.

Главное, что нужно учитывать при таком варианте работы, — это фактическое расположение ресурсов, которые должна обрабатывать такая программа. Если ресурсы находятся на локальной машине, то необходимо разрешить подключение локальных ресурсов к серверу терминалов и т. п.

Для автоматического запуска приложения в версии терминальных серверов Windows 2000/Windows Server 2003 достаточно в свойствах подключения на вкладке **Программы** указать параметры вызываемой задачи (рис. 2.16).

В Windows Server 2008 возможности настройки удаленных приложений (RemoteApp) расширились. Управление производится через **Диспетчер удаленных приложений RemoteApp служб терминалов** выбором опции **Добавить удаленное приложение** в правой панели навигации. После этого мастер проведет вас через все шаги назначения параметров удаленного приложения. Перечень всех приложений, настроенных для удаленного использования, доступен в нижней части окна оснастки (рис. 2.17).

Перенос настроек приложения в параметры подключения предоставил администраторам дополнительные возможности. Удаленное приложение стало возможным централизованно публиковать или устанавливать: достаточно любым средством (через групповые политики или с использованием специализированного ПО разворачивания приложений, создавая файл установки msi и т. п.) предоставить пользователю файл настроек подключения. Более подробно способы публикации удаленных приложений описаны в онлайновой справке. Кроме того, можно управлять разрешениями на запуск: например, разрешать запуск на терминале только приложений, опубликованных через список RemoteApp.

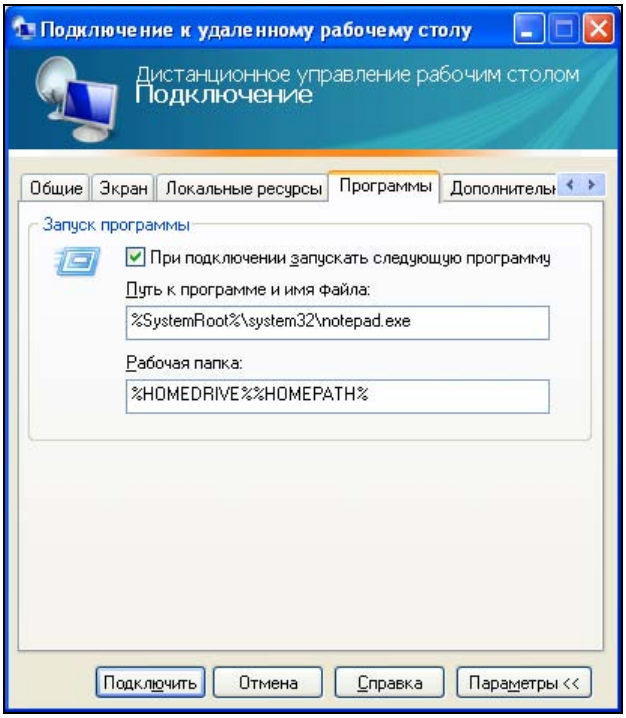


Рис. 2.16. Настройка запуска в терминальной сессии заданного приложения

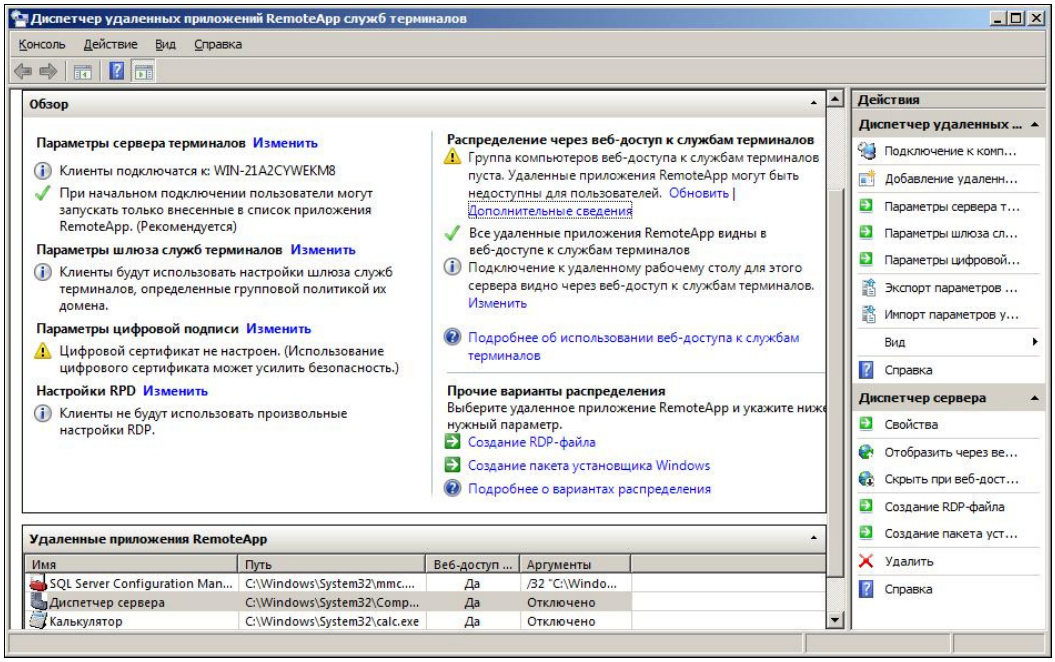


Рис. 2.17. Диспетчер удаленных приложений RemoteApp служб терминалов

Тихая установка программ

"Тихой" (silent) называют такую установку, которая не требует от пользователя ввода каких-либо данных в процессе инсталляции. Поэтому тихая установка может быть полностью выполнена в автоматическом режиме. Это позволяет администратору централизованно устанавливать необходимое программное обеспечение (например, используя сценарии разворачивания, групповые политики и т. п.).

Установочные файлы обычно имеют ключи командной строки, позволяющие выполнить установку в тихом режиме. В этом случае используются настройки установки по умолчанию. К сожалению, синтаксис командных строк инсталляторов различных разработчиков отличается друг от друга.

Стандартным для установочных файлов программ Windows является формат MSI. Формат инсталлятора подробно описан разработчиком и фактически является открытым стандартом. Для файлов в этом формате предусмотрен ключ тихой установки `/q`. При этом следует применять следующий синтаксис запуска (в примере также использован ключ `/n`, наличие которого позволяет выполнить установку скрыто, без интерфейса пользователя):

```
msiexec /i <имя_файла_дистрибутива.msi> /qn
```

Если стандартный MSI-дистрибутив запускается файлом setup.exe, то следует использовать такую строку:

```
setup.exe /s /v"/qn"
```

Дистрибутивы, подготовленные с помощью популярного продукта InstallShield, имеют ключ тихой установки `/s`. Тихая установка требует наличия файла ответов. Если он отсутствует в составе дистрибутива, то пользователь может создать его самостоятельно, записав свои действия в качестве варианта ответов во время тестовой установки продукта. Для этого необходимо использовать режим записи ответов с ключом `/r`:

```
setup.exe /r /f1
```

> ***Примечание***
>
> Ключ `/f1` в командной строке можно не указывать. В этом случае файл ответов будет записан по умолчанию в папку Windows и получит имя setup.iss.

По умолчанию файл ответов должен иметь имя setup.iss и располагаться в той же папке, что и setup.exe. В противном случае при запуске "тихой" установки (с ключом `/s`) следует указать путь к нему в ключе `/f1`.

> ***Примечание***
>
> Программа инсталлятора может закрыться раньше, чем установка продукта будет полностью завершена. Если вы используете последовательность сценариев установки, то это может привести к ошибке их выполнения. В такой ситуации следует добавить ключ `/sms`, который заставляет программу инсталлятора ждать полного окончания установки продукта.

В последнее время приобрели популярность так называемые PackageForTheWeb-дистрибутивы (PFTW). Эти пакеты представляют собой один самораспаковывающийся файл, который после разархивирования автоматически запускает программу setup.exe, содержащуюся в этом архиве. Дистрибутивы PFTW допускают использование двух ключей. Ключ `/s` осуществляет "тихое" разворачивание дистрибутива, а ключ `/a` "передает" последующие ключи программе setup.exe. Например, вы можете использовать запуск PFTW с ключами `/s /a /r` для того, чтобы создать файл ответов.

> ***Примечание***
>
> Большая база рекомендаций по развертыванию популярных продуктов (возможные ключи запуска и трансформаций, советы по переупаковке и т. д.) доступна на сайте AppDeploy (**http://www.appdeploy.com/packages/index.asp**).

Переупаковка

Если в программе не предусмотрен вариант "тихой" установки, то администратор имеет все же возможность настроить продукт для установки без запросов. Для этого используется технология *переупаковки* (repackages).

Технология переупаковки заключается в том, что специальная программа контролирует изменения, вносимые установкой на тестовый компьютер: следит за изменениями файловой системы, ветвями реестра, другими параметрами. После чего сравнивается состояние системы до установки программы и после. Все обнаруженные различия анализируются, и создается *новая* программа установки.

Существует и вторая технология, используемая для переупаковки. Это мониторинг процесса инсталляции. Специальная программа следит за всеми действиями процесса установки; например, ею будет замечено любое обращение к реестру системы с целью проверки существования какого-либо параметра. Мониторинг позволяет создать более точный файл переупаковки, но эта технология содержится только в коммерческих версиях программ.

Не все дистрибутивы допускают переупаковку. Во-первых, нельзя переупаковывать сервис-паки (service pack), горячие заплатки и другие продукты, вносящие изменения в операционную систему (например, DirectX). Такие программы могут выполнять специальные процедуры, например, прямое редактирование двоичных файлов, которые не могут быть верно воспроизведены процедурой переупаковки.

Во-вторых, переупаковка продуктов, устанавливающих драйверы устройств, сетевые протоколы и другие системные агенты, часто не приводит к успеху. В-третьих, переупакованный дистрибутив не сможет заменить файлы, защищаемые технологией Windows File Protection. Такие изменения "разрешены" только для программ изготовителя операционной системы.

Переупаковка достаточно просто реализуется при помощи бесплатных утилит. При этом можно включить в один дистрибутив несколько последовательно устанавливаемых продуктов. Кроме того, с помощью переупаковки легко выполнить пользовательские настройки. Для этого нужно до начала анализа запустить на тестовом

компьютере установленную программу, настроить ее и сохранить изменения. Все эти изменения войдут в переупакованный дистрибутив.

Файлы ответов (трансформаций)

Программные пакеты могут включать возможности создания специальных файлов ответов, которые могут быть использованы при их установке. Например, это установка самой операционной системы, установка программ Microsoft Office и аналогичных.

Для прикладных программ наиболее корректным вариантом является формирование файлов ответов (или *трансформаций*, transform, MST-файлы). Преимущество использования MST-файлов состоит в том, что исходный продукт не подвергается каким-либо изменениям в процессе подготовки к развертыванию. При этом файлов трансформаций может быть создано сколь угодно много — для любого варианта установки продукта.

Для подготовки файлов трансформаций необходимо использовать специальные программы. Так, в случае Microsoft Office они должны быть загружены с сайта изготовителя (обычно включаются в состав Resource Kit). При их использовании администратору достаточно выбрать в графическом режиме желаемые параметры установки, чтобы создать файл трансформации.

К сожалению, большинство программ, с которыми приходится сталкиваться на практике, не имеют описаний файлов трансформаций или мастера создания ответов.

Службы системы

Ряд приложений должен запускаться одновременно с включением сервера. Такие программы принято называть *службами* в операционных системах Windows и *демонами* в Linux.

Установка служб Windows

Обычно настройка режима запуска приложения в качестве службы включается в функционал установочного пакета. Но иногда возникает необходимость настроить запуск произвольного приложения в качестве службы.

> ***Примечание***
>
> Обратите внимание, что не все приложения могут быть настроены для работы в качестве службы. Например, приложение не должно нуждаться ни в каких пользовательских операциях после запуска для начала обслуживания запросов и т. п.

В современных версиях Windows для создания службы используется команда `sc`. С ключом `create` она позволяет создать службу, а с ключом `delete` — удалить.

Обратите внимание, что данная команда только настраивает запуск программы в качестве службы. Если программное обеспечение должно быть установлено, то эту

операцию следует выполнить до создания службы. Соответственно, удаление службы только меняет настройки системы, но не удаляет программный продукт из системы.

Для создания службы нужно выполнить:

```
sc [Servername] create Servicename [Optionname=Optionvalue...
```

Servername задает имя сервера, на котором создается служба. Этот параметр можно не указывать при локальном выполнении задания. *Servicename* определяет имя, присваиваемое разделу службы в реестре (учтите, что это имя не соответствует имени, отображаемому в задаче **Службы** Панели управления).

Параметры *Optionname* и *Optionvalue* используются для указания дополнительных параметров службы. Обратите внимание, что между именем параметра и знаком равенства *не должно быть пробелов*. Полный набор параметров доступен из онлайновой справки. Укажем только, что один параметр является обязательным. Это путь к исполняемому файлу службы:

```
binPath=(строка)
```

Остальные параметры можно не указывать, они будут использованы в значениях по умолчанию.

Кроме этого параметра можно определить `DisplayName` — имя службы, которое будет отображаться для пользователя, указать учетную запись, от имени которой должна запускаться служба (если не используется системная учетная запись) и т. д.

В предыдущих версиях Windows команда `sc` отсутствовала. Вместо нее для создания служб можно было использовать утилиту Instrsrv.exe, входящую в состав пакета Windows NT Resource Kit. Эта утилита позволяла устанавливать (и удалять) системные службы, причем для запуска приложения в качестве службы использовалась программа Srvany.exe, которая также устанавливалась в качестве службы Windows.

Синтаксис утилиты был следующим:

```
INSTSRV.EXE Моя_служба путь\SRVANY.EXE
```

Подробности использования этих средств нужно уточнить по документации, которая содержится в Resource Kit (файл Srvany.wri).

Установка демонов в Linux

Для создания демона необходимо выполнить аналогичные шаги: установить программный продукт и настроить его автозагрузку при старте системы. Обычно если устанавливаемый продукт предназначен для использования в качестве демона, то соответствующие операции выполняются автоматически и не требуют дополнительного вмешательства пользователя.

Существует несколько вариантов автоматического запуска демонов в Linux-системах. Для сервера Ubuntu без графического интерфейса "применяется" классический вариант. Файлы, которыми обеспечивается запуск программы, помещаются

в папку /etc/init.d. В папках[1] /etc/rc0.d, /etc/rc1.d и т. д. размещаются файлы, которые выполняются автоматически при запуске или остановке системы (принято такие файлы запуска называть с символа S (от англ. *Start*), а останова — с символа K (от англ. *Kill*); после этого символа указывается число, определяющее порядковый номер запуска/останова). Для запуска службы в эти папки просто помещают ссылки на командный файл запуска в папке /etc/init.d.

Создать ссылки можно вручную, но проще использовать команду `update-rc.d`. Эта утилита автоматически создает ссылки при установке демона или удаляет их в противном случае. Для создания демона достаточно выполнить:

```
update-rc.d файл_запуска defaults
```

С ключом `remove` эта команда удаляет соответствующие ссылки. Следующий пример показывает отключение демона AppArmor:

```
sudo update-rc.d -f apparmor remove
```

Учтите, что сценарии запуска демона, которые находятся в папке /etc/init.d, должны создаваться по определенным правилам, чтобы можно было применять типовые команды для запуска, остановки демона и т. п. Обычно сценарии запуска поставляются вместе с программным продуктом, но если они отсутствуют, то в качестве шаблона можно воспользоваться файлом /etc/init.d/skeleton. Обратите также внимание, что в этих сценариях содержатся указания о зависимости демонов (какие службы необходимо запустить до старта данного демона и остановить в случае завершения его работы). Эти указания обрабатываются командой `update-rc.d`, которая присваивает запускающим сценариям соответствующий последовательный номер старта.

Запуск программ по времени

Достаточно часто администратору приходится настраивать запуск определенных программ по расписанию.

Настройка расписания запуска программ в Windows

В Windows для настройки запуска программ по расписанию используется задача **Администрирование | Планировщик заданий**. Эта задача снабжена мастером операций (**Создать простую задачу...**), который помогает настроить расписание для выполнения задания. Более опытные администраторы могут использовать ссылку **Создать задачу**, при переходе по которой появится окно свойств новой задачи, где нужно определить желаемые параметры на всех вкладках.

Последний режим предполагает больше возможностей настройки, например, кроме выполнения заданий по расписанию можно настроить запуск задач при входе в систему любого пользователя, при блокировке компьютера, его выключении, при подключении к конкретной сети и т. п.

---

[1] Эти папки соответствуют уровням запуска Linux.

Подобная настройка не вызывает особой сложности. Главное — выбрать правильные ключи запуска задания, которые позволят задаче выполнить свою работу без какого-либо участия пользователя и корректно завершить работу.

> ***Примечание***
>
> Если вы не уверены в правильности ключей, обязательно включайте параметр принудительного завершения задания после истечения некоторого периода ее выполнения.

Выполнение заданий по расписанию в Linux

В Linux за запуск задания в нужное время отвечает специальная программа — `cron`, которая устанавливается по умолчанию при инсталляции системы. Существуют различные способы настройки задания на периодическое выполнение.

Для заданий, которые надо выполнять просто с некоторой периодичностью, например раз в час или в день, достаточно поместить сценарии запуска в папки[1] /etc/cron.daily, /etc/cron.hourly, /etc/cron.monthly, /etc/cron.weekly. Файлы, находящиеся в этих папках, будут запускаться с соответствующей периодичностью (раз в день, в час, в месяц, в неделю соответственно).

Другой способ назначения заданий состоит в использовании утилиты `crontab`. Она позволяет просмотреть существующие задания (ключ `-l`), удалить все задания (`-r`) или перейти в режим непосредственного редактирования расписания. Для этого нужно выполнить

```
crontab -e
```

> ***Примечание***
>
> Список заданий с помощью `crontab` создается для каждого пользователя. Если администратору необходимо создать задание, которое будет исполняться от имени другого пользователя системы, то следует воспользоваться командой `crontab -u <имя> -e`.

Команда открывает файл настроек, в который нужно ввести необходимые параметры, указываемые в одной строке в следующем порядке:

```
минуты часы дни месяц день_недели команда
```

Первые параметры определяют, когда должна быть запущена команда, определенная в конце этой строки. Вы можете указывать:

- точное значение (например, для минут значения от 0 до 59, часов — от 0 до 23 и т. п., дни недели — от 0 до 6 (воскресенье имеет номер 0));
- `*`, если команда должна быть выполнена при любом значении данного параметра;
- несколько значений (например, `15,30` — для минут) через запятую;
- диапазон (например, если нужно выполнять команду только в первые три месяца, то можно указать `1-3`);

---

[1] Существует еще папка /etc/cron.d, в которой хранятся файлы в традиционном для `cron` формате определения периодичности запуска. Можно использовать ее, но более удобно выполнять настройки способом, указанным далее (через `crontab`).

- периодичность (`*/2` означает выполнение, например, каждый второй час, если это указано для определения часов).

Кроме того, возможно применение специальных названий: `@reboot` — для выполнения при каждой загрузке; `@yearly` или `@annually` — для выполнения один раз в год (первого числа в 0 часов 0 минут); `@monthly`, `@weekly`, `@daily` или `@midnight`, `@hourly` — соответственно, для запуска 1 раз в месяц, неделю, день, час (в этом случае в строке останется только это название и команда).

> ***Примечание***
>
> Можно также указывать сокращенные английские названия, например, jan, feb, mon, tue и т. п. Подробности можно уточнить в документации.

После команды можно указывать комментарий, который должен начинаться с символа `#`. Можно включить запуск нескольких команд, перечислив их через точку с запятой или использовав операторы условного выполнения (`&&` или `||`), которые определяют необходимость запуска последующей команды в зависимости от результата предыдущей.

По завершении определения команд нужно сохранить файл (выполнить команды управления используемого редактора, которые отражаются на экране).

Приведем примеры возможных записей таких заданий (листинг 2.3).

Листинг 2.3

```
30 15 * * * <команда>
# Команда запускается каждый день в 15 часов 30 минут
0 0-11/2 01 05 * <команда>
# Команда запускается каждый второй час первого мая
@monthly <команда>
# Команда запускается первого числа каждого месяца в 0 часов 0 минут
```

Выполнение заданий с помощью `cron` происходит в собственном окружении, в котором отсутствуют определения различных системных переменных, в том числе переменных пути, локализации и т. п. Поэтому при планировании заданий с использованием `cron` в расписании необходимо указывать полный путь к исполняемому файлу команды. Например, для выключения компьютера следует указывать не просто `shutdown`, а `/sbin/shutdown` с последующими ключами. А если назначенная к выполнению по графику команда задействует какие-либо языковые настройки (например, программа формирования отчета прокси-сервера free-sa и т. п.), то их следует определить в параметрах запуска команды либо задать соответствующие переменные среды в запускающем сценарии.

ГЛАВА 3

Сетевая инфраструктура

Недостаточное внимание к качеству сети передачи данных может привести к постоянным проблемам при эксплуатации информационной системы.

Строение сети передачи данных

Практически все сети предприятий сегодня базируются на технологии Ethernet и протоколе TCP/IP. Наличие других протоколов, как правило, наследовано исторически и обусловлено эксплуатируемым оборудованием.

Рассмотрим, что необходимо знать системному администратору при работе и модернизации таких сетей.

Размеры сегментов сети

Длина медного кабеля от одного элемента активного оборудования до другого, например от компьютера до коммутатора, в сети Ethernet не должна превышать 100 м. Обычно стандартами предусмотрена максимальная длина самого кабеля 90 м, а 10 м отводится на соединительные кабели.

> ***Примечание***
>
> На практике длина патч-кордов обычно составляет 1 м и более. Обратите внимание, что не имеет смысла применять самодельные короткие патч-корды, например, для подключения сервера к патч-панели, если оба этих элемента расположены рядом ("фирменные" кабели не могут быть короче ~ 60 см). При малой длине кабеля увеличивается уровень помех, возникающих при отражении высокочастотных сигналов от точки соединения кабеля и розетки. Это может привести к увеличению числа ошибок в линии.

В реальных сетях еще сохранились концентраторы *(хабы)*. Для локальной 10-мегабитной сети, построенной на концентраторах, существует правило "5/4" — между любыми двумя сетевыми устройствами должно быть не более пяти сегментов сети с четырьмя концентраторами. При этом размер сети, построенной на витой паре, ограничен величиной 500 м. Ограничение на длину обусловлено самой природой

Ethernet, принципами, на которых строится такая сеть, и не зависит от совершенствования элементной базы.

Хотя в 100-мегабитной сети обычно используются только коммутаторы, на практике в ряде организаций эксплуатируются и концентраторы. Стандартом предусмотрено в этом случае наличие не более *двух* концентраторов с расстоянием между ними не более 5 м.

При необходимости соединения устройств, отстоящих друг от друга на расстоянии свыше 100 м, используются волоконно-оптические линии связи. На небольших расстояниях (порядка 100—300 м) применяются *многомодовые* оптические кабели. Длины сегментов определяются параметрами оптических приемников и передатчиков. (Эти значения отличаются от вендора к вендору и не всегда соответствуют параметрам стандартов.) Стоимость прокладки и эксплуатации такой линии практически соизмерима со стоимостью линии на витой паре. Для длинных соединений предназначен *одномодовый* оптический кабель. Соответствующее оборудование для одномодового кабеля (приемники и передатчики оптического сигнала) в несколько раз дороже, чем модели для многомодовой технологии.

Поскольку на практике эксплуатируются различные технологии, при проектировании расширения сети следует обращать внимание на совместимость использованных решений. Так, например, необходимо учитывать типы оптических разъемов, которые могут отличаться на оборудовании различных вендоров. Нужно принимать во внимание тип оптического кабеля (выпускаются более чем по пяти стандартам), длину волны и т. п.

> ***Примечание***
>
> Некоторые вендоры требуют использования, например, медиаконверторов (SFP-модулей) только собственного изготовления и контролируют тип оборудования на уровне прошивок коммутаторов. В большинстве случаев такие ограничения не имеют под собой оснований. Не представляет особой сложности приобрести модули с "исправленной" конфигурацией (которые "примут" коммутаторы) по цене раз в 5—10 дешевле оригинальных моделей.

Выбор типа коммутаторов

В небольших сетях (и в больших на уровне доступа) традиционно задействуют коммутаторы второго уровня по модели OSI. Коммутаторов данного класса обычно достаточно для организации сети с не очень большим числом компьютеров — в одну-две сотни. Точно назвать границу, когда необходимо уже применять коммутаторы третьего уровня, сложно. Это зависит от специфики организации (имеющихся сетевых сервисов, реальной загрузки сети, наличии трафика реального времени — IP-телефонии и видеоконференций и т. д.). Коммутаторы третьего уровня нужны для того, чтобы разделить сеть на несколько независимых друг от друга сегментов. При этом передача информации из одного сегмента в другой осуществляется путем маршрутизации на коммутаторе третьего уровня.

Коммутаторы лучше приобретать управляемые. Это обеспечит гибкость в настройке сети. Если в сети предполагается использование сервисов реального времени, то

коммутаторы должны поддерживать режимы управления качеством передачи (QoS) и, по возможности, реализовывать режим гарантированного предоставления полосы пропускания.

Топология сети передачи данных

На практике компьютерную сеть пытаются сначала строить по какому-нибудь проекту, а потом, по мере развития организации, подключают новые коммутаторы, и структура принимает достаточно хаотичный вид. Если администратор не контролирует развитие сети, часто формируются каскады из четырех-пяти последовательно включенных коммутаторов, что неизбежно ухудшает качество системы передачи данных.

Администратору нельзя выпускать развитие сетей передачи данных из-под своего контроля: в любой момент он должен знать, как соединены между собой коммутаторы, и быть уверенным, что ни к одному порту не подключено неизвестное ему оборудование.

При построении сети внутри здания обычно придерживаются иерархии связей "здание — этаж — рабочее место": на этажах устанавливают коммутаторы уровня доступа, к которым подключают рабочие места пользователей, после чего эти коммутаторы соединяют каналами связи с коммутатором (или коммутаторами) на каком-либо этаже, который играет в этом случае роль *ядра* сети.

Традиционной проблемой большинства организаций является документирование своей кабельной подсистемы. Специализированные программные продукты, позволяющие поддерживать схемы сети и оперативно учитывать вносимые в нее изменения, стоят весьма дорого, а исходная документация быстро становится неактуальной после нескольких перемещений сотрудников и прокладки дополнительных каналов связи.

Существует много программ, которые анонсируют автоматическое построение топологии сети. По опыту автора более-менее верная топология будет построена только в случае наличия коммутаторов одного вендора и достаточно простой конфигурации (минимум виртуальных сетей, виртуальных маршрутизаторов и т. п.). На практике инфраструктура обычно содержит разнородные модели коммутаторов, что существенно осложняет выполнение задачи. Так, на рис. 3.1 показана автоматически сформированная топология сети, созданной на основе двух марок управляемых коммутаторов. Видно, что даже коммерческая программа (использовалась триальная версия пакета HP iMC) показала сеть состоящей из двух независимых сегментов (см. автономный блок из 4 хостов в правом верхнем углу) и не обнаружила нескольких коммутаторов.

Лучший способ построения схемы сети — это использовать триальные версии коммерческих продуктов (так, упомянутый пакет имеет срок тестирования в 60 суток), которые потом доработать вручную по имеющимся данным и визуальному осмотру оборудования.

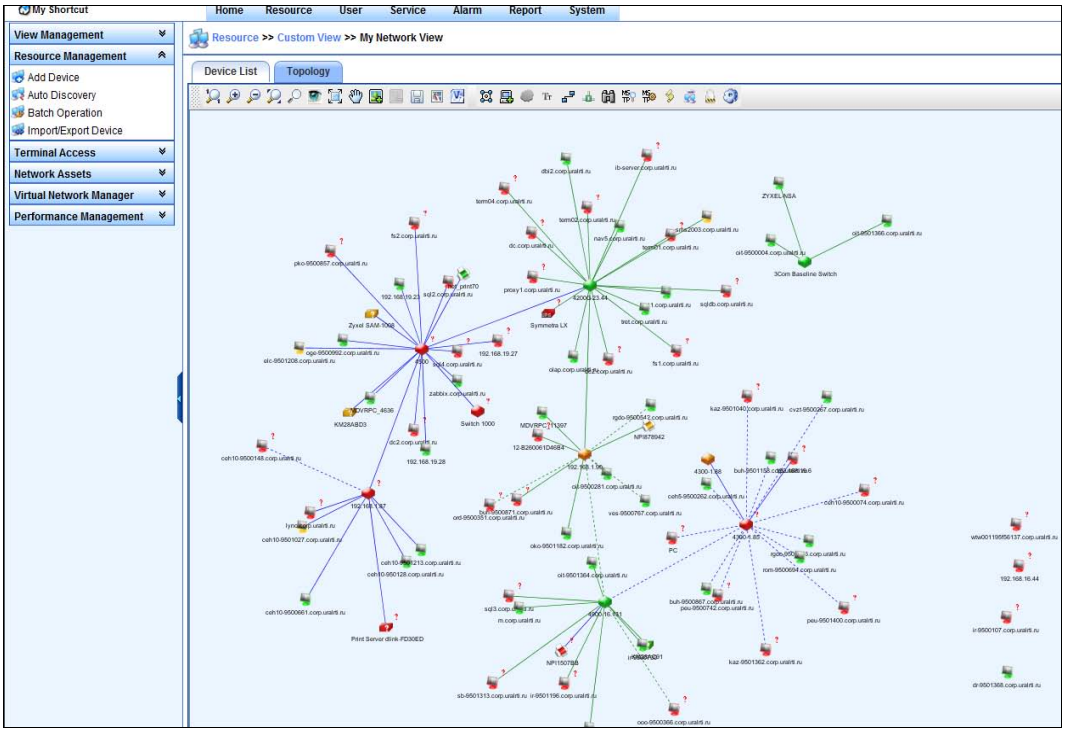


Рис. 3.1. Топология реальной сети, автоматически выполненная пакетом HP iMC

Совет

При необходимости найти и загрузить программу, выполняющую построение схемы сети, можно, если выполнить поиск по ключевым словам *network monitoring tool*.

Ищем точку подключения компьютера

Точку подключения компьютера к порту коммутатора можно определить только в пределах текущего сегмента сети (одной VLAN). За пределами данного сегмента вам будет доступна информация только о том, в какой сети (за каким маршрутизатором) находится этот компьютер.

На практике в небольших организациях часто, несмотря на все рекомендации, отсутствует актуальная схема сети, поэтому поиск точки подключения устройства требует много усилий. Чтобы найти, к какому коммутатору подключен компьютер, следует искать устройство, в таблице MAC-адресов которого зарегистрирована сетевая плата соответствующего компьютера. Такая информация доступна только с управляемых коммутаторов.

Примечание

Существуют программы, позволяющие найти маршрут подключения искомого устройства через все коммутаторы сети. Но они эксплуатируются преимущественно в крупных организациях с разветвленной сетью.

Последовательность действий такова. Сначала определите MAC-адрес устройства, точку подключения которого вы хотите найти. Это значение становится известным для локальной системы после того, как с ним происходили какие-либо сетевые операции. Быстрее всего выполнить команду `ping` на IP-адрес компьютера. После получения ответа посмотрите таблицу `arp`-кэша локальной системы, в ней должна содержаться запись об удаленном MAC-адресе (листинг 3.1).

Листинг 3.1

```
>arp -a
Интерфейс: 192.168.29.100 --- 0x4
Адрес IP       Физический адрес     Тип
192.168.29.1   00-1e-58-81-a0-89    динамический
```

MAC-адрес устройства отображен в столбце `Физический адрес`.

Точно такие же команды следует выполнить и на компьютерах Ubuntu, только вывод на экран результатов будет представлен немного по-иному. Хотя лучше вызвать команду `arp` без параметров (листинг 3.2).

Листинг 3.2

```
# arp
Address           HWtype    HWaddress           Flags Mask  Iface
192.168.32.120    ether     00: C0:9F:3F: D8:13   C          eth0
192.168.177.85    ether     00: 0D:28:F9:5D:80    C          eth1
```

В этом листинге MAC-адрес устройства показан в столбце `HWaddress`.

После того как вы узнали MAC-адрес устройства, нужно найти его в таблице MAC-адресов на коммутаторе. Для этого необходимо подключиться к коммутатору одной из программ управления и выполнить поиск по этому значению (рис. 3.2).

На рис. 3.2 представлен графический интерфейс управления коммутатором 3Com4200G с отображением таблицы зарегистрированных MAC-адресов. Видно, что на некоторых портах имеются записи по нескольким MAC-адресам (например, на первом гигабитном порту). Это говорит о том, что данный порт является магистральным: через него коммутатор подключен к другому коммутатору, и устройство нужно искать на удаленной системе.

Если на том порту коммутатора, на котором вы найдете зарегистрированным искомый MAC-адрес, есть еще MAC-адреса, значит, к данному порту подключен другой коммутатор. В этом случае нужно будет подключиться к следующему коммутатору и так по цепочке найти устройство, к которому подключена искомая система.

Примечание

Работая в командной строке, многие операции можно выполнить быстрее. Так, чтобы найти порт на коммутаторе Cisco, к которому подключено устройство с IP-адресом

10.1.1.1, достаточно выполнить следующий запрос: `show arp-inc 10.1.1.1` (первая часть команды получает список известных MAC-адресов, который фильтруется второй частью).

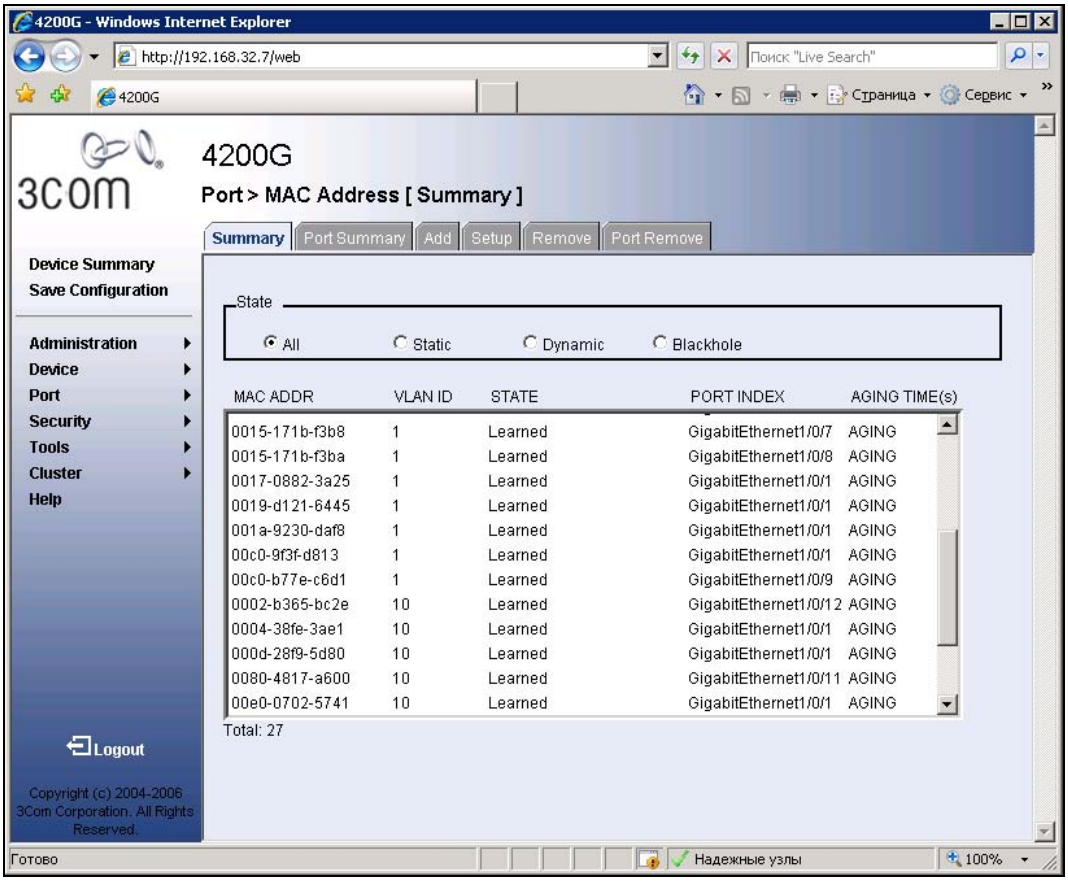


Рис. 3.2. Окно списка найденных на порту коммутатора MAC-адресов систем

Контроль подключения к СКС

Если к вашей сети злоумышленник сможет подключить свой компьютер, то это существенно облегчит ему последующие операции по доступу к коммерческой информации организации. Если организация размещена по нескольким помещениям, то проконтролировать визуально факт подключения администратору невозможно.

Существуют два метода контроля подключаемых устройств. Первый, который поддерживается всеми управляемыми коммутаторами, заключается в контроле MAC-адреса устройства на данном порту. После подключения к порту любого оборудования коммутатор запоминает его MAC-адрес, и каждая последующая попытка другого компьютера (точнее, устройства с другим MAC-адресом) работать через этот порт приведет к блокировке порта. Эта функциональность имеет различные

названия среди вендоров активного оборудования, чтобы ее задействовать, достаточно активировать соответствующую функцию для порта.

Недостатки такого решения состоят, во-первых, в том, что сегодня существует много программных способов смены MAC-адреса компьютера, например, достаточно указать значение соответствующей опции (параметра **Сетевой адрес**) в настройках сетевого адаптера в Windows (рис. 3.3). Во-вторых, блокировка порта резко увеличивает нагрузку на администраторов, поскольку предполагает необходимость ручных операций для возобновления работы в случае замены оборудования и в других штатных ситуациях.

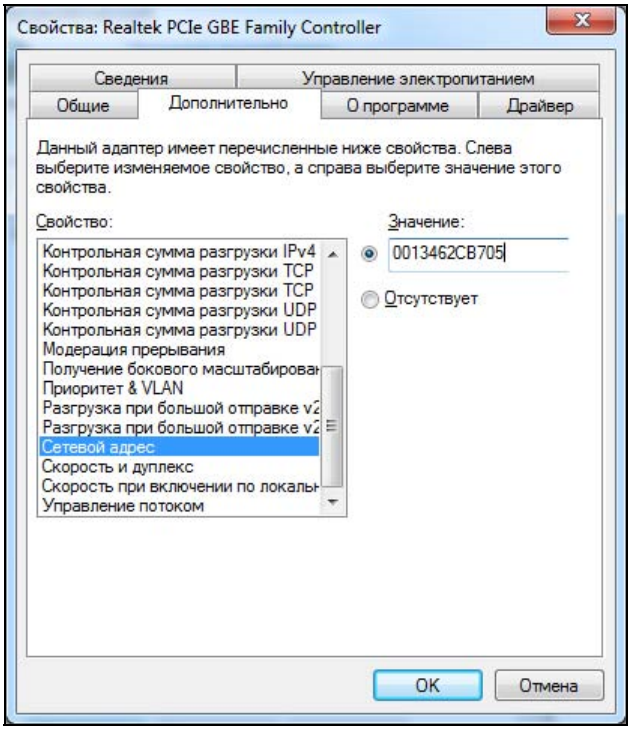


Рис. 3.3. Программная смена MAC-адреса компьютера

Второй метод контроля доступа к локальной сети основывается на протоколе 802.1*x*. Упрощенно схему проверки оборудования с использованием данного протокола можно представить следующим образом (рис. 3.4):

1. При подключении устройства порт коммутатора не пропускает никаких данных в локальную сеть, кроме специальных пакетов аутентификации на заданный в его настройках сервер RADIUS.
2. Сервер RADIUS, получив от устройства необходимые аутентификационные данные, проверяет соответствие их неким параметрам. Обычно используются сертификаты безопасности, выданные контроллерами домена. В этом случае информация проверяется во взаимодействии с сервером сертификатов и сервером службы каталогов.

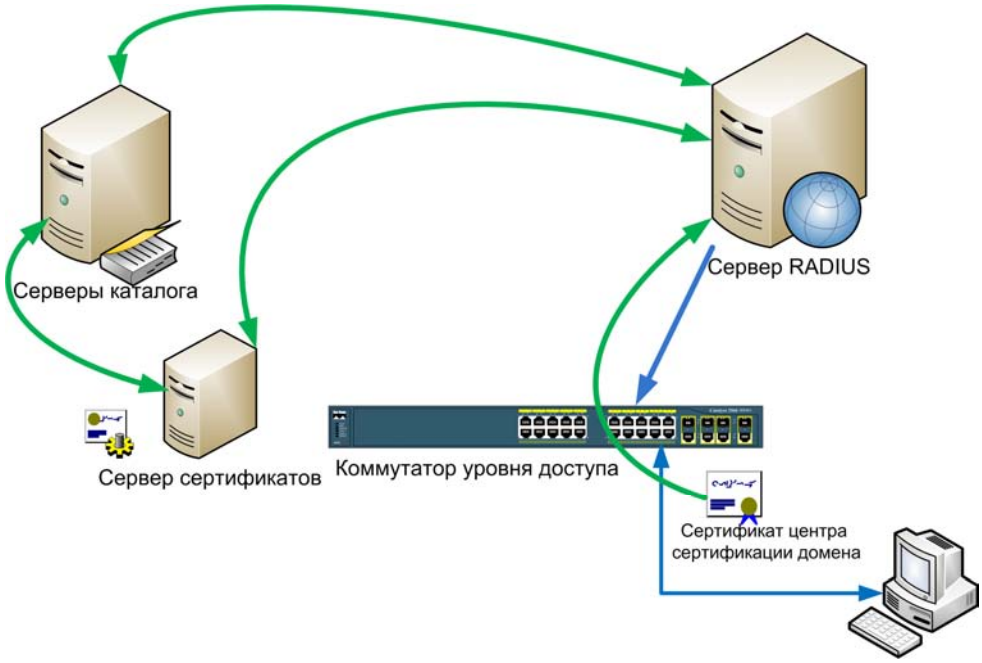


Рис. 3.4. Принципиальная схема взаимодействия компьютера, коммутатора и серверов системы при использовании протокола 802.1*x*

3. В зависимости от результатов проверки сервер RADIUS дает коммутатору разрешение на открытие порта.
4. Коммутатор, получив разрешение, открывает доступ устройству в локальную сеть. Далее, в зависимости от настроек коммутатора, такая проверка может осуществляться периодически через некоторое время, порт может открываться для любых MAC-адресов и т. д.

Сервер RADIUS может не только давать разрешение на открытие порта, но и сообщать коммутатору некоторые данные настройки, например, номер виртуальной сети, в которую должен быть помещен порт этого устройства. Данную функциональность поддерживают не все коммутаторы.

Самая строгая проверка компьютера будет осуществляться по протоколу 802.1*x* с учетом сертификатов, выданных удостоверяющим центром (например, внутренним центром сертификации). Опишем пример настройки коммутатора для такого случая.

Предварительные настройки для использования протокола 802.1*x*

Контроль подключения по протоколу 802.1*x* с использованием сертификатов требует развернутой системы PKI в организации: установленного центра сертификации, наличие процедур выдачи/отзыва сертификатов и т. п. Обычно это реализуется только в достаточно крупных фирмах, тем более что, например, идентификация

сервера RADIUS предполагает получение им самим сертификата, который может быть выдан только сервером сертификации на основе Windows Server Enterprise Edition.

Поэтому в малых организациях можно ограничиться аутентификацией по MD5-откликам. Процедура настройки практически не отличается от описанной далее, за исключением того, что вместо сертификатов нужно выбрать опцию **MD5-отклик** в мастере настройки политик подключения.

Настройка компьютера

Аутентификация на базе протокола 802.1*x* осуществляется службой **Беспроводная настройка**. По умолчанию ее запуск на рабочих станциях установлен в ручной режим. Смените ее на автоматический режим. Далее, с помощью сертификатов можно аутентифицировать как компьютер, так и пользователя. По умолчанию операционная система Windows аутентифицирует пользователя, т. е. до локального входа пользователя на компьютер, работа в сети будет невозможна. Если вы хотите аутентифицировать компьютер, то необходимо в его реестр с помощью команды `regedit`, запускающей Редактор реестра, добавить параметр `HKLM\Software\Microsoft\EAPOL\Parameters\General\Global\AuthMode` со значением 2 и типом `DWORD`.

> ***Примечание***
>
> Эти настройки можно определить централизованно с использованием групповой политики домена.

Настройка домена Windows

Учетные записи, которые будут аутентифицироваться по протоколу 802.1*x*, должны иметь разрешение на входящий звонок в свойствах учетной записи. Обратите внимание, что это касается и учетных записей компьютеров, если вы предполагаете авторизовать их сертификаты. Если вы планируете назначать компьютеры в отдельные VLAN в зависимости от членства в группах безопасности, то в этом случае необходимо создать столько групп безопасности, сколько различных настроек должно передаваться на коммутатор, и включить в эти группы соответствующие учетные записи. Для упрощения администрирования желательно создать групповую политику, предполагающую автоматическую выдачу сертификатов для компьютеров, входящих в домен. Это устранит операции ручного получения сертификатов для учетных записей компьютеров.

Настройка сервера RADIUS

Серверы RADIUS в операционных системах Microsoft носят название **Служба проверки подлинности в Интернете** (входит в состав **Сетевые службы** при выборе опции установки компонентов Windows). Для единообразия в этой книге мы будем называть эту службу сервером RADIUS. Установите RADIUS-сервер на какой-либо системе Windows и зарегистрируйте его в службе каталогов (операция входит в меню свойств сервера IAS). Проверьте, что компьютер с сервером RADIUS включен

в состав группы безопасности RAS and IAS Servers. Установите на сервер сертификат авторизации, предназначенный для серверов RAS и IAS (при ручном запросе сертификата необходимо выбрать соответствующий шаблон в мастере операций).

> ***Примечание***
>
> В Windows 2008 сервер RADIUS включен в состав службы контроля доступа к сети (Network Access Protection, NAP). Для его установки достаточно добавить роль **Службы политики сети и доступа** в **Диспетчере сервера**. Сама настройка протокола 802.1*x* для доступа в локальную сеть принципиально не отличается от описанного далее примера для случая Windows Server 2003.

Добавьте в качестве клиентов сервера RADIUS каждый коммутатор, на котором будет осуществляться авторизация на основе протокола 802.1*x*. При этой операции необходимо указать адрес коммутатора и пароль, который потребуется при связи с ним. Желательно указывать достаточно длинный пароль, не менее 23 символов, как рекомендуют разработчики. Для ключей целесообразно задать различные значения для каждого коммутатора.

Настройка политики доступа на основе протокола 802.1*x*

После предварительных настроек можно приступить непосредственно к созданию правил доступа в локальную сеть на основе протокола 802.1*x*. Эти настройки носят названия *политик RADIUS-сервера*.

> ***Примечание***
>
> Обычно в RADIUS-сервере присутствует несколько политик, например политика по назначению клиента в VLAN1, политика по назначению клиента в VLAN2 и т. д. В этом случае при попытке подключения клиента сервер будет последовательно проверять соответствие параметров клиента значениям политик до первого совпадения, после чего выполнит подключение в соответствии с определенными в ней значениями.

Создавать новую политику желательно с помощью мастера операций. На первом шаге вы определяете название политики, оно может быть любым. На втором необходимо выбрать тип **Доступ по Ethernet** (рис. 3.5). Следующим шагом следует указать группы безопасности, в которые должен входить подключающийся клиент: достаточно просто добавить их названия с помощью соответствующей кнопки.

После выбора групп на следующем шаге работы мастера нужно определить тип аутентификации. Предлагаемое мастером операций значение необходимо сменить на **Smart card or other certificate**. При этом мастер подставит в качестве параметров центра сертификации данные своего сертификата, полученного от доменного центра сертификации.

В результате этих шагов мы получим политику, открывающую порт для компьютера, входящего в указанную группу безопасности домена. Но можно назначить и дополнительные параметры в политике доступа, которые позволят нам автоматически назначить порту подключения определенный номер VLAN.

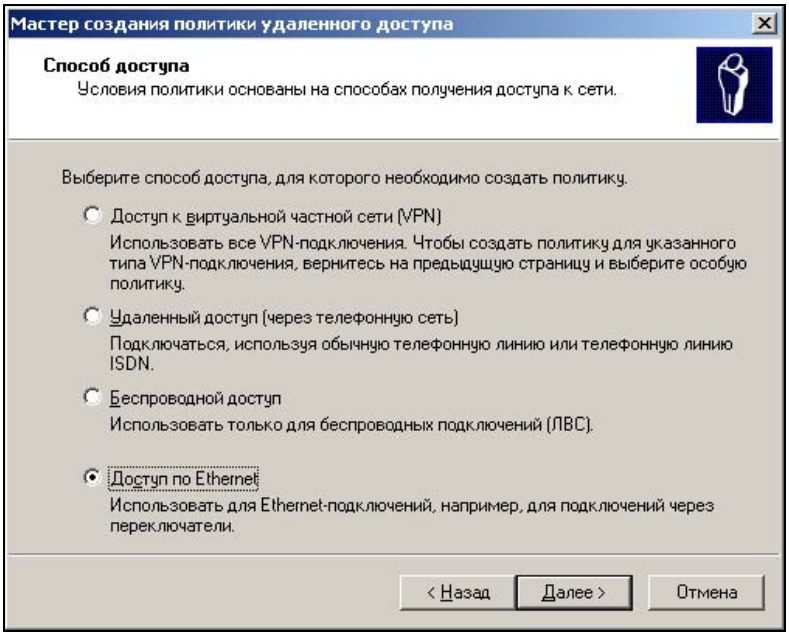


Рис. 3.5. Выбор способа доступа клиентов при создании политики сервера RADIUS

Примечание

Реализация данной возможности зависит от модели коммутатора. Некоторые модели позволяют только открывать порт, некоторые — назначать при этом номер VLAN, другие — кроме номера VLAN для успешно открытого порта могут иметь настройки, предусматривающие подключение порта в случае неудачной аутентификации к другой VLAN.

Для настройки дополнительных параметров откройте соответствующую политику доступа и нажмите кнопку **Изменить профиль**.

Для того чтобы RADIUS правильно сообщил коммутатору параметры VLAN, нужно добавить три атрибута (на вкладке **Дополнительно**):

- **Tunnel-Medium-Type** со значением **802 (includes all 802 media plus Ethernet canonical format)**;
- **Tunnel-Pvt-Group-ID** со значением номера VLAN, в которую должен быть помещен порт при удачной аутентификации;
- **Tunnel-Type** со значением **Virtual LANs (VLAN)**.

Для этого необходимо трижды нажать кнопку **Добавить**, указать в списке желаемый атрибут и настроить его значение. В результате вы должны увидеть приблизительно такие же параметры, как и на рис. 3.6 (атрибут **Tunnel-Pvt-Group-ID** определяет номер VLAN, в которую будет помещен порт коммутатора при прохождении проверки).

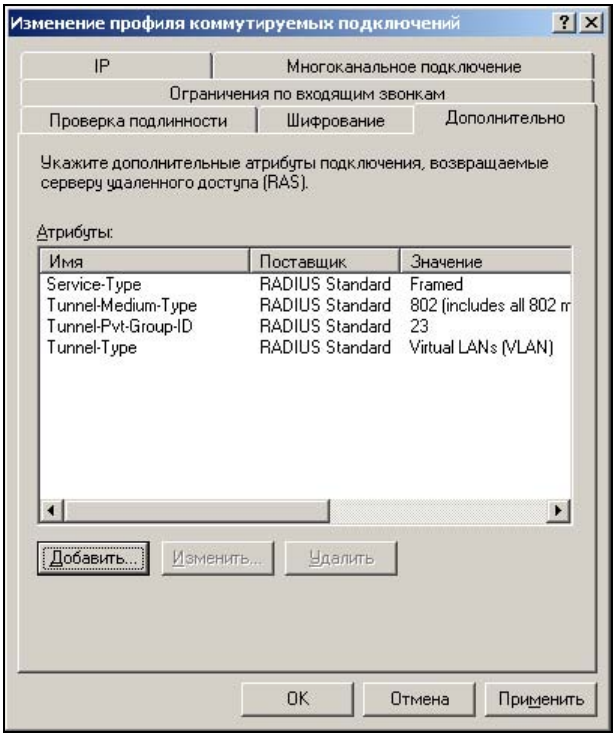


Рис. 3.6. Окно настройки дополнительных атрибутов подключения для сервера RADIUS

Настройка коммутатора для работы с протоколом 802.1*x*

В качестве примера мы рассмотрим настройку коммутатора Cisco. Команды будут отличаться для оборудования других вендоров, но правильно написать их не составит труда при понимании необходимых шагов.

> ***Примечание***
>
> Коммутаторы Cisco позволяют определить VLAN, в которую будут помещены порты в случае неудачной аутентификации (auth-fail vlan) или если клиент не поддерживает 802.1*x* (guest vlan).

Сначала в конфигурации коммутатора необходимо указать создание новой модели аутентификации с использованием сервера RADIUS (мы предполагаем, что консоль управления коммутатором открыта с необходимыми правами для выполнения описываемых операций) (листинг 3.3).

Листинг 3.3

```
aaa new-model
aaa authentication login default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
```

Далее необходимо включить режим использования протокола 802.1*x* и определить параметры RADIUS-сервера (его адрес и ключ аутентификации):

```
dot1x system-auth-control
radius-server host <IP-адрес> key xxxxxxxxxxxx
```

(В этой строке следует указать тот ключ, который определен в установках сервера RADIUS для данного коммутатора.)

Теперь нужно настроить протокол 802.1*x* для каждого порта коммутатора. В листинге 3.4 приведены команды, настраивающие порт с номером 11.

Листинг 3.4

```
interface GigabitEthernet0/11
switchport mode access
dot1x port-control auto
dot1x guest-vlan номер
dot1x auth-fail vlan номер
```

На этом настройка в системе протокола 802.1*x* завершена, и вы можете проверить ее работу, подключая к порту коммутатора компьютер.

В случае каких-либо проблем можно включить протоколирование работы RADIUS-сервера и исследовать причины возникающих неполадок на основе полученной информации.

Технология NAP

При использовании описанной ранее технологии подключения по протоколу 802.1*x* проверяется только сертификат компьютера (или пользователя). Естественно, что разработчики попытались расширить объем проверок. Так появилась технология *NAP* (Network Access Protection, название используется Microsoft, для других продуктов возможно другое имя; например, Network Access Control для продуктов Symantec Endpoint Protection).

Среди продуктов, предназначенных для контроля доступа устройств, можно отметить решения Cisco, Microsoft, Symantec. Технология NAP от Microsoft поддерживается серверами Windows Server 2008. В качестве клиентов могут быть компьютеры с операционной системой Windows XP SP3 и старше.

Технология NAP предусматривает ограничение использования ненадежными системами следующих сетевых служб:

- служб IPsec (Internet Protocol security protected communication);
- подключений с использованием протокола 802.1*x*;
- создания VPN-подключений;
- получения конфигурации от DHCP-сервера.

Идея проверки проста. Клиент, желающий получить один из перечисленных здесь сервисов, должен предоставить о себе определенные данные. Штатно существует возможность проверки выполнения параметров, определяемых центром безопасности сервера: наличия антивирусной программы, обновлений, настроек брандмауэра и т. п. Эти данные предоставляются специальной программой с клиентского компьютера (агентом) и анализируются службами сервера. В случае прохождения проверки (соответствия настроек параметрам, заданным администратором) клиентский компьютер получает сертификат, дающий право на использование запрашиваемых услуг. Если проверка не прошла, то дальнейшее поведение будет зависеть от выбранных администратором настроек: либо будет проведено обновление до нужного уровня безопасности, либо введены некоторые ограничения в работе и т. п.

Для расширения числа контролируемых состояний параметров клиента необходимо разрабатывать собственные модули. Соответствующие интерфейсы (API) описаны, но требуют привлечения подготовленного программиста.

> ***Примечание***
>
> Сходная технология ограничения была предусмотрена в Windows Server 2003 для подключения клиентов удаленного доступа (помещение клиентов в карантин с ограниченным доступом во внутреннюю сеть). На практике эта технология не нашла распространения, поскольку требовала разработки специальных программ, проверяющих выполнение условий, предъявляемых к подключаемым системам.

Внедрение технологии NAP не тривиально и требует настройки нескольких служб домена. За подробностями внедрения мы отошлем читателя на сайт разработчика — страницу Networking and Access Technologies (**http://technet.microsoft.com/en-us/network/bb545879**).

Настройка протокола IP

Сетевой протокол — это набор программно реализованных правил общения компьютеров в сети. Практически это "язык", на котором компьютеры разговаривают друг с другом. В настоящее время стандартом стало использование только протокола TCP/IP. В отличие от других протоколов TCP/IP требует ряда предварительных настроек.

Протоколы UPD, TCP, ICMP

Для передачи данных служат протоколы TCP (Transmission Control Protocol, протокол управления передачей данных) и UDP (User Datagram Protocol, протокол пользовательских дейтаграмм). UDP применяется в тех случаях, когда не требуется подтверждения приема (например, DNS-запросы, IP-телефония). Передача данных по протоколу TCP предусматривает наличие подтверждений получения информации. Если передающая сторона не получит в установленные сроки необходимого подтверждения, то данные будут переданы повторно. Поэтому протокол TCP относят к протоколам, предусматривающим соединение (connection oriented), а UDP — нет (connection less).

Протокол ICMP (Internet Control Message Protocol, протокол управляющих сообщений Интернета) предназначен для передачи данных о параметрах сети. Он включает такие типы пакетов, как ping, destination unreachable, TTL exceeded и т. д.

Протокол IPv6

Бурное развитие Интернета привело к тому, что параметры, первоначально заложенные при создании протоколов IP, стали сдерживать дальнейшее развитие глобальной сети. Прежде всего, это банальная нехватка адресов для выделения компьютерам. Решить многие такие проблемы призван протокол IP версии 6.

Протокол IPv6 устанавливается по умолчанию в новые версии операционных систем Windows и Linux, его поддержка включена в Windows XP (для включения необходимо выполнить команду `ipv6 install`). Некоторые технологии, например DirectAccess, основаны на возможностях этого протокола. Протокол IPv6 принят в качестве основного в некоторых странах (Китай).

В нашей стране пока не создана инфраструктура, поддерживающая данный протокол. Поэтому в случае желания его использовать не только внутри сети организации, когда вся инфраструктура находится под контролем и управлением, нужно учитывать все нюансы (например, система разрешения имен в DirectAccess построена через сервер корпорации Microsoft).

> ***Примечание***
>
> Поэтому в целях предупреждения использования возможных уязвимостей этого протокола для атак на компьютеры целесообразно его отключить.

Параметры TCP/IP-протокола

Для работы с протоколом TCP/IP клиенту необходим ряд параметров. Прежде всего, это IP-адрес, маска и шлюз.

IP-адрес

Каждый компьютер, работающий по протоколу TCP/IP, обязательно имеет *IP-адрес* — 32-битовое число, предназначенное для идентификации узла (компьютера) в сети. Адрес принято записывать десятичными значениями каждого октета этого числа с разделением полученных значений точками, например: 192.168.101.36.

IP-адреса в Интернете уникальны. Это значит, что каждый компьютер имеет свое сочетание цифр, и в сети не может быть двух компьютеров с одинаковыми адресами.

Для построения *локальных сетей* организаций выделены специальные диапазоны адресов: 10.*x*.*x*.*x*, 192.168.*x*.*x*, 10.*x*.*x*.*x*, с 172.16.*x*.*x* по 172.31.*x*.*x*, 169.254.*x*.*x* (под *x* подразумевается любое число от 0 до 254). Пакеты, передаваемые с указанных адресов, не маршрутизируются (иными словами, не пересылаются) в Интернете. Поэтому в различных локальных сетях компьютеры могут иметь совпадающие адреса из указанных диапазонов. Для пересылки информации с таких компьютеров в

Интернет и обратно предусмотрены специальные программы, "на лету" заменяющие локальные адреса реальными при работе с Интернетом. Иными словами, данные в Сеть пересылаются от реального IP-адреса. Этот процесс происходит "незаметно" для пользователя. Такая технология называется *трансляцией адресов*.

Групповые адреса

Если данные должны быть переданы на несколько устройств (например, просмотр видео с одной веб-камеры на различных компьютерах или одновременное разворачивание образа операционной системы на несколько систем), то уменьшить нагрузку на сеть можно с помощью *групповых рассылок*.

Для этого соответствующая программа динамически присваивает компьютеру еще один IP-адрес из специального диапазона: с 224.0.0.0 по 239.255.255.255. Причем диапазоны 224.0.0.0—224.0.0.255 и 239.0.0.0—239.255.255.255 не могут быть задействованы в приложениях и предназначены для протоколов маршрутизации (например, адрес 224.0.0.1 принадлежит всем системам сегмента сети; адрес 224.0.0.2 — всем маршрутизаторам сегмента и т. д.). Адреса групповой рассылки назначает соответствующее программное обеспечение.

Если коммутатор имеет функции работы с групповыми рассылками (поддержка IGMP snoophing, PIM DM/PIM SM), то передаваемые на адреса групповой рассылки данные будут рассылаться только на те порты, к которым подключены устройства, подписавшиеся на соответствующие рассылки. В результате сетевой трафик можно существенно снизить по сравнению с вариантом передачи таких данных независимо каждому устройству сети.

Распределение IP-адресов сети малого офиса

В сетях предприятий обычно задействованы диапазоны IP-адресов, выделенные для локального использования. Часть адресов закрепляется статически, часть — раздается динамически с помощью DHCP (Dynamic Host Configuration Protocol, динамический протокол конфигурации сервера).

Статические адреса закрепляются:

- за шлюзом, которому обычно назначают адрес *xxx.xxx.xxx*.1, но это традиция, а не правило;
- за серверами DNS, DHCP, WINS;
- за контроллерами домена, серверами (например, централизованные файловые ресурсы, почтовый сервер и т. п.);
- за станциями печати, имеющими непосредственное подключение к сети;
- за управляемыми сетевыми устройствами (например, сетевыми переключателями, SNMP-управляемыми источниками аварийного питания и т. п.).

Рабочие станции традиционно имеют *динамические адреса*. При этом часть динамических адресов выдается для локального использования, а часть предназначается для внешних клиентов, "гостей" сети.

Для упрощения администрирования сети рекомендуется выработать план распределения диапазона адресов и предусмотреть в нем некоторый запас для будущего развития информационной системы.

Маска адреса

Чтобы можно было выделить часть IP-адресов одной организации, часть другой и т. д., введено понятие *подсети*. Подсеть представляет собой диапазон IP-адресов, которые считаются принадлежащими одной локальной сети. При работе в локальной сети информация пересылается непосредственно получателю. Если данные предназначены компьютеру с IP-адресом, не принадлежащим локальной сети, то они пересылаются на другие компьютеры в соответствии с таблицей *маршрутизации*. Поэтому при использовании протокола TCP/IP важно знать, к какой сети принадлежит получатель информации: к локальной или удаленной.

Маска — это параметр, который "сообщает" программному обеспечению о том, сколько компьютеров объединено в данную группу ("подсеть"). Маска адреса имеет такую же структуру, как и сам IP-адрес: это набор из четырех групп чисел, каждое из которых может быть в диапазоне от 0 до 255. Чем меньше значение маски, тем больше компьютеров объединено в данную подсеть. Для сетей небольших предприятий маска обычно имеет вид 255.255.255.*x* (например, 255.255.255.224). Маска сети присваивается компьютеру одновременно с IP-адресом.

Так, сеть 192.168.0.0 с маской 255.255.255.0 (иначе можно записать 192.168.0.0/24) может содержать хосты с адресами от 192.168.0.1 до 192.168.0.254.

> ***Примечание***
>
> Здесь число 24 соответствует длине маски, используемой для адресации подсетей. Если записать маску 255.255.255.0 в двоичном виде, то получится последовательность из 24 единиц и 8 нулей. Маска 255.255.255.128 будет представлять собой последовательность из 25 единиц и 7 нулей. Поэтому ее записывают также в виде /25 и т. д.

Адрес 192.168.0.255 — это адрес широковещательной рассылки для данной сети. А сеть 192.168.0.0 с маской 255.255.255.128 (192.168.0.0/25) допускает адреса от 192.168.0.1 до 192.168.0.127 (адрес 192.168.0.128 служит при этом в качестве широковещательного).

Хотя многие сертификационные экзамены содержат вопросы, так или иначе связанные с разбиением на подсети (правильный подсчет маски сети, числа адресов и т. п.), на практике проводить ручной подсчет вряд ли придется. Существует много онлайновых ресурсов, которые предлагают различные варианты калькуляторов сетевых адресов (Network Calculator), например **http://www.subnetmask.info/, http://www.subnet-calculator.com/ и др**.

Тем не менее, при необходимости, определить диапазон адресов сети, в которую входит данный IP-адрес, можно очень простым способом. Запишите маску адреса не в восьмеричном, а в двоичном виде. Так, если последний октет маски равен 240, то это соответствует в двоичной записи 11110000. Первая единица справа (та, что стоит перед нулями) будет соответствовать количеству адресов в подсети, в данном

случае это 16. Теперь отсчитывайте от начального адреса сети (он всегда равен 0) по этому количеству адресов, пока не дойдете до диапазона, который включает ваш адрес. Например, если нужно узнать, к какому диапазону принадлежит адрес 10.10.10.50 с маской 255.255.255.240, то последовательно добавляя по 16 адресов к адресу 10.10.10.0, мы дойдем до диапазона 10.10.10.49—10.10.10.64, внутри которого находится наш адрес.

На практике сети с небольшим возможным числом хостов применяются интернет-провайдерами (с целью экономии IP-адресов). Например, клиенту может быть назначен адрес с маской 255.255.255.252. Такая подсеть содержит только два хоста. При разбиении сети организации используют диапазоны локальных адресов сетей класса С. Сеть класса С имеет маску адреса 255.255.255.0 и может содержать до 254 хостов. Выбор сетей класса С при разбиении на VLAN в условиях предприятия связан с тем, что протоколы автоматической маршрутизации предназначены именно для таких подсетей.

При создании подсетей в организации рекомендуется придерживаться правила, что подсети, относящиеся к определенному узлу распределения, должны входить в одну сеть. Это упрощает таблицы маршрутизации и экономит ресурсы коммутаторов. Например, если к данному коммутатору подключены подсети 192.168.0.0/255.255.255.0, 192.168.1.0/255.255.255.0, 192.168.3.0/255.255.255.0, то другому коммутатору достаточно знать, что в этом направлении следует пересылать пакеты для сети 192.168.0.0/255.255.252.0.

Шлюз

После того как компьютер получил IP-адрес и ему стало "известно" значение маски подсети, программа может начать работу в данной локальной подсети. Чтобы обмениваться информацией с другими компьютерами в сети, необходимо знать правила, куда пересылать информацию за пределы локальной сети. Для этого служит такая характеристика IP-протокола, как адрес шлюза.

Шлюз (gateway) — это устройство (компьютер), которое обеспечивает пересылку информации между различными IP-подсетями. Если программа определяет (по IP-адресу и маске), что адрес назначения не входит в состав локальной подсети, то она отправляет эти данные на устройство, выполняющее функции шлюза. В настройках протокола указывают IP-адрес такого устройства.

Для работы *только* в локальной сети шлюз может не назначаться. Если доступ в Интернет осуществляется через прокси-сервер, то компьютерам локальной сети также может не назначаться адрес шлюза (т. к. они взаимодействуют только с прокси-сервером, который находится внутри локальной сети).

Для индивидуальных пользователей, подключающихся к Интернету, или для небольших предприятий, имеющих единственный канал подключения, в системе назначается только один адрес шлюза — адрес того устройства, которое имеет подключение к Сети. При наличии нескольких маршрутов (путей пересылки данных в другие сети) будет существовать несколько шлюзов. В этом случае для определения пути передачи данных потребуется *таблица маршрутизации*.

Таблицы маршрутизации

Организация может иметь несколько точек подключения к Интернету (например, с целью резервирования или уменьшения стоимости каналов передачи данных и т. п.), а также содержать в своей структуре несколько IP-сетей. В этом случае, чтобы система "знала", каким путем (через какой шлюз) посылать ту или иную информацию, создают *таблицы маршрутизации* (routing), где для каждого шлюза указывают те подсети Интернета, для которых через этот шлюз должна передаваться информация. При этом для нескольких шлюзов можно задать одинаковые диапазоны назначения, но с разной стоимостью передачи данных: информация будет отсылаться по каналу, имеющему самую низкую стоимость, а при его выходе из строя автоматически будет использоваться следующее наиболее "дешевое" подсоединение.

Таблицы маршрутизации имеются на каждом устройстве, работающем по протоколу IP. Администраторы в основном имеют дело с таблицами маршрутизации коммутирующего оборудования. Настройка таблиц маршрутизации компьютеров целесообразна только при наличии нескольких сетевых адаптеров, подключенных к различным сегментам сети. Если у компьютера есть лишь одна сетевая карта (одно подключение к Интернету), таблица маршрутизации имеет наиболее простой вид: в ней записано, что все сигналы должны отправляться на шлюз, назначенный *по умолчанию* (default gateway).

Другой пример — при создании VPN-подключений к компьютеру добавляется сетевой интерфейс. В этом случае с помощью таблиц маршрутизации также можно регулировать (перераспределять) трафик через VLAN и сетевую карту компьютера.

Посмотреть таблицу маршрутизации протокола TCP/IP в Windows можно по команде `route print`, а в Ubuntu — `route` или `netstat -r`. Команда `route` позволяет также добавить новый статический маршрут (`route add`). Чтобы этот маршрут сохранился после перезагрузки компьютера, в Windows команду необходимо выполнить с ключом `-p` (`route add -p`), а в Ubuntu команду добавления маршрута следует включить в сценарий, исполняемый при подключении соответствующего интерфейса *(см. разд. "Подключение к Интернету с использованием серверов Ubuntu" в главе 4)*.

> ***Примечание***
>
> Возможностей настройки таблиц маршрутизации в Linux несравнимо больше, чем в Windows. Так можно настроить несколько таблиц маршрутизации, которые будут применяться выборочно к пакетам на основе анализа каких-либо их признаков. Иными словами, в одном случае пакет из пункта А в пункт Б можно отправить по одному маршруту, а в другом случае — по совершенно иному. Для этого существует специальный набор утилит iproute2, который по умолчанию уже установлен в Ubuntu. Если подобная настройка необходима, то ознакомиться с правилами ее конфигурирования можно, выполнив команду `man ip`.

Назначение адресов при совместном использовании подключения к Интернету

Особая ситуация возникает при настройке совместного подключения к Интернету. В этом случае тот компьютер, на котором создается данное подключение, начинает выполнять функцию сервера DHCP с единственным ограничением, что его адрес *жестко фиксирован* — 192.168.0.1. Клиенты, которые получают от данного сервера адреса из подсети 192.168.0.0/24, автоматически настраиваются на использование его в качестве шлюза по умолчанию и сервера имен.

Поскольку вариант совместного подключения присутствует как на серверных системах, так и на рабочих станциях, то такое решение наиболее оптимально для небольших организаций.

Порт

При передаче данных кроме IP-адресов отправителя и получателя пакет информации содержит в себе номера *портов*. Порт — это некое число, которое необходимо при приеме и передаче данных для идентификации процесса (программы), который должен обработать данные. Так, если пакет послан на 80-й порт, то это свидетельствует, что информация предназначена серверу HTTP.

Номера портов с 1-го по 1023-й закреплены за конкретными программами (так называемые *well-known-порты*). Порты с номерами 1024—65 535 можно использовать в программах собственной разработки. При этом возможные конфликты должны разрешаться самими программами путем выбора свободного порта. Иными словами, порты будут распределяться динамически: возможно, что при следующем старте программа выберет иное значение порта.

Знание того, какие порты задействуют те или иные прикладные программы, важно при настройке брандмауэров. Часть настроек в таких программах для наиболее популярных протоколов предопределена, и вам достаточно только разрешить/запретить протоколы, руководствуясь их названиями. А в некоторых случаях придется обращаться к технической документации, чтобы определить, какие порты необходимо "открыть", чтобы обеспечить прохождение пакетов данной программы.

> ***Примечание***
>
> При настройке брандмауэра следует учитывать, что многие программы при подключении к Интернету открывают не один порт, возможно, даже некоторый диапазон значений. Один из распространенных вариантов настройки брандмауэров для недокументированных программ — это анализ реального их трафика с помощью какой-либо программы перехвата передаваемых по сети пакетов.

Часто возникает необходимость увидеть, какие порты могут принимать трафик или уже имеют соединение с каким-либо компьютером (если порт может принимать трафик, то его состояние отображается как `LISTENING`). Как в Windows, так и в Ubuntu для этого применяется команда `netstat`. В зависимости от версий операционной системы данная команда имеет различный набор ключей, позволяющий детализировать отчет (например, указать программы или процессы, использующие

конкретные порты). В общем случае достаточно запустить команду с ключом `-a` (листинг 3.5).

Листинг 3.5

```
>netstat -a
Активные подключения
Имя   Локальный адрес      Внешний адрес              Состояние
TCP   sasha:http           sasha.ask.ru:0             LISTENING
TCP   sasha:epmap          sasha.ask.ru:0             LISTENING
TCP   sasha:https          sasha.ask.ru:0             LISTENING
TCP   sasha:microsoft-ds   sasha.ask.ru:0             LISTENING
TCP   sasha:1025           sasha.ask.ru:0             LISTENING
TCP   sasha:1033           sasha.ask.ru:0             LISTENING
TCP   sasha:1064           ack-isa2.ask.ru:8080       CLOSE_WAIT
TCP   sasha:1067           ack-exchange.ask.ru:2703   ESTABLISHED
TCP   sasha:1070           ack-exchange.ask.ru:1025   ESTABLISHED
TCP   sasha:1078           ack-frw.ask.ru:8080        CLOSE_WAIT
UDP   sasha:microsoft-ds   *:*
UDP   sasha:isakmp         *:*
UDP   sasha:1041           *:*
UDP   sasha:1053           *:*
```

В данном примере на компьютере готовы к подключению несколько портов (состояние `LISTENING`, это порты http, epmap и т. д. — номера портов вместо названия можно отобразить, если добавить ключ `-n`), порты 1067 и 1079 подключены (`ESTABILISHED`, программа показывает, с какой системой идет обмен данными), передача информации с портов 1064 и 1078 завершена и система находится в состоянии закрытия соединения (`CLOSE_WAIT`) и т. д.

Получить информацию по удаленному компьютеру позволяют специальные программы *сканирования портов*. Данные по отдельному порту (открыт/не открыт) можно получить штатными средствами системы (например, с помощью команды `telnet` или утилиты PortQry из состава Support Tools); для контроля диапазона портов обычно используют утилиту `nmap`. Она есть как в варианте запуска под Linux, так и под Windows. Загрузить ее можно с **http://nmap.org/download.html**.

Имена компьютеров в сети TCP/IP

Человеку удобнее работать с именем компьютера, чем запоминать цифры, составляющие его IP-адрес. В сети на основе протокола TCP/IP компьютерам присваивают имена *хоста (hostname)*.

> ***Примечание***
>
> В сетях Windows компьютеры могут иметь еще одно имя. Это NetBIOS-имя компьютера, используемое в составе рабочих групп. В общем случае необходимо стремиться к тому, чтобы NetBIOS-имя соответствовало имени хоста.

Полное имя хоста, которое называют также FDQN (Fully Qualified Domain Name), составляется из нескольких имен, разделяемых при написании точкой, например, так: **www.ask.ru**. Первая слева группа символов (до точки), в данном примере это **www**, является собственным именем компьютера. Следующая группа символов — от точки до точки — это имя группы компьютеров *(домена)*, которой принадлежит данная система. Следующая группа символов — имя группы компьютеров, которой в свою очередь принадлежат группы компьютеров, имена которых находятся левее. Данную цепочку можно продолжать сколь угодно долго. Для удобства обычно ограничиваются тремя-четырьмя группами символов. Написание полного имени принято завершать символом точки, чтобы отличать полное имя хоста от имени того или иного домена.

В зависимости от того, сколько групп символов входит в доменное имя, различают домены первого, второго, третьего и т. д. уровней. На практике под *именем домена* понимают всю группу символов в полном имени справа от имени компьютера. Самая правая группа символов имени (до первой точки) называется *доменом первого уровня*, вторая справа — *доменом второго уровня*, затем следует *домен третьего уровня* и т. д.

> ***Примечание***
>
> При создании нового домена Windows не следует давать ему имя домена первого уровня. В этом случае действуют некоторые ограничения, с которыми можно ознакомиться в базе данных Microsoft. Целесообразно домену Windows дать имя по принципу ***<название_организации>*.local**.

Имена хостов внутри локального сегмента сети (домена Windows) должны быть уникальными. Имена хостов в разных доменах могут совпадать (в этом случае будут различными *полные имена* — FQDN).

Проверка каналов связи

Любая информационная система нуждается в надежно работающих каналах связи. Опишем некоторые способы, которые помогут проверить работу транспортной подсистемы в условиях обычного офиса.

Диагностика линий связи

Для проверки линий связи на физическом уровне необходимо специальное оборудование, например *кабель-тестеры*. Как правило, эти устройства есть только в специализированных организациях, занимающихся прокладкой и тестированием линий связи. В лучшем случае у администратора может иметься простейший индикатор, отображающий наличие соединения или его обрыв.

Косвенно судить о качестве линии связи можно по числу ошибок в ней, которое отображается управляемым коммутатором (рис. 3.7). Подобная статистика свидетельствует о необходимости принятия незамедлительных мер по устранению причин некачественной работы канала связи.

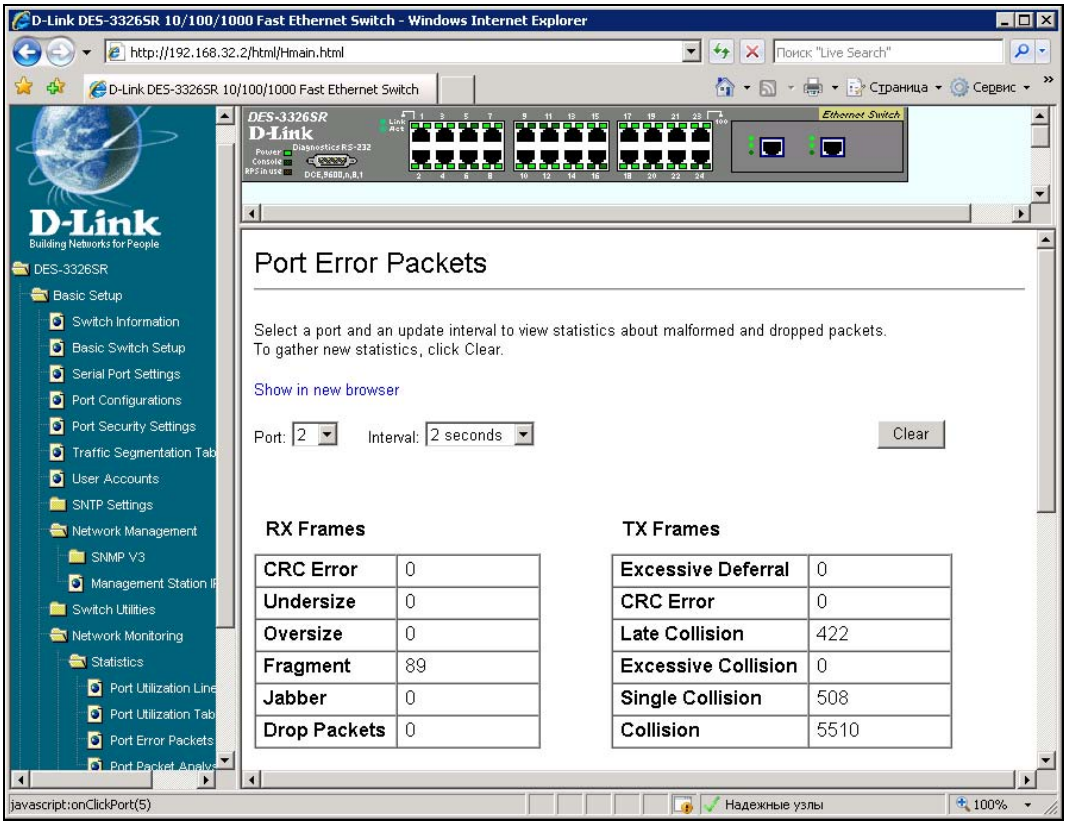


Рис. 3.7. Интерфейс отображения статистики ошибок на порту коммутатора

Поиск причин неудовлетворительного качества линии связи обычно следует начинать с проверки тех элементов, которые проще заменить:

- патч-корды (самодельные патч-корды часто через год-два эксплуатации становятся причинами ошибок);
- разъемы (наличие защелок, отсутствие пыли на оптических коннекторах и т. п.);
- качество расшивки в кроссе или кабельной розетке (потребуется вскрытие розетки, визуальная проверка и, возможно, повторная расшивка специальным инструментом).

Если самостоятельно устранить неполадки не удастся, то придется обратиться в специализированную организацию, которая проведет проверку и сможет указать на причину плохих показателей — например, на повреждение кабеля на расстоянии примерно 26 м от точки замера.

> ***Примечание***
>
> Для поиска места обрыва можно использовать возможности коммутационного оборудования по тестированию линий связи. Однако такими функциями сегодня обладают только топовые устройства.

Диагностика IP-протокола

После проверки качества связи на транспортном уровне можно приступать к диагностике TCP/IP-протокола. Обычно это следует делать в таком порядке:

1. Проверить параметры настройки IP-протокола.
2. Определить достижимость ближайших компьютеров сети.
3. Проверить функционирование серверов имен.
4. Оценить качество канала связи глобальной сети (Интернета).

> ***Примечание***
>
> В Windows существует специальный мастер диагностики сетевого подключения, который выполняет аналогичные операции и выдает результаты соответствующих тестов. Эта программа вызывается из меню утилиты **Сведения о системе** (**Пуск | Все программы | Стандартные | Служебные | Сведения о системе | Сервис | Диагностика сети**).

Проверка параметров настройки IP-протокола

Для отображения параметров IP-протокола предусмотрены утилиты `ifconfig` (Ubuntu), `ipconfig` (Windows NT/200*x*/XP/Vista) и `winipcfg` (Windows 9*x*/ME). Утилиты `ifconfig` и `ipconfig` выполняются в режиме командной строки. Утилита `winipcfg` имеет графический интерфейс.

Утилиты выводят на экран параметры настройки протокола TCP/IP: значения адреса, маски, шлюза. При запуске `ipconfig` с ключом `/all` на экран будут выведены все действующие параметры протокола. Отмечу также ключ `/renew`, который позволяет обновить автоматически полученные параметры IP-протокола, и ключ `/registerdns`, с помощью которого можно обновить запись на DNS-сервере данного компьютера (используется в Windows 200*x*/XP/Vista).

Если утилита покажет, что сетевому адаптеру присвоен адрес 169.254.134.123 (или аналогичный), то можно сделать заключение, что в сети недоступен сервер, автоматически присваивающий параметры IP-протокола. Часто причиной подобной ошибки (если ранее компьютер нормально работал в сети) является нарушение контакта в подсоединении сетевого кабеля.

Проверка достижимости ближайших компьютеров сети

Проверить достижимость компьютеров в сети TCP/IP позволяет команда `ping`, которая посылает на заданный компьютер последовательность символов определенной длины и выводит на экран информацию о времени ответа удаленной системы. Ключами команды можно регулировать количество отсылаемых символов и время ожидания ответа (через этот период выводится сообщение о превышении периода ожидания; если ответ придет позже, то он не будет показан программой).

При тестировании подключения рекомендуется применять такую последовательность операций.

1. Сначала проверяют работоспособность протокола TCP/IP путем "пингования" адреса 127.0.0.1:

```
ping 127.0.0.1
```

Адрес 127.0.0.1 — это "личный" адрес любого компьютера. Таким образом, эта команда проверяет прохождение сигнала "на самого себя". Ее можно выполнить без наличия какого-либо сетевого подключения. Вы должны увидеть приблизительно следующие строки (листинг 3.6).

Листинг 3.6

```
ping 127.0.0.1
Обмен пакетами с 127.0.0.1 по 32 байт:

Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Статистика Ping для 127.0.0.1:
Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
Минимальное = 0 мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Если будет показано сообщение о недостижимости адресата, то это означает ошибку установки протокола IP. В этом случае целесообразно удалить протокол из системы, перезагрузить компьютер и вновь установить поддержку протокола TCP/IP.

> ***Примечание***
>
> По умолчанию команда `ping` посылает пакет в 32 байта. Размер пакета можно увеличить (добавлением соответствующего ключа команды) до 65 Кбайт. Таким образом, можно обнаружить случаи ошибок пересылки пакетов большого размера. За размером тестового пакета отображается время отклика удаленной системы (в нашем случае — меньше 1 мс). Потом показывается еще один параметр протокола — значение TTL (*время жизни пакета*; практически это число маршрутизаторов, через которые может пройти пакет — каждый маршрутизатор уменьшает значение TTL на единицу).

2. На следующем шаге необходимо проверить ответ локального компьютера по присвоенному ему IP-адресу. Для этого следует выполнить команду:

   `ping <адрес>`

   Результат, который должен быть выведен на экран в случае нормальной работы, практически аналогичен предыдущему примеру.

3. Следующая проверка — это выполнение команды `ping` с указанием IP-адреса любого ближайшего компьютера. Можно указать любой адрес, относительно которого вы уверены, что он достижим в локальной сети на момент проверки, например, IP-адрес шлюза или адрес DNS-сервера.

   Наличие отклика свидетельствует, что канал связи установлен и работает. Отсутствие ответа обычно говорит либо о повреждении кабельной сети (например, нет контакта в разъеме), либо о неверно установленных параметрах статического адреса (если адрес получается автоматически, то следует обратиться в службу технической поддержки).

Проверка состояния порта TCP/IP удаленного компьютера

В случае применения брандмауэров для защиты подключения компьютера к Интернету наличие ответа от удаленной системы на команду `ping` совсем не означает, что пакеты, предназначенные другим портам, будут пропущены.

Существуют две возможности удостовериться в правильной настройке брандмауэра. Во-первых, в Support Tools от Windows Server 2003 присутствует утилита portqry.exe, которая позволяет увидеть ответ удаленной системы на запрос по конкретному порту. Так, для проверки достижимости FTP-сервера можно выполнить следующую команду:

```
portqry -n kenin -e 21
```

Возможный результат иллюстрирует листинг 3.7.

Листинг 3.7

```
Querying target system called:
kenin
Attempting to resolve name to IP address...
Name resolved to 192.168.0.29
TCP port 21 (ftp service): LISTENING
Data returned from port:
220 kenin.ask.ru X2 WS_FTP Server 5.0.0 (1845270209)
331 Password required
```

Утилита сообщила, что порт 21 открыт, и отобразила информацию, которую выдает FTP-сервер, работающий на этом компьютере (имя компьютера `kenin`).

Второй способ состоит в применении утилиты `telnet`. Запуская эту утилиту с параметрами в виде имени удаленной системы и номером порта, вы осуществляете попытку подключения к соответствующему порту.

> ***Примечание***
>
> Утилита `telnet` по умолчанию недоступна в Windows 7/Server 2008, этот компонент следует добавить при необходимости.

Если вы не можете подключиться к удаленной системе, то необходимо найти компьютер, на котором происходит фильтрация пакетов. Для этого следует проверить путь прохождения информации с помощью команды `tracert`, после чего протестировать возможность подключения к соответствующему порту каждого компьютера этой цепочки (листинг 3.8).

Листинг 3.8

```
tracert www.ack.ru

Tracing route to ack.ru [212.107.195.12]
over a maximum of 30 hops:
```

```
 1   120 ms  111 ms  112 ms  ask_pdc.ask.ru [192.168.0.67]
 2   117 ms  113 ms  111 ms  frw.ask.ru [192.168.0.2]
 3   121 ms  113 ms  116 ms  cisco.ask.ru [195.161.192.254]
 4  1011 ms  346 ms  136 ms  aa-s0-6-r2.ekaterinburg.rostelecom.ru
[195.161.94.137]
 5   387 ms  181 ms  397 ms  aa-fe0-2-sw1.ekaterinburg.rostelecom.ru
[195.161.94.5]
 6   504 ms  461 ms  134 ms  tschelkun-bbn0-po1-5.rt-comm.ru [217.106.6.149]
 7   751 ms  1146 ms 1712 ms kochenevo-bbn0-po2-0.rt-comm.ru [217.106.6.130]
 8  1855 ms  1796 ms    *    trs20-dsr0-po8-0-0.rt-comm.ru [217.106.6.138]
 9  1221 ms  1313 ms 1212 ms vlad-dsr0-po6-0.rt-comm.ru [217.106.6.158]
10  1223 ms  1212 ms 1212 ms vmts.vladivostok.rostelecom.ru [195.161.4.94]
11     *        *       *    Request timed out.
12     *        *       *    Request timed out.
13  1727 ms  1871 ms 1703 ms ack.ru [212.107.195.12]
Trace complete.
```

По результату выполнения данной команды можно оценить, что наибольшая задержка в прохождении сигнала возникает на каналах связи с узлами, стоящими в строках 7 и 8. Одиночные звездочки свидетельствуют, что ответ от этого узла не получен в заданный диапазон времени. Если в строке стоят все звездочки, то это может обозначать, что администраторы соответствующих хостов не разрешили прохождение ICMP-пакетов (пакеты, которые используются в том числе и командами `ping` и `tracert`).

> ***Примечание***
>
> В Ubuntu утилита `tracert` должна быть доустановлена с использованием пакета traceroute (`apt-get install traceroute`). Кроме того, желательно запускать трассировку с ключом `-w` *<время>*, предписывающим ожидать ответа установленное время. В противном случае со значениями по умолчанию утилита для большинства узлов может вывести ответ только в виде звездочек.

Проверка функционирования серверов имен

Для проверки работоспособности сервера имен Интернета следует выполнить команду `ping`, указав в качестве параметра не IP-адрес, а доменное имя какого-либо компьютера, например, имя WWW-сервера вашего провайдера:

`ping` *<имя>*

Если команда сможет "разрешить" IP-адрес хоста и покажет отклик, то это означает работоспособность системы распознавания имен. Практически это говорит о правильной настройке протокола TCP/IP и работоспособности канала связи. Если не будет ответа на ввод команды с именем существующего хоста, то это может свидетельствовать либо об ошибке в задании DNS-серверов, либо об их неработоспособности.

Проверка качества канала связи

При работе в Интернете одни информационные серверы открываются быстрее, другие медленнее, возникают случаи недостижимости желаемого хоста. Часто при-

чиной этого бывает недостаточное качество канала связи: большое время ожидания данных или существенный процент потерь пакетов, что обычно приводит к повторам передачи.

С помощью утилиты `pathping` в Windows можно оценить качество канала связи по всей цепочке до желаемого источника. Эта утилита посылает на каждый промежуточный хост серию пакетов и выводит информацию о количестве откликов и среднем времени ответа (листинг 3.9).

Листинг 3.9

```
C:\pathping www.microsoft.com
Tracing route to www.microsoft.akadns.net [207.46.230.219]
over a maximum of 30 hops:
0 ask-2002.ack.ru [192.168.0.52]
1 frw.ack.ru [192.168.0.12]
2 cisco.ack.ru [195.161.193.254]
3 aa-s0.ekaterinburg.rostelecom.ru [195.161.94.137]
4 aa-sw1.ekaterinburg.rostelecom.ru [195.161.94.5]
5 tschelkun.rt-comm.ru [217.106.6.149]
6 aksai.rt-comm.ru [217.106.6.97]
7 msk.rt-comm.ru [217.106.6.81]
8...spb.rt-comm.ru [217.106.6.70]
9 213.190.162.5
10 alv2-ge3-0.datanet.tele.fi [192.130.130.61]
11 208.51.142.197
12...pos8-0-2488M.cr1.CPH1.gblx.net [62.12.32.73]
13 pos1-0-2488M.cr2.SEA1.gblx.net [64.214.65.242]
14 so1-0-0-2488M.br2.SEA1.gblx.net [64.213.83.182]
Computing statistics for 375 seconds...
Source to Here This Node/Link
Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0 ask-2002.ack.ru [192.168.0.52] 0/ 100 = 0% |
1 0ms 0/ 100 = 0% 0/ 100 = 0% frw.ack.ru [192.168.0.12] 0/ 100 = 0% |
2 1ms 0/ 100 = 0% 0/ 100 = 0% cisco.ack.ru [195.161.192.254] 2/ 100 = 2% |
3 637ms 2/ 100 = 2% 0/ 100 = 0% aa-s0.ekaterinburg.rostelecom.ru
[195.161.94.137] 0/ 100 = 0% |
4 613ms 4/ 100 = 4% 2/ 100 = 2% aa-sw1.ekaterinburg.rostelecom.ru
[195.161.94.5] 0/ 100 = 0% |
5 562ms 5/ 100 = 5% 3/ 100 = 3% tschelkun.rt-comm.ru [217.106.6.149] 0/ 100 = 0% |
6 605ms 4/ 100 = 4% 2/ 100 = 2% aksai.rt-comm.ru [217.106.6.97] 0/ 100 = 0% |
7 623ms 4/ 100 = 4% 2/ 100 = 2% msk.rt-comm.ru [217.106.6.81] 0/ 100 = 0% |
8 725ms 5/ 100 = 5% 3/ 100 = 3% spb.rt-comm.ru [217.106.6.70] 0/ 100 = 0% |
9 864ms 2/ 100 = 2% 0/ 100 = 0% 213.190.162.5 0/ 100 = 0% |
10 942ms 2/ 100 = 2% 0/ 100 = 0% alv2-ge3-0. datanet.tele.fi [192.130.130.61]
1/ 100 = 1% |
11 868ms 3/ 100 = 3% 0/ 100 = 0% 208.51.142.197 0/ 100 = 0% |
```

```
12 927ms 3/ 100 = 3% 0/ 100 = 0% pos8-0-2488M.cr1.CPH1.gblx.net [62.12.32.73]
1/ 100 = 1% |
13 1040ms 4/ 100 = 4% 0/ 100 = 0% pos1-0-2488M.cr2.SEA1.gblx.net
[64.214.65.242] 0/ 100 = 0% |
14 1059ms 4/ 100 = 4% 0/ 100 = 0% so1-0-0-2488M.br2.SEA1.gblx.net
[64.213.83.182] 96/ 100 = 96% |

Trace complete.
```

После опубликования цепочки хостов, через которые проходит сигнал на пути к заданному серверу, программа `pathping` выводит статистические данные о достижимости каждого промежуточного хоста. Причем время усреднения выбирается исходя из конкретной ситуации (в примере подсчет проводился за период в 375 с). Первый параметр — время доступа к данному хосту, затем показано число посланных на него пакетов и число неполученных ответов (с процентом успеха). После чего отображаются аналогичные значения для достижимости конечного хоста при расчете прохождения пакетов от данной промежуточной точки. Так, в 14-й строке цифры "говорят", что время доступа к хосту составляет 1059 мс, что при посылке на него 100 пакетов на четыре отсутствовал ответ. А если бы сигнал на конечный хост передавался с позиции номер 14, то при посылке 100 пакетов на все был бы получен ответ. И в завершение после имени данного промежуточного хоста утилита сообщила, что число успешных пакетов составило 96%.

Переустановка протокола TCP/IP в Windows

Иногда "последним" средством восстановления работоспособности становится переустановка протокола TCP/IP. Поскольку в Windows данный протокол является практически основным компонентом, то пользователь не может удалить обычными операциями удаления/добавления компонентов.

Чтобы восстановить параметры протокола в первоначальное состояние, следует воспользоваться командой `netsh`. Команда

```
netsh interface ip reset
```

восстановит настройки протокола TCP/IP в значения по умолчанию.

Служба автоматического назначения параметров IP-адреса

Параметры IP-протокола индивидуальны для каждого компьютера. Чтобы облегчить пользователям их назначение, были разработаны специальные механизмы, позволяющие автоматизировать данный процесс.

Адресация APIPA

Для облегчения построения небольших сетей разработчики Microsoft включили в Windows возможность самостоятельного назначения адресов. Если в сети не настроена служба выдачи параметров IP-адреса, то при автоматическом присвоении

параметров Windows назначит сетевой плате адрес из диапазона от 169.254.0.1 по 169.254.255.254 (маска подсети 255.255.0.0), предварительно проверив, не занят ли уже такой адрес в сети.

Естественно, что никаких дополнительных параметров операционная система в этом случае не получает. Например, она не будет знать, куда посылать запросы, чтобы получить данные с серверов Интернета, и работа возможна только в пределах локальной сети.

Поэтому наличие адреса из указанного диапазона на рабочей станции обычно свидетельствует либо о проблеме со службой автоматического присвоения адреса в сети, либо о повреждении физической линии (например, обрыв кабеля).

Серверы DHCP

Для автоматической раздачи параметров IP-протокола в локальных сетях устанавливают так называемый сервер DHCP (Dynamic Host Configuration Protocol, динамический протокол конфигурации сервера). Сервер DHCP автоматически сообщает компьютерам, начинающим работу в составе сети, параметры настройки протокола TCP/IP: в первую очередь это IP-адрес, маска адреса, шлюз. Кроме того, сервер DHCP может предоставлять параметры серверов времени, указывать расположение данных автоматической настройки прокси-клиентов, данные для конфигурации IP-телефонов и т. п.

Обычно IP-адрес от сервера DHCP выделяется компьютеру на определенный срок, заданный в настройках сервера (поэтому его называют также *динамическим IP-адресом*). Если компьютер не будет продолжать работу в данной сети, то этот адрес может быть переназначен другому устройству.

Чтобы сервер начал раздавать адреса, вы должны задать диапазон этих адресов и определить необходимые параметры протокола. Делается это путем создания новой области *(scope)*.

Для области необходимо определить как минимум диапазон распределяемых адресов, маску сети, указать срок аренды IP-адреса. Внутри диапазона адресов можно исключать некоторые адреса (например, если вы предполагаете задать их статически). Срок аренды выбирают исходя из особенностей вашей сети. При малом числе компьютеров его можно существенно увеличить по сравнению со значением по умолчанию в 8 суток (вплоть до неограниченного значения).

Для полноценной работы в составе компьютерной сети получения только IP-адреса и маски сети обычно недостаточно. Так, клиентам минимально необходимы адреса DNS-серверов и адрес шлюза. Кроме того, могут понадобиться DNS-суффикс существующей сети, адрес автоматической конфигурации прокси-сервера и т. п. Все эти параметры может сообщать DHCP-сервер.

Настройка серверов DHCP в Windows

Для установки службы DHCP в Windows достаточно отметить ее в перечне параметров Windows Server и затем авторизовать в службе каталогов. Чтобы авторизо-

вать сервер (этот шаг необходим, если создан домен Windows), пользователю с правами администратора предприятия необходимо в меню консоли управления DHCP-сервером выбрать пункт **Авторизовать сервер**.

> ***Примечание***
>
> Индикатор, свидетельствующий об авторизации сервера, выдает статус с некоторой (обычно до 5 мин) задержкой. Поэтому после авторизации сервера следует выдержать незначительный промежуток времени и открыть консоль управления снова, чтобы убедиться в полной работоспособности сервера.

Параметры, сообщаемые пользовательской системе, определяются *опциями* DHCP. Глобальные опции определяются для всего сервера; они доступны в каждой области. Кроме того, можно определять опции в самой области: в случае, если для параметра назначены и глобальные значения, то будут применены параметры области.

В Windows операция добавления опций производится с использованием графического интерфейса. Достаточно открыть динамическое меню, найти нужную опцию, включить ее и назначить значение. Итоговый перечень опций доступен в окне оснастки управления (рис. 3.8).

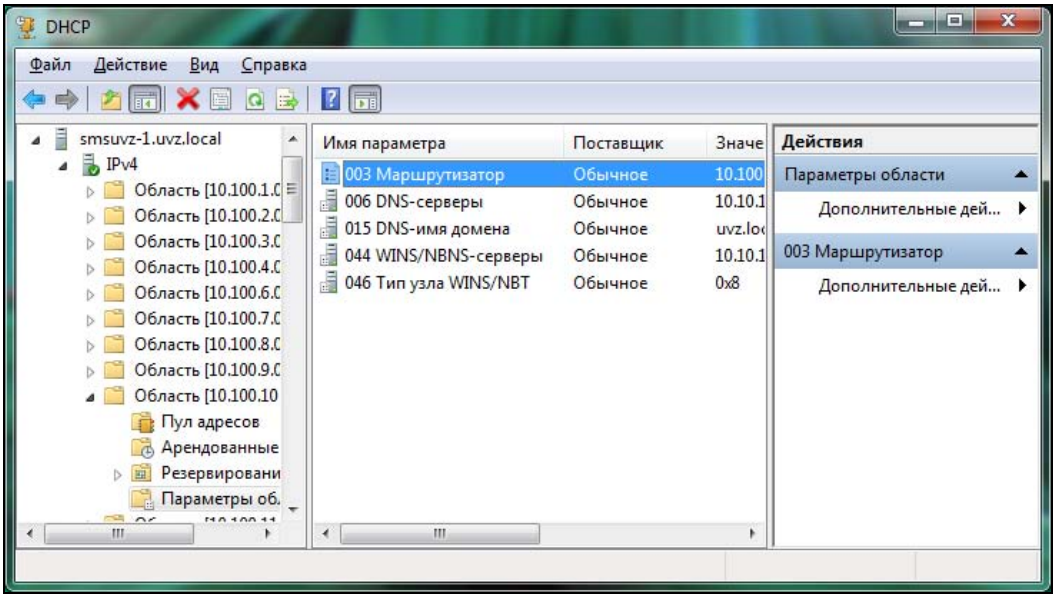


Рис. 3.8. Оснастка управления DHCP-сервером Windows 2008

Кроме перечисленных в оснастке, администратор легко может создать новые опции, руководствуясь описаниями прикладной программы. Две нижние опции в перечне соответствуют глобальным значениям всего сервера, остальные определены для данной области.

DHCP-сервер можно настроить так, чтобы он выдавал клиентам не случайный, а заранее определенный адрес. Чтобы настроить резервирование адреса, необходимо *знать MAC-адрес сетевого адаптера* соответствующего клиента. Этот адрес легко

определить в свойствах соответствующего подключения как для Windows-систем (`ipconfig /all`), так и Linux (`ifconfig`, значение HWaddr). Сам процесс резервирования не представляет сложности, достаточно (в Windows) в оснастке управления DHCP-сервером ввести в окне операции резервирования имя клиента и его MAC-адрес или, в случае Ubuntu, создать по образцу блок описания резервированного адреса и перезагрузить службу.

> ***Примечание***
>
> Для новых сетевых адаптеров MAC-адрес можно определить по их упаковке (вторая часть адреса — это серийный номер адаптера).

Установка и настройка сервера DHCP в Ubuntu

В Ubuntu сервер DHCP устанавливается командой

```
sudo apt-get install dhcp3-server
```

> ***Примечание***
>
> Поскольку часто DHCP-сервер в небольших организациях устанавливают на компьютер, являющийся шлюзом Интернета, следует ограничить его работу только внутренним интерфейсом. Для этого укажите название интерфейса в параметре `INTERFACES` в файле /etc/default/dhcp3-server.

После установки сервера DHCP необходимо выполнить *настройку зоны*. В Ubuntu все параметры зоны настраиваются в файле /etc/dhcp3/dhcpd.cond. В файле подробно описаны все параметры с многочисленными примерами, так что определить по этим образцам свои зоны не представит никакого труда. Достаточно просто скопировать нужный блок и заменить образцы реальными значениями. В листинге 3.10 приведен образец конфигурации сервера DCHP в Ubuntu.

Листинг 3.10

```
ddns-update-style interim;
include "/etc/bind/rndc.key";
ddns-domainname "test.ru";

option domain-name "test.ru";
option domain-name-servers aster.test.ru;
option option-176 code 176 = string;
option netbios-name-servers 192.168.31.1;
option netbios-node-type 8;

default-lease-time 600;
max-lease-time 7200;

authoritative;

log-facility local7;
```

```
subnet 192.168.31.0 netmask 255.255.255.0 {
range 192.168.31.100 192.168.31.200;
option routers 192.168.31.10;
option domain-name "test.ru";
option broadcast-address 192.168.31.255;
option option-176 "MCIPADD=192.168.31.10, TFTPSRVR=192.168.31.10";

zone 31.168.192.in-addr.arpa. {
primary 127.0.0.1;
key "rndc-key";
}

zone test.ru. {
primary 127.0.0.1;
key "rndc-key";
}
}
```

В листинге 3.10 показана конфигурация DHCP-сервера, достаточная для обслуживания клиентов. Сервер дополнительно настроен на выдачу параметров опции с номером 176, которая необходима для работы IP-телефонов. Конфигурация также предполагает обновление сервера DNS (прямой зоны **test.ru** и обратной — 31.168.192.in-addr.arpa) в случае получения клиентом DHCP IP-адреса.

После изменения настроек сервера DHCP в Ubuntu его необходимо перезагрузить:

```
sudo /etc/init.d/dhcp3-server restart
```

Обслуживание DHCP-сервером других сегментов сети

С помощью одного DHCP-сервера администраторы могут раздавать IP-адреса различным сегментам своей сети. Для этого необходимо на DHCP-сервере создать области с диапазонами адресов, соответствующими этим сегментам, и обеспечить получение DHCP-сервером запросов из другого сегмента сети.

Создание областей с различными диапазонами IP-адресов выполняется стандартно: вы создаете область и определяете для нее любой желаемый диапазон адресов. Но чтобы сервер DHCP выдал адрес из этого диапазона, он должен получить запрос из другого сегмента сети.

В большинстве случаев для формирования запросов на получение IP-адреса используются возможности современных коммутаторов. Для этого достаточно выполнить настройку опции **DHCP Relay** (названия могут несколько отличаться) — рис. 3.9.

> ***Примечание***
>
> Агенты ретрансляции DHCP-запросов могут быть и программными, например, такой агент входит в состав сервера маршрутизации и удаленного доступа Windows (Routing and Remote Access Server, RRAS).

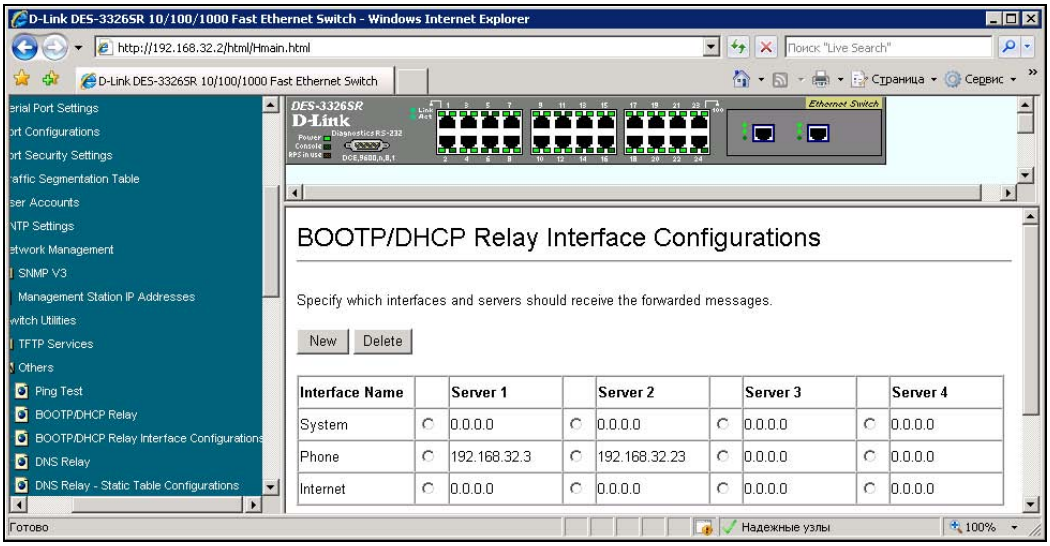


Рис. 3.9. Настройка функции **DHCP Relay** на коммутационном оборудовании

Для настройки пересылки запросов DHCP достаточно в интерфейсе управления коммутатором указать IP-адрес сервера DHCP. Как правило, настройки коммутаторов позволяют определять основной и резервный серверы DHCP. Такие настройки должны быть указаны для каждого IP-интерфейса, созданного на коммутаторе третьего уровня.

Принцип работы агента ретрансляции DHCP весьма прост. Агент прослушивает сеть на наличие пакетов запроса аренды адреса. Если такой пакет получен, то агент ретранслирует запрос на адрес, указанный в настройках опции. Сервер DHCP получает данный запрос и, поскольку он отправлен с адреса другого сегмента сети, предоставляет в аренду адрес именно того диапазона, из которого пришел запрос.

Статическое разрешение имен

В небольшой локальной сети для задания соответствия "IP-адрес — сетевое имя" можно вручную сформировать статические записи. Это позволяет обеспечить функционирование локальной сети без серверов DNS, DHCP и т. п.

Если Windows не может динамически определить имена (IP-адреса) хостов, то система использует содержимое файлов hosts, networks и lmhosts. Первые два файла представляют обычный список соотношений "IP-адрес — имя" в прямом и обратном порядке (листинг 3.11).

Листинг 3.11

Файл hosts:

```
...
195.12.156.31 ads.adximize.com
63.120.34.76 c3.xxxcouter.it
...
```

Файл networks:

```
...
ads.adximize.com 195.12.156.31
c3.xxxcouter.it 63.120.34.76
...
```

Файл lmhosts совместим с Microsoft LAN Manager 2.*x* и предназначен для загрузки специальных NetBIOS-имен (указания сервера домена, серверов приложений и т. п.). Файлы находятся в папке *%systemroot%*/system32/drivers/etc (для Windows 9*x* — в папке Windows). При установке системы обычно создаются примеры (имеют расширение sam), по образцу которых и следует редактировать необходимые файлы.

В Ubuntu для статического разрешения имен предусмотрены файлы hosts (полный путь — /etc/hosts) и resolv.conf (полный путь — /etc/resolf.conf, в этом файле хранятся записи о серверах разрешения имен). Синтаксис записей об именах в этих файлах аналогичен описанному ранее.

Изменять файлы можно в обычном текстовом редакторе (необходимы права администратора/суперпользователя). Запись должна начинаться с первой позиции строки, а столбцы можно отделять любым числом пробелов.

Серверы DNS

Для снижения количества ручных операций в целях разрешения имен существуют специальные серверы — DNS-серверы (Domain Name System, система доменных имен). Серверы DNS обеспечивают получение доменного имени по запросу на основе IP-адреса, и наоборот. Поэтому указание адреса сервера DNS — это одна из основных настроек протокола TCP/IP, необходимых для работы в Интернете.

Адрес сервера DNS обычно назначается автоматически при инициализации протокола IP. Имена серверов DNS сообщаются DHCP-серверами. Обычно указывается несколько DNS-серверов, чтобы система могла использовать второй сервер при временной недоступности первичного DNS.

Основные понятия DNS

Для уверенной работы с DNS необходимо четко представлять себе, что означают те или иные термины.

- **Зоны DNS.** Зона DNS — это часть пространства имен, для которого DNS-сервер может выполнять операции разрешения имен. Существуют зоны прямого и обратного просмотра, которые на практике для удобства называют прямыми и обратными зонами.

  Прямая зона позволяет по имени системы получать ее IP-адрес, *обратная* — по IP-адресу "выдает" информацию об имени хоста. Поэтому если нужно по имени компьютера узнать его адрес, то говорят о прямом *разрешении имени*. Если по

IP-адресу хотят получить имя компьютера, то в этом случае происходит *обратное разрешение имени*. Строго говоря, если в DNS зарегистрировано прямое разрешение имени, то должно быть и обратное.

> ***Примечание***
>
> Если ваша организация зарегистрировала на свое имя домен, то для нормальной работы почтового сервера необходимо зарегистрировать обратное разрешение имени. Проверьте (по протоколу telnet) ответ почтового сервера на обращение "Hello" и зарегистрируйте это имя в обратной зоне. Владельцами обратных зон являются, обычно, провайдеры. Поэтому именно к ним и нужно обращаться с подобной просьбой.

Для разрешения обратных имен в домене самого верхнего уровня создана зона in-addr.arpa. Названия зон обратного просмотра формируются с указанием этого имени и добавлением к нему слева имени трех октетов адреса сети в обратном порядке. Например, для сети 195.161.192.0/24 имя обратной зоны будет 192.161.195.in-addr.arpa.

- **Первичная и вторичная зоны.** У создаваемых записей DNS должен быть один "хозяин". Чтобы все записи были корректны, их необходимо вносить на одном DNS-сервере. В этом случае говорят, что на таком DNS-сервере расположена *первичная* зона. Для отказоустойчивости на других серверах можно создать копии этой зоны. Такие зоны будут называться *вторичными*. Вторичная зона содержит те же записи, что и первичная, но в нее нельзя вносить изменения или добавлять новые записи. Эти операции можно делать только для первичной зоны.

  > ***Примечание***
  >
  > В случае домена Windows 200*x* и использования зоны DNS, интегрированной со службой каталогов, изменения можно вносить на любом DNS-сервере такой зоны.

- **Серверы имен зоны.** Для каждой первичной зоны можно создать сколько угодно копий на других серверах. Принято определять серверы имен, информация которых "официальна". Такие серверы называют NS-записями соответствующего домена. Обычно для каждого домена создаются два или три NS-сервера. Если ответ на запрос разрешения имени получен от NS-сервера, то он считается авторизованным, другие серверы возвращают неавторизованные ответы (принципиально возможна ситуация, что информация с таких серверов уже устарела).

  > ***Примечание***
  >
  > Для обновления записей DNS на клиентских компьютерах следует очистить кэш DNS-записей (`ipconfig /flushdns`).

- **Передача зон.** Так называется специальная операция копирования всех записей данной зоны с одного DNS-сервера на другой. По соображениям безопасности часто передача зон разрешается только на заранее определенный администратором системы список IP-адресов DNS-серверов.

- **Делегирование зон.** Если на DSN-сервере создана, например, прямая зона для домена **test.local**, то запись о домене третьего уровня **level3.test.local** должна со-

держаться на этом же сервере. Если географически домен **level3.test.local** удален от основного домена, то поддержание записей в его зоне на DNS-сервере становится не очень удобным. Проще поручить администратору этого домена вносить изменения в DNS-записи самостоятельно с помощью делегирования зоны. При делегировании DNS-сервер создает у себя запись, указывающую, что запросы разрешения имени для этой зоны должны перенаправляться на другой DNS-сервер, на который произведено *делегирование зоны*.

- **Stub-зоны (зона-заглушка).** При делегировании зоны на исходном сервере сохраняется информация о NS-сервере делегированной зоны. Поскольку администратор делегированной зоны может изменять ее DNS-записи, то он может и сменить записи NS-сервера. Если соответствующее изменение не будет внесено на сервер, который осуществляет делегирование, то процесс разрешения имен нарушится (основной сервер по-прежнему будет отправлять запросы на несуществующий уже адрес, в результате будет формироваться неверный ответ).

  Для исправления подобной ситуации введено понятие *stub-зоны*. При создании stub-зоны в ней определяются NS-записи делегированной зоны. Причем если администратор делегированной зоны меняет эти записи, то соответствующие изменения вносятся и в записи stub-зоны. В результате гарантируется целостность процесса разрешения имен.

- **Зона "точка".** Домен самого верхнего уровня, как уже указывалось, принято называть именем "точка". Если в DNS создать зону "точка", то это будет фактически означать, что данный сервер является корневым в структуре DNS, т. е. он должен разрешать самостоятельно любые запросы имен. Если этот DNS-сервер не может разрешить имя, то его ответ будет гласить, что такого хоста не существует.

Основные типы записей DNS

При создании первичной зоны для своего домена следует обратить внимание на создание некоторых специальных записей ресурсов (resource records), которые полезны для получения информации общего типа.

- **SOA (Start of Authority).** Серийный номер зоны. В DNS автоматически увеличивается при любом изменении записей зоны. Используется в операциях переноса зон (если номер изменился, то происходит обновление записей вторичной зоны). На практике принято этот номер формировать на основе даты последнего изменения: год-месяц-день-(время), например, так: 20090810.
- **NS (Name Server).** Адреса "официальных" серверов имен данной зоны. Эти серверы возвращают *авторизованные* ответы.
- **RP (Responsible Person).** Адрес электронной почты лица, ответственного за внесение изменений в записи зоны. Наличие записи и поддержание ее актуальности желательно, чтобы при возникновении каких-либо вопросов по домену организации у специалистов были реальные контактные данные. Обратите внимание, что символ @ в адресе электронной почты заменяется точкой.

- **A (Host Address).** Эта запись содержит информацию об имени системы и ее IP-адресе. Именно этот тип записи добавляется в DNS-сервер при регистрации хостов.
- **PTR (Pointer, указатель).** Так называется запись в обратной зоне. Настройками DNS локальных доменов обычно предусматривается автоматическое создание (изменение) PTR-записи при добавлении A-записи в прямую зону.
- **CNAME (Canonical NAME).** Записи псевдонима. Используются, если хосту необходимо дать второе DNS-имя.
- **MX (Mail eXchanger).** Запись хранит IP-адрес сервера электронной почты (SMTP-сервера), который обслуживает данный домен. Чтобы на данный домен можно было отправлять электронную почту, в DNS для домена должна быть обязательно создана MX-запись. Для целей резервирования может быть создано несколько MX-записей. Чтобы различать их, каждой записи соответствует определенный *вес*. По умолчанию почта отправляется на адрес, содержащийся в MX-записи с наименьшим весом. Если этот сервер не отвечает, то делаются попытки отправить почту на адреса, соответствующие MX-записям с последующими весами.
- **SRV (Запись службы).** Специальный тип записи для обнаружения служб в домене (например, службы IP-телефонии и т. п.). Записи о системных службах Windows автоматически создаются службой каталогов. Вручную записи добавляют при настройке дополнительных продуктов в соответствии с прилагаемой технической документацией.

Разделение DNS

Все больше сотрудников начинают использовать мобильные компьютеры для доступа к ресурсам организации как изнутри локальной сети, так и из Интернета. Для сокращения затрат на изменение конфигураций персональных компьютеров следует выполнять настройки программного обеспечения так, чтобы доступ к сетевым ресурсам локальной сети осуществлялся *единообразно*, независимо от того, выполняется подключение из локальной или глобальной сети. Реализуется такое требование *разделением DNS* (DNS split).

Технология разделения DNS подразумевает, что разрешение имен локальной сети и Интернета для *одного доменного имени* настраивается на различные *DNS-серверы*. Суть решения будет понятна из рассмотрения двух возможных ситуаций.

Одинаковые имена локального домена и домена Интернета

Если имя домена Windows совпадает с именем домена Интернета, то единственная необходимая операция — это правильная настройка публикации внутренних ресурсов в глобальной сети. Когда клиент локальной сети пытается получить доступ к каким-либо ресурсам, он запрашивает их месторасположение у локального, *внутреннего* сервера DNS. Этот сервер возвращает клиенту внутренний адрес ресурса, к которому и осуществляется подключение (рис. 3.10).

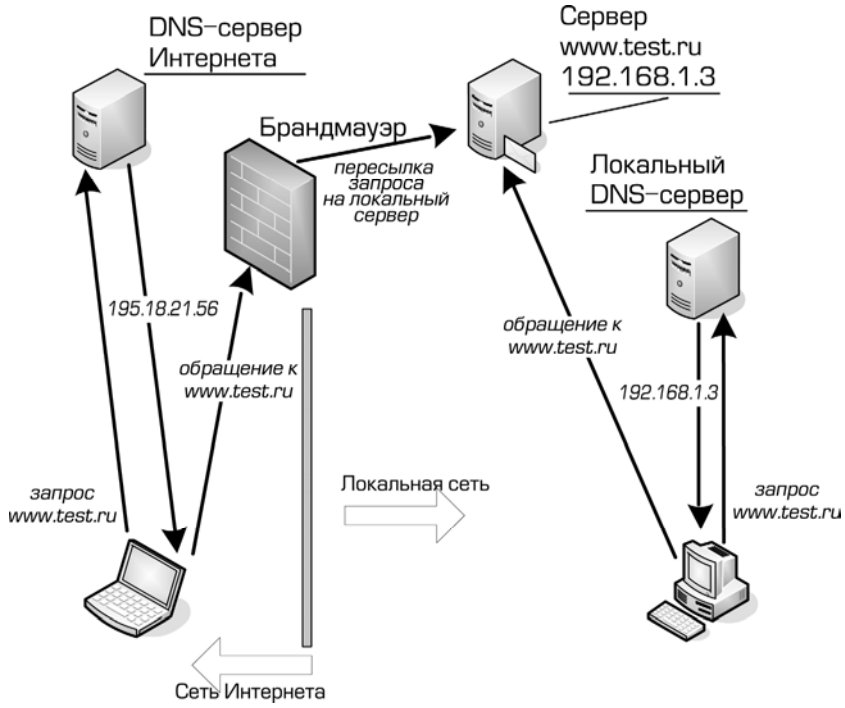


Рис. 3.10. Разделение DNS

Примечание

Ресурсом, для которого наиболее часто приходится реализовывать подключение пользователей как изнутри организации, так и снаружи, является почтовая система. Например, если в организации установлен MS Exchange Server и клиенты применяют MS Outlook (полной версии), то для локального подключения к почтовой системе по умолчанию применяется протокол RPC. Подключение по этому протоколу подразумевает динамическое открытие портов на сервере, что вызывает серьезные сложности в настройке брандмауэра при подключении клиента Outlook из глобальной сети. В результате на практике такое подключение из Интернета фактически не использовалось. Начиная с Windows Server 2003, для реализации всей функциональности полной версии Outlook предназначена специальная технология создания RPC Proxy, которая подробно описана в документах базы данных Microsoft (см. документ "Exchange Server 2003 RPC over HTTP Deployment Scenarios" или KB833401). Обратите внимание, что одновременно следует настроить и клиента Outlook так, чтобы по умолчанию для подключения к почтовому серверу Exchange применялся вариант RPC over HTTP (см. статью "Configuring Outlook 2003 for RPC over HTTP").

На сервере DNS, обслуживающем домен Интернета этой же организации, необходимо настроить A-запись соответствующего ресурса на внешний *адрес* брандмауэра данной организации. А на брандмауэре настроить публикацию внутреннего ресурса таким образом, чтобы запрос, приходящий на брандмауэр и адресованный на данное имя, перенаправлялся на локальный адрес ресурса.

В результате, независимо от точки подключения, запрос клиента всегда будет доставлен на один и тот же локальный ресурс системы.

При реализации технологии разделения DNS клиент локальной сети и компьютер Интернета при разрешении одного и того же имени будут обращаться к различным DNS-серверам. Локальный клиент в результате будет обращаться по локальному адресу, а клиент Интернета перешлет запрос на брандмауэр организации, который и переправит его на локальный адрес запрашиваемого ресурса. В результате никакой перестройки прикладных программ на клиенте осуществлять не придется.

Различные имена локального домена и домена Интернета

Если "внутреннее" и "внешнее" имена домена организации не совпадают, то на внутреннем сервере DNS необходимо создать первичную зону для домена с "внешним" именем. В эту зону внести записи, соответствующие именам систем, предоставляющих необходимые службы (естественно, изменять записи этой зоны придется вручную). Причем в качестве IP-адресов этих записей следует указать *локальные* IP-адреса систем. Таким образом, на внутренних DNS-серверах будет по две зоны: зона, соответствующая "внутреннему" домену (реальные внутренние названия компьютеров локальной сети), и зона с "внешним" именем (содержит фактически синонимы, вторые имена только для компьютеров, публикующих ресурсы в глобальной сети). Так же как и в предыдущем примере, следует настроить публикацию внутренних ресурсов на брандмауэре организации.

Клиентов необходимо настроить (в том числе и в локальной сети) на подключение к ресурсам по *внешним именам*. Если клиент обратится к почтовому серверу *изнутри* организации, то он запросит *внутренний* сервер DNS об адресе, соответствующем внешнему имени почтовой системы. Поскольку на внутреннем сервере DNS существует одноименная первичная зона, то сервер будет считаться авторизованным для ответов и сообщит клиенту *внутренний адрес* почтовой системы. Произойдет подключение по локальному адресу системы.

А если, например, клиенту необходимо обратиться к этому же почтовому серверу из Интернета, то он запросит внешний сервер DNS, получит от него адрес брандмауэра и отправит запрос на него. Брандмауэр, получив запрос, проанализирует его и перешлет на локальный адрес почтовой системы.

Установка сервера DNS

Сервер DNS можно установить только на компьютер со статическим IP-адресом. При этом обратите внимание, чтобы сервер DNS, который предполагается для обслуживания организации, смог правильно разрешать *неполные* имена. Следовательно, он должен сообщить правильный адрес как на запрос для **test.mydomain.local**, так и для запроса на имя **test**. Для этого необходимо, чтобы основной DNS-суффикс компьютера, на котором устанавливается сервер DNS, *совпадал* с суффиксом имени домена организации. Соответствующие настройки выполняются в параметрах TCP/IP-протокола, устанавливаемых по статике для сетевого адаптера сервера DNS. В Ubuntu в этих целях необходимо правильно отредактировать файл /etc/resolf.conf (параметр `search`).

Установка DNS в Windows Server

Службу DNS устанавливают, добавляя соответствующую роль в оснастке **Диспетчер сервера**. Дальнейшие операции проходят под руководством мастера операций и не представляют особых сложностей.

Создание новой зоны также происходит под руководством мастера. Не забудьте только в свойствах созданной зоны определить параметры RP, перечислить серверы, которым вы разрешаете получить полный список зоны, и установить необходимый режим обновлений зоны. Если сервер функционирует, в том числе в режиме кэширования (т. е. за реальными именами Интернета клиенты обращаются на этот же сервер), то необходимо указать адреса DNS-серверов провайдера в свойствах сервера. Для этого откройте свойства DNS-сервера (именно всего сервера, а не зоны) и на вкладке **Пересылка** укажите полученные от провайдера значения.

Управление сервером DNS осуществляется с помощью оснастки **Диспетчер DNS**, в которой представлены все операции, необходимые для управления сервером DNS от Microsoft (рис. 3.11). Текущие операции ограничиваются, как правило, только ручным добавлением необходимых записей.

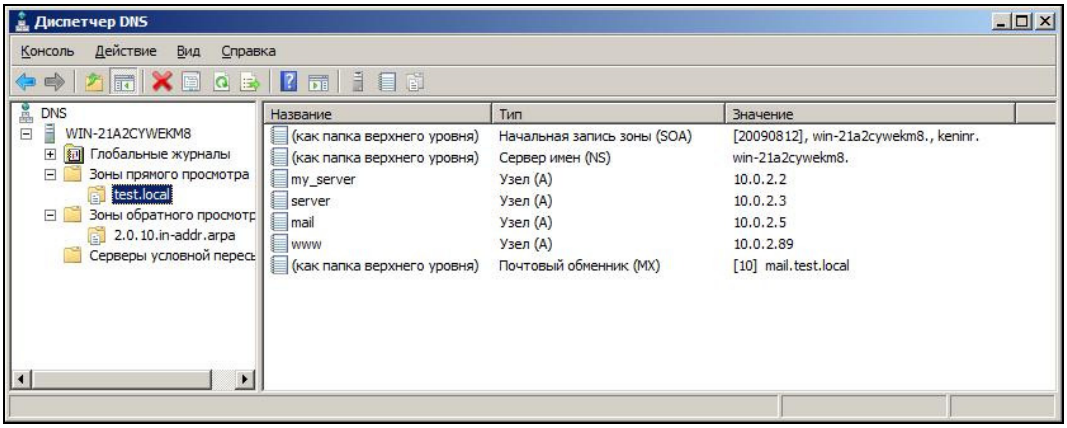


Рис. 3.11. Оснастка **Диспетчер DNS**

Новые зоны на сервер DNS добавляют с помощью мастера операций. Следует учесть, что если сервер предназначен для разрешения имен домена Windows и является контроллером домена, то оптимальным решением будет создание зоны, *интегрированной со службой каталогов*. Такой вариант позволит использовать службы Windows для репликации данных между серверами DNS. При этом зона DNS на каждом сервере будет фактически являться первичной (допускать внесение изменений), а сами данные — безопасными (при работе с зоной будет задействована встроенная в Windows система безопасности).

Интегрированная в службу каталогов система имен реплицируется по всем контроллерам домена. Начиная с Windows Server 2003, добавлена возможность размещения зоны DNS в собственных *разделах каталога*. Это позволяет реплицировать интегрированные в службу каталогов зоны *только* на серверы DNS либо домена,

либо леса, в зависимости от того, какой раздел вы создаете, исходя из структуры организации. Данная операция выполняется из оснастки управления сервером DNS (соответствующая команда меню сервера).

Для зон, обслуживающих домен Windows, обязательно должна быть включена опция динамического обновления. В целях безопасности следует выбрать вариант безопасных динамических обновлений записей. При этом рекомендуется, чтобы служба DHCP была настроена на запуск не от системной учетной записи, а от имени специально созданного для такой цели пользователя.

Если вы не хотите регистрировать всех клиентов в DNS, то можно настроить сервер DNS так, чтобы он перенаправлял неразрешенные запросы имени на WINS-сервер. Для этого в настройках DNS-сервера в свойствах зоны на вкладке **WINS** следует включить опцию пересылки запросов на WINS-сервер и указать соответствующие IP-адреса. Обычно такая настройка необходима для сетей, в которых есть клиенты Windows 9*x*.

После установки и настройки основных параметров DNS-сервера необходимо выполнить его первичное тестирование. В свойствах сервера на вкладке мониторинга следует включить опции проверки как работы самого сервера, так и правильности перенаправления запросов и провести тест.

Установка и настройка сервера DNS в Ubuntu

Наиболее популярный сервер DNS в Linux — Bind — устанавливается командой

```
sudo apt-get install bind9
```

Конфигурация DNS-сервера представлена несколькими файлами в папке /etc/bind9. Это файл named.conf, в который включаются параметры из файлов named.conf.local и named.conf.options. Файл named.conf следует оставить без изменений, а все пользовательские настройки внести в оставшиеся два файла.

Конфигурация DNS-сервера допускает указание многих дополнительных параметров, но в условиях обслуживания внутренней сети обычно нет необходимости, например, скрывать номер версии программного обеспечения или определять, какой диапазон адресов сети будет обслуживаться сервером. Поэтому мы рассмотрим только основные настройки.

Параметры DNS-серверов провайдера (которые вы получили при подключении к Интернету) следует указать в файле named.conf.options, сняв комментарии в строках блока `forwardes` и заменив 0.0.0.0 реальными IP-адресами серверов.

Обратите внимание, что для вступления в силу измененных настроек конфигурации сервера его необходимо перезагрузить командой

```
sudo /etc/init.d/bind9 restart
```

Для создания собственной зоны ее следует определить в файле named.conf.local. В нем вы указываете название зоны и имя файла с ее записями, например, как показано в листинге 3.12.

Листинг 3.12

```
zone "имя.ru" {
type master;
file "db.имя.ru";
};

zone "31.168.192.in-addr.arpa" {
type master;
file "db.31";
};
```

После этого необходимо создать файлы зон с описаниями параметров систем. Если путь к файлам зон явно не указан в named.conf.local, то их необходимо создать в папке /var/cache/bind (это определено в файле named.conf.optios).

В Интернете можно найти много рекомендаций по созданию файлов зон. Листинг 3.13 иллюстрирует пример конфигураций для зон прямого и обратного разрешений.

Листинг 3.13

/var/cache/db.*имя*.ru

```
$TTL 604800; 1 week
@ IN SOA localhost.admin.имя.ru. (
20090118; serial
604800; refresh (1 week)
86400; retry (1 day)
2419200; expire (4 weeks)
604800; minimum (1 week)
)
имя.ru IN NS localhost.
имя.ru IN MX 10 mail.имя.ru
имя.ru IN A 192.168.31.10
www IN A 192.168.31.20
mail IN A 192.168.31.15
```

/var/cache/db.31

```
$TTL 604800; 1 week
31.168.192.in-addr.arpa IN SOA ns.имя.ru.admin.имя.ru. (
20090118; serial
604800; refresh (1 week)
86400; retry (1 day)
2419200; expire (4 weeks)
604800; minimum (1 week)
)
NS localhost.
15 PTR mail.имя.ru.
20 PTR www.имя.ru.
```

Структура файла достаточно ясна из листинга 3.13. Отметим только, что в строке с SOA сначала указывается имя зоны (вместо явного указания имени зоны допустим символ `@`, как в третьей строке), после SOA следует полное имя первичного сервера имен (заканчивается точкой), потом владелец зоны. В качестве серийного номера на практике принято указывать дату внесения изменений. А в строках определения почтового сервера и сервера имен название домена можно опустить. Обратите внимание, что в строке адреса почтового сервера обязательно должен присутствовать номер ("вес" почтового сервера).

Для файлов зон следует установить полные права для учетной записи, от имени которой запускается сервер DNS (bind):

```
chown bind. /var/cache/bind/*
```

После этого нужно перезагрузить зоны. Сделать это можно либо командой

```
sudo /etc/init.d/bind9 reload
```

либо

```
sudo rndc reload
```

> ***Примечание***
>
> Утилита `rndc`, предназначенная для управления сервером DNS, устанавливается в систему по умолчанию с пакетом bind9.

Обязательно проверьте сообщения в журнале системы после перезагрузки зон:

```
tail /var/log/syslog
```

В этом журнале не должно быть сообщений об ошибках и о незагрузке той или иной зоны. Кроме того, проверьте ответы DNS-сервера (то, насколько вы правильно создали записи зон) следующей командой:

```
dig any имя_зоны
```

Динамическое обновление DNS

Поскольку IP-адреса раздаются динамически, то целесообразно настроить обновление DNS-зон на основе выданных параметров DHCP-сервера.

Современные Windows-клиенты реализуют обновление Windows-DNS-сервера при получении IP-адреса. Для предыдущих версий целесообразно включить в настройках DHCP-сервера Windows опцию обновления DNS-сервера (рис. 3.12).

Включение опции динамического обновления записей DNS-сервера для всех клиентов производится из меню свойств сервера DHCP. При наличии в сети клиентов предыдущих версий необходимо настроить сам сервер на обновление DNS после обработки от них DHCP-запроса.

При использовании служб сервера Ubuntu необходимо выполнить несколько больше операций, отредактировав как файлы настроек DHCP-сервера (указать, записи в каких зонах должны обновлять какие DNS-серверы), так и DNS-сервера (в первую очередь, настроив параметры для безопасного доступа к обновлениям).

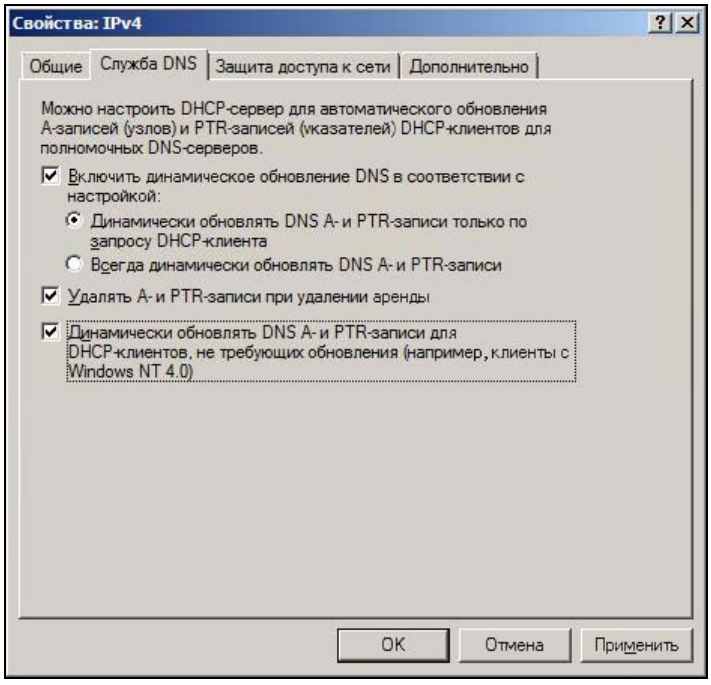


Рис. 3.12. Настройка параметров автоматического обновления DNS-сервера на платформе Windows Server 2008

Отредактируйте следующим образом настройки DNS-сервера. Во-первых, в файле named.conf.options раскомментируйте параметр `query-source` и укажите его так:

```
query-source address *;
```

Во-вторых, в файле named.conf.local добавьте в начало следующие строки:

```
include "/etc/bind/rndc.key";
controls {
inet 127.0.0.1 allow {localhost;} keys {"rndc-key";};
};
```

Это сообщает серверу параметры секретного ключа для осуществления безопасного обмена. Предоставьте право чтения файла /etc/bind/rndc.key всем учетным записям.

Далее, в описание каждой зоны, которая должна автоматически обновляться, добавьте строку

```
allow-update {key "rndc-key";};
```

Примечания

Мы описываем конфигурацию, когда и сервер DHCP, и сервер DNS расположены на одном компьютере. Если они разнесены, то данный файл необходимо скопировать вручную.

Если сервер DNS обслуживает внутреннюю зону, то кроме ее обновления нужно не забыть настроить параметры обновления зоны обратного разрешения имен.

В результате описание зоны в файле named.conf.local должно выглядеть примерно так, как представлено в листинге 3.14.

Листинг 3.14

```
zone "имя.ru" {
type master;
file "db.имя.ru";
allow-update {key "rndc-key";};
};
```

> ***Примечание***
>
> Обратите внимание, что по умолчанию в Ubuntu пакет AppArmor запрещает запись в папку /etc/bind. Поэтому файлы для динамически изменяемых зон DNS следует размещать в папке /var/lib/bind.

В файл конфигурации DHCP-сервера (/etc/dhcp3/dhcpd.conf) внесите следующие строки:

```
ddns-update-style interim;
include "/etc/bind/rndc.key";
ddns-domainname "имя.ru";
```

Добавьте *вовнутрь* описания параметров зоны DHCP указания на те зоны DNS, которые должны обновляться при выдаче IP-адреса этого блока. Описание зоны DHCP при этом будет выглядеть примерно так, как представлено в листинге 3.15.

Листинг 3.15

```
subnet 192.168.31.0 netmask 255.255.0.0 {
range 192.168.31.100 192.168.31.200;
# Далее указание на DNS-зоны, которые нужно обновлять
zone 31.168.192.in-addr.arpa. {
primary 192.168.31.1;
key "rndc-key";
}

zone имя.ru. {
primary 192.168.31.1;
key "rndc-key";
}
}
```

После внесения указанных изменений перестартуйте серверы DHCP и DNS. Обязательно проверьте по журналам системы отсутствие ошибок при их загрузке.

При первом запуске этих серверов после настройки динамического обновления будут созданы файлы журналов, в которые будут вноситься оперативные данные

о выданных IP-адресах. Через некоторый промежуток времени изменения из файлов журналов будут автоматически переноситься в файлы зон DNS-сервера.

Обслуживание и диагностика неисправностей DNS-сервера

Самый простой способ проверить работоспособность сервера DNS на платформе Windows — включить опции мониторинга на соответствующей вкладке консоли управления. Вы должны получить положительную диагностику при тестировании самого сервера и ответа от сервера, на который настроена пересылка запросов. Для серверов на операционных системах Linux нужно проконтролировать удачный перезапуск демона (должны увидеть сообщение **OK** в строке запуска) и просмотреть журналы системы.

В любом случае журнал сервера DNS является основным источником информации по работоспособности службы. В Ubuntu обычно не нужно включать мониторинг каких-либо дополнительных событий — информации системного журнала вполне достаточно для анализа состояния службы. Протоколирование в Windows службы DNS можно расширить, если установить опции *ведения журнала отладки* на соответствующей вкладке консоли управления сервером DNS. Но пользоваться этой возможностью следует *только* в период отладки. В журнал по умолчанию заносится вся информация (подробно — все данные пакетов), что негативно сказывается на производительности сервера.

Универсальная утилита для получения данных с любого DNS-сервера (и, соответственно, проверки его работоспособности) — это `nslookup`. Она по умолчанию присутствует среди утилит в системах с установленным протоколом TCP/IP.

Утилита `nslookup` позволяет вручную получить от сервера DNS такую же информацию, какую системы получают в автоматическом режиме при разрешении имен. Поэтому она часто применяется при диагностике систем.

После запуска утилиты осуществляется подключение к серверу DNS, указанному в настройках сетевого адаптера по умолчанию. Далее в режиме командной строки можно получить ответ на запрос к любому DNS-серверу.

Рассмотрим пример диалога программы `nslookup` (команды, вводимые пользователем, отмечены знаком `>` в начале строки). Листинги 3.16—3.18 иллюстрируют работу с программой.

Листинг 3.16

```
>nslookup
Default Server: ack
Address: 192.168.0.10

>server ns.unets.ru
Default Server: ns.unets.ru
Address: 195.161.15.19
```

После запуска программа выдала сообщение, что подключена к DNS-серверу `ack` с IP-адресом 192.168.0.10.

В окне программы `nslookup` была введена команда подключения к DNS-серверу **ns.unets.ru**. В ответ программа сообщила, что подключилась к этому серверу и сообщила его IP-адрес.

Листинг 3.17

```
>uzvt.ru
Server: ns.unets.ru
Address: 195.161.15.19

Non-authoritative answer:
uzvt.ru nameserver = ns.isp.ru
uzvt.ru nameserver = ns.e-burg.ru
ns.e-burg.ru internet address = 195.12.66.65
```

Пользователь ввел запрос на разрешение имени **uzvt.ru**. Утилита сообщила, что сервер **ns.unets.ru** предоставил неавторизованную информацию (Non-authoritative answer) об этом имени. Из того что сервер "вернул" данные NS-записей, следует, что **uzvt.ru** — это домен Интернета, что его серверы имен — **ns.e-burg.ru** и **ns.isp.ru**.

Листинг 3.18

```
>set type=mx
>uzvt.ru
Server: ns.unets.ru
Address: 195.161.15.19

Non-authoritative answer:
uzvt.ru MX preference = 50, mail exchanger = relay.utnet.ru
uzvt.ru MX preference = 10, mail exchanger = mail.uzvt.ru

uzvt.ru nameserver = ns.isp.ru
uzvt.ru nameserver = ns.e-burg.ru
mail.uzvt.ru internet address = 195.12.67.218
relay.utnet.ru internet address = 195.209.191.2
ns.e-burg.ru internet address = 195.12.66.65
```

Следующими командами пользователь определил, что ему нужна информация о почтовых серверах (`set type=mx`), и вновь указал в запросе тот же домен (**uzvt.ru**). Утилита вернула от сервера DNS ответ, что для домена зарегистрированы два почтовых сервера с разными приоритетами (**mail.uzvt.ru** с приоритетом 10 и **relay.utnet.ru** с приоритетом 50), и сообщила их адреса. Поскольку **mail.uzvt.ru** имеет меньший приоритет, то именно по этому адресу и будет направляться электронная почта для домена **uzvt.ru**.

Примечание

Для проверки разрешения имен DNS почтового сервера MS Exchange предназначена специальная утилита, которую необходимо загрузить с сайта Microsoft — `dnsdiag`. Эта программа должна быть запущена на компьютере почтового сервера из папки информационного сервера (IIS). Выходная информация программы полностью соответствует тем данным, которые получает почтовый сервер в процессе разрешения имен. Эта информация может помочь в диагностике проблемных ситуаций, поскольку почтовый сервер Exchange использует собственные настройки для получения данных DNS, а не те, которые используются для сетевого интерфейса системы.

Листинг 3.19 иллюстрирует вывод этой утилиты.

Листинг 3.19

```
c:\WINNT\system32\inetsrv>dnsdiag mail.ru -v 1

mail.ru is an external server (not in the Exchange Org).
No external DNS servers on VSI. Using global DNS servers.
Created Async Query:
------------
QNAME = mail.ru
Type = MX (0xf)
Flags = UDP default, TCP on truncation (0x0)
Protocol = UDP
DNS Servers: (DNS cache will not be used)
192.168.0.32
192.168.0.10

Connected to DNS 192.168.0.32 over UDP/IP.
Received DNS Response:
------------
Error: 0
Description: Success
These records were received:
mail.ru MX 10 mxs.mail.ru
mxs.mail.ru A 194.67.23.20

Processing MX/A records in reply.
Sorting MX records by priority.

Target hostnames and IP addresses
------------
HostName: "mxs.mail.ru"
194.67.23.20
```

Утилита сообщила параметры MX-записи для домена **mail.ru** и необходимую дополнительную информацию. В примере вызова утилиты после параметра `v` стоит цифра `1`. Это номер виртуального сервера, соответствующего почтовому серверу (может быть иным в зависимости от конфигурации системы).

ГЛАВА 4

Обеспечение доступа в Интернет

Современная работа любой организации не представляется возможной без подключения к глобальной сети — Интернету. В подавляющем большинстве случаев провайдеры обеспечивают выделенный канал передачи данных, а подключаемой организации выделяется Ethernet-порт и сообщаются параметры для настройки сетевого интерфейса.

В этом случае в организации необходимо решить две задачи: обеспечить защиту внутренней сети и организовать работу всех компьютеров в Интернете при наличии только одного IP-адреса. Первая задача решается настройкой *межсетевого экрана (брандмауэра)*, вторая обеспечивается за счет технологии NAT. Комплексно решить проблему подключения небольших организаций можно с помощью аппаратного маршрутизатора на основе Linux.

Подключение к Интернету с использованием аппаратного маршрутизатора

Сегодня в продаже доступны различные модели маршрутизаторов, предназначенные для подключения к Интернету небольшой локальной сети. Обычно такие устройства включают в себя:

- один WAN-порт для подключения к Интернету;
- несколько LAN-портов (обычно до 4) для подключения локальных компьютеров;
- межсетевой экран с возможностями управления через обозреватель Интернета (по веб-интерфейсу);
- маршрутизатор с возможностями NAT, DHCP-сервера и т. п.

После первоначальной настройки такое устройство будет обеспечивать в локальной сети автоматическое предоставление адресов, предохранять сеть от доступа снаружи, работать в качестве коммутатора.

Существуют модели со встроенной точкой беспроводного доступа, что позволит организовать у себя беспроводное подключение таких устройств, как ноутбуки, медиапроигрыватели с беспроводным доступом и т. п. На рис. 4.1 представлен

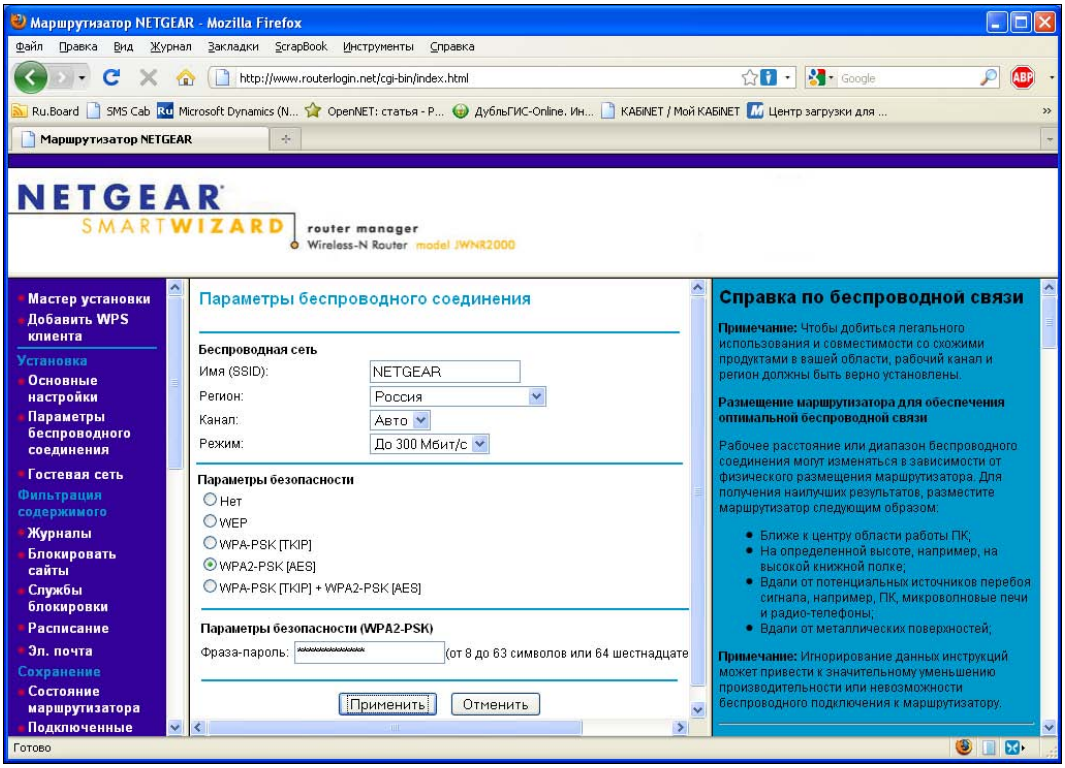


Рис. 4.1. Интерфейс управления маршрутизатором

интерфейс управления одной из моделей маршрутизаторов. Интерфейс локализован, каждая операция снабжена интерактивной справкой, поясняющей возможные параметры настройки. В результате устройство может подготовить к эксплуатации практически любой пользователь.

Как правило, в таких маршрутизаторах встроены простейшие средства фильтрации трафика (например, можно заблокировать сайты по списку), публикации внутренних ресурсов (можно опубликовать в Интернете, например, почтовый сервер организации или FTP-сервер) и т. д.

> ***Примечание***
>
> Если планируется ADSL-подключение, то можно сразу приобрести модели модемов, дополнительно включающие в себя как маршрутизатор, так и коммутатор на несколько портов, межсетевой экран и т. п.

Такие устройства просты в управлении, весьма надежны (как правило, они реализованы на Linux-платформах) и очень дешевы. В то же время у них есть ряд особенностей, которые не позволяют применять их в более крупных организациях. Отметим некоторые из них:

- маршрутизатор не имеет возможностей контролировать трафик по пользователям и формировать журналы (за длительный период) использования канала Интернета;

- в устройствах нет возможности регулировать полосу пропускания в зависимости от типа трафика и других параметров, что может привести к неудобствам работы в Сети нескольких пользователей (один пользователь может монополизировать канал при определенных условиях);
- отсутствует возможность проксирования трафика, что могло бы как ускорить работу в Интернете, так и сэкономить средства при тарификации по объему;
- дешевые модели маршрутизаторов не имеют средств для создания VPN-подключений между офисами. А модели, в которые такая функциональность включена, по стоимости уже сравнимы с программными решениями на основе простейших компьютеров;
- количество правил (публикации, запрета доступа и т. д.) обычно небольшое, этого достаточно для малых организаций или индивидуальных пользователей, но не перекрывает потребности более крупных организаций.

Network Address Translator

Технология трансляции адресов (Network Address Translator, NAT) позволяет осуществить подключение к Интернету практически любого числа компьютеров, задействовав при этом всего лишь один или несколько реальных адресов глобальной сети. Фактически NAT — это IP-маршрутизатор, который способен преобразовывать (транслировать) адреса и номера портов TCP/UDP-пакетов в процессе их пересылки.

Логика работы NAT достаточно проста. При получении от локального компьютера пакета, предназначенного для внешней сети, маршрутизатор пересылает пакет, заменив в нем частный IP-адрес на реальный IP-адрес, выделенный провайдером Интернета, и TCP-порт (или UDP-порт) источника на другой, *перенумерованный* порт. Информация об этом преобразовании сохраняется программой. После получения ответа NAT ищет "в своих записях", для какого локального запроса был выделен соответствующий порт. Если такая информация обнаружена, то NAT пересылает пакет локальному компьютеру, заменяя в пакете перенумерованный порт исходным. Если NAT не находит "у себя" записи о перенумерованном порте, то пакет отбрасывается. Таким образом, NAT одновременно является и межсетевым экраном, предотвращающим доступ из внешней сети к внутренним ресурсам.

Сервер NAT заменяет в пакетах адреса источника (назначения), номера портов и пересчитывает контрольную сумму пакета. Для большинства приложений такие изменения не вызывают каких-либо осложнений. Однако некоторые протоколы, например FTP, передают информацию об IP-адресах в своих данных. Поэтому для корректной работы таких протоколов NAT модифицирует и сами TCP-последовательности. Так, в Windows встроены редакторы для протоколов FTP, ICMP, PPTP, NetBIOS поверх TCP/IP. Если в организации на каком-либо компьютере применяется протокол, для которого необходимо внести аналогичные изменения в сам пакет, а соответствующего редактора не предусмотрено в операционной системе, то работа через NAT будет невозможна без использования для такой системы реального адреса. Например, сложности могут возникнуть при работе IP-телефонов

по протоколу H323 (внутри пакетов пересылаются адреса устройств). В таком случае либо следует искать специализированное программное обеспечение, либо заказывать дополнительный реальный IP-адрес и транслировать его на внутреннее устройство.

Подключение к Интернету в Windows

В Windows можно использовать несколько вариантов организации доступа в Интернет: совместное использование подключения как самый простой вариант и использование возможностей службы маршрутизации и удаленного доступа как серверное решение.

Использование службы маршрутизации и удаленного доступа

NAT в серверах Windows реализован в службе маршрутизации и удаленного доступа. NAT вместе со встроенным межсетевым экраном сервера является вполне надежным и функциональным вариантом подключения организации к Интернету.

Для настройки NAT после установки данной службы в оснастке управления следует добавить интерфейсы подключения к Интернету и локальной сети к протоколу маршрутизации NAT, для чего на вкладке **Общие** свойств интернет-интерфейса установить переключатель **Общий интерфейс подключен к Интернету** (Public Interface connected to the Internet), а для интерфейса локальной сети — **Частный интерфейс подключен к частной сети** (Private interface connected to private network). При наличии одного адреса подключения к Интернету нужно установить переключатель **Преобразовать TCP/UDP-заголовки** (Translate TCP/UDP headers) для свойств интернет-интерфейса.

Если необходимо опубликовать некоторые ресурсы локальной сети в Интернете, то следует создать соответствующие правила в оснастке NAT, которые определят, на какой частный адрес пересылать заданные протоколы.

Такой алгоритм работы достаточно эффективен и подходит в большинстве случаев. Однако он может приводить к неработоспособности отдельных функций программ, если они активизируются внешними запросами. Например, почтовый клиент MS Outlook при работе с сервером MS Exchange использует протокол RPC. Пройдя регистрацию на почтовом сервере, клиент находится в состоянии ожидания сигнала о приходе новой почты. Поскольку инициатором такого сигнала является не клиент, а внешняя система, то эти пакеты будут отброшены. Поэтому в данном примере клиент не будет получать автоматические сообщения о приходе новой почты, хотя сможет принимать и отправлять сообщения по команде пользователя.

Совместное использование интернет-подключения

Самый простой способ подключения к Интернету локальной сети организации на основе Windows, который не требует установки и настройки никаких дополнитель-

ных программ, — это использование *совместного подключения к Интернету*. Такая возможность предусмотрена уже с Windows 2000 Professional (операционной системы для рабочих станций).

Организовать совместное подключение к Интернету можно для любого варианта подключения к Сети (через модем или локальную сеть). Соответствующую настройку легко выполнить аналогично описываемому далее примеру подключения к Интернету с помощью модема.

Если компьютер имеет настроенное подключение к Интернету, то в папке задач **Сетевые подключения** есть значок, соответствующий данному подключению. Щелкните по нему правой кнопкой мыши и выберите команду **Свойства**. На вкладке **Дополнительно** в опции включения совместного использования доступа к Интернету поставьте соответствующий флажок.

При выборе совместного подключения IP-адрес сетевой карты компьютера автоматически изменяется на 192.168.0.1. Компьютер становится для других членов локальной сети сервером DHCP (диапазон 192.168.0.*x*) и сервером DNS. Поэтому на остальных компьютерах протокол TCP/IP нужно настроить с параметрами по умолчанию, которые предполагают автоматическое получение всех необходимых данных.

Публикация компьютеров в Интернете при совместном использовании подключения

Для публикации внутренних ресурсов в Интернете при совместном подключении достаточно создать соответствующее правило.

Покажем на примере, как выполнить в данном случае публикацию внутреннего FTP-сервера в Интернете.

1. Откройте окно свойств соединения с Интернетом, для которого организовано совместное использование. Перейдите на вкладку **Дополнительно**. Нажмите кнопку **Настройки**. Появится окно с перечнем типовых сервисов Интернета, доступ к которым во внутреннюю сеть можно осуществить через данное подключение.
2. Выберите нужный сервис и отметьте флажок, разрешающий его публикацию в Интернете. Появится окно, в котором нужно указать компьютер, где в локальной сети работает данный сервис. Обратите внимание, что можно указать как имя, так и IP-адрес компьютера. Если отдается предпочтение IP-адресу, то целесообразно прописать его на соответствующем компьютере статически, чтобы он не поменялся впоследствии (поскольку стандартно при совместном использовании подключения к Интернету адреса компьютерам выдаются динамически и могут изменяться). После завершения операций закройте все окна настройки, нажимая кнопку **OK**.

В результате данных настроек на FTP-запрос, поступающий из внешней сети на компьютер, непосредственно подключенный к Интернету, будет "отвечать" не этот компьютер, а указанный вами в описанных ранее операциях.

Таким способом можно настроить публикацию в Интернете любых сервисов, которые реализуются на локальных компьютерах сети. Если нужного сервиса нет в стандартном списке, вы можете его добавить, воспользовавшись соответствующей опцией. При определении параметров нового сервиса необходимо указать тип протокола (TCP или UDP) и номера портов.

Главная проблема, которая будет подстерегать вас при подобном решении, — это возможное отсутствие статического IP-адреса компьютера, подключенного к Интернету. Иными словами, если вы имеете в локальной сети информационный сервер и реализуете сеансовое подключение к Интернету, то его реальный адрес подключения будет меняться при каждом сеансе связи с провайдером, что, естественно, не позволит кому-либо обратиться к опубликованным ресурсам. В таком случае вам необходимо воспользоваться возможностями динамического DNS (динамические имена доступны на серверах **http://www.dyndns.com/**, **http://www.dtdns.com/** и др.; достаточно выполнить свободную регистрацию по правилам соответствующей службы).

Ограничения совместного использования подключения к Интернету

Из технических особенностей реализации совместного подключения вытекают ограничения его применения.

В сети организации часто необходимо вести контроль доступа к ресурсам Интернета, иметь возможность выборочно предоставлять доступ одним сотрудникам и запрещать другим, создавать списки запрещенных сайтов и т. п. Эти настройки не выполнить при данном способе подключения к Интернету.

Кроме того, в локальной сети допустим только диапазон адресов 192.168.0.0/24, причем адрес 192.168.0.1 может быть только у компьютера, обеспечивающего совместное подключение к Интернету. Данное ограничение также осложняет задачу настройки безопасного соединения между несколькими площадками организации (или настройку VPN-подключения пользователя к ресурсам другой организации в случае совпадающих диапазонов адресов локальных сетей).

Подключение к Интернету с помощью Microsoft TMG Server

В составе семейства серверных решений от Microsoft есть специализированный сервер для обеспечения безопасного подключения организации к Интернету — Microsoft Forefront Threat Management Gateway Server.

Сервер включает в себя как межсетевой экран с большим количеством настроек, так и прокси-сервер для кэширования трафика. TMG-сервер может выступать в качестве сервера безопасных удаленных подключений (VPN). Корпоративные редакции позволяют объединить несколько серверов в единый массив с общими правилами управления, фильтрации и единым кэшем данных.

Настройка сервера не представляет особых сложностей. Все операции выполняются с помощью мастеров в графическом режиме в оснастке управления (рис. 4.2). А пра-

вила ничем не отличаются от традиционных для межсетевых экранов: нужно указать, какой протокол с каких компьютеров, кому, куда и по какому расписанию необходимо разрешить или запретить.

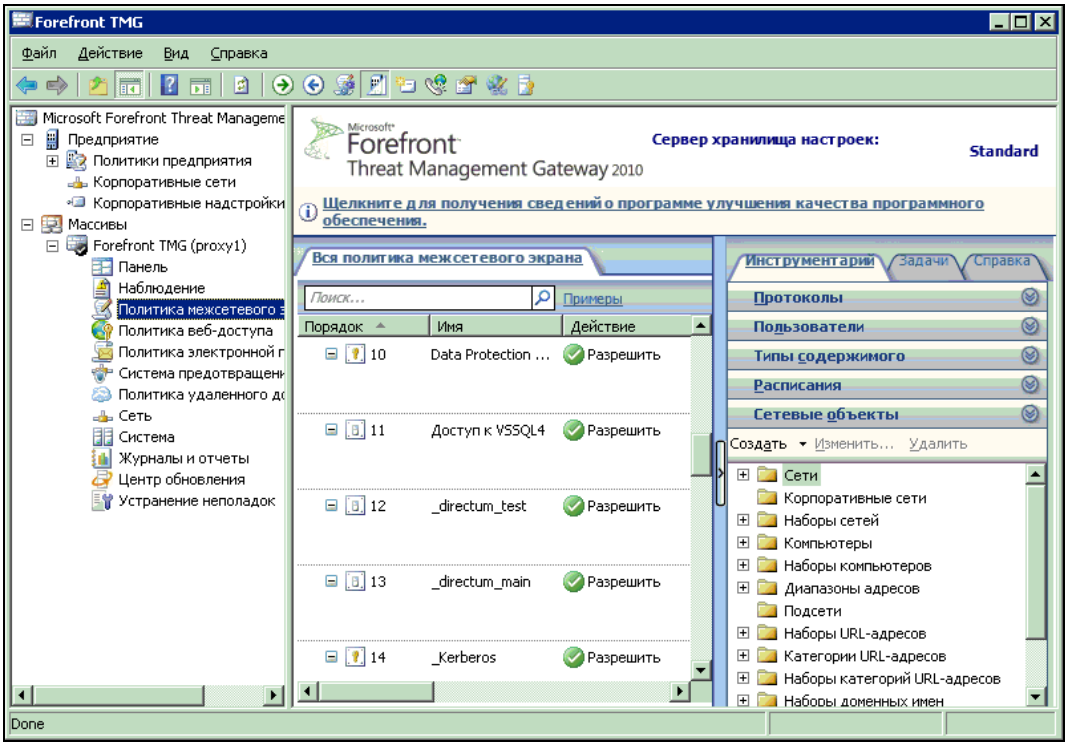


Рис. 4.2. Оснастка управления сервером Microsoft TMG

Опишем основные моменты, которые администраторы, начинающие работу с TMG-сервером, не всегда принимают во внимание.

- Понятие "*все* протоколы" или "*весь* трафик" в TMG-сервере описывают только те протоколы, которые явно определены в параметрах сервера. Иными словами, если протокол не описан, то он и не будет пропущен, если вы включите разрешение для всех протоколов.
- Правила в TMG-сервере применяются последовательно так, как они записаны. Поэтому, если вы хотите что-либо запретить всем, а разрешить конкретным пользователям, то более "верхним" должно быть правило разрешения, а за ним следовать правило запрета. Другой момент, который не всегда учитывается: правила, в которых действие разрешено для всех пользователей, должно быть расположено выше правила, в котором этот протокол разрешается или запрещается конкретному пользователю. В противном случае сервер будет сначала запрашивать аутентификационные данные для проверки пользователей, что сделает невозможным анонимный пропуск протокола.

- Обратите внимание на наличие системных правил в сервере. Например, этими правилами разрешен неконтролируемый обмен с серверами Microsoft. Конечно, такая настройка помогает службам обновления, но часто наличие подобной "бреши" упускается из виду администраторами.
- Сервер Microsoft TMG рекомендуется в тех случаях, когда необходим контроль работы пользователей на основе их членства в группах безопасности домена. В то же время, не все приложения корректно могут передавать аутентификационные данные на сервер. Конкретные советы зависят от установленных приложений. Часто проблемы можно решить, разрешив стандартный вариант аутентификации (по умолчанию включен только интегрированный; настройка производится на вкладке **Web Proxy** окна свойств внутренней сети). В крайнем случае вам придется разрешить анонимную работу для соответствующих протоколов.
- На рабочих местах необходимо устанавливать клиент сервера. Его версию лучше загрузить с сайта Microsoft. Но некоторые приложения не работают при наличии такого клиента. Например, автор встречался с подобной ситуацией при настройке программного IP-телефона и клиентских программ работы со счетами в банке. В этом случае либо необходимо деинсталлировать клиента, либо в его дополнительных настройках отключить клиента для конкретного приложения.
- Еще один класс приложений, для которых лучше отказаться от данного сервера, — это задачи IP-телефонии и IP-видео. Часто для этих приложений необходим специальный редактор для пакетов при использовании NAT.

Поиск причин запрета трафика

В Microsoft TMG Server имеется удобный механизм онлайнового контроля работы сервера — журнал реального времени.

Достаточно выбрать необходимые фильтры и включить просмотр. На экране вы увидите пакеты, которые удовлетворяют заданным условиям фильтрации, и причины, по которым пакет пропущен или остановлен. Обычно следует обращать внимание на название правила, которое не пропустило пакет, и на тип отношения сетей (при наличии нескольких настроенных групп сетей в Microsoft TMG Server). После того как причины будут найдены, устранить их останется только делом администратора.

Подключение к Интернету с использованием серверов Ubuntu

Возможностей тонкой настройки межсетевого экрана и прокси-сервера на Linux-компьютерах несравнимо больше, чем в Windows.

Классический межсетевой экран Linux — это пакет iptables. Функционал NAT встроен в этот пакет. Настройка iptables несколько неудобна для обычного пользователя из-за большой функциональности, поэтому в Ubuntu для управления параметрами межсетевого экрана применяется программа `ufw`, имеющая упрощенный

интерфейс настройки и вполне достаточная для защиты конкретного хоста (компьютера). Если же вы настраиваете доступ в Интернет для офиса, то необходимо задействовать возможности iptables, которые также будут описаны в этой главе.

Настройка *ufw*

После установки системы межсетевой экран в Ubuntu отключен. Включить его можно командой

```
sudo ufw enable
```

Состояние межсетевого экрана (включен или выключен) можно увидеть, выполнив команду `sudo ufw status`.

Если вы управляете сервером удаленно, то активизация межсетевого экрана приведет к потере с ним связи. Поэтому необходимо включить межсетевой экран, предварительно создав правило, разрешающее удаленное управление. Если у вас подключение по протоколу SSH, то для включения межсетевого экрана выполните команду

```
sudo ufw allow proto tcp from any to any port 22
```

перед командой `sudo ufw enable`.

Правильным подходом для системных администраторов является первоначальный запрет на все подключения с последующим открытием нужных протоколов. Для этого служит команда выбора правил по умолчанию:

```
sudo ufw default deny
```

Правила доступа в `ufw` создать достаточно легко. Следует указать только нужное действие (разрешение или запрет: `allow`/`deny`) и параметры протокола. Например, команда `sudo ufw allow 53` разрешит доступ к компьютеру по портам 53 (используется при работе DNS). Вместо указания портов можно писать имена служб (система использует параметры служб, перечисленные в файле /etc/services, просмотрев его, вы можете уточнить допустимые названия), например, `sudo ufw allow smtp`.

При необходимости максимально точно указать параметры фильтрации нужно применять следующий синтаксис:

```
sudo ufw allow|deny proto <протокол> from <источник> port <порт>
to <назначение> port <порт>
```

В качестве протоколов указывают либо `tcp`, либо `udp`; в качестве источника/назначения можно указывать конкретные IP-адреса, подсети (например, 192.168.0.0/24) или `any` для любого назначения.

Межсетевой экран *iptables*

Команды настройки `iptables` потребуются в тех случаях, когда вы предполагаете задействовать межсетевой экран данного сервера для обеспечения работы с Интернетом всего офиса или же включить какие-либо специальные возможности, не реализуемые программой `ufw`.

Последовательность обработки пакета (таблицы)

Самое сложное при работе с `iptables` заключается в том, чтобы первоначально разобраться с принципами фильтрации в этой программе.

Любой пакет на каждом сетевом интерфейсе компьютера несколько раз анализируется на соответствие заданным условиям. При удовлетворении условиям к пакету

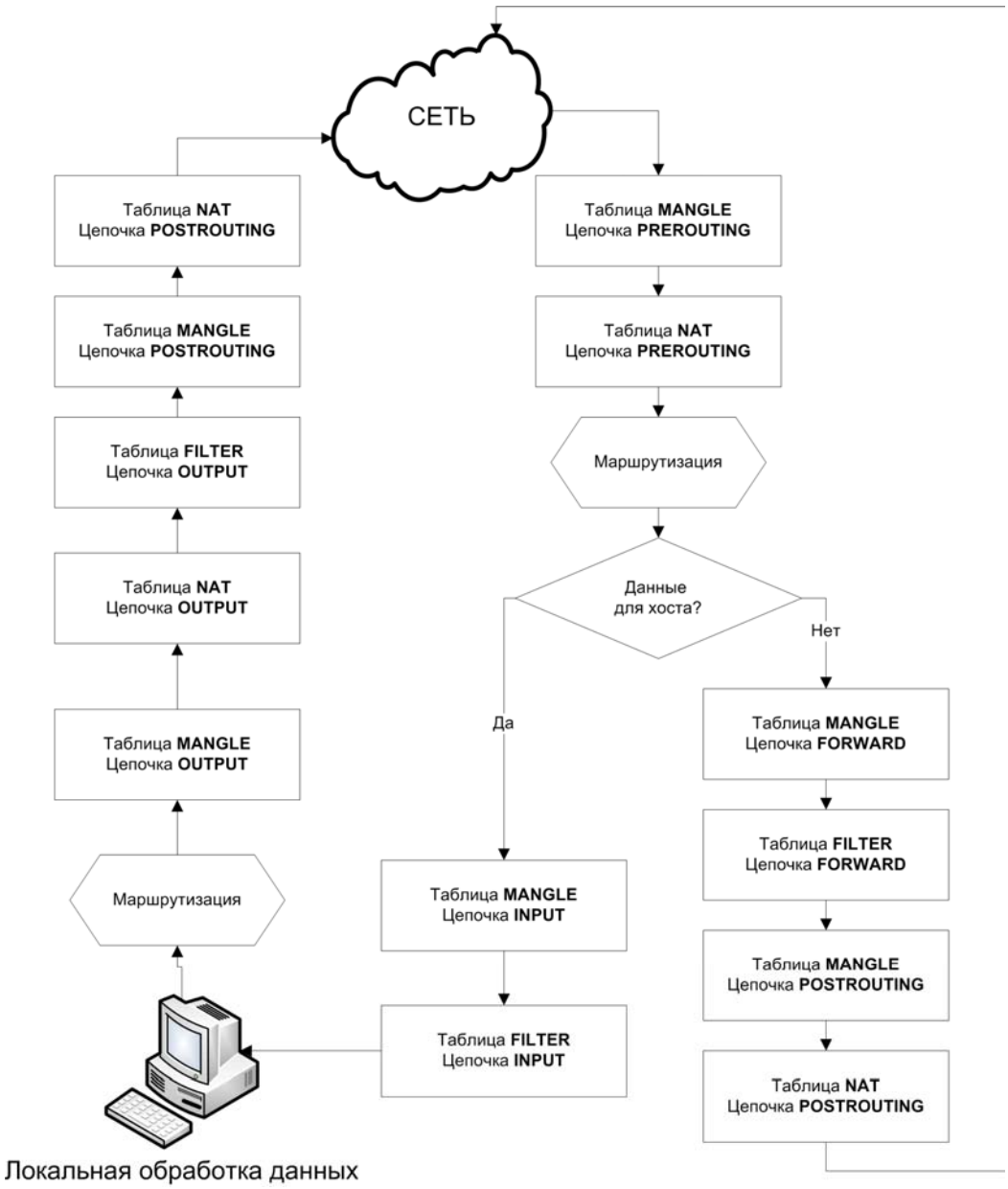


Рис. 4.3. Последовательность применения правил обработки пакета в `iptables`

применяется соответствующее правило, и дальнейший анализ на данном этапе не производится. Если ни одно из правил не содержит условий, соответствующих пакету, к нему применяются правила по умолчанию. Подобные наборы правил носят названия *таблиц*.

Существуют три таблицы правил: *filter* — основная таблица, *nat* — для пакетов, создающих новое подключение (можно менять адреса источника и назначения пакета), и *mangle* — для пакетов специального типа.

Межсетевой экран может анализировать один и тот же пакет несколько раз на различных этапах его обработки. Так, у таблицы filter можно создавать правила, применяемые при *приеме* пакетов данным интерфейсом (INPUT), при *передаче* пакета через этот же интерфейс (через который он принят) — OUTPUT и при *пересылке* пакетов на другой сетевой интерфейс (FORWARD). Для таблицы nat предусмотрены варианты PREROUTING (при приеме пакета данным интерфейсом), OUTPUT (применяется к пакетам *перед* маршрутизацией через данный интерфейс) и POSTROUTING (правило применяется перед тем, как пакет будет передан с данного интерфейса). Таблица mangle имеет только два варианта — PREROUTING и OUTPUT. Их смысл аналогичен одноименным цепочкам таблицы nat.

На рис. 4.3 показана последовательность применения таблиц обработки для пакетов как поступающих на компьютер из сети, так и отсылаемых из компьютера во внешнюю сеть.

Для большей наглядности при составлении правил можно создавать собственные (пользовательские) цепочки. Смысл пользовательских цепочек состоит в том, что определенный блок анализа и обработки пакетов оформляется отдельной частью правил. После чего в заданном месте обработки управление передается на такую пользовательскую цепочку, а потом возвращается назад. Таким способом проще анализировать большой объем правил.

Использование *iptables* в Ubuntu

Перед использованием `iptables` демон `ufw` необходимо отключить (`sudo ufw disable`). Иначе разобраться в совместном действии правил, которые подгружаются `ufw` и создаются явно командами `iptables`, будет практически невозможно.

Ubuntu не содержит сценарий автозапуска `iptables`, поэтому в системе отсутствуют соответствующие файлы настроек и, например, выполнить команду сохранения конфигурации межсетевого экрана (как это делается в других версиях Linux) не получится. Чтобы применить заданные настройки межсетевого экрана `iptables` при каждом запуске системы, вам следует:

1. Создать необходимые правила фильтрации трафика с использованием команды `iptables`.
2. Экспортировать настройки в файл командой `iptables -save`.
3. Настроить автоматическую загрузку настроек из этого файла при каждом запуске Ubuntu.

Автоматическую загрузку проще всего сделать через возможности настройки конфигурации сетевого интерфейса путем добавления строк, описывающих действия, которые следует выполнить *перед* включением сетевого интерфейса и при его *отключении*. Для этого достаточно настроить и сохранить действующие на данный момент правила (например, командой `sudo bash-c "iptables -save > /etc/iptables.rules"`), после чего открыть для редактирования файл /etc/network/interfaces и добавить в конец блока настроек, описывающих сетевой интерфейс, следующие строки (вторая строка обеспечивает автоматическое сохранение настроек конфигурации при выключении системы):

```
pre-up iptables -restore < /etc/iptables.rules
post-down iptables -save -c > /etc/iptables.rules
```

Обратите внимание, чтобы файл /etc/iptables.rules существовал перед перезагрузкой системы, в противном случае сетевой интерфейс не будет включен.

Правила *iptables*

К пакетам, которые будут удовлетворять условиям фильтров, можно применить несколько действий. Они могут быть пропущены (вариант ACCEPT), удалены с сообщением источнику об ошибке передачи данных (REJECT), просто уничтожены без оповещения (DROP). Существует также возможность настройки и применения пользовательского варианта обработки (QUEUE).

Обратите внимание, что правила исполняются последовательно; если пакет удовлетворяет условиям, то к нему применяются правила, заданные в этой строке, и цепочка дальше не обрабатывается. Поэтому порядок правил очень важен. Обратите особое внимание, куда вы добавляете новое правило: в начало списка (параметр `-I`) или в его конец (параметр `-A`).

В общем виде команда редактирования правил межсетевого экрана выглядит следующим образом:

```
iptables [-t table-name] command chain-name parameter-1 option-1
parameter-n option-n
```

Параметр *table-name* позволяет выбрать используемую таблицу. Параметр *command* определяет выполняемое действие: добавление или исключение правила. *Chain-name* — это название соответствующего правила. Далее следует набор пар *parameter-n option-n*, которые, собственно говоря, и определяют конкретные действия программы.

Если в команде опущено название таблицы, то правила добавляются в таблицу filter.

Команды

В табл. 4.1 приведена часть команд (полный перечень можно отобразить в справке `iptables`).

> ***Примечание***
>
> Вместо параметров `-A`, `-D`, `-I`, `-R`, `-L`, `-F` при написании команд можно указывать, соответственно, `--append`, `--delete`, `--insert`, `--replace`, `--list`, `--flush` (обратите внимание на то, что указываются *два дефиса*).

Таблица 4.1. *Команды* `iptables`

Команда	Действие
`-L`	Выводит список действующих правил (для отображения подробного списка используйте параметр `-v`)
`-F`	Удаляет цепочку, имя которой приведено далее в качестве параметра. Если имя не указано, то *удаляет все правила* межсетевого экрана
`-A`	Добавляет новое правило в конец списка
`-D`	Удаляет правило в соответствии с указываемым далее номером
`-I`	Добавляет правило и размещает его по списку с указанным номером. Если номер правила не указан, то оно размещается *первым*
`-P`	Определяет правило по умолчанию для соответствующей цепочки

Параметры

В табл. 4.2 перечислены наиболее часто используемые параметры команды `iptables` (полный перечень отображается в справке команды).

Таблица 4.2. *Параметры команд* `iptables`

Параметр	Назначение
`-d`	Назначение пакета. Можно указывать имя хоста, IP-адрес или подсеть (либо как 192.168.0.0/255.255.255.0, либо как 192.168.0.0/24)
`-s`	Источник пакета. Синтаксис аналогичен параметру `-d`. Заметим, что символы `0/0` определяют *все сети*
`-f`	Правило будет применено только к фрагментированным пакетам (символ `!` после данного параметра определяет область применения для нефрагментированных пакетов)
`-i`	Интерфейс (eth0, ppp0 и т. п.). Если параметр опущен, то правило будет применяться ко всем интерфейсам. Знак `+` используется в качестве маски: `eth+` обозначает *все* интерфейсы Ethernet
`-o`	Выходной интерфейс (в правилах с OUTPUT и FORWARD)
`-j`	Определяет правило (ACCEPT, DROP, QUEUE, ...). Применение без указания опции используется в правилах с подсчетом пакетов (каждый пакет увеличивает значение счетчика на единицу)
`-p`	Протокол IP: обычно указывают `icmp`, `tcp`, `udp` или `all` (для обозначения любого протокола). Перечень протоколов можно уточнить по содержимому файла /etc/protocols

Опции

В табл. 4.3 приведены наиболее распространенные опции (полный перечень отображается в справке команды).

Таблица 4.3. *Опции команд* `iptables`

Опция	Назначение
`--dport`	Порт назначения. Можно указывать диапазон (по принципу `--dport 3000:3200`) и применять символ `!` для указания исключения *(кроме указанных портов)*. Допустимый диапазон значений 0—65 535
`--sport`	Порт источника. Синтаксис аналогичен `--dport`
`--syn`	Тип пакетов — SYN. Можно использовать символ `!` для указания всех остальных пакетов
`--tcp-flags`	Определяет пакеты со специальными флагами: `ACK`, `FIN`, `PSH`, `RST`, `SYN` и `URG`. Допускаются обозначения `ALL` и `NONE`
`--tcp-option`	Определяет дополнительные опции пакетов протокола IP
`--icmp-type`	Имя или номер протокола ICMP. Допустимые имена можно вывести на экран командой `iptables -p icmp -h`

Некоторые опции могут присутствовать при указании в командной строке `iptables` дополнительно загружаемых модулей. Так, при загрузке модуля `limit` можно указывать максимальное число пакетов за единицу времени (например, `--limit 5/hour` определяет максимально 5 пакетов данного типа в час). Модуль `state` позволяет использовать в правилах состояние соединения: `--state ESTABLISHED`, `--state INVALID`, `--state NEW`, `--state RELATED`. Модуль `mac` разрешает включить в правила проверку MAC-адресов (опция `--mac-source`). Полный список дополнительных модулей доступен в справочной подсистеме.

> ***Примечание***
>
> В правиле, которое служит для ограничения числа пакетов, должны присутствовать два параметра: `--limit`, определяющий, как быстро будет уменьшаться счетчик максимально допустимого числа пакетов, и `--limit-burst`, указывающий на максимальное значение пакетов, для которого это правило будет выполняться. Иными словами, правило будет выполняться, пока число пакетов в счетчике будет меньше значения `limit-burst`, которое автоматически уменьшается со скоростью `limit`. Если параметр `limit-burst` не указан, то применяется значение по умолчанию, равное 5. Правила лимитирования необходимо применять парой: первое правило будет пропускать пакеты, пока счетчик не превысил заданного значения, а второе — уничтожать пакеты, скорость поступления которых привела к превышению показателя лимита.

Настройка NAT

Для работы NAT необходимо включить маршрутизацию в ядре Linux. Делается это командой

```
sudo bash-c "echo 1 > /proc/sys/net/ipv4/ip_forward"
```

Однако эта операция не сохранит настройки *после перезагрузки* сервера. Поэтому, если вы собираетесь включить маршрутизацию постоянно, отредактируйте файл /etc/sysctl.conf. Найдите в нем строчку `net.ipv4.ip_forward=1` и удалите в ней комментарий (символ `#` в начале строки). Чтобы эта настройка вступила в силу, нужно

перезагрузить систему (или до перезагрузки включите маршрутизацию согласно предыдущему варианту).

В `iptables` существуют два варианта правил настроек при использовании NAT: для исходящего трафика (SNAT) и входящего (DNAT, иными словами, это публикация внутренних ресурсов сети наружу).

Существует упрощенный вариант правил, предназначенный специально для работы с динамическим внешним адресом (частый случай при dial-up-подключении к Интернету). При этом для включения NAT достаточно добавить следующее правило:

```
iptables --table nat --append POSTROUTING --out-interface eth0
-j MASQUERADE
```

> ***Примечание***
>
> Кроме этого правила, если по умолчанию вы запретили пересылку, следует разрешить получение пакетов из локальной сети по внутреннему интерфейсу, например, командой `iptables --append FORWARD --in-interface eth1 -j ACCEPT`.
>
> В этом примере и последующих предполагается, что `eth0` — это интерфейс Интернета, `eth1` — интерфейс, смотрящий в локальную сеть.

Обратите внимание, что настройки POSTROUTING не отражаются в консоли при исполнении команды `sudo iptables -L` без указания таблицы. Вы увидите по этой команде только правила, включенные в таблицу filter. Для того чтобы увидеть настройки работы в NAT, необходимо не забыть указать имя таблицы:

```
sudo iptables -L -t nat
```

Указанный вариант настройки NAT не рекомендуется для серверов, у которых точно известна настройка внешнего интерфейса. Хороший стиль настройки `iptables` — указание максимально точных параметров, чтобы исключить любые неконтролируемые пути доступа в систему. Поэтому для настройки NAT целесообразно воспользоваться следующим синтаксисом:

```
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4
```

В этом примере `1.2.3.4` — условно принят как внешний IP-адрес сервера.

Чтобы обеспечить пересылку пакетов, поступающих на внешний IP-адрес сервера, на какой-либо адрес из внутренней сети, можно задать команду:

```
iptables -t nat -A PREROUTING -d 1.2.3.4 -p tcp --dport 80 -j DNAT
--to 192.168.1.1
```

В команде можно указывать протоколы, порты и т. п. Например, следующая команда обеспечит публикацию во внешней сети внутреннего почтового сервера:

```
iptables -t nat -A PREROUTING -p tcp -i eth0 --destination-port 25
-j DNAT --to-destination 192.168.1.10
```

Кроме этого, существует возможность преобразования (перенаправления) пакетов с одного порта на другой, например, такой командой:

```
iptables -t nat -A PREROUTING-i eth1 -p tcp --dport 80 -j REDIRECT
--to-port 3128
```

Эта команда отсылает пакеты, предназначенные для адреса 80 (WWW-сервер), на порт 3128. Такая настройка часто встречается при использовании "прозрачного" прокси.

Очистка всех правил *iptables*

Перед началом настройки межсетевого экрана целесообразно очистить все ранее созданные правила. Представленные далее команды удаляют все правила межсетевого экрана (первая команда — в цепочке filter, следующие — в явно указанных цепочках):

```
iptables -F
iptables -t nat -F
iptables -t mangle -F
```

Эти команды удаляют пользовательские правила в соответствующих цепочках:

```
iptables -X
iptables -t nat -X
iptables -t mangle -X
```

Назначение политик по умолчанию

В большинстве случаев политики по умолчанию настраивают как запрет для входящего трафика и как разрешение для исходящего:

```
iptables -P OUTPUT ACCEPT
iptables -P INPUT DROP
iptables -P FORWARD ACCEPT
```

Конечно, для более точной настройки следует установить все политики по умолчанию в DROP. Однако такая настройка более трудоемка и предполагает знание администратором параметров служб системы для создания к ним соответствующих правил доступа. Первоначально вполне достаточно конфигурации, описанной в следующем примере. В дальнейшем, по мере приобретения опыта, администратор сможет создавать все более "жесткие" правила доступа, настраивая не один, а несколько рубежей сетевой защиты сервера.

Пример настройки *iptables*

Чтобы сервер мог выполнять функции межсетевого экрана, необходимо добавить несколько команд:

- разрешение приема трафика по интерфейсу локальной сети;
- разрешение приема трафика локальным интерфейсом (для обеспечения работы сетевых служб сервера);
- разрешение приема из внешней сети ответов на исходящий трафик (состояние пакетов ESTABLISHED и RELATED);
- команду включения NAT (если внутренняя сеть использует механизм трансляции адресов).

Такой настройке соответствует цепочка команд, приведенная в листинге 4.1.

Листинг 4.1

```
iptables -P OUTPUT ACCEPT
iptables -P INPUT DROP
iptables -P FORWARD ACCEPT
iptables -A INPUT -i eth0 -p ALL -m state --state ESTABLISHED,
RELATED -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i eth1 -j ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

В результате мы получили простейшую рабочую конфигурацию `iptables`. На практике правила `iptables` необходимо составлять более конкретно, чтобы заблокировать потенциально нежелательный трафик. Например, вместо разрешения приема пактов из любых сетей на внутренний интерфейс сервера доступ можно ограничить только конкретным диапазоном:

```
iptables -A INPUT -s 192.168.10.0/255.255.255.0 -i eth1 -j ACCEPT
```

Опытные администраторы составляют еще более конкретные правила, явно описывая в правилах весь разрешенный трафик (например, почтовые протоколы, протоколы просмотра веб, работы в ICQ и т. д.).

Пользовательские цепочки команд

Пользовательские цепочки служат для большей удобочитаемости правил фильтрации пакетов (листинг 4.2).

В этом примере сначала создается пользовательская цепочка, в которой планируется выполнить ряд обработок. Это протоколирование пакетов из сети 192.168.1.0/24 с последующим их уничтожением. В этой цепочке присутствуют только две команды фильтрации, а третья команда фактически возвращает управление в исходную точку.

Команды фильтрации на межсетевом экране будут исполняться в такой последовательности. Сначала команда цепочки `INPUT` (`iptables -A INPUT -p ALL -i eth0 -m state...`), после выполнения первой команды пакеты передадутся в цепочку `my_packets`, после выполнения трех команд этой цепочки следующей командой будет правило уничтожения всех широковещательных пакетов (последнее правило данного примера).

Листинг 4.2

```
iptables -N my_packets
iptables -A my_packets -p ALL -i eth0 -s 192.168.1.0/24 -j LOG
--log-prefix "bad_network "
iptables -A my_packets -p ALL -i eth0 -s 192.168.1.0/24 -j DROP
```

```
iptables -A my_packets -p ALL -j RETURN
iptables -A INPUT -p ALL -i eth0 -m state --state ESTABLISHED,
RELATED -j ACCEPT
iptables -A INPUT -p ALL -i eth0 -j my_packets
iptables -A INPUT -m pkttype --pkt-type broadcast -j DROP
...
```

Некоторые полезные функции *iptables*

Ловушки

У специалистов информационной безопасности существует такой метод противодействия атакам, как создание ловушек. Ловушка — это порт, с которым можно установить соединение, но закрыть его не получится. В результате соединение будет завершено только по тайм-ауту (обычно этот период составляет более 10 мин), атакующая система все это время будет ожидать ответов и расходовать ресурсы на поддержание соединения.

Например, таким образом можно ввести злоумышленника в заблуждение, если поставить ловушки на порты NetBIOS:

```
iptables -A INPUT –i eth1 -p tcp -m tcp –m mport --dports 135,139
-j TARPIT
```

Фильтрация по содержимому пакета

В правилах можно задать критерий нахождения заданной последовательности символов в передаваемой информации. Причем вы можете анализировать как служебные данные пакетов, так и передаваемые в нем данные. Подобным способом можно, например, запретить передачу определенного типа файлов, если указать в критерии характерные для них последовательности символов. Многие форматы можно однозначно определить по служебным заголовкам, содержащимся в файлах. Такие последовательности несложно найти в Интернете.

Предупреждение атак

Некоторые сетевые атаки, основанные на отказе в обслуживании, можно пресечь, если на межсетевом экране включить лимитирование пропуска определенных пакетов. Следующие команды вводят ограничение "один пакет в секунду" (предупреждают атаку "Syn-flood") и запрещают атаку "Ping of death":

```
iptables -A FORWARD -p tcp –syn –m limit --limit 1/s -j ACCEPT
iptables -A FORWARD -p icmp --icmp-type echo-request-m limit
--limit 1/s -j ACCEPT
```

Часто осуществляют фильтрацию пакетов с "плохим" состоянием:

```
iptables -A INPUT -p ALL -m state --state INVALID -j DROP
```

или новых пакетов, но без установленного признака `syn`:

```
iptables -A INPUT -p TCP! –syn –m state --state NEW -j DROP
```

Открытие портов по специальным запросам

`Iptables` позволяет выполнить такие специфические настройки, как открытие порта после принятия определенной последовательности пакетов.

Идея заключается в том, что в настройках межсетевого экрана разрешаются установленные соединения, а они открываются только после получения определенной последовательности входных пакетов. Таким способом легко маскируется доступ к серверу Интернета: злоумышленник не сможет никак даже начать подключение, если не знает определенного алгоритма входа. В следующих ссылках вы найдете некоторые варианты реализации такой технологии:

http://www.opennet.ru/base/sec/port_knocking.txt.html

http://gentoo-wiki.com/HOWTO_Port_Knocking

Отладка *iptables*

Для настройки межсетевого экрана используют протоколирование `iptables`. Для этого достаточно создать правило, описывающее необходимые фильтры, и применить к нему действие `LOG` (`-j LOG`). Информация о пакетах, которые будут удовлетворять такому правилу, запишется в системный журнал. Например, если последним правилом в `iptables` поставить протоколирование всех пакетов:

```
iptables -A INPUT -j LOG
```

то в системном журнале появятся сообщения обо всех пакетах, которые достигли этого этапа и впоследствии уничтожены, т. к. политика по умолчанию для таблицы INPUT установлена в DROP.

Существует несколько параметров, которые пригодны в режиме отладки. Наибольший практический интерес представляет ключ `--log-prefix "`*`метка`*`"`, добавляющий к описаниям пакетов символы *`метка`*. Это позволяет легко отфильтровать сообщения от `iptables` в системном журнале, который на рабочих серверах пополняется с достаточно высокой скоростью:

```
tail -f /var/log/syslog | grep метка
```

Задавая различные метки, команды протоколирования можно поместить в различные цепочки `iptables` и быстро найти ошибки настройки, наблюдая за журналом одновременно в нескольких консолях системы.

Блокировка попыток перебора паролей

Если к компьютеру открыт доступ из Интернета, то можно гарантировать наличие попыток его взлома. Одним из самых простых способов защиты является установка программы, блокирующей IP-адрес злоумышленника после обнаружения нескольких попыток перебора паролей.

Для установки подобной программы выполните команду

```
apt-get install fail2ban
```

Эта команда установит демон Fail2Ban на компьютер. Настройки программы хранятся в папке /etc/fail2ban. Файл /etc/fail2ban/fail2ban.conf определяет параметры протоколирования демона.

Более интересен файл /etc/fail2ban/jail.conf, определяющий настройки демона. Этот файл состоит из блоков (секций), первая секция — `[DEFAULT]` — определяет настройки программы по умолчанию, остальные — уточняют параметры для наиболее известных служб системы. Рассмотрим типовую конфигурацию по умолчанию.

```
[DEFAULT]
ignoreip = 127.0.0.1
maxretry = 5
findtime = 600
bantime = 600
```

Эта конфигурация означает следующее. Для локального компьютера проверки отключены. Для всех остальных максимальное число неуспешных попыток подключения — 5 (параметр `maxretry`) в течение 10 минут (параметр `findtime` — 600 секунд), после чего адрес будет заблокирован на 10 минут.

Блокировка адреса производится включением дополнительного правила в межсетевой экран `iptables`.

В папках action.d хранятся конфигурации для запускаемых программой операций (например, отправки почтового сообщения, добавления блокировки и т. д.), а в папке filter.d — правила определения попыток неудачного входа (в этих файлах содержатся шаблоны для поиска соответствующих строк в журналах системы, свидетельствующих о неудачной попытке входа).

Настройка VPN-подключения к интернет-провайдеру

Интернет-провайдеру важно быть уверенным, что он предоставляет доступ именно тем пользователям (организации), с которыми заключен договор. Если в одном здании расположено несколько организаций, подключенных к единой физической сети, то для авторизации доступа в Интернет в таких случаях активно используется технология VPN. Канал Интернета будет открыт только в том случае, если на сервере провайдера успешно завершится аутентификация пользователя.

> ***Примечание***
>
> Описанным далее способом можно осуществлять не только подключение к Интернету, но и к сети удаленного офиса. Следует только настроить правильные таблицы маршрутизации, чтобы сервер знал, какие пакеты отправлять по такому соединению. Единственное отличие состоит в том, что провайдеры не шифруют трафик, а при подключении к удаленному офису эта опция должна быть настроена обязательно.

Настройка такого типа подключения может быть выполнена и средствами Microsoft, но в этом случае — по опыту автора — возможны проблемы с маршрутизацией трафика между сетями офисов. Более рационально настроить такие под-

ключения с использованием возможностей Linux-систем. Рассмотрим необходимые настройки для подключения сервера Ubuntu к интернет-провайдеру, открывающему доступ в Сеть только после успешной авторизации.

Установите VPN-клиента командой

```
sudo apt-get install pptp-linux
```

После завершения установки система полностью готова к соединению с VPN-сервером, имеющим настройки по умолчанию. Необходимо только создать соответствующие конфигурации для подключения.

Откройте файл /etc/ppp/chap-secrets (в целях безопасности права доступа на этот файл по умолчанию установлены только для администратора системы; не следует их менять). Добавьте в него строку с параметрами учетной записи, которая будет использоваться для подключения к VPN-серверу:

```
DOMAIN\\USERNAME PPTP PASSWORD *
```

В случае локальной учетной записи опустите название домена и обратные слеши. Если пароль содержит специальные символы, то его следует взять в кавычки.

В папке /etc/ppp/peers создайте файл с именем, которое будет использоваться для подключения, например my_vpn. Добавьте в него строки из листинга 4.3.

Листинг 4.3

```
pty "pptp имя_сервера_провайдера --nolaunchpppd"
name DOMAIN\\USERNAME
remotename PPTP
file /etc/ppp/options.pptp
persist
maxfail 0
ipparam my_vpn
```

В качестве *имя_сервера_провайдера* укажите доменное имя или IP-адрес VPN-сервера провайдера. Параметр `DOMAIN\\USERNAME` должен совпадать с именем, указанным в файле /etc/ppp/chap-secrets. Параметр `persist` указывает, что это соединение должно оставаться постоянным, иными словами, система будет пытаться установить его при обрыве вновь и вновь (число попыток не ограничено — параметр `maxfail 0`).

Внесите в файл /etc/resolf.conf параметры DNS-серверов, которые сообщили вам при заключении договора.

Теперь для установления VPN-подключения достаточно, имея права суперпользователя, выполнить команду (в качестве параметра указано имя подключения — `my_vpn`)

```
pon my_vpn
```

А для отключения — `poff my_vpn`.

Примечание

Для диагностики процесса подключения можно выполнить команду `pon` со следующими параметрами: `debug dump logfd 2 nodetach`.

Если необходимо, чтобы подключение к Интернету восстанавливалось автоматически при каждой перезагрузке сервера, то добавьте в файл /etc/network/interfaces следующие строки:

```
auto tunnel
iface tunnel inet ppp
provider my_vpn
```

Обычно интернет-провайдеры отключают требование шифрования трафика для таких подключений. Настройка шифрования включена в файле /etc/ppp/options.pptp, опции которого импортируются в файл конфигурации конкретного VPN-подключения. Если шифровать трафик не нужно, то в файле /etc/ppp/options.pptp необходимо закомментировать строку `require-mppe-128`. А для того чтобы подключаться к VPN-серверам, использующим шифрование, эту строку нужно включить в файлы индивидуальных настроек туннелей.

После установления VPN-соединения вы увидите среди сетевых интерфейсов новый с именем `ppp0` (листинг 4.4).

Листинг 4.4

```
$ ifconfig -a
..... часть листинга, соответствующая интерфейсам eth0 и lo, опущена
ppp0 Link encap: Point-to-Point Protocol
inet addr:192.168.32.208 P-t-P:192.168.32.201 Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1396 Metric:1
RX packets:11 errors:0 dropped:0 overruns:0 frame:0
TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:3
RX bytes:486 (486.0 B) TX bytes:500 (500.0 B)
```

При создании VPN-подключения в системе меняется шлюз по умолчанию. Все пакеты за пределы локальной сети будут направляться в интерфейс ppp0. Такая настройка может привести к проблемам установления подключения к Интернету для провайдеров, которые предоставляют клиентам локальные адреса из сети, не совпадающей с сетью, в которой расположен VPN-сервер. Например, если вам предоставлен локальный адрес 10.0.48.13/24, а адрес VPN-сервера провайдера — 10.0.0.1, то это как раз такой случай.

В этой ситуации связь с провайдером будет устанавливаться, рваться, снова устанавливаться и т. д. Причина в том, что пакеты до VPN-сервера в подобной конфигурации система будет пытаться направить через интерфейс ppp0, через который он недостижим. Чтобы исправить это, необходимо добавить статический маршрут до сервера провайдера, минуя ppp0-интерфейс:

```
route add -net 10.0.0.0 netmask 255.0.0.0 dev eth0
```

Примечание

В примере считается, что `eth0` соответствует интерфейсу, подключенному к сети провайдера.

Для того чтобы разрешить доступ NAT-клиентов через установленное VPN-соединение, не забудьте добавить правило `iptables`:

```
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

Примечание

Некоторые провайдеры сохраняют аутентификацию на основе MAC-адреса. Чтобы не утруждать себя лишними операциями по смене данных у провайдера, включите в файл /etc/networks/interfaces строку `hwaddress` со значением зарегистрированного MAC-адреса для соответствующего интерфейса (в примере — `eth0`) по следующему образцу:

```
auto eth0
iface eth0 inet dhcp
hwaddress ether 01:02:03:04:05:06
```

Таким способом можно назначить желаемый MAC-адрес сетевому интерфейсу.

Прокси-сервер

Практика показывает, что некоторая информация пользуется особой популярностью: ее запрашивают многие пользователи, иногда даже не по одному разу в день. Чтобы снизить нагрузку на сети, стали устанавливать так называемые прокси-серверы. На прокси-сервере автоматически сохраняется на некоторый срок вся проходящая через него информация. Если прокси-сервер обнаружит запрос данных, уже находящихся в копии на нем, то именно эта копия и будет направлена пользователю.

Кроме того, включение прокси-сервера в настройки обозревателя Интернета позволяет повысить скорость просмотра сети. Это связано с тем, что многие файлы уже не приходится получать из Сети: скорость загрузки файлов с прокси-сервера, располагающегося обычно "вблизи" пользовательского компьютера, выше скорости получения данных с удаленных хостов.

Прокси-сервер позволяет как сэкономить объем входящего трафика, что важно при оплате Интернета "по факту", так и повысить скорость работы с веб-серверами, если в организации применяется безлимитная схема оплаты (поскольку в этом случае ширина канала доступа в Интернет достаточно серьезно ограничена средствами провайдера). Конечно, реальная эффективность использования прокси-сервера зависит от особенностей работы пользователей. Если данный сайт уже кем-то посещался, то доступ к нему другого пользователя будет более быстрым. Для среднестатистических организаций (по опыту автора) внедрение прокси-сервера позволяет снизить объем входящего трафика примерно на 20%.

Примечание

Для того чтобы повысить эффективность работы через прокси-сервер, следует предусмотреть достаточный объем жесткого диска для хранения данных, получаемых из Интернета. Обычно при оценке размеров кэша стоит ориентироваться на объем месячного трафика организации, обслуживаемой таким сервером.

Автообнаружение прокси-серверов

Рабочие станции можно настраивать на автоматическое обнаружение и использование прокси-сервера. Существуют различные механизмы, при помощи которых клиенты локальной сети могут получать необходимые настройки для автоматического конфигурирования работы через прокси-сервер.

Для автоматической конфигурации параметров прокси-сервера предназначен специальный сценарий. По умолчанию такой сценарий должен иметь имя wpad.dat и публиковаться по протоколу HTTP на сервере с именем хоста WPAD. При установке сервера TMG подобный сценарий создается автоматически и может быть прописан в параметрах локального подключения (рис. 4.4).

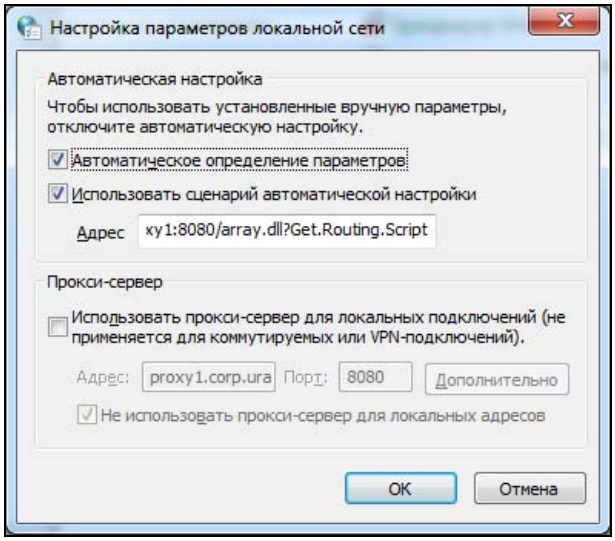


Рис. 4.4. Настройка параметров локальной сети (свойства обозревателя)

Сценарий автообнаружения прокси-серверов написан на языке макропрограммирования. При необходимости его можно откорректировать. Например, при наличии двух точек доступа к Интернету сценарий может содержать функции случайного выбора того или иного канала с заранее определенным весовым коэффициентом (при работе с массивом прокси-серверов). Если необходимо работать с некоторыми серверами Интернета только через один канал, то такую возможность можно реализовать именно через модификацию данного сценария.

Если вы имеете подобный сценарий, то необходимо создать на DNS-сервере запись, которая указывала бы на данный хост (например, можно создать запись-

синоним CNAME). Параметры сценария может сообщать также и сервер DHCP. Для этого нужно добавить новый стандартный параметр (в меню **Predefined Options** оснастки управления сервером DHCP) с номером 252 (этому параметру можно дать любое название, например, Proxy Autodiscovery Option или просто wpad) и установить его значение равным URL сценария автонастройки, например:

```
http://wpad.<имя_домена>:8080/wpad.dat
```

> ***Примечание***
>
> Для Windows-клиентов необходимо записывать URL только строчными символами. Поскольку, например, наличие прописной буквы может привести к ошибке автообнаружения прокси при использовании ISA-сервера (см. KB307502).
>
> В параметрах DHCP можно указывать и номер порта, на котором публикуется сценарий. Для DNS-записей публикация допустима только по стандартному порту HTTP — 80.

Для серверов на основе Linux образец такого файла легко найти в Интернете (можно искать также по названию файла proxy.pac). При наличии только одного прокси-сервера (одного канала доступа в Интернет) файл настроек будет всегда возвращать адрес того же самого прокси-сервера. В листинге 4.5 приведен пример такого файла.

Листинг 4.5

```
function FindProxyForURL(url, host)
{
if (isInNet(myIpAddress(), "192.168.3.0", "255.255.255.0"))
return "PROXY 192.168.3.10:3128";
else
return "DIRECT";
}
```

Установка и настройка прокси-сервера

Стандартный прокси-сервер Интернета — Squid.

> ***Примечание***
>
> В составе пакетов прокси-сервера, доступных для установки, есть стабильные версии Squid 2.7 и 3. Установка Squid версии 3 осуществляется командой `sudo apt-get install squid3`. При этом параметры настройки прокси-сервера останутся теми же, что и описаны далее в данной книге (с учетом небольших изменений в названии программы и папки — squid нужно будет заменить на squid*3*). Однако многие пакеты программ-анализаторов журнальных файлов по умолчанию включают настройки для Squid версии 2. При установке Squid 3 вам необходимо будет самостоятельно подкорректировать соответствующие файлы конфигурации. Поскольку форматы журналов обеих версий идентичны, можно создать ссылку командой `ln -s /var/log/squid3/var/log/squid`, которая обеспечит доступ к журналам по "старому" пути.

Для установки Squid в Ubuntu достаточно выполнить команду

```
sudo apt-get install squid
```

После загрузки и установки пакета Squid практически сразу готов к работе. Единственное, что нужно изменить в его конфигурации, — это добавить разрешение на доступ в Интернет, поскольку по умолчанию предполагается запрет доступа для всех пользователей.

Конфигурация Squid хранится в файле /etc/squid/squid.config. Это очень большой файл, содержащий подробное описание настроек множества параметров. Большинство этих настроек вам не придется менять, если Squid обслуживает в одиночку сеть небольшого офиса. Например, очень много параметров описывают условия пересылки данных между несколькими кэширующими прокси-серверами, при каких условиях пересылать пакеты одним серверам, когда это нужно делать напрямую и т. п. Необходимо только сменить правило по умолчанию, запрещающее доступ в Интернет через Squid, на разрешающее для компьютеров вашей сети.

Чтобы разрешить работу через Squid со всех компьютеров локальной сети, нужно:

1. Откорректировать правило, описывающее диапазон адресов локальной сети.
2. Включить правила разрешения доступа.

Найдите в конфигурации блок, описывающий создание правил доступа (его заголовок — `ACCESS CONTROLS`). В нем присутствует закомментированная строка, описывающая локальную сеть:

```
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
```

> ***Примечание***
>
> Если вы пользуетесь редактором `vi`, то нажмите (в командном режиме) клавишу </>, наберите `our_networks` (ввод будет отображаться в нижней части экрана) и нажмите клавишу <Enter>. Вы сразу перейдете на нужную строку.

Снимите комментарий (удалите `#` в первой позиции строки) и замените приведенные диапазоны теми, которые используются в вашей локальной сети. Раскомментируйте также строку `#http_access allow our_networks`. Сохраните настройки и перезагрузите конфигурацию Squid командой

```
sudo /etc/init.d/squid reload
```

> ***Примечание***
>
> В конфигурации Squid содержится также пожелание раскомментировать строку `#http_access deny to_localhost`, если на компьютере со Squid установлено то или иное веб-приложение.

Теперь нужно только настроить обозреватели Интернета на компьютерах локальной сети, указав параметры прокси-сервера: адрес сервера Squid и номер порта 3128 (это порт, используемый Squid по умолчанию; обычно нет необходимости изменять этот номер).

Дополнительные настройки прокси-сервера

Понятно, что настройка только из разрешения выходить в Интернет с любого компьютера локальной сети всем пользователям может применяться лишь в небольших

организациях. Какие настройки обычно следует добавить? Как правило, это управление полосой пропускания канала, фильтрация трафика и настройка авторизации или режима "прозрачного" прокси-сервера.

Как создавать собственные настройки

Любые настройки Squid выполняются на основе единого подхода. Сначала описываются в конфигурации объекты, к которым правило будет применено. Затем создается само правило. При этом очень важна последовательность, в которой правила встречаются в файле конфигурации: Squid просматривает правила от начала перечня к концу, и если найдет правило, применимое к данному пакету, то использует его и прекратит дальнейший просмотр списка. Поэтому если нужно разрешить кому-то иметь доступ к конкретному сайту, а всем остальным — запретить, то сначала должно быть определено правило разрешения конкретному пользователю, а после него добавлено правило запрета для всех.

Объекты, к которым предполагается применить правила, описываются с помощью так называемых *списков доступа* (Access Control List, ACL). Списки доступа могут определять:

- адреса источника и назначения (как конкретный IP-адрес, так и подсети);
- домены источника и назначения;
- время (часы и дни недели);
- порты источника и назначения, MAC-адреса источника;
- URL-строки запросов обозревателя, в том числе и поиск по подстроке запроса с учетом регулярных выражений;
- протоколы, типы обозревателя, методы запроса (POST, GET), параметры заголовков и т. п.

Для создания списка доступа достаточно включить в файл конфигурации строку

```
acl имя_списка тип_списка перечень_объектов
```

Параметр *тип_списка* в этой строке должен соответствовать одному из вариантов, приведенному в комментариях в файле конфигурации. Перечислять, какие объекты попадут под определение данного списка, можно как в одной строке (например, указать несколько IP-адресов источников через пробел), так и в нескольких строках (при этом необходимо повторить *имя_списка*). Но, чтобы не затруднять работу с файлом конфигурации, особенно при большом перечне объектов, удобнее вынести сам перечень в отдельный файл (в каждой строке этого файла должно быть указание только на один объект), а в строке определения списка доступа указать имя этого файла, взятое в двойные кавычки. Например, так:

```
acl porno dstdomain "/etc/squid/blacklists/porn/domains"
```

После того как списки доступа созданы, можно использовать их имена в правилах обработки запросов прокси-сервером.

Примечание

После изменения правил необходимо перезагрузить конфигурацию Squid командой `/etc/init.d/squid reload`.

Настройка использования полосы пропускания

Squid позволяет регулировать полосу пропускания при работе пользователей в Интернете. Это полезно в организациях, выбравших безлимитные тарифы, которые обычно предполагают искусственное ограничение полосы пропускания. Поэтому, чтобы один пользователь, поставивший на загрузку файл большого размера, не парализовал работу всех других сотрудников, ищущих на сайтах необходимую для текущей деятельности информацию, следует ввести лимиты на использование канала.

Squid предоставляет несколько возможностей управления. Во-первых, можно ограничить полосу пропускания для каждого сотрудника: фактически разделить весь канал между всеми. Как правило, такие настройки применяют только для отдельных "наказанных" сотрудников, поскольку если в Интернете в текущий момент работает только несколько сотрудников с ограничением полосы пропускания, то бóльшая часть канала будет простаивать.

Более удобен второй вариант, при котором первая часть файла загружается на максимально настроенной скорости, а для последующей вступают в силу ограничения. Так можно обеспечить всем сотрудникам максимально быструю работу с сайтами (поскольку оформление веб-страниц обычно не занимает большого объема), но ограничить выделение канала для загрузки файлов большого размера.

Чтобы включить управление полосой пропускания, нужно настроить *пулы задержек*, создать списки доступа, определяющие пользователей или компьютеры, для которых будут вводиться ограничения, и настроить правила.

Фактически, пул задержек — это набор параметров, определяющих использование канала доступа в Интернет. Каждый пул задержек может быть одного из трех *классов*. Первый класс позволяет ограничивать полосу индивидуально, второй — устанавливать лимиты для подсети в целом и, кроме того, лимиты для каждого пользователя. Третий класс устанавливать лимиты для сетей, подсетей и индивидуально. Если представить IP-адрес как *a.b.c.d*, то первый класс может быть применен только индивидуально, это разные значения *d*. Класс 2 учитывает параметры *c* для групповых ограничений, а класс 3 учитывает для первого лимита значения *b*, для второго — *c* и потом устанавливает индивидуальные ограничения.

По умолчанию число пулов задержки равно нулю. В конфигурации Squid нужно сначала определить число создаваемых пулов, а потом указать, какой пул к какому классу относится (листинг 4.6).

Листинг 4.6

```
delay_pools 4   # Будут созданы 4 пула задержек
delay_class 1 1 # Первый пул относится к классу 1
```

```
delay_class 2 2 # Второй пул относится к классу 2
delay_class 3 2 # Третий пул относится к классу 2
delay_class 4 3 # Четвертый пул относится к классу 3
```

Полоса пропускания ограничивается командой `delay_parameters`, ее параметрами должны быть номер пула задержки и лимиты. Лимит для класса 1 всегда общий, для параметров классов 2 и 3 — сначала указывается лимит для сети (или для сетей в случае класса 3), потом — индивидуальное значение, при этом цифры указывают значения в байтах.

> ***Примечание***
>
> В договоре с интернет-провайдером обычно указывается предоставляемая полоса пропускания в битах в секунду. Это следует учитывать при установке ограничений.

Обозначение лимита 600/8000 устанавливает максимальную скорость в 600 байт/с или 4800 бит/с после загрузки первой части файла размером 8 Кбайт. Обозначение –1/–1 применяется при отсутствии ограничения. Посмотрите пример конфигурации настроек, предполагая, что пул с номером 2 относится к третьему классу:

```
delay_parameters 2 32000/32000 8000/8000 600/8000
```

Включать использование пулов задержек следует командой `delay_access`, в качестве ее параметров должны быть указаны номер пула, правило и команда (`allow` или `deny`). Причем команды должны быть написаны в сортированном порядке: сначала команды для пулов класса 1, потом для пулов класса 2, затем — для класса 3. При этом последней командой для каждого пула должен быть включен запрет для всех, чтобы программа вышла из анализа по данному классу (листинг 4.7).

Листинг 4.7

```
delay_access 1 allow users1
delay_access 1 deny  all
delay_access 2 allow users2
delay_access 2 deny  all
delay_access 3 allow users3
delay_access 3 allow users4
delay_access 3 deny  all
delay_access 4 allow users5
delay_access 4 deny  all
```

Блокировка рекламы, порносайтов и т. п.

С помощью прокси-сервера можно ограничить доступ пользователей к сайтам определенной направленности. Для этого нужно создать соответствующие списки доступа и применить к ним правило запрета.

> ***Примечание***
>
> Не стоит обольщаться, что такие списки "закроют", например, все порносайты. Число порносайтов превышает по разным оценкам несколько миллионов, и блокировать их

тем или иным списком доступа нереально. Следует также учитывать, что увеличение числа правил обработки запросов снижает производительность прокси-сервера. Поэтому не стоит особенно увлекаться числом заблокированных доменов, следите за производительностью сервера и находите разумный баланс ограничений и скорости работы прокси. С точки зрения влияния на производительность прокси-сервера, предпочтительнее ограничения по доменам назначения, чем сложные регулярные выражения. При этом обычно несколько тысяч строк с именами блокированных доменов не очень существенно сказываются на производительности сервера.

Основу таких списков блокировки лучше всего найти в Интернете по ключевому термину "blacklist". Так можно использовать перечни с сайта **http://urlblacklist.com/**[1], списки, используемые в дополнениях к Firefox, — см. **http://adblockplus.org/en/subscriptions** или любые другие.

Загрузите их из Интернета, сохраните, например, в папке /etc/squid/blacklists по соответствующим разделам и создайте определения списков доступа. Если файл списка содержит имена доменов, то укажите строку (в примерах указаны названия файлов списка с сайта **Urlblacklist.com**).

```
acl porno dstdomain "/etc/squid/blacklists/porn/domains"
```

Если в файле списка даны регулярные выражения, то нужно определять правило следующим образом:

```
acl banners url_regex "/etc/squid/blacklists/porn/expressions"
```

Для списков по URL потребуются типы `acl url_regex`, `urlpath_regex`, `dstdom_regex` — в зависимости от того, какой вариант вы имеете.

Затем включите в файл конфигурации правила, блокирующие запросы на сайты, включенные в такие списки:

```
http_access deny porno
```

После перезагрузки конфигурации прокси-сервера администратору нужно некоторое время анализировать результаты фильтрации. Как правило, в списках, полученных из Интернета, есть ресурсы, случайно попавшие в такой перечень и нужные для текущей работы. Кроме того, некоторая часть, например, рекламы не будет отфильтрована. Такие случаи нужно отследить по файлам журнала работы Squid и добавить новые условия фильтрации.

Улучшение эффективности использования кэша прокси-сервера

Чтобы увеличить процент объектов, которые будут загружаться из кэша, можно несколько подкорректировать конфигурацию Squid. Для этого нужно увеличить размер дискового пространства, выделенного для размещения кэша, и предписать

[1] Сайт представляет коммерческую службу, поддерживающую актуальность таких списков. Но условия его лицензии позволяют однократно загрузить эти списки. Объем загрузки составляет около 18 Мбайт архивированных файлов.

Squid хранить в кэше объекты более длительный период, чем предусмотрено его настройками по умолчанию или параметрами открываемых веб-страниц.

> ***Примечание***
>
> При наличии возможности кэш прокси-сервера лучше разместить на нескольких дисках. Это повысит производительность системы. Для такой конфигурации достаточно добавить только одну директиву `cache_dir`, указывающую на точку монтирования другого диска. После чего остановить Squid и запустить его командой `squid -z`.

Для увеличения размера кэша найдите в файле конфигурации строку `#cache_dir ufs /var/spool/squid 100 16 256`, раскомментируйте ее. Замените 100 величиной ожидаемого месячного трафика в мегабайтах, хотя обычно вполне достаточно установить ее значение равным нескольким гигабайтам, например, так:

```
cache_dir ufs /var/spool/squid 4096 16 256
```

Теперь можно предписать Squid хранить в кэше объекты более длительный срок, чем предусмотрено настройками. Обычно на страницах веб-серверов самые неизменяемые элементы — это графика. Поэтому добавим в файл конфигурации в блок `OPTIONS FOR TUNING THE CACHE` параметры, которые заставят программу хранить такие файлы длительный период (в примере значение выбрано равным одному месяцу или 43 200 мин), не учитывать пользовательские настройки периода их хранения и не обновлять эти файлы во время операции ручного обновления страницы. Листинг 4.8 иллюстрирует пример такой настройки для графических файлов форматов GIF, JPEG, PDF.

Листинг 4.8

```
refresh_pattern \.gif$ 43200 100% 43200 override-lastmod override-expire
ignore-reload ignore-no-cache
refresh_pattern \.jpg$ 43200 100% 43200 override-lastmod override-expire
ignore-reload ignore-no-cache
refresh_pattern \.pdf$ 43200 100% 43200 override-lastmod override-expire
ignore-reload ignore-no-cache
```

По этому образцу вы легко сможете увеличить число подобных настроек, например, включив в них и другие допустимые для Интернета расширения имен графических файлов, добавив расширения exe, cab, mp3 и т. д. Кроме того, если объем диска позволяет, можно увеличить максимальный размер файла, помещаемого в кэш. По умолчанию это значение равно 4 Мбайт. Его можно увеличить, настроив параметр `maximum_object_size`.

> ***Примечание***
>
> После директивы `refresh_pattern` указано регулярное выражение, определяющее URL-адреса объектов, которые будут помещаться в кэш. Описание синтаксиса таких выражений легко найти в Интернете. Приведенные в примере выражения определяют любые URL-строки, которые заканчиваются на gif, jpg и pdf соответственно (символ `$` используется для указания на конец строки, `\.` — соответствуют любому набору символов).

Аутентификация доступа в Интернет

При использовании списков доступа на основе IP-адресов или MAC-адресов компьютеров у злоумышленников остается возможность присвоения себе чужих параметров для обхода такой защиты. Выходом в такой ситуации является аутентификация *любой* попытки доступа в Интернет.

Squid позволяет реализовать несколько вариантов аутентификации пользователей. В файле конфигурации Squid есть минимальный набор параметров для включения аутентификации пользователей по той или иной схеме (закомментированные строки, начинающиеся с `auth_param`). Необходимо раскомментировать все параметры, соответствующие желаемой схеме (например, *basic* или *ntlm*), при этом следует указать программу, которая будет осуществлять аутентификацию. В комментариях в файле конфигурации приведены указания по наиболее распространенным вариантам. Поскольку на практике наиболее часто применяется аутентификация пользователей по внутренней базе сервера или по базе пользователей домена Windows, мы приведем образцы первых строк параметров для таких случаев.

- Аутентификация по внутренней базе пользователей сервера Ubuntu.

  Нужно раскомментировать блок для схемы basic и указать для программы следующую настройку:

  ```
  auth_param basic program /usr/lib/squid/pam_auth -n passwd
  ```

- Аутентификация с использованием протокола NTLM в домене Windows.

  Для NTLM-аутентификации необходимо включить сервер со Squid в состав домена Windows. Для осуществления аутентификации в домене Windows необходимо раскомментировать блоки параметров для схем basic и ntlm (чтобы сохранить возможность получения от пользователя имени и пароля в ответ на запрос системы) и указать (см. **http://wiki.squid-cache.org/ConfigExamples/WindowsAuthenticationNTLM**) для схемы basic:

  ```
  auth_param basic program /usr/lib/squid/ntlm_auth
  --helper-protocol=squid-2.5-basic
  ```

  для схемы ntlm:

  ```
  auth_param ntlm program /usr/lib/squid/ntlm_auth
  --helper-protocol=squid-2.5-ntlmssp
  ```

  > ***Примечание***
  >
  > Можно добавить в строку параметр `require-membership-of=DOMAIN\\InternetUsers`. В этом случае правило будет считать аутентификацию успешной только для членов группы DOMAIN\InternetUsers.

Остальные строки можно оставить в значениях по умолчанию.

После включения схем аутентификации необходимо создать список доступа, описывающий аутентифицированных пользователей:

```
acl auth proxy_auth REQUIRED
```

А потом включить правило, запрещающее доступ в Интернет всем неаутентифицированным пользователям:

```
http_access deny ! auth
```

Для того чтобы изменения аутентификации вступили в силу, необходимо перестартовать Squid (перезагрузки конфигурации при изменении схемы недостаточно).

"Прозрачный" прокси-сервер

Прокси-сервер можно настроить так, что клиентам, выходящим в Интернет, не придется никоим образом настраивать свои обозреватели. Такой режим работы прокси-сервера называется *прозрачным прокси* (transparent proxy).

Использование режима прозрачного прокси связано с некоторыми ограничениями. Во-первых, прокси-сервер должен быть шлюзом по умолчанию для компьютеров локальной сети. Во-вторых, в этом режиме прокси-сервер не может использовать никакую аутентификацию пользователей для доступа в Интернет (доступ будет разрешен всем анонимным пользователям).

Для перевода Squid в такой режим достаточно выполнить две настройки. Первая — это добавить параметр `transparent` в строку `http_port`, например, так:

```
http_port 3128 transparent
```

Вторая настройка перенаправляет HTTP-пакеты из локальной сети на порт Squid. Выполняется она с помощью команды `iptables`:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT
--to-port 3128
```

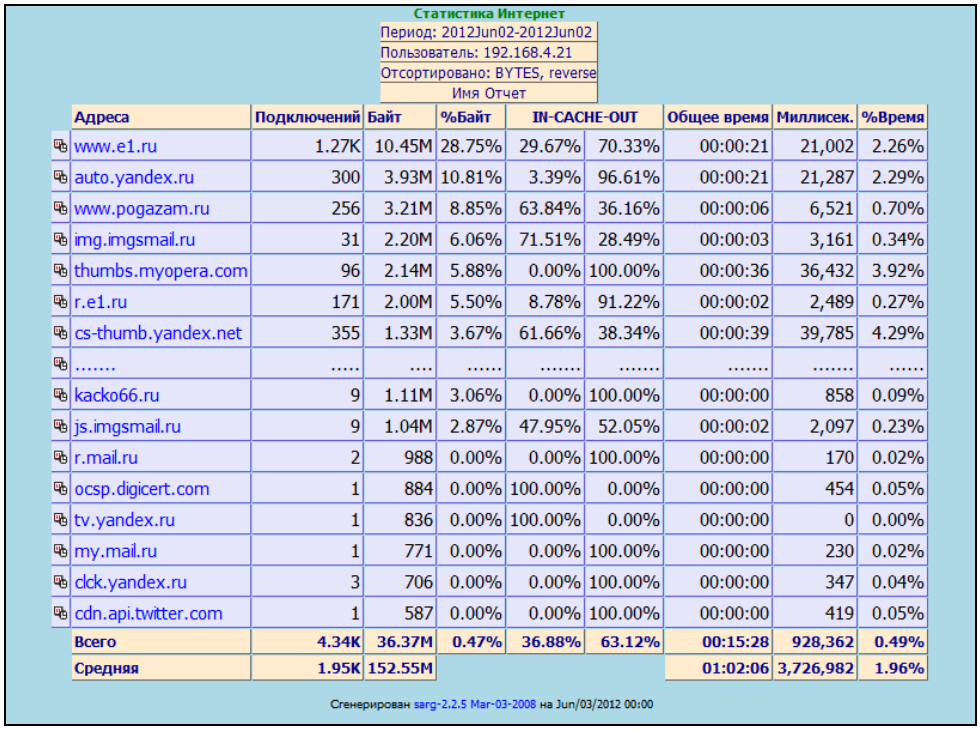
Эти две настройки обеспечат "невидимую" для пользователей работу прокси-сервера.

Анализ журналов работы прокси-сервера

Squid записывает протоколы своей работы по умолчанию в папку /var/log/squid. Файлы cache.log и store.log представляют интерес для оценки работы самой программы. А в файл access.log записываются данные о результатах доступа в Интернет пользователей. Этот файл целесообразно непрерывно анализировать, чтобы, с одной стороны, постоянно уточнять политики доступа в Интернет, с другой стороны, в нем содержатся данные, полезные для оценки работы пользователей (трафик, посещаемые сайты и т. п.).

Для анализа журналов имеется много программ. Часть из них приведена на странице **http://www.squid-cache.org/Scripts/**. Этот список далеко не исчерпывающий. Вы можете найти и другие решения, более точно приспособленные к конкретным целям анализа (например, программа Free-sa для анализа файлов журналов большого объема, см. **http://sourceforge.net/projects/free-sa**). При желании можно формировать несколько вариантов отчета различными утилитами, достаточно только указать параметры их запуска в файле ротации *(см. далее)*.

На рис. 4.5 представлен вариант отчета использования прокси-сервера Squid.



Статистика Интернет

Период: 2012Jun02-2012Jun02

Пользователь: 192.168.4.21

Отсортировано: BYTES, reverse

Имя Отчет

Адреса	Подключений	Байт	%Байт	IN-CACHE-OUT		Общее время	Миллисек.	%Время
www.e1.ru	1.27K	10.45M	28.75%	29.67%	70.33%	00:00:21	21,002	2.26%
auto.yandex.ru	300	3.93M	10.81%	3.39%	96.61%	00:00:21	21,287	2.29%
www.pogazam.ru	256	3.21M	8.85%	63.84%	36.16%	00:00:06	6,521	0.70%
img.imgsmail.ru	31	2.20M	6.06%	71.51%	28.49%	00:00:03	3,161	0.34%
thumbs.myopera.com	96	2.14M	5.88%	0.00%	100.00%	00:00:36	36,432	3.92%
r.e1.ru	171	2.00M	5.50%	8.78%	91.22%	00:00:02	2,489	0.27%
cs-thumb.yandex.net	355	1.33M	3.67%	61.66%	38.34%	00:00:39	39,785	4.29%
.....	.....	....	.....	.....	.....	.....	.....	.....
kacko66.ru	9	1.11M	3.06%	0.00%	100.00%	00:00:00	858	0.09%
js.imgsmail.ru	9	1.04M	2.87%	47.95%	52.05%	00:00:02	2,097	0.23%
r.mail.ru	2	988	0.00%	0.00%	100.00%	00:00:00	170	0.02%
ocsp.digicert.com	1	884	0.00%	100.00%	0.00%	00:00:00	454	0.05%
tv.yandex.ru	1	836	0.00%	100.00%	0.00%	00:00:00	0	0.00%
my.mail.ru	1	771	0.00%	0.00%	100.00%	00:00:00	230	0.02%
clck.yandex.ru	3	706	0.00%	0.00%	100.00%	00:00:00	347	0.04%
cdn.api.twitter.com	1	587	0.00%	0.00%	100.00%	00:00:00	419	0.05%
Всего	**4.34K**	**36.37M**	**0.47%**	**36.88%**	**63.12%**	**00:15:28**	**928,362**	**0.49%**
Средняя	**1.95K**	**152.55M**				**01:02:06**	**3,726,982**	**1.96%**

Сгенерирован sarg-2.2.5 Mar-03-2008 на Jun/03/2012 00:00

Рис. 4.5. Отчет об эффективности работы прокси-сервера Squid

Видно, что прокси-сервер позволил сэкономить 37% трафика Интернета. Другие формы отчета дают возможность проанализировать частоту посещений сайтов, наиболее существенные загрузки, активность пользователей организации и т. п.

Анализаторы журналов подготавливают свои отчеты для публикации на веб-сервере. Поэтому, если вы собираетесь установить такую программу, сначала следует настроить веб-сервер. Для установки веб-сервера Apache выполните команду:

```
sudo apt-get install apache2
```

После установки сервер Apache с параметрами конфигурации по умолчанию сразу начинает работать, при этом корневой каталог его расположен в папке /var/www.

В качестве программы анализа журналов работы установим популярную утилиту `sarg`:

```
sudo apt-get install sarg
```

Файлы конфигурации `sarg` содержат настройки, соответствующие настройкам Squid и Apache по умолчанию. И если вы не меняли пути к файлам журналов и папкам веб-сервера, то в консоли можно просто набрать

```
sarg
```

После чего в папке /var/www/squid-reports появится отчет, сформированный по данным текущего журнала Squid. Просмотреть его можно, открыв страницу **http://*адрес*_squid/squid-reports**.

Файл access.log очень быстро увеличивается в объеме. По умолчанию предусмотрена его *ротация*: через определенный промежуток времени (неделю, если вы не меняли это значение) создается новый файл журнала, старый файл переименовывается и несколько таких копий сохраняется на диске. После того как число копий достигнет заданной величины (2), самая старая копия удаляется.

Эти операции выполняются в Ubuntu утилитой `logrotate`. Файлы настроек опций ротации журналов расположены в папке /etc/logrorate.d. Необходимо исправить небольшую неточность параметров запуска программы `sarg`.

Откройте в этой папке файл squid. Найдите в нем строку `prerotate`. Она начинает блок команд, которые выполняются *перед* началом ротации файлов журналов. В этом блоке нужно подправить название утилиты. Строка должна иметь следующий вид:

```
test! -x /usr/bin/sarg | /usr/bin/sarg
```

(Сценарий проверяет существование исполняемого файла по заданному пути и, в случае успеха, запускает его на выполнение.) Эта строка обеспечит вам регулярное обновление отчетов, составляемых программой `sarg` на основе журнала Squid.

Не забывайте периодически удалять старые отчеты программы `sarg`. Ключей запуска, предусматривающих штатное удаление старых отчетов, в программе не предусмотрено. Вы можете просто удалить файл index.html и все папки, имена которых соответствуют датам отчетов. При последующем запуске утилиты необходимые файлы и папки будут созданы вновь.

Антивирусная проверка HTTP-трафика

Современное программное обеспечение позволяет выполнить антивирусную проверку всего трафика, проходящего через шлюз Интернета. Подобные разработки от Microsoft являются коммерческими. Для шлюзов на основе Linux-операционных систем есть абсолютно бесплатные решения.

Для проверки интернет-трафика на Linux-системах достаточно направить трафик прокси-сервера через программу, выполняющую антивирусную проверку файлов. Наиболее просто это осуществить с помощью еще одного прокси-сервера со встроенной антивирусной проверкой. Используем для этого пакеты havp и ClamAV.

Если вы организуете проверку всего трафика, то будьте готовы выделить на это соответствующие аппаратные ресурсы. Даже в условиях небольшого офиса при числе пользователей около 20 человек и ширине канала 1 Мбит/с проверка всех файлов в HTTP-запросах на наличие вирусов может потребовать несколько сотен мегабайт оперативной памяти и существенную часть процессорного времени (порядка 10—20%).

Прокси-сервер havp (**http://www.server-side.de**) и антивирусная программа ClamAV устанавливаются командой

```
sudo apt-get install havp clamav
```

Примечание

Часто при одновременной установке возникают ошибки настройки, которые можно исправить повторным запуском `sudo apt-get -f install havp`.

После установки этих программ требуется лишь минимальное вмешательство администратора. Во-первых, в файле конфигурации havp (/etc/havp/havp.config) нужно указать на использование русских шаблонов страниц-сообщений. Для этого необходимо найти строку `# TEMPLATEPATH /etc/havp/templates/en` и заменить ее строкой

```
TEMPLATEPATH /etc/havp/templates/ru
```

Во-вторых, целесообразно в самих шаблонах заменить фразу *"Здесь должно быть название Вашей компании"* на более подходящий текст.

Учтите, что по умолчанию программа обновления антивирусных баз пытается выполнить обновления каждый час. Если вы не согласны с такой периодичностью, то измените величину `Checks` в файле /etc/clamav/freshclam.conf на желаемое значение.

Проверьте работу havp попыткой загрузки тестового вируса со страницы **www.eicar.org/anti_virus_test_file.htm**. Havp по умолчанию задействует порт 8080, поэтому для проверки на данном шаге настройки в параметрах обозревателя следует установить это значение порта прокси-сервера.

После проверки следующим шагом должна быть настройка Squid на работу с вновь установленным прокси-сервером в качестве *родительского прокси*. Для этого укажите в файле конфигурации Squid параметры данного сервера:

```
cache_peer 127.0.0.1 parent 8080 0 no-query no-digest
no-netdb-exchange default
cache_peer_access 127.0.0.1 allow all
```

Далее следует указать, какой трафик запрашивать через havp. Для этого нужно создать соответствующий список доступа и правило направления запросов через этот прокси. Можно реализовать два варианта настроек. Самый простой — направить через прокси-сервер havp весь http-трафик. Сделать это можно настройкой конфигурации Squid:

```
acl av_scan proto HTTP
never_direct allow av_scan
```

Первая строка определяет список доступа — весь HTTP-трафик. Вторая указывает, что его необходимо всегда запрашивать через родительский прокси-сервер.

Другой подход предполагает более точное указание тех объектов, которые необходимо проверять на вирусы. Это более трудоемкий способ, но он позволяет снизить нагрузку на сервер. Для этого необходимо создать дополнительные списки доступа, которые будут описывать пропускаемые в антивирусной проверке файлы, например, так:

```
acl no_avir urlpath_regex -i \.avi$ \.jpg$ \.gif$ \.mp3$
always_direct allow no_avir
```

Естественно, что такой список можно делать как более развернутым, снижая нагрузку на процессор и память, так и более узким, проверяя большую часть файлов. Какой уровень проверки выбрать, решит сам администратор.

После того как все настройки будут выполнены, перезапустите havp и Squid (restart) и проверьте работу системы загрузкой тестового вируса (рис. 4.6). Видно, что антивирусная программа заблокировала попытку загрузки тестового вируса. Такая проверка осуществляется на сервере, еще до попадания данных на пользовательский компьютер.

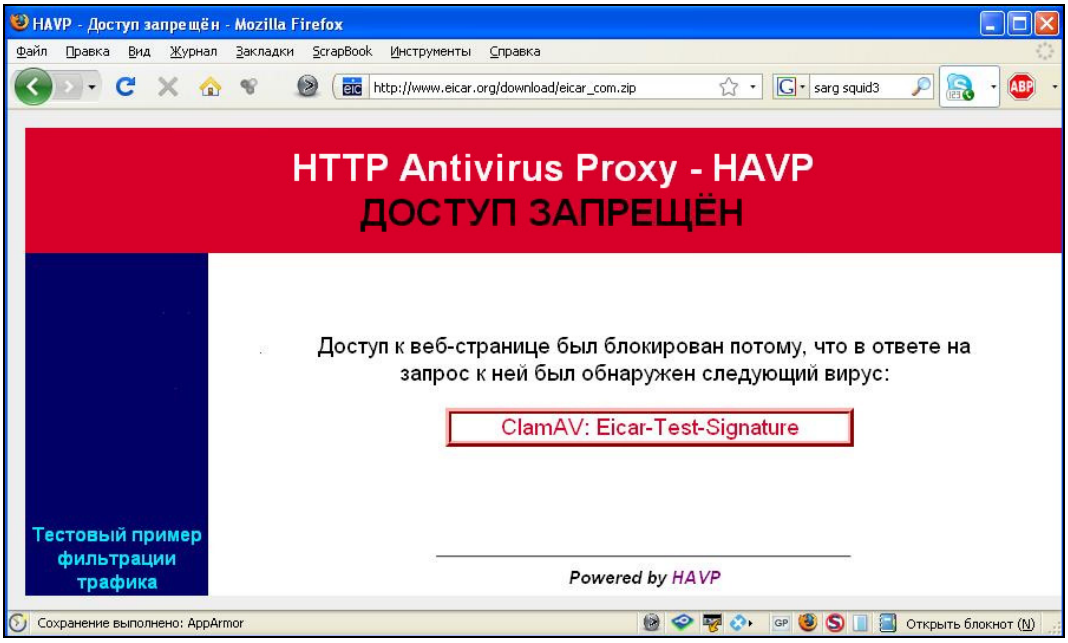


Рис. 4.6. Проверка работы антивирусной фильтрации трафика

ГЛАВА 5

Средства управления

Любому администратору хорошо знакомы стандартные средства управления информационной системой: различные консоли, позволяющие выполнить ту или иную настройку как на локальной системе, так и на любом удаленном компьютере (если выбрать в меню опцию подключения к другой системе).

Управление с помощью групповых политик

Одним из самых эффективных способов управления компьютерной сетью является использование *групповых политик*. Групповая политика позволяет централизованно устанавливать единые параметры для настройки как операционной системы, так и прикладного программного обеспечения.

Политика представляет собой набор настроек и правил, которые могут быть применены к группе компьютеров (состав группы может регулироваться администратором).

При помощи политики возможно:

- автоматически установить на компьютер программное обеспечение;
- настроить права доступа к файлам и папкам на дисках с файловой системой NTFS;
- лимитировать членство пользователей в группах безопасности (например, жестко фиксировать состав группы администраторов);
- изменить параметры реестра, внести настройки в режимы запуска служб компьютера;
- установить параметры использования прикладных программ

и т. п.

Количество настроек, которые можно регулировать при помощи групповых политик, растет с каждой версией операционной системы. Число доступных для настройки параметров перевалило уже за несколько тысяч. Поэтому описать подробно работу с групповыми политиками практически нереально. Отметим только основные моменты использования данной технологии.

Настраивать все параметры, существующие в групповой политике, не имеет смысла. После их применения работать на локальной системе станет практически невозможно из-за введенных ограничений. В каждой конкретной организации перечень параметров управления должен определяться индивидуально. Чтобы применение групповых политик, прежде всего, облегчало работу и пользователя, и администратора. Например, если есть постоянный канал доступа в Интернет, то целесообразно централизованно настроить программу обозревателя на использование соответствующих параметров доступа. Таким образом, новому пользователю не придется вносить никаких индивидуальных настроек в систему, а администратору объяснять, как это нужно сделать.

> ***Примечание***
>
> Центр технологий групповой политики, на сайте которого можно найти технические материалы по созданию и управлению групповыми политиками, доступен по ссылке **http://go.microsoft.com/fwlink/?LinkID=116313**. Перечень всех параметров групповых политик для Windows Server 2003 SP2, Windows Server 2008, Windows Server 2008 R2 содержится в документах, которые можно загрузить со страницы **http://go.microsoft.com/fwlink/?LinkId=131389**.

К чему и как применяются групповые политики

Правила групповой политики могут быть назначены для различных объектов: локальный компьютер, сайт, домен, любое организационное подразделение, причем к каждому такому объекту может быть привязано *несколько* политик.

> ***Примечание***
>
> В Windows 7/Server 2008 групповая политика может применяться раздельно для пользователей из группы администраторов (локальная политика администратора) и остальных пользователей (неадминистративная локальная политика).

В разных политиках один и тот же параметр может быть определен с отличающимися значениями. Например, в связи со спецификой обрабатываемой информации администратор подразделения может потребовать использования более строгих правил создания паролей, чем те, которые заданы администратором домена. Какие правила действуют при разрешении подобных ситуаций?

Очередность применения политик. Политики применяются в соответствии с иерархической структурой организации (структурой службы каталогов). Сначала используется локальная политика, а потом последовательно применяются политики с самого верхнего структурного уровня до самого нижнего (от общего к частному). При наличии на одном уровне нескольких политик они применяются по очереди снизу вверх списка (самая верхняя политика в списке будет применена на данном уровне последней). В результате последовательность применения политик будет выглядеть примерно так:

1. Локальная групповая политика компьютера по умолчанию.
2. Неадминистративная или административная локальная политика пользователя (если имеется — рис. 5.1).

3. Локальная политика пользователя (если имеется).
4. Групповые политики домена по иерархии контейнеров (сайт, домен, подразделение и т. п.).

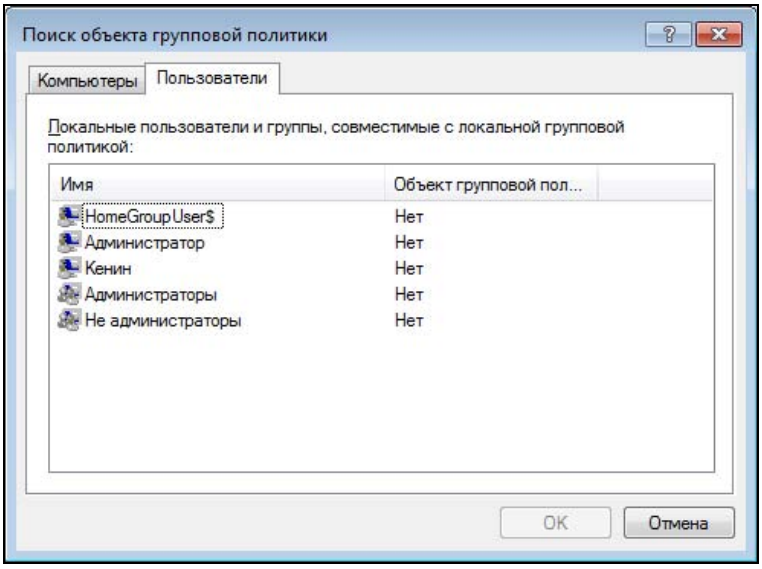


Рис. 5.1. Множественные объекты групповой политики

Разрешение конфликтов политик. Значение параметра, регулируемого одной политикой, может противоречить аналогичному значению, но в другой политике, также применяемой к объекту. При наличии конфликтующих значений будет использован параметр, задаваемой *следующей* по очереди политикой. На практике это соответствует применению политики подразделения — "непосредственного начальника". Если существует конфликт параметров политики для компьютера и пользователя одного уровня, то обычно больший вес имеет параметр, заданный для компьютера.

В случае необходимости администраторы могут устанавливать для политик признаки запрета перезаписи и/или обязательного значения параметра. Если политика описана как не допускающая изменения параметров, то ее настройки будут иметь преимущество и не смогут быть изменены значениями следующей применяемой политики. Администратор может также указать, что значения политики не должны *наследоваться* от политики более высокого уровня. В этом случае "отсекаются" настройки политик, которые применялись до данного уровня.

> ***Примечание***
>
> Если возникает конфликт требований "не переписывать" и "не наследовать", то преимущество имеет установка "не переписывать". Фактически это означает, что администратор подразделения более высокого уровня *всегда* сможет применить свои настройки.

Где хранятся и когда применяются групповые политики

Сами групповые политики представляют собой файлы, хранящиеся на контроллерах домена. Каждая политика соответствует папке Policies с GUID-именем, хранящейся в каталоге Sysvol контроллера домена.

Внутри нее находятся две папки, соответствующие настройкам компьютера и пользователя. В каждой из них имеется файл Registry.pol, в котором и хранятся настройки политик (в сущности, политики — это параметры соответствующих ключей реестра системы). В структуре папки Machine хранится файл gpttmpl.inf. Этот файл включает в себя параметры опций безопасности раздела компьютера.

Для хранения административных шаблонов применяются ADMX-файлы, представляющие собой XML-файлы соответствующих конфигураций.

> ***Примечание***
>
> Для хранения ADMX-файлов используется централизованное хранилище, что позволяет уменьшить размер папки SYSVOL. При желании (если все рабочие станции оснащены операционными системами Windows Vista и старше) можно мигрировать ADM-файлы в ADMX. Соответствующая утилита доступна для загрузки с сайта вендора.

Порядок применения групповых политик можно регулировать, опять же, настройками в групповой политике. Хотя обычно администраторы не меняют установленные по умолчанию значения. Политика компьютера применяется при каждом включении компьютера (так называемое *применение переднего плана*). Политика пользователя — при каждом входе в систему (после нажатия комбинации клавиш <Ctrl>+<Alt>+<Del>). По умолчанию политики применяются *синхронно*, причем при желании можно переопределить порядок применения, например, сменить синхронный вариант на асинхронный и т. д. Это значит, что на экране не появится приглашение для нажатия "заветных" трех клавиш до тех пор, пока не будет применена политика компьютера, а пользователь не увидит своего рабочего стола (после ввода пароля) до завершения применения пользовательской политики.

Во время работы компьютера система проверяет наличие изменений групповых политик. По умолчанию это происходит каждые полтора часа. Если политика изменена, то она будет вновь применена к системе *(фоновое изменение)*. Если изменений не обнаружено, то никаких действий не выполняется. Чтобы не создавать пиковую нагрузку на контроллеры домена, момент проверки наличия изменений случайным образом меняется до получаса в ту или иную сторону. Если контроллер домена в момент проверки недоступен по причинам отсутствия связи с ним, то обновление политики будет проведено сразу после восстановления связи (в домене Windows 2003 в этом случае проверка просто пропускалась до следующего события в графике).

Политику можно обновить и вручную. Для этого следует воспользоваться командой `gpupdate /force` (в системах на базе Windows 2000 и Windows XP без SP1 необходимо использовать команду `secedit`: `secedit /refreshpolicy {machine_policy user_policy} /enforce`). Для ускорения процесса возможно указывать дополнитель-

ный ключ (`target`), сужающий область применяемой политики (компьютер или пользователь).

Последствия отключений политик

Параметры политик условно можно разделить на две группы. Первая группа — это параметры настройки, существующие во временных ключах реестра системы. Действует политика — есть ключи. Политика отключена — ключи не создаются. Иными словами, отключение политики осуществится "безболезненно".

Вторая группа параметров задает значения существующих ключей реестра или создает такие ключи при первом применении. Главное, что такие параметры не будут удалены при снятии политики. В первую очередь это свойственно настройкам, импортируемым из файлов административных шаблонов, и предпочтениям групповых политик *(см. далее в этой главе)*.

Если политика устанавливает такой параметр, то снятие политики ничего не меняет в настройках системы. Ведь параметр реестра уже создан, а отсутствие политики означает просто сохранение его в том значении, которое было установлено политикой. Чтобы восстановить значения по умолчанию для таких параметров, администратору недостаточно просто снять политику. Нужно создать новые настройки, которые соответствуют значениям настройки по умолчанию, и применить их к компьютерам (пользователям).

Поэтому если необходимость применения какой-либо политики отпала, то рекомендуется просто отключить привязку (link) данной политики к конкретному подразделению, а саму политику не удалять. Во-первых, эти настройки могут вам опять понадобиться. А во-вторых, наличие ранее выполнявшихся настроек может помочь проанализировать действующие в подразделении параметры компьютеров и пользователей.

Чем редактировать групповую политику

Групповые политики домена Windows 2008 (R2) можно создавать и редактировать как на серверах Windows Server 2008 (R2), так и с рабочих станций Windows 7.

Средства удаленного администрирования сервера

Консоль редактирования групповой политики входит в состав сервера, но ее необходимо установить в диспетчере сервера как дополнительный компонент управления групповыми политиками. Если необходимо управлять групповыми политиками с рабочей станции, то на компьютер сначала следует установить средства удаленного администрирования сервера (Remote Server Administration Tool, RSAT), которые бесплатно доступны со страницы **http://go.microsoft.com/fwlink/?LinkId=130862**. После установки RSAT нужно включить новые компоненты в Панели управления: для этого надо выбрать **Программы и компоненты | Включение или отключение компонентов Windows**, затем установить флажок **Средства управления групповыми политиками** по пути **Средства удаленного администрирования сервера | Средства администрирования возможностей**.

После этих операций в составе программ меню **Администрирование** появится задача **Управление групповыми политиками**.

В оснастке **Управление групповыми политиками** четко видна иерархическая структура политик, с помощью которой удобно назначать ("привязывать", создавать *линк*) политики к подразделениям. Можно воспользоваться специализированными интерфейсами, которые покажут, какие параметры политики реально заданы администратором (в отличие от параметров по умолчанию). При наличии разветвленной структуры групповых политик определить, какие параметры будут применены из создаваемой политики, крайне затруднительно. В оснастке есть два интерфейса: моделирование политики и просмотр результирующего значения, позволяющие сформировать отчет о применяемых показателях. Для этого достаточно вызвать команду **Создать...** и далее следовать указаниям мастера (выбрать анализируемую политику, подразделение, пользователей и т. д.). На рис. 5.2 показан пример окна моделирования политики (для отображения конкретных значений параметров нужно перейти по ссылкам **показать**).

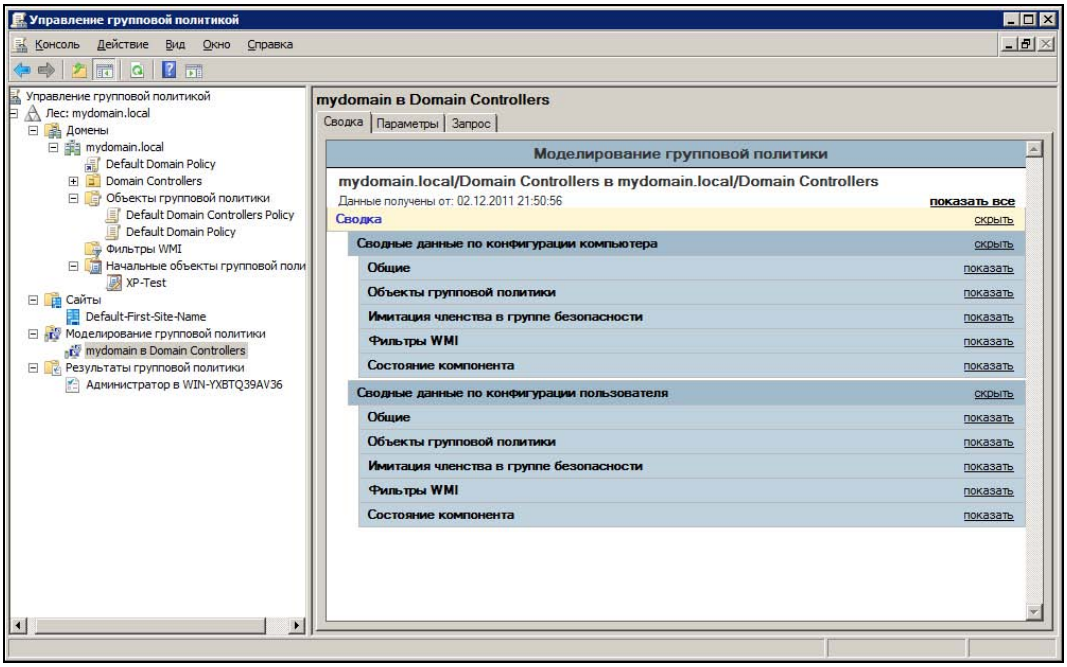


Рис. 5.2. Консоль управления групповой политикой (режим моделирования)

Групповая политика изменяется в Редакторе управления групповыми политиками (рис. 5.3), для этого достаточно выбрать соответствующую команду в меню. Новую групповую политику можно либо создать с нуля, либо скопировать в нее параметры уже существующей. Все зависит от конкретной ситуации.

Отметим новую особенность Редактора управления групповыми политиками. Теперь администраторы имеют возможность искать определенные параметры или

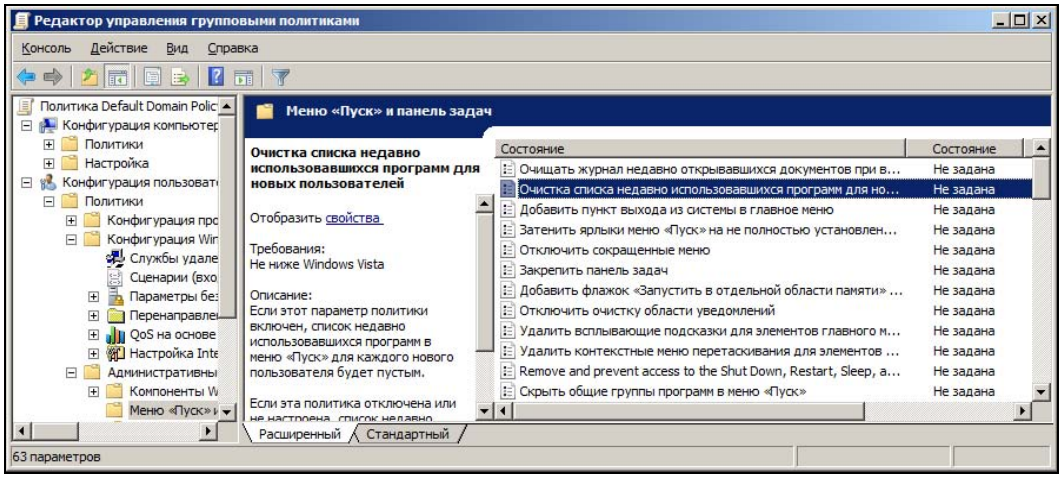


Рис. 5.3. Редактор управления групповыми политиками

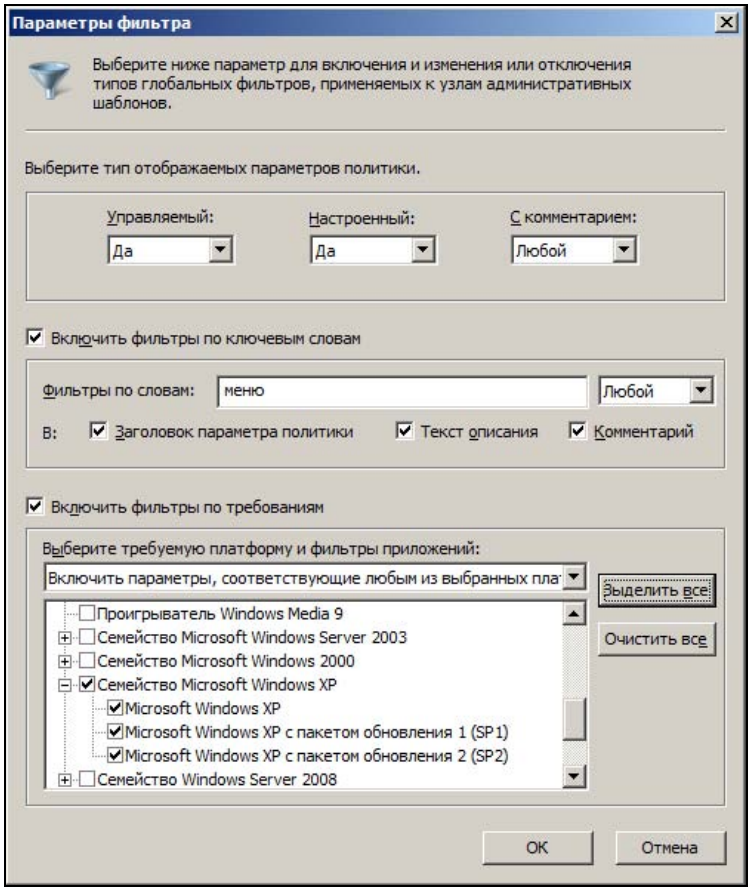


Рис. 5.4. Настройка параметров фильтра редактора групповой политики

оставлять на экране только те параметры, которые действуют для конкретной операционной системы. Для этого используется специальный фильтр (рис. 5.4), в котором необходимо установить необходимые параметры для отбора.

Назначение и удаление политики

Чтобы применить созданную политику, достаточно установить для нее связь (link) на соответствующий объект службы каталогов в оснастке **Управление групповыми политиками**.

Для удаления политики нужно удалить эту связь. Саму политику удалять не следует (для возможностей последующего анализа).

Если применение политики привело к ошибкам работоспособности системы, то в некоторых случаях отключение политики не восстановит работу системы *(см. разд. "Последствия отключений политик" ранее в этой главе)*. В некоторых ситуациях можно попытаться возвратить групповую политику к параметрам по умолчанию. На ПК с ОС Windows Server 2003/2008 это можно сделать с помощью утилиты `dcgpofix`. Подробности запуска можно получить, запустив команду `dcgpofix /?`.

Начальные объекты групповой политики

Начальные объекты групповой политики представляют собой подготовленные вендором комплекты настроек, предназначенные для быстрой настройки рабочих станций Windows XP/Vista/Windows 7. Эти объекты включены в состав Windows Server 2008 R2/Windows 7 с RSAT (параметры этих политик — только для чтения, они предназначены для импорта в групповые политики).

Начальные объекты групповой политики служат для настройки компьютеров по конфигурации *"предприятие"* (Enterprise Client) и повышенной *безопасности с ограниченной функциональностью* (Specialized Security Limited Functionality). Описание этих конфигураций доступно по ссылкам **http://go.microsoft.com/fwlink/?LinkID=121852** и **http://go.microsoft.com/fwlink/?LinkID=121854**.

Расширенное управление групповыми политиками

Новым продуктом для управления групповыми политиками, после приобретения очередной компании, стал Advanced Group Policy Management (AGPM). Данное средство входит в состав пакета оптимизации рабочей среды Microsoft Desktop Optimization Pack (MDOP). MDOP доступен тем организациям, которые заключили с Microsoft соглашение о поддержке операционных систем Microsoft Software Assurance.

AGPM устанавливает службу, контролирующую изменения в групповых политиках. На системах, в которых планируется внесение изменений в групповые политики, должны быть установлены клиенты AGPM. После установки AGPM в оснастке **Управление групповой политикой** появляется новый контейнер — **Изменение**

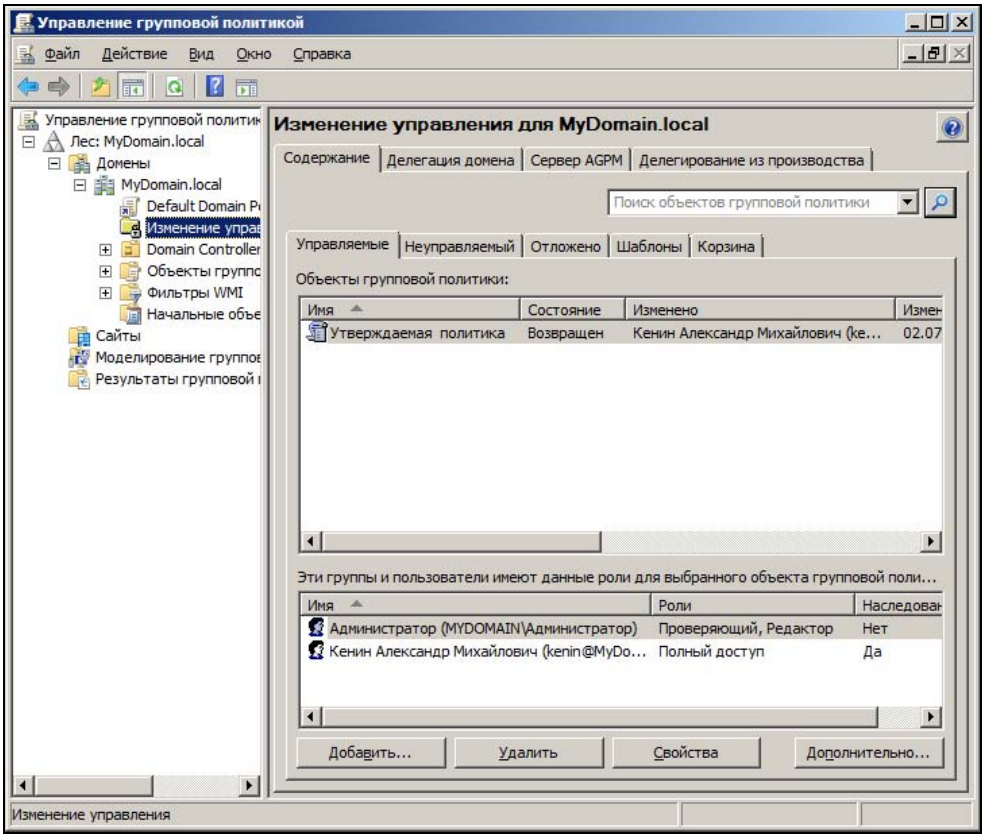


Рис. 5.5. AGPM: контролируемая политика

управления. Операции над групповой политикой можно теперь контролировать (рис. 5.5).

AGPM позволяет контролировать процесс внесения изменений в групповые политики. Можно так настроить процесс внесения изменений, что операции, выполняемые одним администратором, не будут применены, пока их не одобрит другой, более опытный специалист. При этом администраторам, вносящим изменения в групповую политику, не будут доступны функции публикаций изменений в реальной структуре, несмотря на то, что они также могут обладать правами администраторов домена (рис. 5.6).

Отметим также еще такие возможности, как:

- создание резервных копий групповых политик и возможность отката системы к сохраненному состоянию в случае применения настроек, приведших к нестабильной работе;
- возможность сравнения двух объектов групповых политик с установлением различий;
- развитая система протоколирования и отчетности.

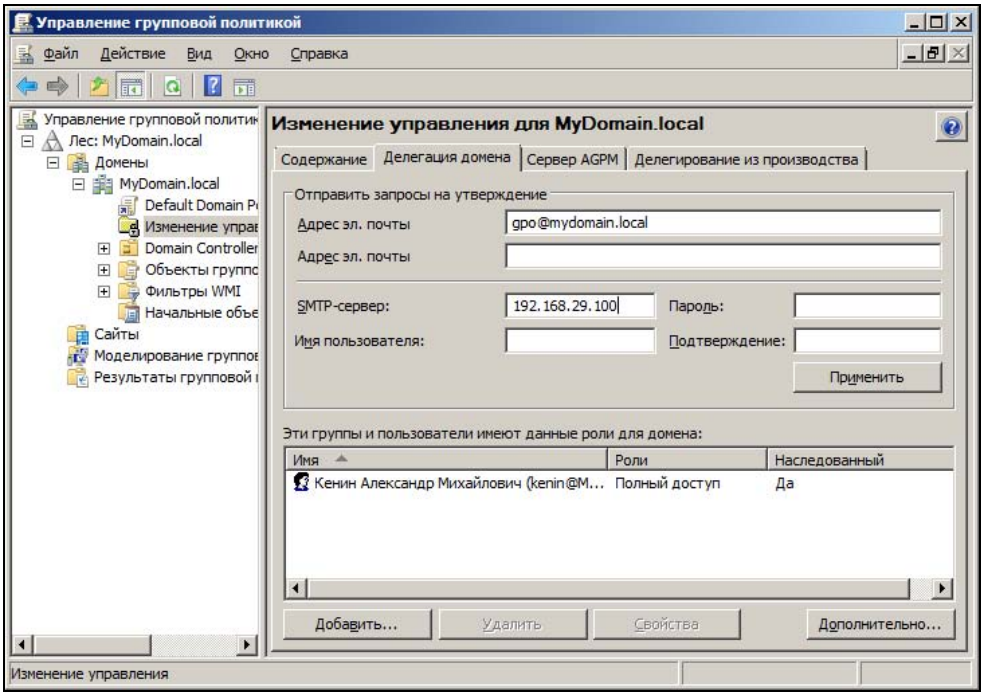


Рис. 5.6. Назначения прав администраторов по управлению групповыми политиками

"Обход" параметров пользователя

В некоторых случаях необходимо специальным образом учитывать параметры, задаваемые политиками для пользователей. Например, при работе на терминальном сервере не нужно устанавливать программное обеспечение, определенное групповыми политиками для каких-либо пользователей. Для таких случаев предназначен параметр **Loopback** *(замыкание на себя)* свойств групповой политики.

Параметр позволяет задать два варианта "обхода" политики пользователя. В режиме **Merge** система применяет все предусмотренные для данного компьютера и пользователя политики, после чего еще один раз применяет *все политики компьютеров*. То есть, если для данного пользователя и компьютера должны быть применены по иерархии три политики, назовем их A1, A2, A3, то при выборе режима **Merge** параметра **Loopback** политики будут применены в следующем порядке: A1 (параметры компьютера + параметры пользователя), A2 (параметры компьютера + параметры пользователя), A3 (параметры компьютера + параметры пользователя), A1 (параметры компьютера), A2 (параметры компьютера), A3 (параметры компьютера).

Режим **Replacement** предусматривает применение *только* параметров политики, относящихся к компьютерам. Для приведенного ранее примера при выборе данного режима были бы применены следующие политики: A1 (параметры компьютера), A2 (параметры компьютера), A3 (параметры компьютера).

Фильтрация объектов при применении групповой политики

Групповые политики привязываются к контейнерам службы каталогов. Обычно в подразделение объединено много систем, и если необходимо выполнить настройку групповыми политиками только для части систем, то приходится применять дополнительные настройки.

Самый простой способ состоит в создании дополнительной структуры службы каталогов (дополнительные подразделения) и привязки к ним соответствующих групповых политик. Но при большом числе задач такое решение неоправданно увеличит сложность структуры каталогов.

Выделить часть систем для применения политики из всего состава можно несколькими способами:

- настройкой WMI-фильтров;
- настройкой параметров безопасности для групповой политики;
- настройкой *нацеливания на элемент* для параметров **Настройки** *(см. разд. "Предпочтения групповых политик" далее в этой главе)*.

Фильтрация при помощи WMI-запросов

Существует возможность уточнять область применения политики на основе WMI-фильтров. Администратор, знакомый с основами программирования и использования WMI, может создать фильтры применения политики, учитывающие любые параметры конфигурации систем (как аппаратного, так и программного обеспечения).

При помощи фильтров можно выполнить сколь угодно точную фильтрацию, однако интерфейс назначения фильтров в групповой политике не содержит никаких средств проверки правильности запроса (это можно сделать уже при моделировании или проверке результирующих значений). Поэтому, чтобы исключить ошибки в настройках, WMI-запросы должны быть предварительно проверены другими средствами.

Настройка параметров безопасности групповых политик

Фильтровать доступ к групповой политике можно с помощью настройки ее параметров безопасности. Достаточно соответствующим образом определить те группы (или индивидуально) безопасности, которые будут иметь или не иметь право доступа и установки групповой политики.

Метод не требует дополнительных разъяснений. Но фактически при его использовании мы вместо усложнения структуры каталогов создаем соответствующую структуру групп безопасности.

Предпочтения групповых политик

В составе групповых политик сервера Windows 2008 появились *предпочтения*, доступные ранее в виде отдельного коммерческого продукта и приобретенные корпорацией Microsoft.

Предпочтения групповых политик предназначены для настройки пользовательской среды на конечной системе. С их помощью можно легко выполнить большинство повседневных административных задач, не обладая навыками программирования, не создавая большое количество подразделений или групп безопасности в структуре каталогов.

Особенности предпочтений групповых политик

Предпочтения групповых политик имеют несколько особенностей.

Во-первых, предпочтения групповых политик производят только установку настраиваемых параметров в значения, предложенные администратором, но не исключают возможности изменения их самим пользователем. Например, администратор может создать на рабочем столе компьютера ярлыки доступа к корпоративным программам, но если пользователь не предполагает их запускать, то он может просто удалить их. "Традиционные" же групповые политики жестко регулируют настройки операционной системы и приложений: если какой-либо параметр установлен в политике, то изменить его уже локальному пользователю практически невозможно.

Некоторые параметры можно задать как через традиционные настройки в групповых политиках, так и путем настройки предпочтений. Администратору нужно выбрать в этом случае, какие позиции должны быть жестко оговорены, а в каких случаях нужно предоставить пользователю возможность выбора и выполнить установку желаемых значений через предпочтения групповых политик.

Во-вторых, индивидуальная настройка традиционной групповой политики достаточно сложна: администратору нужно обладать опытом программирования (в случае использования WMI-фильтров), создавать большое количество групп безопасности (если выбирается вариант фильтрации области действия через назначение прав доступа на объекты) и т. д. Предпочтения групповой политики снабжены простым графическим средством, которое позволяет создавать любые условия отбора компьютера для последующей настройки (функционал нацеливания на элемент описан далее в этой главе).

В-третьих, предпочтения позволяют выполнить преднастройку не только тех приложений, которые разработаны под использование групповых политик, но и большинства других. Предпочтения содержат механизмы централизованного управления файлами конфигураций (ini-файлами), включают средства копирования папок и файлов, настройки реестра и т. п.

Особенностью предпочтений является также и то, что, будучи примененными к компьютеру, настройки не отключаются в случае удаления соответствующей груп-

повой политики. Если вы уже скопировали на компьютер файлы настройки, то они так и останутся при отключении предпочтений. Этот факт нужно учитывать при планировании развертывания приложений.

Клиенты предпочтений групповых политик

Предпочтения групповых политик включены в состав сервера Windows 2008. Клиентами предпочтений являются компьютеры с операционной системой Windows 7. Но разработчик выпустил специальные пакеты обновлений, позволяющие использовать предпочтения групповых политик и в операционных системах Windows XP SP2 (и старше), Windows Vista и Windows Server 2003 SP1 (см. KB943729). Для этого на них должны быть установлены следующие патчи (табл. 5.1).

Таблица 5.1. *Клиенты предпочтений групповых политик*

Клиент	Ссылка на загрузку
Windows Vista (x86)	**http://go.microsoft.com/fwlink/?LinkId=111859**
Windows Vista (x64)	**http://go.microsoft.com/fwlink/?LinkID=111857**
Windows XP (x86)	**http://go.microsoft.com/fwlink/?LinkId=111851**
Windows XP (x64)	**http://go.microsoft.com/fwlink/?LinkId=111862**
Windows Server 2003 (x86)	**http://go.microsoft.com/fwlink/?LinkId=111852**
Windows Server 2003 (x64)	**http://go.microsoft.com/fwlink/?LinkId=111863**
Все ОС, кроме Windows Vista (XMLLite low-level XML parser)	**http://go.microsoft.com/fwlink/?LinkId=11184**

Эти файлы можно загрузить по указанным ссылкам и распространить любым доступным способом (через групповую политику, устанавливая вручную — файлы занимают менее 1 Мбайт — и т. п.). Но самый простой способ установить необходимые компоненты — это воспользоваться службой установки обновлений от Microsoft.

Если в вашей организации работает сервер WSUS, то настройками по умолчанию на нем не предусмотрена загрузка и публикация для клиентов пакетов новых функций. Вам следует включить на WSUS возможность распространения пакетов новых функций, для чего достаточно открыть настройку **Продукты и классы**, перейти на вкладку **Классы** и установить флажок **Пакеты новых функций** (рис. 5.7).

После очередного цикла загрузки и установки обновлений ваши клиенты будут готовы к использованию предпочтений групповой политики.

Общие свойства параметров групповых политик

Прежде чем описывать возможности элементов предпочтений, кратко остановимся на их общих свойствах. Данные настройки присутствуют во всех элементах (рис. 5.8), назначение их приведено в табл. 5.2.

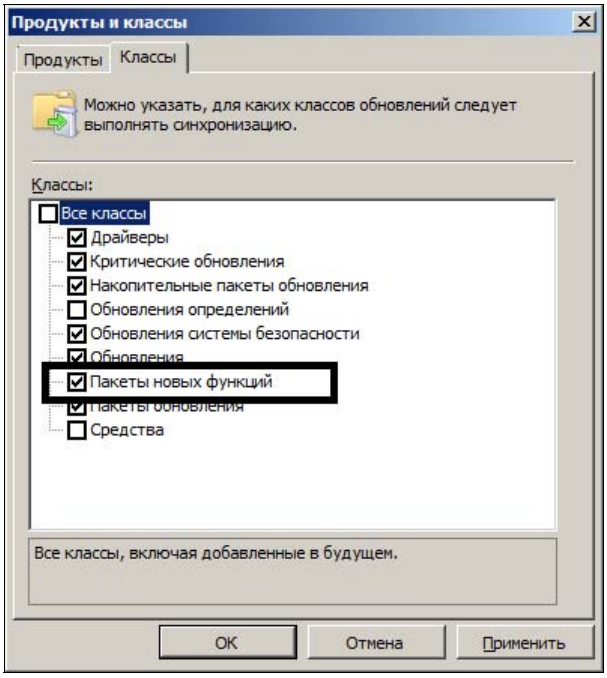


Рис. 5.7. Включение распространения пакетов новых функций на сервере WSUS

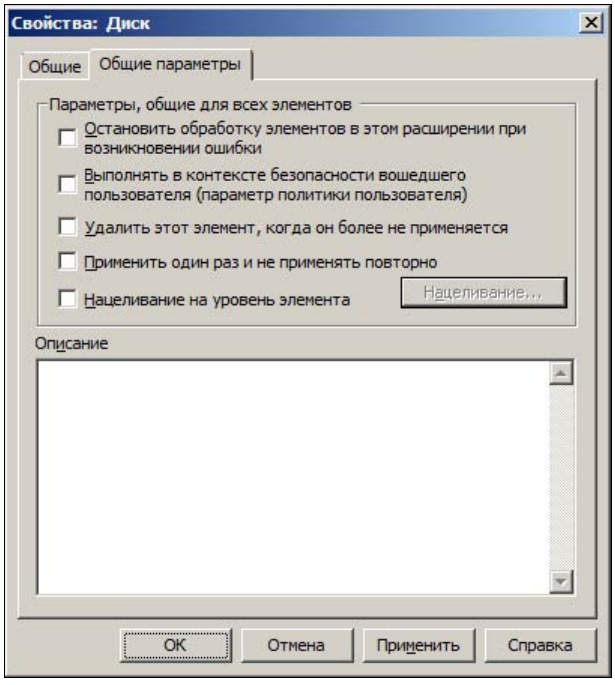


Рис. 5.8. Общие свойства параметров предпочтений

Таблица 5.2. *Описание свойств предпочтений*

Параметр	Описание
Остановить обработку элементов в этом расширении при возникновении ошибки	Определяет, будет ли выполняться настройка предпочтения, если при обработке других элементов групповой политики произойдет ошибка. Касается только данной групповой политики
Выполнять в контексте безопасности вошедшего пользователя (параметр политики пользователя)	Задания предпочтений могут выполняться как от имени системной учетной записи (System), так и от имени вошедшего пользователя. Системная учетная запись обладает максимальными локальными правами, но она не может быть использована, если операция требует идентификации пользователя. Например, при подключении к сетевым дискам
Удалить этот элемент, когда он более не применяется	Удаляет элемент, создаваемый данным предпочтением. Еще раз обратите внимание, что в общем случае при отключении предпочтений система не возвращается к настройкам по умолчанию
Применить один раз и не применять повторно	Групповая политика к работающему компьютеру применяется постоянно, через периодические интервалы времени (по умолчанию примерно каждые полтора часа). Включение повторного применения параметра фактически означает, что пользователь не сможет сменить рекомендованное администратором значение на собственное. Однократное применение параметра предоставляет такую возможность
Нацеливание на уровень элемента	Параметр позволяет произвести отбор компьютеров, к которым будет применена данная настройка. Для создания условий отбора следует нажать кнопку **Нацеливание**. Описание правил нацеливания на уровень элемента приведено далее в этой главе
Описание	Область для записи комментариев

Нацеливание на уровень элемента

Нацеливание на уровень элемента позволяет создать условие, только при выполнении которого параметр настройки будет применен к системе. В качестве условий можно задавать, например, скорость процессора, имя компьютера, членство в группах безопасности, наличие свободного места на диске, тип компьютера (ноутбук или стационарный) и т. п. Можно создавать собственные условия отбора, включая запросы LDAP или WMI, но большинство операций легко выполняется в графическом режиме при помощи мыши.

После нажатия кнопки **Нацеливание** откроется Редактор нацеливания (рис. 5.9).

Для создания условий отбора нужно выполнить операцию **Создать элемент**. Причем можно создать несколько условий, достаточно просто повторить операцию создания нового элемента.

При выборе операции создания элемента появится список доступных для включения в условие отбора элементов (рис. 5.10), в котором нужно выбрать желаемую

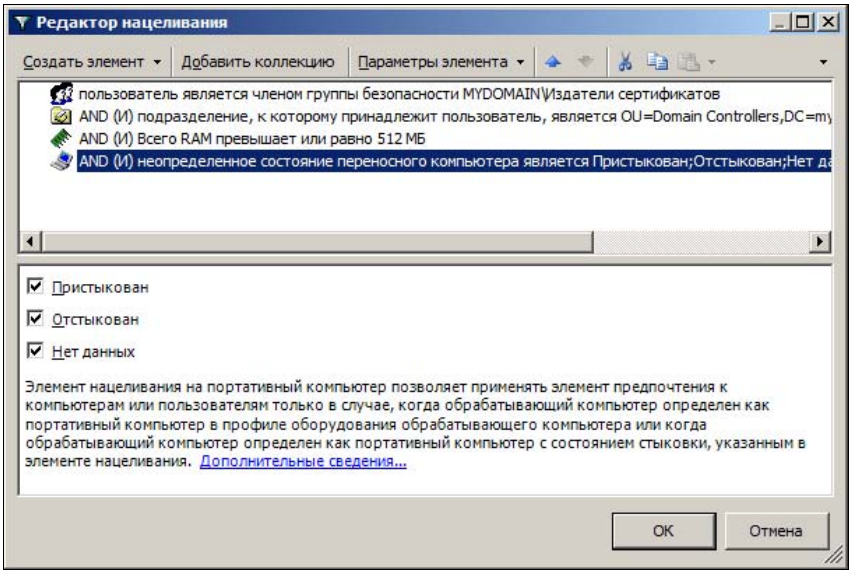


Рис. 5.9. Редактор нацеливания

позицию. В зависимости от выбранного элемента в редакторе будут отображены поля для установки критериев отбора. Так, для параметра отбора **Состояние переносного компьютера** возможными вариантами выбора являются состояния **Пристыкован** или **Отстыкован** (к док-станции, если она предусмотрена конструкцией ноутбука). Для процессора это будет его частота, для места на диске — объем свободного пространства и т. п.

При создании нескольких элементов условия могут объединяться по принципу "И" (к компьютеру будет применен параметр настройки в том случае, если все условия будут выполнены) и/или "ИЛИ" (должно выполняться либо одно, либо другое условие). Выбор И/ИЛИ производится через команду **Параметры элемента** в окне редактора.

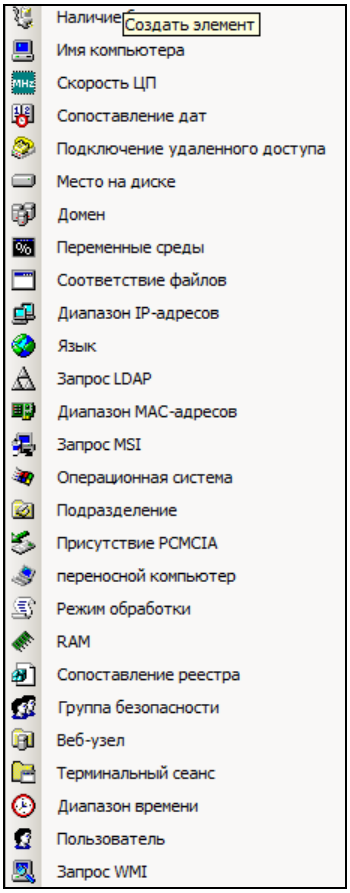


Рис. 5.10. Состав элементов отбора

Если нужно создать более сложное условие отбора, то можно воспользоваться командой **Добавить коллекцию**. Условия, объединенные в коллекцию, как бы заключаются в скобки: вся коллекция рассматривается как один элемент с истинным или ложным значением в зависимости от выполнения включенных в нее условий. При необходимости коллекции можно вкладывать одну в другую, что позволяет создать условия отбора любой сложности.

Параметры, настраиваемые предпочтениями групповой политики

Настройки расширений групповых политик отображаются в консоли групповых политик в разделе **Настройки** как для компьютера, так и для пользователя (рис. 5.11).

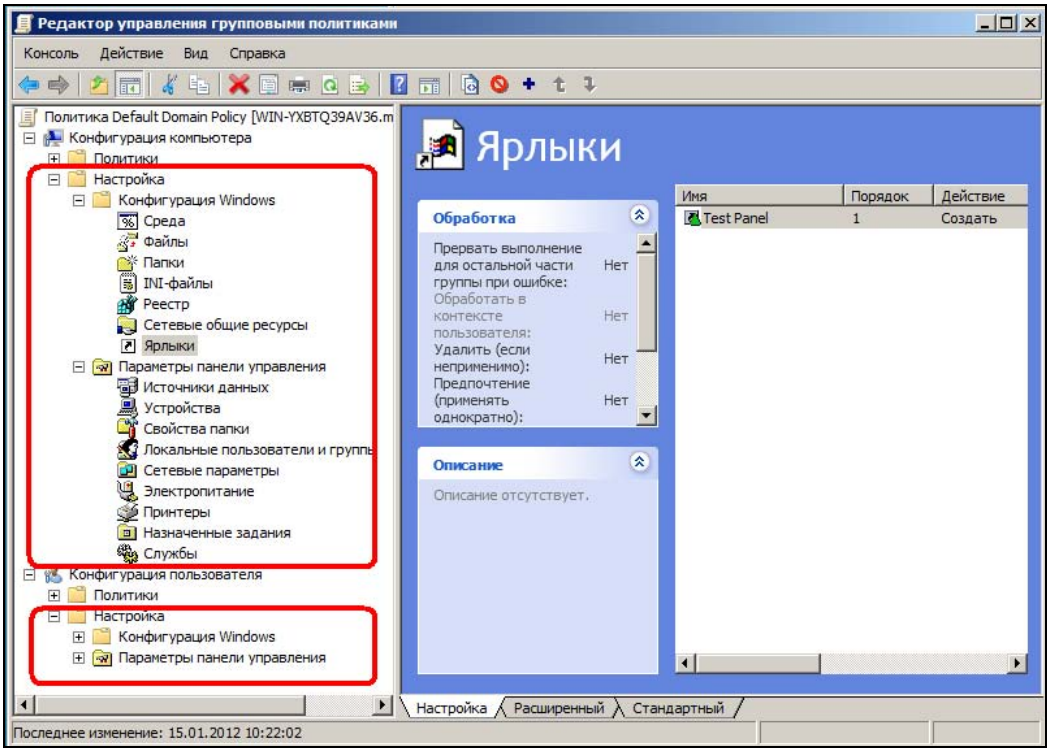


Рис. 5.11. Блоки настройки предпочтений групповой политики

Примечание

Расширения групповой политики отсутствуют в варианте локальной политики.

Большинство параметров, регулируемых предпочтениями групповой политики, предусматривает операции создания нового элемента, замены существующего, редактирования его и удаления. Описание особенностей использования каждого параметра приведено в табл. 5.3.

Состав параметров несколько отличается для конфигурации компьютера и пользователя (различия отмечены в таблице), при этом и объем настраиваемых позиций может быть отличен (например, опция **Принтеры** включает дополнительную позицию для сетевых принтеров в конфигурации пользователя).

Таблица 5.3. *Описание параметров предпочтений групповой политики*

Параметр	Присутствует в настройках		Описание
	компьютера	пользователя	
Среда	Да	Да	Параметр позволяет создать (или изменить уже существующее значение, или удалить) переменную среды. Переменные среды часто используются в прикладных программах для задания определенных настроек. Например, так можно переопределить путь для сохранения документов и т. п.
Файлы	Да	Да	Параметр позволяет создавать (менять, удалять) файлы. При указании файлов можно применять как шаблоны имени, так и использовать переменные среды. Обычно данный функционал служит для копирования на локальный компьютер файлов настроек используемых программ
Папки	Да	Да	Так же как и для файлов, позволяет копировать, удалять элементы, но это уже будут папки. Обратите внимание, что при указании путей в этом параметре нельзя использовать шаблоны (как в настройках для файлов), но можно применять переменные среды. Так же из особенностей отметим возможность очистки папки. Таким способом можно, например, регулярно очищать временную папку системы, которая часто засоряется большим количеством мелких и ненужных файлов
INI-файлы	Да	Да	Предназначен для установки значений параметров в INI-файлах. INI-файлы часто используются для конфигурирования, например, при помощи INI-файла осуществляется настройка клиента мониторинга Windows системы Nagios — Nclient++, упомянутого в этой книге. Один параметр настраивает одно значение в INI-файле. Поэтому обычно необходимо создать несколько настроек для конфигурации программы
Реестр	Да	Да	Параметр позволяет управлять реестром системы. Можно создать (отредактировать) отдельный параметр реестра, можно выполнить операцию над целой ветвью. Отметим наличие мастера операций, который позволяет выполнить настройки параметра по образцу, взяв за основу настройки конкретного компьютера. Таким способом можно выполнить настройки, которые не поддерживаются иным способом

Таблица 5.3 *(продолжение)*

Параметр	Присутствует в настройках		Описание
	компьютера	пользователя	
Сетевые общие ресурсы	Да	Нет	Параметр позволяет централизованно настраивать сетевые общие ресурсы (создавать их и настраивать количество подключений). Отметим, что других стандартных механизмов централизованного управления сетевыми ресурсами в Windows нет
Ярлыки	Да	Да	Ярлыки можно создать и при помощи параметра **Файлы**, но эта опция позволяет осуществлять более тонкие настройки. Вы можете создать ярлык для объекта файловой системы, для страницы веб-ресурса (URL) или создать специальный элемент оболочки (специальные папки Windows — такие, как папка Избранное, Панель быстрого доступа и т. д.). Параметры настройки ярлыка не отличаются от принятых в Windows
Приложения	Нет	Да	Параметр предназначен для управления приложениями раздельно по их версиям. Но для его работы должны быть установлены соответствующие модули (для каждого управляемого приложения). Несмотря на наличие ссылок в документации вендора, автору не удалось найти такие модули. Тем не менее, интерфейс является открытым, и возможность появления их не исключается
Сопоставления дисков	Нет	Да	Позволяет подключать сетевые диски к локальному компьютеру. Удобная возможность для пользовательской настройки, поскольку на практике подключения дисков используются для доступа к корпоративным ресурсам. Без такой возможности подключения дисков реализовывались достаточно сложно, например, через сценарии входа в систему с использованием анализа состава групп безопасности (утилитой `ifmember` и аналогичными)
Источники данных	Да	Да	Данный параметр позволяет настроить параметры источников данных ODBC для локальной системы. Заметьте, что других способов централизованного управления настройками ODBC нет. Ранее администраторам приходилось, в случае необходимости, создавать такие источники данных вручную или требовать от разработчиков предусматривать настройки при создании установочных пакетов прикладных программ (что усложняло как их разработку, так и централизованное распространение)
Устройства	Да	Да	Параметр позволяет контролировать устройства, например, заблокировать те или иные USB-порты. Этот функционал может быть использован для ограничения доступа пользователя к определенным классам устройств в случае предъявления повышенных требований по защите информации.

Таблица 5.3 *(продолжение)*

Параметр	Присутствует в настройках		Описание
	компьютера	пользователя	
			Однако следует учитывать, что этот механизм будет обеспечивать требуемый уровень защиты только в том случае, если пользователь обладает рядовыми правами. При этом получить права администратора — при наличии физического доступа к компьютеру и без внедрения дополнительных организационных мер — не представляет никакой сложности
Свойства папки	Да	Да	Параметр предназначен для настройки свойств папки. Обратите внимание, что таким способом определяются ассоциации для типов файлов: какая программа будет запущена для обработки файла при его выборе, например, в программе Проводник
Локальные пользователи и группы	Да	Да	Настройка позволяет управлять локальными пользователями и группами: переименовывать пользователей, сбрасывать их пароли, управлять содержимым локальных групп (например, включать в них доменные учетные записи). Возможности параметра перекликаются с функциями соответствующих настроек групповой политики
Сетевые параметры	Да	Да	При помощи этого параметра можно создать на локальной машине подключение удаленного вызова (dial-up) или VPN-подключение. Администратору необходимо только указать все требуемые для создания такого подключения данные (имя, адрес, пароль и т. д.)
Электропитание	Да	Да	Параметры настройки электропитания. Позволяют централизованно регулировать схемы сохранения электроэнергии. Например, установить действие, запускаемое при закрытии крышки ноутбука
Принтеры	Да	Да	Позволяет на локальной системе осуществить подключение к принтеру. В отличие от других вариантов подключение настраивается очень просто и эффективно
Назначенные задания	Да	Да	Управляет назначенными заданиями. Таким способом можно настроить, например, периодические операции обслуживания компьютеров (дефрагментация дисков и т. п.). Кроме создания задания, выполняемого по расписанию, существует возможность настройки мгновенного выполнения задания (при применении групповой политики). Таким образом можно выполнить тонкую настройку пользовательской среды при первом включении компьютера

Таблица 5.3 *(окончание)*

Параметр	Присутствует в настройках		Описание
	компьютера	пользователя	
Службы	Да	Нет	Параметр позволяет управлять службами в локальной системе: устанавливать вариант запуска, назначать учетную запись для старта службы, определять действия в случае непредусмотренного завершения работы службы (перезапуск службы, перезапуск компьютера и т. д.)
Параметры обозревателя	Нет	Да	Настраивает параметры обозревателя Интернета — Internet Explorer (разные настройки в зависимости от версий обозревателя)
Региональные параметры	Нет	Да	Настройка региональных параметров (форматы даты, времени и т. п.)
Главное меню	Нет	Да	Позволяет настраивать на локальных системах меню **Пуск**: выбирать стиль, включать/отключать отдельные его элементы, чистить список недавно использовавшихся документов и т. п.

Регулярные выражения

Системному администратору необходимо владеть основами работы с регулярными выражениями. Задача правильно составить регулярное выражение может встретиться при составлении собственного сценария на PowerShell или Visual Basic, в случае составления фильтра просмотра каталога (LDAP, AD), при настройке графиков отображения параметров системы в Nagios и т. д. Регулярные выражения используются в операциях поиска программ OpenOffice и др.

> ***Примечание***
>
> Следует учитывать, что реализация регулярных выражений имеет некоторые особенности в различных языках и интерпретаторах. Поэтому составляемые выражения следует проверять в каждом конкретном случае.

Синтаксис регулярных выражений достаточно сложен. В этой книге приведены только базовые понятия, которые необходимы для начала работы. Все необходимые руководства легко могут быть найдены в Сети.

Используемые символы. Метасимволы

В регулярных выражениях можно использовать большинство традиционных символов, за исключением перечисленных в табл. 5.4.

Таблица 5.4. *Специальные символы в регулярных выражениях*

Символ	Значение	Примечание
`[]`	Обозначает *класс* символов	Класс сообщает интерпретатору, что в выражении может быть использован любой из перечисленных в скобках символов, например, по выражению `с[оу]к` будут найдены сочетания как `сук`, так и `сок`
`()`	Выделяет *группу* символов	Группа используется для приоретизации операций и выделения области действия (например, в случае указания числа повторений группы символов и т. п.)
`{}`	Используется в квантификаторах	Квантификатор после символа (группы или класса) обозначает, сколько раз может повторяться этот символ. Так, `абв{2,3}` найдет группы символов `абвв` и `абввв` (символ `в` должен присутствовать от 2 до 3 раз)
`\`	Используется для *экранирования*	Экранирование позволяет использовать в выражениях специальные символы (см. далее в тексте). В целях однотипности можно экранировать и символы, которые не нуждаются в экранировании, например, символы угловых скобок (`<` и `>`)
`^`	Обозначает начало строки. Кроме того, используется для отрицания в классах	Выражение `^а` будет искать символ `а`, который находится *только в начале* строки. Если символ `^` применен в первой позиции класса, то класс будет соответствовать символам, не перечисленным *внутри скобок*: так, `[^0-9]` будет определять все *нецифровые* символы
`$`	Символ конца строки	Выражение `а$` будет искать символ `а`, который находится *только в конце* строки
`.`	Один любой символ	—
	Перечисление	Знак разделяет допустимые варианты. Например, по выражению `м[ас|ы]ло` будут найдены сочетания `масло` и `мыло`. Примечание: если варианты односимвольные, то для повышения скорости обработки желательно использовать вариант, указанный в первой строке этой таблицы
`?`	Указывает число повторений ноль или один раз	Эквивалентно `{0,1}`
`*`	Указывает число повторений ноль или более раз	Эквивалентно `{0,}`
`+`	Указывает число повторений один или более раз	Эквивалентно `{1,}`

Чтобы использовать в выражениях сами эти символы (например, чтобы найти символ `*`), их нужно *экранировать*. Для этого их следует предварить символом `\`, например: `\*`. При этом допускается экранировать целую последовательность символов, если заключить их между символами `\Q` и `\E`: `\Q*+?\E`.

В классах можно использовать диапазоны символов, указывая их как [*начало-конец*], например, класс `[а-яА-Я]` соответствует любой букве русского алфавита, кроме ё и Ё (поскольку в кодовой таблице эти символы находятся вне последовательных диапазонов букв а—я и А—Я). А класс `[0-9]` определяет любую цифру.

В регулярных выражениях можно использовать метасимволы. Наиболее часто употребляемые из них перечислены в табл. 5.5.

Таблица 5.5. *Метасимволы регулярных выражений*

Метасимвол	Обозначает
`\d`	Обозначает цифру. Эквивалентно `[0-9]`
`\D`	Обозначает нецифровой символ. Эквивалентно `[^0-9]`
`\s`	Обозначает любой пробельный символ (пробел, знак возврата каретки, знак перевода строки, знак табуляции и т. д.)
`\S`	Обозначает любой непробельный символ
`\w`	Обозначает любую букву или цифру и знак подчеркивания. Обратите внимание, что этот метасимвол обозначает, в том числе, и букву ё
`\W`	Обозначает любой символ, кроме буквы, цифры или знака подчеркивания
От `\0` до `\9`	Эквивалентно последней найденной группе символов. Например, по выражению `(т[иа]к)-\1` в тексте будут найдены строки `тик-тик` и `так-так`, но не `тик-так` (вторая группа должна совпадать с первым найденным результатом)

Модификаторы

Модификаторы позволяют переключать режимы работы интерпретатора. Например, модификатор `(? i)` включает режим нечувствительности к регистру, а `(?-i)` — отключает его, модификатор `(? x)` включает режим без учета пробелов, а `(?-x)` — отключает. Модификаторы действуют от одного до другого (от включения до выключения) или на все выражение, если нет противоположного модификатора.

Комментарии

Комментарии в выражениях должны быть заключены в скобки и начинаются с символов `#?`. Пример комментария: `(#? Это пример комментария)`.

Поиск с учетом окружающего текста

Иногда нужно найти текст, обрамленный другими символами, не включая их в результат поиска. Например, нужно найти содержимое HTML-тега, не включая в результат обрамляющие угловые скобки. Для этого используются следующие конструкции (табл. 5.6).

Таблица 5.6. *Шаблоны поиска*

Выражение	Используется для...	Пример
(?<=*шаблон*)	Поиска символов, слева от которых находятся символы *шаблон*	Выражение (?<=<)пример найдет символы **пример** в тексте <пример, но не в тексте пример
(?=*шаблон*)	Поиска символов, справа от которых находятся символы *шаблон*	Выражение пример(?=>) найдет символы **пример** в тексте пример>, но не в тексте пример
(?<! *шаблон*)	Поиска символов, слева от которых не находятся символы *шаблон*	Выражение (?<!<)пример найдет символы **пример** в тексте <пример, но не в тексте пример
(?! *шаблон*)	Поиска символов, справа от которых не находятся символы *шаблон*	Выражение пример(?!>) найдет символы **пример** в тексте пример, но не в тексте пример>

Средства тестирования

Создать собственное регулярное выражение, особенно если оно использует условия и сложные операторы, не просто. Помнить особенности синтаксиса можно только в случае постоянного проектирования регулярных выражений, поэтому лучше всего использовать свободно доступные в Интернете средства тестирования: программы, позволяющие проверить (или составить по некоторому шаблону) регулярные выражения на том или ином примере. В качестве возможного выбора приведем Expresso 3.0 (**http://www.ultrapico.com/ExpressoDownload.htm**).

Эта утилита (рис. 5.12) включает в себя составитель выражений (Expression Builder), позволяющий в интерактивном режиме составить регулярное выражение, а затем проверить его работу на любом тексте.

В составе продукта присутствует большое количество подготовленных шаблонов (адрес электронной почты, IP-адрес, валидаторы номеров кредитных карт, почтовых кодов и т. д.). На экране можно и провести анализ регулярного выражения. Например, для регулярного выражения — адреса электронной почты

```
([a-zA-Z0-9_\-\.]+)@((\[[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.)|(([a-zA-Z0-9\
-]+\.)+))([a-zA-Z]{2,4}|[0-9]{1,3})
```

анализатор дает следующий разбор выражения:

- первая группа представляет набор символов класса [a-zA-Z0-9_\-\.], повторяемый один и более раз;
- далее должен присутствовать символ @;
- затем — группа символов в одном из двух вариантов: первый — группы символов класса [a-zA-Z0-9\-], повторенные один или более раз и разделенные символом "точка" и т. д.

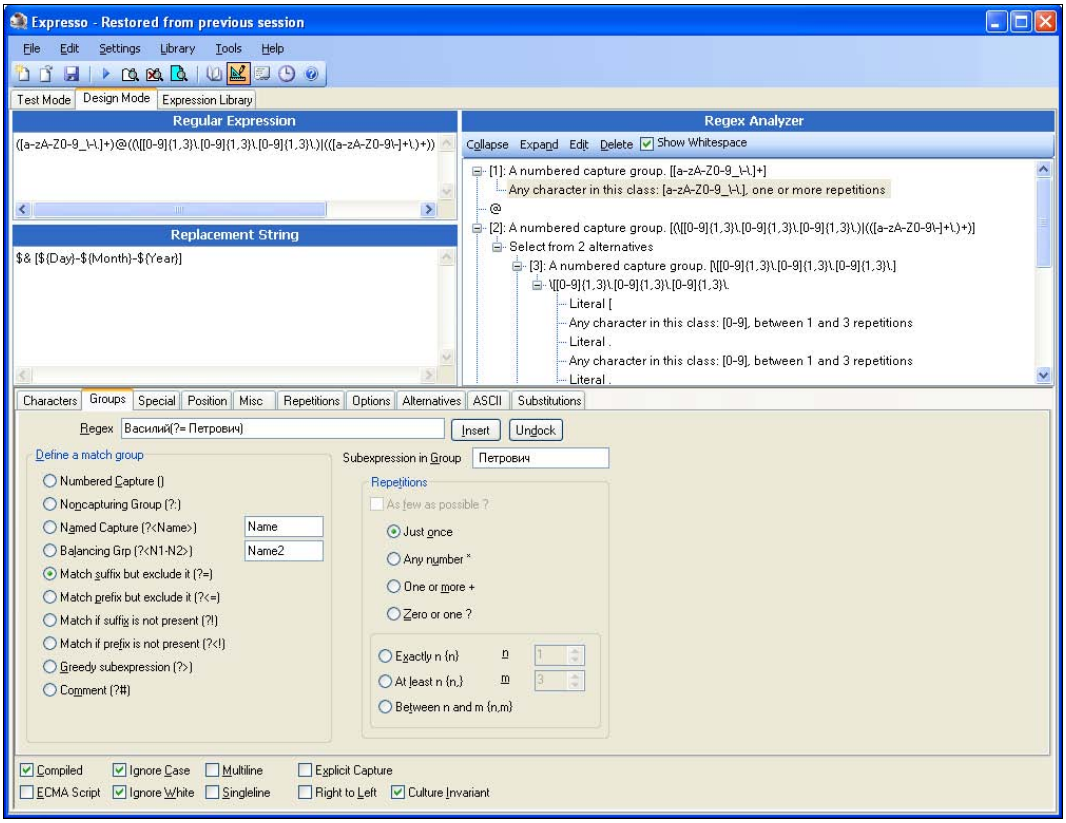


Рис. 5.12. Окно программы Expresso в режиме проектирования (design mode)

Удаленное управление в режиме консоли

Часто возникает необходимость выполнить команды на удаленном компьютере. Например, посмотреть список процессов, больше других использующих ресурсы процессора, или получить конфигурацию сетевых интерфейсов. Обычно для выполнения таких задач администраторы подключаются к удаленному рабочему столу, выполняют команду и копируют результат на локальную систему через буфер. Путь не короткий, но привычный. Использовать же его для администрирования рабочих станций не получится: стандартные функции рабочего стола Windows 7/ Vista/XP предлагают отключить текущего пользователя при подключении к удаленному рабочему столу.

Существуют различные способы выполнять команды консоли на удаленном компьютере.

Во-первых, в Windows Vista/7/Server 2008 можно задействовать службу удаленного управления — WinRM.

WinRM представляет собой интерпретацию от Microsoft протокола WS-Management Protocol, основанного на стандарте Simple Object Access Protocol (SOAP).

Это веб-сервис, запускаемый на компьютере для обеспечения удаленного управления.

> ***Примечание***
>
> Сама команда WinRM.cmd представляет собой VB-сценарий для управления службой WS-Management.

При помощи WinRM можно получить доступ как к параметрам оборудования, так и к настройкам операционных систем. Причем, поскольку этот протокол поддерживается различными вендорами, то такая информация может быть доступна не только с операционных систем от Microsoft. В частности, материнские платы, поддерживающие Platform Management Interface (IPMI) или имеющие контроллеры BMC (Baseboard Management Controllers), могут управляться при помощи WinRM.

> ***Примечание***
>
> Описание WinRM от разработчика доступно по ссылке **http://msdn.microsoft.com/en-us/library/aa384426%28v=vs.85%29.aspx**.

Самое простое использование WinRM — выполнение команды в консоли (Windows Remote Shell) или команды PowerShell на другом компьютере.

По умолчанию служба WinRM не настроена и не включена. Чтобы выполнить быструю ее конфигурацию, достаточно выполнить

```
winrm quickconfig
```

и подтвердить продолжение операций. При этом будет произведена настройка службы, сама служба запущена (в варианте отложенной загрузки), настроена локальная политика, разрешающая удаленное предоставление административных полномочий локальным пользователям, запущен прослушиватель http://* и созданы правила для межсетевого экрана.

> ***Примечание***
>
> Для включения возможностей мониторинга оборудования на сервере Windows Server 2003 R2 необходимо добавить компонент управления оборудованием (через установку компонентов Windows). Обратите внимание, что команды WinRS для сервера Windows 2003 нет.

Включить возможность удаленного управления можно при помощи групповой политики. Для этого в групповой политике **Конфигурация компьютера | Административные шаблоны | Конфигурация Windows | Удаленное управление Windows | Служба удаленного управления Windows** настройте и включите параметр **Разрешить автоматическую настройку прослушивателей**. В настройку входит указание диапазона адресов компьютеров, которые будут прослушиваться службой. Правила описания приведены в пояснениях к параметру (рис. 5.13).

Не забудьте, что если ручное включение управления выполняет настройку межсетевого экрана, то при включении через групповую политику исключения для МСЭ (по умолчанию это порт 5985) необходимо создать вручную. Для этого также можно воспользоваться мастером операций, разрешив в нем предопределенные правила для удаленного управления (разрешить удаленное управление компьютером и удаленное управление МСЭ).

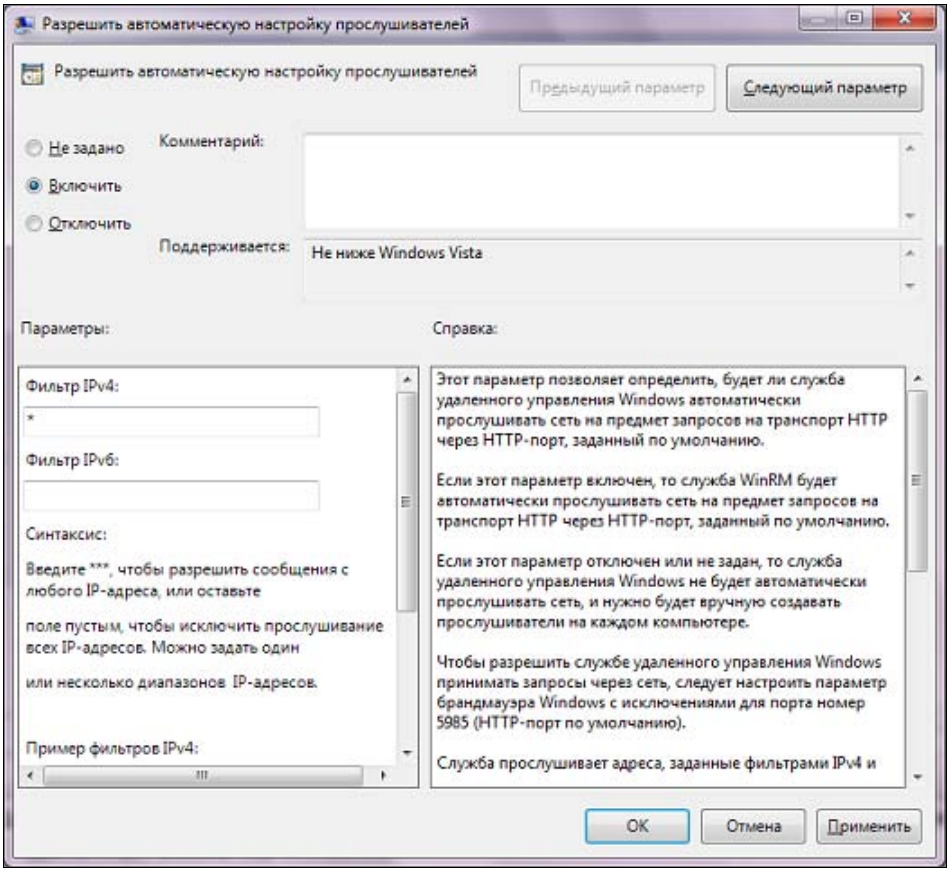


Рис. 5.14. Включение прослушивателя служб WinRM через групповую политику

Для возможности выполнения операций должно существовать доверительное отношение к компьютеру, с которого будет проводиться запуск команды. В случае, если компьютеры являются членами одного домена, то все настройки могут быть выполнены с использованием групповых политик. Расположение данной настройки: **Конфигурация компьютера | Административные шаблоны | Конфигурация Windows | Удаленная оболочка Windows**.

Если компьютеры автономны (не используется протокол HTTPS или билеты Kerberos), то для установки доверительных отношений нужно выполнить команду

```
winrm set winrm/config/client @{TrustedHosts="имя_компьютера или IP-адрес"}
```

> ***Примечание***
>
> Вариант управления по протоколу HTTPS является безопасным и предпочтительным, но требует предварительной настройки систем (установки сертификатов). В данной книге эти операции не описываются, читатель сможет найти их в исходных документах разработчика по указанным ссылкам.

Команда на удаленной системе выполняется по следующему образцу:

```
winrs -r:имя_компьютера команда
```

Например:

```
winrs -r:comp.domain.local ipconfig
```

В качестве имени компьютера можно использовать как NetBIOS-имя, так и FQDN. А для доступа можно указывать, в том числе, и протокол HTTP/HTTPS. При доступе по протоколу HTTP придется указать имя и пароль по следующему примеру:

```
winrs -r:http://comp.domain.local -u:пользователь -p:пароль команда
```

(Если параметр пароля опущен, то он будет запрошен.)

Запуск удаленного процесса через WMI

Возможности запуска процесса на удаленном компьютере предоставляет и инструментарий WMI. Его можно использовать как в собственных сценариях, так и из интерпретатора WMIC. Если вы запустите WMIC с ключом `/NODE:"имя_компьютера"`, то сможете выполнять запросы на удаленной системе. В частности, такой запуск

```
wmic /NODE:"my-comp" process call create notepad
```

запустит на компьютере my-comp программу Блокнот. При этом сама оболочка вернет только идентификатор процесса в случае удачного запуска (программа Блокнот будет видна в Диспетчере задач, но не на экране компьютера; управлять ею необходимо при помощи сценариев).

Запуск команд с использованием PsExec

Существует бесплатная программа PsExec от Windows Sysinternals (**http://technet.microsoft.com/ru-ru/sysinternals/bb897553**), которая позволяет запускать процессы на удаленном компьютере.

Программа не требует установки, после запуска копирует на удаленный компьютер исполняемый файл, запускает его как службу, подключается к ней с локальной системы и выполняет указанное задание. При этом интерфейс удаленной командной строки копируется на локальный компьютер:

Пример использования команды:

```
c:\>hostname
kenin-pc
c:\>PsExec.exe \\remote-1 -h hostname
PsExec v1.98 — Execute processes remotely
Copyright © 2001-2010 Mark Russinovich
Sysinternals — www.sysinternals.com
REMOTE-1
hostname exited on remote-1 with error code 0.
```

Программа PsExec работает в различных выпусках Windows, в том числе в 64-разрядных версиях ОС.

Коммерческие утилиты

Возможность удаленного запуска команд широко представлена в коммерческих продуктах. Найти их нетрудно, обычно возможности таких утилит превосходят бесплатные аналоги.

Например, программа RemoteExec (рис. 5.15) позволяет выполнить задание на компьютерах из указанного списка, задействовав настраиваемые фильтры запуска.

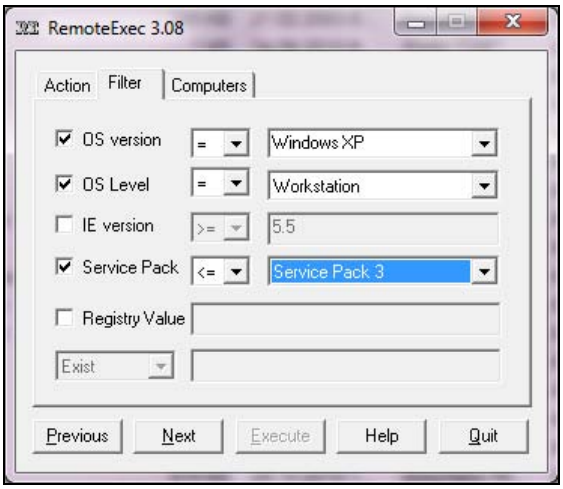


Рис. 5.15. Фильтрация условий запуска задания на удаленных системах в RemoteExec

Использование WinRM в сценариях

Возможности удаленного доступа можно включать в сценарии, для этого нужно создать объект

```
Set objWsman = CreateObject("WSMan.Automation")
```

и затем — сессию к удаленной системе:

```
Set objSession = objWsman.CreateSession("http://" & RemoteComputer)
```

За описанием подробностей такого использования WinRM мы отошлем читателя к документации изготовителя.

PowerShell

PowerShell (PS) — это средство, разработанное Microsoft для автоматизации различных задач и состоящее из интерпретатора и языка высокого уровня. PowerShell входит в состав Windows 7/Server 2008 и может быть бесплатно загружен для предыдущих версий. Язык реализован на Microsoft .NET Framework, интегрирует в себя доступ к WMI, COM, ADSI. Поэтому все возможности программирования на .NET доступны и в оболочке PowerShell.

PS можно управлять файлами на диске и параметрами операционной системы, изменять значения реестра, администрировать почтовый сервер (Microsoft Exchange) и сервер баз данных (Microsoft SQL 2008), управлять кластерами и виртуальными машинами и т. п. Число операций, которые можно выполнить с помощью PS, легко увеличивается за счет установки дополнительных модулей, разрабатываемых как сообществом, так и различными вендорами.

PowerShell во многом напоминает сценарии Linux-систем, поэтому использование его будет особенно комфортным для *nix-администраторов, уже привыкших к подобному синтаксису, а для Windows-пользователей облегчит освоение Linux-подобных операционных систем и упростит текущие операции обслуживания информационной системы.

Необходимость изучения PowerShell поясним на простом примере. Часто возникает задача точного подсчета типов операционных систем, эксплуатируемых в организации. Например, для подтверждения лицензирования. При помощи PowerShell список операционных систем получается простым запросом:

```
get-adcomputer -Filter '*' -Properties OperatingSystem | Group-Object
OperatingSystem | ft count, name
Count Name
----- ----
12    Windows Server 2003
3     Windows Server 2008 R2 Enterprise
9     Windows Server 2008 R2 Standard
2     Windows Server 2008 R2 Datacenter
115   Windows XP Professional
60    Windows 2000 Professional
1     Windows 7 Корпоративная
36    Windows 7 Профессиональная
16    Windows NT
1     Windows ServerR 2008 Enterprise
1     Windows ServerR 2008 Standard
1     Mac OS X
```

Примечание

Первая команда получает список всех компьютеров в службе каталогов со свойством описания операционной системы. Вторая — группирует список по типу ОС. Можно было бы завершить операцию на этом этапе (использовав ключ `-noelement`), но при выводе были бы урезаны названия ОС. Поэтому включена третья команда, которая выводит на экран только название ОС и количество компьютеров с нею.

Запуск PowerShell

Папка с ярлыками запуска PowerShell доступна в папке стандартных программ. Кроме того, пиктограмма запуска PowerShell включена в панель быстрого запуска Windows 7/Server 2008 R2 и добавлена в группу административных задач (в варианте с импортом системных модулей).

PowerShell доступен не только в полной версии сервера, но и в варианте установки Core с версии Windows Server 2008 R2. Обратите внимание, что в Интернете опубликованы рекомендации, позволяющие задействовать этот компонент и в предыдущих выпусках. Они доступны по адресу **http://dmitrysotnikov.wordpress.com/2008/05/15/powershell-on-server-core/**.

В папке PowerShell расположены два[1] ярлыка запуска: оболочки PowerShell в режиме командной строки и графической среды — интегрированной среды сценариев (ISE) Windows PowerShell.

Примечание

PowerShell ISE официально не поддерживается в режиме Core.

Режим командной строки PowerShell напоминает окно "обычной" командной строки. Графическая среда соответствует традиционным возможностям отладчиков

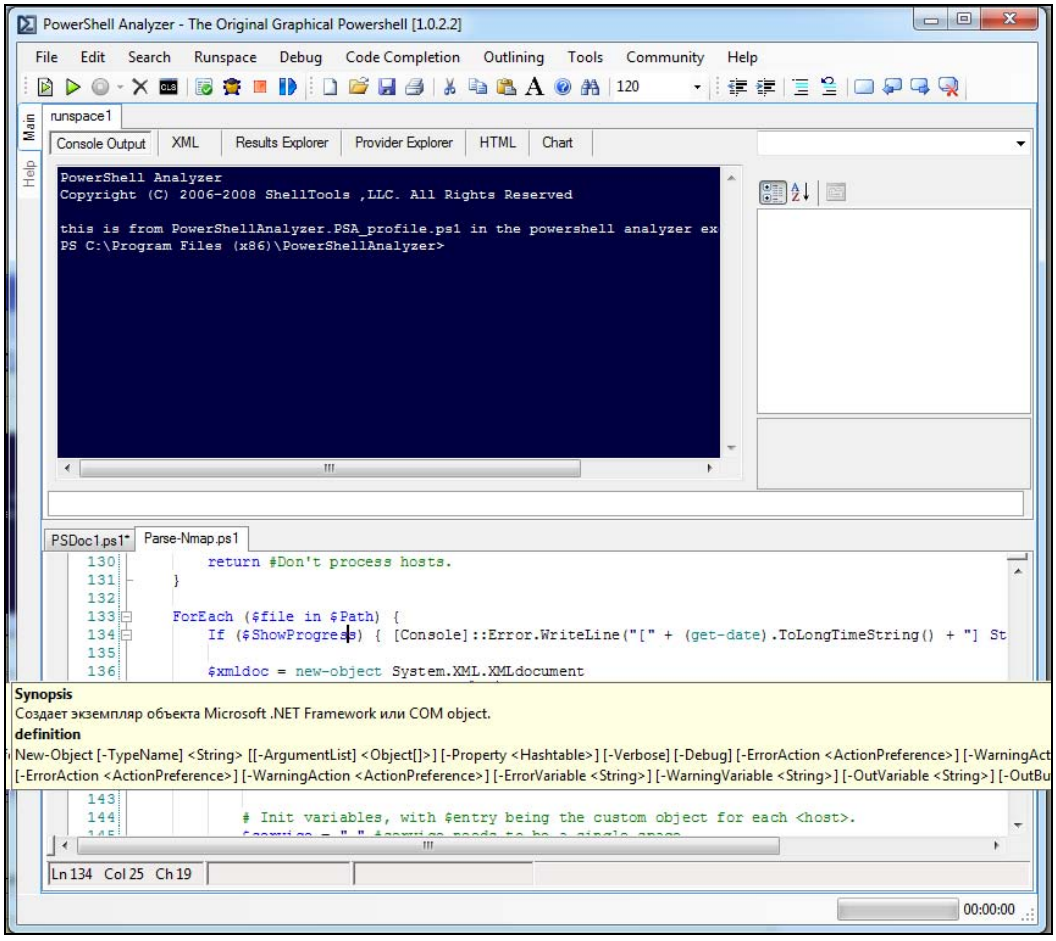


Рис. 5.16. Окно бесплатного редактора — PowerShell Analyzer

[1] Для *x*64-версий — четыре, в вариантах для *x*86- и *x*64-сред.

сценариев: одновременно можно работать с несколькими файлами, объекты сценария выделяются различными цветами, можно добавлять точки прерываний, производить отладку, для команд доступна интерактивная подсказка и т. д.

PowerShell ISE от Microsoft не является единственным отладчиком. При желании в Интернете можно найти много средств, как коммерческих, так и бесплатных, отличающихся своим функционалом. Например, на рис. 5.16 показано окно бесплатной программы PowerShell Analyser (**http://www.powershellanalyzer.com/**).

На рисунке видно, как программа отображает подсказку по команде Read-Host, на которую был наведен курсор мыши.

А на рис. 5.17 приведено окно другой бесплатной программы — от Quest — PowerGUI Administrative Console (**http://www.powergui.org/index.jspa**).

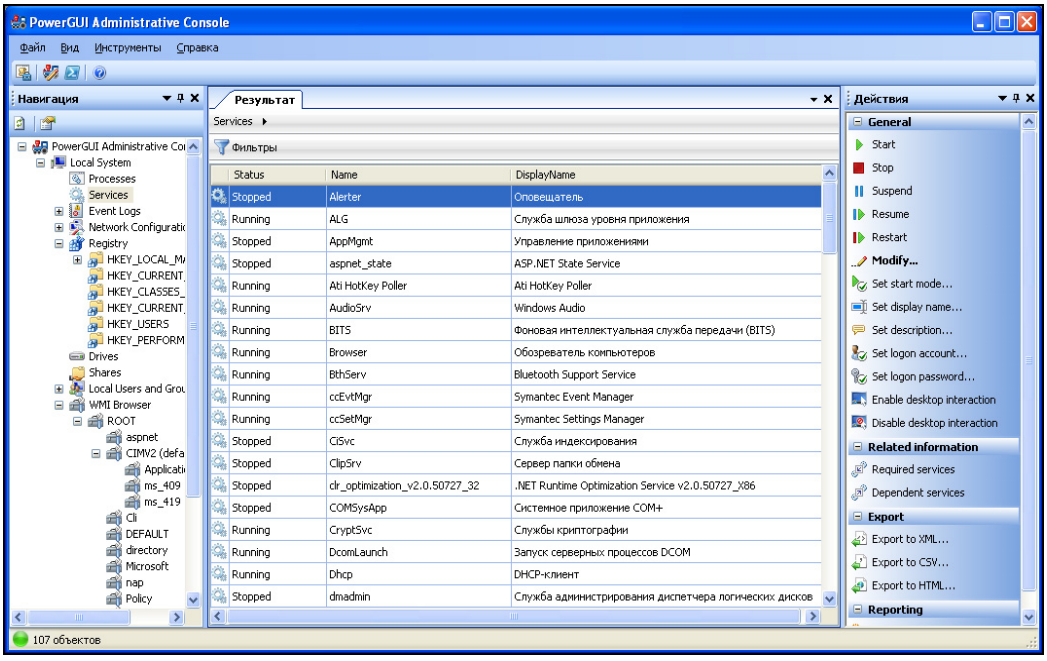


Рис. 5.17. PowerGUI Administrative Console

Эта программа представляет собой аналог административной консоли управления, но выполненной с использованием PowerShell. Вы можете управлять как локальной системой, так и удаленными компьютерами, при этом доступны не только те параметры, которые отображаются в классической консоли, но и ряд дополнительных. При этом из одной консоли имеется доступ ко всем управляемым объектам: службам, WMI-объектам, журналам событий и т. д. Число объектов управления может быть пополнено установкой дополнительных библиотек, причем поиск необходимых компонентов можно осуществить в Интернете непосредственно из интерфейса программы. Например, можно загрузить пакет управления Hyper-V, который добавляет к PowerGUI функциональность управления гипервизором.

Программы для отладки PowerShell от различных вендоров во многом идентичны по возможностям, выбор конкретного варианта базируется на стоящих задачах, личных предпочтениях и опыте пользователя.

Профиль пользователя

Особенности настройки программы для конкретного пользователя берутся из его *профиля*. Профиль позволяет точно настроить окружение: например, определить пользовательские функции, которые будут подгружаться при каждом запуске оболочки, настроить синонимы и т. д. Профиль фактически является сценарием PS. При запуске оболочки PowerShell система ищет и последовательно выполняет определенные файлы сценариев:

- *$pshome*\profile.ps1;
- *$pshome*\Microsoft.PowerShell_profile.ps1;
- *%homepath%*\My Documents\WindowsPowerShell\profile.ps1;
- *%homepath%*\My Documents\WindowsPowerShell\
  Microsoft. PowerShell_profile.ps1.

В указанных строках переменные *$pshome* и *%homepath%* обозначают "домашние" папки для PowerShell и пользователя соответственно. Значения этих переменных отличаются в разных версиях PowserShell и в разных операционных системах. Чтобы узнать их, можно выполнить следующие операции:

- *%homepath%* — открыть командную строку Windows и выполнить команду `set homepath`, в окне появится значение этой переменной;
- *$pshome* — запустить оболочку PowerShell и выполнить команду `gv pshome`.

Четыре файла позволяют точно настраивать окружение PowerShell с учетом используемой оболочки и конкретного пользователя. Первый файл выполняется для всех пользователей и всех оболочек PowerShell, второй — для всех пользователей, но только для оболочки от Microsoft, третий и четвертый — соответственно, для текущего пользователя во всех оболочках и для текущего пользователя только в оболочке Microsoft.

> ***Примечание***
>
> Пример файла сценария копируется в папку Examples установки PowerShell. Его можно использовать в качестве образца при создании собственного профиля.

Проверить наличие профиля можно командой

```
test-path $profile
```

Если профиль присутствует, то ответ команды будет `True`, в противном случае — `False`. Если профиль отсутствует, то его можно создать следующей командой:

```
new-item -path $profile-itemtype file -force
```

Далее достаточно будет открыть созданный файл профиля в редакторе для внесения необходимых настроек. Например, для открытия в Блокноте выполните

```
notepad $profile
```

Консоль PowerShell

Консоль PowerShell напоминает окно командной строки Windows. А поскольку PowerShell позволяет выполнять непосредственно команды консоли, то многие пользователи часто используют эту оболочку, например, для ввода команд типа `ping`, `ipconfig` и т. п.

Но функционал PowerShell существенно превосходит возможности командной строки. PS — объектно-ориентированный язык. Результат работы в PS — это получение не данных (чисел, строк и т. п.), а объектов, представляющих собой набор данных, свойств и методов. Например, объектом может быть учетная запись компьютера в службе каталогов или файл на диске. Свойства объекта — это его параметры, например, для компьютера такими параметрами являются имя, дата включения в домен, имя последнего входа в систему и т. д. Для файла — его имя, размер, дата создания, права доступа и т. д. Методы объекта — это те операции, которые могут быть с ним выполнены. Например, можно сменить имя компьютера, заблокировать его членство в домене, удалить компьютер из домена и т. д. Для файла методы — это чтение информации из файла или запись в него, создание или удаление и т. д.

Если говорить упрощенно, то сценарии объектно-ориентированного языка строятся по следующему принципу. Сначала производится отбор объектов по некоторым условиям (например, поиск учетных записей компьютеров, которые неактивны в домене в течение последних двух месяцев), а потом для найденных объектов вызываются необходимые методы (скажем, просто удаление таких учетных записей) или получается список параметров (например, экспортируется в текстовый файл, который потом подается в докладной записке руководству).

Команды, выполняемые в PowerShell, фактически являются программами, которые обрабатывают заданные пользователем условия. Чтобы отличить их от обычных операций командной строки, они получили название *командлетов* (cmdlet).

В PS принято называть командлеты однообразно, составляя их имена из двух частей по принципу "выполняемая операция — цель", или, как принято называть такое правило именования у разработчиков, — "глагол — существительное" (verb-noun). Так, выполняемая операция может быть *get* (получить), *set* (установить), *out* (вывод), *list* (перечислить) и т. п. Например, командлет вызова справки называется Get-Help: *Получить-Помощь*. А Get-Content возвратит содержимое (content) того элемента, который будет указан в параметрах: `Get-Content c:\test.txt` выведет на экран содержимое файла c:\test.txt.

При использовании командлетов обычно нужно указывать достаточно большое число параметров. Понятно, что запомнить их невозможно. Для вывода на экран правил использования командлета достаточно выполнить

```
Get-Command <имя_командлета> -syntax
```

Кроме того, обычно можно посмотреть на экране список примеров использования соответствующего командлета добавлением ключа `-example`. Следующая команда

выведет на экран примеры использования командлета Write-Host, позволяющего использовать в основном сценарии данные ввода пользователя с клавиатуры:

```
Get-Help Write-Host -example
```

Длинные названия командлетов набирать неудобно. Существует несколько способов упрощения ввода. Первый — создание синонимов (alias). Иными словами, командлету можно дать второе, короткое имя (или несколько имен), которое и использовать при вводе. Часть синонимов уже определена по умолчанию, например, вместо Invoke-Command можно использовать icm, командлету Get-Content соответствует синоним type, Get-ChildItem — синонимы dir и gci и т. д. Узнать синоним для конкретного командлета (Get-Command) можно следующей командой:

```
get-alias | where-object {$_. definition -eq "Get-Command"}
```

> ***Примечание***
>
> Вывести на экран весь список существующих командлетов и синонимов можно с помощью Get-Command.
>
> Получить список всех команд для работы с псевдонимами можно, если выполнить `Get-Command *-Alias`.

Второй способ — это автоматическое дополнение ввода по нажатию клавиши <Tab>. При наборе имени командлета достаточно только ввести первые его символы и нажать клавишу <Tab>. Если по введенным символам можно однозначно найти командлет, то система закончит его название; если вариантов несколько, то каждое последующее нажатие клавиши <Tab> будет выводить по очереди имена командлета, начинающиеся с указанных символов.

Третий вариант — это указать только первые символы имени, по которым можно однозначно определить командлет. Этого будет достаточно для выполнения команды, хотя если будет допущена ошибка (например, нет однозначного указания на командлет), то оболочка просто сообщит об ошибке и не станет подсказывать варианты. Кстати, обратите внимание, что такой принцип сокращения относится и к параметрам, причем если порядок параметров фиксирован в синтаксисе, то вы можете даже опускать ввод имени параметра.

Безопасность сценариев

Разработчик предпринял несколько шагов для того, чтобы снизить вероятность несанкционированного использования сценариев PowerShell.

Во-первых, по умолчанию, после установки PowerShell можно работать только в оболочке: любая попытка запуска сценария на этом языке будет заблокирована. Эта настройка определяется политикой исполнения *(execution policy)*, которая по умолчанию установлена в значение Restricted и может принимать следующие значения (табл. 5.7).

Чтобы увидеть, какая политика исполнения сценариев действует в текущий момент, следует выполнить команду `Get-ExecutionPolicy`, а для установки — `Set-ExecutionPolicy` с указанием названия желаемой политики. Можно также просто

установить необходимое значение параметра `ExecutionPolicy` по следующему пути: `HKLM\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell`, но для исключения ошибок лучше выполнять настройку политики через оболочку.

Таблица 5.7. *Политики выполнения сценариев PowerShell*

Политика	Описание
Restricted	Выполнение сценариев запрещено
AllSigned	Будут выполняться только сценарии, имеющие цифровую подпись
RemoteSigned	Будут выполняться все локальные сценарии, но сценарии, загруженные из Интернета или хранящиеся на сетевых ресурсах, должны иметь цифровую подпись
Unrestricted	Будут выполнять все сценарии

> ***Примечание***
>
> В Windows Vista/7/Server 2008 для смены политики выполнения сценариев оболочку необходимо запускать с эскалированными привилегиями (**Запуск от имени администратора**).

Во-вторых, по умолчанию для файлов сценариев PowerShell ассоциирована программа Блокнот: если вы захотите дать команду на выполнение сценария, он будет просто загружен в Блокнот для редактирования. Не следует менять такую настройку, в целях безопасности при автоматизации запуска лучше явно указывать командный файл оболочки с параметром в виде имени файла сценария.

> ***Примечание***
>
> Для включения возможности запуска сценариев по выбору их файлов следует выполнить команду
>
> ```
> FType microsoft.powershellscript.1=%windir%\system32\windowspowershell\
> v1.0\powershell.exe "&'%1' %*"
> ```
>
> Кроме того, сценарии из текущей папки нельзя запустить простым указанием их имени: необходимо набрать путь к ним в виде `./<имя_сценария>`.

Чтобы подписать сценарий, необходимо установить на компьютер сертификат, позволяющий создавать электронные подписи кодов.

> ***Примечание***
>
> Создавать заверенные сценарии лучше в командной строке, поскольку графическая утилита (PowerShell ISE) сохраняет сценарии в формате Unicode BigEndian, который не поддерживается при подписании (вы получите ошибку). Можно, конечно, создать соответствующий командлет, но проще использовать режим командной оболочки.

Для того чтобы добавить к сценарию электронную подпись, необходимо:

1. Получить в переменную PowerShell допустимый сертификат.
2. Подписать им файл сценария.

Получить допустимый сертификат можно несколькими способами. Сертификаты пользователя хранятся на PowerShell-диске cert в папке текущего пользователя. Если установлен только один сертификат, используемый для подписания кода, то можно получить его следующей командой:

```
$cert=(dir cert:currentuser\my\ -CodeSigningCert)
```

Если установлено несколько сертификатов, то выбрать нужный поможет следующий вариант:

```
$cert = @(Get-Childltem cert:\currentuser\my-CodeCigningCert)[0]
```

(Номер сертификата — 0 — нужно будет заменить необходимым значением, для этого, например, можно просто сначала вывести список всех сертификатов.)

Следующим шагом можно подписать файл сценария:

```
Set-AuthenticodeSignature <имя_файла_сценария> $cert
```

> ***Примечание***
>
> Рекомендуем после подписания первого файла выполнить его. Система может запросить реакцию пользователя на установление доверия данному сертификату (перенос его в папку доверенных сертификатов).

В доменной структуре для подписания сценариев необходимо применять сертификаты, выданные центром сертификации домена. При этом не забудьте поместить (импортировать) сертификат пользователя, которым будут подписываться сценарии, в папку доверенных сертификатов предприятия.

Удаленное выполнение команд PowerShell

В PowerShell имеется возможность выполнять команды на удаленном компьютере. Эта опция поддерживается в PowerShell версии 2.

> ***Примечание***
>
> PowerShell 2.0 включен в состав Windows 7/Server 2008 R2, а для других выпусков (Windows XP SP3, Windows Vista, Windows Server 2003/2008 — для каждой версии свой патч) необходима установка интегрированного пакета расширения, включающего компоненты удаленного управления, который может быть загружен по ссылке, описанной в статье KB968930 (**http://support.microsoft.com/kb/968930**).

По умолчанию команды PowerShell 2.0 можно выполнять только локально. Чтобы включить возможность удаленного выполнения сценария, следует выполнить от имени администратора (**Запуск от имени администратора**) команду в консоли:

```
WinRM qc
```

(рекомендуемый вариант) или непосредственно в среде PowerShell командой

```
Enable-PSRemoting –force
```

После чего для выполнения набранной команды на удаленном компьютере достаточно будет ввести

```
icm имя_компьютера {команда PowerShell}
```

Например:

```
PS C:\Users\kenin> hostname
kenin-PC
PS C:\Users\kenin> icm myserver {hostname}
myserver
```

> ***Примечание***
>
> Разрешение на удаленное выполнение команд PowerShell можно включить через групповую политику.

Обратите внимание, что в случае удаленного выполнения команд будут недоступны настройки, содержащиеся в вашем профиле PowerShell. Например, если в профиле определены функции или синонимы, то они не будут распознаны, если вы примените их в командах, выполняемых на удаленном компьютере.

Импорт расширений

Функциональность PowerShell расширяется путем добавления в него различных программных библиотек. Исторически существуют два названия для таких библиотек: оснастка (SnapIn), принятая для версии 1.0 PowerShell, и модуль (Module) — для версии PowerShell 2.0. Возможности модулей несколько шире, они включают в себя не только программные библиотеки, но и готовые сценарии. Но в Сети можно найти большое количество оснасток, поэтому на практике используется импорт так тех, так и других расширений PowerShell.

Такие расширения выпущены как самим разработчиком (например, модули[1] управления службами каталога — AD), так и доступны для скачивания из Интернета. Например, бесплатно доступны PowerShell Community Extensions — **http://pscx.codeplex.com/**, PsGet — **http://psget.net/**, Posh-Git project — **http://poshhg.codeplex.com/**, набор PowerShell Pack от Microsoft — **http://archive.msdn.microsoft.com/PowerShellPack**, PowerCli Book — **http://www.powerclibook.com/powercli-book-download-scripts-functions-and-modules/** и др. Выбор и использование их определяется администратором индивидуально в зависимости от потребностей. Обычно сначала ищется возможность реализовать тот или иной функционал управления с помощью PowerShell, а затем импортируются библиотеки, используемые в подходящих примерах.

Например, для управления DHCP-сервером можно загрузить модуль со страницы **http://gallery.technet.microsoft.com/scriptcenter/05b1d766-25a6-45cd-a0f1-8741ff6c04ec** (на странице приведен текст самого модуля, а также даны рекомендации по его установке и использованию). После импорта его в сессию PowerShell появляются такие команды, как просмотр серверов DHCP, создание и настройка областей и их опций и т. п.

---

1 Описаны в статье **http://technet.microsoft.com/en-us/library/ee617195.aspx**.

После загрузки на компьютер модули и библиотеки должны быть *подключены* (импортированы). Чтобы уточнить, какие оснастки и модули установлены и доступны для импорта, их можно перечислить соответственно следующими командами:

```
get-pssnapin
get-module -listAvailable
```

> ***Примечание***
>
> Get-PSSnapin показывает перечень всех оснасток текущей сессии, как зарегистрированных в системе, так и добавленных в сессию. Если вы создали собственный модуль (как, например, упомянутый ранее модуль DHCP-управления), то для его импорта необходимо явно указать путь к соответствующему файлу.

Для добавления расширений используются команды Add-PSSnapin и Import-Module. Так, чтобы импортировать все доступные модули в текущую сессию, можно воспользоваться следующим конвейером:

```
get-module -listAvailable | import-module
```

А если нужно импортировать только конкретные модули (оснастки), то в соответствующем командлете следует перечислить их имена.

> ***Примечание***
>
> Не забывайте, что эти команды добавляют расширения только в текущую сессию PowerShell. Чтобы расширения были доступны при последующих обращениях к PowerShell, команды добавления необходимо включить в файл профиля пользователя (описание профилей приведено далее в этой главе).

Часть модулей является системной. Это те модули, которые разработаны вендором операционной системы и установлены при добавлении в систему компонентов и ролей. Их загрузку можно включить через параметр запуска оболочки PowerShell. Для этого достаточно в ярлык запуска PowerShell добавить ключ `-ImportSystemModules`:

```
%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe
-ImportSystemModules
```

В Windows 7/Server 2008 R2 если добавить значок PowerShell в панель быстрого вызова, то опция импорта системных модулей будет доступна при вызове динамического меню этого ярлыка (если щелкнуть по значку правой кнопкой мыши). Обратите внимание, что команда **Импорт системных модулей** появляется после первого запуска PowerShell (рис. 5.18).

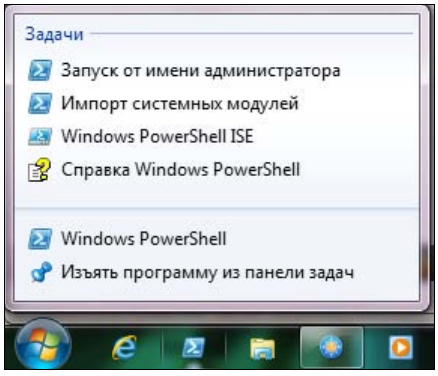


Рис. 5.18. Ярлык запуска PS с импортом системных модулей

Асинхронное выполнение заданий

Команды, вводимые пользователем в оболочке PowerShell, выполняются в синхронном режиме: вы не сможете набрать новую команду до тех пор, пока на экране не отобразится результат выполнения текущего задания.

> ***Примечание***
>
> Фоновые задания требуют настроенной функции удаленного выполнения команд даже при локальном выполнении.

PowerShell 2.0 позволяет настроить фоновое, или асинхронное, выполнение заданий. Для этого используется командлет Start-Job. Логика использования фонового задания проста. Командлет Start-Job запускает задание, которое описывается в его параметрах (блок после параметра `-scriptblock`, блок должен быть заключен в фигурные скобки). Это задание (точнее, объект задания) должно быть присвоено переменной. В этой переменной будут храниться как состояние выполнения задания, так и его результаты. Далее, нужно опросить состояния задания и, если оно завершено, получить его результаты командлетом Receive-Job в основной сеанс.

> ***Примечание***
>
> Receive-Job выводит результаты в том объеме, в котором они существуют на момент запроса. Причем выведенные результаты командлет удаляет из своего кэша (при следующем запросе он уже не отобразит их). Поэтому если вы не проверили успешное завершение задания на текущий момент, то рискуете получить только часть результатов, а не полные данные.

Запуск фоновых заданий на удаленном компьютере можно осуществлять несколькими способами. Например, можно открыть сессию на удаленном компьютере и выполнить в ней фоновое задание. А можно создать фоновое задание на локальной системе, которое будет работать с удаленным компьютером. Во втором случае используется параметр `AsJob` (например, в командлете Invoke-Command). Эти варианты имеют некоторые особенности использования (с точки зрения надежности, сохранения результатов и т. п.). Поэтому для уточнения деталей мы отошлем читателя к разделу справки по удаленным фоновым заданиям (`get-help about_remote_jobs`).

Как получить подсказку в PowerShell

В PowerShell включена мощная система подсказки, позволяющая выводить на экран разнообразную информацию.

Для получения подсказки используется командлет Get-Help. Чтобы увидеть полный набор справочных разделов, достаточно выполнить `Get-Help *`.

> ***Примечание***
>
> В PowerShell присутствует функция `help`, которая определяет некоторые параметры командлета Get-Help и используется для более дружественного вывода информации (например, выводит информацию на экран постранично). Она может быть использована вместо командлета Get-Help в большинстве случаев (не забывайте только, что

форматированный вывод всегда является фильтрацией полной информации). Функция `help` имеет синоним `man`, являющийся стандартной командой вызова подсказки в Linux-системах.

Обратите внимание, что в командлете Get-Help есть параметр `-full`, использование которого приводит к выводу на экран всей информации по запрашиваемому объекту.

Ранее мы уже упоминали возможность вывода на экран списка всех командлетов командой `Get-Command *`. Отметим еще две ее возможности.

Во-первых, можно фильтровать команды по их названиям. Так, команда `Get-Command Get*` выведет на экран список тех командлетов, названия которых начинаются с `Get`. Во-вторых, можно отбирать не только по началу названия, но и по цели (существительному), используя параметр `-noun`. Так, следующая команда выведет на экран список всех командлетов управления службой каталогов от Quest (эти командлеты имеют в названии существительных первыми символами QAD):

```
Get-Command -noun QAD*
```

В составе подсказки присутствуют специально подобранные блоки, описывающие, как использовать ту или иную возможность PowerShell. Эти блоки называются по принципам `about_`*`имя`*. Полный их список можно получить командой `help about*`, а вывести на экран соответствующий раздел — командой `help about_`*`имя`* (`about_`*`имя`* следует заменить значением имени блока подсказки). Например, чтобы показать раздел справки, описывающий правила работы с профилем пользователя, достаточно выполнить команду:

```
help about_profiles
```

Чтобы отобразить справочную информацию по командлету, нужно выполнить `Get-Help` *`имя_командлета`*. Работает и традиционный способ вызова справки — с использованием ключа `-?`. Например, команды `get-help new-service` и `new-service -?` выведут на экран одну и ту же информацию.

Кроме того, в справку включены примеры, иллюстрирующие использование командлетов. Чтобы вывести их на экран, следует использовать параметр `-examples` в командлете Get-Help, например:

```
Get-Help New-Service -examples
```

Вывести информацию по командлету можно не только при помощи Get-Help. В PowerShell присутствует команда Get-Command. Для получения справки можно использовать как `Get-Help` *`имя_командлета`*, так и `Get-Command` *`имя_командета`*. Для большинства случаев использования оба варианта идентичны, но Get-Command выводит больше информации, чем Get-Help. Так в нее включена информация и по сценариям, функциям и т. п. Выполните для примера следующие команды и сравните результаты.

```
Get-Command prompt
Get-Help prompt
prompt -?
```

Конвейеры

Результаты, полученные одним командлетом, можно передать в другой. Такое перенаправление вывода получило название *конвейера* (pipeline). Оператор конвейера обозначается как `|`.

Обратите внимание, что в конвейере передаются объекты, полученные в результате работы командлета. Поэтому при дальнейшей обработке надо, в случае необходимости, выбирать нужные свойства объекта, организовывать цикл по всем объектам (если командлет выбирает несколько объектов) и т. п. Например, следующий конвейер

```
Get-Process | Sort CPU -desc | Select Name, CPU -first 5
```

выведет на экран 5 процессов системы, которые использовали максимальные ресурсы процессора. Поясним работу каждого элемента конвейера. С помощью первого командлета мы получаем список всех процессов системы (это объекты) и передаем на обработку второму оператору, который производит их сортировку в порядке убывания параметра `CPU` (сортировку по параметру `CPU`). Полученный результат (объекты — процессы) передаем на последнюю обработку, которая отбирает только первые пять объектов и выводит на экран для них указанные параметры процесса: название и значение времени CPU.

Условные операторы, регулярные выражения, циклы

В PowerShell поддерживаются циклы, регулярные выражения, обработка условий — в общем, все те функции, которые присущи современным языкам программирования.

Для создания циклов можно использовать командлет Foreach-Object и операторы `Foreach`, `For`, `Do`, `While`. Для ветвлений можно применять операторы `If` (`If-Elseif-Else`), `switch`. Особенности их использования можно уточнить по онлайновой справочной документации или по многочисленным примерам, которые доступны в Сети.

Например, следующий сценарий выведет на экран список созданных в течение последнего дня файлов:

```
Get-childitem c:\ -R | ? {$_.creationtime -gt $(get-date).adddays(-1)}
```

Первый командлет возвращает список всех файлов на диске C: (ключ `R` выполняет рекурсивный поиск), полученные данные передаются на обработку, сценарий выбирает параметр `creationtime` (дату создания) и сравнивает его с текущей датой минус 1 день (оператор `?` является синонимом для команды Where-Object). Этот сценарий можно модифицировать, например, изменить маску и выбирать файлы журналов (`-Filter *.log`), сменить условие (меньше — `-lt`) и перенаправить вывод на команду удаления (`% {del $_}`). Таким образом, можно автоматически удалять устаревшие журналы с компьютера, если подобную команду запускать по заданному графику.

Функции

В PowerShell повторяемые блоки кода можно описывать в виде функций. В отличие от Visual Basic, в PS функции могут и возвращать, и не возвращать значения.

Подробное описание синтаксиса можно прочесть, выполнив

```
get-help about_functions
```

Во многих случаях для написания собственной функции бывает достаточно воспользоваться примерами. В качестве примера посмотрите функцию, которая проверяет доступность компьютеров в сети:

```
function Check-Online {
  param(
    $compname
  )
test-connection -count 1 -ComputerName $compname -TimeToLive 5 -asJob |
Wait-Job | Receive-Job | Where-Object {$_. StatusCode -eq 0} |
Select-Object -ExpandProperty Address
}
```

Смысл ее использования в том, что команда `test-connection` выдает ошибку в случае отсутствия ответа от компьютера, а в предложенном варианте отфильтровываются только успешные подключения. В результате такую функцию можно уже использовать в цикле для проверки компьютеров в некотором диапазоне, например, так:

```
$ipaddr = 1...254 | ForEach-Object {"192.168.0.$_"}
$compexist = Check-Online-compname $ipaddr
$compexist
```

Чтобы посмотреть тело функции, можно использовать следующую команду: `cat function:`*`имя_функции`*. Например, `cat function:help` выводит на экран следующие строки:

```
PS > cat function:help

<#
. FORWARDHELPTARGETNAME Get-Help
. FORWARDHELPCATEGORY Cmdlet
#>
[CmdletBinding(DefaultParameterSetName='AllUsersView')]
param(
[Parameter(Position=0, ValueFromPipelineByPropertyName=$true)]
[System. String]
${Name},

[System. String]
${Path},
...
```

(Вывод сокращен для удобства.)

Примечание

Другой возможный способ отображения текста функции приведен в *разд. "Диски PowerShell" далее в этой главе*.

При создании функций обратите внимание на область действия переменных. Если вы хотите, чтобы значение переменной, которую вы создали в функции, было доступно и вне функции, например, в теле сценария после вызова этой функции, то область действия переменной должна быть определена как глобальная. Для этого определение переменной должно выглядеть примерно так:

```
$Global:имя_переменной
```

Функция может быть использована в качестве фильтра: принимать на вход поток данных, а "выдавать" отфильтрованные значения. Такие функции называют *фильтрами*, описываются они аналогичным образом (при необходимости синтаксис доступен в подсказке).

Переменные

Переменные — это именованная часть памяти, в которой хранится некоторая информация. В PowerShell переменные могут быть пользовательскими (создаются вручную пользователем в сценарии), автоматическими (в них хранится служебная информация PowerShell) и привилегированными (для хранения настроек PowerShell). Принято именовать переменные строкой символов, которая начинается со знака `$`.

Список существующих переменных доступен по командлету Get-Variable, для отображения конкретной переменной достаточно просто ввести в строке его имя (включая знак `$`).

Примечание

В случае необходимости использования специальных знаков в названии переменной следует заключать ее имя в фигурные скобки.

Обратите внимание, что в PowerShell переменные могут обозначать не только строки или числа, но и массивы и другие объекты. Например, следующий пример сначала инициализирует пустой массив, а потом добавляет в него элементы (`"а"` и `"б"`), последняя строка отображает на экране все элементы массива:

```
PS > $a = @()
PS > $a += "а"
PS > $a += "б"
PS > $a
а
б
```

Акселераторы типов

Как уже говорилось, переменные могут соответствовать объектам. Если мы хотим создать объект путем инициализации новой переменной, то должны указать пол-

ностью название класса .NET, на основании которого создается новая переменная. Существует ряд сокращений, называемых акселераторами, которые можно использовать вместо полного написания имени класса. Например, при создании объекта пользователя службы каталогов нужно было бы написать

```
$User = [System.DirectoryServices.DirectoryEntry]"LDAP://CN=name,OU=my_OU,
DC=my_domain,DC=ru"
```

С использованием акселераторов описание класса можно заменить на ADSI и сама запись получается более удобной для использования:

```
$User = [ADSI]"LDAP://CN=name,OU=my_OU,DC=my_domain,DC=ru"
```

Далее приведены наиболее часто используемые акселераторы:

- ADSI;
- ADSISearcher;
- array;
- byte;
- char;
- decimal;
- double;
- float;
- hashtable;
- Int;
- IPAddress
- long;
- pscustomobject;
- psmoduleinfo;
- psobject;
- ref;
- regex;
- Runspace;
- RunspaceFActory;
- scriptblock;
- single;
- string;
- switch;
- type;
- Wmi;
- WmiClass;
- WmiSearcher;
- xml.

Примеры использования акселераторов доступны в онлайновой справочной документации PowerShell.

Диски PowerShell

PowerShell работает с информацией, расположенной на *дисках*. Дисками, в понимании PS, могут быть диски системы, реестр (`HKLM`, `HKCU`), сертификаты (cert), функции, переменные и т. д. Список всех дисков — их количество может меняться после установки дополнительных модулей PS — можно вывести командлетом Get-PSDrive. Дополнительное описание дисков доступно, если отформатировать вывод этого командлета: `Get-PSDrive | Format-List`. Пример такого вывода (сокращенный) приведен далее:

```
Name: Alias
Description: Диск, содержащий представление псевдонимов, сохраненное
в состоянии сеанса.
Provider: Microsoft.PowerShell.Core\Alias
Root:
CurrentLocation:

Name: C
Description:
Provider: Microsoft.PowerShell.Core\FileSystem
Root: C:\
CurrentLocation: Documents and Settings\Kenin_Alexander
```

```
Name: cert
Description: Поставщик сертификатов X509
Provider: Microsoft.PowerShell.Security\Certificate
Root: \
CurrentLocation:

Name: Env
Description: Диск, содержащий представление переменных среды для процесса.
Provider: Microsoft.PowerShell.Core\Environment
Root:
CurrentLocation:

Name: Function
Description: Диск, содержащий представление функций, сохраненное в состоянии
сеанса.
Provider: Microsoft.PowerShell.Core\Function
Root:
CurrentLocation:

Name: HKCU
Description: Параметры программы для текущего пользователя.
Provider: Microsoft.PowerShell.Core\Registry
Root: HKEY_CURRENT_USER
CurrentLocation:
...
```

Обращение непосредственно к дискам удобно, если вам необходимо, например, перечислить возможности соответствующего провайдера. Так, чтобы вывести на экран список всех функций PowerShell, достаточно вызвать команду `dir` для диска Function:

```
PS > dir Function:
CommandType Name        Definition
----------- ----        ----------
Function    A:          Set-Location A:
Function    B:          Set-Location B:
Function    cd\         Set-Location \
Function    Clear-Host  $space = New-Object System.Management.Automation...
...
```

(Вывод команды сокращен для удобства.)

А чтобы показать на экране саму функцию, можно воспользоваться командлетом Get-Item для выбора нужной функции, а затем отформатировать вывод, включив в него отображение блока сценария (в примере показана часть вывода для функции `mkdir`):

```
PS Function:\> get-item mkdir | fl name, scriptblock
Name: mkdir
```

```
ScriptBlock:
<#
. FORWARDHELPTARGETNAME New-Item
. FORWARDHELPCATEGORY Cmdlet
#>
[CmdletBinding(DefaultParameterSetName='pathSet',
...
```

Примечание

Обратите внимание, что для выполнения этой команды текущей папкой должен быть диск Function:. Вы можете либо предварительно перейти на него (`Function:`), либо явно указать имя диска в команде. Понятно, что при постоянной работе с данным диском удобнее сначала перейти на него для экономии ввода.

PowerShell и WMI

Возможности доступа к параметрам оборудования, настройкам операционной системы реализуются во многом с использованием WMI. PowerShell позволяет очень просто обратиться к объектам WMI и передать полученные от них данные для последующей обработки в сценарии. Следующий пример показывает, как полученные при помощи WMI-запроса данные о времени последней загрузки системы преобразуются к удобочитаемому виду:

```
PS > Get-WMIObject Win32_OperatingSystem -Property LastBootUpTime | foreach
{[System.Management.ManagementDateTimeConverter]::ToDateTime($_.LastBootUpTime)}
6 февраля 2012 г. 20:52:00
```

Для получения или установки данных WMI в PowerShell используются командлеты Get-WmiObject, Invoke-WmiMethod, Register-WmiEvent, Remove-WmiObject, Set-WmiInstance. Например, чтобы вывести на экран серийный номер материнской платы локального компьютера, достаточно выполнить

```
Get-WmiObject Win32_BIOS SerialNumber
```

Примечание

Если серийный номер необходим для целей инвентаризации, то сценарий следует немного модифицировать, чтобы получить только сам номер. Для этого сначала надо получить коллекцию элементов, а затем выбрать нужный:

```
$colItems = Get-WmiObject Win32_BIOS -Namespace "root\CIMV2"
foreach($objItem in $colItems) {Write-Host "Serial Number:"
$objItem.SerialNumber}
```

Естественно, что при запросе серийного номера на другом компьютере необходимо будет указать его имя (параметр `Computer`) и данные учетной записи.

Перечислить все доступные для работы объекты WMI можно командой

```
Get-WMIObject -list
```

Список можно отфильтровать, например, отобразить только те классы WMI, в название которых входит строка "OperatingSystem":

```
Get-WMIObject -list *OperatingSystem*
```

Следует учитывать, что по умолчанию при выводе на экран отображается только часть свойств, которые перечислены в файле настройки (файлы *.ps1xml в папке установки PowerShell). Поэтому для вывода полного списка свойств можно использовать командлет Format-List, например, так:

```
Get-WmiObject Win32_BIOS | Format-List *
```

Помочь в составлении сценариев на WMI может утилита Scriptomatic PowerShell Version, свободно доступная к загрузке с сайта Microsoft.

В этой программе можно выбрать необходимое пространство имен WMI, при этом в списке классов отобразится перечень соответствующих элементов. В окне сценария появится текст, который можно использовать в сценарии при получении искомых параметров.

PowerShell и Visual Basic

Visual Basic (VB) является COM-объектом, который может быть вызван из сценария PS. Соответствующие рекомендации широко представлены в Сети. Однако мы советуем преобразовать сценарии VB и составить сценарии на языке PowerShell. Это оптимальное решение.

PowerShell и ADSI

Многие операции администрирования требуют работы со службой каталогов. В PS первой версии выполнять такие операции можно было, но не так удобно, как, например, работать с WMI, реестром и т. д. Во второй версии добавился модуль взаимодействия со службой каталогов, но данный вариант требует использования в качестве контроллеров домена серверов Windows 2008 R2. Поэтому имеет смысл воспользоваться дополнительными свободными командлетами, разработанными компанией Quest Software (**http://www.quest.com/powershell/activeroles-server.aspx**). С указанной страницы можно загрузить пять новых командлетов, с помощью которых можно выполнять операции с пользователями и группами Active Directory.

Командлеты от Quest Software снабжены развернутой справочной документацией, по которой легко настроить собственные сценарии. В качестве примера приведем из руководства сценарий, с помощью которого текущий пользователь подключается к контроллеру домена (любому) и получает список записей в указанном контейнере:

```
get-QADUser -SearchRoot 'company.com/UsersOU'
```

Несколько советов по созданию собственных сценариев

Описать все нюансы использования PowerShell практически невозможно. Поэтому, отсылая читателя к поиску соответствующих ресурсов в Сети, мы дадим несколько кажущихся нам важными советов.

Комментируйте сценарии

Не думайте, что через полгода вы вспомните нюансы программирования конкретного сценария, цели его создания и т. п. Комментируйте, комментируйте и еще раз комментируйте. Обязательно предваряйте сценарий заголовком (кто и когда его создал, какие изменения вносились в него, для чего сценарий предназначен, опишите его параметры, если они есть, и т. д.) и добавьте описания к неочевидным операциям.

Не забывайте, что результат выполнения запроса — объект

Иногда упущение факта, что результат выполнения запроса в PowerShell является объектом, может привести к ошибкам, которые просто можно не заметить. Посмотрите следующий пример:

```
$ts = Get-TSServers
$ts

Server   IsOpen
------   ------
SERVER1  False
SERVER2  False
SERVER3  False
Foreach ($server in $ts) {Get-TSSession-Computername $server -Filter
{$_.ConnectionState -eq 'Disconnected' -OR $_.ConnectionState -eq 'Active'}
-ErrorAction silentlycontinue}
```

В примере используется модуль управления сессиями терминального сервера, загруженный по ссылке **http://archive.msdn.microsoft.com/PSTerminalServices**. Первая команда примера получает в переменную `$ts` список всех терминальных серверов организации. Вторая команда выводит этот список на экран. Далее мы хотим получить данные обо всех терминальных сессиях на всех серверах. Делаем цикл по списку и получаем нулевой вывод.

Внешне все нормально. Но если запросим информацию по конкретному серверу командой Get-TSSession, то получим уже ненулевой вывод. В чем причина?

Причина ошибки в том, что список терминальных серверов — это список объектов. Когда мы выводим его просто на экран, то PowerShell применяет специальные форматы для вывода данных, в нашем случае заголовки вывода обозначены как "Server" и "IsOpen". Если мы попробуем указать в параметрах команды цикла название объекта, то ничего не получим.

Попытаемся понять, какое свойство объекта нужно указать в параметрах команды. Посмотрим список серверов в более подробном формате вывода:

```
$ts | fl
ServerName: SERVER1
Local: False
IsOpen: False
Handle: Cassia.Impl.RemoteServerHandle
```

```
ServerName: SERVER1
Local: False
IsOpen: False
Handle: Cassia.Impl.RemoteServerHandle
....
```

Из этого вывода понятно, что имя терминального сервера — это свойство `ServerName`, именно его нужно указать в цикле. Поэтому следующая команда сформирует уже правильный результат:

```
Foreach ($server in $ts) {Get-TSSession-Computername $server.ServerName -Filter
{$_.ConnectionState -eq 'Disconnected' -OR $_.ConnectionState -eq 'Active'} -
ErrorAction silentlycontinue}
```

Используйте примеры

Большинство администраторов при составлении собственных сценариев использует в качестве прототипа образцы, опубликованные в Интернете. Они только дорабатываются под конкретные требования: исправляются имена доменов, подразделений, фильтры, часто объединяются (например, сценарий, получающий список некоторых объектов, со сценарием, удаляющим объекты такого типа) и т. д.

Узнайте свойства объектов

Конечно, можно начать создание сценария "с нуля", воспользовавшись своим знанием объектов языка программирования, но такой путь оправдан только для профессиональных программистов. На практике найти подходящий пример не представляет никакой сложности.

При написании или модификации сценариев на PowerShell необходимо правильно указывать названия тех свойств и методов объекта, которые будут использованы при обработке. Хорошо, если в примере уже указана фильтрация по желаемому параметру. Но и отобразить на экране весь список параметров и методов объекта не представляет никакой сложности.

Получить список параметров и методов объекта можно различными способами.

Для отображения полного комплекта свойств и методов объекта используется командлет Get-Member. Например, если запустить Блокнот, то следующей строкой можно вывести на экран все параметры соответствующего процесса:

```
Get-Process notepad | Get-Member
```

В результате можно увидеть, значения каких параметров можно получить, какими методами воспользоваться для управления процессом и т. д.

Можно воспользоваться и командлетом Format-List. В этом случае на экран будет выведен перечень параметров/методов с указанием текущих их значений. Например, для процесса notepad вывод будет примерно таким (сокращенно):

```
Get-Process notepad | Format-List *
__NounName: Process
Name: notepad
```

```
Handles: 34
VM: 27840512
WS: 1683456
PM: 741376
NPM: 2080
Path: C:\WINDOWS\system32\notepad.exe
Company: Корпорация Майкрософт
CPU: 0,765625
FileVersion: 5.1.2600.5512 (xpsp.080413-2105)
ProductVersion: 5.1.2600.5512
Description: Блокнот
...
```

Если вывод команды не содержит необходимую информацию, то самый простой способ включить ее отображение — это узнать (с использованием командлета Get-Member) название соответствующего свойства, а потом включить его с помощью команды Format-List. Например, так можно узнать путь к исполняемым файлам процессов:

```
get-process <имя_процесса> | format-list name, path
```

Так, для процесса winlogon мы получим следующий результат:

```
> get-process winlogon | fl name, path
Name: winlogon
Path: \??\C:\WINDOWS\system32\winlogon.exe
```

Отображайте весь вывод

Командлеты выводят на экран только часть данных в соответствии с настройками по умолчанию. Самый простой способ вывести на экран всю информацию — это использовать конвейер на команду Format-List:

```
<командлет с параметрами> | Format-List
```

Семь раз проверьте, потом выполняйте

Одной строчкой в PS можно внести очень серьезные изменения в настройки системы, например, удалить большую группу компьютеров из домена или файлы определенного типа по всему компьютеру. Небольшая ошибка в использовании параметров команды приводит к неожиданному результату. Поэтому золотым правилом использования PS для администрирования является принцип обязательной тщательной проверки сценариев перед началом их применения.

Помочь избежать влияния ошибок в сценарии может специальный ключ, который есть в командах, вносящих изменения: `-WhatIf`. Если добавить этот ключ, то изменения в настройках произведены не будут, но на экран будет выведена информация о тех операциях, которые были бы осуществлены без этого ключа. Посмотрите пример сценария, который устанавливает права доступа к группе файлов по образцу:

```
$newACL = get-acl my_file.txt
get-childitem c:\my_folder -recurse-include *.txt -force | set-acl
-aclobject $newacl -WhatIf
```

При использовании параметра `-WhatIf` на экран будут выведены следующие сообщения:

```
WhatIf: Выполнение операции "Set-Acl" над целевым объектом
"Microsoft.PowerShell.Core\FileSystem:: C:\my_folder\test.txt
```

Администратор может оценить список, уточнить критерии отбора, и после проверки новых параметров для реального выполнения команды ему нужно будет только вернуть на экран выполненную команду и удалить из нее `-WhatIf`.

Предусматривайте обработку ошибок

Если вы начинаете использовать сценарии PowerShell для практического администрирования, то их желательно дополнить обработкой возможных ошибок. Например, целевой компьютер будет недоступен или какая-то команда управления выполнится с ошибкой. Существуют специальные операторы, позволяющие описать различное поведение сценария в случае возникновения ошибки. Это:

```
Try {блок PowerShell операторов}
Catch {операторы, выполняемые при возникновении ошибки в блоке Try}
Finally {операторы, которые выполняются всегда}
```

Используйте их для корректной обработки ошибок.

Windows Management Interface

Windows Management Interface (WMI) — это технология управления Windows-компьютерами, реализующая стандарты веб-управления предприятием (WBEM, Web-based Enterprise Management). Если вы захотите выполнить какую-либо WMI-команду, то делать это следует путем создания WMI-сценария и исполнения его в интерпретаторе wmic.

> ***Примечания***
>
> WBEM разработан Distributed Management Task Force (**http://www.dmtf.org/**). В некотором смысле можно считать WMI "развитием" протокола SNMP для программных сред.
>
> Технология WMI реализована для всех операционных систем Windows, начиная с Windows 95. Однако устанавливается эта подсистема по умолчанию только в Windows Millennium Edition, Windows 2000, Windows XP, Windows Server 2003 и последующих операционных системах. Для других поддерживаемых версий Windows файлы установки доступны для бесплатной загрузки.

Практическое использование WMI для получения данных о состоянии оборудования или программной среды во многом напоминает работу с базой данных: вам необходимо указать, какие параметры от какого объекта должны быть получены и при каких ограничениях (фильтрах). Язык запросов для WMI так и называют — WMI Query Language (WQL). Даже команды WQL принято называть *запросами*.

В Windows WMI выполняет функции сбора данных и управления конфигурацией компьютера через специализированные программные модули, называемые *провайдерами* (providers). Существуют провайдеры для управления драйверами Windows, операционной системой, Internet Explorer, Microsoft Office, службами каталогов и т. п. Этот список постоянно пополняется, и при установке на компьютер какого-либо программного обеспечения перечень управляемых объектов может существенно расшириться.

На практике для применения WMI с целью контроля системы нужно знать, какие классы и пространства имен доступны, какие названия имеют соответствующие элементы *(instance)*. Полный перечень доступных к использованию в конкретной системе элементов WMI можно получить, например, с помощью средств WMI Object Browser и WMI CIM Studio, входящих в состав WMI Administrative Tools (рис. 5.19).

> ***Примечание***
>
> Эти программы бесплатно можно загрузить с сайта по ссылке **http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=6430f853-1120-48db-8cc5-f2abdc3ed314**.
>
> Хотя, чтобы не набирать столь длинную строку, быстрее будет воспользоваться поиском на странице загрузки Microsoft по их названию.

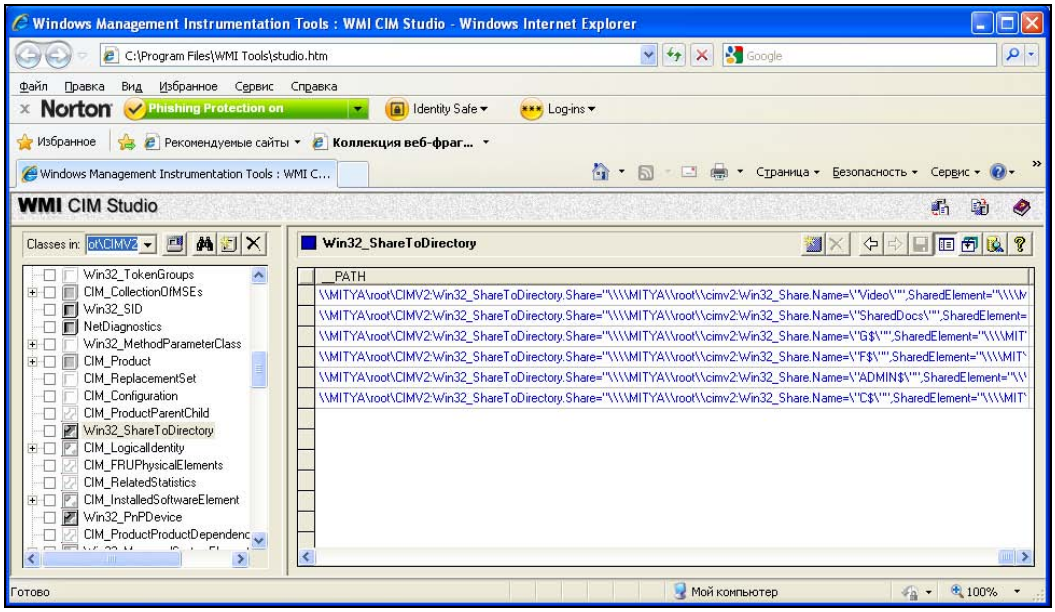


Рис. 5.19. Один из экранов WMI Administrative Tools

Для использования WMI необходимо знать иерархическую структуру объектов системы. Запомнить ее практически невозможно, поэтому при составлении запросов могут помочь такие продукты, как WMI CIM Studio. С помощью данной про-

граммы администратор имеет возможность подключиться к любому пространству имен, зарегистрированному в системе, отобразить существующие классы объектов, увидеть свойства класса (те характеристики, которые можно получить при исполнении запроса) и методы (те параметры, которые можно установить в команде), перечислить существующие экземпляры. Здесь же можно открыть окно, в котором попробовать создать собственный WMI-запрос и сразу увидеть его результаты. Пакет WMI Administrative Tools удобен тем, что наряду с просмотром существующих на компьютере классов WMI администратор может получить значения реальных объектов (на рисунке показано перечисление всех предоставляемых в совместный доступ папок на компьютере), составить и отладить WQL-запросы.

Эти утилиты отображают полный список существующих классов, значения их свойств и т. п. Часто требуется получить значения типовых характеристик, например, состояния служб, параметров физических или логических дисков и т. д. В этом случае можно воспользоваться подборкой уже готовых WMI-сценариев — программой Scriptomatic (бесплатно доступна к загрузке с сайта Microsoft по ссылке

http://www.microsoft.com/downloads/details.aspx?familyid=09DFC342-648B-4119-B7EB-783B0F7D1178&displaylang=en).

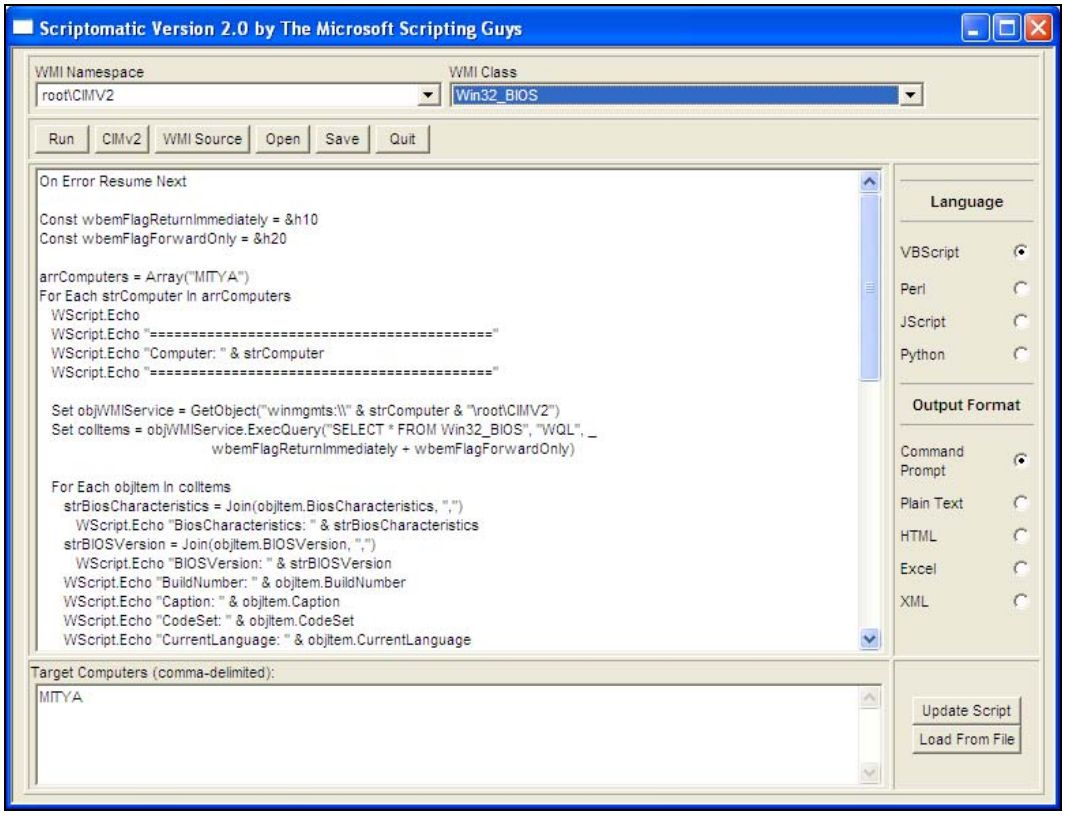


Рис. 5.20. Утилита Scriptomatic 2.0

Примечание

Доступна также и подборка бесплатных сценариев TechNet Script Center Sample Scripts — **http://www.microsoft.com/downloads/details.aspx?familyid=B4CB2678-DAFB-4E30-B2DA-B8814FE2DA5A&displaylang=en**. Большая подборка решений представлена в TechNet Script Repository и т. д.

Scriptomatic (рис. 5.20) позволяет найти сценарий, с помощью которого можно получить желаемые сведения о работе системы, и на его основе составить WQL-запрос для использования в CheckWMI. Утилита содержит большую подборку готовых сценариев, пригодных для составления необходимых запросов.

ГЛАВА 6

Доменная организация информационной системы

В современной информационной системе большинство данных предоставляется с общих ресурсов. Для упрощения управления в подобной структуре обычно создается та или иная система централизованного управления. Сегодня системы управления основываются на той или иной реализации централизованного *каталога*.

Указать некое число компьютеров, когда более выгодно переходить к централизованному управлению, достаточно сложно. Все зависит от конкретной практики администрирования. Хотя наличие 20—30 компьютеров обычно уже является причиной отказа от индивидуальных настроек систем.

Существует несколько реализаций единого каталога. В случае Windows систему централизованного управления принято называть *доменом*.

Домены Windows

В доменах Windows каждый компьютер "теряет" свою автономность, он подчиняется общим правилам *(политикам)*, а администратор домена получает полные права на каждой системе, включенной в домен. Локальный администратор может осуществлять свои функции в некоторых пределах, пока они не противоречат настройкам, заданным администратором домена.

Домены Windows могут быть реализованы и средствами Linux. За создание и работу домена Windows "отвечает" пакет Samba. Так же, как и в Windows, данные домена могут храниться в службе каталогов (пакет OpenLDAP), аутентификация происходить с использованием Kerberos (точнее, в Windows реализован открытый протокол Kerberos, применяемый в UNIX-системах) и т. п.

Структура домена Windows

В настоящее время домены Windows хранят информацию о своей структуре с помощью *службы каталогов* (Active Directory). Взаимодействие со службой каталогов происходит по протоколу LDAP (Lightweight Directory Access Protocol, протокол облегченного доступа к каталогам). Он является открытым стандартом, что

позволяет осуществлять взаимодействие со службой каталогов различным приложениям.

> ***Примечание***
>
> Утилитами, использующими протокол LDAP, из состава Windows можно работать с серверами LDAP из состава Linux и наоборот. Конечно, существуют некоторые ограничения и особенности реализации, в том числе и каталогов различных вендоров, например, IBM, Novell и т. д., но мы не будем их касаться в данной книге.

В терминах службы каталогов мы в домене работаем с объектами. Пользователи, компьютеры, подразделения, территории, предприятия и т. п., — все это объекты службы каталогов. Каждый объект описывается различными характеристиками — *свойствами*. Например, у пользователя это имя, фамилия, группа, в которую он входит, время действия учетной записи, допустимые часы работы в компьютерной сети, адрес электронной почты и т. п.

Работа со всеми объектами службы каталогов производится с учетом прав доступа (кто может создать нового пользователя, кому разрешено перевести его в другую штатную структуру и т. п.), сами операции специфичны для каждого объекта. Набор объектов, их атрибутов (свойств) и методов (допустимых операций) принято называть *схемой каталога*.

Служба каталогов Windows имеет следующую организационную структуру:

- ❒ лес;
- ❒ дерево;
- ❒ домен;
- ❒ организационное подразделение (OU);
- ❒ сайты.

Основная структурная единица домена, с которой придется работать администратору, — это *подразделение*. Подразделение (Organization Unit, OU) OU — это своеобразный контейнер, в который можно помещать как компьютеры, так и пользователей (естественно, что речь идет о соответствующих логических объектах). Основная причина создания OU для администраторов системы — возможность применения к объектам OU *групповых политик*.

Каждое OU может, в свою очередь, содержать внутри себя любое количество вложенных OU, учетные записи компьютеров и пользователей, группы (пользователей).

Если на одном предприятии существует несколько доменов с различными пространствами имен (например, **testorg.ru** и **testorg.cs**), то представленная графически такая структура будет напоминать *лес*. Лес — это коллекция (одного или более) доменов Windows, объединенных общей схемой, конфигурацией и двусторонними транзитивными доверительными отношениями.

Если домены и OU описывают логическую организацию, то *сайты* (Sites) предназначены для описания *территориальных делений*. Считается, что *внутри одного сайта* присутствуют скоростные каналы связи (иными словами, компьютеры сайта нахо-

дятся в одном сегменте локальной сети). А различные сайты связаны друг с другом относительно медленными каналами связи. Поэтому между ними создаются специальные механизмы репликации данных. Например, можно задать график репликации (использовать периоды наименьшей загрузки каналов связи), выбрать определенный протокол (IP или путем приема/передачи сообщений по протоколу SMTP) и т. п.

Соотношение территориальной и логической структуры выбирают исходя из конкретной конфигурации предприятия. Например, можно создать несколько сайтов в одном домене или сформировать в каждом сайте свой домен и т. п.

Для небольшого предприятия обычно создают структуру "один лес — один домен — несколько подразделений — один сайт".

Функциональные уровни

Служба каталогов (раздельно весь лес и домены) характеризуется *функциональным уровнем.* Функциональный уровень определяет набор возможностей, который поддерживается каталогом. Обычно, если нет особых причин, выбирается максимальный функциональный уровень. Если в домене присутствуют контроллеры с предыдущей версией операционной системы, то необходимо использовать и соответствующий функциональный уровень. Отличия уровней описаны в технической документации, так что администратор в любой момент сможет оценить, имеет ли смысл переключать службу каталогов на более высокий уровень или нет.

> ***Примечание***
>
> Операции повышения функционального уровня необратимы. Понизить уровень службы каталогов невозможно. Поэтому, выбирая операции повышения уровня, необходимо тщательно оценить данный шаг и его последствия.

Хозяева операций

В домене Windows 200*x* все контроллеры *равнозначны*. Однако для обеспечения правильной синхронизации данных между различными контроллерами некоторые функции зафиксированы только за одной системой. Такие функции носят название Flexible Single Master Operation role (FSMO). В доменах Windows 200*x* их пять:

- Schema master (один на лес);
- Domain naming master (один на лес);
- RID master (один на домен);
- PDC emulator (один на домен);
- Infrastructure master (один на домен).

При первоначальной установке домена все пять ролей зафиксированы за первым контроллером. Впоследствии их можно переносить на другие контроллеры, учитывая специфику структуры организации. Важно только, чтобы при исключении контроллера домена администратор был уверен, что все эти пять операций не потеряли хозяина.

Три роли (PDC, RID, Infrastructure) легко переносятся с помощью оснастки **AD Пользователи и компьютеры**. Необходимо просто открыть оснастку, подключиться к тому контроллеру домена, на который планируется перенести соответствующую роль, и выполнить соответствующую команду в меню.

Все операции по переносу ролей можно выполнить в командной строке. Для этого служит утилита `ntdsutil`. Главное, что эта утилита пригодна не только для переноса ролей при *работающих* контроллерах, но и для *назначения* нового владельца роли в случае аварийного выхода из строя прежнего хозяина.

> ***Примечание***
>
> Роли следует назначать с осторожностью, при полной уверенности в том, что прежний хозяин не будет вновь доступен в сети. Появление двух хозяев одной роли может привести к неработоспособности всего домена.

Опишем кратко последовательность операций, которые необходимо выполнить для назначения контроллеру домена новой роли.

1. Открыть утилиту и набрать команду `ROLES`.
2. Указать, к каким контроллерам необходимо подключиться, для чего набрать команду `CONNECTIONS` и ввести команду подключения к необходимому контроллеру. После этого закрыть опцию `CONNECTIONS`, набрав `QUIT`.
3. Выбрать нужную команду `SEIZE`..., чтобы переписать соответствующую роль.

Утилита сначала попытается корректно перенести выбранную роль и лишь при недоступности соответствующего контроллера будет выполнена операция перезаписи.

Сервер глобального каталога (GC)

Контроллеры домена хранят информацию об объектах *текущего* (собственного) домена. Поскольку в логической структуре предприятия может существовать несколько доменов, то для выполнения операций, затрагивающих объекты разных доменов, необходим доступ к соответствующим контроллерам. Для ускорения операций в домене существуют специальные контроллеры, которые в режиме только для чтения хранят *все объекты леса*, но не с полным, а с частичным набором атрибутов. Такие контроллеры называются *серверами глобального каталога* (Global catalog, GC).

В качестве GC может быть назначен любой контроллер домена. Назначение контроллера домена сервером глобального каталога производится через оснастку **Active Directory — сайты и службы**. Раскрыв узел, соответствующий нужному контроллеру, в его свойствах на вкладке **Общие** необходимо включить параметр использования контроллера в качестве GC (рис. 6.1).

Серверы GC хранят наиболее часто используемые атрибуты объектов. Условно можно считать, что объем хранимых на GC данных снижается примерно в два раза по сравнению с "полным" вариантом описания объекта. Но если конкретным приложениям необходим частый доступ к нереплицированным атрибутам, то админи-

стратор может внести изменения в параметры GC, откорректировав *схему организации*. Для этого достаточно в консоли управления оснасткой **AD Schema** (по умолчанию этой оснастки нет в списке меню, ее следует добавить в консоль управления) включить репликацию в свойствах соответствующих атрибутов.

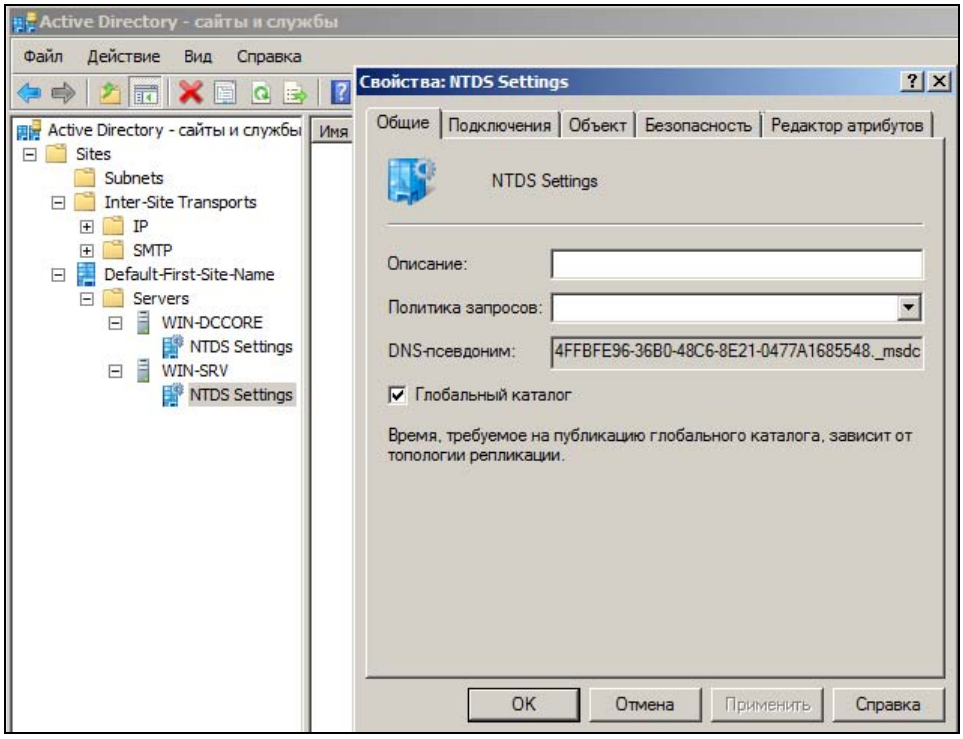


Рис. 6.1. Настройка контроллера в качестве сервера глобального каталога

Создание нового домена

Как уже говорилось, домены Windows могут быть созданы как с помощью серверов Windows, так и с использованием Linux-систем.

Создание домена на серверах Windows

Создание домена в Windows 2008 начинается с добавления соответствующей роли сервера. После установки служб каталогов для создания нового домена необходимо запустить утилиту `dcpromo`. В зависимости от ответов на вопросы мастера операции вы сможете добавить новый контроллер в существующем домене либо создать новый домен. Можно создать новый домен внутри уже существующего, либо создать новое дерево доменов, дав домену уникальное имя. Все операции достаточно просты и обычно выполняются в течение нескольких минут. После чего, перезагрузив компьютер, вы получаете новый контроллер домена.

Перед началом операции следует тщательно обдумать то доменное имя, которое вы дадите вновь создаваемому домену. Если ваша организация имеет уже зарегистрированное в Интернете доменное имя, то имя домена Windows может быть основано на нем. Ничто не запрещает вам избрать для внутреннего домена имя, которое не соответствует реальным доменам Интернета, например, дать название **myorg.local**.

> ***Примечание***
>
> Можно присвоить внутреннему домену реальное имя Интернета, а можно дать только локальное название. В любом случае по соображениям безопасности данные структуры домена Windows (DNS-сервера) не публикуются в глобальной сети.
>
> Обратите внимание, чтобы полное доменное имя *не являлось именем первого уровня*, а обязательно состояло из двух частей. В противном случае необходимо выполнить ряд дополнительных настроек, которые следует уточнить по документации с сайта разработчика.

Создание домена обязательно требует наличия сервера DNS. По умолчанию (если сервер DNS не настроен) программа установки предлагает создать и настроить локально сервер DNS. В общем случае служба каталогов не требует обязательного DNS-сервера разработки Microsoft. AD может быть установлена, например, на сервер BIND. При этом следует учесть, что BIND версии 4.9.7 и старше поддерживает возможность создания SRV-записей, которые необходимы для работы службы каталогов. А начиная с версии 8.2.2, поддерживаются и динамические обновления записей данного типа.

В целях обеспечения отказоустойчивости домена рекомендуется создавать не менее двух контроллеров, чтобы служба каталогов была работоспособна при отказе (выключении) любого контроллера домена.

Настройка Ubuntu в качестве контроллера домена

Сразу следует сказать, что сегодня Linux-системы не могут выступать в качестве полноценных аналогов контроллеров домена, аналогичных службе каталогов Windows Server 2008. С использованием пакета Samba 4 поддерживается следующая функциональность:

- аутентификация в службе каталогов административных протоколов для систем Windows XP/7 и OS X;
- групповые политики;
- внутренние LDAP-сервер (с AD-семантикой) и Kerberos-сервер;
- интеграция DNS-сервера Bind 9 со службой каталогов;
- асинхронные процессы работы служб, улучшенная масштабируемость от малых до крупных организаций

и т. д.

Учтите, что сейчас к разработке пакета Samba официально подключилась и компания Microsoft.

Примечание

Учитывая фактический состав информационных систем, использование доменов Windows на Linux-системах оправдано для небольших и средних организаций...

Серверы Linux в качестве контроллеров домена

В качестве контроллера домена может быть настроена любая Linux-система, как рабочая станция, так и сервер. Для этих целей предназначен пакет Samba. Настройка Linux-системы для использования в качестве контроллера домена широко описана в Интернете. Найти информацию по настройкам и устранению возможных проблем достаточно легко. Например, на странице **http://help.ubuntu.ru/wiki/samba4_as_dc_12.04** описаны операции создания домена Windows на сервере Ubuntu 12.04 с использованием пакета Samba 4.0. Другой справочный документ — **https://help.ubuntu.com/12.04/serverguide/samba-dc.html** — подскажет, как настроить контроллер домена в случае использования версии Samba 3, когда в домене будет поддерживаться только централизованная аутентификация пользователей и компьютеров (аналог домена Windows NT4).

При изучении справочной документации учтите, что существует несколько вариантов организации домена на Linux-системах. Традиционные конфигурации предполагают хранение паролей пользователей в файлах на контроллерах домена. Сегодня существует более прогрессивная технология — хранение идентификационных данных в службах каталогов (серверах LDAP). Преимущества таких решений, во-первых, в универсальности: многие прикладные программы сегодня используют службы каталогов. Во-вторых, базы служб каталогов хорошо реплицируются между серверами, что позволяет создать отказоустойчивую структуру.

Настройка Samba+LDAP несколько более трудоемка. Она предполагает установку пакетов, настройку LDAP на функционирование по схеме Samba (иными словами, добавление в базу службы каталогов новых параметров для работы в домене), настройку Samba на аутентификацию в LDAP. Эти процедуры весьма подробно описаны и рекомендации широко представлены в Сети (достаточно выполнить поиск на ключевые слова sabma, OpenLDAP-LDAP, ubuntu; например, **https://help.ubuntu.com/12.04/serverguide/openldap-server.html**). Интересующихся читателей мы отошлем к таким руководствам.

Мы же опишем более подробно настройку сервера Ubuntu в качестве контроллера домена при наличии пакета OpenLDAP из состава Zimbra — бесплатной системы корпоративной работы, включающей в себя электронную почту, общие адресные книги, календари, общие папки и т. д.

Настройка контроллера домена на сервере корпоративной почты Zimbra

Примечание

В описании настроек данной конфигурации были использованы рекомендации, содержащиеся на странице **http://wiki.zimbra.com/index.php?title=UNIX_and_Windows_Accounts_in_Zimbra_LDAP_and_Zimbra_Admin_UI**. Эти рекомендации соответствуют версии Zimbra 7.

Для настройки домена на основе службы LDAP из состава Zimbra необходимо:

- ❒ настроить LDAP из состава Zimbra для работы с Samba;
- ❒ установить расширения для управления учетными записями служб Postfix и Samba из административной консоли Zimbra;
- ❒ установить службу Samba в Ubuntu и настроить ее для LDAP-аутентификации;
- ❒ настроить аутентификацию в Ubuntu на использование сервера LDAP.

Обратите также внимание, что время на рабочих станциях и контроллере домена должно быть синхронизировано. Отличия в текущем времени являются типовыми причинами ошибок добавления рабочих станций в домен.

Настройка LDAP

Сервер LDAP установлен в составе пакета Zimbra. Необходимо только расширить его схему для настройки системы в качестве контроллера домена.

Файлы конфигурации схем находятся в папке /opt/zimbra/data/ldap/config/cn=config/cn=schema (в случае установки Zimbra в папку по умолчанию). Это файлы с расширением ldif, имена которых содержат номер загрузки соответствующей схемы при старте сервера (cn={3}zimbra.ldif — загружается третьим по очереди).

Шаблон нужной схемы хранится уже на сервере, его необходимо только немного отредактировать. Выполните последующие шаги от имени пользователя zimbra.

1. Остановите сервер LDAP и скопируйте шаблон в папку схем с новым именем cn={10}nis.ldif:

```
ldap stop
cp /opt/zimbra/openldap/etc/openldap/schema/nis.ldif
/opt/zimbra/data/ldap/config/cn\=config/cn\=schema/cn\=\{10\}nis.ldif
cd /opt/zimbra/data/ldap/config/cn\=config/cn=\schema
```

2. Замените следующие строки в нем:

```
dn: cn=nis,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: nis
```

   на

```
dn: cn={10}nis
objectClass: olcSchemaConfig
cn: {10}nis
```

3. Назначьте права доступа и запустите сервер LDAP:

```
chmod 600 cn\=\{10\}nis.ldif
ldap start
```

4. Для настройки LDAP необходимо также "представить" схему, используемую пакетом Samba, которая зависит от версии Samba и включена в состав пакета samba-doc. Установите этот пакет и скопируйте схему (файл samba.schema, находится в архивированном виде как /usr/share/doc/samba-doc/examples/LDAP/

samba.schema.gz, для распаковки введите команду `gunzip` *`имя_архива`*) в папку /opt/zimbra/openldap/etc/openldap/schema/.

Эта схема выполнена в "старом" формате, ее необходимо преобразовать в новый формат следующими командами (от имени пользователя zimbra, операции выполним во временной папке, замените в следующих примерах `path` на фактическое значение пути к схеме samba):

```
mkdir -p /tmp/ldap/schema
cd /tmp/ldap
cp /path/to/samba.schema /tmp/ldap/schema
```

5. Создайте файл test.conf со следующим содержимым:

```
include /opt/zimbra/openldap/etc/openldap/schema/core.schema
include /opt/zimbra/openldap/etc/openldap/schema/cosine.schema
include /opt/zimbra/openldap/etc/openld
```

6. После чего выполните

```
/opt/zimbra/openldap/sbin/slaptest -f /tmp/ldap/test.conf -F /tmp/ldap
```

В результате в папке /tmp/ldap/cn=config/cn=schema/ будут созданы несколько файлов конфигураций. Нас интересует файл cn={3}samba.ldif, который придется переименовать в cn={11}samba.ldif, поскольку первые 10 номеров используются сервером Zimbra:

```
mv cn\=\{3\}samba.ldif cn\=\{11\}samba.ldif
```

7. В этом файле также нужно заменить следующий блок:

```
dn: cn={3}samba
objectClass: olcSchemaConfig
cn: {3}samba
```

на

```
dn: cn={11}samba
objectClass: olcSchemaConfig
cn: {11}samba
```

8. После чего следует скопировать конфигурацию в папку сервера LDAP и запустить его:

```
ldap stop
cp /tmp/ldap/cn\=config/cn\=schema/cn\=\{11\}samba.ldif
/opt/zimbra/data/ldap/config/cn\=config/cn\=schema/
ldap start
```

9. Для использования возможностей NIS следует вручную добавить индексы к LDAP. Выполняется операция командой `ldapmodify`, которой нужно указать пароль сервера LDAP. Узнать его можно следующей командой:

```
zmlocalconfig -s ldap_root_password
```

10. Теперь, зная пароль, выполните

```
ldapmodify-x -H ldapi:/// -D cn=config -W
```

и введите следующий текст:

```
dn: olcDatabase={2}hdb,cn=config
changetype:modify
add: olcDbIndex
olcDbIndex: uidNumber eq
olcDbIndex: gidNumber eq
olcDbIndex: memberUid eq
```

Завершите ввод нажатием клавиш <Ctrl>+<D>. В результате этого сервер LDAP автоматически начнет создавать индексы для новых атрибутов.

11. После всех этих изменений следует перестартовать службы Zimbra (`zmcontrol stop & zmcontrol start`) и проверить их состояние (running).

12. Теперь необходимо создать две учетные записи для служб Posix и Samba. При добавлении их в LDAP нужно указать хэши их паролей, которые можно получить следующей командой:

```
/opt/zimbra/openldap/sbin/slappasswd -s пароль
```

13. Для создания пользователей нужно подготовить файл (например, /tmp/posixusers.ldif) со следующим содержимым (замените пароль на полученные хэши паролей пользователей):

```
dn: uid=zmposix,cn=appaccts,cn=zimbra
uid: zmposix
objectClass: zimbraAccount
objectClass: organizationalPerson
cn: zmposix
sn: zmposix
zimbraAccountStatus: active
zimbraIsSystemResource: TRUE
zimbraId: 59BC2282-98CC-11DE-9492-C023E3CEB16B
description: The zimbra posix account
userPassword: {SSHA}хэш пароля

dn: uid=zmposixroot,cn=appaccts,cn=zimbra
uid: zmposixroot
objectClass: zimbraAccount
objectClass: organizationalPerson
cn: zmposixroot
sn: zmposixroot
zimbraAccountStatus: active
zimbraIsSystemResource: TRUE
zimbraId: 6ED47B38-98CC-11DE-AAC1-9F159BA35B33
description: The zimbra posix root account
userPassword: {SSHA}хэш пароля
```

14. Для добавления учетных записей нужно выполнить следующую команду:

```
ldapadd -f /tmp/posixusers.ldif-x -H ldapi:/// -D cn=config -W
```

15. Теперь надо предоставить этим учетным записям права на работу с объектами каталога. Для этого подготовьте следующий файл, заменив в нем `dc=my_server,dc=zimbra,dc=com` на имя вашего сервера Zimbra:

```
dn: olcDatabase={2}hdb,cn=config
changetype:modify
delete: olcAccess
olcAccess: {0}
-
add: olcAccess
olcAccess: {0}to attrs=userPassword by anonymous auth by
dn.children="cn=admins,cn=zimbra" write by
dn.exact="uid=zmposixroot,cn=appaccts,cn=zimbra" write

dn: olcDatabase={2}hdb,cn=config
changetype:modify
delete: olcAccess
olcAccess: {9}
-
add: olcAccess
olcAccess: {9}to attrs=entry by dn.children="cn=admins,cn=zimbra" write by
dn.exact="uid=zmposixroot,cn=appaccts,cn=zimbra" write by * read

dn: olcDatabase={2}hdb,cn=config
changetype:modify
add: olcAccess
olcAccess: {10}to dn.subtree="dc=my_server,dc=zimbra,dc=com" by
dn.children="cn=admins,cn=zimbra" write by
dn.exact="uid=zmposixroot,cn=appaccts,cn=zimbra" write by
dn.exact="uid=zmposix,cn=appaccts,cn=zimbra" read by * none
olcAccess: {11}to dn.subtree="ou=machines,dc=my_server,dc=zimbra,dc=com" by
dn.children="cn=admins,cn=zimbra" write by
dn.exact="uid=zmposixroot,cn=appaccts,cn=zimbra" write by
dn.exact="uid=zmposix,cn=appaccts,cn=zimbra" read by * none
olcAccess: {12}to dn.subtree="ou=groups,dc=my_server,dc=zimbra,dc=com" by
dn.children="cn=admins,cn=zimbra" write by
dn.exact="uid=zmposixroot,cn=appaccts,cn=zimbra" write by
dn.exact="uid=zmposix,cn=appaccts,cn=zimbra" read by * none
olcAccess: {13}to dn.subtree="ou=people,dc=my_server,dc=zimbra,dc=com" by
dn.children="cn=admins,cn=zimbra" write by
dn.exact="uid=zmposixroot,cn=appaccts,cn=zimbra" write by
dn.exact="uid=zmposix,cn=appaccts,cn=zimbra" read by * none
```

16. Для внесения изменений выполните

```
ldapmodify -f /tmp/acl.ldif-x -H ldapi:/// -D cn=config -W
```

и завершите настройку следующими командами:

```
zmprov mcf +zimbraAccountExtraObjectClass posixAccount
zmprov mcf +zimbraAccountExtraObjectClass sambaSamAccount
```

Установка расширений Zimbra для управления служебными учетными записями

Чтобы управлять служебными учетными записями в административной консоли Zimbra, необходимо установить расширения zimbraSamba и ZimbraPosixAccount.

Расширения zimbraSamba и ZimbraPosixAccount входят в состав установочного комплекта Zimbra, но их необходимо перед установкой отредактировать, указав параметры вашего домена. После установки Zimbra их файлы находятся в папке /opt/zimbra/zimlets-admin-extra.

В обоих архивах необходимо отредактировать содержимое config_template.xml, для этого нужно извлечь этот файл, внести в него описанные далее изменения, сохранить их и этим файлом заменить исходный файл в архиве. Эти операции можно выполнить и за один шаг, если, например, воспользоваться возможностями пакета Midnight Commander по редактированию файлов внутри архива.

В файле config_template.xml необходимо установить реальное значение для параметра `ldapSuffix`. Его значение должно указывать на ваш домен. Например, если домен имеет имя **example.com**, то `ldapSuffix` следует заменить на `dc=example,dc=com`. Если у вас домен третьего уровня, то значение `ldapSuffix` может выглядеть примерно так: `dc=my_server,dc=example,dc=com`.

> ***Примечание***
>
> Можно также откорректировать параметры `uidBase` и `gidBase`. Они определяют начало нумерации идентификаторов при создании учетных записей пользователей и групп соответственно. По умолчанию они установлены в `10000`, и если нет особых причин, то можно эту настройку сохранить.

После того как вы внесете необходимые изменения в оба архива, эти расширения нужно установить в Zimbra. Для чего достаточно зайти в административную консоль управления, слева в панели навигации выбрать **Конфигурация | Admin Extensions**, нажать кнопку **Инсталляция** в правой части консоли и указать на отредактированные вами файлы архивов. Если администрирование ведется с удаленной системы, то эти файлы нужно предварительно на нее скопировать (выбор файлов возможен только с локальных дисков).

> ***Совет***
>
> Автор советует устанавливать расширения последовательно и после каждого шага перезагружать административную консоль (закрыть и снова открыть).

Установка Samba и сопутствующих пакетов

Для настройки сервера Zimbra в качестве контроллера домена необходим пакет Samba 3.

```
apt-get install samba samba-doc
```

После установки пакетов можно приступать к редактированию настроек Samba (/etc/samba/smb.conf). Основные параметры конфигурации должны соответствовать указанным в листинге 6.1.

Листинг 6.1

```
[global]

workgroup = EXAMPLE
netbios name = my_server
os level = 33
preferred master = yes
enable privileges = yes
wins support =yes
dns proxy = no
name resolve order = wins bcast hosts
security = user
encrypt passwords = true
ldap passwd sync = yes
passdb backend = ldapsam:ldap://my_server.example.com/
ldap admin dn = "uid=zmposixroot,cn=appaccts,cn=zimbra"
ldap suffix = dc=my_server,dc=example,dc=com
ldap group suffix = ou=groups
ldap user suffix = ou=people
ldap machine suffix = ou=machines
obey pam restrictions = no
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\spassword:* %n\n *Retype\snew\spassword:* %n\n
*password\supdated\ssuccessfully*.
domain logons = yes
logon path =
logon home =
logon script = logon.cmd
add user script = /usr/sbin/adduser --quiet --disabled-password --gecos "" %u
add machine script = /usr/sbin/adduser --shell /bin/false --disabled-password -
-quiet --gecos "machine account" --force-badname %u
socket options = TCP_NODELAY
domain master = yes
local master = yes

[homes]
comment = Home Directories
browseable =yes
read only = No
valid users = %S

[netlogon]
comment = Network Logon Service
path = /var/lib/samba/netlogon
guest ok = yes
locking = no
```

```
[profiles]
comment = Users profiles
path = /var/lib/samba/profiles
read only = No
```

В листинге 6.1 представлена только часть параметров, которые относятся к настройке LDAP-конфигурации Samba. Естественно, что имена из примера необходимо заменить реальными названиями серверов.

Дадим некоторые пояснения к примененным параметрам:

- `passdb backend` — в качестве его значения нужно указать имя вашего сервера LDAP (сервера Zimbra);
- `ldap admin dn` — параметр подключения к LDAP для Zimbra;
- `ldap suffix` — имя домена. Мы его указывали при редактировании файлов config_template.xml (параметр `ldapSuffix`);
- `ldap group suffix`, `ldap machine suffix` и `ldap user suffix` — определены в файле config_template.xml. Указанные значения — это их величины при установке Zimbra по умолчанию.

Сохранив настройки конфигурации, проверьте конфигурацию на отсутствие ошибок (командой `testparm`) и перестартуйте сервер Samba. Далее, Samba нужно сообщить пароль для доступа к LDAP в Zimbra. Как узнать этот пароль, описано в *разд. "Настройка LDAP" ранее в этой главе*. Для указания пароля выполните:

```
smbpasswd -w пароль
```

Настройка параметров аутентификации

Для LDAP-аутентификации нужно добавить в систему пакеты pam_ldap и nss_ldap:

```
apt-get install libpam-ldap libnss-ldap nss-updatedb libnss-db
```

В процессе установки необходимо определить ряд параметров настройки, ответив на вопросы мастера операций. При настройке имени сервера следует указать ldap://*имя_сервера_Zimbra*. Параметр Distinguished name of search base определить в соответствии с именем домена — точно таким же, как и значение `ldapSuffix`, которое вы настроили в файлах zimbraSamba и ZimbraPosixAccount: `dc=example,dc=com` или `dc=my_server,dc=example,dc=com`.

Далее нужно задать версию LDAP равной 3, локального суперпользователя не следует определять администратором LDAP, но укажите, что сервер LDAP требует параметров учетной записи для подключения. Эта учетная запись должна быть введена как `uid=zmposix,cn=appaccts,cn=zimbra`, на следующем шаге нужно указать пароль этой записи (мы его узнали чуть ранее, когда настраивали параметры доступа для службы Samba).

После завершения установки пакетов необходимо вручную внести некоторые дополнительные изменения. Во-первых, проверьте содержимое файла /etc/ldap.conf, чтобы в нем присутствовали строки по образцу, приведенному в листинге 6.2.

Листинг 6.2

```
host my_server.zimbra.com
base dc=my_server,dc=zimbra,dc=com
binddn uid=zmposix,cn=appaccts,cn=zimbra
bindpw пароль
rootbinddn uid=zmposixroot,cn=appaccts,cn=zimbra
port 389
bind_policy soft
nss_reconnect_tries 2
uri ldap://my_server.zimbra.com/
ssl start_tls
tls_cacertdir /opt/zimbra/conf/ca
# tell to not check the server certificate
tls_checkpeer no
# optional
pam_password md5
# where nss find the information
nss_base_passwd ou=people,dc=my_server,dc=zimbra,dc=com?one
nss_base_shadow ou=people,dc=my_server,dc=zimbra,dc=com?one
nss_base_group ou=groups,dc=my_server,dc=zimbra,dc=com?one
nss_base_hosts ou=machines,dc=my_server,dc=zimbra,dc=com?one
```

Примечание

Указанные строки находятся в разных частях файла и обычно закомментированы. Вам необходимо снять комментарий и отредактировать содержимое строк по фактическим именам сервера и домена.

В строке `bindpw`, строго говоря, указывается пароль для другой учетной записи. Но при установке по умолчанию этот пароль совпадает с полученным нами ранее значением. Проверить пароль можно командой `zmlocalconfig -s zimbra_ldap_password`.

Во-вторых, создайте файл с паролем пользователя `uid=zmposixroot,cn=appaccts,cn=zimbra` и сохраните его как /etc/ldap.secret. В целях безопасности назначьте ему права чтения только для владельца.

Ubuntu использует 4 файла: /etc/pam_ldap.conf, /etc/pam_ldap.secret, /etc/libnss-ldap.conf и /etc/libnss-ldap.secret. Для упрощения для второй пары файлов лучше создать символические ссылки к первым файлам.

Теперь необходимо изменить содержимое ряда файлов, отвечающих за аутентификацию пользователей. В качестве образца подходят рекомендации, содержащиеся в файле /etc/auth-client-config/profile.d/ldap-auth-config. В листинге 6.3 приведены названия файлов, которые следует отредактировать, и их новое содержимое.

Листинг 6.3

```
/etc/pam.d/common-auth
auth sufficient pam_ldap.so
auth sufficient pam_unix.so
```

```
/etc/pam.d/common-account
account sufficient pam_ldap.so
account sufficient pam_unix.so

/etc/pam.d/common-password
password sufficient pam_unix.so
password sufficient pam_ldap.so

/etc/pam.d/common-session
session required pam_mkhomedir.so skel=/etc/skel/
session sufficient pam_unix.so
session sufficient pam_ldap.so
```

Следующим шагом отредактируйте файл /etc/nsswitch.conf (по умолчанию он настроен на хранение паролей в файлах). Замените строки, начинающиеся так же, как и в последующем примере, на такие значения:

```
passwd: files ldap
group: files ldap
shadow: files ldap
```

Перезагрузите сервер Ubuntu, чтобы изменения вступили в силу.

> ***Примечание***
>
> Следует быть внимательным при редактировании перечисленных файлов. Перед изменением сохраните оригинальные версии файлов в виде копий. В случае ошибки может возникнуть ситуация, когда вы даже не сможете войти в систему, указывая верные параметры учетной записи. Тогда необходимо при старте Ubuntu выбрать вариант безопасной загрузки, зайти в систему в однопользовательском режиме (пароль не будет запрошен) и исправить файлы конфигурации.

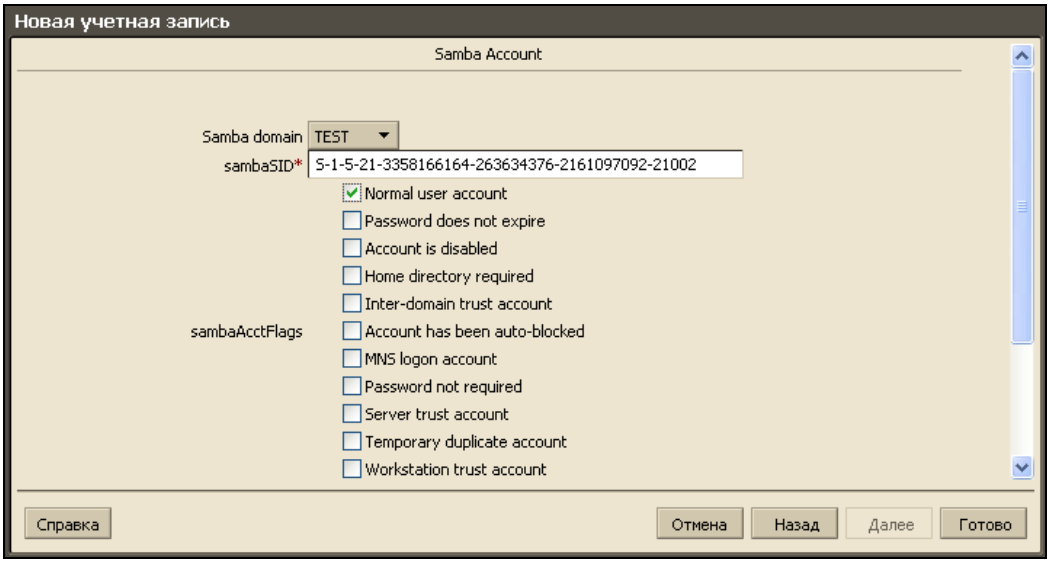


Рис. 6.2. Этап создания новой учетной записи ZCS в домене

После этих операций пользователей и группы Linux можно создавать в административной консоли Zimbra (рис. 6.2).

Обязательно проверьте, что службе Samba доступны учетные записи, созданные в административной консоли Zimbra. Чтобы проверить индивидуальные учетные записи, нужно ввести команду `getent passwd`, которая должна показать как локальные учетные записи Ubuntu, так и учетные записи, хранящиеся на сервере LDAP Zimbra. Для проверки списка групп используйте команду `getent group`.

При возникновении ошибок в настройке следует проанализировать файлы журналов (журнала Samba, авторизации — auth.log и др.). Как правило, причины ошибок видны по соответствующим записям (например, отсутствие контакта с сервером LDAP из-за неверно назначенного пароля или невозможность завершения авторизации пользователя домена в силу необходимости смены пароля при первом подключении и т. п.).

Создание специальных групп

Для работы в качестве домена Windows должны быть созданы специальные группы. Для этого в консоли управления Zimbra необходимо создать группы Domain Admins и Domain Users (следует указать вариант создания специальных групп и просто выбрать эти группы из предлагаемого списка). Другие специальные группы, соответствующие стандартным группам домена Windows, можете создавать или не создавать по своему усмотрению.

Группе Domain Admins необходимо назначить специальные привилегии, с помощью которых будут реализовываться права администраторов домена. Для этого в командной строке выполните:

```
net rpc rights grant "EXAMPLE\Domain Admins" SeAddUsersPrivilege
SeMachineAccountPrivilege SePrintOperatorPrivilege
```

Этими шагами можно ограничиться в настройке сервера Ubuntu с пакетом Zimbra 7 в качестве контроллера домена.

Добавление новых членов домена

Членами домена могут быть как Windows-системы, так и Linux. При этом объем изменений, вносимых в локальные настройки компьютеров, существенно зависит от типа операционной системы.

Добавление Windows-систем

Для того чтобы Windows-систему включить в состав домена, достаточно в свойствах компьютера на вкладке **Имя компьютера** выбрать вариант изменения его членства в рабочей группе или домене. Такую операцию может провести пользователь, обладающий административными правами над локальной системой и имеющий право добавления рабочей станции в домен.

По умолчанию каждый пользователь домена может включить в состав домена до 10 рабочих станций. Это значение определяется в атрибуте **ms-DS-Machine-AccountQuota** объекта "домен" службы каталогов. Изменить данное значение можно с помощью программы ADSI Edit из состава Resource Kit. Установка в 0 разрешает создание любого числа рабочих станций.

Более управляемым вариантом является предварительное создание администратором в службе каталогов объекта типа *компьютер* и предоставление права конкретным пользователям на его управление и включение в домен (рис. 6.3).

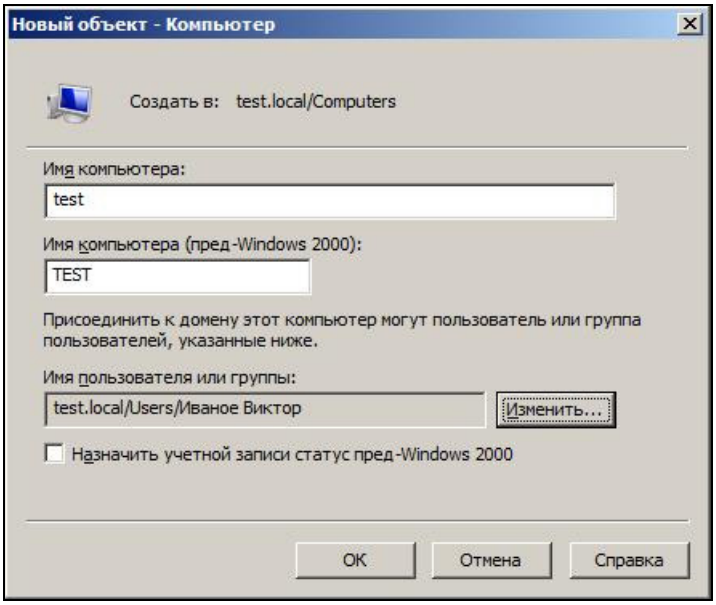


Рис. 6.3. Создание нового объекта службы каталогов — компьютера

При создании нового компьютера можно сразу назначить пользователя (или группу), которому будет предоставлено право добавления этой системы в домен. Этот вариант предпочтителен для использования в организациях, когда первоначальная и окончательная настройки системы выполняются различными специалистами, часто на разных участках.

> ***Примечание***
>
> Рабочую станцию можно добавить в домен удаленно командой `net computer /add` (см. онлайновую справку команды). Но это возможно только в том случае, если добавляемая система уже была ранее в составе какого-либо домена.

В небольших организациях операцию включения в домен администратор проводит непосредственно на рабочем месте пользователя. При этом администраторы на соответствующий запрос указывают свой пароль. Причем на этом этапе невозможно вместо пароля предоставить параметры аппаратной аутентификации, например, смарт-карты администратора. Такая ситуация не является вполне безопасной, поскольку на компьютере могут быть установлены различные перехватчики клавиа-

туры. Лучше создать специальную учетную запись с минимальными правами в домене, которую и использовать только для операций добавления рабочих станций.

Модификация настроек Windows-систем при добавлении их в домен

При включении компьютера в домен в локальную группу безопасности **Администраторы** добавляется группа администраторов домена, а в группу локальных пользователей — группа пользователей домена. Именно потому, что администратор предприятия состоит в группе локальных администраторов, он и получает право управления этим компьютером. А пользователи домена могут работать в системе, поскольку они состоят в группе пользователей домена, входящей в группу пользователей этого компьютера.

Кроме того, назначаются новые ресурсы для совместного использования: корневые каталоги всех локальных дисков (под именами C$, D$ и т. д.), каталог установки системы (ADMIN$), создается совместный ресурс IPC$ (для установки соединений *named pipes*), PRINT$ (для управления принтерами) и FAX$ (при наличии факса с совместным доступом). Эти ресурсы носят название *административных*, поскольку они предназначены для управления системами.

Данные ресурсы *невидимы* при просмотре сети (как и все другие совместные ресурсы, имя которых заканчивается знаком $). Если вы попытаетесь удалить их, то после перезагрузки системы они вновь восстановятся (настройкой реестра системы эти ресурсы можно отключить). За счет наличия этих ресурсов можно осуществлять копирование необходимых файлов на локальную систему (установку приложений), подключаться к принтерам и т. д.

При включении компьютера (при входе в домен) будут автоматически выполняться назначенные администратором сценарии. Это могут быть как обычный сценарий входа, так и групповые *политики*, выполняющие установку большого числа параметров системы.

Добавление Linux-систем в домен Windows

Примечание

Если в вашей информационной системе контроллерами домена являются серверы Windows 2008, то по умолчанию включен параметр использования строгих алгоритмов шифрования, которые несовместимы как с предыдущими версиями Windows, так и с клиентами Samba. Для разрешения такой ситуации необходимо выполнить рекомендации, изложенные в статье базы знаний KB942564. Открыть для редактирования групповую политику контроллеров домена (**Администрирование** | **Управление групповой политикой**, в панели навигации в левой части перейти **Лес** | **Домены** | ***имя_домена*** | **Domain Controller**, щелкнуть правой кнопкой мыши по вкладке **Default Domain Controllers Policy** и открыть пункт меню **Изменить**), найти вкладку **Конфигурация компьютера** | **Политики** | **Административные шаблоны** | **Система** | **Сетевой вход в систему**, в правой части окна найти параметр **Разрешить алгоритмы шифрования, совместимые с Windows NT 4.0** и установить его в значение **Включен**.

Если в вашей организации существует домен, который поддерживается сервером Windows, то в него можно добавить в качестве члена компьютер с операционной системой Linux. Это позволит использовать учетные записи домена для доступа к ресурсам Linux. Одновременно можно будет предоставить ресурсы Linux-системы для совместного доступа пользователям домена.

Существуют различные варианты включения Linux-системы в домен Windows. Поскольку наиболее современный способ аутентификации — использование Kerberos, то мы и опишем процедуры подключения в такой конфигурации.

Процедуры подключения имеют незначительные отличия для различных клонов Linux. Мы рассмотрим случай подключения к домену систем Ubuntu.

Для Ubuntu разработаны специализированные пакеты, которые предназначены для подключения к домену на основе службы каталогов. Установите пакет likewise-open командой

```
apt-get install likewise-open
```

Чтобы подключение выполнилось без проблем, следует проверить правильность настройки разрешения имен в Ubuntu. Проверьте, что вы можете разрешать доменные ресурсы по их полному имени (с помощью команды `nslookup`).

Подключение к домену производится командой `domainjoin-cli` с указанием полного имени домена (не NetBIOS-имени, а именно FDQN — Fully Qualified Domain Name):

```
domainjoin-cli join example.local имя_пользователя
```

При вводе данной команды система запросит пароль учетной записи *имя_пользователя*, которая должна иметь право подключения компьютеров в домен. Результатом работы команды должно быть сообщение:

```
SUCCESS
```

Процедура произведет все необходимые настройки файлов конфигурации, так что после получения этого сообщения вы можете заходить на сервер Ubuntu, используя доменные учетные записи.

> ***Примечание***
>
> Доменные учетные записи будут иметь права обычных пользователей Ubuntu. При необходимости иного варианта соответствия групп пользователей домена и Ubuntu требуемые корректировки следует выполнить вручную. Например, чтобы предоставить администраторам домена права суперпользователя Ubuntu, следует отредактировать конфигурацию `sudo` (командой `visudo`), добавив следующую строку: `%YOURDOMAINNAME\\domain^admins ALL=(ALL) ALL`.

Командой `domainjoin-cli` можно отключиться от домена, выполнить подключение к заданному подразделению (в этом случае компьютер будет помещен в соответствующую группу службы каталогов) и т. д. Подробности следует изучить по справке команды (`man domainjoin-cli`).

Есть еще несколько полезных утилит, которые устанавливаются вместе с пакетом Likewise. Это `lwinet` — возвращает информацию о домене и сетевом окружении и

`lwiinfo` — показывает информацию о различных параметрах домена. Например, команда

```
lwiinfo --dsgetdcname=mydomain.local
```

отобразит имя системы, несущей роль первичного контроллера домена mydomain.local.

Описанный вариант не является единственно возможным. Администраторы, предпочитающие контролировать все настройки подключения, легко найдут в Сети рекомендации по настройке Kerberos-клиента, по конфигурированию Samba, настройки параметров аутентификации и командам присоединения к домену. Обратите только внимание, какой способ подключения вы будете использовать: традиционный или по протоколу Kerberos.

Диагностика службы каталогов

Следствием неисправностей функционирования службы каталогов (Active Directory, AD) неизбежно являются отказы информационной системы. Поэтому в задачи системного администратора входит предупреждение отказов, своевременное их обнаружение и устранение в сжатые сроки.

Описываемые далее методы диагностики относятся, в первую очередь, к станциям на основе операционных систем Windows. Хотя утилиты, входящие в состав Windows Server, пригодны и для работы с соответствующими службами Linux-систем.

На работоспособность AD оказывают влияние как "собственные" службы, так и подсистемы, обеспечивающие функционирование сетевой инфраструктуры: службы динамического назначения параметров протокола и разрешения имен (DHCP, DNS, WINS), службы аутентификации пользователей (Net Logon, Kerberos), репликации данных (FRS), синхронизации времени, собственные службы AD: KDC (Key Distribution Center), KCC (Knowledge Consistency Checker), ISTG (Intersite Topology Generator), TRS (Time Reference Server) и т. д.

Поэтому работы по поиску неисправностей должны включать анализ всех компонентов системы, начиная от проверки кабельной структуры.

Обнаружение неисправностей AD

Системный администратор должен принять максимум усилий, чтобы обнаружить и правильно интерпретировать первые предвестники неисправности AD. В первую очередь, этому поможет анализ файлов протоколов систем. Особое внимание необходимо уделить событиям, перечисленным в табл. 6.1. Более подробную информацию можно получить по ссылке **http://go.microsoft.com/fwlink/?LinkId=122877**.

Примечание

К сожалению, появление записей об ошибках в протоколах событий, как правило, уже свидетельствует о наличии проблем. Конечно, можно включить расширенные возмож-

ности аудита, но в нормальных условиях эта настройка обычно не используется, поскольку снижает полезную производительность системы. Если администратор хочет своевременно обнаруживать проблемы функционирования AD и ликвидировать их еще до того момента, как они приведут к сбоям служб бизнес-структуры, следует задействовать любую систему мониторинга реального времени.

Таблица 6.1. *Перечень событий журнала, подлежащих анализу*

Источник	Номер события
FRS	13508, 13509, 13512, 13522, 13567, 13568
Netlogon	5774, 5775, 5781, 5783, 5805
NTDS	1083, 1265, 1388, 1645
UserEnv	1085
W32Time	13, 14, 52—56, 60—64

Следует также внимательно относиться ко всей информации, получаемой от пользователей. Например, известие о том, что система второй раз запросила смену пароля пользователя, может косвенно свидетельствовать о проблемах репликации двух контроллеров AD.

Средства тестирования AD

Для проверки функционирования службы каталогов подходят любые утилиты, которые взаимодействуют с AD.

В первую очередь это три стандартные консоли управления AD: пользователи и компьютеры, доверительные отношения и домены, сайты. Часть утилит входит в состав Resource Kit для сервера Windows 2003; этот пакет (отдельные утилиты) можно установить на актуальную версию сервера и использовать для проверки работы системы.

Упомянем несколько утилит для тестирования инфраструктуры (табл. 6.2).

Таблица 6.2. *Утилиты для тестирования инфраструктуры*

Утилита	Назначение
`wevtutil`	Позволяет получить информацию из различных журналов Windows, настроить параметры протоколирования
`Nslookup`	Получает информацию о DNS-записях
`nltest`	Встроенная утилита. Отображает состав домена, проверяет доверительные отношения, состояния secure channel и т. п. Должна запускаться с повышенными привилегиями
`logman`	Позволяет создавать и управлять сбором информации со счетчиков Windows
`gpresult`	Отображает результирующую политику для пользователя (компьютера)

Таблица 6.2 *(окончание)*

Утилита	Назначение
dcdiag	Диагностика контроллера домена. Должна запускаться с повышенными привилегиями. Утилита ориентирована на конечного пользователя, выполняет значительный объем тестирования и позволяет вывести подробную информацию о состоянии службы каталогов
auditpol	Отображает и управляет политиками аудита
Утилиты Windows Server 2003	
netdiag	Проверка сетевой инфраструктуры
netdom	Проверка и управление доверительными отношениями
ntfrsutl	Управление службой репликации файлов
dsastat	Анализ состояний AD на различных контроллерах
repadmin	Проверка репликации данных AD, возможность инициировать частичную или полную репликацию заданного контекста
replmon	Контроль репликации данных и запуск ручной репликации (графическая утилита)

СОВЕТ

Утилиты имеют много ключей для точной настройки проверки. Обязательно ознакомьтесь с их справочной документацией!

Порядок работы с утилитами достаточно прост. Необходимо выполнить ее и просмотреть отображаемые результаты. Если есть предупреждения (или ошибки), то следует поочередно устранить их и добиться отсутствия предупреждений при тестировании (листинг 6.4).

Листинг 6.4

```
>dcdiag

Диагностика сервера каталогов

Выполнение начальной настройки:
Выполняется попытка поиска основного сервера...
Основной сервер = WIN-21A2CYWEKM8
* Идентифицирован лес AD.
Сбор начальных данных завершен.
Выполнение обязательных начальных проверок

Сервер проверки: Default-First-Site-Name\WIN-21A2CYWEKM8
Запуск проверки: Connectivity
WIN-21A2CYWEKM8 — пройдена проверка Connectivity
```

```
Выполнение основных проверок

Сервер проверки: Default-First-Site-Name\WIN-21A2CYWEKM8
Запуск проверки: Advertising
WIN-21A2CYWEKM8 — пройдена проверка Advertising
Запуск проверки: DFSREvent
За последние 24 часа после предоставления SYSVOL в общий доступ
зафиксированы предупреждения или сообщения об ошибках. Сбои при
репликации SYSVOL могут стать причиной проблем групповой политики.
WIN-21A2CYWEKM8 — не пройдена проверка
DFSREvent
Запуск проверки: SysVolCheck
WIN-21A2CYWEKM8 — пройдена проверка SysVolCheck

<...блок сообщений удален...>

Выполнение проверок разделов на: test
Запуск проверки: CheckSDRefDom
... test — пройдена проверка CheckSDRefDom
Запуск проверки: CrossRefValidation
... test — пройдена проверка CrossRefValidation

Выполнение проверок предприятия на: test.local
Запуск проверки: LocatorCheck
... test.local — пройдена проверка LocatorCheck
Запуск проверки: Intersite
... test.local — пройдена проверка Intersite
```

В листинге 6.4 (часть сообщений опущена для краткости) присутствуют предупреждения (выделено полужирным). Администратор обязательно должен разобраться с причинами, их вызвавшими.

Можно также воспользоваться утилитами, позволяющими отображать необходимую структуру AD и менять параметры объектов (табл. 6.3).

Таблица 6.3. *Утилиты операционной системы для отображения структуры AD и изменения параметров объектов*

Утилита	Можно использовать для
ADSI Edit	Просмотра и редактирования объектов AD, установки списков доступа (Access Control Lists, ACLs)
ldp	Взаимодействия с AD по протоколу LDAP

Проверка разрешения имен

В оперативных случаях следует быть готовым выполнить простейшие проверки службы каталогов стандартными средствами операционной системы. Обычно дос-

таточно проконтролировать возможность разрешения имен с помощью утилит `ping` и `nslookup`. Следует проверить достижимость контроллера домена по его краткому (без доменного суффикса) и полному имени. Желательно проверить разрешение адресов служб AD. Соответствующая структура DNS создается автоматически, и обычно достаточно проконтролировать ее наличие в оснастке управления сервером DNS. Если такая возможность отсутствует, то нужно вручную, с помощью `nslookup`, выполнить попытку разрешения имен, перечисленных в табл. 6.4.

Таблица 6.4. *Перечень имен, проверяемых в процессе теста*

Имя	Тип записи	Соответствие
_ldap._tcp.dc._msdcs.<*DNS_имя_домена*>	SRV	Контроллер домена
_ldap._tcp.pdc._msdcs.<*DNS_имя_домена*>	SRV	Эмулятор первичного контроллера
_ldap._tcp.gc._msdcs.<*DNS_имя_леса*>	SRV	Сервер глобального каталога
_kerberos._tcp.dc._msdcs.<*DNS_имя_домена*>	SRV	Расположение службы Kdc

Примечание

Для разрешения имен служб (записи типа SRV) следует в `nslookup` предварительно выполнить команду `set type=all` или `set type=srv`. Обратите также внимание, что в операции разрешения имени сервера глобального каталога указывается имя леса, а не домена. Обычно в малых организациях эти имена совпадают.

Обратите внимание на весьма простую операцию, удачное выполнение которой зависит от правильности настройки системы разрешения имен и от функционирования контроллера домена. Попробуйте открыть следующий сетевой ресурс: \\<*DNS_имя_домена*>\SYSVOL. Если попытка неудачна, то либо в организации неверно настроено разрешение имен, либо контроллер домена неработоспособен.

Снимки службы каталогов

В Windows 2008 появилась возможность создания снимков *(snapshot)* службы каталогов. Снимки позволяют сохранить текущее состояние параметров службы каталогов и сравнить его впоследствии с актуальными значениями. Это может помочь восстановить ошибочно измененные данные, провести анализ изменений в службе каталогов и т. п.

Использование снимков подразумевает выполнение нескольких операций.

Во-первых, нужно просто создать снимок на заданный момент времени. При необходимости эту операцию можно настроить на выполнение по расписанию, что позволит иметь копии данных службы каталогов на заданный диапазон дат.

Во-вторых, для того чтобы получить доступ к сохраненным таким способом данным, нужно *смонтировать* снимок и предоставить к нему доступ по протоколам LDAP.

В завершение работ следует размонтировать снимок и удалить более ненужные данные.

Создание снимков службы каталогов

Создать снимки можно на компьютере, на котором установлена служба каталогов. Выполнить эту операцию могут пользователи с правами администраторов домена (предприятия).

Для создания снимка нужно открыть окно командной строки с правами администратора, набрать `ntdsutil` и нажать клавишу <Enter>. На экране появится приглашение утилиты `ntdsutil`. Вам необходимо последовательно набрать следующие команды:

```
activate instance ntds
snapshot
create
```

В итоге этих шагов в окне должно появиться сообщение (номер снимка у вас будет другим):

Успешно создан набор снимков {2f9a5a87-f2f8-4511-8de7-ea1466c8a684}.

Чтобы вывести на экран перечень всех созданных в системе снимков, следует выполнить команду

```
list all
```

Для выхода из окна `ntdsutil` последовательно выполните две команды `quit`. После чего закройте окно командной строки.

> ***Примечание***
>
> `Ntdsutil` позволяет выполнить указанные операции за один шаг, если перечислить набранные команды в качестве параметров. В нашем случае для создания снимка можно было выполнить в окне командной строки следующую команду: `ntdsutil "Activate Instance NTDS" snapshot create quit quit` (команды с пробелами должны быть заключены в кавычки).

Монтирование снимков службы каталогов

Монтирование службы каталогов также осуществляется при помощи утилиты `ntdsutil`. Для выполнения этой операции нужны права администратора домена (предприятия).

Войдите в окно `ntdsutil`, запустив командную строку с правами администратора. Выведите на экран список всех снимков (командой `list all`) — рис. 6.4.

Информация о существующих снимках будет отображаться парами строк. При дальнейших операциях при выборе снимка можно указывать значения номера как для первой, так и второй строки.

Для подключения снимка выполните команду `mount` с указанием номера нужного снимка. После сообщения об удачном подключении снимка можно выйти из утилиты `ntdsutil`.

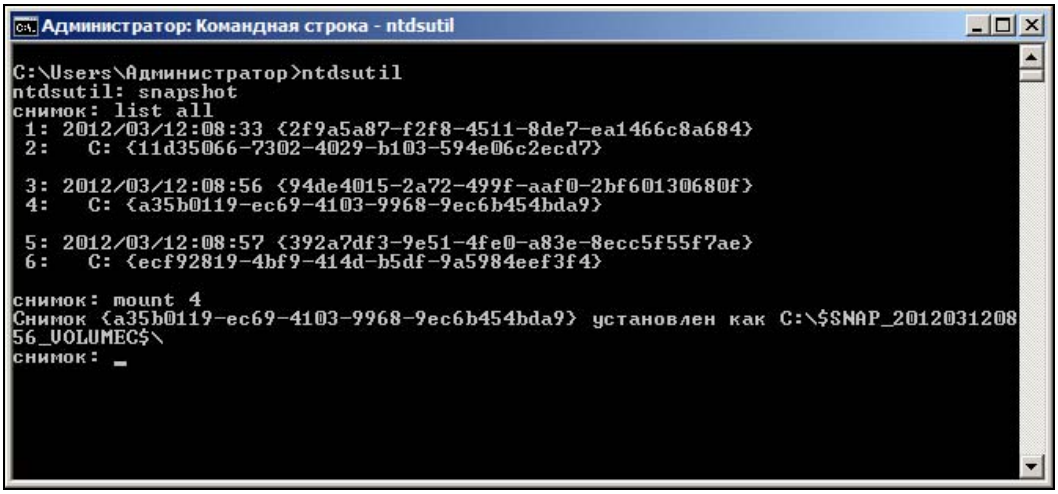


Рис. 6.4. Вывод списка снимков службы каталогов

Публикация данных снимков

После монтирования снимка его необходимо опубликовать. Делается это при помощи утилиты `dsamain` — браузера автономных данных AD/DS/LDS. Эта утилита доступна в операционной системе с установленной службой каталогов.

При ее использовании необходимо учесть следующее. Во-первых, данные снимков предоставляются в режиме "только для чтения". При необходимости внесения изменений файл NTDS.dit должен быть перенесен на носитель, допускающий запись. Во-вторых, утилита сохраняет права доступа к данным службы каталогов, поэтому если администраторы не имеют доступа к некоторой части параметров для их чтения, то они не смогут их увидеть.

При запуске утилиты нужно указать полный путь к файлу ntds.dit (включая название самого файла) и значения четырех портов, по которым будут доступны данные — LDAP, LDAP/SSL, GC, GC/SSL. Обычно достаточно указать только номер порта для LDAP, далее порты будут назначены последовательно на единицу больше. При успешном запуске браузер сообщит о монтировании снимка:

```
>dsamain -dbpath "C:/$SNAP_201203120856_VOLUMEC$/Windows/NTDS/ntds.dit"
-ldapPort 10400
EVENTLOG (Informational): NTDS General / Управление службой: 1000
Завершен запуск доменных служб Active Directory (Майкрософт)
версии 6.1.7601.175 14
```

> ***Примечание***
>
> Окно утилиты необходимо оставить открытым до завершения операций со снимками.

После такой публикации снимка доступ к данным осуществляется с помощью любой утилиты, предназначенной для работы со службой каталогов по протоколам

LDAP, например, ldp.exe, adsi edit, ldifde/csvde, JXplorer и аналогичным. В том числе и с помощью стандартной оснастки работы со службами каталогов (хотя эти оснастки предоставляют только частичную выборку значений снимка, а не все параметры, доступные по протоколам LDAP). Для этого откройте, например, оснастку Active Directory **Пользователи и компьютеры**. Щелкните правой кнопкой мыши по верхней строчке в левой части окна и выберите команду **Сменить контроллер домена**. В качестве контроллера домена укажите имя компьютера, на котором опубликован снимок, и номер порта, указанного в параметрах `dsamain` (рис. 6.5).

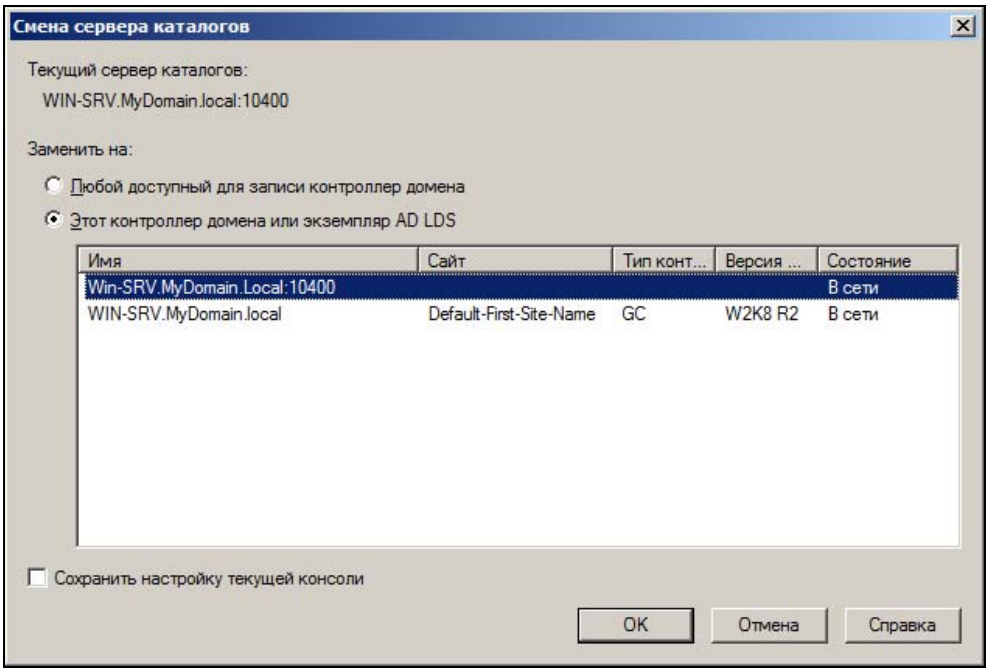


Рис. 6.5. Подключение к серверу каталогов

Если вы попытаетесь открыть в этой оснастке любой объект, то заметите, что все опции настройки недоступны — используется режим "только для чтения".

По завершении работы со снимком следует отключить его публикацию, для чего нажать в окне утилиты `dsamain` клавиши <Ctrl>+<C>.

Удаление снимков

Удаление снимков производится в утилите `ntdsutil`. Необходимо открыть ее с правами администратора, перечислить снимки (`list all`), а затем размонтировать активный снимок (`unmount` *номер*).

После этого для удаления снимка следует выполнить команду `delete` *номер*.

Службы Active Directory облегченного доступа к каталогам

Службы Active Directory облегченного доступа к каталогам (прежнее название Active Directory Application Mode, ADAM) предназначены для использования возможностей службы каталогов прикладными приложениями. Фактически данная служба предоставляет собой копию службы каталогов, но не привязанную к домену. Программисты могут размещать на ней данные для своих приложений, которые требуют централизованного хранения, репликации, контроля доступа и т. п. В результате для прикладных программ появляется возможность использования таких функций без влияния (взаимодействия) со службой каталогов домена, что облегчает настройки приложений, поиск и исправление ошибок и т. д.

Параметры Службы Active Directory облегченного доступа к каталогам должны быть настроены соответствующими программистами. Для администрирования службы используются традиционные утилиты работы с AD, кроме того, имеется утилита Adamsync, предназначенная для синхронизации данных службы каталогов с данными службы облегченного доступа. Особенности ее применения описаны в статье **http://technet.microsoft.com/ru-ru/library/cc770408.aspx**.

Контроллер домена только для чтения

Многие компании территориально размещены по нескольким офисам, будь то это в одном городе или в нескольких регионах. Стабильная работа в филиалах — в случае единого централизованного IT-управления — требует постоянного соединения с центральным офисом, что не всегда реально достижимо. Одним из способов организации работы при нестабильном канале связи является размещение в филиале дополнительного контроллера домена. Однако в филиале гораздо сложнее обеспечить необходимый уровень безопасности сервера, а при наличии физического доступа к системе злоумышленнику не представляет особого труда скомпрометировать ее. С выходом ОС Windows Server 2008 появилась возможность установки контроллера домена "только для чтения" — RODC (Read-Only Domain Controller). RODC в некоторой степени можно рассматривать как расширение функционала Backup Domain Controller — контроллеров в домене Windows NT 4.0, на которые также нельзя было вносить изменения.

RODC имеет несколько особенностей.

- **Односторонняя репликация.** Данные копируются на RODC с других контроллеров. Если программа пытается внести изменения в базу, хранящуюся на RODC, то операция записи будет транслироваться на "обычные" контроллеры и выполняться там.
- **Ограниченный набор атрибутов.** На RDOC кэшируется только часть атрибутов каталога. Настройками на контроллере-хозяине схемы администратор может изменить состав этих атрибутов, но часть их помечена как критические, и их

нельзя реплицировать на RODC. На RODC можно установить сервер DNS в режиме "только для чтения".

- **Возможность хранения данных аутентификации.** Администратор может настроить список учетных записей, для которых данные аутентификации будут храниться (кэшироваться) на RODC. Эти пользователи смогут входить в домен и выполнять другие действия даже в случае отсутствия соединения с центральным офисом. В случае же компрометации RDOC администратор будет знать, к каким учетным записям злоумышленник мог получить доступ, и сможет принять необходимые меры.
- **Делегирование прав локального администратора.** На "обычных" контроллерах домена локальный администратор является администратором домена. Для выполнения задач обслуживания RODC (установка драйверов и аналогичные операции, требующие наличия прав администратора) предусмотрено, что любая учетная запись, включенная в группу локальных администраторов, будет обладать правами локального администратора, но не получит никаких прав по управлению доменом.

> ***Примечание***
>
> В случае взлома RODC злоумышленник может настроить репликацию на него дополнительных атрибутов службы каталогов, которые не копируются в филиал в нормальных условиях по соображениям безопасности. При взаимодействии с контроллером на Windows 2008 последний откажет в операции копирования. Если связь будет установлена с контроллером на Windows Server 2003, то *данные будут скопированы*. Поэтому в целях безопасности необходимо устанавливать RODC в домене, режим которого переведен на уровень Windows 2008.

Установка RODC не представляет никакой сложности. Администратору необходимо начать установку контроллера домена (`dcpromo` или из консоли управления). Далее на соответствующем шаге мастера указать, что необходимо установить контроллер в режиме "только для чтения", а затем выбрать политику репликации паролей учетных записей. Обычно достаточно согласиться с предложением мастера операций: настройки по умолчанию подходят в большинстве случаев.

Отметим также, что RODC может быть установлен как на полную версию сервера Windows 2008, так и на вариант Core. При использовании RODC не требуется вносить никаких изменений на клиентские станции.

Особенности установки RODC

RODC не требует перевода домена (а также и леса) в режим 2008-го сервера, достаточно функционального уровня Windows Server 2003. Но для установки соответствующих прав доступа ко всем DNS-разделам необходимо обновить схему, выполнив для леса команду

```
adprep /rodcprep
```

Односторонняя репликация RODC реализуется только для AD DS и папки SYSVOL распределенной файловой системы (DFS). "Входящие" изменения выполняются на

RODC обычным способом, причем RODC также осуществляет автоматическую балансировку входящих подключений, как и полноценные контроллеры домена.

Примечание

Обратите внимание, что другие совместно используемые ресурсы DFS реплицируются в обе стороны.

Особенности кэширования учетных данных

По умолчанию RODC не кэширует никаких данных, кроме параметров учетной записи самого компьютера RODC и специальной учетной записи krbtgt (соответствующие учетные записи имеются на всех контроллерах домена).

Чтобы обеспечить возможность входа в домен при отсутствии подключения к центральному офису, необходимо вручную настроить кэширование учетных записей. В этом случае *после первого обращения* на аутентификацию учетной записи RODC запрашивает на "основных" контроллерах домена данные пользователя и, в случае настройки кэширования, сохраняет их локально. После этого новый вход учетной записи в домен может быть выполнен без наличия подключения к центральному офису.

Для настройки кэширования паролей следует открыть свойства RODC, на вкладке **Политика репликации паролей** нажать кнопку **Дополнительно** и добавить необходимые учетные записи (рис. 6.6).

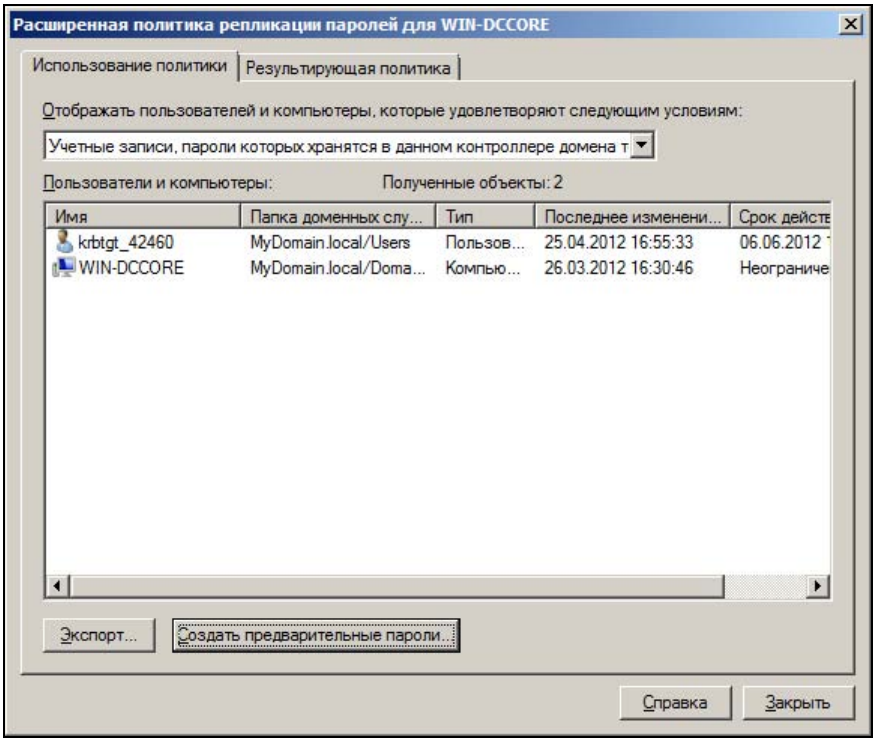


Рис. 6.6. Добавление учетных записей для кэширования паролей на RODC

Примечание

Обратите внимание, что для успешного входа в домен с рабочей станции Windows на RODC должны кэшироваться не только учетные записи пользователей, но и соответствующих компьютеров, являющихся членами домена.

Настройка предварительных паролей

Как уже описывалось ранее, кэш параметров учетной записи по умолчанию создается после первой попытки входа в домен. Если необходимо обеспечить возможность входа учетной записи в домен при отсутствии подключения к центральному офису, то следует вручную настроить предварительное кэширование.

Для этого в форме **Расширенная репликация паролей...** (см. рис. 6.6) нужно нажать кнопку **Создать предварительные пароли**, выбрать необходимые учетные записи и подтвердить свое намерение.

Коррекция состава учетных записей кэширования на RODC

В процессе работ состав пользователей меняется, и администратор не всегда может проконтролировать местонахождения пользователя и настроить ему кэширование паролей в случае перемещения рабочего места в филиал.

Для облегчения рутинных операций администратор может проанализировать список учетных записей, которые пытались аутентифицироваться на RODC и добавить их в настройки кэширования. Откройте форму **Расширенная репликация паролей...** (см. рис. 6.6), как было описано ранее в этой главе, и смените в раскрывающемся списке выбора строку на **Учетные записи, прошедшие проверку подлинности для данного контроллера**.

Можно добавить настройки кэширования индивидуально, а можно и установить разрешение кэширования для всех перечисленных учетных записей. Для этого следует воспользоваться командой

```
repadmin /prp move
```

(Подробности использования команды описаны на странице синтаксиса **http://go.microsoft.com/fwlink/?LinkId=112118**.)

Сброс паролей кэшированных учетных записей RODC

Если RODC дискредитирован (например, украден или есть подозрение, что к нему имел доступ злоумышленник), то необходимо в кратчайшие сроки заменить пароли тех учетных записей, которые были настроены на нем для кэширования.

Для этого необходимо на полнофункциональном контроллере домена выделить данный RODC и выполнить операцию **Удалить**. После подтверждения удаления на экране появится предложение о блокировании соответствующих учетных записей и об экспорте их списка (рис. 6.7).

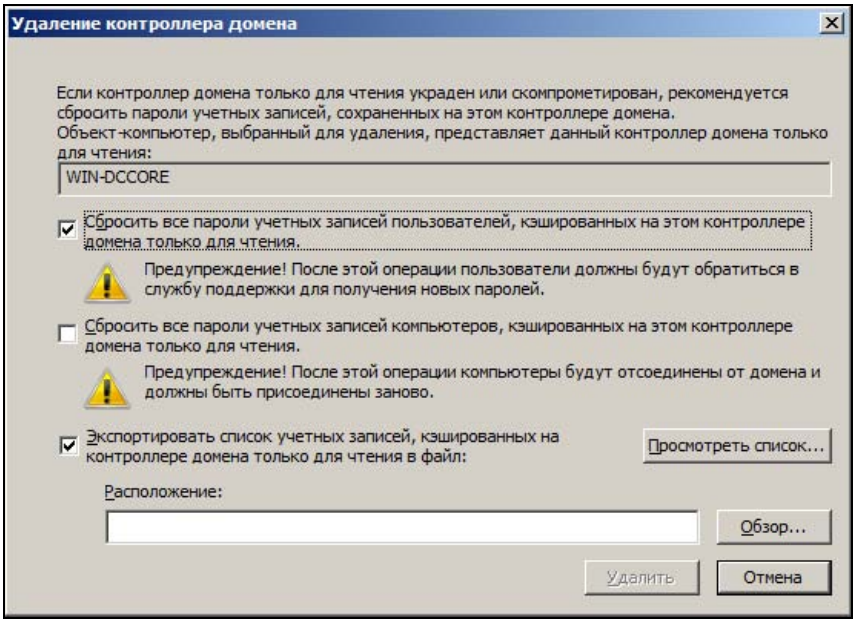


Рис. 6.7. Удаление контроллера домена "только для чтения"

Известные проблемы использования RODC

Если в филиале настроены RODC, то известны некоторые проблемы их использования.

- **Ошибки регистрации Service Principle Names (SPNs).** Если приложение регистрирует в домене специальный идентификатор — SPN, то учетная запись соответствующей службы также должна быть настроена на локальное кэширование. Без такого кэширования, даже при наличии подключения к домену, будут возникать ошибки регистрации приложений.
- **Ошибки регистрации при работе контроллера Windows Server 2003 с записями служб DNS.** Если основной контроллер домена установлен на Windows Server 2003 и на нем зарегистрированы записи служб DNS (записи DNS SRV) для филиала с RODC, то клиенты такого филиала не будут аутентифицироваться на RODC. Для исправления ситуации необходимо либо обновить контроллер до версии Windows 2008, либо установить пакет совместимости (**http://go.microsoft.com/fwlink/?LinkID=122974**).
- **Невозможность использования аппаратных средств аутентификации в филиале.** По умолчанию RODC не получают автоматически сертификаты, которые нужны для аутентификации учетных записей с использованием смарт-карт и аналогичных технологий. Для исправления ситуации нужно изменить в шаблоне сертификатов контроллеров домена право **Enroll** и добавить в него группу **ERODC**. Также эта группа должна быть добавлена в шаблон Domain Controller Authentication and Directory E-Mail Replication.

- **Проблемы с эталонным временем.** RODC при установке в существующий лес Windows Server 2003 не может выступать в качестве эталона времени. Для исправления необходимо установить сервер Windows 2008 и мигрировать на него роль PDC домена.
- **Ограниченность кэшированных атрибутов.** На RODC копируется не полный состав всех атрибутов объектов службы каталогов. Если приложениям, эксплуатируемым в филиале, эти атрибуты необходимы, то следует выполнить точную настройку политики репликации. Подробности операций описаны в технической документации вендора.

ГЛАВА 7

Управление учетными записями

Обеспечение безопасности информационной системы существенно зависит от того, какие права предоставлены учетным записям и процессам, как настроен доступ на уровне файловой системы, какие ограничения введены в системе.

Понятие учетной записи

Программа, которая выполняется на компьютере, всегда запущена от имени какого-либо пользователя и обладает данными ему правами. Если вы начали работу на компьютере, введя свое имя и пароль, то любая начатая вами задача: графический редактор или почтовый клиент, дефрагментация диска или установка новой игры — будет выполняться от этого имени. Если запущенная программа вызывает в свою очередь новую задачу, то она также будет выполняться в контексте вашего имени. Даже программы, являющиеся частью операционной системы, например служба, обеспечивающая печать на принтер, или сама программа, которая запрашивает имя и пароль у пользователя, желающего начать работу на компьютере, выполняются от имени определенной учетной записи (например, **Система** в Windows). И так же, как программы, запускаемые обычным пользователем, эти службы имеют права и ограничения, которые накладываются используемой учетной записью.

Операционная система "различает" пользователей не по их имени (полному или сокращенному), а по специальному уникальному номеру (идентификатору безопасности — Security Identifier (SID)), который формируется в момент создания новой учетной записи.

Примечание

Существуют многочисленные утилиты, которые позволяют по имени входа пользователя определить его SID и наоборот. Например, `getsid`. В статье KB276208 базы знаний Microsoft приведен код на Visual Basic, который позволяет выполнить запросы SID/имя в обычном сценарии. Код хорошо комментирован и легко может быть применен без поиска специализированных утилит. Можно также установить на компьютер утилиты Account Lockout and Management Tools (см. рис. 7.1), добавляющие к оснастке управления пользователями в домене еще одну вкладку свойств, на которой в том числе отображается и SID пользователя.

Поэтому учетные записи можно легко переименовывать, менять любые иные их параметры. Для операционной системы после этих манипуляций ничего не изменится, поскольку такие операции не затрагивают идентификатор пользователя.

> ***Примечание***
>
> При создании новой учетной записи обычно определяются только имя пользователя и его пароль. Но учетным записям пользователей — особенно при работе в компьютерных сетях — можно сопоставить большое количество различных дополнительных параметров: сокращенное и полное имя, номера служебного и домашнего телефонов, адрес электронной почты и право удаленного подключения к системе и т. п. Такие параметры являются дополнительными, их определение и использование на практике зависит от особенностей построения конкретной компьютерной сети. Эти параметры могут быть использованы программным обеспечением, например, для поиска определенных групп пользователей (например, *группы по запросу*).

Стандартные учетные записи в Windows имеют отличающиеся названия для различных локализаций операционной системы, но идентичные SID (перечень Well Known Security Identifiers приведен, например, в документе KB243330). Например, `S-1-5-18` — это SID учетной записи **Local System**; `S-1-5-19` — учетной записи **NT Authority\Local Service**; SID `S-1-5-20` "принадлежит" учетной записи **NT Authority\Network Service** и т. д. Учетные записи пользователя домена "построены" по такой же структуре, но обычно еще более "нечитаемы". Вот пример реального доменного SID:

```
S-1-5-21-61356107-1110077972-1376457959-10462
```

В Linux учетные записи обычно имеют следующие идентификаторы: суперпользователь (root) — идентификатор 0, локальные пользователи нумеруются с 1000 и далее, для доменных учетных записей выбирается диапазон от 10 000 и далее.

После установки пакета Account Lockout and Management Tools в свойствах учетной записи отображается вкладка, на которой администратор может увидеть различные параметры: идентификатор безопасности, уникальный идентификатор, время входа, количество неудачных попыток входа в систему (**Bad Password Count**) и т. д. (рис. 7.1).

Подобные характеристики можно получить и выполнив непосредственный запрос к службе каталогов. Например, для получения значения числа неудачных попыток входа в качестве фильтра запроса к службе каталогов можно указать следующую строку:

```
(&(objectclass=user)(!(objectclass =computer))(!(badPwdCount=0))
(badPwdCount=*))
```

Если при изменении имени входа пользователя в систему ничего "существенного" для системы не происходит — пользователь для нее не изменился, то операцию удаления учетной записи и последующего создания пользователя точно с таким же именем входа операционная система будет оценивать как появление *нового* пользователя. Алгоритм формирования идентификатора безопасности пользователя таков, что практически исключается создание двух учетных записей с одинаковым номером. В результате новый пользователь не сможет, например, получить доступ

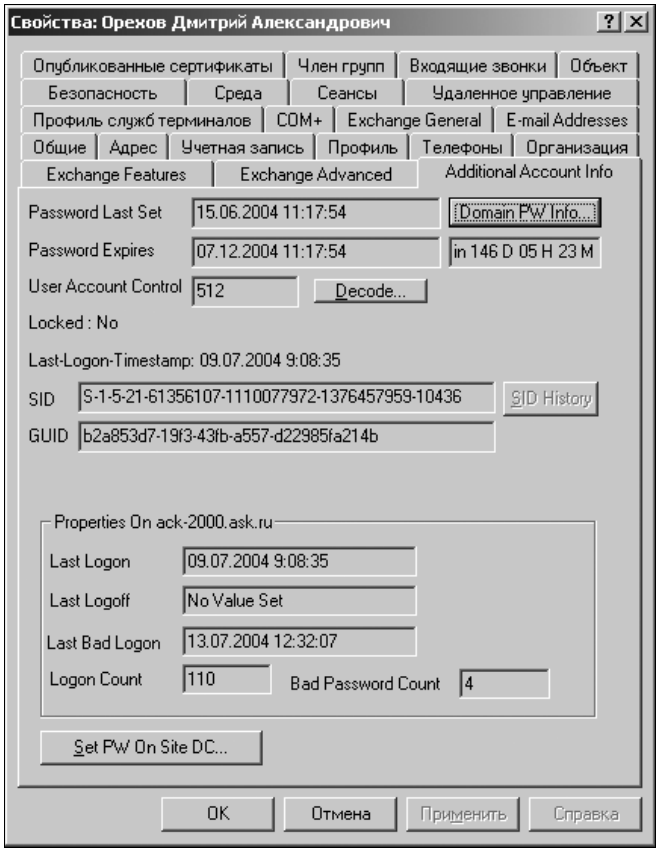


Рис. 7.1. Дополнительные параметры учетной записи

к почтовому ящику, которым пользовался удаленный сотрудник с таким же именем, и не прочтет зашифрованные им файлы и т. п.

Локальные и доменные учетные записи

При работе в компьютерной сети существуют два типа учетных записей. *Локальные учетные записи* создаются на данном компьютере. Информация о них хранится локально (в локальной базе безопасности компьютера) и локально же выполняется аутентификация такой учетной записи (пользователя).

Доменные учетные записи создаются на контроллерах домена. И именно контроллеры домена проверяют параметры входа такого пользователя в систему.

Чтобы пользователи домена могли иметь доступ к ресурсам локальной системы, при включении компьютера в состав домена Windows производится добавление группы пользователей домена в группу локальных пользователей, а группы администраторов домена — в группу локальных администраторов компьютера. Таким образом, пользователь, аутентифицированный контроллером домена, приобретает права пользователя локального компьютера. А администратор домена получает права локального администратора.

Необходимо четко понимать, что одноименные учетные записи различных компьютеров — это *совершенно различные пользователи*. Например, учетная запись, созданная на локальном компьютере с именем входа `Иванов`, и доменная учетная запись `Иванов` — это два пользователя. И если установить, что файл доступен для чтения "локальному Иванову", то "доменный Иванов" не сможет получить к нему доступ. Точнее, доменный Иванов сможет прочесть файл, если его пароль *совпадает* с паролем локального Иванова. Поэтому если на компьютерах одноранговой сети завести одноименных пользователей с одинаковыми паролями, то они смогут получить доступ к совместно используемым ресурсам автономных систем. Но после изменения одного из паролей такой доступ прекратится.

Создание и удаление учетных записей

Операции создания и удаления учетных записей наиболее часто выполняются администраторами информационной системы.

Создание учетных записей в Windows

После установки Windows вы начинаете работу с правами учетной записи **Администратор** (Administrator — для интернациональных версий ОС). Пользователь **Администратор** обладает максимальными правами в данной операционной системе; используя права администратора, можно создавать, модифицировать, удалять другие учетные записи, выполнять любые операции по настройке системы и т. п.

Целесообразно назначить этой учетной записи длинный и сложный пароль, состоящий из цифр и символов только английского алфавита. Это упростит возможные операции по восстановлению операционной системы. Кроме того, в целях безопасности рекомендуется переименовать учетные записи администраторов (сделать это в домене можно централизованно, используя групповую политику) и запретить для анонимных пользователей просмотр базы идентификаторов безопасности.

Для управления учетными записями используются специальные оснастки: управление компьютером в локальном случае (рис. 7.2) и оснастка управления AD **Пользователи и компьютеры** при создании доменных пользователей.

Процедура создания новой учетной записи очевидна. Объем заполняемых необязательных полей определяется сложившейся практикой в организации. Единственное, на что следует обратить внимание, что при создании новых пользователей домена рекомендуется устанавливать для них требование смены пароля при первом входе в сеть. Администратор домена не должен знать пароль пользователя.

Управлять учетной записью можно из командной строки. Так, добавить пользователя можно командой `NET USER <имя> <пароль> /ADD`, а удалить — `NET USER <имя> /DELETE`.

> ***Примечание***
>
> В домене Windows учетные записи создаются и для компьютеров с операционными системами Windows 200*x*/Windows XP/Windows 7. Эти учетные записи можно использовать для контроля доступа к сетевым ресурсам.

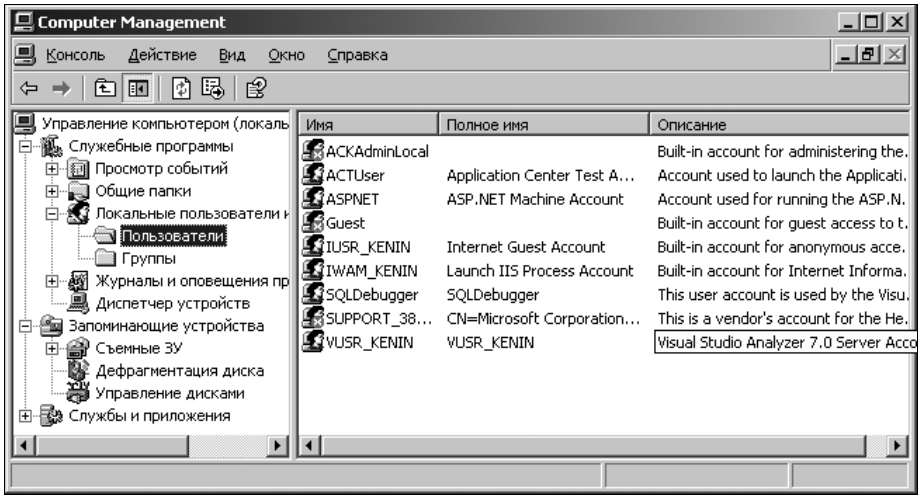


Рис. 7.2. Добавление нового пользователя локальной системы

Если в организации используются дополнительные параметры учетной записи (название отдела, адрес и т. п.), то удобнее при создании нового пользователя перенести в его учетную запись максимум настроек, которые имеют аналогичные пользователи. Для этих целей можно воспользоваться операцией *копирования учетной записи*. При копировании программа создает новую учетную запись, в настройки которой будут перенесены те параметры, которые не являются личными характеристиками. Например, новая учетная запись будет уже включена в те группы, в которые входила исходная учетная запись, но такой параметр, как номер телефона (который также может являться одной из характеристик пользователя), скопирован не будет.

Для того чтобы узнать SID учетной записи, членство ее в группах безопасности и привилегии, можно воспользоваться встроенной командой Windows 7/Server 2008 — `whoami`:

```
whoami /all
```

Создание учетных записей в Linux

Основная команда для создания учетных записей пользователей в Linux — это `useradd`. Будучи выполненной без указания параметров (только с параметром имени новой учетной записи — `useradd newuser`) эта команда создает новую учетную запись с параметрами по умолчанию. А именно[1]. Для пользователя создается новая группа (имя группы совпадает с именем новой учетной записи), членом которой становится новая учетная запись пользователя. Домашняя папка пользователя создается в папке /home с названием, совпадающим с именем учетной записи, структурой, копируемой из /etc/skel, и оболочкой sh. Для пользователя устанавливается

[1] Параметры приведены для случая Ubuntu.

бессрочный пароль и не создается почтовая структура. Все эти параметры по умолчанию можно увидеть, если запустить команду с ключом `-D`:

```
useradd -D
```

> ***Примечание***
>
> Поскольку наиболее частой модификацией является включение пользователя в группу по умолчанию, то такой вариант достижим использованием ключа `-n`. В этом случае пользователь будет включен в группу с ID 100.

Далее, чтобы с вновь созданной учетной записью можно было работать, нужно назначить ей пароль:

```
passwd newuser
```

Параметры по умолчанию можно изменить, если запустить команду `useradd` с ключом `-D` и указанием соответствующего ключа. Например, для изменения используемой оболочки:

```
useradd -D --shell=<SHELLNAME>
```

Можно включать в качестве параметров при вызове `useradd` все необходимые значения, но запоминать все нужные ключи не всегда удобно. В Debian (а Ubuntu создано на основе этого клона Linux) существует команда `adduser`, которая позволяет создать учетную запись пользователя интерактивно: система будет запрашивать вас о каждом параметре, предлагая значение по умолчанию.

В случае создания большого количества учетных записей можно воспользоваться командой `newusers`. Она создает учетные записи на основе списка из файла. Этот список должен быть подготовлен в следующем формате:

```
loginname:password:uid:gid:comment:home_dir:shell
```

Регулирование членства в группах в Linux

Каждый пользователь состоит в какой-либо группе. Ее можно указать как при создании пользователя, так и изменить с помощью команды `usermod`:

```
useradd -G admins, ftp, www, nagios <login>
```

Для того чтобы узнать, каким группам принадлежит учетная запись, следует выполнить

```
groups <учетная_запись>
```

Если команда набрана без имени учетной записи, то на экране появится информация по вашей учетной записи.

Иногда необходимо добавить пользователя в существующую группу. Для этого можно воспользоваться следующей командой:

```
usermod -a -G group пользователь
```

Эта команда добавит учетную запись *пользователь* в группу *group*.

Для удобства работы наиболее часто используемые команды для работы с учетными записями пользователей Linux сведены в табл. 7.1.

Таблица 7.1. *Основные команды управления учетными записями Linux*

Команда	Назначение
`id`	Отображает идентификатор пользователя и групп, в которые он входит
`whoami`	Отображает информацию по текущему пользователю
`useradd`	Создание новой учетной записи или настройка параметров по умолчанию
`adduser`	Интерактивная команда создания учетной записи пользователя и настройки ее параметров
`usermod`	Редактирование параметров учетной записи пользователя
`userdel`	Удаление учетной записи пользователя и его домашней папки
`deluser`	По умолчанию команда удаляет учетную запись пользователя, но сохраняет его домашнюю папку, почтовые файлы и т. д.
`groupadd`	Создание новой группы
`groupmod`	Редактирование параметров существующей группы
`groupdel`	Удаление группы
`groups`	Отображает на экране список групп, в которых состоит учетная запись пользователя
`passwd`	Смена (назначение) пароля учетной записи
`cat /etc/passwd`	Фактически данная команда отобразит на экране список учетных записей, созданных в локальной системе (вместе с идентификаторами групп, названиями используемых командных оболочек и т. д.)

Автоматически создаваемые учетные записи

При установке операционной системы автоматически создается несколько учетных записей пользователей. Например, в Windows учетная запись **Администратор**. Эта особая учетная запись. Ранее ее нельзя[1] было даже удалить или исключить из группы администраторов. Сделано это было из соображений безопасности, чтобы пользователь случайно не удалил всех администраторов и система не стала неуправляемой.

В Linux учетная запись суперпользователя носит имя root. В процессе установки системы создается также несколько служебных учетных записей, используемых для запуска отдельных служб (демонов).

В Windows 7 учетная запись **Администратор** как бы разделилась на две: одна учетная запись соответствует той, с которой вы входите в систему, другая — учет-

[1] В версиях, более ранних чем Windows XP. В новых версиях Windows упомянутые операции допустимы.

ная запись, которая используется, если вызывается команда **Запустить от имени администратора**. С этим связаны некоторые ошибки, когда пользователи не могут понять, почему не выполняется сценарий, исполняемый от имени **Администратора**. А потому, что фактически учетных записей две и права у них отличаются.

Другая автоматически создаваемая учетная запись — это **Гость** (Guest). Она не имеет пароля и предназначена для обеспечения возможности работы с данным компьютером пользователя, у которого в системе нет учетной записи. К примеру, вы приезжаете со своим ноутбуком в другую организацию и хотите распечатать документ. Если в той организации принтер предоставлен в совместное использование и действует учетная запись **Гость**, вы можете подключиться к принтеру и выполнить печать, в противном случае вам должны сообщить имя входа и пароль, которые можно использовать для подключения к серверу печати.

Учетная запись **Гость** по соображениям безопасности заблокирована. Однако если ваша сеть полностью автономна и объединяет немного компьютеров, то для облегчения использования сетевых ресурсов вы можете ее разблокировать.

Так делает, например, мастер конфигурирования домашней сети: если вы определили, что компьютер используется в рамках домашней сети, то мастер разрешает использование учетной записи **Гость**. В этом случае, если вы разрешите совместное использование ресурсов компьютера, то к ним будет возможно подключение любых пользователей, независимо от того, существуют ли для них учетные записи на вашем компьютере или нет.

Учетная запись **HelpAssisstant** применяется в случаях обращения к удаленному помощнику. Удаленный пользователь подключается к компьютеру с правами, предоставленными данной учетной записи.

Учетная запись **SUPPORT_*номер*** используется службами технической поддержки Microsoft. Обычно рекомендуют просто удалить эту учетную запись.

Если на компьютере устанавливается информационный сервер Интернета (Internet Information Server, IIS), то создаются две учетные записи. Это **IUSR_*имя_компьютера*** и **IWAM_*имя_компьютера***. Учетная запись **IUSR_*имя_компьютера*** применяется при предоставлении веб-ресурсов анонимному пользователю. Иными словами, если информационный сервер Интернета не использует аутентификацию пользователя (предоставляет ресурсы анонимно), то в системе такой пользователь регистрируется под именем **IUSR_*имя_компьютера***. Вы можете, например, запретить анонимный доступ к каким-либо ресурсам информационного сервера, если исключите чтение таких файлов данным пользователем. Пароль пользователя **IUSR_*имя_компьютера*** создается автоматически и синхронизируется между операционной системой и информационным сервером.

Пароли учетных записей **IUSR_*имя_компьютера*** и **IWAM_*имя_компьютера*** легко можно узнать при помощи сценария, имеющегося на компьютере. Найдите файл Adsutil.vbs (обычно он расположен в папке административных сценариев IIS, например, InetPub\AdminScripts), замените в текстовом редакторе строку сценария (иначе сценарий покажет пароль в виде звездочек)

```
IsSecureProperty = True
```

на

```
IsSecureProperty = False
```

и выполните:

```
cscript.exe adsutil.vbs get w3svc/anonymoususerpass
```

для отображения пароля IUSR-пользователя или

```
cscript.exe adsutil.vbs get w3svc/wamuserpass
```

для показа пароля IWAM-пользователя.

Учетная запись **IWAM_*имя_компьютера*** используется для запуска процессов информационного сервера (например, для обработки сценариев на страницах с активным содержанием). Если вы случайно удалите какую-либо из этих записей и вновь создадите одноименную, то, скорее всего, столкнетесь с неработоспособностью информационного сервера. Конечно, можно обратиться к справочной базе разработчика, правильно настроить службы компонентов на использование новой учетной записи, синхронизовать с помощью специальных сценариев пароли учетных записей и т. п. Но гораздо эффективнее в этой ситуации будет просто удалить службу информационного сервера и вновь добавить этот компонент, предоставив программе установки выполнить все эти операции.

Кроме перечисленных учетных записей новые пользователи системы часто создаются прикладными программами в процессе их установки. Обычно создаваемые таким образом учетные записи имеют необходимое описание в своих свойствах.

Учетная запись *Система*

При необходимости можно настроить службы Windows для старта от имени любого пользователя. Однако в этом случае вам необходимо установить соответствующей учетной записи постоянный пароль и предоставить ей достаточно большие права по отношению к локальному компьютеру. Из такого сочетания требований очевидно вытекает настоятельная рекомендация: не использовать учетные записи пользователей для запуска служб по соображениям безопасности.

Учетная запись **Система** (Local System) предназначена для запуска служб компьютера. Она обладает полными правами по отношению к локальному компьютеру и фактически является частью операционной системы. Ее права существенно выше, чем права любой учетной записи пользователя. Для учетной записи **Система** выполняется обход проверок безопасности, поэтому для нее не существует *пароля*, который можно было бы дешифровать или взломать. Эта учетная запись не может быть использована для доступа к сетевым ресурсам.

Использования учетной записи **Система** для запуска служб компьютера без особых на то причин следует избегать, поскольку данное решение понижает уровень безопасности. Например, если пользователю удастся подменить запускаемый файл службы на пакетный файл и затем прервать выполнение этого пакетного файла нажатием комбинации клавиш <Ctrl>+<C>, то он получит возможность запуска в этом командном окне задач с приоритетом учетной записи **Система**. Поэтому для

использования при запуске служб введены еще две учетные записи. Это **Local Service** и **Network Service**. Так же, как и учетная запись **Система**, эти учетные записи являются частью самой операционной системы и не имеют *паролей*. При этом они обладают гораздо меньшими правами, чем учетная запись **Система**, но бóльшими правами, чем пользователь. Обе учетные записи по умолчанию имеют права пользователя и аутентифицированного пользователя и привилегии **SE_AUDIT_NAME**, **SE_CHANGE_NOTIFY_NAME**, **SE_UNDOCK_NAME**. Если учетная запись **Local Service** используется также только при запуске локальных программ, то **Network Service** может осуществлять доступ к сетевым ресурсам. При этом данная учетная запись аутентифицируется в удаленной системе как учетная запись соответствующего компьютера.

> ***Примечание***
>
> Следует быть внимательным при назначении прав доступа к локальным ресурсам компьютера. Автор неоднократно сталкивался с ситуацией, когда недостаточно опытные пользователи, желая ограничить доступ к ресурсам своего компьютера, работающего в составе сети, запрещали доступ к файлам на диске всем, кроме самого себя. Исключив специальных пользователей, они сделали невозможным запуск многих служб, необходимых для работы операционной системы.

Настройка отдельных параметров паролей

В реальной системе администраторам обычно приходится подстраивать некоторые параметры паролей учетных записей. Отметим некоторые возможности.

Настройка отличающихся политик паролей в Windows Server 2008

Политика паролей домена Windows устанавливает требования к сложности пароля, времени его действия и т. д. Эта политика привязана ко всему домену и не может быть изменена созданием соответствующих настроек в групповых политиках подразделений.

Начиная с Windows Server 2008, появилась возможность создавать различные настройки паролей внутри одного домена. Такие настройки, или, иными словами, политики, можно привязывать к группам безопасности, в которые включаются соответствующие пользователи из некоторого подразделения. При этом синхронизация состава такой группы безопасности и состава подразделения должна будет выполняться вручную: если учетная запись пользователя будет перемещена в другое подразделение, то ее нужно будет вывести из соответствующей группы безопасности.

Для того чтобы создать отдельную политику паролей, нужно выполнить следующие шаги.

1. Создайте глобальную группу безопасности в домене. Например, SpecialPassword.
2. Откройте ADSI Edit и подключитесь к вашему домену. Перейдите к контейнеру **System | Password Settings Container**. Щелкните по нему правой кнопкой мыши и выберите операцию **Создать | Объект** (рис. 7.3).

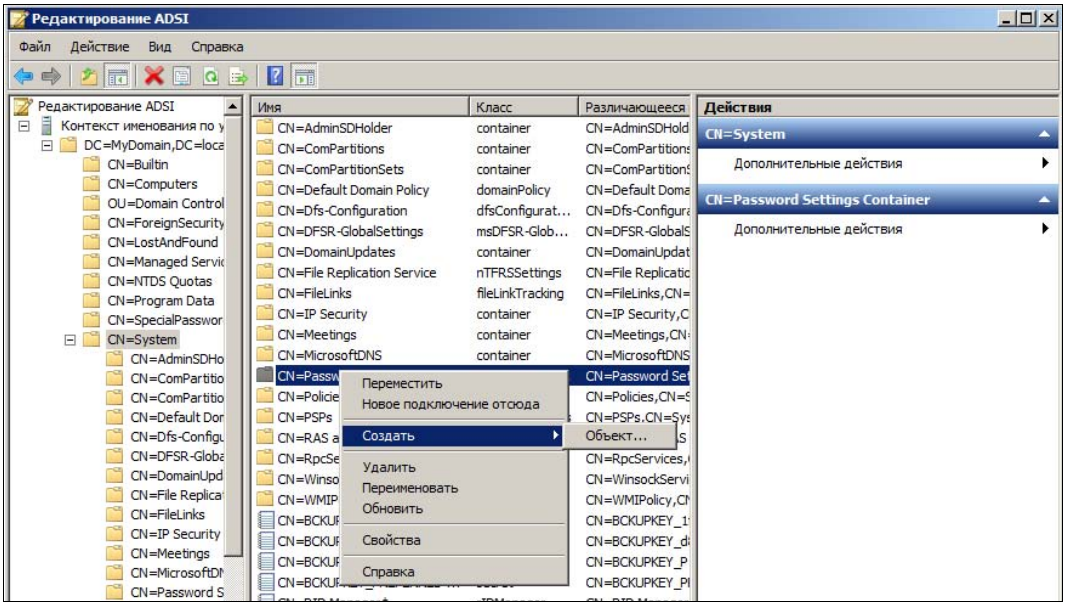


Рис. 7.3. Создание нового объекта в контейнере паролей

3. Согласитесь с предложенным классом (msDC-PasswordSettings) и нажмите кнопку **Next**.
4. Для атрибута **cn** введите имя группы безопасности, созданной вами на первом шаге, и нажмите кнопку **Next** (так сделать удобно, хотя можно и ввести произвольное название для объекта).
5. Для атрибута **msDS-PasswordSettingsPrecedence** укажите значение 1, а на последующих шагах введите параметры новой парольной политики. Обратите внимание, что данные для сроков действия паролей, периода блокировки и т. п. должны вводиться в формате дд:чч:мм:сс, например, 1:00:00:00.
6. После завершения ввода необходимых параметров (если вы допустите ошибку, то появится соответствующее сообщение в ADSI Edit, указывающее на неправильно введенные значение) в контейнере Password Settings Container появится новый объект (в нашем случае с именем SpecialPassword). Отметьте его и выберите команду **Свойства**. Появится окно, аналогичное изображенному на рис. 7.4.
7. Найдите строку **msDS-PSOAppliesTo** и откройте ее для редактирования, нажав кнопку **Изменить**. Появится окно **Редактор многозначных различаемых имен субъектов безопасности**, в котором вы должны добавить группу, созданную ранее.
8. Завершите редактирование, последовательно нажимая кнопки **OK**.

Указанным способом можно создать необходимое число объектов точной настройки паролей и привязать их к соответствующим группам безопасности.

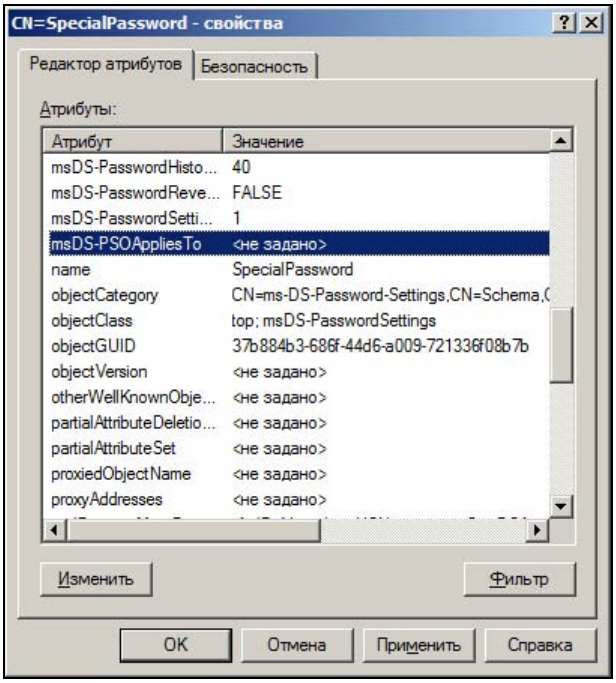


Рис. 7.4. Окно свойств нового объекта паролей

Настройка правил смены пароля в Linux

По умолчанию учетная запись пользователя в Linux создается с постоянно действующим паролем. Это не является рекомендуемой практикой, обычно требования смены пароля присутствуют в параметрах безопасности информационной системы.

Если нужно внедрить периодическую смену пароля в автономной системе Linux, то можно использовать пакет chage (`apt-get install chage`). Этот пакет позволяет настроить требования периодической смены паролей (и соответствующие блокировки после истечения сроков смены). Для установки срока жизни пароля администратор должен выполнить команду:

```
chage -M число_дней имя
```

Пользователь может сам запустить команду `chage` для просмотра информации о сроках своего пароля (`chage -l имя`).

За установленное число дней перед сроком смены пароля пользователю будет выдаваться предупреждение, а затем вход в систему станет недоступен до смены пароля.

Блокировка учетных записей

Иногда необходимо временно отключить учетную запись. Большинству пользователей не надо объяснять, как выполнить эту операцию в Windows. Обычно блоки-

ровку пользовательских учетных записей администраторы осуществляют при помощи оснастки **AD Пользователи и компьютеры**. Для блокировки достаточно выделить учетную запись и выбрать команду **Отключить** в меню ее свойств.

В Linux отключение учетной записи можно сделать различными способами. Проще всего выполнить командой, используемой для смены пароля:

```
passwd -l <учетная запись>
```

> ***Примечание***
>
> Некоторые администраторы предпочитают просто поставить вместо *x* звездочку в файле паролей (/etc/passwd) или отключить доступ пользователю к командному процессору (`usermod -s /bin/false <учетная_запись>`). Но предпочтительнее стандартный способ блокировки учетной записи.

Для включения учетной записи нужно выполнить такую же команду, только с ключом `-u`. Для запоминания: `l` — сокращение от *lock*, `u` — от *unlock*.

Группы пользователей

Разные пользователи должны иметь различные права по отношению к компьютерной системе. Если в организации всего несколько сотрудников, то администратору не представляет особого труда индивидуально распределить нужные разрешения и запреты. Хотя и в этом случае возникают проблемы, например, при переходе сотрудника на другую должность администратор должен вспомнить, какие права были даны ранее, "снять" их и назначить новые, но принципиальной необходимости использования каких-либо объединений, групп пользователей не возникает.

Иная ситуация в средней организации. Назначить права доступа к папке для нескольких десятков сотрудников — достаточно трудоемкая работа. В этом случае удобно распределять права не индивидуально, а по *группам пользователей*, в результате чего управление системой существенно облегчается. При смене должности пользователя достаточно переместить его в другую группу. При создании новых проектов права доступа к ним будут назначаться на основе существующих групп и т. п.

Исторически сложилось так, что существует несколько типов групп в Windows. Связано это в основном с необходимостью совместимости различных версий операционных систем.

Во-первых, есть группы, которым, как и пользователям, присваивается идентификатор безопасности. Это означает, что вы можете назначать права доступа, основываясь не на индивидуальном членстве, а сразу всей группе пользователей. И есть группы, которые не имеют такого SID. Например, Distribution Group. Объясняется это наличием групповых операций, для которых не нужно контролировать параметры безопасности. Например, создание группы пользователей для распространения программного обеспечения или группы для централизованной рассылки почты. Отсутствие SID не мешает в этом случае правильному функционированию программ, но существенно снижает нагрузку операционной системы.

Во-вторых, группы могут различаться по области действия. Например, существуют локальные группы, глобальные и универсальные.

В-третьих, группы могут иметь постоянных членов (каждый пользователь назначается в соответствующую группу администратором) или основываться на выборке пользователей по каким-либо правилам. Например, можно создать группу, в которую будут включаться пользователи с записью в их свойствах, что они работают в "отделе 22". Изменилось соответствующее поле в свойствах пользователя — и при очередных операциях с данной группой система проведет выборку пользователей, "увидит" новых членов группы и выполнит необходимые действия. Обратите внимание, что такие группы с динамическим членством не имеют *SID*, т. е. не могут быть использованы для контроля прав доступа.

> ***Примечание***
>
> В Windows пользователь "получает" список групп, в которых он состоит, *при входе в систему*. Поэтому если администратор сменил у пользователя членство в группах, то это изменение начнет действовать *только* после нового входа в систему. Если пользователь должен быстро получить доступ к ресурсам, ему следует завершить работу в системе (`log off`) и сразу же вновь войти в нее (`log on`).

Встроенные группы Windows

При установке операционной системы Windows на компьютере автоматически создается несколько групп. Для большинства случаев персонального использования этих групп достаточно для безопасной работы и управления системой.

- **Администраторы** (Administrators). Члены этой группы имеют все права на управление компьютером. После установки в системе присутствуют только пользователи — члены этой группы (в Windows XP в ходе установки можно создать несколько администраторов системы, в предыдущих версиях создавалась только одна запись).
- **Пользователи** (Users). Это основная группа, в которую надо включать обычных пользователей системы. Членам этой группы запрещено выполнять операции, которые могут повлиять на стабильность и безопасность работы компьютера.
- **Опытные пользователи** (Power Users). Эти пользователи могут не только выполнять приложения, но и изменять некоторые параметры системы. Например, создавать учетные записи пользователей, редактировать и удалять учетные записи (но только те, которые были ими созданы), предоставлять в совместный доступ ресурсы компьютера (и управлять созданными ими ресурсами). Но опытные пользователи не смогут добавить себя в число администраторов системы, не получат доступ к данным других пользователей (при наличии соответствующих ограничений в свойствах файловой системы NTFS, у опытных пользователей отсутствует право становиться владельцем объекта), кроме того, они не смогут выполнять операции резервного копирования, управлять принтерами, журналами безопасности и протоколами аудита системы.
- **Операторы архива** (Backup Operators). В эту группу следует включить ту учетную запись, от имени которой будет осуществляться резервное копирование

данных компьютера. Основное отличие этой группы в том, что ее члены могут "обходить" запреты доступа к файлам и папкам при операции резервного копирования данных. Независимо от установленных прав доступа в резервную копию данных будут включены все отмеченные в операции файлы, даже если у оператора резервного копирования нет права чтения такого файла.

- **Гости** (Guests). Эта группа объединяет пользователей, для которых действуют специальные права для доступа "чужих" пользователей. По умолчанию в нее включена только одна заблокированная учетная запись **Гость**.
- **Пользователи удаленного рабочего стола.** Ее члены могут осуществлять удаленное подключение к рабочему столу компьютера. Иными словами, если вы хотите иметь возможность удаленно подключиться к своему компьютеру, то необходимо включить в эту группу соответствующую учетную запись. По умолчанию членами этой группы являются администраторы локального компьютера.
- **DHCP Administrators.** Группа создается только при установке DHCP. Пользователи группы имеют право на конфигурирование службы DHCP (например, с помощью графической оснастки управления или командой `netsh`). Используется при делегировании управления DHCP-службой.
- **DHCP Users** и **WINS Users**. Группы создаются только при установке соответствующих служб. Пользователи групп имеют право лишь на просмотр параметров настройки служб DHCP (или WINS). Применяются при делегировании прав техническому персоналу (например, для сбора информации о состоянии сервисов).
- **Операторы настройки сети.** Пользователи группы имеют право изменения TCP/IP-параметров. По умолчанию группа не содержит членов.

Специальные группы Windows

В Windows существуют так называемые *специальные группы*, членством в которых пользователь компьютера управлять не может. Они не отображаются в списке групп в оснастках управления группами, но доступны в окнах назначения прав доступа.

Это группы **Все** (Everyone), **Интерактивные пользователи** (Local Users), **Сетевые пользователи** (Network Users), **Пакетные файлы** (Batch), **Прошедшие проверку** (Authenticated) и т. д. Предназначение групп ясно уже по их названию. Так, в группу **Интерактивные пользователи** автоматически включаются все пользователи, осуществившие вход в систему с консоли (клавиатуры). **Сетевые пользователи** — это те пользователи, которые используют ресурсы данного компьютера через сетевое подключение и т. п.

Данные группы предназначены для более точного распределения прав пользователей. Например, если вы хотите, чтобы с каким-либо документом была возможна только локальная работа, то можно просто запретить доступ к нему сетевых пользователей.

Заострим внимание читателей на группе **Все**, поскольку именно с ней связано наибольшее количество ошибок в предоставлении прав доступа. Эта группа включает

не любых пользователей, а только тех, кто имеет учетную запись на данном компьютере. Иными словами, если вы предоставили ресурс в общий доступ с правами чтения для группы **Все**, то использовать его могут только те, кто "прописан" на данном компьютере. Если вы предпочитаете, чтобы ресурс мог применять действительно "кто угодно", то для этого нужно разрешить использование учетной записи **Гость**.

> ***Примечание***
>
> В последних версиях Windows пересматривался состав группы **Все**. Во избежание ошибок следует уточнить состав данной группы в каждом конкретном случае.

Возможные члены групп. Области применения групп

Универсальные группы появились с выходом ОС Windows 2000. В *смешанном режиме* допустимы были только группы **Distribution Group**, при переходе в основной режим стало возможным создавать и универсальные группы безопасности.

Универсальные группы могут включать учетные записи (и другие группы) из любого домена предприятия и могут быть использованы для назначения прав также в любом домене предприятия.

Глобальные группы могут включать другие группы и учетные записи *только* из того домена, в котором они были созданы. Но группа может быть использована при назначении прав доступа в любом домене.

Локальные группы могут включать объекты как из текущего домена, так и из других доменов. Но они могут быть использованы для назначения прав *только в текущем домене*.

В группы можно включать как учетные записи пользователей и компьютеров, так и другие группы. Однако возможность вложения зависит от типа группы и области ее действия (табл. 7.2).

Таблица 7.2. *Группы пользователей*

Группа	Включает объекты	Допустимые вложения групп
Локальная	Пользователи	Универсальные и глобальные группы *любого* домена
Локальная безопасности	Пользователи	Глобальные группы
Глобальная	Пользователи	Глобальные группы этого же домена
Глобальная безопасности	Глобальная группа	Нет
Универсальная	Пользователи и компьютеры	Универсальные и глобальные группы *любого* домена

Начиная с Windows 2000 и режима native mode, администраторы могут изменять типы групп, а именно преобразовывать группу безопасности в **Distribution Group**, и наоборот. Возможна также смена области действия группы с универсальной на доменную.

Обратите только внимание, что наличие вложенных групп в некоторых случаях может препятствовать преобразованию типа родительской группы.

Контроль состава групп

Поскольку основная практика предоставления прав заключается во включении учетной записи в соответствующую группу, то контроль состава групп является эффективным средством поддержания режима безопасности.

В Windows состав групп домена можно контролировать через настройки групповой политики. Для этого используется параметр **Группы с ограниченным доступом**. Если вы определите через групповую политику состав какой-либо группы (создав соответствующие настройки в этой части групповой политики), то пользователи уже не смогут вносить в нее изменения. Например, если через групповую политику определить состав локальной группы администраторов, то даже если пользователь получит доступ к системе и назначит себя администратором компьютера, то при подключении к домену его учетная запись будет исключена из группы администраторов.

Целесообразно настроить мониторинг изменения состава групп администраторов домена и предприятия. Для этого достаточно включить протоколирование событий безопасности и отслеживать события в журналах безопасности контроллеров домена (табл. 7.3).

Таблица 7.3. *Идентификаторы событий изменения групп Windows*

Тип группы	Область	Создание	Изменение	Удаление	Члены групп	
					добавлены	удалены
Безопасности	Локальная	635	641	638	636	637
	Глобальная	631	639	634	632	633
	Универсальная	658	659	662	660	661
Распространения	Локальная	648	649	652	650	651
	Глобальная	653	654	657	655	656
	Универсальная	663	664	667	665	666

Запуск команд от имени другого пользователя

Необходимость запуска команды от имени другого пользователя возникает в том случае, если требуется воспользоваться правами доступа чужой учетной записи.

Эскалация прав *Администратора* в Windows

Начиная с Windows Vista, пользователю, состоящему в группе локальных администраторов, не предоставляются полные права управления компьютером. Если операция требует наличия административных прав, то система выдаст предупреждение, на которое необходимо вручную дать подтверждение. Другой вариант — сразу запустить операцию от имени администратора, воспользовавшись соответствующей строчкой в меню исполняемого файла.

> ***Примечание***
>
> Если программа требует эскалирования прав, то целесообразно соответствующую настройку включить в ярлык ее запуска.

Если администратору необходимо выполнять программу, нуждающуюся в эскалировании прав, в пакетном режиме, то возможным выходом будет настройка варианта ее запуска с помощью пакета обеспечения совместимости (Microsoft Application Compatibility Toolkit, пакет доступен к бесплатной загрузке с сайта вендора). Для этого нужно будет создать новый пакет исправлений совместимости для выбранной программы, указать в его настройках нужный вариант запуска программы (рис. 7.5) и установить данное исправление в локальную базу сервера.

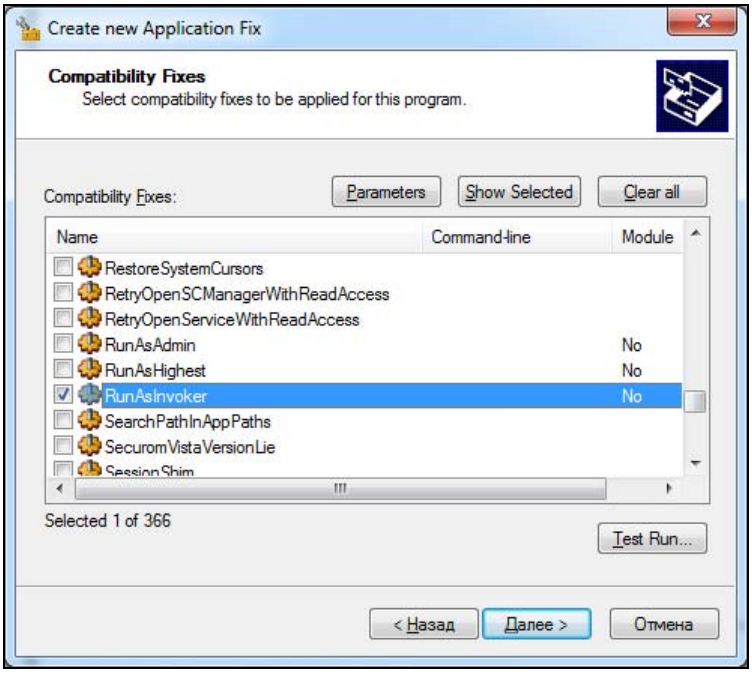


Рис. 7.5. Настройка вариантов запуска с помощью создания исправления совместимости

Запуск от имени другого пользователя в Windows

Если нужно запустить операцию от имени другого пользователя, то следует при нажатой клавише <Shift> щелкнуть правой кнопкой мыши по значку исполняемого файла (или ярлыка к нему). Откроется контекстное меню, в котором будет присутствовать команда **Запустить от имени другого пользователя**. При выборе данного пункта появится диалоговое окно, в котором нужно ввести параметры (имя и пароль) учетной записи.

При запуске от имени другого пользователя можно использовать аппаратные средства аутентификации. Для этого достаточно выбрать соответствующий способ аутентификации и ввести PIN-код доступа к ключу или смарт-карте.

Запуск от имени другого пользователя в Linux

В Linux для смены пользователя в текущей сессии используется команда `su`. В качестве ее параметра нужно указать название учетной записи. Следующая команда переключит пользователя на учетную запись `nagios`:

```
su – nagios
```

После ввода команды нужно указать пароль соответствующей учетной записи в ответ на запрос системы.

Команда `su` — (без указания имени учетной записи) переключает сессию на использование учетной записи суперпользователя (root).

> ***Примечание***
>
> Определить, что сессия выполняется от имени учетной записи root, очень легко. По умолчанию в строке приветствия для учетной записи root отображается символ `#`. А в случае других учетных записей — символ `$`.

Для переключения с учетной записи root на любую другую не требуется *вводить пароль*. Поэтому, зная пароль учетной записи root, можно переключиться на любого пользователя системы, даже не зная его пароля.

Предоставление дополнительных прав командой *sudo*

Помимо команды `su` в Linux есть пакет sudo, предназначенный для предоставления дополнительных прав учетной записи при выполнении операций. В частности, в Ubuntu по умолчанию не предусмотрено переключение в сеанс пользователя root (поскольку пароль[1] этой учетной записи не задан). Команды, требующие наличия

[1] Те, кто хочет сохранить традиционное использование учетной записи root, могут включить данную возможность, присвоив этой учетной записи пароль: `sudo passwd root`. После назначения пароля вы можете переключаться в учетную запись root с помощью команды `su -`. Для возврата достаточно удалить запись о пароле из файла учетных записей.

административных прав, следует выполнять, указывая в начале строки символы sudo, например, так:

```
sudo apt-get update
```

При этом в качестве ответа на запрос пароля следует вводить пароль текущего пользователя.

> ***Примечание***
>
> При желании можно отключить запрос ввода пароля для определенных пользователей и групп, отредактировав файл настроек.

Применение sudo более безопасно, чем переключение в режим суперпользователя с помощью команды su. Во-первых, команда sudo отключает ряд переменных среды, что исключает риск подмены библиотек. Во-вторых, с помощью sudo можно осуществить точные настройки прав пользователей, например, явно указав, какие команды можно выполнить данному пользователю с правами суперпользователя и т. п. То есть, при необходимости можно разрешить конкретному пользователю запуск нескольких команд, требующих административных прав, не предоставляя никаких излишних полномочий.

По умолчанию право работы с командой sudo предоставлено членам группы adm (пользователь, имя которого было введено в момент установки системы, включен в эту группу). Настроить права на использование команды sudo можно, открыв файл настройки командой visudo:

```
sudo visudo
```

> ***Примечание***
>
> Прямое редактирование файла sudoers в текстовом редакторе не рекомендуется. Хотя внешне данная операция идентична работе в редакторе nano, но, например, при попытке сохранения изменений в файле конфигурации система проверяет синтаксис и не дает выйти из режима редактирования до устранения ошибок. Кроме того, использование visudo предупреждает одновременное редактирование файла sudoers двумя пользователями и т. п. Все это позволяет избежать ошибок настройки параметров предоставления прав.

Структуру правил файла можно уточнить либо обратившись к справочной документации, либо воспользовавшись примерами в самом файле. Например, чтобы предоставить администраторам домена возможность выполнять операции на сервере Ubuntu с правами суперпользователя, добавьте в конец файла следующую строку:

```
%DOMAIN\\Domain\ Admins ALL=(ALL) ALL
```

> ***Примечание***
>
> Обратите внимание, что символ \ предваряет слеш в паре "домен — пользователь" и пробел в названии группы (это зеркалирование специальных символов, к которым относятся как слеш, так и пробел).

Если необходимо выполнить несколько операций с полными правами, то можно открыть сессию в режиме суперпользователя, применив ключ -s в команде sudo:

```
sudo -s
```

В результате выполнения этой команды откроется новая консоль с правами пользователя root.

Кто работает на компьютере

Чтобы узнать, кто работает на Linux-компьютере, достаточно набрать в командной строке одну букву `w`:

```
$ w
12:32:12 up 1 day, 1:32, 1 user, load average: 0,00, 0,00, 0,00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
kenin pts/0 192.168.0.9 10:35 1.00s 0.08s 0.00s w
```

Вывести на экран всех пользователей Linux (как вошедших с консоли, так и подключенных по ssh, pptp и т. д.) можно командой `who`. Обратите внимание, что команда отображает имя пользователя, вошедшего в систему, а не того, с параметрами которого он сейчас работает. Например, если вы переключились в сеанс с правами суперпользователя, то на экране отобразится не его имя, а исходное:

```
root@geny:~# who
kenin pts/0 2008-12-26 11:35 (192.168.31.252)
```

В Windows 7/Server 2008 для отображения информации о текущем пользователе применяется команда `whoami`.

Права учетной записи

Настройка прав доступа в операционных системах является основным методом разграничения возможностей различных пользователей. Права доступа устанавливаются для:

- объектов файловой системы (папок, файлов);
- ключей реестра системы;
- служб Windows.

Традиционные способы назначения прав доступа

Администраторы обычно используют назначение прав доступа с помощью графических средств. Для назначения прав доступа следует отметить нужный объект, выбрать в контекстном меню команду **Свойства** и перейти на вкладку **Безопасность** (рис. 7.6). После чего можно менять состав пользователей, которым предоставлены права доступа, уточнять разрешения и т. п.

Обычно такая процедура не вызывает сложностей даже у начинающего администратора. На что при этом следует обратить внимание.

Права доступа *наследуются* так: файл, создаваемый в некоторой папке, получит те права доступа, которые была назначены на всю папку. К наследованным правам можно добавить новое разрешение. Но если попытаться изменить в более строгую

сторону существующие разрешения (например, исключить определенных пользователей), то система предложит заменить унаследованные явно назначенными, скопировав действующий набор прав.

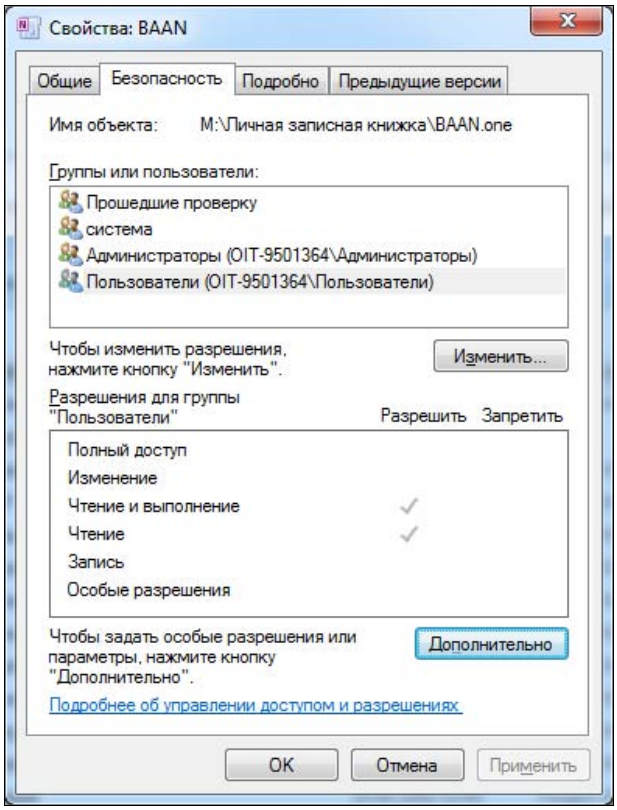


Рис. 7.6. Назначения параметров безопасности для файла

Разрешения общего доступа и разрешения безопасности

Для объектов файловой системы, предоставляемых в совместное использование, существуют два типа разрешений. Это разрешения общего доступа и разрешения безопасности. Разрешения *общего доступа* определяют право на использование данного ресурса при сетевом подключении. Если у пользователя нет такого права (или это действие запрещено явно), то он просто не сможет *подключиться* к запрашиваемому ресурсу.

Разрешение *безопасности* — это разрешение на уровне прав доступа файловой системы. Оно существует при использовании файловой системы типа NTFS в Windows и файловых систем Linux (ext3 и т. п.) и проверяется *независимо* от разрешений общего доступа. Иными словами, если пользователю разрешено подключаться к этому ресурсу по сети, но доступ к файлам запрещен разрешениями безо-

пасности, то в итоге работа с такими файлами будет невозможна. Если на диске с ресурсами использована файловая система FAT (FAT32), то доступ по сети будет контролироваться *только* разрешениями общего доступа.

> ***Примечание***
>
> Типичной ошибкой пользователей, связанной с наличием двух типов разрешений, является предоставление в совместное использование папок, находящихся на рабочем столе Windows. После предоставления общего доступа к таким папкам другие пользователи не могут открыть файлы и т. п. Связана эта ошибка с тем, что рабочий стол — это папка в профиле пользователя. А разрешение безопасности на профиль пользователя по умолчанию разрешает доступ к нему *только* этому пользователю и администратору компьютера. Поэтому для возможности работы других пользователей с такой общей папкой необходимо добавить для них *разрешения безопасности* на уровне файловой системы.

Поскольку эти разрешения в определенной степени дублируют друг друга (с точки зрения результата), то на практике их обычно комбинируют в зависимости от желаемых условий доступа.

- *Права доступа ко всем объектам сетевого ресурса одинаковы для всех пользователей.* В этом случае разрешения общего доступа и разрешения безопасности выставляются идентичными для всех заданных групп пользователей.
- *Права доступа различны для разных объектов сетевого ресурса.* Часто бывает так, что к одним файлам нужно предоставить полный доступ, а другие разрешить только просматривать и т. д. В этом случае можно настроить права доступа следующим образом.

  Разрешения общего доступа устанавливаются по максимально возможным правам. Так, если часть файлов должна быть доступна только для чтения, а часть и для редактирования, то разрешения общего доступа следует установить как *"полный доступ"* для всех групп пользователей, которым ресурс должен быть доступен по сети. А разрешениями безопасности нужно выполнить точную настройку: установить разрешение только для чтения для одних папок, полный доступ — для других, запретить доступ к определенным папкам для некоторых групп пользователей и т. д.

  Такой подход упростит структуру ресурсов сети при сохранении всех необходимых разрешений.

Порядок проверки прав доступа

Обычно система сначала проверяет наличие запретов, а только потом — разрешения на доступ. Поэтому часто ошибкой пользователей является назначение для себя полного доступа к файлу при одновременном запрете доступа к нему группы **Пользователи**. Поскольку сам пользователь также входит в эту группу, то доступ к файлу будет ему закрыт, несмотря на наличие явного разрешения.

Поэтому при назначении явных запретов следует проявлять особую осторожность, тщательно анализируя состав групп, для которых предполагается установить явный запрет.

Правила записи прав доступа

При автоматизации операций управления информационной системой администратору необходимо правильно описывать регулируемые права доступа к объектам. Права доступа принято записывать в соответствии с синтаксисом SDDL (Security Descriptor Definition Language, дескрипторный язык определений безопасности).

Параметр, описывающий права доступа к объекту для какой-либо учетной записи, называется ACE (access control entry, параметр управления доступом). ACE на языке SDDL представляет собой строку символов, которая состоит из шести полей, разделенных точкой с запятой. Причем часть полей может быть опущена, в этом случае в строке будет стоять подряд несколько символов точки с запятой.

Первое поле строки ACE — это всегда тип доступа: разрешение (A от англ. *allow*) или запрет (D от англ. *deny*). Второе поле определяет тип объекта: контейнер (например, папка с файлами) или непосредственно сам объект. Это поле называется *флагом ACE*.

В третьем поле, собственно, и записываются сами права доступа. Права могут быть записаны как в виде символьной строки (по правилам языка SDDL), так и в виде двоичного числа — *маски*. (Такой способ применяется в программировании на языках C: единица на определенном месте соответствует наличию соответствующего права; подробности можно уточнить по документации MSDN. Например, маска 0x100e003f соответствует правам READ_CONTROL, WRITE_DAC, WRITE_OWNER, GENERIC_ALL и Others(0x0000003f).)

В четвертом и пятом полях можно записывать уникальные идентификаторы (GUID) объекта и наследования. Эти поля не используются для назначения прав к файлам и папкам и обычно применяются при назначении делегирования прав для доступа к объектам службы каталогов.

В шестом поле содержится идентификатор учетной записи пользователя или группы, для которой создается данная настройка разрешений. Это может быть SID учетной записи, идентификатор для стандартных записей в форме S-1-X-X-X-X-X-X или код учетной записи, список которых приведен в табл. 7.4.

> ***Примечание***
>
> Строго говоря, за шестым полем могут быть записаны условия применения данного права (в круглых скобках). Например, должен ли для использования данного права доступа существовать какой-то атрибут объекта или право доступа будет применено, только если данный атрибут будет иметь определенное значение.

Приведем несколько примеров ACE:

```
A;;FA;;;BA              (полные права для встроенных
                         учетных записей администраторов)
A;;FA;;; S-1-5-21-3927846150-1660447138-1319031662-5627 (полные права
                         для конкретной учетной записи домена)
A;;0x1301bf;;;AU        (набор прав, заданный маской,
                         для прошедших проверку пользователей)
```

Для облегчения "перевода" дескриптора безопасности на доступный пользователю язык можно использовать различные утилиты. Например, `sddlparse`, которую можно загрузить по ссылке **http://blogs.microsoft.co.il/files/folders/guyt/entry70399.aspx**. Пример вывода данной утилиты для случая анализа приведенного выше примера с маской в поле прав показан в листинге 7.1. Вывод этой программы уже более понятен для администратора.

Листинг 7.1

```
>sddlparse.exe D:(A;;0x1301bf;;;AU)
SDDL: D:(A;;0x1301bf;;;AU)
Ace count: 1
**** ACE 1 of 1 ****
ACE Type: ACCESS_ALLOWED_ACE_TYPE
Trustee: NT AUTHORITY\AccessMask:
ADS_RIGHT_DELETE
ADS_RIGHT_READ_CONTROL
ADS_RIGHT_DS_CREATE_CHILD
ADS_RIGHT_DS_DELETE_CHILD
ADS_RIGHT_ACTRL_DS_LIST
ADS_RIGHT_DS_SELF
ADS_RIGHT_DS_READ_PROP
ADS_RIGHT_DS_WRITE_PROP
ADS_RIGHT_DS_LIST_OBJECT
ADS_RIGHT_DS_CONTROL_ACCESS
Inheritance flags: 0
```

Каждое ACE определяет права доступа для одной учетной записи. Такое ACE называют *дискретным* (соответственно, и весь дескриптор безопасности имеет название дискретного — DACL).

Понятно, что для объекта обычно назначаются права для нескольких учетных записей (групп). Для записи в этом случае каждое ACE заключают в круглые скобки и просто перечисляют все ACE без пробелов в одной строке.

Полный дескриптор безопасности включает в себя еще несколько параметров. В начале его указывается владелец объекта (owner) как `O:`*<символы>* (*<символы>* соответствуют группам, перечисленным в табл. 7.4). После чего идет название первичной группы в формате `G:`*<символы>*. И только затем собственно права (набор ACE), которые предваряются символами `D:`. В итоге дескриптор безопасности будет выглядеть примерно так:

```
O:BAG:SYD:(A;;FA;;;WD)
```

В соответствии с этим описанием владельцами объекта являются встроенные администраторы (`BA`), первичная группа — встроенная системная учетная запись (`SY`, так называется группа для встроенной учетной записи системы), к объекту предоставлены полные права (`FA`) доступа (`A`) для всех (`WD`).

System ACL

System ACL (SACL) представляют собой описания правил аудита над объектами. Составляются они по такой же форме, что и дискретные ACL, только начинаются они с символа `S`, за которым после двоеточия идет несколько флагов (параметров аудита, например, наследование от родительского объекта) и далее в скобках строка символов, по структуре аналогичная ACE. Отличается она только используемыми символами. Например, вместо `A` или `D` в первой группе применяется `AU` (audit) и т. д.

На практике системному администратору с дескрипторами SACL приходится работать крайне редко, поэтому мы не будем описывать особенности интерпретации этой строки и отошлем читателя к справочной документации.

Коды типов пользователей в SDDL

Коды во многом основаны на аббревиатурах английских терминов, поэтому в табл. 7.4 приведены как английские расшифровки, так и локализованные значения.

Таблица 7.4. *Коды стандартных учетных записей Windows*

Код	Пользователь	
	Оригинальное название	**Локализованное название**
DA	Domain administrators	Администраторы домена
DG	Domain guests	Гости домена
DU	Domain users	Пользователи домена
ED	Enterprise domain controllers	Контроллеры домена предприятия
DD	Domain controllers	Контроллеры домена
DC	Domain computers	Компьютеры домена
BA	Built-in administrators	Встроенные (локальные) администраторы
BG	Built-in guests	Встроенные (локальные) гости
BU	Built-in users	Встроенные (локальные) пользователи
LA	Local administrator	Учетная запись локального администратора
LG	Local guest	Учетная запись локального гостя
AO	Account operators	Операторы учета
BO	Backup operators	Операторы архива
PO	Printer operators	Операторы принтера
SO	Server operators	Операторы сервера
AU	Authenticated users	Прошедшие проверку
PS	Personal self	Личный (SELF)
CO	Creator owner	Создатель-владелец
CG	Creator group	Группа-создатель

Таблица 7.4 *(окончание)*

Код	Пользователь	
	Оригинальное название	**Локализованное название**
SY	Local system	Локальная система
PU	Power users	Опытные пользователи
WD	Everyone	Все (Общий доступ)
RE	Replicator	Репликатор
IU	Interactively logged-on user	Пользователь интерактивного входа
NU	Network logon user	Сетевой пользователь
SU	Service logon user	Пользователь с правами службы
RC	Restricted code	Запрещенный код
WR	Write Restricted code	Код, защищенный от записи
AN	Anonymous logon	Анонимный вход
SA	Schema administrators	Администраторы схемы
CA	Certificate server administrators	Администраторы служб сертификации
RS	RAS servers group	Группа серверов удаленного доступа
EA	Enterprise administrators	Администраторы предприятия
PA	Group Policy administrators	Администраторы групповой политики
RU	Alias to allow previous Windows 2000	Псевдоним для запуска версий Windows до Windows 2000
LS	Local service account	Учетная запись локальной службы (для служб)
NS	Network service account	Учетная запись сетевой службы (для служб)
RD	Terminal server users (remote desktop)	Пользователи удаленного рабочего стола (для служб терминалов)
NO	Network configuration operators	Операторы настройки сети
MU	System Monitor Users	Пользователи системного монитора
LU	Log service users	Пользователи журналов производительности
IS	Internet Service logon user	Анонимные пользователи Интернета
CY	Cryptographic configuration users	Операторы криптографии
OW	Owner	SID с правами владельца
RM	Right Management service logon users	Служба RMS

Права доступа для служб несколько отличаются (табл. 7.5). Подробно с описаниями этих прав можно ознакомиться по ссылке **http://support.microsoft.com/kb/914392/ru**.

Для управления правами доступа к службам (процессам) в Windows применяется утилита `sc`. Подробности ее использования доступны в онлайновой справке.

Таблица 7.5. *Права доступа к службам Windows*

Пара	Право или разрешение
CC	Право чтения (запроса) конфигурации службы
DC	Право удаления дочерних объектов службы (delete child)
LC	Право чтения (запроса) состояния службы
SW	Право перечисления зависимых служб
RP	Право чтения всех параметров службы (Read all properites)
WP	Право остановки службы
DT	Право временной остановки службы и последующего запуска *(пауза — старт)*
LO	Право запроса текущего статуса службы
CR	Право отправки службе сигнала управления, созданного автором службы
GA	GenericAll
GX	GenericExecute
GW	GenericWrite
GR	GenericRead
SD	Право удаления службы
RC	Право чтения дескриптора безопасности службы (Read Control)
WD	Право изменения дескриптора безопасности службы
WO	Право смены владельца

Права доступа в Linux

Права доступа в Linux-системах назначаются единым образом как для файлов и папок, так и для устройств (например, для принтера).

Типы прав доступа в Linux

Права назначаются для трех категорий пользователей: для владельца файла (тот, кто его создал), для группы, в которую входит владелец файла, и для всех остальных пользователей. В Linux принято отображать права доступа в виде последовательности символов — `-rwxr-x--x`. Первый символ обозначает тип файла (`-` — обычный файл, `d` — папка, возможны также псевдофайлы), следующие три символа обозначают права владельца файла, следующие три — права группы, к которой принадлежит владелец, и последние три символа обозначают права для всех остальных пользователей. В каждой тройке первый символ свидетельствует о наличии права чтения (`r` — право есть, — (дефис) — нет права), второй — право записи (`w`) и третий — исполнения (`x`). Часто права записывают также в виде трех цифр, например, `753`. Если представить каждую цифру в двоичном виде, то получится `111101011`, что соответствует `rwxr-x-wx`.

Такая форма является сокращением от полного варианта записи. В нем присутствует еще первая тройка битов. Первые два бита — SUID и SGID, если установлены, разрешают выполнение файла не с правами пользователя, который инициировал процесс, а с правами владельца файла или с правами группы, которой принадлежит файл. Третий бит — *t*-бит — будет описан в *разд. "Особенности назначения прав доступа к папкам Linux" далее в этой главе*.

Использовать права SUID и SGID нужно с крайней осторожностью, постоянно контролируя владельца соответствующих командных файлов. Поскольку неверное их применение может позволить обычному пользователю запустить задачу от имени суперпользователя.

Команды назначения прав доступа Linux

Для настройки прав доступа используются команды `chown`, `chgrp`, `chmod`.

Предоставить (отобрать) права на файл/папку можно командой `chmod`. Обычно в качестве параметров указывают, кому нужно предоставить права (в формате `ugoa` — сначала пользователь, затем его группа, далее группа остальных пользователей, а потом — все пользователи; если этот параметр опущен, то подразумевается назначение прав для всех пользователей), добавить, удалить или назначить — `+`/`-`/`=`, и какие права (варианты — `rwxXst` или в цифровом виде, например, `777`). Чтобы назначить права на все вложенные папки/файлы, добавьте ключ `-R`.

Например, чтобы отобрать права чтения файла для остальных пользователей, выполните

```
chmod o-r файл
```

А для предоставления права запуска файла всем пользователям можно выполнить команду:

```
chmod +x файл
```

Команда `chown` осуществляет смену владельца файла/папки. Обычно ее применяют, когда администратору нужно настроить права доступа для тех объектов, к которым у него нет доступа. Сначала администратор становится владельцем файла, а после этого уже может назначить желаемые права. Пример использования, когда администратор становится владельцем папки /1 и всех вложенных в нее папок и файлов:

```
chown -R root /1
```

Для смены группы у данного файла или папки служит команда `chgrp`.

На первых порах, пока вы не приобретете уверенность в использовании команд назначения прав, можно прибегнуть к программе Midnight Commander для установки необходимых разрешений доступа.

Особенности назначения прав доступа к папкам Linux

Для папок назначаются такие же права доступа, как и для отдельных файлов. Но их реализация имеет некоторые особенности, которые надо учитывать администраторам, обучавшимся на Windows-системах.

Если на каталог предоставлено право чтения (r), то пользователь может узнать список файлов, но не сможет получить информацию об их атрибутах (размере, правам доступа и т. д.).

Право исполнения (x), назначенное на папку, означает возможность просмотра файлов и их атрибутов и их изменения. Но при этом нельзя будет менять названия файлов.

Если на каталог назначено право записи (w), то с файлами можно выполнять любые операции. В том числе можно удалить, переименовать и т. п. файлы, для которых не назначено право доступа соответствующему пользователю. Это представляет собой опасность при публичном доступе к такой папке. Для такой ситуации используется дополнительный бит — так называемый *t*-атрибут *(sticky-бит)*. Если он установлен для папки, то пользователи могут менять только свои файлы.

Специальные атрибуты файлов Linux

Помимо перечисленных выше прав доступа файлы могут иметь специальные атрибуты (табл. 7.6), которые ограничивают некоторые операции с ними. Эти атрибуты поддерживаются в современных версиях Linux, но могут иметь некоторые отличия в реализации в различных клонах.

Таблица 7.6. *Специальные атрибуты файлов Linux*

Атрибут	Описание
-A	Система не меняет значение времени доступа к файлу (atime, access time)
-S	Изменения на диске происходят в синхронном режиме
-a	Файл может быть открыт только для добавления данных. Если атрибут применен к папке, то файлы можно изменять, но не удалять
-i	Запрет любых изменений файла. Если атрибут применен к папке, то уже имеющиеся файлы можно менять, но нельзя удалять файлы или создавать новые
-d	Данный файл будет проигнорирован при создании резервной копии
-c	Использование прозрачной компрессии для файла (внешняя программа работает с несжатыми данными, сжатие/разархивирование производятся при записи/чтении)
-s	При удалении файла занимаемые им участки диска переписываются нулями
-u	При удалении файла система должна сохранить блоки на диске, занимаемые им, для возможности последующей операции восстановления

Для назначения этих атрибутов используется команда chattr. Так, для разрешения только добавления данных к файлу нужно выполнить:

```
chattr +a
```

Для просмотра специальных атрибутов используется утилита lsattr.

Особое внимание к учетной записи оператора резервного копирования

Учетная запись Windows с правами оператора резервного копирования является достаточно серьезной брешью в системе безопасности организации. Как правило, особое внимание "безопасников" уделяется пользователям, имеющим административные права. Да, они могут стать владельцами любой информации, доступ к которой для них явно запрещен. Но при этом такие действия протоколируются и контролируются службой безопасности предприятия. Пользователь, на которого возложена рутинная вроде бы обязанность резервного копирования, легко может выполнить резервную копию *всех данных* и восстановить секретную информацию из этой копии на другой компьютер, после чего говорить о наличии установленных прав доступа к файлам и папкам уже бессмысленно.

Но есть и более простые способы копирования информации, право доступа к которой запрещено на уровне файловой системы. В Windows имеется[1] утилита для массового копирования файлов — robocopy.exe. Эта программа может выполнять копирование данных в режиме использования права резервного копирования (естественно, что она должна быть запущена пользователем, состоящим в группе операторов резервного копирования). В результате в новую папку будут скопированы все файлы, причем пользователю даже не нужно становиться владельцем файлов — все запреты будут уже сняты.

Изначально программа Robocopy предназначена для того, чтобы скопировать структуру файлов из одной папки в другую. Если на файлы наложены ограничения доступа, то выполнять такую операцию штатными средствами (через резервное копирование и восстановление данных) не всегда удобно. Robocopy позволяет переместить данные, сохранив всю структуру прав. Возможность "снятия" ограничений, описываемая в настоящем разделе, просто является одной из функций данной утилиты.

Изменение атрибутов объектов при операциях копирования и перемещения

При операциях копирования/перемещения файлов могут меняться их атрибуты. Неточное понимание вариантов изменения разрешений может привести к незапланированному результату. Так, если при копировании файла он перестанет[2] быть зашифрованным, а вы по-прежнему считаете информацию, содержащуюся в нем, защищенной, то такой факт может привести к неприятным последствиям.

> ***Примечание***
>
> Описываемые далее правила изменения атрибутов имеют смысл только при файловых операциях на дисках с системой NTFS. Если файл копируется/перемещается на

[1] В Windows 7 она входит в состав операционной системы. Для предыдущих выпусков ее можно бесплатно загрузить в составе Resource Kit или просто найти в Интернете.

[2] Такое поведение было свойственно Windows XP, в последующих версиях система выдает предупреждение, что файл после копирования или перемещения будет уже незашифрованным.

диск с файловой системой FAT32 (FAT), то он теряет атрибуты шифрования, сжатия и т. п. Иными словами, после копирования шифрованного файла на дискету он не будет оставаться зашифрованным. Следует учитывать это и при копировании файлов на сетевые ресурсы, поскольку они могут размещаться на дисках с файловыми системами FAT.

Что необходимо учитывать при выполнении файловых операций? По умолчанию вновь создаваемые объекты *наследуют* те разрешения, которые присвоены их родителям. Так, файл будет иметь те же параметры безопасности, что и папка, в которой он создается. Иными словами, если вы создаете новый файл в папке, которой присвоен атрибут "зашифрованный", то этот файл также будет зашифрованным. Или если вы создаете файл в папке, к которой нет доступа пользователю `Иванов`, то и к файлу этот пользователь доступа не получит.

При операциях копирования файл *создается* заново. Поэтому по новому месту он всегда будет иметь атрибуты той папки, в которую скопирован. В результате если вы скопируете зашифрованный файл в незашифрованную папку, то файл в этой папке после завершения операции окажется незашифрованным. Если вы копируете обычный файл в папку с атрибутом "сжатый", то новый файл будет подвергнут динамическому сжатию.

Операции перемещения имеют некоторые особенности. Если файл перемещается с одного *диска на другой*, то операция фактически будет состоять из двух этапов: копирования файла, а потом его удаления с прежнего места расположения. Поэтому атрибуты файлу будут присвоены по правилам операции копирования. Файл будет иметь атрибут той папки, в которую он помещен.

Если файл перемещается в пределах *одного диска*, то операционная система не выполняет операцию копирования. Файл остается на прежнем месте, только в таблице размещения файлов для него меняется соответствующий указатель. Иными словами, все атрибуты файла остаются неизменными. Таким образом при перемещении незашифрованного файла в зашифрованную папку на том же диске информация в файле останется незашифрованной.

Результирующие права и утилиты

Как правило, в организации существует достаточно сложная структура групп пользователей с отличающимися правами доступа к информации. При этом часть прав наследуется от родительских групп, некоторые права прописываются за пользователями или группами явно. А для доступа по сети к совместно используемым ресурсам необходимо интегрировать как права доступа, заданные для файловой системы, так и права доступа совместного использования.

Поскольку обычно пользователь одновременно входит в несколько групп, то определить, получит ли он в итоге право доступа к данному объекту, часто бывает очень сложно. Поэтому в системе введена возможность отображения *результирующего права* пользователя.

Для того чтобы узнать, какие права пользователь (группа) будет иметь по отношению к некоторому объекту, достаточно открыть свойства объекта, на вкладке **Безо-**

пасность нажать кнопку **Дополнительно** и выбрать вкладку **Действующие разрешения**. После чего необходимо выбрать пользователя, для которого будут определяться действующие права, и посмотреть итоговый результат (рис. 7.7).

Примечание

Средствами групповой политики администратор имеет возможность отключения просмотра результирующих прав.

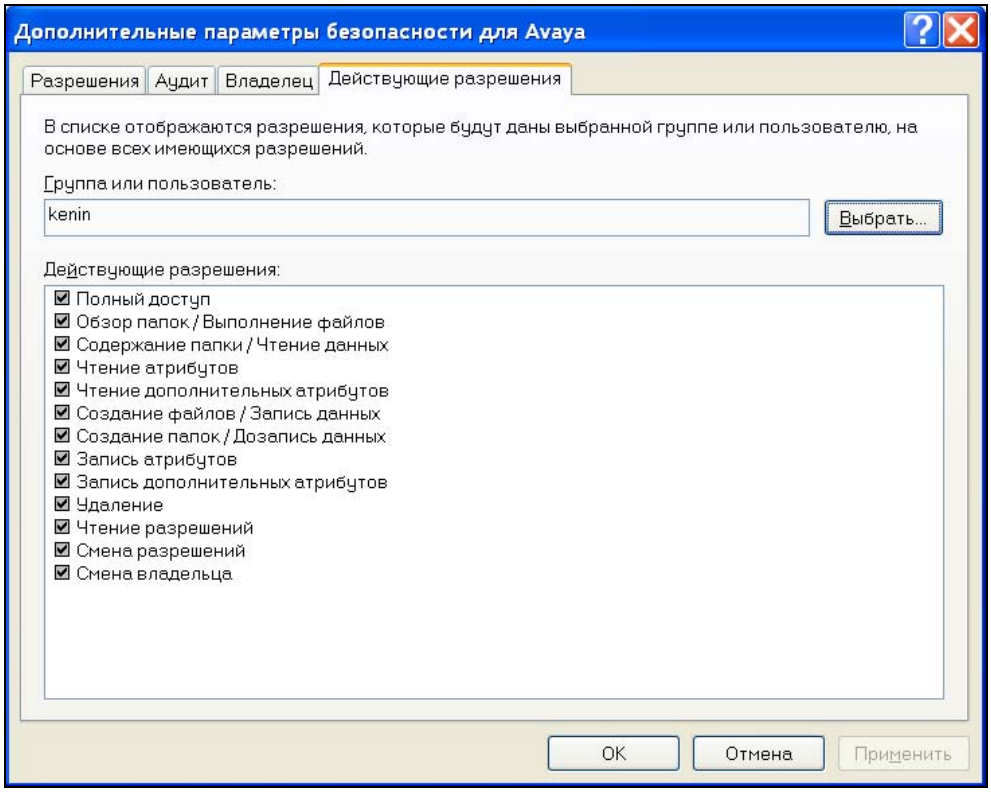


Рис. 7.7. Отображение действующих прав доступа к файлу для выбранного пользователя

Рекомендации по применению разрешений

Общая рекомендация при назначении прав доступа состоит в преимущественном использовании групп по сравнению с назначением прав для отдельных пользователей. Такой подход упрощает администрирование, позволяет гораздо быстрее, проще и понятнее устанавливать разрешения.

Например, для локального компьютера можно создать несколько локальных групп, объединить в них как пользователей данной системы, так и доменные учетные записи, после чего уже с использованием данных групп назначать разрешения на доступ к тем или иным объектам.

В общем случае рекомендуется придерживаться следующего порядка назначения разрешений. Необходимые учетные записи следует добавить в глобальные группы домена, глобальные группы домена включить в локальные группы домена и уже для этих локальных групп назначать желаемые разрешения.

Назначение прав на выполнение операций

Кроме разрешений доступа к файлам, пользователь Windows может быть ограничен в выполнении ряда операций. Например, проверяется наличие у пользователя разрешения на локальный вход в систему и на завершение работы компьютера, на установку нового оборудования и на удаление учетной записи, право на доступ к компьютеру по сети или право на отладку программ и т. д. Причем основная масса прав после установки системы даже не задействована: администратор может использовать имеющиеся параметры при последующей точной настройке системы.

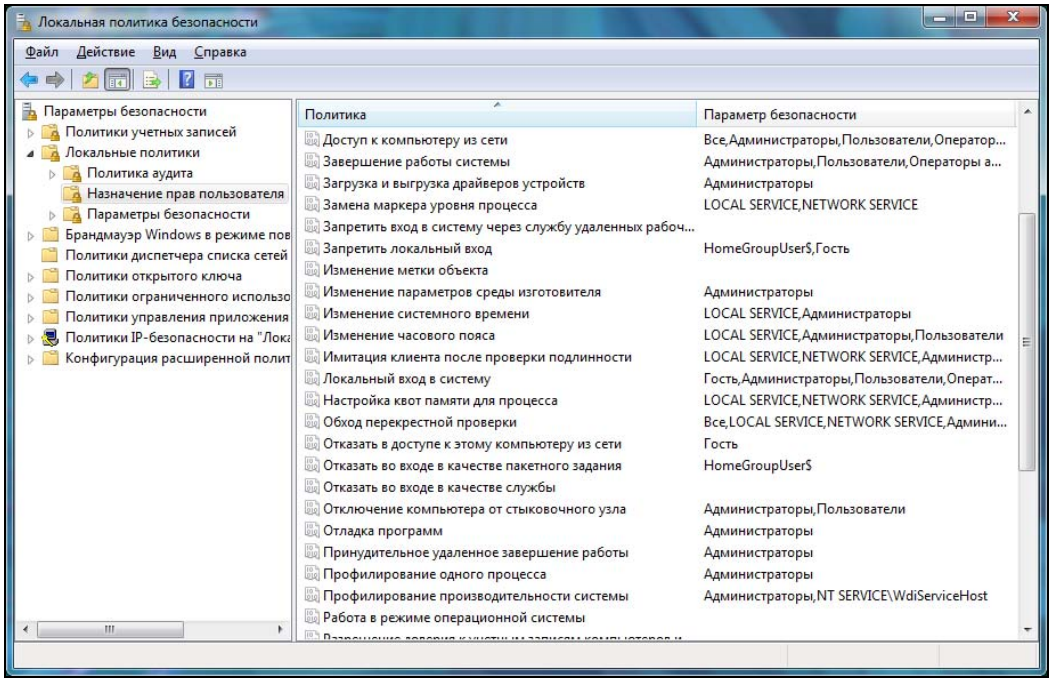


Рис. 7.8. Окно настройки прав пользователя в системе

Права пользователей в системе назначаются через оснастку **Локальная политика безопасности**, расположенную в группе административных задач (рис. 7.8). В случае работы в составе домена администраторы регулируют права пользователей с помощью соответствующих групповых политик. Использование этих инструментов достаточно очевидно, и мы не будем подробно описывать такие операции.

Обход перекрестной проверки

Если пользователю запрещен доступ к текущей папке, но разрешен к вложенной, то он сможет, например, открыть файл из последней, указав явным образом полный путь к нему. Эту особенность принято называть *обходом перекрестной проверки*.

Настройкой параметров безопасности можно запретить данную возможность. Однако такое решение должно применяться только в особых, специально аргументированных случаях, поскольку оно повлечет сбои в работе многих программ (например, невозможность работы в Outlook Web Access).

Администратору следует учитывать данный вариант предоставления прав доступа и правильно настраивать соответствующие параметры.

Утилиты для работы с параметрами безопасности

В этом разделе мы опишем некоторые инструменты, которые используются для регулирования прав доступа.

Стандартные графические утилиты

Для назначения индивидуальных прав используются стандартные графические средства Windows (примеры таких утилит приведены на рисунках этой главы). Думаю, что все администраторы имеют опыт работы по назначению прав доступа к файлам и папкам. Поэтому особо останавливаться на этих средствах мы не будем.

Назначение прав доступа при помощи групповых политик

Параметры безопасности могут быть применены с помощью групповых политик. Групповые политики позволяют централизованно определить:

- **параметры доступа к файловой системе.** Можно установить права доступа и правила аудита на любые объекты файловой системы. Для этого достаточно добавить в папку Файловая система соответствующие объекты и явно указать их параметры безопасности. Таким способом можно задавать централизованно права доступа к папкам на локальных компьютерах;
- **параметры реестра локальной системы.** Данные настройки позволяют установить (если ключ реестра отсутствует, то он будет создан) значение параметра реестра и назначить на него необходимые права доступа. Для создания настройки следует правильно добавить раздел реестра. Если на компьютере, с которого производится настройка, такого раздела нет, его имя можно отредактировать. Только следует проявлять особую внимательность, чтобы исключить возможные ошибки при написании названий разделов, ключей и их значений. Поскольку такие ошибки способны серьезно нарушить работу системы;

- **системные службы.** Настройки в данном разделе позволяют указать параметры запуска служб (режим запуска, параметры учетной записи) и установить для них права доступа;
- **группы с ограниченным доступом.** Эта настройка позволяет централизованно контролировать состав групп. Например, вы можете ограничить состав группы локальных администраторов конкретными учетными записями. И если пользователь попытается (получив тем или иными образом права администратора над локальной системой) внести свою учетную запись в группу администраторов, то такая попытка завершится неудачей.

Кроме того, не забываем, что через групповые политики можно настроить практически любые параметры безопасности: организовать аудит, настроить протоколирование и т. д. Большинство таких операций не представляет особой сложности и легко выполняется в редакторе групповой политики.

Специализированные утилиты

Часто необходимо выполнять операцию над большим количеством объектов, например, в случае увольнения сотрудника заменить его права доступа к файлам в большой структуре папок на аналогичные, но только для другого пользователя (для новой учетной записи). Понятно, что воспользоваться графическими средствами для такой замены можно, но при значительном количестве файлов — практически невозможно.

В таких случаях помогут утилиты, имеющиеся в системе, либо доступные для бесплатной загрузки. Упомянем некоторые из них.

Утилита *icacls*

> ***Примечание***
>
> Такое название утилита имеет с выпусков Windows Vista и Windows Server 2003 SP2. Ранее аналогичная утилита носила название `cacls`.

Утилита позволяет сохранить списки доступа в файл и выполнить обратную операцию — восстановить списки доступа на основе информации из файла.

Возможности сохранения данных в файл в целях архивирования используются редко (информация меняется часто, и такие файлы быстро теряют актуальность). Но эту возможность можно использовать, чтобы произвести поиск и замену каким-либо специальным образом (хотя все можно сделать и ключами команды, но наличие промежуточного этапа позволяет иметь дополнительную точку контроля и возможность создавать какую-либо специальную замену, скажем, для произвольной выборки файлов). Например, заменить права доступа одного пользователя правами другого.

При восстановлении прав следует учитывать, что перечень файлов уже содержится в списке, поэтому команду надо применять *к папке*. Кроме того, не следует упускать из виду, что команда восстановления должна выполняться с повышенными правами.

Пример замены разрешений одного пользователя на другого

Достаточно часто возникает ситуация, когда пользователю был предоставлен специальный набор прав доступа к файлам, а потом данный сотрудник уволился, и необходимо новому пользователю предоставить такой же доступ к файлам, как и прежнему сотруднику. В этой ситуации поможет возможность замены SID при помощи команды `icacls`.

Для этого нужно экспортировать права доступа к файлам в искомой папке, провести замену SID в файле экспорта и потом применить полученный список доступа к папке. Причем вместо SID можно указывать имена учетных записей. Пример такой операции показан в листинге 7.2.

Листинг 7.2

```
C:\>icacls m:\1.txt
m:\1.txt BUILTIN\Администраторы:(F)
NT AUTHORITY\система:(F)
1364\user 0252:(F)

Успешно обработано 1 файлов; не удалось обработать 0 файлов

C:\>icacls m:\1.txt /save acls.bin
обработанный файл: m:\1.txt
Успешно обработано 1 файлов; не удалось обработать 0 файлов

C:\>icacls m: /substitute "1364\user 0252" "MYDOMAIN\Kenin-AM" /restore
acls.bin
обработанный файл: m:1.txt
Успешно обработано 1 файлов; не удалось обработать 0 файлов

C:\>icacls m:\1.txt
m:\1.txt BUILTIN\Администраторы:(F)
NT AUTHORITY\система:(F)
MYDOMAIN\Kenin-AM:(F)
```

Первая команда вывела права доступа к файлу на экран. Далее мы хотим заменить права локального пользователя "1364\user 0252" на аналогичные права доменной учетной записи MYDOMAIN\Kenin-AM. Для этого сначала сохраняем данные в файл, а потом восстанавливаем права с заменой одного SID на другой (явно указывая традиционные названия учетных записей, поскольку учетная запись содержит пробел, то обрамляем ее кавычками). В завершение проверяем результат — у файла права доступа заменены необходимым нам образом.

> ***Примечание***
>
> Замену SID лучше проводить указанным образом, поскольку в некоторых версиях утилиты редактирование сохраненного файла в Блокноте приводило к ошибкам (формат файла в Unicode не имел начальных служебных символов).

Пример поиска файлов, доступных конкретному пользователю

Иногда необходимо проверить, к каким файлам имеет доступ та или иная учетная запись. Для каждого конкретного файла можно посмотреть установленные права, но если необходимо проверить файлы в папке с разветвленной структурой, то такая задача становится сложно выполнимой.

Подобную задачу легко решить с использованием утилиты `icacls`.

Так, чтобы посмотреть список файлов, к которым есть доступ у группы MYDONAIN\TEST, достаточно выполнить команду:

```
icacls <путь к анализируемой папке> /findsid "MYDONAIN\TEST" /t
```

> ***Примечание***
>
> Следует учитывать, что утилита в этом случае будет искать явное вхождение SID в право доступа. Если право доступа к файлам (папкам) предоставляется данной учетной записи через членство в какой-либо группе безопасности, то указанная выше команда не покажет такие файлы/папки.

Пример замены явных прав на наследованные

Часто бывает, что необходимо удалить явно заданные для файлов права доступа и заменить их унаследованными от родительской папки. Это также легко можно сделать командой `icacls`:

```
icacls "имя файла" /reset
```

Утилита *takeown*

Программа позволяет администратору восстанавливать доступ к файлу, если таковой был ему запрещен пользователем. Данная утилита захватывает права владельца, после чего на файл могут быть настроены необходимые права доступа.

Справка по использованию утилиты — `takeown /?`.

Утилита SubInAcl

Утилита SubInAcl позволяет выполнить практически любые настройки прав доступа. Она доступна к бесплатной загрузке по ссылке **http://go.microsoft.com/fwlink/?LinkId=90971**.

Ролевое управление

Для выполнения определенных обязанностей в организации (директора, главного бухгалтера, администратора баз данных и т. п.) пользователю обычно необходимо предоставить целый набор прав по доступу в файловой системе, по возможности запуска тех или иных процессов (открытию приложений) и т. д. Причем часть таких прав будет характеризоваться максимальными возможностями доступа, дру-

гая — представлять только ограниченный набор доступа. Понятно, что выполнение соответствующих настроек, причем часто на нескольких компьютерах, представляет собой трудоемкую операцию.

Для ускорения индивидуальных настроек, соответствующих потребностям бизнеса, используется *ролевое управление*[1]. Ролевое управление представляет собой совокупность прав доступа. Практически роль — это предварительно настроенный набор прав пользователя (по доступу к файловым ресурсам, по возможности запуска процессов на компьютере и т. п.), оптимизированный для выполнения конкретных функциональных обязанностей. Если в системе настроен ролевой доступ, то при приеме на работу нового пользователя его достаточно включить в соответствующую роль. А в случае перехода из одного подразделения в другое — просто заменить одну роль другой.

Создание ролей должно осуществляться прикладным программным обеспечением. В зависимости от варианта реализации роли в системе могут создаваться группы безопасности, соответствующие определенным ролям (традиционный подход) и в которые нужно включать соответствующих пользователей.

Второй способ работы с ролями заключается в применении Диспетчера авторизации.

Служба авторизации Windows позволяет хранить права, соответствующие определенным ролям пользователей, как в службе каталогов, так и в XML-файлах или в базе данных. Примером (единственным, известным автору на момент создания книги) такого варианта управления является гипервизор Hyper-V. По умолчанию

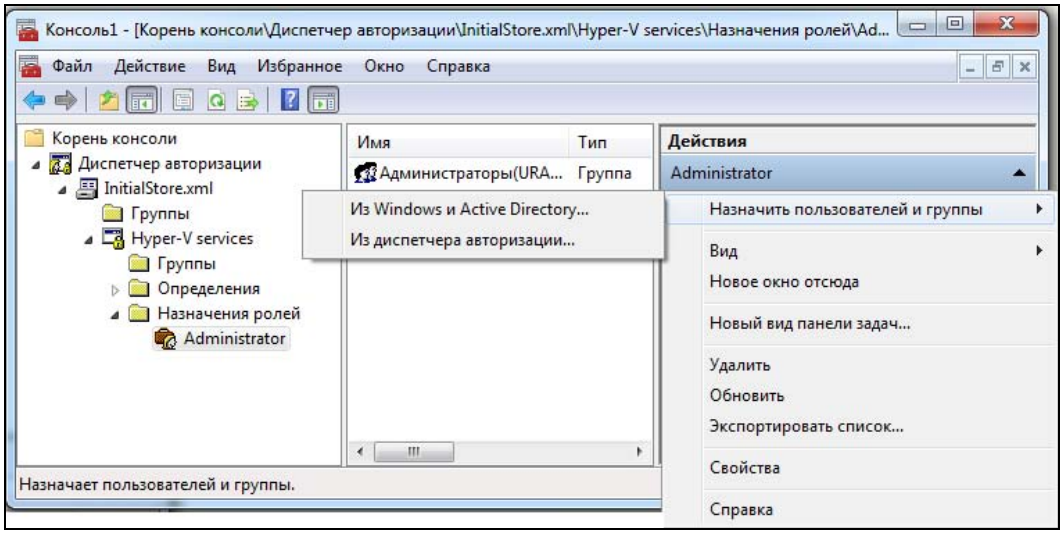


Рис. 7.9. Консоль Диспетчера авторизации (добавление пользователей в роль)

[1] Иногда еще используется термин *управление доступом на основе ролей* (англ. Role Based Access Control, RBAC).

для управления Hyper-V необходимы административные права. Используя ролевые настройки, можно предоставить необходимые права любой учетной записи.

Ролевые настройки для Hyper-V хранятся в файле InitialStore.xml (путь по умолчанию \ProgramData\Microsoft\Windows\Hyper-V\). Для его редактирования нужно запустить Диспетчер авторизации, для чего открыть консоль (mmc) и добавить в нее оснастку Диспетчера авторизации (рис. 7.9).

После чего вы можете создать в программе новую роль, выбрать для нее права (отметить любое количество из 33 наличествующих возможностей) и добавить в эту роль желаемых пользователей.

Сервисные операции управления ролями

Опишем некоторые типовые операции обслуживания информационной системы, связанные с редактированием назначенных прав доступа.

Восстановление параметров безопасности по умолчанию (графический режим)

В случае смены администраторов новому специалисту обычно не известны, например, те изменения прав доступа, которые выполнил прежний сотрудник. В некоторых случаях некорректное назначение прав может повлиять на стабильность работы системы.

В Windows существуют специальные средства, которые позволяют вернуть параметры безопасности к тем значениям, которые определены для вновь устанавливаемой операционной системы. С этой целью используется оснастка **Анализ и настройка безопасности**. По умолчанию эта оснастка не включена в меню. Чтобы начать работу с ней, следует открыть консоль управления (команда `mmc`) и выполнить операцию добавления оснастки. В окне **Добавить изолированную оснастку** следует отметить строку **Анализ и настройка безопасности** и закрыть все последующие окна, нажимая на кнопки подтверждения операции.

В операционной системе хранятся шаблоны безопасности (шаблоны по умолчанию размещены в папке *%windir%*\Security\Templates), разработанные поставщиком, для нескольких типовых конфигураций компьютера. Это шаблон настроек безопасности, соответствующий установке системы, шаблоны безопасности для компьютеров (отдельно для рабочих станций, серверов и контроллеров домена), соответствующие различным уровням защищенности: совместимого с программным обеспечением предыдущих версий и т. д.

Программа позволяет сравнить значения, определенные в этих шаблонах, с фактическими параметрами настройки системы. Полученные результаты сохраняются в виде базы данных, которая может быть проанализирована пользователем: все отличия настроек специально выделены в отчете программы.

Строго говоря, можно проанализировать следующие параметры:

- политики учетных записей — политику паролей, политику блокировки учетных записей и политику Kerberos;

- ❒ локальные политики — политику аудита, назначение прав пользователя и параметры безопасности;
- ❒ журнал событий — параметры журналов приложений, системы и событий безопасности;
- ❒ группы с ограниченным доступом — членство в чувствительных к безопасности группах пользователей;
- ❒ системные службы — запуск системных служб и разрешения для них;
- ❒ реестр — разрешения для разделов реестра;
- ❒ файловую систему — разрешения для папок и файлов.

Если администратор сочтет необходимым, то он может с помощью данной оснастки применить один из шаблонов безопасности — применение шаблона фактически означает установку соответствующих параметров системы (разрешений, прав) в те значения, которые определены в данном шаблоне.

Для анализа или применения настроек необходимо выполнить следующие действия:

1. Создать пустую базу данных.
2. Загрузить в нее желаемый шаблон.
3. Провести анализ и/или настройку системы.

Для применения шаблона следует выполнить команду **Настроить компьютер**. В завершение желательно проанализировать результаты операции.

> ***Примечание***
>
> Обратите внимание на шаблон compatws.inf, который позволяет перейти в режим совместимости с предыдущей версией ОС. В этом режиме учетным записям пользователей даются дополнительные права на доступ к ресурсам системы. В результате появляется возможность запуска программ, не в полной мере совместимых с последними версиями операционной системы. Эта операция в новых ОС разрешена только администраторам, но после применения данного шаблона необходимые разрешения будут предоставлены.

Восстановление параметров безопасности по умолчанию (командная строка)

Произвести сброс параметров безопасности можно и не прибегая к графическому интерфейсу.

Сбросить параметры можно запуском следующей команды:

```
%windir%\system32\secedit.exe /configure /cfg %windir%\repair\secsetup.inf /db
secsetup.sdb /log C:\secedit.log /verbose
```

Эту команду можно использовать и в случае удаленной настройки систем.

Восстановление доступа к ресурсам

В условиях предприятия нередки ситуации, когда необходимо получить доступ к ресурсам, разрешения на использование которых не существует. Это могут быть файлы уволившегося пользователя или ресурсы, ставшие недоступными для всех пользователей вследствие ошибки, произошедшей при наложении разрешений.

Для разрешения подобных ситуаций используется специальное право — право владельца объекта.

Владелец объекта — эта та учетная запись, от имени которой создан данный объект. У владельца объекта есть *неотъемлемое право* — назначать разрешения безопасности. Иными словами, если пользователь создал файл, а потом администратор запретил ему с помощью разрешений безопасности доступ к этому файлу, то пользователь как владелец этого файла сможет в любой момент восстановить работу с данным ресурсом (или предоставить право работы другому пользователю).

Владельца объекта можно заменить. По умолчанию возможностью присвоить себе право владельца объекта обладают только администраторы.

Для получения доступа к объектам в общем случае администратор должен выполнить следующие действия:

1. Сначала стать владельцем этих объектов (выполняется с помощью кнопки **Дополнительно** в настройках безопасности).
2. Воспользовавшись правом владельца объекта, установить для него желаемые разрешения безопасности.

> ***Примечание***
>
> Обратите внимание, что квоты использования дискового пространства рассчитываются согласно владельцам объектов, поэтому после того как для получения разрешения безопасности администратор стал владельцем некоей папки, объем этой папки перешел из квоты пользователя в квоту администратора.

В случае Linux суперпользователь может стать владельцем файла (папки) с помощью команды `chown`. После чего он может откорректировать права доступа к объекту нужным образом.

Удаление неактивных учетных записей

В целях безопасности служба каталогов периодически должна очищаться от неактивных учетных записей, например, от уволенных сотрудников. Существуют бесплатные утилиты, которые позволяют автоматически удалять соответствующие учетные записи, задавая параметр неактивности (например, Free Solarwinds tools). Но подобную операцию легко провести с помощью любого сценария.

Мы опишем один такой способ, реализуемый с помощью PowerShell с установленными модулями взаимодействия со службой каталогов от Quest.

Выбор неактивных учетных записей обычно осуществляется по атрибуту последнего времени входа (lastlogontimestamp). При этом следует учитывать два момента.

Первый — атрибут реплицируется между контроллерами домена со значительным запозданием (примерно на 2 недели). Поэтому реальное время последнего входа может быть несколько иным, чем полученное по запросу к конкретному домену. Однако для упрощения сценария мы пренебрежем этим свойством. Вторая особенность — атрибут может быть пустым, если учетная запись ни разу не входила в домен.

С учетом вышесказанного, один из вариантов сценария по отображению неактивных учетных записей может выглядеть так, как представлено в листинге 7.3.

Листинг 7.3

```
# Зададим количество дней, прошедших с последнего входа в домен (60)
$LastLogon = (get-date).AddDays(-60).ToFileTime()
# Определим LDAP-фильтр для запроса
$Filter =
"(&(objectCategory=person)(objectcategory=user)(|(lastLogonTimestamp<=$LastLogo
n)(!(lastLogonTimestamp=*))))"
# Выполним запрос
Get-QADUser -ldapFilter $Filter -IncludedProperties lastLogonTimestamp |
Select Name,dn,lastLogonTimestamp,AccountIsDisabled | ? {-not
$_.AccountIsDisabled} | Sort-Object Name | ft -AutoSize
```

Для отображения списка неактивных компьютеров можно использовать аналогичный сценарий (листинг 7.4).

Листинг 7.4

```
$LastLogon = (get-date).AddDays(-60).ToFileTime()
$Filter = "(&(objectcategory=computer)(|(lastLogonTimestamp<=$LastLogon)
(!(lastLogonTimestamp=*))))"
Get-QADComputer -ldapFilter $Filter -IncludedProperties pwdLastSet,
useraccountcontrol |
Select Name, pwdLastSet, Description, @{Name="Disabled";
Exp={$_.useraccountcontrol -band 2}}, dn | ? {$_.Disabled -eq 0} | Sort-Object
pwdLastSet | ft -AutoSize
```

Сброс пароля администратора сервера

Иногда возникает необходимость смены пароля администратора. Эта операция может быть выполнена как для Windows, так и для Linux-систем.

Сброс пароля администратора Windows

Для Windows существует несколько утилит, позволяющих заменить пароль администратора (в том числе и администратора домена). Эти программы просто записывают новый пароль в соответствующие базы сервера, для чего используется доступ

к ним при отключенном контроле операционной системы (при загрузке с внешнего устройства).

Среди бесплатно распространяемых программ можно отметить Offline NT Password Editor (**http://pogostick.net/~pnh/ntpasswd/**), которая неоднократно успешно применялась автором для восстановления паролей на различных версиях системы — начиная от NT 4.0. С этого сайта вы можете скопировать себе образ загрузочного диска (если компьютер оборудован дисководом гибких дисков, то образы для диска есть, в общем случае придется закачивать образ загрузочного компакт-диска, но все равно объем закачки составит порядка 3 Мбайт).

После загрузки образа его необходимо "прожечь" на матрицу компакт-диска (или записать на USB-устройство, если система поддерживает такой запуск). Стартовав с такого компакт-диска, вы получаете доступ к реестру системы и можете заменить любой пароль. По умолчанию опции программы предполагают смену пароля локального администратора. Так что вам достаточно только соглашаться с предложениями программы на каждом ее шаге.

Обратим внимание только на некоторые особенности этого процесса.

Обычно на компьютерах с предустановленной Windows 7 создается специальный небольшой раздел для загрузки системы. Объем его составляет порядка 100 Мбайт. Сама же операционная система располагается на втором разделе. Программа смены пароля по умолчанию предлагает выбрать первый раздел. Поэтому вам нужно оценить размеры разделов, которые будут показаны программой, и указать нужный (на рис. 7.10 выделены список разделов и строка, в которую нужно ввести ваш выбор — по умолчанию в ней отображается раздел с номером 1, нужно же ввести 2).

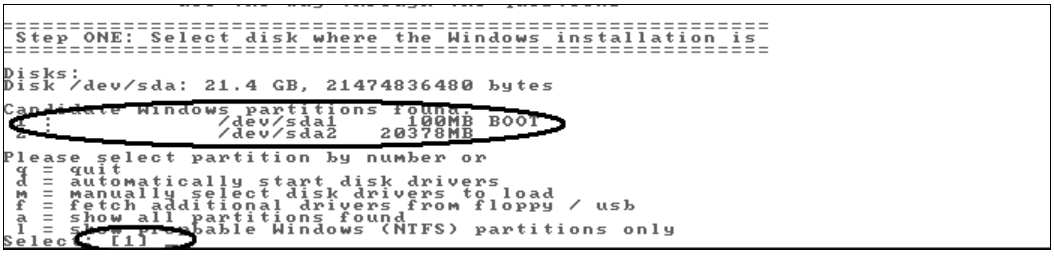


Рис. 7.10. Выбор раздела с операционной системой

Примечание

Если вы хотите сменить пароль, то необходимо соблюсти требования политики паролей, которая присутствует в системе (например, минимальную длину пароля). Поэтому лучше всего не редактировать пароль (устанавливать новое его значение), а просто удалить его (будет использован вход с учетной записью без указания пароля).

Обратите внимание также на параметры блокировки учетных записей. Иногда учетные записи локальных администраторов блокируются (например, централизованно в домене групповыми политиками). В этом случае, чтобы зайти с ее помощью в систему, надо не забыть снять блокировку в данной программе (статус учетных записей отображается на экране).

Не забудьте после завершения операций сброса пароля сохранить изменения (ввести **Y** на предложение сохранения результатов). После перезагрузки системы в нормальном режиме вы сможете получить к ней доступ.

Заметим, что в случае локализованных версий программа отобразит на экране "бессмысленный" набор символов вместо имени учетной записи. Это единственный неудобный момент в использовании утилиты.

> ***Примечание***
>
> При смене пароля в Windows следует учитывать, что если на компьютере имелись файлы или папки, зашифрованные с использованием свойств файловой системы (EFS), то они после смены пароля станут недоступными. Принципиально можно попытаться подобрать к ним пароль, применяя одну из утилит восстановления пароля к EFS, но такая попытка будет удачна только в том случае, если пароль был выбран недостаточно сложным (хотя к таковым, по практике автора, относится подавляющее число паролей пользователей).

Сброс пароля учетной записи root

Смену пароля учетной записи суперпользователя можно сделать штатными средствами системы. Для этого необходимо иметь доступ к консоли системы и загрузить ее в однопользовательском режиме.

В большинстве систем сегодня используют загрузчик на основе Grub. В этом случае необходимо при запуске компьютера войти в меню загрузки (обычно нажать клавишу <Esc> при отображении соответствующей записи), выбрать в вариантах загрузки ту строку, которая начинается с `kernel`, открыть ее для редактирования (нажать клавишу <e>). В конец строки параметров загрузки следует добавить символ "S", сохранить изменения (нажать клавишу <Enter>) и загрузиться в этом варианте (нажать клавишу <b>). Перед вводом команды смены пароля необходимо убедиться, что жесткий диск подключен в режиме записи-чтения (командой `mount`), в противном случае выполнить

```
mount -o remount, rw /диск
```

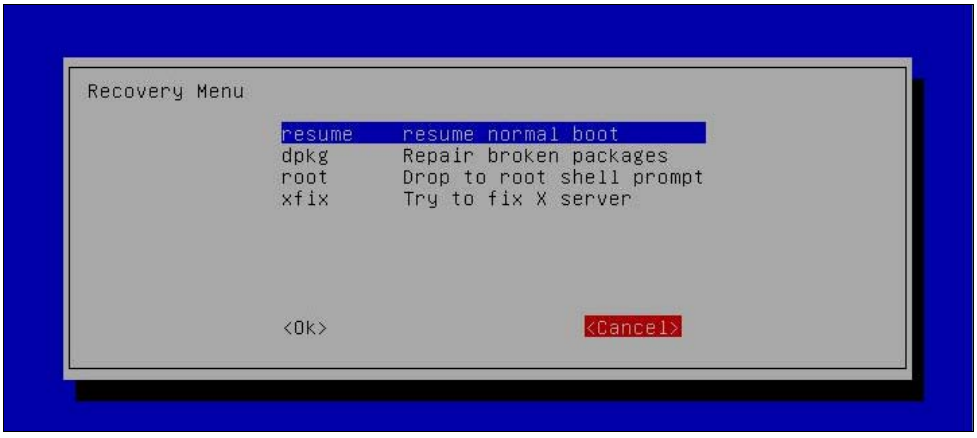


Рис. 7.11. Меню загрузки Ubuntu

Если вы используете Ubuntu, то для сброса пароля следует войти в режим восстановления (зайти в меню загрузки системы и указать второй вариант загрузки). После выполнения ряда команд на экран будет выведено приглашение выбора варианта дальнейшей загрузки (рис. 7.11). Необходимо выбрать третью строку (`root Drop to root shell prompt`).

После завершения загрузки по этому варианту вы войдете в режим консоли с правами суперпользователя. Здесь вы можете сменить пароль суперпользователя командой `passwd`, после чего перезагрузить систему и войти в нее с полными правами доступа.

Изоляция приложений

Для обеспечения повышенной безопасности информационных систем разработчики предпринимают много усилий по контролю запущенных приложений.

Контроль приложений Windows

В Windows, помимо описанного ранее назначения прав на выполнение операций, реализован механизм контроля приложений. В корпоративной версии Windows этот компонент называется AppLocker, в других версиях данная технология реализуется путем настройки параметров политик ограниченного использования программ. Оба этих решения позволяют администраторам настраивать контролируемый запуск программ и процессов.

Консоль AppLocker запускается из редактора объектов групповой политики: **Конфигурация компьютера | Настройки Windows | Настройки безопасности | Политики управления приложениями | AppLocker**. По умолчанию правила регулирования программ не настроены.

Правила контроля программ могут применяться к исполняемым файлам (*.exe), сценариям (*.bat, *.cmd, *.vbs, *.js, *.ps1), файлам инсталляторов (*.msi, *.msp) и системным библиотекам (*.dll, *.ocx).

В AppLocker предусмотрены три типа правил: правила издателя (Publisher Rules), правила пути (Path Rules) и правила хэша (File Hash Rules).

Правила пути позволяют регулировать запуск приложений по пути их исполняемого файла. Например, можно разрешить запуск только программ из папки Program Files. Данное правило следует назначать с учетом наличия или отсутствия у пользователя возможности самостоятельно устанавливать программы и/или дописывать файлы в определенные папки.

Правила пути могут настраиваться с использованием системных и пользовательских переменных окружения и знаков подстановок (`?` и `*`). Основная сложность в использовании данного типа правил заключается в том, что на практике достаточно сложно заранее определить все пути запуска программ, например, предусмотреть, что пользователь сможет запустить программу с сервера. Соответственно, сопровождение данного типа правил достаточно трудоемко.

Правила хэша основаны на использовании криптографической хэш-функции. Для приложения вычисляется хэш-функция исполняемого файла, которая проверяется при запуске программы. Любое изменение файла (подмена его, заражение вирусом и т. п.) приведет к изменению хэш-функции и отказу от запуска. Основной недостаток данного правила — необходимость коррекции после установки каждого обновления или заплатки (поскольку меняются исполняемые файлы).

Правила издателя задают ограничения на запуск программ на основе цифровой подписи от разработчика. Правила напоминают правила сертификатов, но несколько отличаются от них и позволяют настраивать запуск с учетом вендора, названия продукта, его версии. Естественно, что исполняемые файлы должны иметь соответствующие цифровые подписи, чтобы такое правило можно было создать. В настоящий момент подписи обычно ставят только крупные вендоры программного обеспечения.

В каждом правиле можно указать исключения, причем исключение может быть основано на правиле другого типа.

Безопасная среда исполнения Linux

В Linux большое внимание уделяется тому, чтобы запущенное приложение не смогло нанести вред системе в целом.

Для этого приложение "помещали" в специальное окружение, которое препятствовало выполнению операций, не предусмотренных администратором. Например, изолировало от приложения файловую систему (chroot). В настоящее время существуют две технологии создания безопасной среды выполнения. Это SELinux, разработанный в содружестве с National Security Agency (NSA) и используемый в ОС Red Hat. И пакет AppArmor (**http://en.opensuse.org/FAQ#AppArmor**), разработанный Novell (OpenSUSE) и используемый в Ubuntu.

Идея, реализованная в AppArmor, очень проста. Приложение запускается в специальном режиме в надежных условиях, когда есть уверенность в отсутствии каких-либо вредоносных кодов. Работа в приложении происходит "под наблюдением" специальной программы, которая фиксирует всю активность. Эта активность сравнивается с теми разрешениями, которые установлены для программы (говорят, что для прикладной программы создан *профиль защиты*). Любой доступ, не предусмотренный профилем защиты прикладной программы, блокируется.

Пакет AppArmor устанавливается на сервере по умолчанию и включается для некоторых программ (например, для защиты DNS-сервера). С его помощью можно защитить любые другие программы.

Для включения защиты AppArmor для какой-либо программы необходимо иметь ее профиль. Для наиболее популярных пакетов существуют подготовленные профили, которые можно загрузить командой

```
sudo apt-get install apparmor-profiles
```

В общем случае профиль для программы можно сформировать самостоятельно. Принцип создания прост, хотя для этого может потребоваться достаточно длитель-

ный период времени на отладку и тестирование. Прикладная программа запускается в контролируемом режиме, при этом все ее действия протоколируются, например, доступ к каким-либо файлам, вызов других программ и т. п. На основе анализа этих записей специальной утилитой создается профиль программы. Далее обучение продолжается с учетом созданных настроек профиля. По истечении некоторого периода тестирования, когда вы посчитаете, что с использованием программы выполнялись все возможные операции, режим обучения прекращается, создается окончательный профиль и работа программы переводится в режим полной защиты.

> ***Примечание***
>
> Режим обучения называется *complain*, режим защиты — *enforce*, если программа не контролируется и не тестируется в режиме обучения, то ее статус показывается как *not confined*.

Указанные операции выполняются при помощи следующих команд:

- просмотр списка пакетов, для которых используется режим AppArmor:

  ```
  sudo apparmor_status
  ```

- создание профиля защиты и включение режима обучения для программы (путь к исполняемому файлу программы можно отобразить, набрав команду `which` *программа*):

  ```
  sudo aa-genprof /путь_к_исполняемому_файлу_программы
  ```

Утилита предложит вам получить данные из репозитория профилей, после чего создаст начальный профиль программы и переведет ее в режим обучения. Для обучения вам необходимо запустить программу в другой консоли, не закрывая `aa-genprof`, и выполнять типовые операции. Для внесения изменений в созданный профиль нужно вернуться в окно команды `aa-genprof` и выполнить операцию `Scan`.

Если программа, для которой проводится обучение, вызывает, в свою очередь, другую программу, то при сканировании журналов вам будет предложено либо `Inherit` — использовать профиль основной программы для вызываемой, либо `Profile` — создать новый профиль, либо `Unconfined` — запустить эту программу без защиты AppArmor. Последний вариант не стоит выбирать, поскольку вы решили защищать основную программу. Оптимальный вариант — создание собственного профиля.

Вам придется ответить также на ряд вопросов, разрешая или запрещая определенный доступ для программы. После чего вы можете либо продолжить режим обучения, либо завершить его (выбрав команду `Finish`). Это переведет программу в режим защиты.

- Если вы хотите перевести программу в режим обучения, то выполните:

  ```
  sudo aa-complain /путь_к_исполняемому_файлу_программы
  ```

- Чтобы внести изменения в профили программ, нужно использовать следующую команду:

  ```
  sudo aa-logprof
  ```

- Перевод конкретной программы в режим защиты осуществляется по команде:

```
sudo aa-enforce /путь_к_исполняемому_файлу_программы
```

Если на сервере существует профиль защиты для программы, то отключить защиту можно, если создать ссылку на этот профиль в папке /etc/apparmor.d/disable (в ней хранятся отключенные профили), например, командой:

```
sudo ln -s /etc/apparmor.d/имя_профиля /etc/apparmor.d/disable/
```

Для включения отключенной таким образом защиты необходимо просто удалить эту ссылку. После чего включить для программы защиту, загрузив профиль командой `apparmor_parser -a` с указанием имени профиля.

Чтобы отключить защиту без перезагрузки сервера, нужно задать команду:

```
sudo apparmor_parser -R /etc/apparmor.d/имя_профиля
```

ГЛАВА 8

Почтовая система предприятия

Наличие почтового обслуживания стало сегодня обязательным атрибутом любой информационной системы.

Варианты почтового обслуживания

Существует несколько вариантов организации электронной почты для малых и средних организаций.

Бесплатные почтовые серверы Интернета

Как правило, у каждого пользователя создано не по одному ящику бесплатной электронной почты. Такие ящики пригодны как для обмена сообщениями внутри организации, так и для общения с внешним миром. Неоспоримый плюс такого решения — простота и достаточно высокая надежность при доступности информации с любой точки Интернета.

Среди недостатков можно отметить не столь высокую скорость обмена сообщениями, как в локальной сети, необходимость дополнительных расходов в случае оплаты трафика по объему, неудобные адреса (из-за занятости коротких имен на наиболее популярных серверах), отсутствие средств групповой работы и т. д. Ну и, конечно, указание бесплатных адресов в контактах фирмы часто воспринимается как свидетельство не очень "серьезной" организации.

Облачное почтовое обслуживание

В настоящее время на рынке доступно много предложений по размещению ресурсов организации в "облаке". Одним из наиболее известных ресурсов является Google Apps. В отличие от бесплатных почтовых сервисов подобные предложения обеспечивают:

- заключение договора с гарантией доступности ресурсов;
- предоставление в аренду дискового пространства (увеличенные квоты по сравнению с бесплатными ресурсами);

- возможность использования собственного доменного имени;
- предоставление услуг корпоративного взаимодействия (общие календари, задачи, адресные книги и т. д.);
- возможность подключения дополнительных приложений (например, ПО поддержки проектов, ПО обеспечения взаимодействия с клиентами — CRM и т. д.).

Стоимость облачных услуг сравнима с ценой поддержания аналогичных систем в самой организации.

Размещение почтового сервера у провайдера

Данный вариант предполагает получение почты на домен организации на сервер провайдера с последующей пересылкой на локальный почтовый сервер или с непосредственным доступом к почтовым ящикам самих пользователей.

Вариант предпочтителен тем, что провайдер обеспечивает повышенную надежность и доступность сервера, что трудно обеспечить в небольшой организации. При условии последующей ретрансляции почты стоимость услуги весьма незначительна.

Собственный почтовый сервер

Собственный почтовый сервер имеет то преимущество, что выбирать его функционал, выполнять точную настройку и т. п. каждая организация может "под себя". Однако при выборе данного варианта необходимо обеспечить надежность его функционирования: если почтовый сервер откажет, то на время его простоя почта на организацию просто не будет доставляться.

Установка собственного почтового сервера требует регистрации домена организации и соответствующей настройки MX-записи (указывает на адрес почтовой системы домена).

Кроме собственно настройки служб обмена сообщениями, администратору необходимо принять меры к защите от спама и для фильтрации почтового трафика от вирусов и иных зловредных вложений. Соответствующие рекомендации описаны далее в этой главе.

Протоколы для работы с почтовыми ящиками

Почтовые серверы обмениваются друг с другом сообщениями по протоколу SMTP (Simple Mail Transfer Protocol, простой протокол передачи почты). Существуют варианты безопасного протокола (с шифрованием), различные разработки дополнений, призванных так или иначе аутентифицировать серверы и т. п. Но реально большинство серверов работает в соответствии со стандартом SMTP. Протокол задействует для работы порт 25, который необходимо открыть на соответствующих межсетевых экранах.

Почтовые серверы могут предоставлять почтовые ящики пользователям по разным протоколам, серьезно отличающимся сервисными возможностями. Дадим им краткую оценку, чтобы вы могли осознанно выбирать опции конфигурации при настройке почтовых серверов.

- **POP3** (Post Office Protocol 3, протокол обслуживания почтового офиса) — наиболее распространенный протокол для чтения сообщений с почтовых серверов Интернета. Обычно используется пакетный прием сообщений: все письма копируются на компьютер пользователя и удаляются затем с сервера. Позволяет загружать письма *только* из папки **Входящие**. Существует вариант протокола с шифрованием трафика: POP3S.

  На корпоративных серверах данный протокол лучше отключать, чтобы почтовые сообщения не переносились автоматом на компьютеры пользователей (это обычно настройка по умолчанию для почтовых клиентов, работающих с протоколом POP3).

- **IMAP** (Internet Message Access Protocol, протокол доступа к сообщениям Интернета) — при подключении по этому протоколу пользователь может не только читать входящую почту, но и создавать дополнительные папки на почтовом сервере. Это более удобный вариант работы с почтой, поскольку дает возможность организовать структуру папок с сообщениями, "читать" папки специальной конфигурации — контакты и т. п., выбирать отображаемую на локальной машине структуру папок и т. д.

- **HTTP** (Hypertext Transfer Protocol, протокол передачи гипертекста) — возможность работы с почтовым ящиком через программу обозревателя Интернета (Mozilla Firefox, Opera, MS Internet Explorer и т. п.).

  При работе по протоколу HTTP объем передаваемой и принимаемой информации существенно выше, чем при чтении почты с помощью POP3 или IMAP. Кроме того, каждое сообщение необходимо индивидуально загружать в окно программы для прочтения. Все это существенно снижает скорость работы с почтовым ящиком (по сравнению с традиционным почтовым клиентом). Но поскольку протокол открыт в программах межсетевых экранов, это позволяет получить доступ к почтовому ящику практически из любого места.

  Также существует безопасный вариант с шифрованием трафика — HTTPS.

- **"Поддержка MS Exchange"** — работа с почтовым сервером Microsoft Exchange осуществляется на основе функций удаленного вызова процедур (RPC, Remote Procedure Call). Этот вариант обозначается в настройках Outlook как "поддержка MS Exchange". Протокол встречается практически только в локальных сетях, поскольку требует динамического открытия большого числа портов. Начиная с Windows Server 2003/Exchange 2003, предусмотрена возможность работы RPC поверх протокола HTTP. Это позволяет организовать доступ к корпоративной сети через Интернет на основе полнофункциональных версий программы Outlook. Такой вариант требует большого количества дополнительных настроек почтового сервера, прокси-сервера RPC и описан подробно в KB833401

и в специальном руководстве (**http://www.microsoft.com/downloads/details.aspx?FamilyId=EF58395D-3710-49CF-9698-938E2BEF39E8&displaylang=en**).

Корпоративные почтовые системы

Современные почтовые системы перестают выполнять только функции пересылки сообщений электронной почты. При этом к серверам корпоративного уровня предъявляются специальные требования по обеспечению надежной работы служб в условиях крупной организации: возможность кластеризации сервера, распределения данных по нескольким базам (для снижения времени обслуживания в случае повреждения отдельных элементов), дополнительные возможности по восстановлению (технологии восстановления отдельных почтовых ящиков и сообщений, наличие специальных интерфейсов для взаимодействия с антивирусными службами и т. д.

Среди коммерческих корпоративных почтовых серверов можно выделить двух лидеров: IBM Lotus Notes и Microsoft Exchange Server. Одним из наиболее функциональных серверов корпоративного взаимодействия бесплатного сегмента является Zimbra[1] Collaboration Suite.

Сервисы корпоративной почты

Электронная почта в организациях перестает быть только средством передачи сообщений. Она все более приобретает черты программного продукта, обеспечивающего корпоративное взаимодействие. Можно упомянуть следующие характеристики, которые фактически стали стандартом для корпоративной электронной почты:

- поддержка подключения к электронной почте по всем стандартным протоколам, в том числе мобильных клиентов (с предоставлением экономичного, мобильного интерфейса), телефонов и т. п.;
- единые адресные книги организации;
- предоставление сведений о занятости сотрудников, ведение календарей сотрудников и групп;
- возможности организации совещаний (планирования мероприятий);
- создание поручений и отслеживание их исполнения;
- совместный доступ к документам и обсуждениям

и т. п.

[1] После покупки компанией VMware стала активно развиваться и коммерческая ветка продукта — Zimbra Network Edition. Эта редакция отличается добавлением ряда модулей, состав которых можно уточнить по ссылке **http://www.zimbra.com/products/compare_products.html**.

Почтовый сервер Microsoft Exchange

Почтовый сервер от Microsoft для доменов Windows — Exchange. Текущая (на момент подготовки книги) версия — Exchange 2010.

Преимущество данного сервера заключается в его интеграции с другими решениями от Microsoft: во-первых, со всеми офисными продуктами, в том числе с порталом, во-вторых, с решениями IP-телефонии, мгновенных сообщений, в-третьих, с продуктами межсетевых экранов (Forefront TMG), обеспечения безопасности и т. д. Сам сервер глубоко интегрируется в службу каталогов, и поэтому следует тщательно планировать его разворачивание.

Почтовая служба Microsoft Exchange может быть распределена по нескольким серверам, выполняющим различные функции (например, пограничный сервер обмена сообщениями). Для небольшой и средней организации все роли могут быть сосредоточены на одном сервере.

Для управления сервером используется графическая консоль (рис. 8.1), при этом определенная часть операций может быть выполнена только из командной строки с использованием командлетов PowerShell.

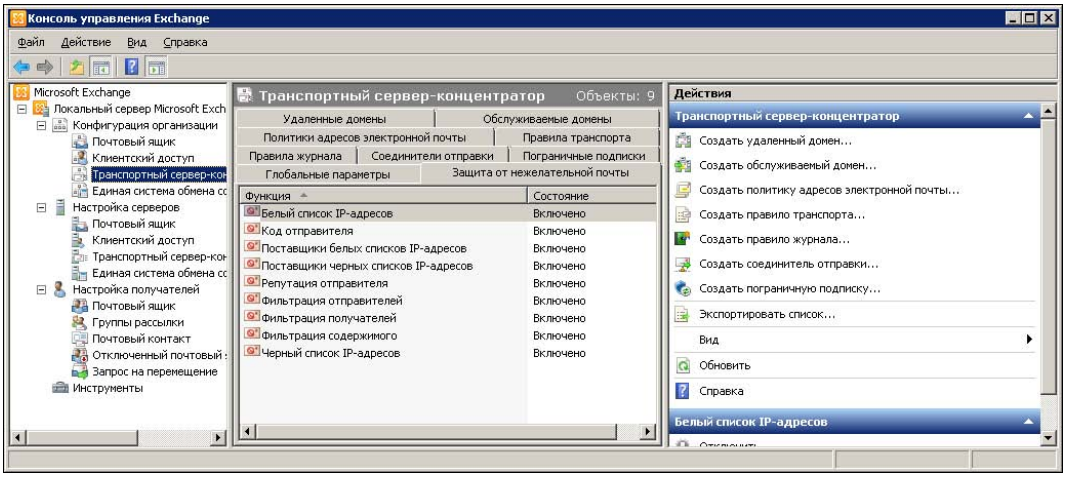


Рис. 8.1. Пример окна консоли управления Exchange Server 2010

Сервер является достаточно сложным в сопровождении. Поэтому за недостатком объема мы не будем рассматривать вопросы его настройки и отошлем читателя к документации разработчика — **http://technet.microsoft.com/ru-RU/library/bb124558**.

Обратим особое внимание администраторов на лицензирование сервера Exchange. Этот продукт требует как покупки серверной лицензии (которая, в сущности, примерно соответствует стоимости операционной системы), так и клиентских лицензий для *каждого пользователя*. При этом на момент подготовки книги стоимость клиентской лицензии более чем в 2 раза превышала стоимость клиентской лицензии на подключение к Windows-серверу. Также следует учитывать, что наибольший

функционал Exchange-сервера реализуется при подключении к нему Microsoft Outlook в качестве клиента, который также является коммерческим продуктом.

Zimbra Collaboration Suite

Описание бесплатного пакета Zimbra Collaboration Suite (ZCS) доступно на сайте **http://www.zimbra.com/**. Там же присутствуют ссылки на загрузку установочного пакета.

Для взаимодействия с ZCS может быть использован любой почтовый клиент, работающий по стандартным протоколам (HTTP, POP3, IMAP, iClalendar) — Thunderbird, Outlook Express (или полная его версия) и т. д. Но максимальная функциональность реализуется при доступе с использованием обозревателя Интернета или собственного, также бесплатного клиента. Причем из практики работы предпочтительным обозревателем Интернета является Firefox, поскольку в Microsoft Internet Explorer медленнее отрабатывает Java-сценарии, особенно на не очень производительных компьютерах.

Возможности совместной работы в ZCS

ZCS обеспечивает не только обмен почтовыми сообщениями. ZCS это:

- электронная почта, позволяющая создавать и отправлять почтовые сообщения, отслеживать сообщения с помощью функции "Разговор", присоединять вложения, осуществлять поиск сообщений и вложений по конкретным характеристикам или указанному тексту, создавать собственные папки и теги для систематизации почты, создавать фильтры для направления входящей почты по различным папкам;
- "Адресная книга", для создания собственных списков контактов с возможностью работы со службами глобальных каталогов;
- функция "Ежедневник" (с возможностью создания и управления несколькими ежедневниками), позволяющая планировать встречи и собрания, просматривать расписания занятости других пользователей;
- функция "Задачи", позволяющая создавать списки задач, устанавливать приоритеты и отслеживать выполнение;
- функции "Папки документов" и "Портфель", позволяющие хранить в почтовом ящике документы пользователя и самому пользователю организовать совместную работу с ним, предоставляя соответствующие права доступа

  и т. д.

В состав ZCS включены бесплатные антивирусный модуль и обучаемый модуль проверки на спам, которые осуществляют проверку всей почты.

Пакет ZCS может быть настроен для работы в домене Windows (аутентифицировать пользователей в домене, использовать глобальный адресный лист, обмениваться информацией о занятости пользователей), в том числе возможна настройка

совместной работы с Microsoft Exchange, когда часть пользователей обслуживается ZCS, а другая — MS Exchange (для снижения числа необходимых клиентских лицензий).

Интерфейс ZCS полностью локализован. При наличии обозревателей, не вполне поддерживающих новые технологии Ajax, Java, или на медленных соединениях, можно переключиться на "классический" HTML. Имеется специальный интерфейс для подключения мобильных клиентов (КПК).

Пакет ZCS объединяет в себе многие открытые решения: Postfix в качестве агента передачи сообщений, OpenLDAP для аутентификации, MySQL как сервер базы данных, ClamAV и SpamAssassin для фильтрации почты, Jetty в качестве сервера веб-приложений и др. Консоль администрирования и пользовательская веб-консоль доступа к почте написаны на Java.

Установка Zimbra

Самый простой вариант установки ZCS — инсталляция полного комплекта на один сервер. Такая конфигурация достаточна для обслуживания нескольких сотен пользователей.

Для установки[1] ZCS подойдет любой компьютер с процессором частотой более 2 ГГц и оперативной памятью 2—4 Гбайт. Объем дискового пространства должен обеспечивать хранение почтовых ящиков пользователей. При этом нежелательно формировать RAID 5-го уровня из-за не очень высокой его производительности.

Для установки желательно использовать подготовленные вендором пакеты для соответствующей операционной системы. При желании можно выполнить установку и их исходных кодов, но такая операция, особенно при выборе операционной системы, отсутствующей в списке готовых пакетов, требует хорошей подготовки администратора Linux.

Требования к операционной системе

Для установки следует использовать ту версию операционной системы, для которой существует подготовленный разработчиком пакет. В случае Ubuntu (на момент подготовки книги) — это Ubuntu 10.04 TLS. Лучше использовать 64-разрядную версию ОС.

> ***Примечание***
>
> При желании можно воспользоваться готовыми виртуальными машинами с уже установленным пакетом ZCS, например, со страницы **http://www.turnkeylinux.org/messaging**.

Установку Ubuntu нужно провести со значениями по умолчанию. Для удаленного управления нужно включить OpenSSH-сервер (выбрать его среди устанавливаемых

[1] Мы приводим оценку требуемых параметров из условия размещения на сервере почтовых ящиков примерно 200 пользователей. На практике требования к аппаратному обеспечению могут быть несколько иными.

компонентов). Установку других пакетов можно не проводить (например, веб-сервер устанавливается в составе пакета ZCS).

Для безошибочной установки ZCS необходимо:

- при разбиении дисков на Ubuntu выделить для swap-раздела объем в 2 раза больший установленного объема оперативной памяти;
- назначить статические адреса сетевых интерфейсов;
- прописать в файле hosts за сервером Ubuntu полное и краткое имена, обратив внимание, чтобы соответствующая строчка была указана не за локальным адресом (127.0.0.1), а за реальным: `192.168.10.34 mail.mydomain.com mail`;
- убедиться, что разрешение имен правильно работает, определяет сервер по краткому и полному именам и "видит" MX-запись почтового домена (проверить командами `hostname` и `hostname -f`, которые должны вывести краткое и полные имена соответственно). Если в организации отсутствует DNS-сервер, то его можно установить в Ubuntu и прописать на нем домен организации;
- установить имеющиеся обновления (`apt-get update && apt-get upgrade`).

Установка пакета ZCS

Загруженный с сайта разработчика установочный пакет нужно разархивировать, перейти в папку установки и запустить сценарий install.sh:

```
tar xzvf <имя_пакета_установки>.tgz
cd <имя_пакета_установки>
./install.sh
```

Программа установки проверит наличие необходимых компонентов и предложит установить их. Например, при установке на новую систему Ubuntu потребовались пакеты libgmp3c2, libstdc++5, libltdl3. Мы не стали приводить список требуемых пакетов, поскольку он меняется в различных версиях; проще посмотреть список неудовлетворенных зависимостей, выводимый сценарием, и выполнить установку отсутствующих приложений.

В случае удовлетворения всем требованиям сценарий предложит подтвердить установку необходимых пакетов и модернизировать систему. Нужно согласиться (можно просто нажимать клавишу <Enter> до момента ответа на запрос "Continue", когда нужно будет явно нажать клавишу <Y>).

Обратите внимание, что сценарий установки по умолчанию предлагает создать почтовый домен с именем, совпадающим с именем хоста, на котором производится разворачивание Zimbra. Если вы хотите создать почтовое обслуживание *домена* Windows или Linux, то введите его имя на запрос в сценарий (в любом случае после установки Zimbra почтовые домены можно создать средствами административного управления).

После этого на экране появится меню, в котором будут описаны все параметры установки (для раскрытия меню нажмите цифровую клавишу, соответствующую номеру пункта меню, а затем клавишу <Enter>). Те позиции, для которых необходимо

указать параметры, будут отмечены звездочками. По умолчанию предлагается только назначить пароль администратора. В листинге 8.1 в целях экономии приведена только часть меню настройки Zimbra.

Листинг 8.1

```
Main menu

1) Common Configuration:
2) zimbra-ldap: Enabled
3) zimbra-store: Enabled
+Create Admin User: yes
+Admin user to create: admin@ack.ack
******* +Admin Password UNSET
+Enable automated spam training: yes
....
```

Для изменения параметра нужно перейти в соответствующий пункт (переход нажатием клавиши с номером меню; так для назначения пароля администратора нужно будет сначала ввести `3`, а потом, в новом меню, — `4`) и ввести нужные значения. Возврат в меню нажатием клавиши <r>. После редактирования следует сохранить изменения конфигурации (вводом команды `a` — от англ. *apply*) и дать согласие на изменение конфигурации системы.

Успешность установки можно проверить командой `zmcontrol status`. Все службы должны быть запущены (листинг 8.2).

Листинг 8.2

```
sudo -s
sudo — zimbra
zmcontrol status
Host <имя_системы>
antispam Running
antivirus Running
ldap Running
logger Running
mailbox Running
mta Running
snmp Running
spell Running
stats Running
```

Если какая-либо служба не запущена, нужно стартовать ее (`zmcontrol start`). Обычно никаких проблем при установке не возникает, и сразу же можно переходить к административному интерфейсу Zimbra.

Примечание

Деинсталляция ZCS производится командой `./install.sh -u`. После ее выполнения следует вручную удалить папку установки ZCS.

Настройка безопасного доступа к почте

По умолчанию после установки доступ к почте производится по протоколу HTTP. Если планируется публиковать ZCS в Интернете (да и в условиях локальной сети эта рекомендация будет не лишней), нужно настроить доступ к серверу по безопасному протоколу HTTPS. Возможен вариант как использования обоих протоколов, так и только одного. Установка это значения производится следующими командами (их нужно выполнить от имени пользователя zimbra):

`zmtlsctl https`	для выбора протокола HTTPS
`zmtlsctl http`	для выбора протокола HTTP
`zmtlsctl mixed`	в случае использования обоих протоколов

При переходе к использованию протокола HTTPS Zimbra использует собственный сертификат для защиты сообщений. Поэтому его необходимо импортировать в домен Windows и обеспечить доверие. При этом нужно выбрать формат, который распознается ОС Windows. Выполняется экспорт сертификата следующей командой:

```
openssl x509 -in /opt/zimbra/ssl/zimbra/ca/ca.pem -out
/srv/samba/share/cacert.der -outform DER
```

Теперь сертификат нужно скопировать на ресурс, доступный серверу Windows (например, через сменный носитель или подключив общий ресурс Windows), импортировать его в доменную политику, сохранив в папке доверенных сертификатов (Trusted Root Certification Authorities).

Можно не распространять этот сертификат через групповые политики, но тогда придется его импортировать на каждой рабочей станции Windows, работающей с Zimbra.

Примечание

По умолчанию сертификат Zimbra создается на один год. Через год нужно сгенерировать новый сертификат удостоверяющего центра Zimbra, создать на его основе новый сертификат для почты и применить его. После чего импортировать сертификат аналогично описанному ранее способу в домен Windows. Для генерации нового сертификата нужно выполнить:

```
/opt/zimbra/bin/zmcertmgr createca –new
/opt/zimbra/bin/zmcertmgr createcrt –new –days 365
/opt/zimbra/bin/zmcertmgr deploycrt self
/opt/zimbra/bin/zmcertmgr deployca
```

Администрирование ZCS

Администрирование ZCS выполняется как из веб-интерфейса, так и из командной строки. Причем в первом режиме доступны не все опции настройки.

Примечание

Документация по ZCS доступна в Интернете, прежде всего, по адресу **http://wiki.zimbra.com/**.

После установки ZCS доступ к управлению осуществляется по адресу хоста и порту 7071 (рис. 8.2). При подключении к интерфейсу администрирования первоначально отображается состояние всех служб сервера. Для настройки параметров Zimbra достаточно выбрать соответствующую позицию в панели навигации слева.

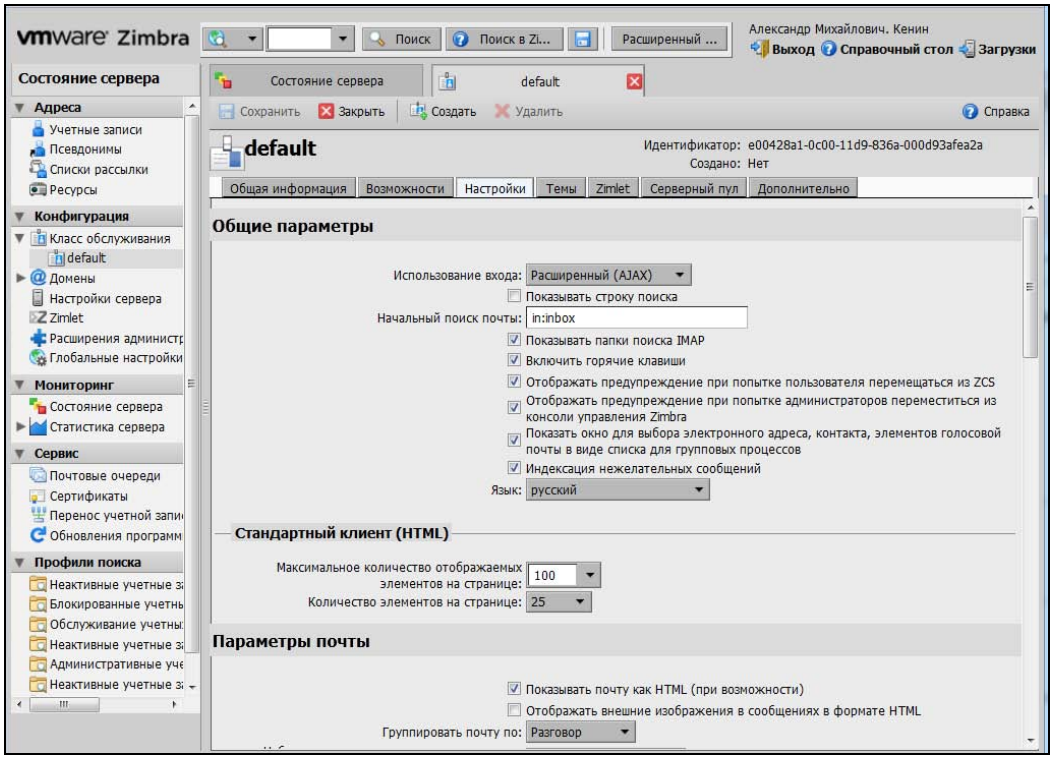


Рис. 8.2. Интерфейс администрирования Zimbra (настройки класса обслуживания)

Желательно проверить все настройки сервера, которые отображаются на страницах управления. Прежде всего, проконтролируйте часовой пояс и глобальные установки. Обратите внимание на перечень типов файлов, которые запрещены к пересылке, и, при необходимости, откорректируйте его. Установите максимальные размеры вложений в сообщения почты и максимальные объемы документов, которые можно сохранять на сервере Zimbra.

Убедитесь, что вас удовлетворяют настройки пользовательских учетных записей (лимиты почтовых ящиков, правила составления паролей, тайм-ауты работы с почтовым ящиком и т. п. — все это настраивается в параметрах класса обслуживания).

После настройки параметров сервера можно приступать к созданию учетных записей пользователей.

Обратите внимание, что вы можете создать еще и ресурсы. Ресурсы необходимы при планировании совещаний, заданий и т. п.; их можно "бронировать" для проведения мероприятия, причем настройки допускают автоматическое закрепление ресурса при получении заявки пользователя.

В целом, веб-интерфейс администрирования Zimbra достаточно понятен, и настройки обычно не вызывают сложностей.

Класс обслуживания определяет настройки пользователей. При необходимости можно добавить новые классы обслуживания и назначить их соответствующим группам.

Кроме веб-интерфейса в Zimbra присутствует ряд команд управления, которые выполняются из консоли. Они находятся по умолчанию в папке /opt/zimbra/bin. Запускать эти команды необходимо от пользователя Zimbra. Листинг 8.3 иллюстрирует, как это можно сделать.

Листинг 8.3

```
sudo -s
sudo — zimbra
zmprov gacf
```

Из особенностей работы с программой отметим, что написание команд чувствительно к регистру (нужно внимательно следить, где строчные, а где прописные буквы). Также, если параметр команды должен включать пробелы, его следует заключить в кавычки.

Консольные команды управления целесообразны в тех случаях, когда необходимо:

- ❒ настроить учетные записи в пакетном режиме (например, создать несколько записей путем импорта списка);
- ❒ вручную остановить или запустить какую-либо службу;
- ❒ переместить почтовые ящики (в случае установки нескольких серверов Zimbra);
- ❒ осуществить поиск по нескольким почтовым ящикам сразу;
- ❒ установить сертификаты безопасности на сервер (требуются для создания защищенных каналов);
- ❒ изменить локальную конфигурацию сервера.

Список наиболее употребительных консольных команд Zimbra приведен в табл. 8.1.

Таблица 8.1. *Команды администрирования Zimbra*

Команда	Функция
`postconf`	Редактирование конфигурации `postfix` (отвечает за передачу сообщений)
`postfix`	Остановка/запуск/обновление `postfix`
`qshape`	Проверка очереди сообщений `postfix`

Таблица 8.1 *(окончание)*

Команда	Функция
`zmantispamctl`	Остановка/запуск/состояние службы проверки спама
`zmantivirusctl`	Остановка/запуск/состояние службы антивирусной проверки
`zmcontrol`	Остановка/запуск/состояние сервера Zimbra
`zmhostname`	Отображает имя сервера Zimbra
`zmldappasswd`	Используется для смены пароля доступа к LDAP
`zmlmtpinject`	Утилита тестирования
`zmlocalconfig`	Отображает или настраивает локальную конфигурацию Zimbra
`zmmailboxctl`	Остановка/запуск/состояние компонентов почтового ящика (Tomcat, MySQL, convert)
`zmmsgtrace`	Трассировка сообщений
`zmprov`	Осуществление любых операций в Zimbra LDAP, в том числе создание учетных записей, доменов, списков рассылки и т. д. Например, команда `zmprov sm` *`имя_ящика`* `emptyFolder /contacts` очищает папку контактов для указанного пользователя
`zmtlsctl`	Настраивает веб-сервер на протокол HTTP, HTTPS или обоих протоколов сразу
`zmvolume`	Управление томами хранения данных почтового сервера

Команды могут использоваться для различных операций, поэтому, в целях экономии, мы отошлем читателя к онлайновой справке по этим утилитам (вызывается ключом `-h`).

Резервное копирование Zimbra

Бесплатная версия ZCS не включает в себя средств резервного копирования (они входят в состав коммерческой версии). Поэтому администратору нужно настроить любой сценарий, позволяющий выполнить такую операцию.

Некоторые сценарии представлены на странице **http://wiki.zimbra.com/wiki/Open_Source_Edition_Backup_Procedure**.

Логика работы всех сценариев примерно одинаковая. Сначала производится пересылка в локальную папку резервного копирования незаблокированных данных (для минимизации времени остановки служб Zimbra), потом останавливаются процессы Zimbra (если процесс не останавливается за выделяемое в сценарии время, он удаляется) и проводится окончательная синхронизация с локальной копией. Затем службы Zimbra запускаются, а сценарий начинает передачу данных из локальной папки резервного копирования на удаленный сервер. После завершения сценарий фиксирует продолжительность всех операций.

Особенности пользовательских почтовых ящиков Zimbra

Пользовательский веб-интерфейс кажется достаточно понятным. В то же время для большинства пользователей необходимо дать некоторые разъяснения по его применению.

Веб-интерфейс поддерживает операции drag-and-drop, например, при получении сообщения пользователь может перетащить его непосредственно в обозревателе на календарь, и программа автоматически предложит создать встречу на основе этого сообщения в указанный день.

Zimbra позволяет легко создавать общие папки. При этом, в отличие от Microsoft Exchange, права доступа к папке определяет сам пользователь.

В общий доступ папка предоставляется из меню ее свойств. Вы должны указать права доступа и направить приглашения для подключения к папке другим пользователям (рис. 8.3). Поиск пользователей осуществляется по глобальной адресной книге, так что обычно достаточно набрать только первые символы адреса, чтобы система предложила найденную учетную запись.

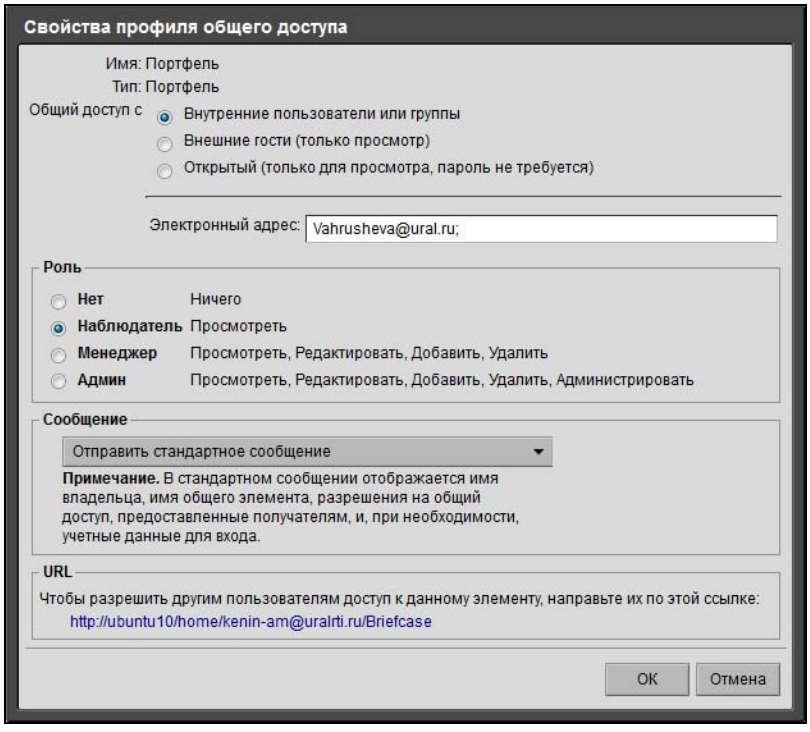


Рис. 8.3. Предоставление папки с документами в общий доступ

Обратите также внимание пользователей на раздел **Настройки**, в котором содержатся операции настройки параметров учетной записи. В том числе, смена пароля пользователя, создание фильтров, сортировка почты, настройка типа отображения сообщений (по теме или дате), параметры автоответов, создание оповещений о по-

лучении почты (удобно при настройке оповещений о получении почты через SMS на сотовый телефон и т. п.).

Пользователи могут создавать несколько календарей и использовать, например, напоминания о предстоящих событиях из нескольких источников.

Кроме того, пользователи должны знать, что спам-фильтрация в Zimbra является обучаемой: если сообщения перетаскивать из папки спама в папку **Входящие** или наоборот, то программа впоследствии будет допускать меньше ошибок классификации сообщений.

Настройка взаимодействия с доменом Windows

Пользователи Zimbra могут проходить аутентификацию в домене Windows и использовать глобальную адресную книгу для выбора адресатов.

Для этого достаточно в настройке параметров почтового домена (или в параметрах класса обслуживания, если настройка делается по умолчанию) выбрать команду **Настроить проверку подлинности** и указать необходимые параметры (рис. 8.4). После указания этих параметров можно проверить правильность взаимодействия с доменом, выполнив проверочный тест мастера настройки.

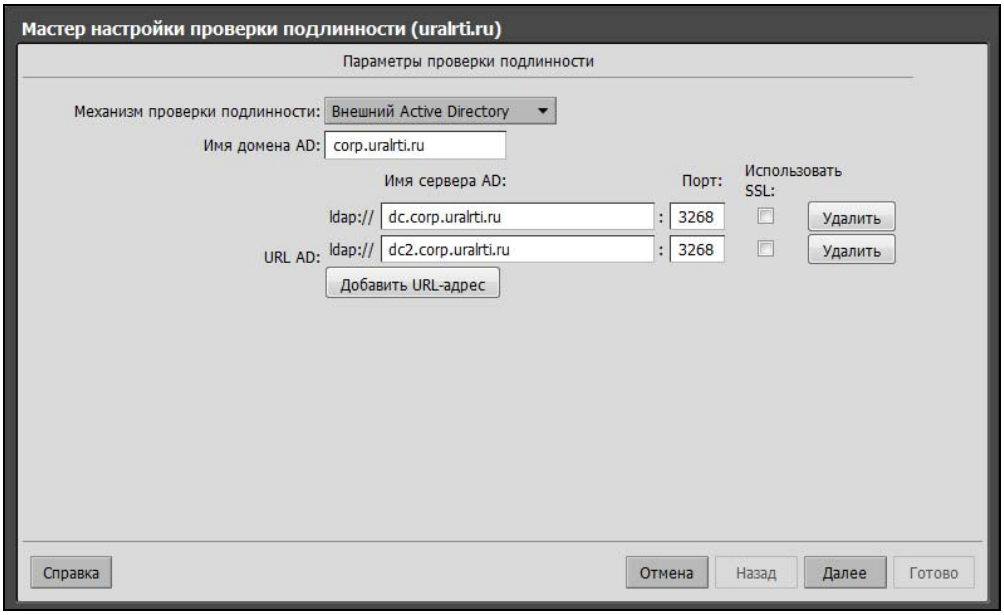


Рис. 8.4. Настройка проверки подлинности на домен Windows

Аналогично выполняется и настройка использования глобальной адресной книги домена. При этом нужно будет указать параметры учетной записи домена, которая будет использоваться для осуществления операций поиска.

При настройке аутентификации пользователей в домене Windows следует иметь в виду, что для таких учетных записей должны быть созданы почтовые ящики на сервере Zimbra. В Интернете существуют различные сценарии, позволяющие авто-

матизировать такой процесс. Их легко найти. Например, автор использует (с небольшими доработками) сценарии со страницы **http://www.zimbra.com/forums/administrators/30856-active-directory-script-import-users-zimbra-4.html**.

Совместная работа Zimbra и Microsoft Exchange

В целях оптимизации расходов на лицензирование можно настроить совместную работу серверов Zimbra и Exchange. Существуют разные варианты организации такой работы (например, первым принимает почту сервер Zimbra и отсылает сообщения на сервер Exchange для тех пользователей, у которых там созданы ящики, или наоборот). Поскольку это достаточно специфичная ситуация, то мы отошлем читателей к онлайновой документации (ищите на Wiki-сервере Zimbra или в Интернете по ключевым словами *split domain*).

Кроме разделения пользователей, в данном случае необходимо выполнить и синхронизацию информации занятости пользователей (для планирования мероприятий). Соответствующие рекомендации описаны на странице h**ttp://wiki.zimbra.com/wiki/Free_Busy_Interop_for_Exchange**.

Миграция с Microsoft Exchange

ZCS включает в себя специальное средство, которое позволяет мигрировать как пользователей, так и данные их почтовых ящиков с сервера Microsoft Exchange на сервер Zimbra.

Описание средства представлено в онлайновой документации администратора.

Почтовый клиент Zimbra

Для Zimbra разработан специальный почтовый клиент — Zimbra Desktop. Программа доступна к бесплатной загрузке с сайта Zimbra и предназначена для установки как на операционные системы Windows, так и Linux (рис. 8.5).

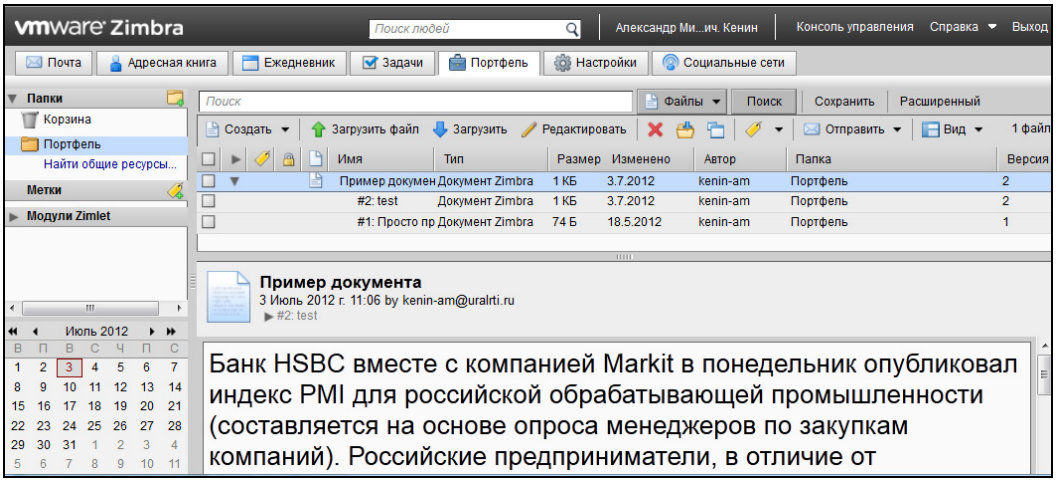


Рис. 8.5. Почтовый клиент Zimbra Desktop

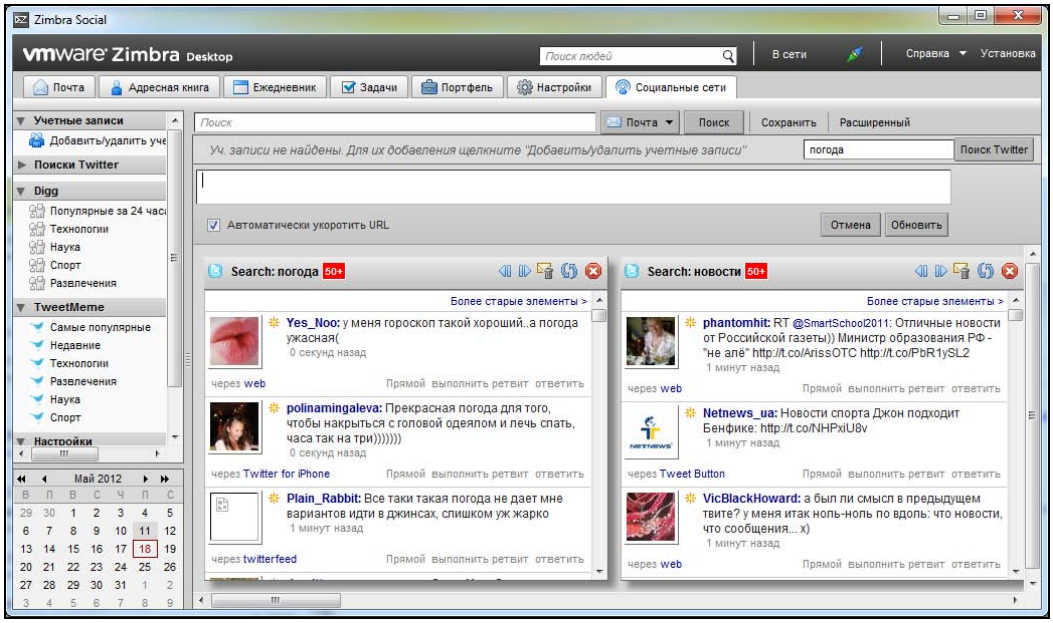


Рис. 8.6. Клиент Zimbra Desktop при поиске в Twitter

Zimbra Desktop обеспечивает подключение не только к ящикам на серверах Zimbra, но и к Yahoo Mail, Gmail, Microsoft Live Hotmail, а также к любым другим серверам по протоколам IMAP и POP. В том числе, поддерживая современные технологии социальных сетей (рис. 8.6).

Особенности настройки фильтрации спама в ZCS

В ZCS каждое сообщение оценивается некоторой численной величиной, свидетельствующей о "спам-подозрительности". Делает это компонент SpamAssassin. В ZCS оценка от SpamAssassin используется для пропуска или удаления сообщений. Уровень в 20 единиц от SpamAssassin в ZCS принимается за 100%. При уровне от 33 до 75% сообщение попадает в ящик нежелательной почты пользователя, а при бóльших значениях — удаляется по умолчанию. Эти уровни можно изменить в графическом интерфейсе управления.

В ZCS доступно обучение системы на спам. Для этого пользователь должен в веб-интерфейсе отметить нежелательные сообщения как спам, а случайно попавшие в ящик нежелательной почты — как благонадежные. Такие сообщения попадают в специальные почтовые ящики, обрабатываются сценарием и формируют базу нежелательной почты.

Кроме описанного способа оценки спама, в ZCS можно дополнительно включить стоп-листы реального времени (по умолчанию они отключены). Можно включить следующие стоп-листы:

- dnsbl.njabl.org;
- cbl.abuseat.org;

- bl.spamcop.net;
- dnsbl.sorbs.net;
- sbl.spamhaus.org;
- relays.mail-abuse.org.

Для этого необходимо добавить соответствующий стоп-лист с помощью команды `zmprov`. В параметрах команды следует указать все блокировки, причем перечисленные стоп-листы должны быть указаны каждый по типу `zimbraMtaRestriction "reject_rbl_client` *`стоп-лист`*`"`. Таким образом, учитывая три включенных фильтра по умолчанию, строка команды будет выглядеть в максимальном случае так, как в листинге 8.4.

Листинг 8.4

```
zmprov mcf zimbraMtaRestriction reject_invalid_hostname
zimbraMtaRestriction
reject_non-fqdn_hostname zimbraMtaRestriction
reject_non_fqdn_sender
zimbraMtaRestriction "reject_rbl_client dnsbl.njabl.org"
zimbraMtaRestriction
"reject_rbl_client cbl.abuseat.org" zimbraMtaRestriction
"reject_rbl_client
bl.spamcop.net" zimbraMtaRestriction "reject_rbl_client dnsbl.sorbs.net"
zimbraMtaRestriction "reject_rbl_client sbl.spamhaus.org"
zimbraMtaRestriction
"reject_rbl_client relays.mail-abuse.org"
```

Трассировка сообщений в Zimbra

Чтобы узнать состояние отправки или получения сообщения, в Zimbra необходимо выполнить команду `zmmsgtrace`. В качестве ее параметров (фильтров) можно указать идентификатор сообщения, адрес отправителя или получателя, IP-адрес почтового сервера и временной диапазон.

По умолчанию данные трассировки хранятся 30 дней.

Например, можно ввести команду, чтобы увидеть информацию по всем сообщениям, отправленным пользователем. Листинг 8.5 иллюстрирует результат.

Листинг 8.5

```
zmmsgtrace -s user@rrr.ru
Tracing messages
from user@rrr.ru

Message ID '15614059.101246175945950.JavaMail.SYSTEM@desktop'
user@rrr.ru -->
```

```
aaa.bbb@isory.ee
Recipient aaa.bbb@isory.ee
2011-06-28 13:59:29 — mail.rrr.ru (192.168.31.20) --> mail
201-06-28 13:59:34 — mail --> 127.0.0.1 (127.0.0.1]:10024) status sent

Message ID '30004518.21246795150656.JavaMail.SYSTEM@desktop'
user@rrr.ru -->
sfn@list.ru
Recipient sfn@list.ru
2011-07-05 17:59:41 — mail.rrr.ru (192.168.31.20) --> mail
2011-07-05 17:59:46 — mail --> 127.0.0.1 (127.0.0.1]:10024) status sent
...
26 messages found
```

По этой информации видно, что пользователь отправил 26 сообщений. Статус сообщений — *отправленные*.

Иногда такой информации недостаточно для выяснения причин недоставки сообщений. В таком случае придется обращаться к журналам отдельных компонентов почтового сервера. Так, журнал агента сообщений хранится как /var/log/mail.log. В этом журнале можно узнать, например, на какой сервер было передано сообщение:

```
Jul 23 01:10:10 mail postfix/smtp[2652]: 3C9B252A002: to=<kenin@ask.ru>,
relay=mail2.ask.ru[81.91.63.38]:25, delay=2.3, delays=0.04/0.02/0.04/2.2,
dsn=2.6.0, status=sent (250 2.6.0
<698422244.8981248289804948.JavaMail.root@mail> Queued mail for delivery)
```

Приведенный отрывок журнала говорит, что сообщение было удачно (код 250) отправлено на почтовый сервер **mail2.ask.ru** с адресом 81.91.63.38 для пользователя **kenin@ask.ru**. Такие сведения позволят уже конкретно выяснить прохождение сообщения на другом сервере.

Если подобная подробная информация будет постоянно востребована, то необходимо изменить период хранения данных журналов. По умолчанию они архивируются ежедневно программой `logrotate`, и система хранит семь таких архивов (информация доступна только за прошедшую неделю).

Самый простой способ — изменить настройку числа хранимых копий в файле /etc/logrotate.d/zimbra. В строке, начинающейся со слова `rotate`, введите необходимое вам значение и сохраните изменения.

Поиск неисправностей ZCS

При возникновении проблем в работе служб ZCS следует увеличить объем протоколирования. По умолчанию уровень протоколирования настроен в режиме INFO. Для увеличения протоколирования следует добавить строку

```
log4j.logger.zimbra.soap=DEBUG
```

в файл /opt/zimbra/conf/log4j.properties.in и перезагрузить сервер. Чтобы режим протоколирования сменился без перезагрузки, можно выполнить команду `zmmtaconfig mailboxd`. В этом случае возможна небольшая пауза до того момента, когда изменения начнут действовать.

Протоколирование можно установить не в целом для всего сервера, а только для одного пользователя. Это более щадящий режим с точки зрения дополнительной нагрузки на сервер. Такая операция выполняется командой `zmprov` следующим образом:

```
zmprov addAccountLogger адрес_пользователя zimbra.soap debug
```

Подробности использования данной команды следует уточнить по онлайновой документации.

> ***Примечание***
>
> Описание всех журналов Zimbra содержится на странице **http://wiki.zimbra.com/wiki/Log_Files**.

ГЛАВА 9

Организация корпоративных ресурсов

Традиционно под общими ресурсами системы понимаются предоставленные в общее пользование файлы на сервере (и рабочих станциях). На сегодня это наиболее быстрый и легко настраиваемый тип общего ресурса, наиболее часто используемый, но не самый удобный вариант общих данных.

> ***Примечание***
> Мы не будем в этом разделе рассматривать совместное использование серверов печати.

Требования к качеству обслуживания

Требования, предъявляемые к корпоративным ресурсам, существенно зависят от размеров организации и специфики бизнеса. При небольшом числе пользователей достаточно просто создать общие ресурсы на одном или нескольких серверах, если пользователей становится больше — необходимо структурировать ресурсы, предусмотреть политики хранения данных. В больших организациях — условно, при числе пользователей более 1 тысячи — целесообразно использовать системы управления содержимым (ECM), автоматизирующие процесс включения документа в хранилище (модерируемое сохранение, процессы утверждения, версионность и т. п.).

Политики общих ресурсов

Целесообразно разработать *политику общих ресурсов* предприятия. Подобный документ позволит администратору, с одной стороны, предъявлять соответствующие ограничения к пользователям, контролировать размещения информации, с другой — наложит требования по качеству обслуживания.

В политике общих ресурсов можно описать, что хранится на общих ресурсах, установить владельцев ресурсов, лимиты хранения, порядок удаления устаревшей информации, частоту операций резервного копирования и т. п.

Вы можете задать корпоративные правила именования документов и описать структуру ресурсов (чтобы пользователи знали, куда сохранять информацию и как

ее быстро найти). Задать требования к карточке документа (если она используется) и правила добавления ключевых слов в описания (для упрощения поиска). В этом же документе может быть определена и матрица доступа к ресурсам (набор прав доступа для различных категорий пользователей).

Не лишним будет и зафиксировать требования к мониторингу общих ресурсов: кто и как часто будет следить за динамикой роста объемов за длительный период, нужно ли проводить анализ хранилищ в разрезе по тематике документов и т. п., какое время доступа к ресурсу будет считаться оптимальным, а когда следует перейти к операциям оптимизации и т. д.

Объемы и сроки хранения. Возможности восстановления

Корпоративные ресурсы должны храниться на серверах. Политикой организации должно быть определено, можно ли хранить локально промежуточные версии, какие форматы документов допустимы, сколько времени хранятся документы того или иного типа.

Периодически должна выполняться резервная копия всех совместно используемых данных. Политика резервного копирования должна предусматривать частоту копирования и количество хранимых копий документов. Для минимизации обращений к администраторам желательно предусмотреть возможность самостоятельного восстановления пользователями своих документов.

Производительность

Время сохранения/открытия документа с корпоративного ресурса не должно существенно — более чем на 0,5—0,8 с — превышать длительность операции локального сохранения документа. Лучшей производительностью отличаются FTP-ресурсы, худшей — портальные решения.

Поиск информации. Карточка документа

Для корпоративных ресурсов должна быть разработана структура хранения данных, предполагающая легкую возможность нахождения документа по его типу. Следует ввести и соблюдать правила именования документа, обязательного заполнения свойств: минимально это могут быть стандартные поля свойств в программе офисного редактора, в лучшем случае — специальная форма карточки документа (особенно для конструкторской документации и т. п.).

Также в организации необходимо предусмотреть систему поиска (как по ключевым словам/полям документа, так и полнотекстовую), объединяющую все варианты хранения данных.

Контроль объемов и типов документов

Если пользователям не предоставлена возможность обмениваться личной информацией (фильмами, музыкой и т. п.), то они будут использовать любую возможность для сохранения таких файлов на доступных им общих ресурсах.

Для контроля ресурсов используются технологии, препятствующие сохранению определенных типов файлов (по расширениям) и контролирующие объем папок.

Варианты организации корпоративных ресурсов

Существуют различные варианты создания общих ресурсов:

- FTP-сервер;
- общие файловые ресурсы (общие папки в Windows, сетевая файловая система NFS);
- ресурсы на веб-серверах (преимущественно портальные решения).

FTP-сервер

FTP-сервер позволяет максимально быстрым способом загрузить файл с сетевого ресурса (или сохранить на ресурсе). В Windows FTP-сервер является частью IIS, но данный компонент используется редко, поскольку доступные бесплатные решения более удобны в работе и более функциональны.

Для доступа к ресурсам FTP-сервера необходим клиент. Вообще говоря, ftp-клиент встроен в Проводник Windows, и работать с сервером можно, просто открыв любое окно и введя в адресную строку параметры доступа (**ftp://<*имя_ftp-сервера*>**). Для доступа на сайт с использованием имени и пароля следует в IE выбрать команду **Файл | Войти как** и ввести параметры учетной записи FTP-сервера (рис. 9.1). Кроме того, работает традиционный способ задания параметров учетной записи в строке адреса — для доступа нужно ввести имя и пароль следующим образом: **ftp://*user*:*password*@*url*/**.

Если с FTP-ресурсом приходится работать достаточно часто, то можно добавить ссылку на него в **Сетевое окружение**, воспользовавшись соответствующим мастером операций. В этом случае вы можете для подключения сразу указать имя учетной записи для доступа на сервер.

В Проводнике с FTP-ресурсом можно работать обычным образом: переходить по папкам, перетаскивать файлы и т. д. Однако следует заметить, что встроенный в Проводник клиент не открывает часть FTP-серверов, в таких случаях необходимо использовать любой бесплатный FTP-клиент, найти их не представляет сложности. Например, можно использовать популярную программу FileZilla (**http://filezilla-project.org/**), но целесообразно работать в клиенте, поддерживающем как FTP-протокол, так и современные протоколы для доступа к ресурсам Linux-систем:

SFTP (SSH File Transfer Protocol) и SCP (Secure Copy Protocol), например, WinSCP (**http://winscp.net/**).

С помощью FTP-сервера можно оперативно предоставить в доступ тот или иной файл, причем сделать это для конкретного пользователя (достаточно создать его в самом FTP-сервере, не меняя состав пользователей организации). Протокол удобен для работы с Интернетом, правила межсетевого экранирования просты и легко настраиваются. Как уже говорилось, скорость работы с использованием данного протокола приближается к максимальным пропускным значениям.

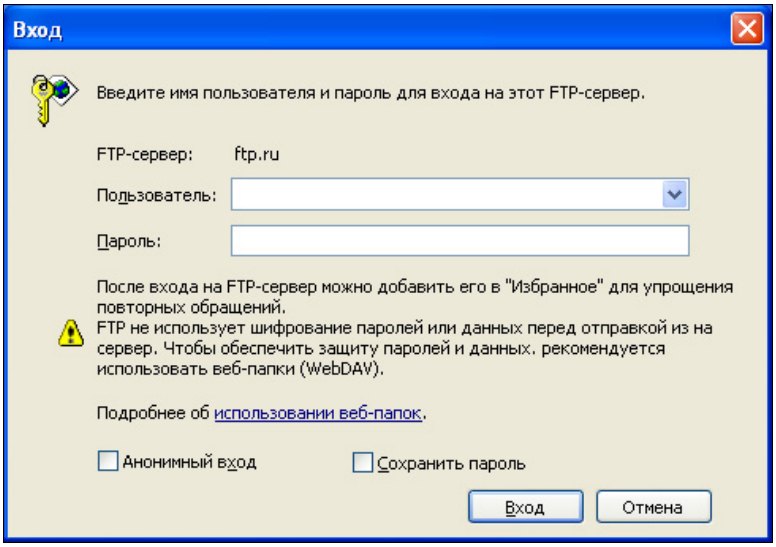


Рис. 9.1. Ввод параметров учетной записи на доступ к FTP-серверу

Главный недостаток заключается в сложности организации поиска информации. FTP-сервер может отображать клиенту сообщения при входе в каждую папку, но поиск проводится по именам файлов, чего не всегда достаточно. Для обхода этой проблемы часто в корне сервера сохраняют *индексный файл*, в котором описывают расположения файлов и их параметры. При регулярных обновлениях FTP-сервера сопровождение такого индексного файла представляет определенные сложности.

Установка FTP-сервера

Администраторам доступны различные решения FTP-серверов. Самый простой вариант — включить встроенный в Windows FTP-сервер. Однако это решение весьма ограниченно и неудобно, если предполагается эксплуатировать FTP-сервер, а не только разово принять или передать файлы.

Гораздо большей функциональностью обладают FTP-серверы, которые доступны для установки из Интернета, в том числе и бесплатные версии, например, FTP-сервер для Windows от FileZilla (**http://filezilla-project.org/**). Установка и настройка таких серверов не представляют сложности, поэтому мы рассмотрим в качест-

ве примера установку FTP-сервера, работающего в консольном режиме сервера Ubuntu.

Установка собственного FTP-сервера Windows

В состав Windows входит FTP-сервер. Он является составной частью IIS-сервера и устанавливается путем добавления роли **Веб-сервер (IIS)** с последующим выбором службы **Служба FTP-публикации**. После завершения работы мастера необходимо выполнить первичную настройку FTP-сервера: подтвердить папки хранения документов, выбрать пользователей и предоставить им права.

Управление FTP-сервером производится из консоли **Администрирование | Диспетчер служб IIS 6.0** (рис. 9.2).

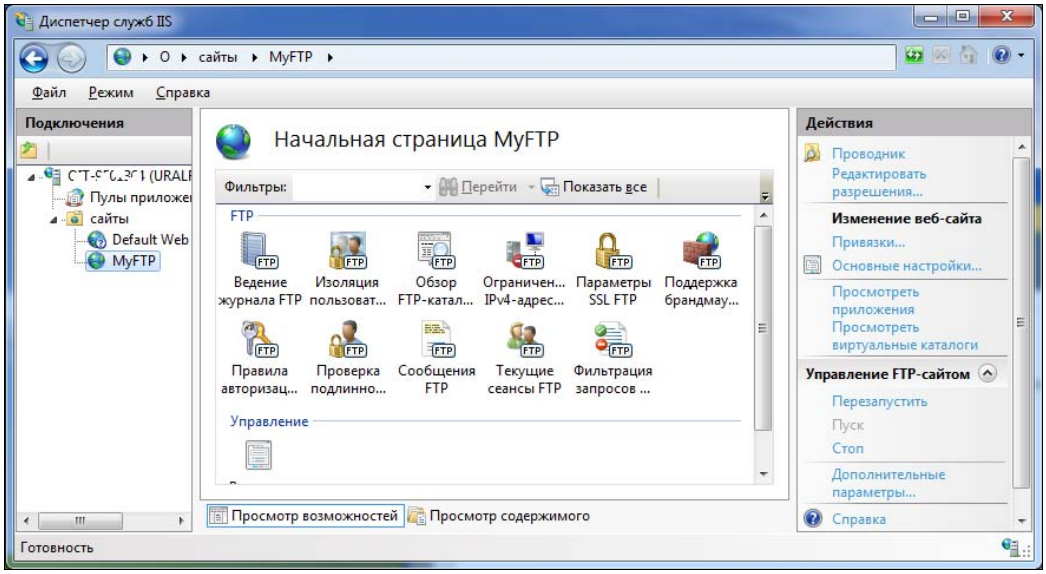


Рис. 9.2. Консоль управления встроенным FTP-сервером Windows

Созданный по умолчанию FTP-сервер первоначально остановлен. Корневой каталог его настроен на папку C:\inetpub\ftproot, доступ к серверу разрешен анонимным пользователям только для чтения, информация о сессиях будет записываться в журнал веб-сервера.

На что нужно обратить внимание? Пользователи аутентифицируются по учетным записям Windows. Настройки сервера не позволяют управлять правами доступа для разных пользователей: вы можете либо установить право только чтения для всех, либо включить возможность записи. Поэтому, если необходимо предоставить FTP-сервер для записи анонимным пользователям из Интернета (например, для получения каких-либо файлов от определенной организации), то можно поступить следующим образом. На корень FTP-сервера предоставить только права чтения, добавить новый каталог (через соответствующую опцию в свойствах узла), для которого установить права записи. После чего сообщить пользователям имя новой

папки, в которую они должны перейти после установления сеанса связи с FTP-сервером для записи файлов. На рис. 9.2 показано отображение такого узла FTP — с созданным каталогом Private.

Другой способ заключается в использовании прав доступа к FTP-узлу совместно с правами доступа к файловой системе. Анонимному пользователю соответствует учетная запись IUSR_<*имя_компьютера*>. Чтобы безопасно предоставить FTP-узел на запись, можно:

- ❒ разрешить запись средствами управления FTP-сервера;
- ❒ запретить запись на уровне файловой системы для пользователя IUSR_<*имя_компьютера*>;
- ❒ разрешить запись в папку для локального пользователя компьютера.

После чего можно сообщить параметры этой учетной записи удаленному пользователю.

После проверки и настройки свойств узла необходимо запустить его, воспользовавшись соответствующей командой в консоли управления. Правила межсетевого экрана, разрешающие доступ к FTP-серверу, при этом будут автоматически созданы в процессе установки.

Установка vsftp

Для установки в сервере Ubuntu можно рекомендовать FTP-сервер VSFTP (**v**ery **s**ecure **FTP** server, домашняя страница — **https://security.appspot.com/vsftpd.html**). Продукт обладает многими возможностями (виртуальные IP-адреса, виртуальные пользователи, персонифицированные настройки — по пользователю и IP-адресу, контроль полосы пропускания, шифрование трафика и т. д.). Сервер устанавливается из репозитория:

```
sudo apt-get install vsftpd
```

Файл настроек сервера — /etc/vsftpd.conf. Кроме того, в файле /etc/ftpusers содержится список пользователей, которым запрещен доступ к серверу (по умолчанию в него включены учетные записи root, daemon, nobody и др.).

В Интернете широко представлены руководства по настройке конфигурации этого FTP-сервера, поэтому остановимся только на некоторых особенностях.

После установки конфигурация по умолчанию предусматривает доступ к серверу пользователей системы. Чтобы разрешить анонимный доступ, необходимо откорректировать следующую строку в файле конфигурации:

```
anonymous_enable=Yes
```

Настройками по умолчанию предусмотрена только возможность загрузки файлов с сервера. Чтобы разрешить запись (upload), нужно внести следующие изменения:

```
write_enable=YES
```

При этом запись для анонимных пользователей по-прежнему будет запрещена. Чтобы разрешить ее, нужно отредактировать настройку: `anon_upload_enable=YES`. Однако включать такую опцию следует очень осторожно.

В целях безопасности пользователям[1] можно предоставлять доступ только в их домашние папки. Для этого внесите в конфигурацию следующую настройку:

```
chroot_local_user=YES
```

Папка по умолчанию соответствует домашней папке пользователя, от имени которого запущен сервер — ftp. Чтобы сменить ее, достаточно создать новую папку и переопределить домашний каталог пользователя ftp:

```
sudo usermod -d <новый путь> ftp
```

Сервер VSFTP позволяет создать собственную базу пользователей, хранить ее можно как в файле, так и на SQL-сервере. Подробности опций создания виртуальных пользователей легко найти в Сети.

> ***Примечание***
>
> После редактирования конфигурации для вступления изменений в силу необходимо перезапустить `vsftpd`.

Использование распределенной файловой системы

При создании общих файловых ресурсов целесообразно отказаться от предоставления ресурсов с конкретного сервера. В случае выхода из строя сервера или необходимости перемещения ресурса на другую систему (например, из-за нехватки дискового пространства) администратору придется менять точки подключения на всех компьютерах своей сети. Выходом из данной ситуации является создание *сетевой* файловой системы.

Распределенная файловая система (Distributed File System, DFS) представляет собой коллекцию ссылок на совместные ресурсы, находящиеся на различных компьютерах сети, доступ к которым производится через единую точку входа. Структура DFS напоминает дерево каталогов: на самом "верху" расположена одна точка входа, называемая *корнем DFS*, к которой подключены вложенные папки.

DFS в Windows может быть привязана к домену (имена ресурсов начинаются с имени всего домена) или к какому-либо серверу. DFS в Linux реализуется с привязкой корня (точки, в которой видна структура общих ресурсов данного DFS) к серверу.

> ***Примечание***
>
> Использование доменного корня DFS в системах Linux представляет определенные сложности, поскольку по умолчанию запрос доменного корня не возвращает имени сервера хранения. Поэтому для подключения к такому ресурсу системы Ubuntu необходимо указывать адрес ссылки DFS на конкретном сервере.

---

[1] Эту возможность можно включить только для части пользователей, если перечислить пользователей в списке: `chroot_list_enable=YES chroot_list_file=/etc/vsftpd.chroot_list`.

Если администратору по каким-либо причинам необходимо переместить ресурс в структуре DFS на другой сервер, достаточно просто скопировать файлы по новому пути и заменить ссылку со старой сетевой папки на новую. При этом все сетевые пути для клиентов (если, конечно, они указывали на структуру DFS) останутся неизменными.

Создание DFS в Windows-системах

Корень DFS можно создать на любом сервере Windows 200*x*. Причем на рядовых серверах возможно создание только одного корня DFS, в домене может поддерживаться *несколько корней DFS* (разными контроллерами).

В качестве корня DFS указывают любую совместно используемую папку (мастер создания DFS позволяет создать такую папку в процессе настройки). Рекомендуется не хранить в этой папке никаких файлов, а задействовать ее только для создания ссылок на сетевые ресурсы.

Создание корня DFS выполняется мастером операций (из меню **Администрирование | Управление DFS |** вызвать операцию **Новое пространство имен**) — рис. 9.3.

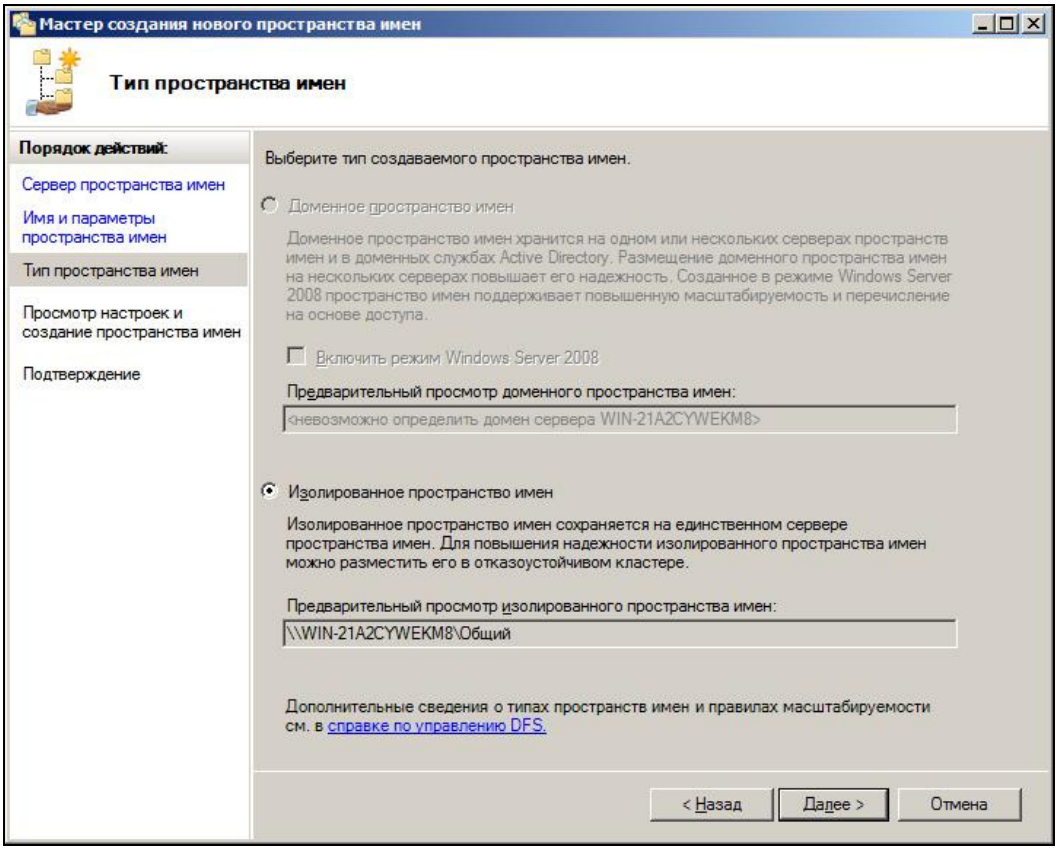


Рис. 9.3. Мастер создания нового пространства имен в Windows Server 2008

Мастер позволяет настроить разрешения сетевого доступа для общей папки, в которой будет размещен корень DFS.

После создания корня DFS необходимо начать собирать структуру папок распределенной файловой системы. Для этого с помощью оснастки управления следует добавить папки, указав в их свойствах ссылки на уже существующие *совместно используемые ресурсы сети*. Причем можно указать несколько ссылок на аналогичные ресурсы на разных компьютерах. Операция обычно не представляет никакой сложности.

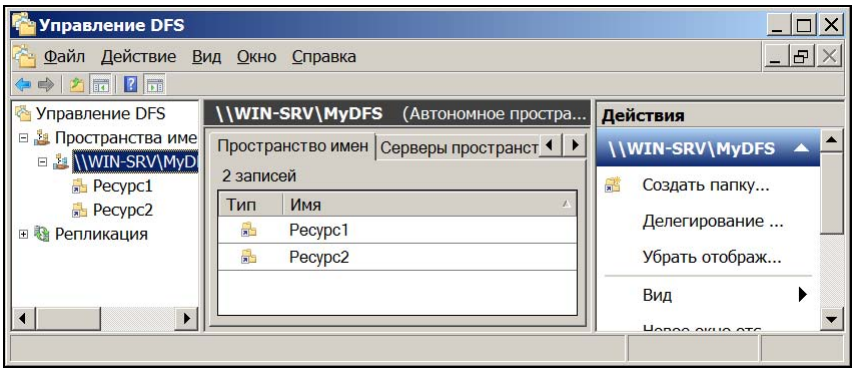


Рис. 9.4. Пространство имен с настроенными ссылками

В окне оснастки управления DFS на рис. 9.4 можно проконтролировать, какие совместно используемые папки включены в это пространство имен, просмотреть серверы имен, найти объекты и т. д.

Репликация DFS в домене Windows

В домене Windows возможна настройка репликации DFS — автоматическое поддержание копий данных на нескольких компьютерах. Например, можно создать копию папки с файловыми ресурсами центрального офиса в удаленном филиале, и система самостоятельно будет синхронизировать изменения, независимо (в каждом офисе) вносимые пользователями. Причем пользователи будут автоматически подключаться к тому компьютеру, данные которого расположены "ближе" к пользователю.

Подобная структура DFS является *отказоустойчивой*. Каждую ссылку можно продублировать, создав вторую ссылку на аналогичный сетевой ресурс на другом компьютере. В результате при недостижимости одного ресурса клиенты будут перенаправлены к функционирующему компьютеру. Причем система может *автоматически синхронизировать* эти ресурсы. Если данные будут изменены в папке по одной ссылке, то в папке по другой ссылке они будут продублированы.

Реплицируемые ресурсы нужно располагать в папках с NTFS 5.0, поскольку в процессе задействована система протоколирования этой файловой структуры для отслеживания изменений.

По умолчанию репликация не включена. В Windows Server 2008 она создается операцией **Репликация | Новая группа репликации**. Откроется мастер операций, который выполнит последующие настройки в зависимости от ответов администратора (рис. 9.5). Мастер настроит все параметры репликации в зависимости от ответов пользователя: подключит папки, настроит график репликации и ограничения по пропускной способности, если используются каналы Интернета, и т. п.

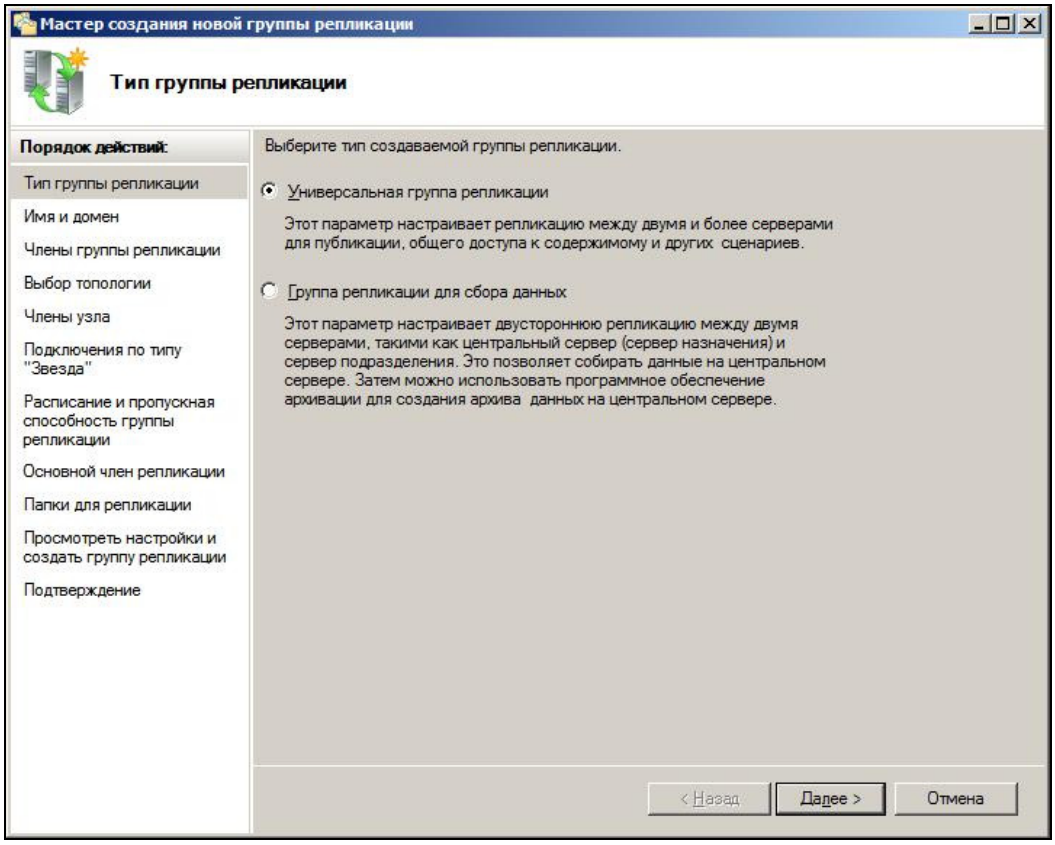


Рис. 9.5. Мастер настройки репликации в Windows Server 2008

Для серверов Windows 2003 для настройки репликации DFS необходимо выделить несколько ссылок на аналогичные ресурсы, выбрать команду **Синхронизовать**, указать основной ресурс (*мастер*, он будет считаться эталонным при начале репликации). А настройка графика репликации производится в задаче **AD Пользователи и компьютеры**. Открыв оснастку, следует включить отображение дополнительных функций (**Вид | Дополнительные функции**) и найти необходимый корень DFS. Открыв его свойства на вкладке **Набор репликации**, нужно нажать кнопку **Изменить расписание** и отредактировать график.

Автоматически синхронизируются не все файлы. Из репликации исключаются временные файлы (список расширений можно просмотреть в настройках). Сами файлы

реплицируются только после того, как пользователь завершает работу с ними. Иными словами, если пользователь открыл файл и работает с ним в течение всего дня, то копия файла по реплицируемой ссылке изменится только *после завершения работы — вечером*.

Если два пользователя одновременно работают с одним и тем же файлом в различных репликах, то система разрешит такой конфликт путем сохранения тех изменений, которые были внесены в файл, сохраненный позже.

Репликация папок в рабочих группах

Описанная автоматическая репликация работает только в условиях домена Windows. Если у вас рабочая группа или необходимо синхронизировать данные между двумя компьютерами через Интернет, то можно воспользоваться одной из бесплатных программ, которые легко найти в Сети (см., например, **http://www.softsoft.ru/search/freeware/8021/index.htm**). Программы напоминают одна другую, хотя каждая и имеет некоторые несущественные отличия.

Основные недостатки таких бесплатных программ по сравнению с коммерческими версиями — это выполнение заданий периодически, по некоторому графику (данные не синхронизируются в реальном времени) и отсутствие поддержки режима копирования только измененных данных внутри файла (поддерживается современными версиями Windows; это позволяет снизить объем данных, передаваемых по каналам связи). В подавляющем большинстве случаев эти характеристики несущественны. Так, автор эксплуатирует без нареканий одну из таких программ синхронизации папок уже более полутора лет.

Настройка DFS в Ubuntu

Настройка распределенной файловой системы в Ubuntu не представляет особой сложности и работает со всеми версиями Windows. Требуется лишь добавить несколько опций в файл конфигурации Samba.

Для включения DFS необходимо в файле конфигурации Samba в секции `global` добавить строку `host msdfs = yes`:

```
[global]
...
host msdfs = yes
...
```

А в описание для папки в файле конфигурации Samba, которая должна быть корнем DFS, — строку `msdfs root = yes`:

```
[dfs]
path = /<путь к папке>
msdfs root = yes
```

Чтобы в совместно используемой папке появились сетевые папки, необходимо создать в ней символические ссылки на эти ресурсы по следующему образцу:

```
ln -s msdfs:serverA\\shareA linka
ln -s msdfs:serverB\\share,serverC\\share linkb
```

В первом примере в папке создана ссылка `linka`, указывающая на общую папку `shareA` на сервере `serverA`, во втором — ссылке `linkb` сопоставлены два сетевых ресурса.

Ограничение предоставляемых файловых ресурсов

Если не осуществлять контроль записи файлов в общие папки, то через некоторое время ресурс будет заполнен полностью, а "вычистить" его от балласта окажется крайне сложно.

Настройка квотирования в Windows

В Windows возможно применение различных вариантов квотирования. На уровне файловой системы можно включить ограничения по объему для каждой учетной записи. А для сервера версии R2 можно устанавливать ограничения на объем папки и на типы файлов, которые можно размещать в ней.

Квотирование на уровне файловой системы

Квотирование диска возможно для компьютеров на дисках с файловыми системами NTFS. Чтобы включить квоту, следует открыть свойства жесткого диска, перейти на вкладку **Квота** и настроить опции (рис. 9.6).

В параметрах настройки можно запретить запись на диск при превышении квоты, а также настроить квоты, которые будут назначаться для вновь создаваемых пользователей. При включении опции **Регистрация...** в журнал системы будут записываться сообщения о превышении заданных лимитов. Кнопка **Записи квот...** позволяет увидеть реальные значения квот на жестком диске.

После создания первоначальных квот изменить их можно в списке **Записи квот**. Достаточно отметить необходимую строчку, через контекстное меню открыть свойства соответствующей записи и назначить новые параметры.

Квотирование на уровне файловой системы Windows неудобно тем, что не позволяет устанавливать квоты на группы. Так, если на сервере будут храниться какие-либо общие документы, то их объем будет включаться в квоту того пользователя, который их создал. Это не всегда удобно. В таких случаях администратору можно стать владельцем подобных файлов (для файла или папки выполните последовательность команд: **Свойства | Безопасность | Дополнительно | Владелец | Изменить**). Поскольку квоты считаются по владельцам файлов, то такая операция перенесет квоты с пользователя на администратора, который может для себя отключить контроль квот.

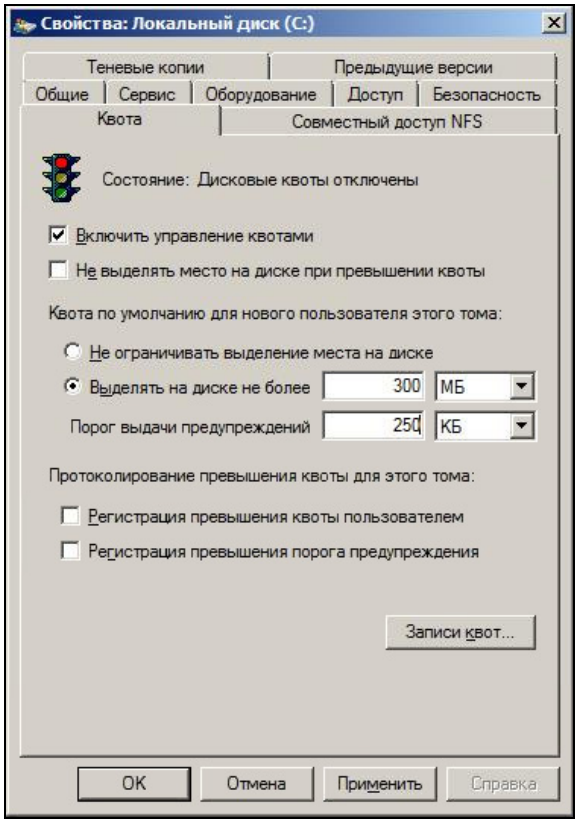


Рис. 9.6. Настройка квот на диске Windows

Квотирование общих папок

В составе выпуска R2 присутствуют компоненты, позволяющие реализовать политику ограничений для совместно используемых ресурсов. В частности, можно установить лимиты на объемы папок и запретить размещение в них определенных типов файлов. Эта функциональность добавляется с ролью **Файловые службы**.

В **Диспетчере ресурсов файлового сервера** (рис. 9.7) можно создавать квоты, настраивать поведение системы при их достижении и включать запреты на запись определенных типов файлов.

Методика использования квот проста. Вы создаете новую квоту, указывая, к какой папке она будет применена. В квоте вы определяете максимальный объем данной папки, тип ограничения (в случае жесткого ограничения превысить указанный в квоте порог невозможно). Кроме того, для каждой квоты можно задать несколько действий, которые будут выполняться при достижении некоторого объема: например, можно указать, что при достижении 80% от предельного значения объема папки будет направлено сообщение пользователю по электронной почте, а при достижении 90% аналогичное сообщение уйдет администратору. Возможными действиями системы может быть отсылка сообщений электронной почты (текст сообще-

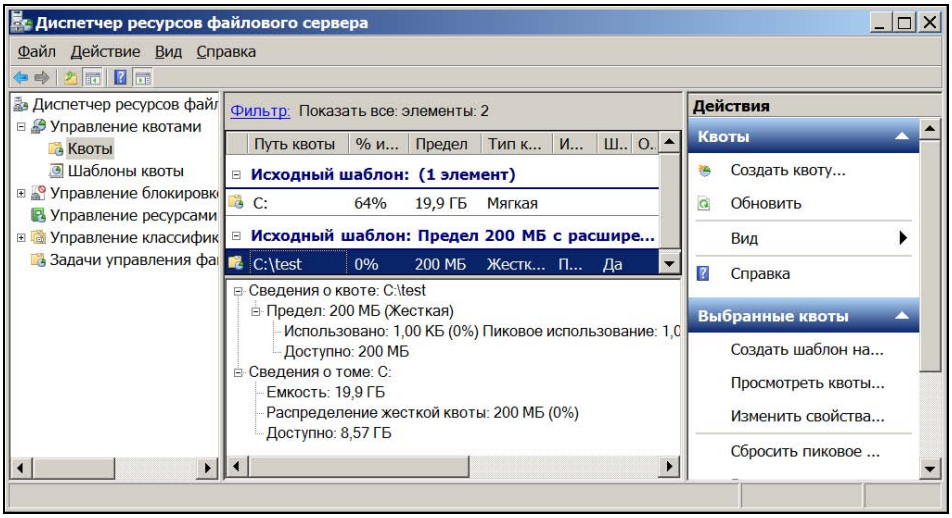


Рис. 9.7. Управление квотами в **Диспетчере ресурсов файлового сервера**

ния доступен для редактирования), запись в журнал событий, выполнение любой команды операционной системы.

Блокировка записи в папки по типам файлов в Windows

Вторая возможность, предоставляемая консолью **Диспетчера ресурсов файлового сервера**, — это блокировка записи в папку определенных типов файлов. Такая настройка позволяет запретить запись в папку файлов по заданному шаблону имени. Как правило, устанавливаются ограничения по типу файлов (по расширениям имени файла), но можно задавать и маски на само имя. В системе существует несколько заранее подготовленных шаблонов (аудио- и видеофайлы, файлы программ офиса и т. п.), легко можно добавить и свои настройки (рис. 9.8).

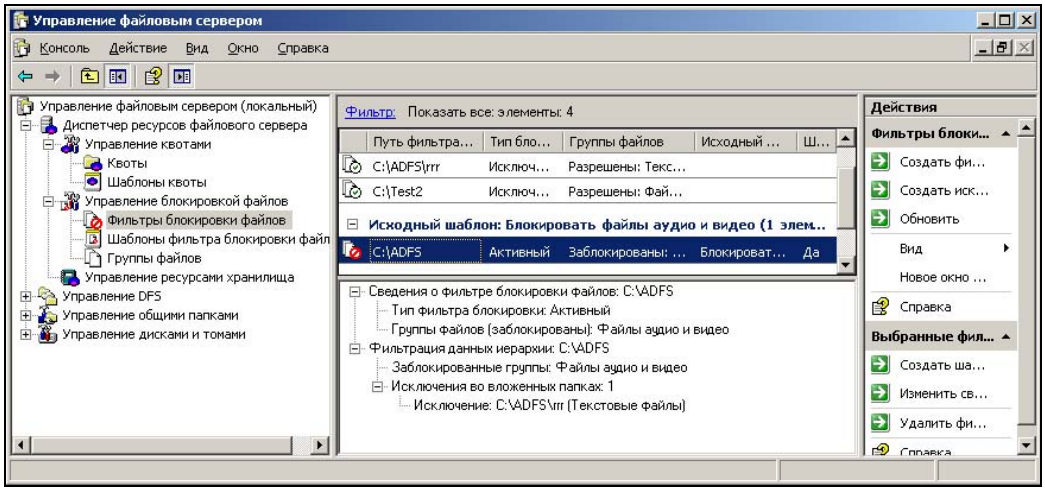


Рис. 9.8. Интерфейс операции блокировки файлов

Ограничения как по объему, так и по типу файлов можно наложить на саму папку и отдельно на вложенные каталоги. Таким способом можно достаточно точно настроить политики хранения информации.

> ***Примечание***
>
> Обратите внимание, что при задании шаблона блокировки имеется возможность явно указать разрешенные файлы. Например, можно заблокировать все видеофайлы, но разрешить те, названия которых начинаются с символов "мои" и т. п.

Блокировка по типу файлов привносит только некоторые неудобства в работу пользователей. Программа не проверяет тип содержимого сохраняемой информации, поэтому пользователи могут либо сохранять файлы в архивах, либо просто давать им другие расширения. При этом, настроив у себя новые ассоциации для типов файлов, пользователи смогут легко открывать такие файлы в программах для работы.

Настройка квотирования в Ubuntu

В Ubuntu можно настроить квоты на дисковое пространство для пользователей и для групп. Между этими квотами установлена следующая связь: если лимит для группы исчерпан, то всем пользователям, входящим в эту группу, запись на диск будет запрещена. Несмотря даже на то, что по их индивидуальным квотам они могли бы еще дозаписывать данные.

По умолчанию программы квоты в Ubuntu не установлены, необходимо добавить как собственно программу квотирования, так и комплект утилит управления квотами:

```
apt-get install quota quotatool
```

Следующим шагом необходимо включить возможность квотирования для дисков. Для этого нужно открыть в текстовом редакторе (также с правами суперпользователя) файл /etc/fstab и найти строки, монтирующие ваши диски. В листинге 9.1 приведен пример реального файла fstab и соответствующая строка, которая монтирует диск в качестве корневой файловой системы (/), выделена полужирным шрифтом.

> ***Примечание***
>
> Для удобства чтения значение UUID диска укорочено.

Листинг 9.1

```
# /etc/fstab: static file system information.
#
# <file system> <mount point> <type> <options> <dump> <pass>
proc /proc proc defaults 0 0
# /dev/sda1
UUID=a116dc47- / ext3 relatime, errors=remount-ro 0 1
# /dev/sda5
```

```
UUID=75aa5a1d-... none swap sw 0 0
/dev/scd0 /media/cdrom0 udf,iso9660 user,noauto,exec,utf8 0 0
/dev/fd0 /media/floppy0 auto rw,user,noauto,exec,utf8 0 0
```

Добавьте в выделенной строке в блок опций (через запятую) ключевое слово `usrquota` для включения квот для пользователей, `grpquota` — для включения квот для групп, или оба (включаются все квоты):

```
UUID=a116dc47-... / ext3 relatime,errors=remount-ro,
usrquota,grpquota 0 1
```

Теперь необходимо указать системе, в каком файле хранятся значения квот. Сделать это можно было и в файле fstab (указать как `usrquota=...`), но удобнее создать отдельный файл quota.user для квот пользователей и файл quota.group для квот групп. Эти файлы должны быть на каждом диске, на котором вы включаете квоты, и находиться всегда в корне диска. Создадим пустые файлы в корне диска и запретим другим пользователям доступ к этим файлам, установив разрешение с маской 600:

```
touch /quota.user /quota.group
chmod 600 /quota.*
```

Квотирование включается после перемонтирования тома. Это можно сделать после перезагрузки системы либо в процессе работы:

```
mount -o remount /
```

Теперь необходимо пересчитать реальные значения квот:

```
quotacheck -avugm
```

Не обращайте внимания на предупреждения программы, они вызваны тем, что файлы quota.user и quota.group были созданы вручную. И последняя операция по установки программы квотирования — включение квот:

```
quotaon -avug
```

После установки программы необходимо при помощи команды `edquota` настроить квоты для пользователей и групп (с ключом `-g` команда будет редактировать квоты групп):

```
edquota -u имя_пользователя
```

Эта команда открывает в текстовом редакторе файл настроек. При создании квоты на экране вы увидите примерно такое содержимое:

```
Disk quotas for user kenin (uid 1000):
Filesystem blocks soft hard inodes soft hard
/dev/sda1 25256 0 0 11 0 0
```

Параметры `block` и `inodes` показывают, сколько блоков (размером по 1 Кбайт) и дескрипторов файлов в настоящее время используется этим пользователем. Для определения квоты необходимо установить желаемое значение в блоки `soft` и `hard`. `Soft` — это "мягкое" ограничение, пользователь получит предупреждение, но даль-

нейшая запись будет возможна в течение некоторого периода времени. По умолчанию этот период установлен равным семи дням, его можно настроить командой `edquota -t`.

`Hard` — жесткое ограничение, при достижении этого значения последующая запись будет невозможна. Чтобы отключить квоту, просто установите в 0 значение соответствующего блока.

Ускорить редактирование можно, записав квоту какого-либо пользователя в качестве шаблона. Следующая команда создаст записи квот для всех пользователей (`*`, можно указать имена явно) по шаблону пользователя

`kenin`: `edquota -p kenin -u *`.

> ***Примечание***
>
> При некорректных выключениях сервера информация о реальном использовании дискового пространства может исказиться. Поэтому существует рекомендация о периодическом, по расписанию, выполнении команды `repquota -avugm`. Например, раз в месяц.

Еще несколько полезных команд: `quota` — отображает на экране параметры квоты для пользователя/группы; `repquota` — формирует отчет по реально установленным объемам и квотам для дисков.

Запрет записи на сетевые ресурсы Ubuntu по типам файлов

Скрыть файлы в папке при просмотре пользователем в Ubuntu позволяет директива Samba `veto files`. Перечисленные в такой строке файлы не будут видны пользователю и, соответственно, не смогут быть им созданы. По правилам синтаксиса строка параметров в `veto files` должна начинаться и заканчиваться слешем, все перечисляемые в ней элементы также должны разделяться слешами:

```
veto files = /*.dll/
veto files = /*.dll/*.exe/
```

> ***Примечание***
>
> Если в предоставленной в общее пользование папке существуют файлы, подпадающие под описание параметра `veto files`, и пользователям предоставлено право удаления папки, то такая папка будет удалена только в том случае, если для нее включено следующее описание: `delete veto files = yes`.

Корпоративные порталы

Корпоративные порталы обеспечивают возможность безопасного и удобного доступа пользователей к разнородной информации, позволяют интегрировать данные различных приложений, позволяют применять регламенты публикации данных (функции документооборота) и т. д.

Один из наиболее перспективных решений открытых кодов — портал LifeRay (**http://www.liferay.com/**), в нашей стране распространены также решения на основе eGroupware (**http://www.egroupware.org/**) во многом благодаря наличию русскоязычного интерфейса. Эти два решения занимают по разным оценкам порядка 2/3 эксплуатируемых порталов на основе открытого кода. Из коммерческих решений, на взгляд автора, лидирует IBM WebSphere. В последнее время разработчики предпринимают активные действия по распространению решения Microsoft SharePoint Server.

Следует обратить особое внимание, что сам портал — это платформа для реализации тех или иных решений в информационной системе конкретного предприятия. Поэтому, даже покупка коробочной коммерческой версии не позволит быстро создать корпоративный портал. Скорее всего, вы будете иметь набор разрозненных базовых функций. Внедрение корпоративного портала — достаточно сложный процесс, зависящий от состояния информационной системы предприятия, ожиданий заказчика и опытности команды внедрения. Поэтому в данной книге мы опишем только базовые моменты инсталляции бесплатных портальных решений, которые помогут вам установить портал и получить первый опыт работы с ним. После некоторого периода опытной эксплуатации вы сможете уже более обоснованно подойти к выбору программного решения и его наполнению.

Особенности порталов

Портал, по сути, является конструктором, позволяющим создать по желанию пользователя веб-сервер из отдельных кирпичиков (веб-приложений) — *портлетов*, каждый из которых предназначен для решения отдельной задачи: отображения текста или иллюстрации, вывода ленты новостей, представления библиотеки документов, реализации процедуры публикации документов и т. п. Для каждого пользователя портала создаются индивидуальные страницы из различных наборов таких модулей. Обычно они генерируются из шаблонов — предварительно разработанных страниц, оптимизированных под конкретные интересы (задачи) пользователя.

Для управления доступом к документам портала на нем создаются пользователи, объединяемые в группы. Учетные записи пользователей портала могут храниться в его базе данных, но в случае корпоративного портала обычно синхронизируются с сервером каталогов (параметры учетной записи при входе на портал проверяются на сервере каталогов предприятия, с него же копируется и свойства пользователя: фамилия, имя, телефон, адрес электронной почты и т. д.).

На портале пользователям обычно предоставляются следующие права: читателя (доступ к материалам только для чтения), полные права доступа к документам (часто называют правами редактора или автора, это право создания и редактирования документов) и права администратора страницы или сайта (возможность управлять правами пользователей, создавать новые страницы/сайты и т. п.). Эти права хранятся в собственной базе портала.

При большом числе пользователей и разнообразии предоставляемой на портале информации существует большой риск превращения веб-сервера в мусорную свал-

ку. Чтобы портал не захламился, он оснащается *системами управления содержимым* (WCM, web context management). Документы, например, могут быть доступными на портале только в заданный диапазон времени (автоматически появятся после установленного момента времени и станут недоступными по истечении срока актуальности). Кроме того, сам процесс публикации информации можно сделать регулируемым: после размещения документа на портале он будет доступен только после утверждения редактором.

Порталы интегрируются с почтовыми серверами. Наиболее часто используется возможность *подписки*: пользователь уведомляется по электронной почте в случае изменения информации, например, добавления или редактирования документа в определенной библиотеке.

Резервное копирование портала имеет некоторые особенности. Необходимо сохранить как настройки собственно веб-сервера, так и хранимые на нем данные. Сохранение настроек веб-сервера должно производиться по правилам самого сервера. Например, для Linux-серверов обычно достаточно сохранить папку размещения файлов (папку, соответствующую корню веб-сервера) и конфигурацию веб-сервера. Для IIS необходимо применять специальную утилиту, которая экспортирует настройки в файл. Поскольку данные портала хранятся на сервере баз данных, то необходимо выполнить и резервное копирование сервера баз данных по его правилам.

Установка Liferay на сервере Ubuntu

Liferay — кроссплатформенное решение. Это Java-приложение. Для его работы нужен сервер приложений. Это может быть коммерческое решение (WebSphere, WebLogic и аналогичные) либо одно из бесплатных, которые, например, включены в комплекты *(bundle)*, загружаемые с сайта разработчика (Tomcat, Glassfish, Jboss и др.). Сам портал соответствует стандартам (JSR 168, JSR 286), поэтому портлеты могут создаваться независимыми разработчиками, а пользователи смогут расширять функциональность своих решений.

Предлагаемые к загрузке бесплатные *(community edition)* версии портала полностью готовы к работе. Нужно только сохранить загруженные файлы на диск и запустить сервер приложений. Далее следовать указаниям мастера операций, который завершит локальные настройки портала и, при необходимости, создаст на портале образец организации — 7 Cogs и заполнит его некоторой информацией.

> ***Примечание***
>
> Загружаемые комплекты настроены на работу с внутренней базой данных портала. Такая конфигурация может использоваться для тестирования, разработки страниц, но должна быть заменена при переходе к эксплуатации: информацию необходимо перенести на один из специализированных серверов баз данных.

Liferay является, по сути, профессиональным порталом, позволяющим реализовать практически любые функции на основе стандартов, принятых для построения порталов. Прежде чем начать настраивать и эксплуатировать его, обязательно следует изучить сопроводительную документацию.

Для Liferay доступны для загрузки как собственно портал, так и готовые его сборки с различными серверами приложений (см. **http://www.liferay.com/**). Далее описан запуск бесплатного варианта портала, который на момент подготовки книги имел версию 6.1.

Портал Liferay предоставляется в нескольких вариантах (с разным сервером приложений). Выбор определяется в первую очередь предпочтением администратора. Загрузка программы производится со страницы **http://www.liferay.com/downloads/liferay-portal/available-releases**.

Для работы портала необходимо наличие на компьютере пакета Sun Java Development Kit. В силу некоторых лицензионных особенностей установка этого пакета через репозиторий недоступна. Поэтому нужно воспользоваться операциями, описанными на странице **https://help.ubuntu.com/community/Java**.

После установки JDK следует разархивировать загруженный файл портала. Например, в случае пакета на основе Tomcat нужно выполнить следующую команду:

```
unzip liferay-portal-tomcat-6.1.0-ce-ga1-20120106155615760.zip
```

> ***Примечание***
>
> Архив желательно распаковать в папку с программными кодами, поскольку приложение не требует установки и будет работать из созданной папки.

После разархивирования нужно стартовать портал с помощью сценария startup.sh, располагающегося в папке tomcat-<*версия*>/bin/. При необходимости автозапуска ссылку на этот файл нужно поместить в папку /etc/rc5.d/.

Чтобы войти в него, достаточно набрать в строке обозревателя адрес **http://<*имя_сервера*>:8080**. Портал может запускаться довольно долго (зависит от конфигурации системы). При первом входе нужно настроить параметры портала

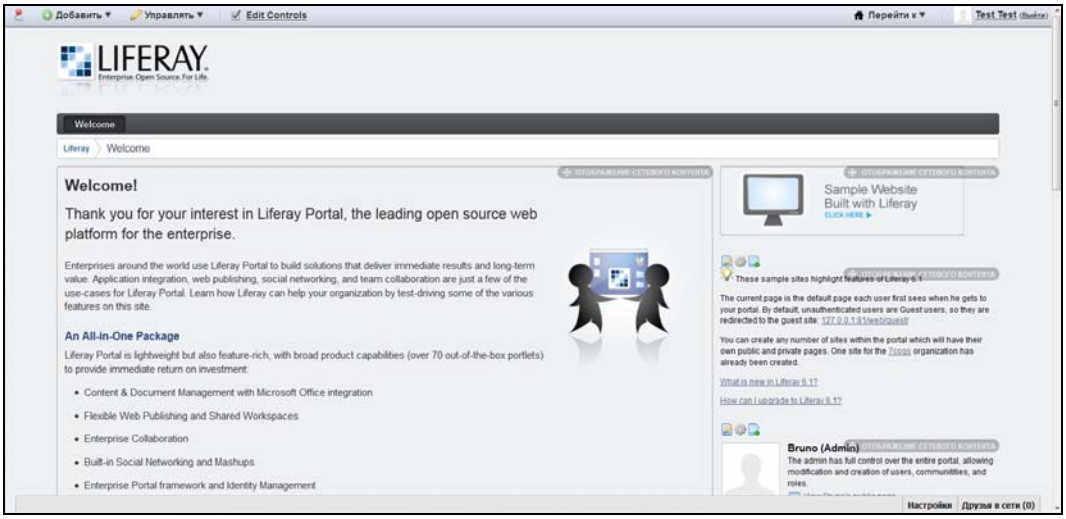


Рис. 9.9. Пример страницы портала Liferay

(по умолчанию предлагается использовать встроенную базу), установить язык и задать пароль пользователя. После чего вы попадете на страницу приветствия (рис. 9.9) и можете начать создавать свой портал.

Интерфейс портала во многом русифицирован (рис. 9.10). Сам процесс построения портала ничем не отличается от традиционного: вы создаете страницы, размещаете на них портлеты, заполняете информацией и назначаете права доступа.

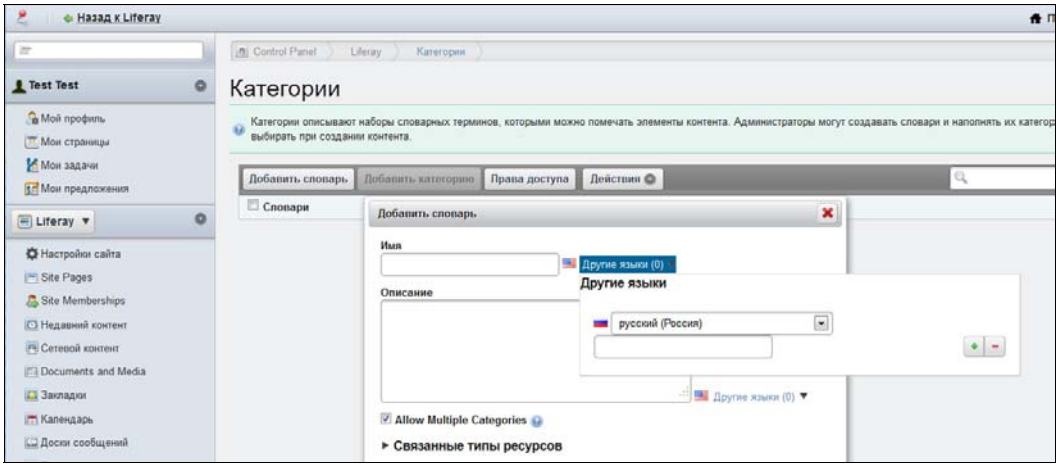


Рис. 9.10. Русифицированный интерфейс портала Liferay

Портальные решения от Microsoft

Портальные решения от Microsoft представлены несколькими продуктами. Во-первых, сама технология представлена решением SharePoint Foundation 2010 (название предыдущей версии — Windows SharePoint Services 3.0, иногда ее называют также SharePoint Services 2007, чтобы отличить от Windows SharePoint Services 2.0, которые было принято называть просто Windows SharePoint Services). Технология содержит все компоненты, необходимые для создания портала: "движок" (веб-приложение портала), веб-части (так разработчик называет портлеты в своем решении), средства управления содержимым и т. д. Сама технология полностью бесплатна, установочный пакет входит в состав R2-выпусков сервера Windows 2008 и может быть свободно загружен для других выпусков сервера.

> ***Примечание***
>
> SharePoint Foundation 2010 может быть установлен на 64-разрядные версии Windows 7/Vista в целях отладки (тестирования) проектов.

Во-вторых, разработчик выпустил серверы портала — SharePoint Server 2010 (SharePoint Server 2007 предыдущей версии портала). Серверы являются коммерческим продуктом и отличаются рядом дополнительных возможностей (дополнительные веб-части, некоторые функциональные возможности — отличия описаны на

странице **http://sharepoint.microsoft.com/en-us/buy/pages/editions-comparison.aspx**). Серверное портальное решение встроено также в новый продукт — Office 365.

> ***Примечание***
>
> Прежде чем покупать серверное решение (а это стоимость лицензии сервера и клиентских лицензий на подключение), следует оценить возможность реализации требований организации на бесплатном решении. В большинстве случаев достаточно будет установки только самой технологии.

В-третьих, для проектирования и отладки собственно портала (если функционала имеющихся веб-частей недостаточно) доступен продукт SharePoint Designer 2010. Этот продукт бесплатен, может быть загружен свободно с сайта изготовителя в версиях как для 64-битных платформ, так и 32-битных.

В-четвертых, администраторам доступны для свободной загрузки образцы (шаблоны) различных портальных решений, которые могут быть использованы для расширения функциональности.

При выборе решения следует учитывать требования к порталу (зачастую предполагаемая функциональность обеспечивается менее ресурсоемкой версий портала), имеющиеся аппаратные ресурсы (так, требования для установки SharePoint Foundation 2010 существенно выше, например, только оперативной памяти требуется не менее 8 Гбайт, а платформа должна соответствовать *x*64), доступность бесплатных шаблонов (например, для SharePoint Services 3.0 есть локализованные шаблоны, в то время как для более новой версии автор смог найти только английские варианты).

Где найти помощь по SharePoint

Портальным технологиям Microsoft посвящено значительное число материалов. Домашняя страница служб SharePoint 3.0 — **http://technet.microsoft.com/en-us/windowsserver/sharepoint/**, SharePoint Foundation 2010 — **http://technet.microsoft.com/ru-ru/sharepoint/ee263910.aspx** (ссылка на нее есть на домашней странице служб).

Порядок установки описан в статье **http://technet.microsoft.com/ru-ru/library/cc288751.aspx**. Если требуется установить решение на Windows 7/Vista, то с особенностями такого процесса можно ознакомиться по ссылке **http://msdn.microsoft.com/ru-ru/library/ee554869%28office.14%29.aspx**.

В библиотеке MSDN раздел, посвященный данной технологии, находится по адресу **http://msdn.microsoft.com/ru-ru/library/bb931739%28v=office.12%29.aspx**.

Техническая библиотека Windows SharePoint Services 3.0 в формате CHM доступна к загрузке по ссылке **http://www.microsoft.com/download/en/details.aspx?id=22086**.

Особенности установки решения на линейку Windows Small Business Server описаны в статье **http://technet.microsoft.com/en-us/library/cc671966%28WS.10%29.aspx**.

Установка портала Windows

Установка портала (как сервера, так и собственно портальной технологии) проводится в несколько этапов:

1. Подготовка операционной системы.
2. Запуск мастера установки технологии SharePoint Services/SharePoint Foundation.
3. Запуск мастера настройки продуктов и технологий.
4. Установка обновлений.
5. Административная настройка параметров портала.
6. Установка дополнительных шаблонов.
7. Создание и настройка пользовательских страниц/узлов.

Подготовка операционной системы

Портальные решения должны быть установлены на серверные операционные системы Windows. Как SharePoint Services, так и SharePoint Foundation могут быть установлены на Windows Server 2008 и на Windows Server 2003, причем версия SharePoint Foundation 2010 требует *только* 64-битной операционной системы. Поэтому если вы используете 32-битный сервер Windows, то выбор решения будет однозначен — SharePoint Services 3.0.

Обратите внимание, что службы Windows SharePoint Services являются весьма "тяжелым" продуктом, для достижения приемлемой производительности необходимо устанавливать их на современный, не менее чем двухпроцессорный сервер с объемом оперативной памяти не менее 2 Гбайт и, желательно, с быстрыми дисками (например, объединенными в RAID-массив). В противном случае задержки при выполнении операций сделают работу пользователей некомфортной.

До начала установки портальной технологии на сервер должен быть установлен/добавлен ряд компонентов. Если говорить о SharePoint Foundation 2010, то необходимо добавить полтора десятка пакетов: собственный клиент Microsoft SQL Server 2008, исправление для Microsoft Windows (KB976462), Windows Identity Foundation (KB974405), среду выполнения Microsoft Sync Framework 1.0 (*x*64) и т. д. При наличии подключения к Интернету эти установки не представляют сложности: мастер операций предлагает перейти на страницы загрузки компонентов, проблемы могут возникнуть только из-за потери времени, необходимого для загрузки достаточно объемных пакетов установки. Если необходимо установить портал на сервер в локальной сети без выхода в Интернет, то сначала надо загрузить все дистрибутивы. Помочь в этом может сценарий на PowerShell, который копирует из Интернета все пакеты за одну операцию. Сценарий — *Sharepoint Prerequisites Windows PowerShell Script* — доступен по ссылке **http://gallery.technet.microsoft.com/bcf3332d-f726-4ac7-b01a-eeda4b7ece8e**. При желании из него можно получить список файлов (правда, в сценарии приведены ссылки на англоязычные версии, так что их необходимо подкорректировать для локализованной версии) и загрузить их, например, при помощи утилиты `wget`.

При установке SharePoint Services 3.0 на Windows Server 2008 необходимо только включить все компоненты .NET Framework 3.0. Сделать это можно через приложение **Диспетчер сервера**, но быстрее воспользоваться командной строкой:

```
Servermanagercmd -install NET-Framework -allSubFeatures
```

Стандартная установка технологии SharePoint для хранения конфигурации страниц и данных использует бесплатную версию SQL-сервера. Эта версия ограничена в объеме хранения, поэтому в случае необходимости полная версия сервера баз данных должна быть подготовлена до запуска процесса установки.

Запуск мастера установки технологии

Для установки технологии нужно загрузить с сайта Microsoft инсталляционный пакет и запустить его на выполнение.

Первым шагом следует проверить наличие необходимых компонентов, установить требуемые роли. Делается это выбором ссылки **Установить необходимое ПО** (рис. 9.11).

Рис. 9.11. Установка SharePoint Foundation 2010

Если программа установки обнаружит отсутствие необходимых компонентов, то вы их должны загрузить (страница со ссылками загрузки — **http://technet.microsoft.com/ru-ru/library/cc262485.aspx** — открывается по ссылке **Дополнительные сведения об этих необходимых компонентах** внизу окна программы проверки).

Операция установки имеет только два варианта: автономно (стандартный для SharePoint Services) или на ферму (расширенный). В автономном варианте установка всех компонентов выполняется на локальный сервер и используется бесплатная версия сервера баз данных. При выборе расширенного варианта можно, например, для хранения информации задать уже установленный сервер баз данных, указать его расположение, параметры доступа и т. д.

> ***Примечание***
>
> Windows SharePoint Services позволяют распределить нагрузку на несколько серверов, если выполнить установку *фермы*. В данной книге мы не будем рассматривать этот вариант, поскольку режимы установки отличаются несущественно и необходимые действия хорошо описаны в документации. Следует также учесть, что установка в режиме фермы предполагает наличие сервера баз данных, являющегося коммерческим продуктом.

Обратите внимание, что если вы ставите службы SharePoint не в первый раз (например, ранее удалили службы и пытаетесь поставить их заново), то необходимо вручную удалить существующую базу до начала операций. Используйте для этого средства управления SQL-сервера.

Запуск мастера настройки продуктов и технологий

Если установка компонентов прошла без ошибок, то мастер операций установки при завершении своей работы предложит сразу запустить мастер настройки продуктов и технологий. Если были ошибки, то после их устранения вызвать данный мастер можно будет из папки **Администрирование**.

Мастер выполняет операции создания базы данных конфигурации, настройки прав, защиты ресурсов, регистрации служб, настройки приложения администрирования и т. д. — всего 10 этапов. Во время работы мастера от администратора не требуется выполнять никаких действий: даже нет ни одного выбора той или иной опции.

Установка обновлений

Сразу после завершения операций установки не забудьте обновить систему. Например, для установки SharePoint Services 3.0 к загрузке доступен пакет со встроенным вторым сервис-паком. При этом — на момент подготовки данного издания — был доступен к загрузке третий пакет обновления (он называется пакетом обновления 3 (SP3) для Windows SharePoint Services 2007) и первый сервис-пак для SharePoint Foundation 2010 (в установочный пакет сервис-пак не встроен).

Для нахождения обновлений можно использовать поиск по узлу загрузок Microsoft (**http://www.microsoft.com/download/**) или посетить **Центр обновления Windows** (ссылка на него включена в окно установки программы).

Административная настройка параметров портала

После завершения работы мастера настройки продукта можно открыть страницу портала и начать с ним работу (рис. 9.12). Однако лучше выполнить еще несколько административных настроек, перейдя на страницу администрирования.

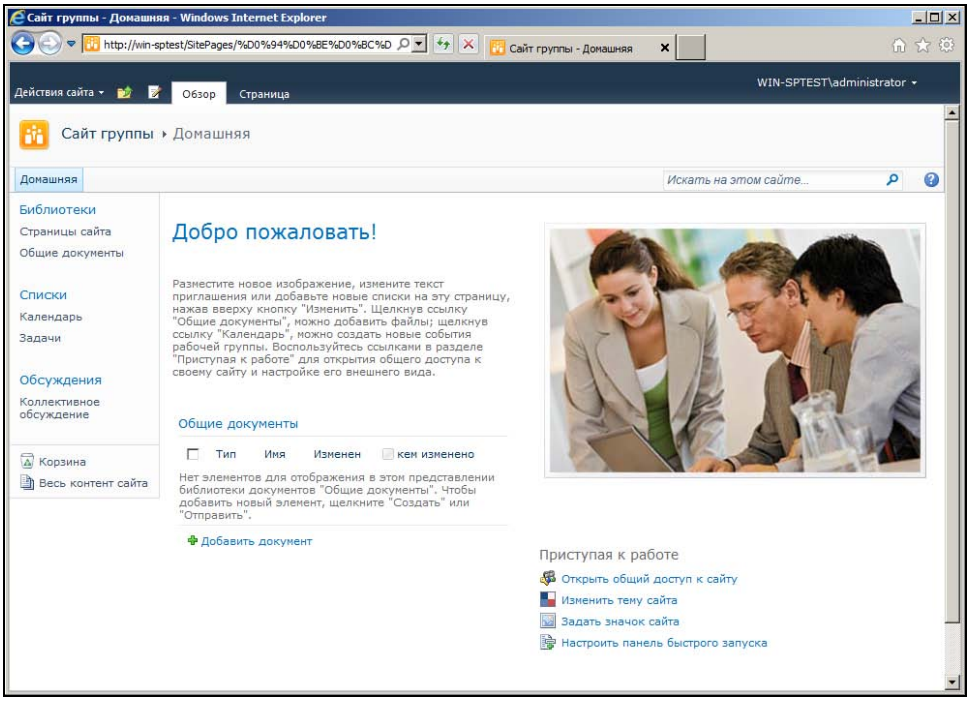


Рис. 9.12. Стартовая страница SharePoint Foundation 2010

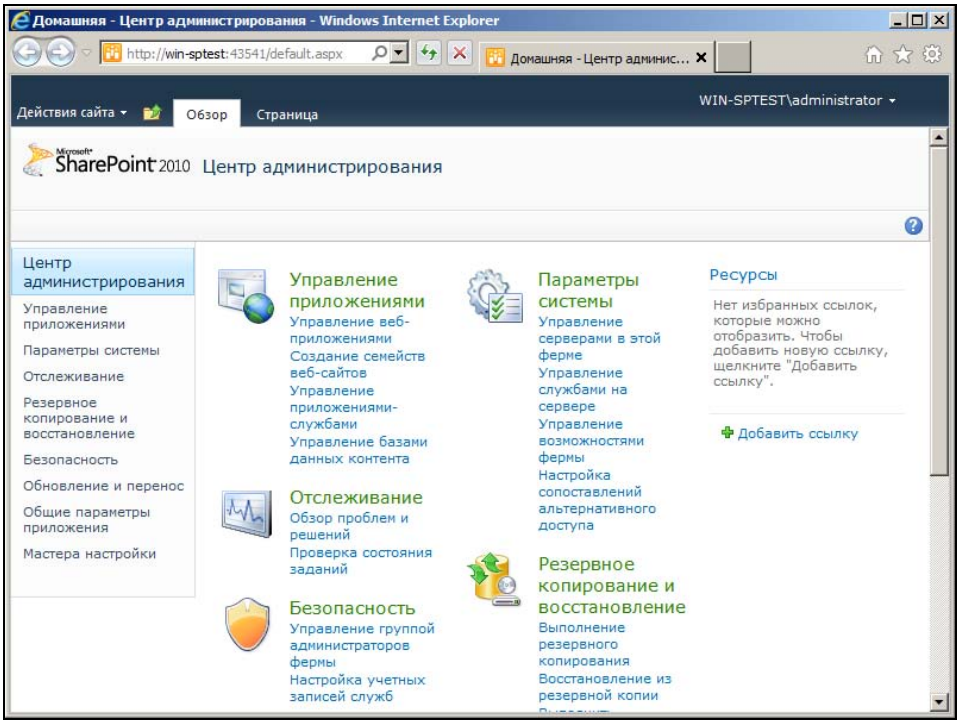


Рис. 9.13. Центр администрирования SharePoint 2010 (вид **Обзор**)

Задача **Центр администрирования SharePoint** (рис. 9.13) объединяет в себе административные операции над узлом и при первом посещении отображает список задач, которые должен выполнить администратор узла. Достаточно поочередно перейти по соответствующим ссылкам и настроить те параметры, о которых сообщает система. Каждая задача содержит подробное описание необходимых действий и ссылки для перехода к соответствующим интерфейсам управления.

> ***Примечание***
>
> Задача администрирования SharePoint включает возможность настройки многих дополнительных опций (например, создание нового пула приложений). Начиная работу с SharePoint, не стоит менять настройки по умолчанию для неизвестных вам опций.

Обычно на первом этапе администрирования служб достаточно сконфигурировать почтовый сервер, определиться с учетными записями администраторов и настроить параметры резервного копирования.

Создание и редактирование страниц узла

Функциональность портала расширяется за счет добавления новых *узлов и страниц* в уже существующие узлы. Обе эти операции легко могут быть выполнены обычным пользователем, которому на портале предоставлены соответствующие права.

Узлы SharePoint создаются буквально одним щелчком мыши. Поэтому создать новый узел очень удобно, например, для подготовки конкретного совещания. На узле можно разместить обсуждаемые документы, список участников, перечень заданий (с отслеживанием состояния), организовать обсуждение (по типу онлайновых конференций) или опрос.

Новые страницы портала создаются на основе *шаблонов.* Шаблоны фактически являются страницами узла с типовыми элементами, подобранными и настроенными для использования по требуемым целям. Например, заменены заголовки списков, другие имена даны столбцам списков и т. п.

Подобную оптимизацию легко выполнить на любой странице. Зайдите на необходимую страницу с административными правами и перейдите в режим редактирования (нажатием на кнопку **Действия узла** в правом верхнем углу). В этом режиме можно как отредактировать параметры веб-частей, так и добавить на страницу новые элементы (рис. 9.14).

> ***Примечание***
>
> В узел можно добавлять веб-части (Web-part). Некоторые из них доступны бесплатно в Сети. Однако в большинстве случаев для прикладных целей необходима разработка новых веб-частей. При отсутствии в штате компании специалистов, имеющих опыт программирования, соответствующие работы придется заказывать в специализирующихся компаниях.

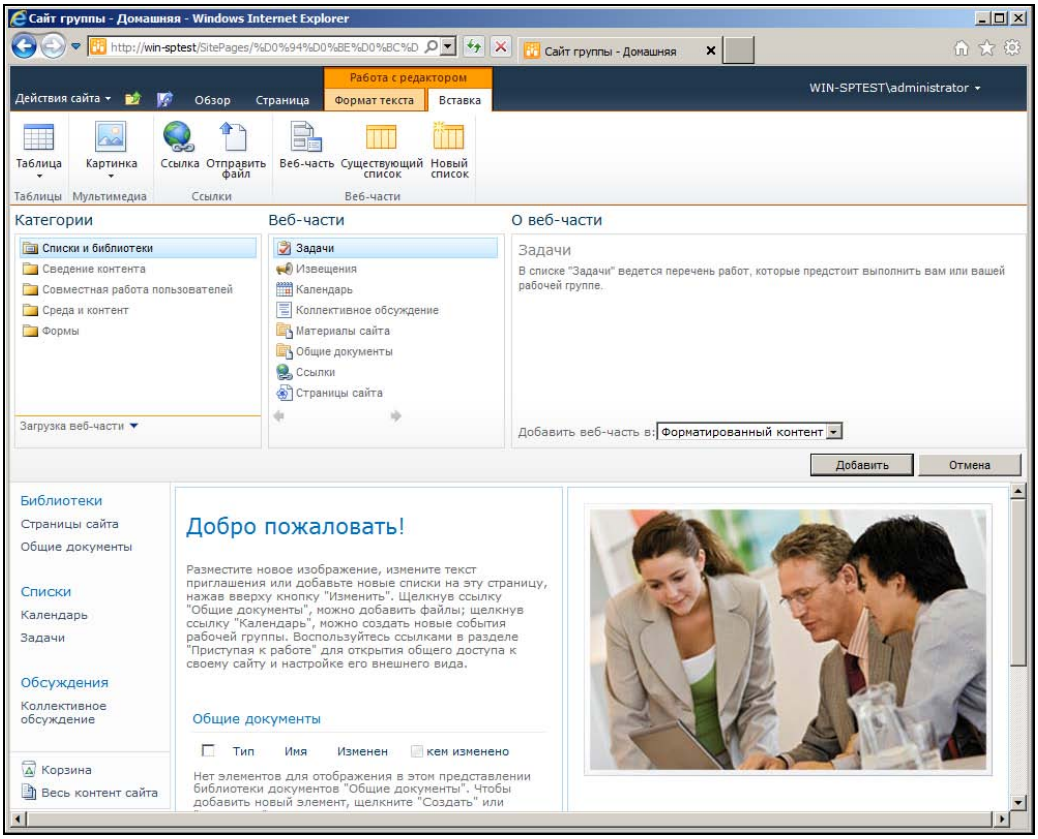


Рис. 9.14. Режим редактирования страницы узла SharePoint

Используйте возможности штатных элементов SharePoint

Входящие в состав SharePoint элементы обладают рядом интересных возможностей, на которые часто не обращают внимания, сохраняя настройки по умолчанию.

Так, библиотеки документов можно настроить на версионность. Иными словами, если какой-то документ, хранящийся на узле, будет изменен, то на сервере сохранятся как исходная копия, так и отредактированная версия. Это очень удобная функция, которая включается в свойствах библиотеки.

Для библиотек можно настраивать различные варианты отображений. Можно добавлять новые столбцы данных, фильтровать списки по любым критериям и т. п. Таким образом, на основе одной библиотеки документом можно создать оптимизированные для различных страниц списки данных.

Другая возможность — наличие оповещений. При включении этой функции вы можете настроить получение сообщений по электронной почте в случае появления в библиотеке нового документа или изменении существующего. Таким способом очень удобно следить, например, за библиотекой нормативных документов в компании.

В SharePoint Foundation включена возможность настройки *workflow* — связанных операций создания документов (например, отправки на подтверждение и публикацию). Для настройки этого процесса по типовым шаблонам нужно использовать SharePoint Designer, а для создания собственных процессов необходимо привлечение программиста и работа в Visual Studio.

Установка поискового сервера по общим ресурсам

Поддерживать идеальную структуру хранения документов на практике невозможно. Поэтому функция поиска зачастую становится единственной возможностью быстро найти необходимый документ. При использовании служб Windows SharePoint Services можно легко добавить в среду совместной работы возможности поиска по сайтам SharePoint, файловым ресурсам общего доступа, веб-сайтам, общим папкам Exchange и сторонним репозиториям с помощью Microsoft Search Server Express 2010.

Express-выпуск поискового сервера бесплатен, доступен к загрузке со страницы **http://www.microsoft.com/enterprisesearch/searchserverexpress/en/us/default.aspx**. Сервер можно установить вместе с существующими службами SharePoint, при этом возможен как вариант смены основного узла группы на поисковый интерфейс, так и установка поискового сервера в качестве нового узла с доступом по произвольному порту.

> ***Примечание***
>
> Добавление функции поискового сервера еще больше увеличивает нагрузку на компьютер. Обратите внимание, что полноценная работа возможна только при наличии в системе не менее 4 Гбайт оперативной памяти и современного многоядерного процессора.

Сайт поискового сервера нуждается в административной настройке. Для нормальной работы нужно указать, что индексировать, как (какой учетной записью, необходимость прокси-сервера) и когда (создать расписание). Кроме того, необходимо определить параметры электронной почты, поскольку они потребуются для создания оповещений.

Обратите внимание, что по умолчанию поисковый сервер использует учетную запись локальной системы. Эта запись не имеет прав доступа к сетевым ресурсам, поэтому при необходимости индексирования сетевых ресурсов в правилах обхода следует определить учетную запись для соответствующей области поиска. Такая учетная запись должна иметь права для чтения файлов из области поиска, но желательно, чтобы эти права не были административными на удаленном сервере. При большом объеме индексируемых документов можно ограничить интенсивность операции через пункт меню **Правила воздействия программы-обходчика**.

После добавления областей поиска и запуска индексирования поисковый сервер готов к работе. Другие операции (например, резервное копирование, смену оформления страниц и т. п.) вы можете проделать в последующее время.

Настройка автоматических оповещений об изменениях документов на чужих серверах

В службах SharePoint, как уже говорилось, настраиваются оповещения по электронной почте об изменениях любого элемента (библиотеки, списка, документа и т. д.). Этот функционал позволяет с помощью поискового сервера наблюдать за различными веб-страницами (не только в локальной сети, но и в Интернете) и оповещать вас по электронной почте в случае их изменения. Так вы сможете следить за новостями по интересующим вас темам.

Для этого достаточно сформировать запрос, который будет показывать в качестве результатов документы с нужной вам страницы Интернета. При отображении результатов запроса в заголовке поискового сервера появляется пункт **Оповещать меня**. Если перейти по этой ссылке, то вы попадете на страницу настройки оповещений. Выберите наиболее подходящий вариант контроля и предоставьте серверу самостоятельно отслеживать изменения и сообщать об этом вам.

ГЛАВА 10

Обеспечение работы мобильных пользователей

Сегодня обеспечение работы мобильных пользователей становится едва ли не главной задачей администратора информационной системы. Пользователь должен из любого места получить доступ по Интернету к той информации организации, которая ему потребуется. Кроме того, создание филиалов компаний требует настройки их взаимодействия с информационной системой центрального офиса. При этом возникает еще одна, сугубо внутренняя, задача дистанционного управления оборудованием удаленного офиса.

Традиционные способы решения перечисленных задач:

- организация удаленного доступа к почтовым ресурсам и порталу компании;
- настройка терминального доступа;
- предоставление пользователям прав доступа к внутренней сети по технологии VPN;
- настройка транспорта между удаленными офисами (VLAN, VPN);
- синхронизация данных центрального офиса и филиалов;
- внедрение технологий управления по Интернету (управление по отдельной сети, управление поверх IP);
- перенос данных в облачные хранилища.

Удаленный доступ к почте и порталу обычно реализуется по протоколу HTTP(S) соответствующей настройкой правил входящего трафика межсетевого экрана. Сложностей в реализации данного требования у администраторов обычно не возникает. Поэтому более подробно рассмотрим специфику выполнения оставшихся требований.

Терминальный доступ

Терминальный доступ обеспечивает работу пользователя на удаленной системе. Все вычисления производятся на мощном удаленном компьютере (его называют *терминальным сервером*), а пользовательский компьютер является лишь локальной

консолью. Пользовательский компьютер практически использует только монитор, клавиатуру, мышь.

Терминальные решения существуют как для систем Windows (для использования подключений к удаленным рабочим столам требуется оплата дополнительных лицензий), так и для Linux (существуют как проприетарные решения, например, SunRay от компании Sun Microsystems, так и бесплатные продукты — NX Server/Client, VNC-сервер и др.).

Терминальные серверы Linix

Для удаленной работы на сервере Linux обычно используется подключение по протоколу SSH. После подключения пользователь начинает выполнять задания на удаленной системе. Каких-либо специальных настроек для этого (кроме установки сервера SSH) на сервере не требуется. При необходимости может быть реализовано отображение графического экрана удаленной системы локально.

Соответствующие описания даны в *разд. "Удаленный доступ к Linux" главы 2*.

Терминальные серверы от Microsoft

Серверы Windows включают в себя все необходимое для настройки терминального сервера. При этом включение данного режима возможно в двух вариантах. Один предназначен только для настройки системы администраторами сервера. Он включается в свойствах сервера, разрешает одновременное функционирование до двух учетных записей администраторов и не требует никаких дополнительных лицензий. Режим удаленных рабочих столов позволяет подключить неограниченное количество пользователей (лимитируется только мощностью аппаратной части и числом лицензий), но требует приобретения дополнительных лицензий.

Для использования подключений к удаленным рабочим столам в локальной сети должен присутствовать сервер лицензий, который обязательно должен быть активизирован через сайт изготовителя. То же относится к клиентским лицензиям. Без активизации лицензий сервер создает временные лицензии, которые действуют в течение 90 дней.

> ***Примечание***
>
> При необходимости администраторы легко найдут в Сети любые рекомендации по выполнению данной операции.

Постоянные лицензии "привязываются" к пользователям или компьютерам (в зависимости от приобретенного типа), но периодически обновляются (эта возможность присутствует с Windows 2000 SP3), чтобы восстановить лицензии, "отданные" компьютерам, которые уже больше не работают в сети (например, вышли из строя).

Установка самого терминального сервера не представляет сложности. Достаточно добавить соответствующий компонент (роль) системы.

Особенности установки ПО на сервере терминалов

Режим терминального сервера не предназначен для работы программ, вызывающих интенсивную нагрузку на процессор. Такие задачи целесообразнее решать на локальных системах. Терминальный сервер предназначен прежде всего для "обычных" офисных программ.

> ***Примечание***
>
> Новая версия RDP-протокола реализует возможности технологии RemoteFX, которая использует графические возможности сервера. В этом случае увеличивается трафик между сервером и клиентом (поскольку производится пересылка уже самих изображений, а не инструкций), но снижаются требования к графической подсистеме клиента. Поддерживают данную технологию только клиенты Windows 7.

Установка прикладных программ в режиме приложений подразумевает наличие специальных условий, которые реализуются автоматически при запуске установки через утилиту установки и удаления программ, расположенную в Панели управления. Этот режим автоматически включается при попытке запуска стандартных файлов установки (setup.exe), но в него можно перейти и вручную, если набрать в командной строке `change user /install`. А по завершении установки восстановить нормальный режим командой `change user /execute`.

После установки приложения имеет смысл проанализировать дополнения, внесенные в раздел `Run` реестра. Например, многие программы, инсталлируемые на терминал, выводят в системной области панели задач некие индикаторы. Так, антивирусная программа показывает наличие и состояние защиты на компьютере. В большинстве случаев такие индикаторы только отнимают лишние ресурсы системы и могут быть отключены в целях повышения производительности.

Некоторым программам могут понадобиться особые конфигурации установки для режима терминальных служб. Например, пакет MS Office XP невозможно установить без специального файла настроек, который следует загрузить с информационного сервера Microsoft.

> ***Примечание***
>
> Разработчики не гарантируют работоспособность всех прикладных программ на терминальном сервере в режиме приложений. Но за все время работы с сервером автору не приходилось встречаться с ситуацией, когда прикладная программа не работала в этих условиях.

Для корректной работы приложений в режиме терминального сервера должен выполняться ряд условий, прежде всего, отсутствие записи данных в каталоги самой программы или в четко прописанные папки жесткого диска. Понятно, что на практике можно встретить программу, которая будет некорректно работать в режиме терминала. Исправить подобную ситуацию призваны специальные сценарии, исполняемые при входе пользователя в систему.

По умолчанию при каждом входе в терминальную сессию исполняется сценарий USRLOGON.CMD. Если программе необходима дополнительная подготовка окружения, то ее можно включить в подобный сценарий.

Примечание

Администратор может добавить свои файлы сценариев, выполняемых при входе в систему, откорректировав значение параметра `AppSetup` в ключе `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`.

Безопасность при работе с терминальным сервером

Подключение к удаленному рабочему столу реализуется по безопасному протоколу. Лучший вариант защиты — использование сертификатов, требует разворачивания в организации системы публичных ключей (PKI). Наименее защищенный вариант предполагает традиционное шифрование RDP-протокола. Администратор имеет возможность установить, например, нижний предел безопасности: использовать только максимальные возможности, в этом случае подключения от клиентов с предыдущими версиями ОС станут невозможны.

Выбор степени защиты осуществляется администратором через **Конфигурацию узла сеансов удаленных рабочих** столов путем редактирования свойств подключения (рис. 10.1).

В этом же окне можно выбрать сертификат, который будет использован для защиты подключения (по умолчанию выбирается автоматически сгенерированный).

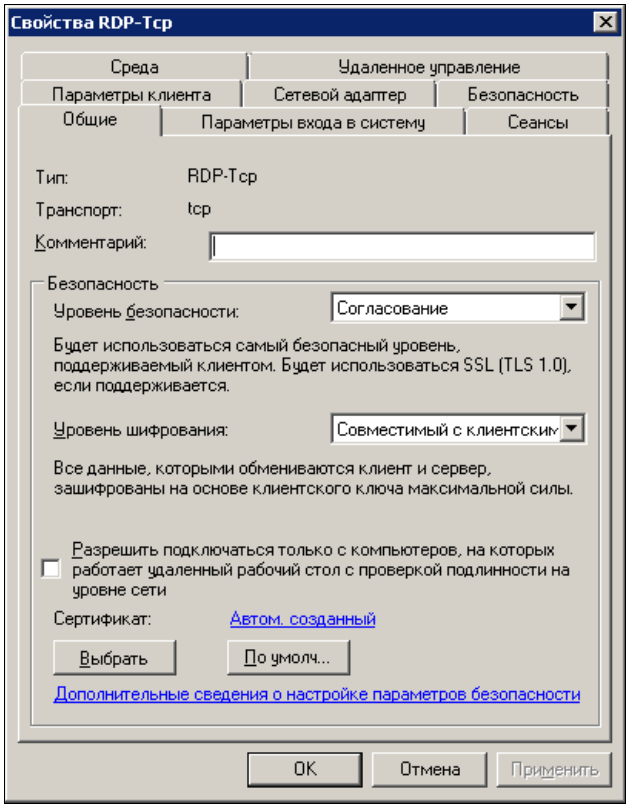


Рис. 10.1. Настройка параметров безопасности RDP-подключения

Если к используемому сертификату нет доверия на клиентском компьютере, то при попытке подключения пользователю придется выбрать необходимое действие (рис. 10.2).

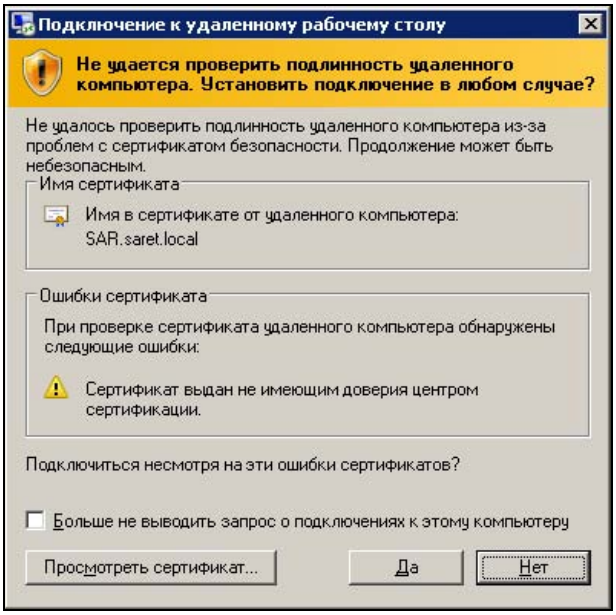


Рис. 10.2. Ошибка проверки подлинности удаленного компьютера

При подключении к терминальной сессии возможен также вход с помощью смарт-карты. Это существенно повышает безопасность работы в системе.

По умолчанию подключение к удаленному рабочему столу разрешено только администраторам и членам группы **Пользователи удаленного рабочего стола**. Поскольку эта группа первоначально пуста, то в нее нужно добавить соответствующих пользователей.

Второе место, где контролируется право подключения, — это параметр учетной записи пользователя (на вкладке **Профиль** удаленных рабочих столов). По умолчанию это право *включено* для каждой учетной записи. Но администраторы могут задействовать этот параметр для индивидуальных настроек.

Администратор узла удаленных рабочих столов (точнее, тот пользователь, которому такое право дано протоколом RDP; по умолчанию это только администраторы сервера; но при необходимости данное значение можно изменить, воспользовавшись оснасткой управления параметрами RDP-протокола) имеет возможность подключиться к пользовательской сессии и полностью видеть все, что делает пользователь. Данный режим обычно служит для оказания помощи пользователям сервера. Эта возможность включается через задачу управления терминальными сессиями. По умолчанию для подключения администратора система сначала запрашивает согласие пользователя. Но администратор может включить режим, при котором подключение будет происходить и без согласия пользователя.

Удаленные приложения

Часто пользователи подключаются к терминальному серверу для работы только в каком-либо конкретном приложении. Существуют специальные технологии публикации одного приложения, лидером таких решений являются продукты Citrix. Для терминалов Microsoft можно реализовать такие настройки подключения, которые внешне соответствуют подключению к одной задаче.

В версии терминальных серверов Windows 2000/2003 подобная настройка решалась просто. Достаточно в свойствах подключения на вкладке **Программы** указать параметры вызываемой задачи (рис. 10.3). Настройку запускаемого приложения администраторы обычно выполняли для бухгалтеров: подключение к терминальному серверу для них воспринималось просто как запуск программы 1С.

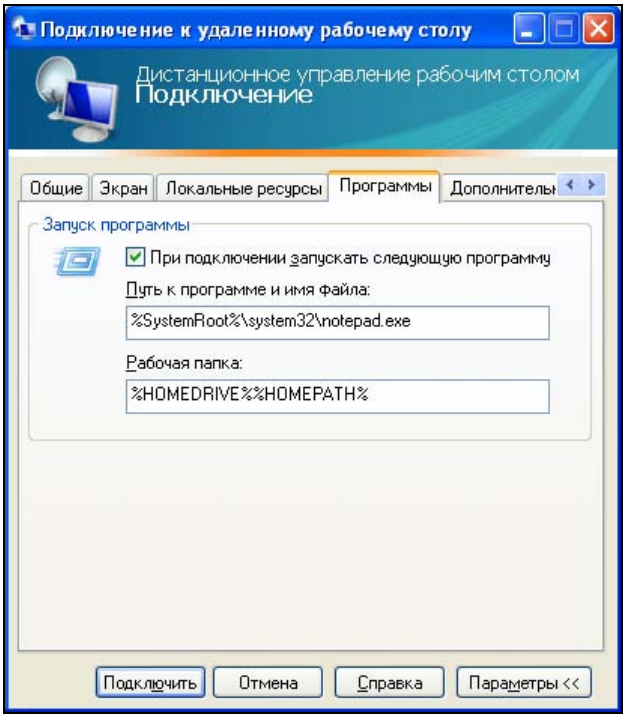


Рис. 10.3. Настройка запуска в терминальной сессии заданного приложения

После этого при подключении пользователя к терминальному серверу автоматически запускалось указанное приложение. Если пользователь завершал работу в приложении, то вслед за его закрытием прерывалось и подключение к терминальному серверу.

С появлением новой версии протокола подключения к терминальному серверу возможность указания запускаемого приложения появилась не только на клиентской стороне, но и на сервере. При этом технология подключения не изменилась. При подключении пользователя также полностью формируется терминальная сессия и

только после этого осуществляется запуск программы. Причем для клиентов, использующих предыдущую версию протокола (предыдущую версию программного обеспечения терминального клиента), будет просто открываться рабочий стол терминального сервера — параметры настройки подключаемого приложения игнорируются.

Удаленные приложения в Windows Server 2008 настраиваются через **Диспетчер удаленных приложений служб терминала** выбором опции **Добавить удаленное приложение** в правой панели навигации. После этого мастер проведет вас через все шаги назначения параметров удаленного приложения. Перечень всех приложений, настроенных для удаленного использования, доступен в нижней части окна оснастки (рис. 10.4). Данная оснастка позволяет из одного места настраивать основные параметры терминального сервера. Панель навигации в правой части окна отображает операции, доступные для каждого выделяемого объекта.

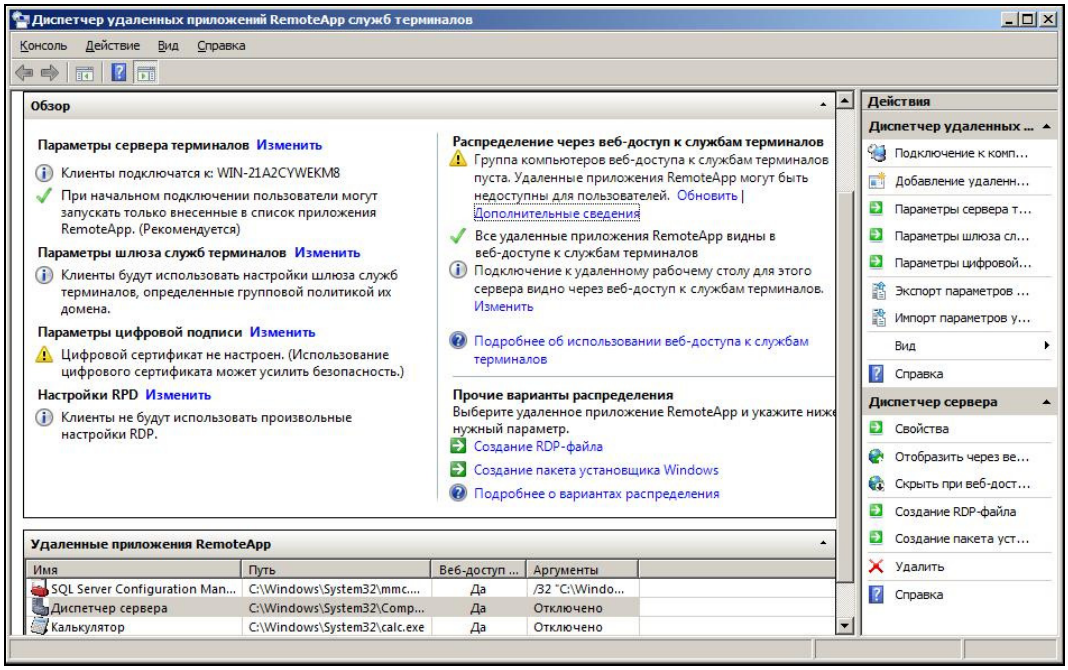


Рис. 10.4. Диспетчер удаленных подключений

Перенос настроек приложения в параметры подключения предоставил администраторам дополнительные возможности. Удаленное приложение стало возможным *публиковать* или устанавливать: достаточно любым средством (через групповые политики, с помощью специализированного ПО — System Management Server, Acronis и др., создавая msi-файл установки и т. п.) предоставить пользователю файл настроек подключения. Более подробно способы публикации удаленных приложений описаны в онлайновой справке.

Веб-доступ к терминальному серверу. Шлюз терминалов

Веб-доступ к терминальному серверу появился в тот момент, когда программное обеспечение терминальных клиентов не устанавливалось по умолчанию на рабочих станциях Windows. Фактически это решение представляет собой ActiveX-модуль, автоматически устанавливаемый на локальный компьютер при обращении из обозревателя к терминальному серверу. Соответственно, работать можно только с Internet Explorer, и требуются права и необходимые разрешающие настройки обозревателя для установки ActiveX. Реальное подключение к терминальной сессии осуществляется по протоколу RDP, что требует открытого порта 3389.

Веб-доступ в версии Windows Server 2008 несколько изменился. Теперь на исходной странице публикуются не только ссылки на доступ к терминальной сессии, но и перечень опубликованных приложений (рис. 10.5).

По умолчанию веб-интерфейс доступен по пути **http://<*имя_сервера*>/ts**.

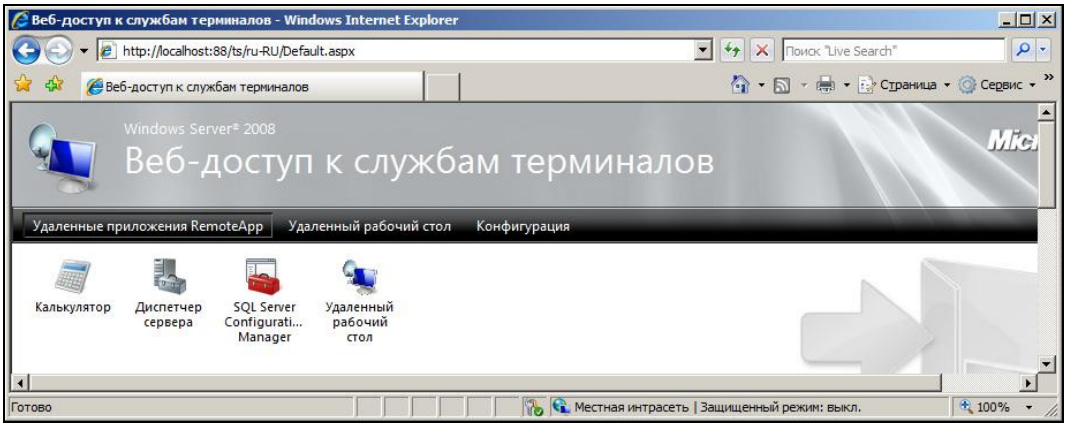


Рис. 10.5. Веб-интерфейс терминального сервера

Веб-интерфейс удобен для разового доступа к необходимому приложению не с компьютеров локальной сети. При постоянной работе рациональнее ссылку на такое приложение сохранить на локальном компьютере. Администраторы могут настроить веб-интерфейс так, что на нем будут опубликованы приложения с различных терминальных серверов внутри организации. Но это, конечно, решение уже для крупных предприятий.

Отметим интересную новую возможность Windows 2008 Server — наличие шлюза терминалов. Шлюз терминалов позволяет публиковать в Интернете несколько внутренних терминальных серверов, подключение к которым производится в зависимости от устанавливаемых политик. И главное, доступ к шлюзу, а потом к терминальному серверу осуществляется клиентом по порту 443 — это порт протокола HTTPS, который обычно открыт в межсетевых экранах. Это расширяет возможности доступа к терминальным серверам из Интернета.

Настройка шлюза терминалов не представляет особой сложности, и мы не будем специально останавливаться на ней.

Некоторые особенности работы в режиме терминального доступа

Пользователь может подключать к узлу удаленных рабочих столов свои локальные ресурсы. Это позволит сохранять результаты работы непосредственно на локальный диск. Администратор должен разрешить или запретить возможность такой операции, исходя из принятых в организации правил.

Обычно пользователям разрешают подключать локальные принтеры. Драйвер принтера будет автоматически устанавливаться только при наличии цифровой подписи. В противном случае лучший выход — предварительная установка драйвера администратором сервера.

Поскольку узел удаленных рабочих столов предоставляется в пользование многим пользователям, то администратору крайне важно сохранить его работоспособность, не давая пользователям устанавливать лишнее программное обеспечение, менять настройки и т. д. Мы не будем останавливаться на описании возможных административных настроек, отметим только, что для терминального сервера очень развиты опции тюнинга через политики безопасности. В политиках безопасности можно установить практически любые ограничения. В Windows Server 2008 удобно ввести ограничения и через настройку удаленных приложений (включая опцию разрешения запуска только RemoteApp).

Одна из наиболее часто происходящих проблем на терминальном сервере — зависания заданий печати пользователей в различных сессиях. Для того чтобы удалить их, достаточно периодически выполнять следующий сценарий:

```
net stop spooler
del %systemroot%\system32\spool\printers\*.* /q
net start spooler
```

Командная строка управления терминальными сессиями

Перечислим несколько команд, которые будут полезны администраторам для управления режимом терминальных служб. Подробности использования команд легко уточнить по справочной документации системы.

- `shadow` — позволяет наблюдать (переключиться) за другими терминальными сессиями.
- `change user` — переключает удаленный рабочий стол в режим установки программного обеспечения.
- `change logon` — разрешает или запрещает новые подключения пользователей к терминальному серверу. Программа полезна, если вы хотите временно, на период работ по настройке сервера, запретить пользователям создавать новые сессии.
- `query` — в числе прочего команда позволяет запросить список терминальных серверов организации, что вряд ли представляет особую ценность. Главное — команда показывает список текущих пользователей на сервере, идентификаторы их сессий. Эта информация полезна, если вы захотите отключить конкретного пользователя (например, в случае зависания его сессии) от терминала.

- `logoff` — завершает работу пользователя и удаляет его сессию. В параметрах команды нужно указать тот номер, который вы получили при запросе параметров пользователя командой `query`.
- `reset session` — в отличие от предыдущей команды завершает сеанс пользователя "силовыми методами". Полезно в случае зависших сеансов.
- `MSG` — позволяет послать сообщение пользователю терминальной сессии (конкретному или всем). Например, если вы выключаете сервер, то этой командой можно попросить пользователей завершить работу к заданному сроку.
- `TSPROF` — копирует профиль пользователя.
- `TSSHUTDN` — выключает (перезагружает) сервер.

Технологии доставки виртуального рабочего стола

С развитием технологий виртуализации появилась возможность создания виртуальных систем не только для серверов, но и для рабочих станций. Подобные технологии стали называть VDI (Virtual Desktop Interface).

В этом случае для каждого рабочего места создается отдельная виртуальная машина. Преимущество такого подхода по сравнению с терминальными режимами состоит в бóльших возможностях настройки параметров рабочих станций и управления их ресурсами. При этом созданы решения, позволяющие экономить ресурсы сервера, например, хранить типовые файлы различных рабочих станций (файлы операционных систем, программного обеспечения и т. д.) централизованно.

Однако на сегодня технологии доставки виртуального рабочего стола испытывают сложности, если:

- на рабочей станции требуется использовать технологии аппаратного ускорения (например, DirectX);
- необходима передача голосового трафика на рабочую станцию;
- требуется использование локально подключенного принтера;
- используются аппаратные ключи защиты ПО от копирования;
- необходимо использовать сканер, видеокамеру и другое оборудование, подключенное к рабочей станции.

Кроме того, до сих пор многие вопросы лицензирования в таких конфигурациях остаются неясными.

Для оценки эффективности внедрения данной технологии приведем параметры, на которые ориентируются западные менеджеры и результаты расчета по которым приводятся на наших семинарах (табл. 10.1).

Как видно из таблицы, экономия от внедрения решений VDI получается только за счет разницы в стоимости рабочих станций и затрат на их обслуживание (электро-

питание, стоимость ремонта и т. п.). Поэтому экономически эффективным VDI-решение будет только при существенном числе рабочих станций и учете, например, не менее 3-летнего периода эксплуатации. Так, калькулятор эффективности от Oracle — Oracle Desktop Virtualization TCO Calculator — устанавливает минимальную границу числа рабочих станций в 25 единиц (см. **http://www.oracle.com/us/media/calculator/vdi/vdi-tco-calculator-detailed-406401.html**).

Таблица 10.1. *Показатели экономической эффективности технологии VDI*

Параметр	Эффект	Примечание
Стоимость приобретаемого ПО (серверного и клиентских лицензий)	Затраты	Сумма варьируется для решений различных вендоров. Стоимость клиентских лицензий обычно составляет 100—150 долларов
Стоимость рабочей станции	Экономия, зависит от периода использования	В качестве рабочих станций можно использовать упрощенные варианты ("тонкие" клиенты и т. п.). Возможен отказ от приобретения индивидуальных источников аварийного питания. Кроме того, необходимо учесть разницу в ежегодных расходах на обслуживание (составляет примерно от 5 до 10% от стоимости станций)
Стоимость электропитания	Экономия, зависит от периода использования	Экономия на электроснабжении рабочей станции (меньшая мощность), затраты на электропитание серверов, систем хранения
Стоимость оборудования: сервера, СХД, фермы	Затраты	Минимально от одного сервера и системы хранения, оптимально — отказоустойчивые решения с выделенными серверами управления, обеспечения доступа из Интернета и т. п.

Удаленное подключение пользователей к внутренней сети предприятия

Обеспечить доступ пользователей ко всем ресурсам внутренней сети предприятия можно на основе технологии VPN. В этом случае удаленный компьютер пользователя становится членом локальной сети предприятия.

Данные между компьютером пользователя и офисом по Интернету передаются безопасным образом (с применением шифрования). Возможные проблемы вызваны тем фактом, что специалисты офиса не контролируют подключаемый компьютер. Поэтому на нем могут быть вирусы или другое опасное программное обеспечение, средства, которые можно использовать для подготовки атаки на информационную систему предприятия, и т. п. Несмотря на развитие технологий контроля доступа в сеть, обеспечить полную безопасность информационной системы со стороны пользовательского компьютера практически невозможно. Поэтому возможность подключения по VPN следует предоставить только доверенным пользователям. Тем более что к основным информационным ресурсам пользователи могут обратиться через терминальный доступ или порталы (в том числе, и к корпоративной почте).

Безопасное объединение локальных сетей офисов

Существует несколько вариантов объединения локальных сетей офисов в единую сеть. Самый надежный способ заключается в использовании маршрутизирующего оборудования путем создания защищенных соединений. Однако, учитывая стоимость маршрутизаторов, не каждая организация может их приобрести. Маршрутизаторы можно легко настроить и на основе компьютеров с Linux-системой, но надежность системного блока такого компьютера конечно ниже.

Самый дешевый способ соединения нескольких офисов — использование программных средств для создания безопасного канала и маршрутизации трафика. В случае Windows подобную функциональность реализует сервер маршрутизации и удаленного доступа. В Linux-системах никаких дополнительных компонентов не требуется, нужно только настроить безопасное подключение и отредактировать правила маршрутизации.

Для создания безопасного подключения обычно используется протокол PPTP в силу исторических причин. Подключения можно реализовать и по протоколам L2TP/IPsec. Преимущества их в том, что они исходно разрабатывались для коммутационного оборудования и могут быть реализованы специальными аппаратными модулями.

В Windows Server 2008 для создания подключения может быть использован протокол SSTP (Secure Socket Tunneling Protocol). Он предоставляет механизм инкапсуляции трафика протокола HTTPS. Использование HTTPS означает возможность подключения через межсетевые экраны, блокирующие трафик PPTP и L2TP/IPsec.

Подключение офисов через виртуальную сеть провайдера

Современные модели коммутаторов имеют возможность "пробрасывания" VLAN по Интернету. Это самый простой способ объединения офисов. Провайдер просто предоставляет вам параметры IP-адреса, а вы настраиваете необходимую маршрутизацию.

Технология (MPLS) позволяет назначать пакетам конечные точки маршрута, что обеспечивает доставку данных, например, из одного диапазона локальных адресов в другой. Функционал обеспечивается исключительно средствами оборудования сети передачи данных, поэтому он доступен только для тех офисов, которые подключены к совместимому оборудованию. К сожалению, это выполняется лишь в крупных городах и далеко не у всех провайдеров.

Преимущества данной технологии, кроме простоты создания соединения двух частных сетей, состоит в обеспечении заданного качества обслуживания: прежде всего, такой канал может обеспечить гарантированную полосу пропускания от точки входа до точки выхода.

Недостатки технологии, кроме упомянутой малодоступности на сегодняшний день, в том, что пакеты данных передаются через глобальные сети в незашифрованном виде. Это потенциально позволяет легко прослушивать такой трафик. Кроме того,

провайдеры обычно берут за данную услугу арендную плату, что ограничивает ее доступность для некрупных организаций.

Подключение с использованием VPN-серверов Windows

VPN-доступ в серверных операционных системах реализуется **Службой маршрутизации и удаленного доступа** (RRAS).

Служба маршрутизации и удаленного доступа установлена в серверах Windows Server 2000/2003. В Windows Server 2008 эту службу необходимо установить путем добавления роли **Службы политики сети и доступа**. При добавлении роли следует выбрать ее в списке **Службы маршрутизации и удаленного доступа**.

VPN-подключение может быть создано для индивидуального пользователя или для всего офиса. Отличие между этими вариантами, что в случае подключения офиса наряду с созданием канала настраивается и маршрутизация между двумя площадками. Поэтому вариант подключения удаленного офиса в Windows-сервере имеет специальное название — создание *интерфейса по требованию* (dial-in-интерфейса).

Создание интерфейса по требованию осуществляет мастер. Для этого достаточно выбрать в меню **Службы маршрутизации и удаленного доступа** опцию создания безопасного соединения между двумя частными сетями и завершить операции. Для успешного завершения операций необходимо знать адрес удаленного сервера, параметры учетной записи, которой разрешено создавать подключение, диапазоны IP-адресов, маршрутизация которых будет осуществляться через создаваемый интерфейс.

Система отличает подключение удаленного пользователя от подключения интерфейса по требованию *только по имени пользователя*, выполняющего эту попытку. Поэтому при настройке подключений двух сетей имя подключающегося *пользователя должно совпадать с названием интерфейса*. Иными словами, на сервере с интерфейсом по требованию с именем `Int1` должен быть указан пользователь `Int2` для подключения к удаленному интерфейсу по требованию с именем `Int2`, а на другом сервере — `Int1`.

В качестве учетных записей, используемых в интерфейсах по требованию, целесообразно применять только локальных пользователей, чтобы не зависеть от доступности контроллера домена (если сеть построена по доменному варианту).

Другие настройки подключений интерфейсов по требованию (должно ли соединение инициироваться сервером или ему следует только ожидать попытки подключения, время "простоя", после которого можно разъединять связь, или необходимость постоянного соединения и т. п.) достаточно очевидны и легко настраиваются через консоль управления службой маршрутизации и удаленного доступа. Состояние соединений контролируется оснасткой службы (рис. 10.6).

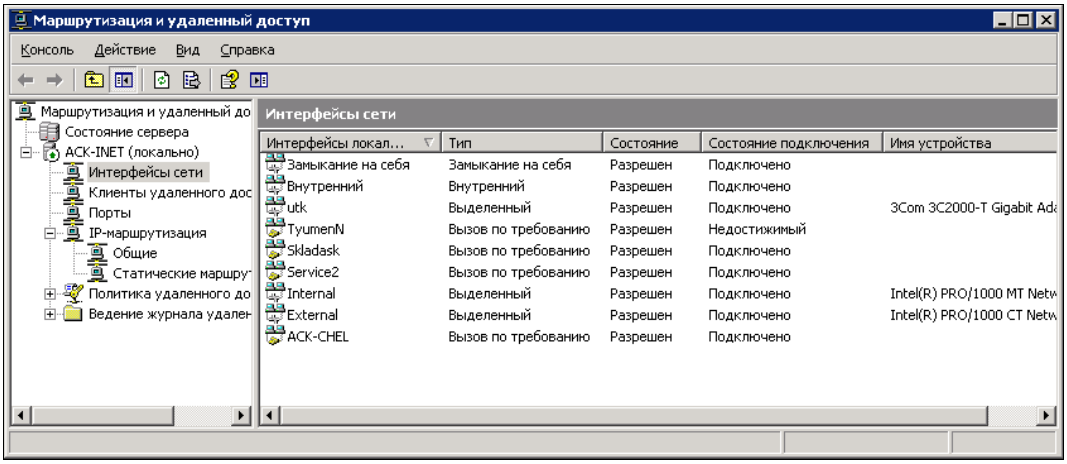


Рис. 10.6. Окно программы маршрутизации и удаленного доступа

Фильтрация VPN-трафика

Для создания связи между офисами необходимо с обеих сторон установить VPN-серверы. Часто VPN-серверы объединяют с серверами межсетевого экрана (Microsoft Forefront TMG), но можно и разместить их внутри периметра сети. В этом случае на межсетевых экранах нужно настроить пропуск на эти серверы соответствующих протоколов.

Опишем параметры протоколов, которые необходимо пропустить внутрь периметра для работы VPN-сервера.

- Для подключения к VPN-серверу по протоколу PPTP следует разрешить:
  - IP-протокол на порт 1723 (это разрешает передачу управляющего трафика PPTP);
  - IP-протокол с идентификатором 47 (разрешение передачи данных по PPTP);
  - IP-протокол на порт 1723 в варианте **TCP [established]** (настройка нужна в случае, если инициатором соединения выступает сам VPN-сервер).

  Не забывайте, что необходимо разрешить прохождение как *входных* пакетов, так и соответствующих симметричных *выходных*.
- При подключении к VPN-серверу по протоколу L2TP необходимо разрешить:
  - пакеты на UDP-порт номер 500;
  - прохождение протокола с идентификатором 50;
  - пакеты на UDP-порт номер 1701.

  Как и в предыдущем примере, фильтры должны быть настроены симметрично для входных и выходных пакетов.

В случае разрыва канала при доменной организации офиса...

Удаленные офисы небольших предприятий обычно укомплектованы всего лишь несколькими компьютерами. Достаточно часто качество канала связи с центральным офисом (Интернетом) оставляет желать лучшего. В результате при обрыве связи удаленные пользователи теряют возможность доступа не только к ресурсам головного офиса, но и к локальным (документы, хранимые в папках совместного доступа на компьютерах других сотрудников филиала, локальный принтер и т. п.), если для доступа к ресурсам применяются *доменные учетные записи*.

Существует несколько возможных путей решения данной проблемы. Первый — это создание на удаленных компьютерах локальных учетных записей, совпадающих по имени с доменными и имеющими тот же пароль, что в домене. Тогда при обрыве связи и недоступности контроллера домена доступ к ресурсам на других компьютерах будет осуществляться по *локальным учетным записям*. Недостаток этого варианта состоит в том, что необходимо постоянно синхронизовать учетные записи домена и локальных компьютеров в случае смены паролей пользователей.

Второй путь — размещение таких ресурсов филиала (общие папки, принтер) на терминальном *сервере*. Поскольку в новых версиях Windows существует кэширование параметров последних входов пользователя, то при обрыве связи пользователь сможет войти на терминальный сервер *без наличия подключения к контроллеру домена*, используя параметры последнего входа, хранимые в кэше. Однако подключиться к совместным папкам на других компьютерах будет невозможно.

Третий путь заключается в установке в филиале контроллера домена. В филиале предпочтительнее устанавливать контроллер домена "только для чтения", особенности которого были рассмотрены ранее *(см. разд. "Контроллер домена только для чтения" в главе 6)*.

Подключение удаленных клиентов с помощью VPN-серверов Linux

VPN-сервер имеет смысл настраивать только для обеспечения к филиалу подключения Windows-клиентов. Собственно VPN-сервер очень легко настраивается. В Ubuntu VPN устанавливается командой

```
sudo apt-get install pptpd
```

Параметры настройки сервера по умолчанию обеспечивают подключение клиентов VPN, в том числе и с компьютеров под управлением операционных систем Microsoft Windows. Единственное, что нужно указать, — это описать IP-адреса сервера (его самого и диапазон адресов, предоставляемых клиентам) и добавить параметры учетных записей, которым разрешено подключение. Для настройки VPN-сервера откройте файл /etc/pptpd.conf. Укажите адрес сервера и диапазон адресов для клиентов:

```
localip 192.168.0.1
remoteip 192.168.0.200-250,192.168.0.252
```

Примечание

Настройки по умолчанию предполагают возможность одновременного подключения до 100 клиентов. Если диапазон выделенных IP-адресов меньше, то число клиентов будет ограничено этим значением. При необходимости подключения более 100 клиентов, эту настройку необходимо осуществить для VPN-сервера.

Для VPN-клиентов с операционных систем MS Windows желательно также указать получаемые ими параметры DNS-сервера и WINS-сервера (при наличии). Эта настройка осуществляется в файле /etc/ppp/pptpd-options в строках

```
ms-dns 10.0.0.1
ms-wins 10.0.0.2
```

Учетные записи, которые должны быть использованы для подключения, нужно указать в файле /etc/ppp/chap-secrets по следующему образцу:

```
user pptpd password *
```

В этом примере `*` означает, что клиент при подключении получит адрес из указанного в настройках сервера диапазона. Если клиенту нужно предоставить определенный адрес, то вместо `*` укажите его значение (или диапазон адресов, например, 192.168.0.0/24).

После выполнения этих настроек перестартуйте сервер:

```
/etc/init.d/pptpd restart
```

Для того чтобы клиенты могли подключаться к вашему серверу, необходимо также создать разрешающие правила для межсетевого экрана (открыть порт 1723 и разрешить протокол GRE):

```
iptables -A INPUT -p gre -j ACCEPT
iptables -A INPUT -m tcp -p tcp --dport 1723 -j ACCEPT
```

В рабочей среде следует разрешать подключения *только* с определенных адресов, поэтому приведенные примеры правил `iptables` нужно конкретизировать.

Если планируется создать через VPN-подключение связь двух офисов, то необходимо настроить маршрутизацию (или NAT с помощью `iptables`). Для этого вы должны знать, какие диапазоны IP-адресов задействованы в подключаемой сети. Кроме того, после подключения вам необходимо настроить правила фильтрации трафика (`iptables`).

В реальных условиях могут требоваться несколько VPN-подключений, осуществляемых независимо и в произвольное время. В этой ситуации для создания правил маршрутизации необходимо знать, какое подключение выполняется. В табл. 10.2 приведен перечень переменных при выполнении сценариев PPP-подключения, позволяющих получить информацию о том подключении, которое выполнено в текущий момент (полный список переменных см. в файле /etc/ppp/ip-up).

В листинге 10.1 приведен пример сценария подключения.

Таблица 10.2. *Список переменных для PPP-подключения*

Переменная	Описание
PPP_LOCAL	IP-адрес, получаемый от VPN-сервера, к которому осуществляется подключение, либо IP-адрес локального VPN-сервера (если регистрируется входящее подключение)
PPP_IPPARAM	Название туннеля при исходящем подключении либо IP-адрес клиента, который подключается к локальному VPN-серверу
PPP_REMOTE	Адрес удаленного VPN-сервера (при исходящем подключении) или адрес, который получил удаленный клиент при входящем VPN-подключении
PPP_IFACE	Имя интерфейса (подключаемого или отключаемого)

Листинг 10.1

```
#!/bin/sh
case "$PPP_IPPARAM" in
my_provider)
route add default dev $PPP_IFACE
;;
1.2.3.4)
route add -net 192.168.10.0 netmask 255.255.255.0 dev $PPP_IFACE
iptables --insert INPUT 1 \
--source 192.168.10.0/24 \
--destination 0.0.0.0/0.0.0.0 \
--jump ACCEPT --in-interface ${IFNAME}
;;
*)
echo "No PPP_IPPARAM defined"
;;
esac
```

При подключении `my_provider` мы добавляем маршрут по умолчанию через установленное соединение, при подключении с внешнего адреса 1.2.3.4 добавляем в таблицу маршрутизации маршрут на подключаемую сеть и разрешаем с нее получение пакетов. Понятно, что набор этих команд вы должны определить на основе своих потребностей.

Сценарии, которые выполняются при установлении соединения, нужно сохранить в папке /etc/ppp/ip-up.d/. Соответственно, сценарий удаления маршрутов следует сохранить в папке /etc/ppp/if-down.d/. Не забудьте после сохранения сценариев предоставить на созданные файлы права выполнения:

```
chmod +x /etc/ppp/ip-up.d/имя_файла
```

Подключение "офис — офис" на основе технологии SSH

Для UNIX-систем более удобно настроить подключение к сети офиса (или соединить сети двух офисов) на основе технологии SSH. Описываемый далее вариант подключения легко настроить с одного рабочего места, имея только возможность удаленного подключения к другому офису для своей учетной записи.

По опыту работы SSH-подключение обеспечивает большую надежность связи, поэтому именно этот вариант следует выбирать при использовании в качестве шлюзов Linux-систем.

Опишем, как настроить связь по зашифрованному каналу с применением технологии SSH между двумя офисами.

> ***Примечание***
>
> Мы приводим описание настройки подключения с помощью пакета OpenSSH, который устанавливается в Ubuntu (версию можно уточнить командой `ssh-V`). При подключении к системам с SSH2 необходимо конвертировать ключи ssh2 в формат OpenSSH. Соответствующие рекомендации легко найти в Интернете.

Для этого нужно:

- настроить SSH для использования ключей, чтобы при подключении не возникала необходимость ручного ввода пароля;
- настроить туннель между офисами.

Рассмотрим последовательно эти операции.

Для использования ключей вместо паролей предварительно нужно их сгенерировать. Для этого служит утилита `ssh-keygen`. Согласитесь на все запросы команды с параметрами по умолчанию, в том числе не указывайте пароль доступа к ключу. Это позволит впоследствии осуществить аутентификацию по ключу в автоматическом режиме (без необходимости ввода вручную пароля).

> ***Примечание***
>
> Ключи доступа часто применяют для аутентификации на удаленных компьютерах. Обычно один и тот же ключ служит для входа на многие системы. Необходимо предотвратить возможность его появления в чужих руках. Безопаснее создавать отдельные ключи для различных подключений к удаленным серверам, если предполагается наличие нескольких туннелей.

При выполнении команды вы увидите текст листинга 10.2 (в этом примере имя условно обозначает название учетной записи пользователя).

Листинг 10.2

```
ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/имя/.ssh/id_rsa):
Created directory '/home/имя/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

```
Your identification has been saved in /home/имя/.ssh/id_rsa.
Your public key has been saved in /home/имя/.ssh/id_rsa.pub.
The key fingerprint is:
97:e0:13:c3:ea:00:c8:5b:15:c0:33:70:c3:24:71:32 имя@сервер
```

В результате выполнения этой команды будет создана пара файлов: публичный ключ (если вы не указывали свое имя) — /home/*имя*/.ssh/id_rsa.pub и персональный ключ — /home/*имя*/.ssh/id_rsa. Далее в примерах мы будем предполагать, что вы создали ключи с именем my_tunnel.

На созданные файлы (точнее, на открытый ключ) необходимо назначить права, предотвращающие их использование другими учетными записями. В противном случае при попытке выполнения команды с указанием ключа вы получите предупреждение и отказ в выполнении команды:

```
chmod 600 /root/.ssh/my_tunnel.pub
```

Для того чтобы на удаленный компьютер можно было зайти по протоколу SSH без ввода пароля, публичный ключ необходимо скопировать на этот компьютер и добавить содержимое файла ключа в файл /home/*имя*/.ssh/authorized_keys. Проще всего это сделать с помощью имеющегося сценария `ssh-copy-id`:

```
ssh-copy-id-i ~/.ssh/my_tunnel.pub удаленный_сервер
```

В этом варианте ключ будет установлен в папку суперпользователя. Если вы хотите получить подключение с правами иной учетной записи, то укажите название сервера как *имя_пользователя@имя_сервера*. Программа запросит пароль доступа к удаленному серверу и выполнит операцию по добавлению данных ключа в файл authorized_keys профиля суперпользователя.

> ***Примечание***
>
> Первый вход на удаленную систему происходит достаточно долго. Целесообразно вначале просто подключиться к серверу по протоколу SSH и подтвердить доверие к установленному ключу.

Теперь настройки для подключения без паролей выполнены. Чтобы подключиться к удаленному серверу, достаточно предоставить ему созданный таким образом ключ. Сделать это можно двумя способами.

Если вы подключаетесь вручную, то следует загрузить специального агента, который будет предоставлять идентификационные данные. В пакетном режиме достаточно явно указать в параметрах команды `ssh` путь к идентификационному файлу.

Для загрузки агента выполните следующие две команды:

```
ssh-agent $SHELL
ssh-add
```

Вторая команда, запущенная без параметров, добавляет ключи, расположенные в папке по умолчанию. При ее выполнении необходимо указать введенный при соз-

дании ключа пароль (если таковой был назначен). Проверить загрузку ключей можно командой `ssh-add-L`.

В пакетных режимах допустим синтаксис с явным указанием пути к публичному ключу учетной записи, что предотвратит просьбы ввода пароля:

```
ssh -i /root/.ssh/my_tunnel имя_сервера
```

> ***ВНИМАНИЕ!***
>
> Обратите внимание, что в этой команде указывается только имя ключа, без ввода расширения.

Для успешной аутентификации по ключам на удаленном сервере должна быть разрешена эта опция. По умолчанию в Ubuntu она отключена. Для ее включения необходимо на сервере раскомментировать строку `AuthorizedKeysFile` в файле /etc/ssh/sshd_config. Кроме того, в конфигурации SSH необходимо включить опцию, разрешающую создавать каналы. Для этого добавьте в файл /etc/ssh/sshd_config строку

```
PermitTunnel yes
```

и перестартуйте SSH (/etc/init.d/ssh restart).

> ***ПРИМЕЧАНИЕ***
>
> Можно более безопасно настроить конфигурацию SSH, разрешив вход учетной записи суперпользователя только для создания туннелей и явно настроив разрешенные к выполнению операции. Это потребует некоторых ручных операций редактирования конфигурации, которые описаны, например, в **http://www.debian-administration.org/articles/539**.

Канал между двумя системами создается следующей командой:

```
ssh -f -w 0:0 -i /root/.ssh/my_tunnel имя_сервера true
```

Здесь параметр `-f` определяет запуск команды в фоновом режиме, параметр `-w` указывает номера создаваемых туннелей. Номера выдаются, начиная с нуля, так что в примере показано создание первого туннеля; если туннель уже существует на одной из систем, то номер нужно увеличить (например, `-w 0:1`).

После образования туннеля нужно создать его сетевые интерфейсы как на клиенте, так и на сервере и настроить маршрутизацию. Интерфейсы туннеля должны иметь свои IP-адреса из отдельной подсети. Выберите любую подсеть, которая не задействована в вашей структуре, и присвойте ее адреса интерфейсу туннеля с одной стороны и с другой.

Например, на клиенте:

```
ifconfig tun0 10.0.0.1 10.0.0.2 netmask 255.255.255.252
```

И на сервере:

```
ifconfig tun0 10.0.0.2 10.0.0.1 netmask 255.255.255.252
```

Обратите внимание, что адреса на клиенте и на сервере указаны в разном порядке (сначала "свой", потом адрес интерфейса с другой стороны).

Чтобы через созданный туннель осуществлялась связь между сетями, необходимо добавить маршруты в сеть удаленного офиса через созданные интерфейсы и разрешить прием пакетов на него в межсетевом экране, например, так:

- на клиенте:

```
route add -net 192.168.10.0 netmask 255.255.255.0 gw 10.0.0.2
iptables -A INPUT -i tun0 -j ACCEPT
```

- на сервере:

```
route add -net 192.168.20.0 netmask 255.255.255.0 gw 10.0.0.1
iptables -A INPUT -i tun0 -j ACCEPT
```

На этом настройка туннелей завершена. Проверьте достижимость сетей удаленного офиса, например, командой `ping`.

Для автоматического создания туннелей при запуске системы соответствующие команды можно добавить в /etc/network/interfaces. При этом лучше добавить в команду установки туннеля опции поддержания его в активном состоянии и включение так называемого мастер-режима, позволяющего совместно использовать данное подключение. Поскольку соединение инициируется только с одной стороны и протокол SSH позволяет выполнить на удаленном сервере необходимые команды, то конфигурацию интерфейса можно осуществить лишь на клиенте так, как показано в листинге 10.3.

Листинг 10.3

```
auto tun0
iface tun0 inet static
pre-up ssh-i /root/.ssh/my_tunnel -S /var/run/my_tunnel.pid-M -f -w 0:0 -o
'TCPKeepAlive yes' имя_сервера true
pre-up sleep 5
address 10.10.10.1
pointopoint 10.10.10.2
netmask 255.255.255.252
up route add -net 192.168.10.0/24 gw 10.10.10.2 tun0
up ssh-i /root/.ssh/my_tunnel имя_сервера ifconfig tun0 10.10.10.1 10.10.10.2
netmask 255.255.255.252
up ssh-i /root/.ssh/my_tunnel route add -net 192.168.10.0/24 gw 10.10.10.1 tun0
post-down ssh -S /var/run/my_tunnel.pid -O exit имя_сервера
post-down ssh-i /root/.ssh/my_tunnel имя_сервера ifconfig tun0 down
post-down ssh-i /root/.ssh/my_tunnel имя_сервера route del -net 192.168.10.0/24
```

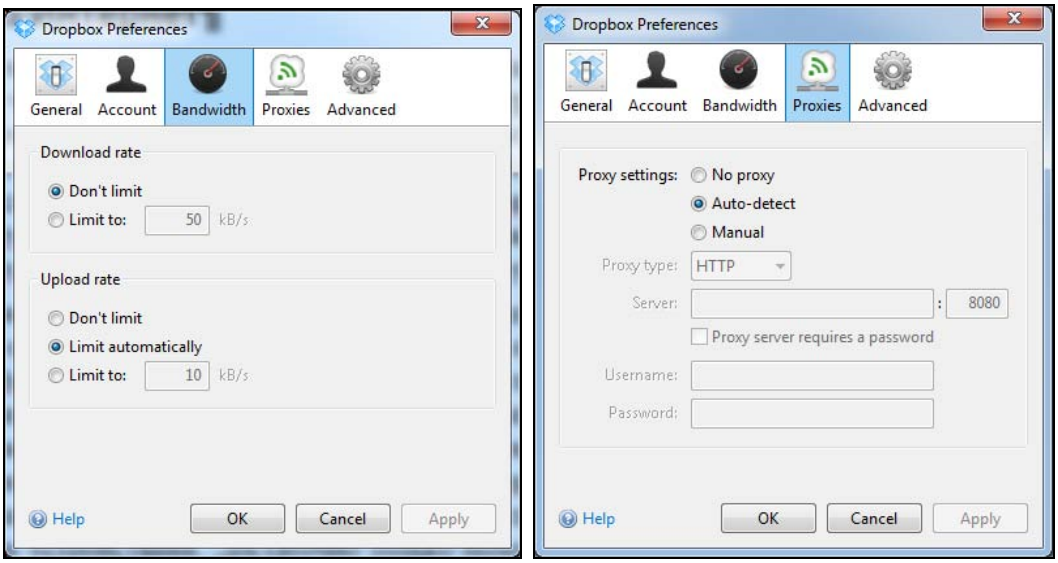
Примечание

В примере опущены команды создания и удаления правил межсетевого экрана. При наличии запрещающей политики по умолчанию вам необходимо добавить разрешающие правила для туннелей.

Облачные ресурсы

Пользователи и организации сегодня имеют возможность размещать на серверах Интернета свои ресурсы, причем для большинства потребностей такое решение будет абсолютно бесплатным. Так, пользователям SkyDrive (**https://skydrive.live.com/**) бесплатно предоставляется 7 Гбайт для хранения своих данных, пользователи GdoscDrive (**http://www.gdocsdrive.com/**, бывшее Google Docs) могут рассчитывать на 5 Гбайт, V-Drive (**https://vdrive.maxthon.com/**) — на 6 Гбайт, DropBox (**https://www.dropbox.com/**) — на 2 Гбайт с возможностью расширения за счет привлечения друзей и т. д.

Работать с такими ресурсами можно как при помощи соответствующих приложений, запускаемых (устанавливаемых на устройствах), так и через обозреватель Интернета в любой точке Сети. Настройки агентов позволяют выполнить подключение через прокси-сервер, лимитировать использование полосы пропускания канала Интернета и т. п. (рис. 10.7).



а *б*

Рис. 10.7. Интерфейсы настройки синхронизации с сервером Dropbox

Каждая служба имеет свои особенности реализации. Например, на взгляд автора, сервис Dropbox наиболее удобен для синхронизации данных между разнородными устройствами: вы можете загрузить приложения для Windows, Linux, для мобильных устройств (Android, Windows Phone) и т. д. и поддерживать на всех них идентичность информации.

Помимо собственно возможностей хранения информации, данные сервисы предлагают удобные функции совместного использования: вы можете предоставить данные в общее пользование некоторой группе лиц, разослав им, например, уникальные ссылки на соответствующие файлы. В результате администратор организации

освобождается от необходимости хранения таких файлов и обеспечения к ним безопасного доступа.

В случае необходимости можно заключить договор с соответствующей службой, который будет гарантировать юридически качество обслуживания (процент времени доступности, увеличение объемов хранения и т. д.).

Некоторые организации уже начинают переводить свою инфраструктуру в облако. В этом случае можно, например:

- настроить почтовый сервер облака на использование доменного имени организации;
- создать единые адресные книги, календари занятости и т. п.;
- реализовать общие файловые ресурсы требуемого объема;
- подключить дополнительные модули (например, систем взаимодействия с пользователями — CRM, работы с проектами и т. п.).

С описанием одной из наиболее известных облачных служб — Google Apps — можно ознакомиться на сайте **http://www.google.com/apps/intl/ru/business/**.

Управление оборудованием по Интернету

Администратор должен иметь возможность выполнить в удаленном офисе любые операции, в том числе и восстановить работоспособность "зависшей" системы, иметь возможность установить операционную систему "с нуля", используя локальный дистрибутив и т. п. Подобные ситуации, хотя и встречаются не столь часто в обыденной работе, могут принести существенные убытки компании из-за остановки в обслуживании.

Существует несколько вариантов решения таких проблем.

Intelligent Platform Management Interface

Современные серверы поддерживают внешнее управление по спецификации IPMI (Intelligent Platform Management Interface). Обычно серверные платформы имеют специально выделенный порт для такого управления, но некоторые модели могут использовать одно сетевое подключение как для нормальной работы, так и для управления.

Если сервер не имеет такого порта, то в некоторых случаях в него можно добавить специальный модуль, который будет реализовывать эту функциональность (возможность следует уточнить по документации).

Мониторинг и управление через порт IPMI может осуществляться даже при зависании операционной системы. Главное, чтобы сохранялась доступность порта по сети передачи данных. Именно поэтому в серьезных проектах для подсистемы управления и мониторинга создают выделенную сеть, а такой вариант контроля называют *out-of-band management*.

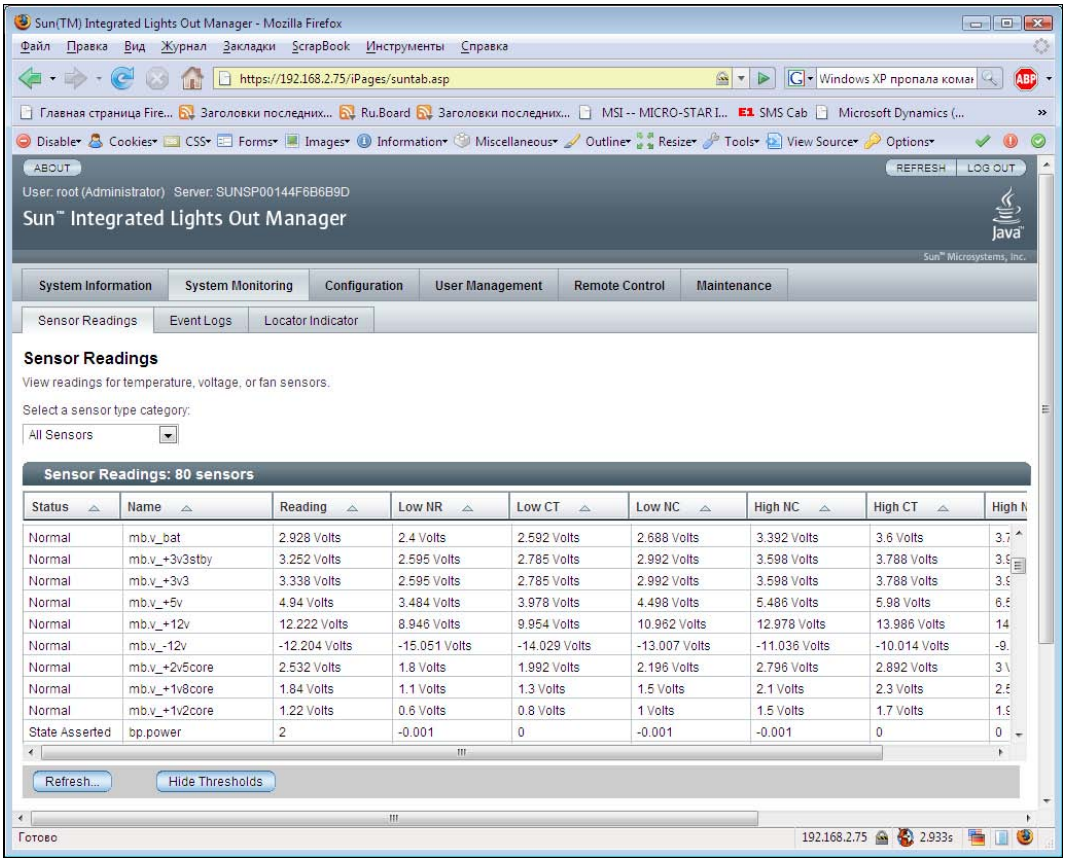
Подключение к серверу для удаленного администрирования можно осуществить и через последовательный порт (обычно через модем). Это вариант для самого критического случая, когда все другие возможности связи с сервером потеряны.

> ***Примечание***
>
> Модем позволяет подключиться к серверу даже при полном отказе инфраструктуры. Стоимость же данного решения (модем плюс один внутренний номер на АТС предприятия) весьма невысока.

Для управления через порт IPMI предусмотрены специальные программы. Обычно консоли управления реализуются в виде веб-интерфейсов с подключением по безопасному каналу (HTTPS). Кроме того, через этот порт можно обычно управлять и в режиме командной строки, и по SNMP-протоколу.

Данный вариант управления дает возможность администратору:

- удаленно включать, выключать и перезагружать сервер независимо от состояния операционной системы;
- обновлять BIOS;



Status	Name	Reading	Low NR	Low CT	Low NC	High NC	High CT
Normal	mb.v_bat	2.928 Volts	2.4 Volts	2.592 Volts	2.688 Volts	3.392 Volts	3.6 Volts
Normal	mb.v_+3v3stby	3.252 Volts	2.595 Volts	2.785 Volts	2.992 Volts	3.598 Volts	3.788 Volts
Normal	mb.v_+3v3	3.338 Volts	2.595 Volts	2.785 Volts	2.992 Volts	3.598 Volts	3.788 Volts
Normal	mb.v_+5v	4.94 Volts	3.484 Volts	3.978 Volts	4.498 Volts	5.486 Volts	5.98 Volts
Normal	mb.v_+12v	12.222 Volts	8.946 Volts	9.954 Volts	10.962 Volts	12.978 Volts	13.986 Volts
Normal	mb.v_-12v	-12.204 Volts	-15.051 Volts	-14.029 Volts	-13.007 Volts	-11.036 Volts	-10.014 Volts
Normal	mb.v_+2v5core	2.532 Volts	1.8 Volts	1.992 Volts	2.196 Volts	2.796 Volts	2.892 Volts
Normal	mb.v_+1v8core	1.84 Volts	1.1 Volts	1.3 Volts	1.5 Volts	2.1 Volts	2.3 Volts
Normal	mb.v_+1v2core	1.22 Volts	0.6 Volts	0.8 Volts	1 Volts	1.5 Volts	1.7 Volts
State Asserted	bp.power	2	-0.001	0	-0.001	-0.001	0

Рис. 10.8. Удаленное управление серверной платформой

- ❒ просматривать состояние сервера (температуру, уровни напряжения, состояние датчиков, установленных на сервере), в том числе автоматически получать по сети оповещения о событиях в работе системы;
- ❒ подключать к серверу локальные CD/DVD или их образы.

В качестве примера на рис. 10.8 представлен интерфейс удаленного управления сервером Sun.

На рис. 10.8 показано одно из окон программы удаленного управления серверной платформой — Integrated Lights Out Manager. Программа представляет собой Java-приложение и позволяет удаленно по безопасному каналу (HTTPS) контролировать работу сервера. В число возможностей программы входят мониторинг сенсоров платформы (на рисунке), управление электропитанием (в том числе присутствует функция как корректного выключения с сохранением данных средствами операционной системы, так и простое отключение питания), удаленный контроль системы. Вы имеете также возможность подключить к серверу удаленный CD-ROM, гибкий диск или их образы.

Управление оборудованием по сети IP

Устройства, которые не снабжены возможностью независимого управления (подобно описанной технологии IMPI), также могут стать причиной отказа информационной системы. Для их удаленного обслуживания можно использовать KVM-переключатели с управлением по сети IP, а также удаленно управляемые распределители питания.

KVM с управлением по сети IP представляют собой переключатели клавиатуры, мыши и монитора, которые обеспечивают передачу по IP-сети нажатий клавиш и движений мышью и отображение монитора удаленного компьютера на локальной системе. Иными словами, вы можете сидеть за своим компьютером, подключиться к удаленной системе через Интернет, выполнять любые действия клавиатурой и мышью и видеть, что происходит на экране чужой системы (в том числе и в моменты ее перезагрузки).

Существуют различные модели, рассчитанные как на одно устройство (для управления несколькими системами нужно подключить KVM-переключатель), так и сразу на несколько. Современные модели могут подключать к удаленной системе не только клавиатуру и мышь, но и устройства USB. В этом случае к удаленному компьютеру можно подключить и флеш-память, и DVD-ROM и обеспечить с него загрузку компьютера.

Управление такими коммутаторами производится либо через обозреватель, либо при помощи специальной программы по защищенному каналу.

Понятно, что таким способом не всегда можно перезагрузить удаленный компьютер — кнопка "Reset" такими устройствами не поддерживается. В некоторых системах можно настроить в BIOS сочетания клавиш, которые позволяют включить питание компьютера. Это может помочь в отдельных ситуациях. Но для особо важных случаев можно применить распределители питания с управлением по сети.

При этом можно отключить питание от конкретной розетки и потом снова включить его, решив таким образом проблему холодной перезагрузки системы.

Мы не приводим описания конкретных моделей. Выпускаются они несколькими вендорами, и необходимую информацию легко найти в Интернете.

Синхронизация данных в офисах

Если организация распределена по нескольким офисам, то на плечи администратора ложится задача обеспечения каждого офиса актуальной копией документов. Проблема возникает из-за того, что связь между офисами обычно существенно медленнее локального подключения, возможны отказы канала связи, а работа компании не должна прерываться.

Кэширование информации на компьютерах филиала

Доступ к документу будет существенно ускорен, если в филиале будет храниться его копия, иными словами, документ будет *кэширован*. Для реализации такой задачи используется механизм BranchCache. Технология BranchCache появилась только в Windows 7/Windows Server 2008 R2, соответственно и доступна она только пользователям домена, работающим в этих операционных системах. Точнее, клиентами технологии могут быть компьютеры с ОС Windows 7 только выпусков Профессиональный и Максимальный.

Технология BranchCache позволяет кэшировать в филиале информацию из основного офиса, предоставляемого с Windows Server 2008 R2, как по протоколу SMB (Server Message Block, блок сообщений сервера) (обычные сетевые папки общего доступа), так и по протоколу HTTP/HTTPS (с веб-сервера IIS).

Существуют два варианта настройки технологии. Вариант *выделенного кэша* предполагает наличие в филиале сервера Windows 2008 R2, на котором хранится и обновляется кэш. В варианте *распределенного кэша* данные хранятся на пользовательских системах (Windows 7). Выбор варианта осуществляется при настройке технологии (определяется в групповой политике), каждый имеет сильные и слабые стороны и должен быть выбран в зависимости от конфигурации филиала.

Если достаточно грубо описать технологию BranchCache, то процесс происходит следующим образом. При запросе данных клиент сначала обращается на сервер основного офиса (поэтому, если этот сервер недоступен, например, в случае отказа канала, то и воспользоваться кэшированными данными, хранящимися в офисе, не удастся). Сервер предоставляет метаданные файла (строго говоря, файл разбивается на блоки и контролируется именно хэш-функция блока). В силу особенностей работы IIS хэш-функция клиентом будет сформирована только при втором обращении к файлу по протоколу HTTP, соответственно, данные из кэша можно будет получить только при *третьем* обращении к этому файлу. При работе по протоколу SMB данные в кэше будут доступны при втором обращении к файлу. Клиент, по-

лучив хэш-функцию, проверяет наличие файла в филиале (широковещательным[1] запросом в случае распределенного кэша и уникастовым — при хранении кэша на сервере). Если файл есть в кэше, он получается с компьютеров филиала, если нет (или, например, обновлен на сервере и хэш-функции не совпадают), то копируется по каналу связи центральный офис — филиал. Естественно, что на каждом этапе проверяются права доступа к файлу.

В результате того, что хэш-функция примерно в две тысячи раз меньше размера файла, операции с ней по каналу связи между офисами выполняются существенно быстрее, чем копирование собственно данных. Но эффект от включения функции BranchCache будет в том случае, если сами данные меняются редко, а обращения к ним с компьютеров филиала достаточно часты.

Для того чтобы включить BranchCache, следует добавить компонент BranchCache (BranchCache для удаленных файлов в случае файлового сервера) в настройках сервера и настроить групповую политику как для сервера, так и для клиентов. Для этого в политике конфигурации компьютера (раздел **Административные шаблоны | Сеть | BranCache**) нужно включить BranchCache, выбрать тот тип кэширования, который лучше подходит вам в конкретной ситуации. Если в организации настроен межсетевой экран, то надо не забыть и разрешить входящие подключения по протоколу HTTP (TCP-порт 80) и по протоколу UDP на порт 3702. Настройки параметров автоматического определения медленных соединений и процента используемого дискового пространства можно оставить по умолчанию.

Дополнительно желательно — для повышения уровня защищенности данных — настроить для серверов использование сертификатов (описание доступно в документации по технологии).

> ***Примечание***
>
> На клиентских компьютерах можно включить кэширование командой `nesth`:
>
> `netsh branchcache set service mode=distributed` (для распределенного кэша)
>
> или
>
> `netsh branchcache set service mode=hostedclient location=<сервер>` (для кэша, сохраняемого на сервере).

Проверить, работает ли кэширование, лучше всего по значениям счетчиков BranchCache, которые отображают объем переданных из кэша данных.

Синхронизация папок DFS

Информация между филиалами может быть синхронизирована с помощью функций распределенной файловой системы *(см. разд. "Репликация DFS в домене Windows" в главе 9)*.

---

[1] Поэтому компьютеры в случае не использования сервера Windows 2008 R2 должны находиться в пределах локального сегмента сети, без маршрутизатора.

Синхронизация может выполняться как в реальном режиме времени (при наличии каналов связи достаточной пропускной способности), так и по графику (например, синхронизация объемных файлов только в ночное время, когда трафик канала связи между офисами минимален). При этом технологии Windows Server 2008 R2 позволяют пересылать по каналу связи не весь файл, а только измененный его блок, что еще более снижает нагрузку на канал.

Среди минусов данного решения можно отметить тот факт, что оно может быть использовано только при наличии структуры домена Windows.

Синхронизация с помощью утилит

Существует много бесплатных утилит, которые позволяют синхронизировать данные между несколькими системами. При этом для работы таких средств достаточно только наличия канала связи: для каждого назначения в утилите может быть настроен вариант доступа (например, по FTP- или SMB-протоколу) и сохранены параметры подключения.

Синхронизация обычно производится по заданному графику (например, раз в час в течение рабочего дня), параметры разрешения конфликтов настраиваются администратором (поведение в случае одновременного изменения документа на обоих ресурсах).

Утилиты синхронизации файлов и папок

Лично автор имеет многолетний опыт эксплуатации одной из таких программ — SyncBack (**http://www.2brightsparks.com/syncback/index.html**). Аналогичные программы легко найти простым поиском в Сети.

Для синхронизации данных Linux-систем активно применяется команда `rsync`. Она позволяет выполнить защищенную синхронизацию данных (файлов и папок), причем по умолчанию команда пересылает только измененные блоки. Утилита поддерживает копирование ссылок, файлов устройств, атрибутов владельца, группы и прав. Можно настроить различные опции: определить маски для копирования файлов, сохранить параметры файла (права доступа, временные метки и т. п.), настроить варианты репликации (например, не переписывать измененные файлы по пути назначения, удалять в папке назначения те файлы, которых нет в источнике и т. д.).

Для запуска утилиты не нужны права суперпользователя. Очень часто эту команду применяют в операциях резервного копирования (для подключения к другим компьютерам используется протокол SSH).

Приведем несколько примеров использования команды.

```
rsync -azv /folder1/ /folder2/
```

Команда синхронизирует папки с сохранением параметров файлов и рекурсивно (ключ `a`), с использованием сжатия (ключ `z`) и с подробным отчетом (ключ `v`).

```
rsync -zvr /folder1/ user@192.168.100.3:/folder2/
```

Команда синхронизирует папку локального компьютера с удаленным (192.168.100.3), используя учетную запись пользователя `user` рекурсивно (ключ `r`), с применением сжатия (ключ `z`) и с подробным отчетом (ключ `v`). Временные параметры файлов не сохраняются.

```
rsync -avz --include 'A*' --exclude '*' /folder1/ /folder2/
```

Программа выполнит синхронизацию только файлов, название которых начинается с символа "A" (`include 'A*'` и `exclude` все остальные).

Отметим еще ключи: `-u` — запрещающий удаление модифицированных файлов в папке назначения; `--delete` — удаляет файлы, созданные в папке назначения, если их нет в папке источника; `--existing` — запрещает создавать новые файлы в папке назначения (синхронизирует только существующие данные); `-i` — отображает различия между папками (не копируя файлы); `--max-size` — устанавливает максимальный размер синхронизируемых файлов.

Синхронизация данных со сменным носителем

Часто возникает необходимость синхронизировать данные жесткого диска и сменного носителя (например, вы берете с собой файлы для работы дома или в командировке). Для этих целей существуют специальные программы. Проще всего для Windows-систем использовать бесплатную утилиту от Microsoft — SyncToy. Программа может проверять идентичность файлов не только по дате, но и по контрольной сумме, имеет разнообразные настройки операции (рис. 10.9).

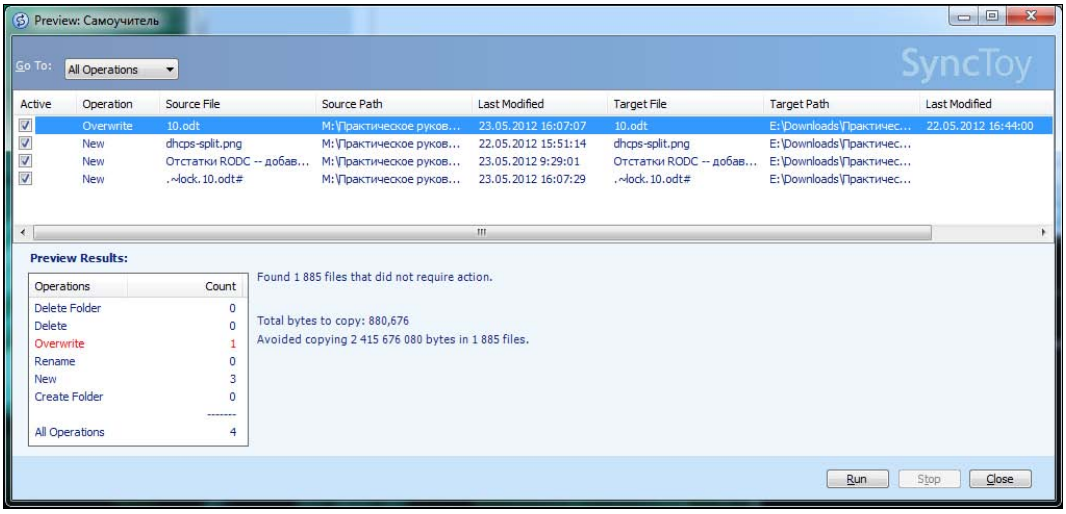


Рис. 10.9. Окно программы SyncToy (режим предварительного просмотра операций)

При сравнении информации в источнике и назначении при подобной синхронизации по умолчанию в большинстве случаев используется дата создания файла. Поэтому крайне важно иметь синхронизированное время на компьютерах, между которыми проводится операция.

Также следует учитывать, что если файл будет одновременно изменен по обоим путям, то утилита, как правило, сочтет самый новый файл правильным и заменит им все остальные копии. Если вы не хотите потерять данные в условиях возможной одновременной работы с обеими копиями, то нужно предпринимать дополнительные организационные меры.

Более корректно отрабатывает изменения функция "Портфель". Для создания портфеля достаточно выбрать соответствующую опцию в динамическом меню папки. Для переноса файлов на сменный носитель нужно просто скопировать на него папку портфеля. После чего в этой папке на сменном носителе можно продолжить работу с данными. Для синхронизации папок нужно отметить папку портфеля на сменном носителе и выбрать операцию **Обновить все**. Если изменения проведены над одним файлом в обеих папках, то программа выдаст предупреждение (рис. 10.10). В таком случае для объединения информации нужно использовать другие средства (например, в случае офиса воспользоваться операцией сравнений и объединения двух файлов, для текстовых файлов — утилитами поиска отличий и т. д.).

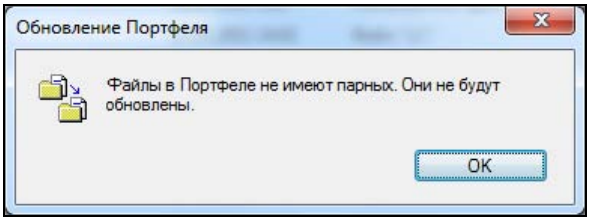


Рис. 10.10. Программа синхронизации портфеля обнаружила факт одновременных изменений данных

Автономные файлы

Функция автономных файлов позволяет автоматически сохранять на локальном диске информацию из подключенных сетевых ресурсов. В результате можно продолжить работу с файлами и после отключения от компьютерной сети (например, на ноутбуке в автономном режиме), а затем автоматически синхронизировать все изменения.

> ***Примечание***
>
> В первых версиях операционных систем при кэшировании зашифрованных файлов локальные копии данных во временной папке не шифровались. Впоследствии этот недостаток был устранен. Но при разрешении автономной работы с такими данными в целях предотвращения утечки данных администратору следует убедиться, что у пользователей установлены последние версии операционных систем.

Для того чтобы иметь возможность работать с автономными файлами, соответствующая опция должна быть включена на компьютере. Для этого нужно открыть **Центр синхронизации** (из Панели управления), перейти по ссылке **Управление автономными файлами** и нажать кнопку **Включить автономные файлы**. Об-

ратите внимание, что для вступления изменений в силу нужно перегрузить компьютер.

Сделать файлы сетевой папки доступными в автономном режиме можно, разрешив ее кэширование. Эта операция выполняется из контекстного меню подключенной сетевой папки выбором команды **Свойства** и установкой флажка **Всегда доступны вне сети** на вкладке **Автономные файлы** появляющегося диалогового окна. Обратите внимание, что по умолчанию не кэшируются файлы следующих типов: *.slm; *.mdb; *.ldb; *.mdw; *.mde; *.pst; *.db*, но эта установка может быть изменена с помощью групповой политики. Кроме того, контролируйте объем выделенного под размещение автономных файлов пространства, чтобы автономные копии нужной информации не были автоматически удалены из-за установленного лимита диска.

Работа с файлом при наличии подключения к сетевому ресурсу будет проводиться именно с сетевой копией. Синхронизация сетевой и автономной копии будет проводиться автоматически. Но вы можете инициировать эту операцию вручную из **Центра синхронизации**. Там же можно уточнить результаты синхронизации, наличие ошибок и т. д.

Чтобы начать работать с автономными файлами при отсутствии сетевого подключения, можно перейти по ссылке **Управление автономными файлами** и нажать кнопку **Просмотреть автономные файлы**. А после этого начать работу с нужным документом.

> ***Примечание***
>
> Windows автоматически переключает работу на автономные файлы при обнаружении медленного канала связи. Но режим работы с автономными файлами может быть включен и вручную. В этом случае можно нажать кнопку **Вне сети** (появляется в папке автономных файлов при включенной настройке), отредактировать нужную информацию и после чего осуществить подключение. Изменения будут автоматически синхронизированы.

Разрешение конфликтов

В случае работы с автономными копиями файлов возможно возникновение ситуаций, когда документ редактировался автономно, также и был изменен другим пользователем на сетевом ресурсе. В этом случае программа предложит вам выбрать один из трех вариантов разрешения данного конфликта: либо сохранить обе версии файлов, либо использовать версию на сетевом ресурсе, либо локальную копию.

Удаление автономных файлов

Удалить автономные копии файлов можно двумя способами. Первый способ — это удалить файлы из папки, в которой они хранятся для автономной работы (ярлык к этой папке часто выводят на рабочий стол для возможности работы с файлами в автономном режиме). Второй способ — это выбрать операцию удаления автономных файлов в окне настройки соответствующих опций папок компьютера.

Но обратите внимание, что такое удаление не отключает само кэширование файлов. При следующем соединении с сетевыми ресурсами кэширование будет проведено

снова и на локальном диске опять будут созданы автономные копии файлов. Чтобы отключить кэширование, необходимо изменить опции настройки папок системы.

Настройка автономных почтовых папок

Если политика организации предусматривает хранение почты сотрудников только на почтовом сервере или вы работаете с открытыми почтовыми системами Интернета, то для ускорения удаленной работы с почтой следует создать локальные копии почтовых сообщений. Для этого нужно установить локальный почтовый клиент.

Обычно программы почтовых клиентов сохраняют копии сообщений в локальных папках. Но настройки популярных программ имеют некоторые особенности.

Настройка автономных папок в Outlook 20*x* производится через меню **Сервис | Параметры |** вкладка **Настройка почты**. На этой вкладке нужно нажать кнопку **Отправить** и получить, чтобы открылось окно настройки параметров отправки и получения корреспонденции, в котором и следует выполнить необходимые действия.

После настройки автономных папок сообщения (для выбранных папок) будут скопированы на локальный компьютер. В дальнейшем по выбранному графику содержимое папок будет синхронизироваться с почтовым сервером. Причем пользователь сможет продолжать работу с почтой и при отсутствии связи: сообщения будут отосланы или приняты сразу после восстановления соединения.

При использовании программы Outlook совместно с сервером возможность кэширования почтовых папок позволяет снизить нагрузку на почтовый сервер и продолжать работу при отсутствии подключения.

Перенаправление папок хранения документов

Для систем Windows администратор может с помощью групповой политики осуществить перенаправление целого ряда специальных папок на сетевые ресурсы. Так можно перенаправить Рабочий стол, Мои документы, Мои рисунки, меню **Пуск**, папку Application Data. Это выполняется в разделе **Конфигурация пользователя | Конфигурация Windows | Перенаправление папок**.

Такое решение может быть рекомендовано, поскольку позволяет хранить на сервере актуальные копии всех документов, с которыми работают пользователи. Это облегчает операции резервного копирования данных и снижает риск утери информации в случае выхода из строя клиентского компьютера. Однако сохранение файлов на сервере неизбежно выполняется медленнее, чем локально, что может вызывать некоторые недовольства пользователей. Одновременно повышается нагрузка на сервер и увеличивается объем необходимого для него дискового пространства.

> ***Примечание***
>
> Не забудьте отключить эти установки для профилей, применяемых при удаленном подключении.

Доступ к локальной системе из-за межсетевого экрана

Часто пользователям требуется получить доступ к своему компьютеру из Интернета. Заблуждением многих администраторов является мнение, что межсетевой экран препятствует любой попытке подключения извне к локальной системе. Если компьютеру разрешен доступ в глобальную сеть, то нельзя исключить и обратную возможность: подключение к нему из внешнего мира.

Мы не будем рассматривать возможности, использующие уязвимости межсетевых экранов. Они есть и будут. Но чтобы воспользоваться ими, нужно иметь достаточный опыт. Есть способы, доступные любому пользователю. На рис. 10.11 представлено окно бесплатной версии программы TeamViewer, показывающее готовность подключения к клиенту, находящемуся в локальной сети организации за межсетевым экраном.

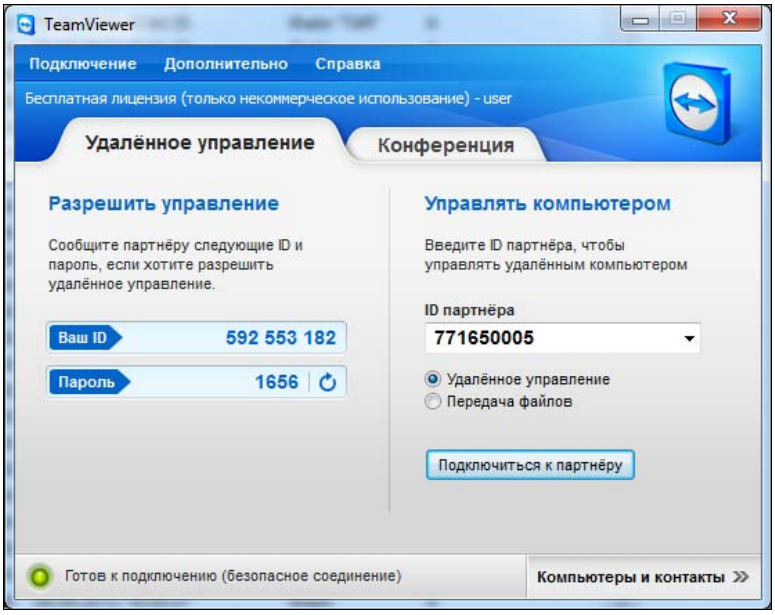


Рис. 10.11. Подключение к данным компьютера возможно из любой точки Интернета

Идея доступа к локальному компьютеру извне заключается в следующем. На компьютер устанавливается программа, которая инициирует подключение к некоему серверу в глобальной сети. Поскольку это подключение осуществляется изнутри сети по разрешенным протоколам, то оно пропускается межсетевым экраном. На компьютер, с которого требуется подключиться к системе за межсетевым экраном, доступ к целевому компьютеру осуществляется через сервер соответствующей программы. После чего обычно устанавливается прямое подключение. Как правило, для подключения можно использовать обозреватель Интернета. Это обозначает, иными словами, возможность подключения к локальной системе из любой точки

Сети, поскольку обозреватели Интернета имеются на любых компьютерах в любых интернет-кафе и других публичных точках.

Подобных решений существует много. Можно упомянуть LogMeIn (бесплатное решение, **https://secure.logmein.com/solutions/personal/**), TeamViewer (разрешено бесплатное некоммерческое использование, **http://http://www.teamviewer.com/ru/index.aspx**), Anyplace Control (**http://www.anyplace-control.com/solutions.shtml**) и др. Поэтому блокирование на межсетевом экране списка таких серверов не решает кардинально проблему безопасности: не исключена возможность появления нового сервера или перехода на иное программное решение.

Предотвратить описанный способ нарушения безопасности информационной системы можно только тотальным контролем запускаемого программного обеспечения.

ГЛАВА 11

Мониторинг информационной системы

Как правило, начинающие системные администраторы сопровождают несколько небольших информационных систем (сервер плюс до десятка рабочих станций) и слабо представляют, зачем нужны системы мониторинга.

Зачем нужен мониторинг?

Мониторинг компьютеров и сетевых устройств дает возможность:

- узнавать о неисправностях не от руководства или рассерженных пользователей, а от системы контроля. Это позволяет получить определенный запас времени на поиск причин ошибок и восстановление работы, а в некоторых случаях пользователи могут даже и не узнать о том, что система какой-то промежуток времени была частично неработоспособной;
- для повторяющихся ситуаций настроить автоматическое реагирование на возникающие события. В результате неисправность можно устранить автоматически, сразу после ее возникновения, не влияя на работу сотрудников предприятия;
- часто *предупредить* отказ той или иной службы. Простейший пример: контроль свободного пространства на жестких дисках может предотвратить отказ, вызванный нехваткой места для записи новой информации. Таких "предсказывающих" параметров существует достаточно много, и они активно используются в сценариях мониторинга.

Это лишь несколько примеров, свидетельствующих о крайней желательности реализации возможностей систем мониторинга.

Системы мониторинга

Контролировать состояние информационной системы можно различными способами. Учитывая, что любой контроль — это анализ возвращаемых сценариями наблюдения данных, простую систему для ограниченных целей нетрудно собрать на основе образцов скриптов из Интернета.

Существующие системы мониторинга позволяют не изобретать велосипед, а воспользоваться уже готовыми проработками. В сообществе присутствует много разработок для мониторинга информационных систем как небольших организаций, так и крупных предприятий с многочисленными филиалами. Лидером среди профессиональных систем мониторинга является Nagios (бесплатное решение, работающее практически со всем спектром систем). Для систем на основе Windows наибольшим спектром возможностей обладает выделить Microsoft System Control Center (коммерческий продукт).

Многие вендоры выпустили специальные версии систем мониторинга, предназначенные для небольших организаций. Эти версии либо отличаются крайне низкой стоимостью, либо вообще бесплатны. Например, OpManager (**http://www.manageengine.com/products/opmanager/download.html**), который может контролировать бесплатно до 10 систем (включая серверы Windows и Linux, активное сетевое оборудование).

Агентный и безагентный способы мониторинга

Контролировать систему можно несколькими способами. Во-первых, можно проверять реакцию служб на внешние запросы, например, ответ почтового сервера при подключении по одному из почтовых протоколов или результаты запроса какой-либо информации с сервера баз данных. Такой способ не требует "вмешательства" в контролируемые системы, но предполагает достаточную интеллектуальность программы, которая должна смоделировать все правила общения с удаленной службой и проанализировать ответ (естественно, что простейшие методы контроля, например проверку достижимости систем командой `ping`, можно реализовать очень просто). Понятно, что возможности контроля ограничены тем функционалом, который доступен извне контролируемой системы.

Второй способ предполагает установку на контролируемую систему некоторой программы, ее принято называть *агентом*, который либо самостоятельно выполняет проверки по заданному графику, либо обеспечивает выполнение задания контроля, получаемого с сервера. Результаты проверки агентом возвращаются на сервер мониторинга. При данном способе контроля наблюдению доступны практически любые параметры как оборудования, так и программной среды. Недостатки этого способа — необходимость предварительной установки агентов, затраты производительности на исполнение агентов (ресурсы отнимаются от основных задач, для которых и установлен сервер). В зависимости от числа проверок, их частоты, производительности контролируемой системы и т. п. накладные затраты могут достигать величины 3—5% и более.

Какие параметры системы обычно контролируют

Программы мониторинга настраивают на контроль параметров, которые свидетельствуют о штатном функционировании системы. Например, процент загрузки про-

цессора не должен превышать заданной величины, в системе должна иметься свободная память, на дисках оставаться некоторый свободный объем и т. п. В зависимости от решаемых прикладных задач к числу контролируемых параметров добавляют проверку ответов сервера баз данных на типовые запросы, проверку возвращаемой информации от веб-сервера, от почтовой системы и т. п.

Поскольку практически невозможно охватить контролем все задачи, то стараются включить в объем контроля сообщения системы о неисправностях. Операционная система постоянно фиксирует состояние выполнения тех или иных операций в журналах. На практике записи в журналах являются для администратора "первой ласточкой", предупреждающей о неполадках в работе. В случае Windows — это журналы системы (основные: приложений, безопасности, системы и дополнительные), для Linux-систем — журнал syslog.

В хорошо настроенной системе в журналах должны быть только записи информационного характера. Поэтому любое сообщение о неисправности (уровня предупреждения или ошибки) обязательно должно анализироваться администратором. Очень плохо, если администратор не обращает внимания на сообщения о некоторых ошибках, не влияющих на работу системы (например, об ошибках аутентификации по протоколу Kerberos с последующим использованием протокола NTLM). В этом случае очень легко пропустить сообщение, которое обязательно должно быть обработано.

В то же время нужно четко представлять, что системы мониторинга могут предупреждать только о тех ошибках, информация о которых доступна операционной системе. Например, если в сервере есть аппаратный RAID-массив, а программный компонент, считывающий информацию с него, отсутствует, то вы не сможете быть предупреждены об отказе одного из дисков в массиве.

В любом случае никакая система мониторинга не сможет заменить квалифицированного системного администратора, она в состоянии только избавить его от рутинных операций.

Простейший вариант мониторинга по журналам

Операционная система фиксирует сообщения о неполадках работы своих компонентов в журналах событий. Поэтому сбор информации из журналов системы является простейшим способом мониторинга системы, причем полностью бесплатным и не нуждающимся в установке и настройке каких-либо компонентов. К тому же очень легко настроить сбор событий журналов с нескольких серверов организации на одну систему.

Log Parser

Для обработки событий журнала можно использовать бесплатную утилиту Log Parser, которая позволяет анализировать файлы журналов системы, XML- и CSV-файлы, реестр Windows, данные службы каталогов Active Directory.

Для использования Log Parser необходимо с помощью ключей команды указать источник данных и вариант обработки (например, выбрать события только от заданного источника за некоторый период времени определенного типа). Результаты запроса можно получить в текстовом формате или в специализированных форматах, например для загрузки в сервер баз данных, в формате SYSLOG или даже получить в виде диаграммы.

Мы не будем останавливаться специально на описании возможностей и особенностей использования данного средства. Соответствующие рекомендации доступны в Сети, в том числе и на русском языке.

Централизованная обработка журналов Windows

Журналы Windows системные администраторы имеют возможность анализировать централизованно. Для этого достаточно настроить *подписку* (рис. 11.1). При настройке подписки вы указываете правила сбора сообщений (фильтрации: какие сообщения нужно собирать), определяете компьютеры, с которых ведется сбор данных и т. д. Обычно (это настройки по умолчанию) все собранные таким образом сообщения направляют в журнал **Пересланные события**.

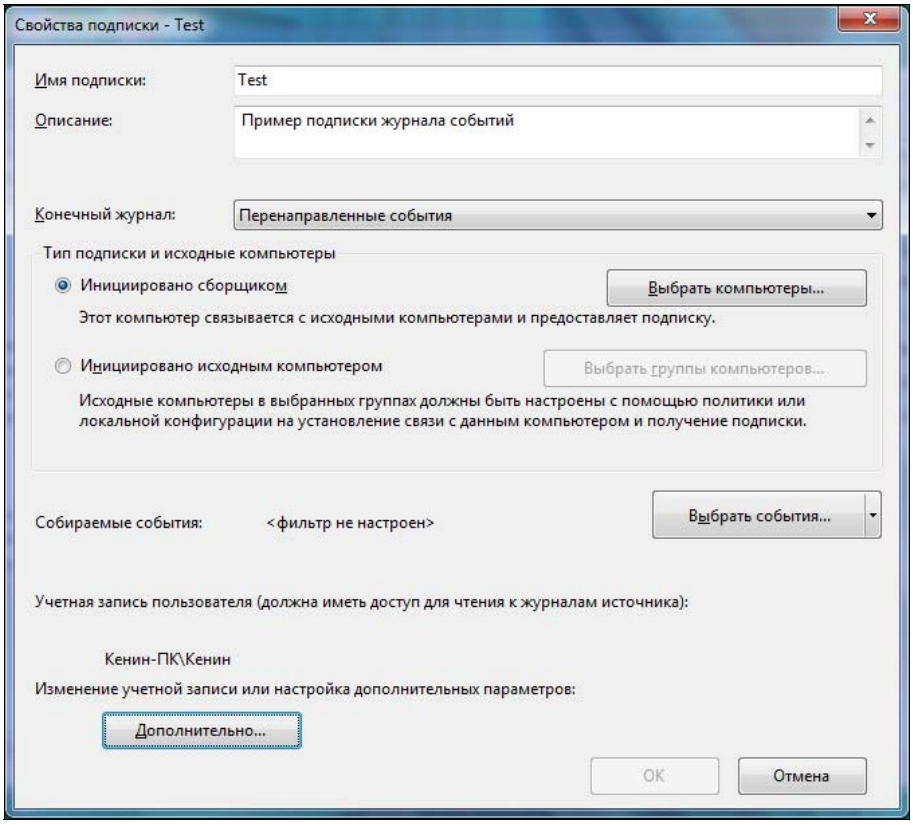


Рис. 11.1. Окно мастера настройки подписки

Примечания

В Windows Server 2003 функционал подписки на события журнала отсутствует, однако можно использовать встроенный сценарий EVENTQUERY.vbs, который позволяет анализировать события как с локального, так и с удаленных компьютеров, используя необходимые фильтры (по дате, по номеру события, типу и т. п.). Сценарий включает подробную справку, поэтому мы не будет останавливаться на описании использования. А сценарий EVENTTRIGGERS позволяет привязать обработку к некоторому событию.

Кроме того, централизованно анализировать журнал событий можно и другими средствами. Так, имеется утилита EventCombMT от Microsoft, имеющая графический интерфейс и позволяющая настроить централизованный сбор событий. Есть утилита LogParser, предназначенная для обработки не только журналов системы, но и различных прикладных программ и т. д.

Основной недостаток такого контроля в том, что за журналом нужно следить. Понятно, что на практике это делается далеко не всегда. Поможет в этом случае возможность *привязки задания к событию*. Для этого в панели **Действия** оснастки **Просмотр событий** необходимо выбрать операцию **Привязать задачу к...** и настроить необходимые параметры оповещения. В качестве реакций можно назначать запуск программы (например, отправку сообщения по сети с помощью команды `net send`), оповещение администратора по электронной почте и т. д.

Созданная задача будет отображаться в оснастке **Планировщик заданий**. На рис. 11.2 показано подобное задание в окне Планировщика.

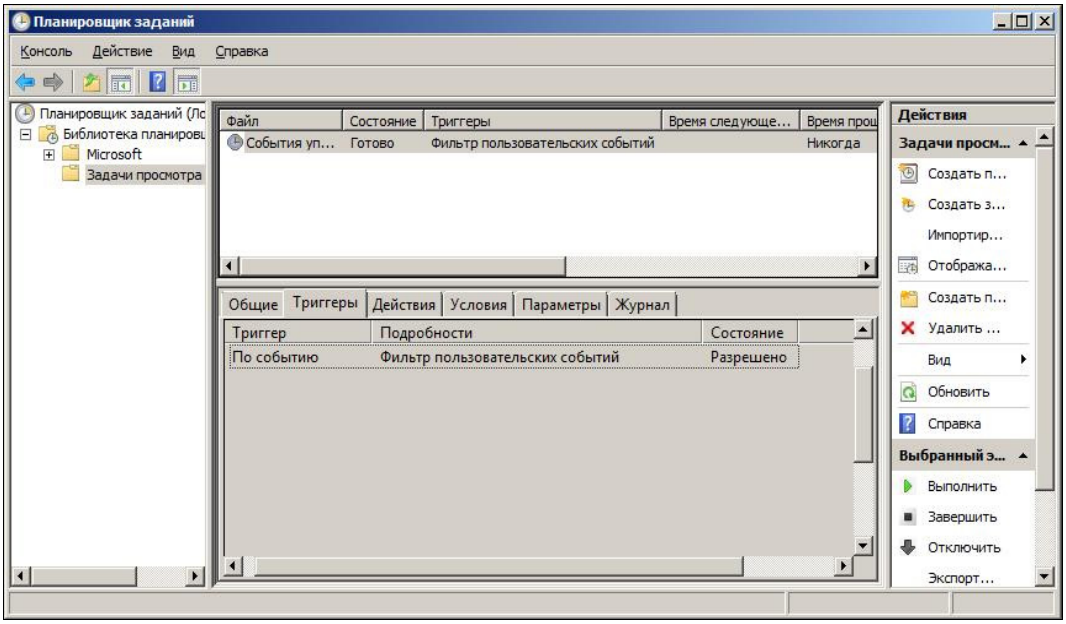


Рис. 11.2. Планировщик заданий Windows Server 2008

Syslog — системный журнал в Linux

Системный журнал в Linux создается специальным демоном (syslogd), которому "шлют" свои сообщения программы. Этот демон сравнивает сообщения с теми правилами обработки, которые записаны в его конфигурации (обычно это /etc/syslog.conf). При обнаружении соответствия в журнал записывается сообщение.

Конфигурация демона представляет собой перечень строк, в которых первый столбец указывает правило отбора, а второй — действия демона. Источник записи принято называть *категорией* (facility), каждая категория имеет несколько *уровней* (level) — ошибка, важно, информация и т. п.

В качестве действий можно указывать журналы (тогда сообщение будет записано в этот журнал), пользователей (им будет отослано сообщение, если они работают в системе), другие компьютеры (их имя должно быть написано с символа "@"), программы (в этом случае название программы должно быть предварено символом перенаправления потока — "|").

Таким образом, настройка syslog — это не только настройка собственно журнала, но и фактически настройка и операций автоматического оповещения, и реагирования на события.

Следующие строки конфигурации иллюстрируют приведенное выше описание:

```
# Следующая настройка записывает все сообщения почты в один журнал
mail.* /var/log/maillog
# Все аварийные сообщения доводятся до всех пользователей
*.emerg *
# Дополнительно все аварийные сообщения протоколируются на другую систему
*.emerg @myhost.test.local
```

Nagios

Nagios является практическим стандартом систем мониторинга. Nagios бесплатен, но на его основе создана коммерческая версия Nagios XI, отличающаяся наличием большого количества мастеров, облегчающих выполнение настроек (например, мастера создания новых контролируемых систем, шаблоны мониторинга серверов MS Exchange, Oracle и т. п.). С точки зрения функциональности эти продукты идентичны, приложив некоторые усилия, администратор может настроить бесплатную версию по нуждам своей организации.

Nagios позволяет (это далеко не полный список возможностей):

- контролировать хосты (загрузка процессора, использование диска, события в журналах и т. д.) с разнообразными операционными системами — Windows, Linux, AIX, Solaris и т. д.;
- контролировать сетевые службы (SMTP, POP3, HTTP, SSH и т. д.);
- контролировать системы на основе протокола SNMP;

- подключать дополнительные модули расширения (плагины) на любом языке программирования (Shell, C++, Perl, Python, PHP, C# и др. — архитектура модулей открыта);
- осуществлять параллельную проверку систем (для повышения производительности);
- отправлять оповещения в случае возникновения проблем с помощью электронной почты, сообщений SMS и т. п.;
- автоматически реагировать на события службы или хоста.

Помимо Nagios можно упомянуть также проекты мониторинга, как Cacti (**http://cacti.net/**), Munin (**http://munin.projects.linpro.no/**), OpenNMS (**http://www.opennms.org/**), ZABBIX (**http://www.zabbix.com/**) и др. Для каждого из них в Сети доступны многочисленные расширения, позволяющие достаточно просто обеспечить контроль работы информационной системы.

Установка Nagios в Ubuntu из репозитория

Nagios для пользователей Ubuntu доступен в качестве готового пакета. К сожалению, последняя его версия (Nagios 3) подготовлена только для актуальных выпусков Ubuntu. Ее можно установить командой

```
apt-get install nagios3
```

Это гарантирует установку всех необходимых для его работы библиотек и является самым простым способом, рекомендуемым для обычных пользователей.

Для предыдущих версий ОС (если по каким-то причинам вы не планируете переход на актуальные редакции) пакет Nagios 3 нужно установить из исходных кодов или устанавливать предыдущую версию (Nagios 2) командой

```
apt-get install nagios
```

Установка Nagios из исходных кодов

При желании использовать самую последнюю версию продукта, ее следует установить из исходных кодов. Мы остановимся на описании этого процесса, чтобы показать читателю, что подобные операции не представляют никакой сложности.

Подготовка операционной системы

Для установки Nagios выбрана серверная версия операционной системы Ubuntu (без графического интерфейса).

Процедура быстрой установки программы на Ubuntu описана на сайте в разделе документации (**http://nagios.sourceforge.net/docs/3_0/quickstart-ubuntu.html**). Хотя статья описывает процесс для седьмой версии сервера Ubuntu, все рекомендации применимы и для последующих версий. Мы приведем далее описание установки Nagios с краткими пояснениями, поскольку страницы указанного сайта не доступны в русской локализации.

Операционную систему Ubuntu нужно установить с дистрибутива, загруженного с первоисточника (**http://www.ubuntu.org**). Установку производить с параметрами по умолчанию с локализацией для Российской Федерации и выбором часового пояса. После установки система должна быть обновлена с официальных источников командой `apt-get update && apt-get upgrade`.

После этого необходимо установить командой `apt-get install` следующие пакеты операционной системы:

- пакет unzip — для обеспечения работы с архивами;
- пакет mc — для упрощения файловых операций;
- build-essential — для обеспечения возможности компиляции приложений.

Nagios требует наличия в системе ряда пакетов:

- apache2;
- apache2-utils;
- exim4 exim4-base;
- exim4-config;
- exim4-daemon-light;
- libapache2-mod-php5;
- libapr1;
- libaprutil1;
- libgd2-noxpm;
- libgd2-xpm-dev;
- libgd-tools;
- libglib2.0-dev;
- libjpeg62;
- libjpeg62-dev;
- libperl-dev;
- libpng12-dev;
- libpq5;
- librrds-perl;
- libsnmp15;
- mailutils;
- mrtg;
- perl-base;
- rrdtool.

Установка пакетов должна быть произведена с использованием команды `apt-get`.

> ***Примечание***
>
> Версии пакетов (перечисленных здесь и далее) могут отличаться от указанных. Соответственно необходимо подправить команды установки.

Установка пакета net-snmp

Пакет net-snmp необходим для мониторинга SNMP-устройств. Его установка должна быть проведена до инсталляции сервера Nagios. Страница загрузки — **http://www.net-snmp.org/download.html** (желательно выбрать последнюю стабильную версию длительной поддержки).

Предварительно необходимо скопировать файл установки на компьютер, разархивировать его и перейти в папку с кодом. Установка выполняется следующими операциями:

```
./configure
make
make install
```

Установка собственно Nagios и базового набора плагинов

Перед установкой пакета необходимо создать учетные записи, которые будут использованы пакетом мониторинга. Эти операции выполняются следующими командами:

```
useradd -m nagios
passwd nagios
groupadd nagios
usermod -G nagios nagios
groupadd nagcmd
usermod -a -G nagcmd nagios
usermod -a -G nagcmd www-data
```

Для установки необходимо загрузить с сервера последние версии стабильного кода самого пакета и плагинов (**http://www.nagios.org/download/** — **http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-3.4.1.tar.gz**). Установка выполняется следующими командами:

```
tar xzfp nagios-3.4.1.tar.gz
tar xzfp nagios-plugins-1.4.15.tar.gz
cd nagios
./configure --with-command-group=nagcmd
make all
make install
make install-init
make install-config
make install-commandmode
make install-webconf
cd...
cd nagios-plugins-1.4.15
./configure --with-nagios-user=nagios --with-nagios-group=nagios
make
make install
```

Далее надо создать пользователя, которому будет разрешен доступ к веб-интерфейсу программы, и назначить ему пароль (этот пароль необходимо запомнить для последующей работы) следующей командой:

```
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Для вступления в силу внесенных изменений следует перегрузить веб-сервер:

```
/etc/init.d/apache2 reload
```

После этих операций Nagios практически готов к работе.

Для того чтобы система мониторинга запускалась автоматически, необходимо добавить ссылки на сценарий запуска в соответствующие папки каталога запуска. Эта операция выполнена командой

```
update-rc.d nagios defaults
```

Настройка модуля построения графиков

Для построения графиков работы устройств необходима установка соответствующего пакета. Существует несколько достаточно сходных решений (см., например, PNP4Nagios, **http://www.pnp4nagios.org/**), незначительно отличающихся по настройкам интеграции с Nagios. В этой главе мы рассмотрим реализацию ПО Nagiosgraph.

> ***Примечание***
>
> Установка модуля может быть проведена с помощью сценария установки. Но обычно начинающему пользователю трудно правильно ответить на вопросы о путях размещения файлов. Поэтому мы описываем ручные операции настройки.

Этот модуль нужно загрузить с **http://sourceforge.net/projects/nagiosgraph/**, перенести на сервер и разархивировать:

```
tar xzfv nagiosgraph-1.4.4.tar.gz
```

Затем скопировать настройки программы в папку /etc/nagiosgraph:

```
mkdir /etc/nagiosgraph
cd nagiosgraph-1.4.4
cp etc/* /etc/nagiosgraph
```

Далее модифицировать сценарии программы (Perl-скрипты в папке cgi и сценарий lib/insert.pl), отредактировав строку `use lib` так, чтобы она указывала на /etc/nagiosgraph:

```
use lib '/etc/nagiosgraph';
```

После чего скопировать исполняемый файл в папку nagios:

```
cp lib/insert.pl /usr/local/nagios/libexec
```

Затем скопировать CGI-сценарии, шаблоны и Java-сценарии в папки веб-сервера:

```
cp cgi/*.cgi /usr/local/nagios/sbin
cp share/nagiosgraph.css /usr/local/nagios/share
cp share/nagiosgraph.js /usr/local/nagios/share
```

Отредактировать файл конфигурации /etc/nagiosgraph/nagiosgraph.conf, заменив значения указанных переменных по образцу:

```
rrddir = /var/nagios/rrd
nagiosgraphcgiurl = /nagios/cgi-bin
javascript = /nagios/nagiosgraph.js
stylesheet = /nagios/nagiosgraph.css
logfile = /var/nagios/nagiosgraph.log
cgilogfile = /var/nagios/nagiosgraph-cgi.log
```

После чего создать файлы журналов и настроить права доступа для файлов программы:

```
mkdir -p /var/nagios/rrd
chown nagios /var/nagios
```

```
chmod 755 /var/nagios
chown nagios /var/nagios/rrd
chmod 755 /var/nagios/rrd
touch /var/nagios/nagiosgraph.log
touch /var/nagios/perfdata.log
chown nagios /var/nagios/perfdata.log
chmod 666 /var/nagios/perfdata.log
chown nagios /var/nagios/nagiosgraph.log
chmod 664 /var/nagios/nagiosgraph.log
touch /var/nagios/nagiosgraph-cgi.log
chown www-data /var/nagios/nagiosgraph-cgi.log
chmod 664 /var/nagios/nagiosgraph-cgi.log
```

Отредактировать файл /usr/local/nagios/etc/nagios.cfg:

```
process_performance_data=1
service_perfdata_file=/var/nagios/perfdata.log
service_perfdata_file_template=$LASTSERVICECHECK$||$HOSTNAME$||$SERVICEDESC$||
$SERVICEOUTPUT$||$SERVICEPERFDATA$
service_perfdata_file_mode=a
service_perfdata_file_processing_interval=30
service_perfdata_file_processing_command=process-service-perfdata
```

Добавить команду Nagios (в файле /usr/local/nagios/etc/objects/commands.cfg необходимо отредактировать существующий блок описания этой команды):

```
define command {
command_name process-service-perfdata
command_line /usr/local/nagios/libexec/insert.pl
}
```

Скопировать пиктограмму ПО:

```
cp share/graph.gif /usr/local/nagios/share/images/action.gif
```

Отредактировать файлы сценария Nagiosgraph (в папке исходных кодов — share/nagiosgraph.ssi), заменив значение `src="/nagiosgraph/nagiosgraph.js"` на `src="/nagios/nagiosgraph.js"` и скопировав файл:

```
cp share/nagiosgraph.ssi /usr/local/nagios/share/ssi/common-header.ssi
```

Отредактировать боковую панель интерфейса Nagios (/usr/local/nagios/share/side.php), вставив следующий блок после заголовка 'Trends':

```
<li><a href="<?php echo $cfg["cgi_base_url"];?>/trends.cgi" target="<?php echo
$link_target;?>">Trends</a>
<ul>
<li><a href="<?php echo $cfg["cgi_base_url"];?>/show.cgi" target="<?php echo
$link_target;?>">Graphs</a></li>
<li><a href="<?php echo $cfg["cgi_base_url"];?>/showhost.cgi" target="<?php
echo $link_target;?>">Graphs by Host</a></li>
<li><a href="<?php echo $cfg["cgi_base_url"];?>/showservice.cgi" target="<?php
echo $link_target;?>">Graphs by Service</a></li>
```

```
<li><a href="<?php echo $cfg["cgi_base_url"];?>/showgroup.cgi" target="<?php
echo $link_target;?>">Graphs by Group</a></li>
</ul>
</li>
```

Чтобы не описывать график для каждой службы, нужно создать специальное описание службы, например, в файле nagiosgraph.cfg со следующим содержимым:

```
define service {
name graphed-service
action_url /nagios/cgi-bin/show.cgi?host=$HOSTNAME$&service=$SERVICEDESC$'
onMouseOver='showGraphPopup(this)' onMouseOut='hideGraphPopup()'
rel='/nagios/cgi-bin/showgraph.cgi?host=$HOSTNAME$&service=
$SERVICEDESC$&period=week&rrdopts=-w+450+-j
}
```

Этот файл нужно поместить в папку, все файлы которой подгружаются при старте Nagios (или явно указать на его загрузку).

В дальнейшем, при желании показать график работы службы достаточно в ее описание добавить следующие строки по образцу:

```
define service {
use local-service,graphed-service
...
}
```

Настройка почтового клиента

Для отправки сообщений от Nagios по электронной почте используется клиент mail. Его необходимо настроить командой

```
dpkg-reconfigure exim4-config
```

В процессе работы мастера установки следует указать вариант отправки почты только через smarthost. В качестве такой системы необходимо указать сервер электронной почты предприятия.

Первичное подключение к Nagios

Для отображения информации системы мониторинга достаточно открыть страницу **http://localhost/nagios/** (вместо **localhost** следует указать имя сервера Nagios при открытии страницы с удаленного компьютера). На запрос параметров авторизации необходимо ввести имя nagiosadmin и тот пароль, который вы назначили для этой учетной записи на предыдущих шагах.

На рис. 11.3 показана одна из страниц программы — структура состояния служб небольшой системы с различными статусами (нормальное состояние, критическое, предупреждения, неустойчивые состояния).

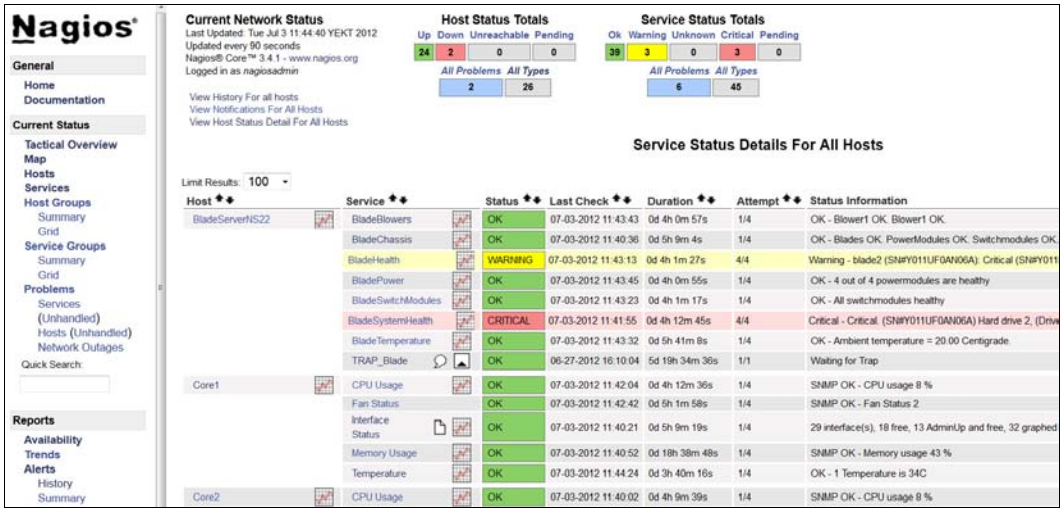


Рис. 11.3. Страница состояния служб системы в Nagios

Немного о логике работы Nagios

Nagios может осуществлять как активную проверку систем, так и пассивную.

Активная и пассивная проверки

Активная проверка подразумевает запуск операции проверки самим сервером. Это может быть операция с использованием агента, установленного на контролируемой системе (например, запуск какого-либо сценария на удаленном компьютере), так и без агента (например, отправка HTTP-запроса на веб-сервер и последующий анализ полученного сообщения).

Пассивная проверка предполагает обработку сообщений о событиях, которые отправляются системами на сервер Nagios самостоятельно, по мере возникновения. Такими событиями могут быть SNMP-трапы (так принято называть сообщения от самих систем по протоколу SNMP) и любые другие сообщения.

Программы агентов Nagios

Понятно, что проверка системы с использованием установленного агента обладает максимальной функциональностью. Существуют различные версии клиентов, но наиболее часто для систем на основе Linux используется программа NRPE (ссылка на этот плагин присутствует на официальном сайте Nagios — **http://www.nagios.org/**), а для Windows-компьютеров — NSClient++ (**http://trac.nakednuns.org/nscp/**). Способы автоматической установки клиентов на все системы в этой книге не рассматриваются, интересующиеся читатели могут обратиться к книге "Самоучитель системного администратора"[1]. Обратим только внимание на то, что для

[1] Кенин А. М. Самоучитель системного администратора. — 3-е изд. — СПб.: БХВ-Петербург, 2012.

каждого клиента должна быть настроена конфигурация так, как описано в последующих разделах.

Терминология Nagios

Плагины

Для того чтобы проверить какой-либо параметр, сервер Nagios должен выполнить определенную команду. Например, запустить сценарий, который выполнит подключение к контролируемому почтовому серверу и проанализирует его ответ. Или выполнить запрос свободной памяти на клиенте. Или проанализировать состояние ряда интерфейсов коммутационного оборудования.

В терминах Nagios такие команды принято называть *плагинами* (plugin).

При стандартной установке на сервере доступны плагины, которые перечислены в табл. 11.1.

Таблица 11.1. *Базовые плагины Nagios*

Плагин	Назначение
check_apt	Контроль состояния обновлений систем Linux, производимых с помощью команд `apt-get`. Позволяет запустить процесс обновления при соответствующей настройке
check_breeze	Контроль мощности сигнала Wi-Fi стандарта Breezecom
check_by_ssh	Этот плагин позволяет запускать на удаленной системе команды, используя протокол SSH
check_clamd	Проверка соединения CLAMD (антивирусная программа) с удаленным хостом
check_cluster	Проверка состояния хостов кластера Linux
check_dhcp	Проверка доступности DHCP-серверов в сети
check_dig	Проверка работы DNS-службы на хосте (командой `dig`)
check_disk	Проверка объемов использования дискового пространства (собственных и примонтированных дисков)
check_disk_smb	Проверка объемов использования дисков, подключенных по протоколу SMB (обычно это диски от Windows-систем)
check_dns	Проверка работы сервера DNS с помощью программы `nslookup`
check_dummy	Плагин для настройки: просто возвращает численный параметр и строку, описанные при его запуске
check_file_age	Проверка времени создания файлов
check_flexlm	Проверка службы Flexlm license manager
check_ftp	Проверка FTP-соединения с удаленным хостом
check_hpjd	Проверка состояния принтеров Hewlett-Packard с установленной картой JetDirect (проверка осуществляется по протоколу SNMP)

Таблица 11.1 *(продолжение)*

Плагин	Назначение
check_http	Проверка HTTP-соединений с удаленной системой. Проверка может осуществляться как по протоколу HTTP, так и по HTTPS. Можно контролировать время установки соединения, срок действия сертификатов сервера, а также ответ сервера (по поиску в ответе некоторой заданной строки, в том числе, допускается использование регулярных выражений)
check_icmp	Проверка удаленных хостов по протоколу ICMP
check_ide_smart	Проверка состояния локального диска (в Linux-системе) по технологии SMART
check_ifoperstatus	Проверка состояния работы сетевого интерфейса на заданной Linux-системе
check_ifstatus	Проверка состояния сетевого интерфейса на заданной Linux-системе
check_imap	Проверка работы удаленного хоста по протоколу IMAP. Можно анализировать ответ сервера на посылаемую на него строку imap-запроса
check_ircd	Проверка IRCD-плагина Nagios
check_jabber	Проверка JABBER-подключения к удаленному хосту
check_ldap	Проверка LDAP-сервера (можно отправить запрос на поиск соответствующего атрибута)
check_ldaps	Тоже проверка LDAP-сервера, только с использованием защищенных соединений (по протоколу SSL)
check_load	Проверка загрузки Linux-системы
check_log	Проверка журналов Linux-системы на наличие некоторой последовательности символов
check_mailq	Проверка числа сообщений в очереди почтового сервера (работает с различными версиями sendmail, qmail)
check_mrtg	Проверяет заданную переменную в журнале MRTG (Multi Router Traffic Grapher) на минимальное/максимальное значения (для контроля параметров производительности необходимо использовать check_mrtgtraf)
check_mrtgtraf	Проверяет значения исходящего и входящего трафиков коммутаторов, записанные в журнал MRTG. Требуется первоначальная установка пакета MRTG (**http://ee-staff.ethz.ch/~oetiker/Webtools/mrtg/mrtg.html**)
check_nagios	Проверяет состояние процесса nagios на локальной машине
check_nntp	Проверяет NNTP-соединение с указываемым хостом
check_nntps	То же, но с использованием протокола NNTPS
check_nrpe	NRPE плагин Nagios
check_nt	Этот плагин осуществляет сбор данных со службы NSClient на Windows-системах
check_ntp	Проверка NTP-сервера. Вместо этого плагина рекомендуется применять check_ntp_peer
check_ntp_peer	Проверка NTP-сервера. Позволяет оценивать, в том числе, дрожание (jitter) сигнала времени

Таблица 11.1 *(продолжение)*

Плагин	Назначение
check_ntp_time	Этот плагин проверяет разницу времени между локальным сервером и указываемым удаленным NTP-сервером
check_nwstat	Служит для сбора данных с Novell-серверов. Требует установки дополнительных пакетов
check_oracle	Проверяет подключение к серверу Oracle, позволяет оценить размеры баз данных и наличие свободного места, состояние буферов кэширования и т. д.
check_overcr	Проверяет состояние Over-CR collector daemon на удаленной системе (**http://www.molitor.org/overcr**)
check_ping	Проверяет соединение с удаленной системой с использованием пакетов ping
check_pop	Проверяет удаленные хосты по протоколу POP. Позволяет отправить на почтовый сервер строку запроса и проанализировать ответ сервера
check_procs	Проверяет состояние процессов Linux-системы
check_real	Проверяет состояние службы REAL (RTCP-подключений)
check_rpc	Проверяет состояние RPC-службы на указанном хосте
check_sensors	Проверяет состояние аппаратных датчиков системы Linux. Информация с датчиков получается с помощью пакета lm_sensors
check_simap	Проверяет IMAP-подключение по безопасному каналу к серверу. Контролируется время ответа и содержание (по анализу ответа на заданный запрос), правильность сертификатов
check_smtp	Проверяет SMTP-подключение к серверу. Ответ почтового сервера может анализироваться на наличие заданных строк. Также контролируется время отклика
check_snmp	Проверка удаленных систем (и получение с них данных) по протоколу SNMP
check_spop	Проверяет POP-подключение по безопасному каналу к серверу. Контролируется время ответа и содержание (по анализу ответа на заданный запрос), правильность сертификатов
check_ssh	Проверка подключения к SSH-серверу
check_ssmtp	Проверяет SMTP-подключение по безопасному каналу к серверу. Ответ почтового сервера может анализироваться на наличие заданных строк. Также контролируется время отклика
check_swap	Проверяет свободное пространство в SWAP-файле локальной системы
check_tcp	Проверка TCP-подключения к указанной системе. Проверяется наличие отклика, его время, присутствие в отклике заданных строк и т. п.
check_time	Проверка времени на указанном хосте
check_udp	Проверка UDP-подключения к указанной системе. Проверяется наличие отклика, его время, присутствие в отклике заданных строк и т. п.
check_ups	Проверка состояния источников бесперебойного питания на локальной или удаленной Linux-системе. Для работы плагина требуется, чтобы в системе был установлен демон UPSD (**http://www.networkupstools.org**)

Таблица 11.1 *(окончание)*

Плагин	Назначение
check_users	Проверка числа пользователей, вошедших в локальную систему
check_wave	Проверка уровня Wi-Fi-сигнала

Каждый из этих плагинов содержит справочную информацию, описывающую особенности его применения (вывод справки по команде `<плагин> -h`).

Перечисленные плагины являются базовыми. Если какая-либо задача не может быть проконтролирована с их помощью, то обычно в Сети легко можно найти несколько вариантов бесплатно доступных плагинов. Существует специальный сайт обмена плагинами — **http://exchange.nagios.org/**; многие решения можно найти и обычным поиском.

Особенности установки Perl-плагинов

Для работы многих плагинов[1], написанных на языке Perl, необходим модуль Net::SNMP. Наиболее быстрый способ его установки — использование команды CPAN в системе, подключенной к Интернету. Для этого нужно выполнить:

```
perl -MCPAN -e shell
```

В появившемся окне ввести команду

```
install Net::SNMP
```

При запуске CPAN могут появиться запросы по первоначальным настройкам этой утилиты. На них необходимо ответить соответствующим образом. В случае работы через прокси следует выполнить настройки CPAN следующими командами:

```
o conf http_proxy http://user:password@прокси:порт/
o conf ftp_proxy http://user:password@прокси:порт/
o conf commit
```

В случае невозможности подключения системы к Интернету следует воспользоваться рекомендациями с сайта **http://nagios.manubulon.com/faq.html**.

Команды Nagios

Плагины, которые собственно и выполняют проверку систем, создаются в различных языках (bash, Perl и т. п.), имеют отличающиеся ключи для задания параметров запуска и т. д. Чтобы иметь возможность использовать единообразные описания проверок, в Nagios введено понятие команд.

Команда — это плагин, описанный стандартным образом в специальном файле. В этом конфигурационном файле плагину дается название и описываются парамет-

[1] Например, для контроля параметров оборудования Cisco по протоколу SNMP удобно применять модули check_snmp_cisco_stack.pl, check_snmp_cisco_t.pl, check_snmp_env.pl, check_snmp_temperature.pl и др.

ры его запуска. В листинге 11.1 приведен пример описания простейшей команды — проверки достижимости хоста при помощи команды `ping`.

Листинг 11.1

```
define command{
command_name check-host-alive
command_line $USER1$/check_ping -H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$ -p 5
}
```

Это описание создает команду `check-host-alive`, в качестве исполняемого файла используется плагин check_ping из базового комплекта Nagios. Символы, заключенные в знаки доллара, указывают переменные. `$HOSTADDRESS$` традиционно заменяется при вызове на имя тестируемой системы, а `$ARG1$`, `$ARG2$` и т. д. — последовательно на аргументы, указываемые в описании службы.

Ключи `w` и `c` определяют значения, которые будут использованы для формирования статуса предупреждения (`w` от `warning`) или ошибки (`c` от `critical`). Правила задания пороговых значений (в абсолютных или относительных, процентных единицах и т. п.) определяются в плагине (нужно уточнить по справочной информации).

Последний ключ (`-p`) указывает, что команда `ping` должна послать пять проверочных пакетов.

Службы Nagios

Служба является основным элементом в Nagios, который определяет особенности мониторинга: что проверять, как часто запускать команду проверки, кто отвечает за данный сервис (кого предупреждать в случае ошибки), что делать в случае получения сообщения об ошибке (например, выполнить повторно несколько проверок через сокращенные интервалы или сразу же отослать информацию об ошибке администратору), делать ли перерывы в ее использовании (например, не выполнять в определенные дни недели или в заданные периоды суток и т. п.). Совокупность таких настроек в Nagios принято называть *службой* (service), а определяются они специальным блоком описаний.

Типовое определение службы может выглядеть примерно так, как показано в листинге 11.2.

Листинг 11.2

```
define service{
use generic-service
host_name winserver
service_description Memory Usage
check_command check_nt!MEMUSE!-w 80 -c 90
}
```

В этом примере служба с названием `Memory Usage` использует для работы настройки из шаблона `generic-service` для хоста, описанного под именем `winserver`. В качестве команды служба запускает `check_nt` с параметрами командной строки `MEMUSE` и `-w 80 -c 90` (вторые параметры указывают, какое возвращаемое значение используемой памяти нужно считать критическим — 90%, а для какого установить состояние в предупреждение — от 80 до 90%; сами параметры перечисляются через символ `!`).

Мы рекомендуем особенно тщательно изучить возможности определений службы, поскольку они задают качество мониторинга. Полный набор допустимых опций в описаниях службы нужно уточнить по онлайновой документации.

Обратите внимание, что Nagios может характеризовать службы (и хосты) следующими состояниями:

- Unknown (u) — неизвестное (например, если команда проверки еще не выполнялась или же выполнилась с ошибкой);
- Critical (c) — критическое. Порог критического состояния должен быть определен в параметрах команды проверки;
- Warning (w) — состояние предупреждения. Аналогично, задается параметрами в команде проверки;
- Recovered (r) — восстановленное. Это состояние возникает после восстановления из критического;
- Flapping (f) — состояние мерцания. В это состояние служба или хост переводятся в том случае, когда их состояние периодически меняется из нормального на ошибочное.

(Для хостов состояния могут быть Unreachable (u), Down (d), Recovered (r), Flapping (f).)

> ***Примечание***
>
> Вы можете настраивать, например, оповещения в зависимости от состояния контролируемого объекта.

Также следует обратить внимание на возможность эскалации. Если оператор в течение заданного срока (определяется в настройках службы) не устранил неисправность, то сервер переключится на оповещение следующего администратора, заданного в параметрах эскалации.

Шаблоны Nagios

В приведенном ранее примере в описании службы присутствовала опция использования шаблона `generic-service`. Шаблоны в Nagios представляют собой набор параметров, которые можно импортировать в описания конкретных объектов, например, в описание службы, описание временного параметра, контролируемого объекта и т. д.

Посмотрите пример шаблона для описания Windows-систем (листинг 11.3).

Листинг 11.3

```
define host{
name windows-server   ; название шаблона
use generic-host      ; данный шаблон сам включает
                      ; в себя настройки из этого шаблона
check_period 24x7     ; по умолчанию система контролируется круглосуточно
check_interval 5      ; команда контроля запускается каждые 5 минут
retry_interval 1      ; повтор осуществляется через минуту
                      ; (если система не ответила)
max_check_attempts 10 ; максимальное число попыток 10
check_command check-host-alive ; здесь указана команда контроля
notification_period 24x7       ; определен период, когда отсылаются
                               ; оповещения — круглосуточно
notification_interval 30 ; определен период для повторной
    ; отправки предупреждений (оповещения будут отправляться непрерывно,
    ; пока система не перейдет в нормальное состояние)
notification_options d,r   ; здесь указаны состояния системы,
                           ; для которых высылаются предупреждения
contact_groups admins      ; здесь определяются операторы,
                           ; которым будет высылаться оповещение
hostgroups windows-servers ; эта строка определяет группы,
                           ; в которые будет входить система
register 0                 ; в данном случае 0, поскольку
                           ; регистрировать не нужно — это шаблон
}
```

Примечание

Шаблоны отличаются от описаний собственно объекта только строкой `register 0`, которая говорит, что это описание не нужно регистрировать в качестве объекта.

После того как шаблон описан, на него можно ссылать при описании самого объекта (`use <имя шаблона>`). После этого все параметры, описанные в шаблоне, можно не описывать повторно в описании объекта (если же сделать это (т. е. повторно описать), описание объекта будет перекрывать описание шаблона).

Таким способом можно экономить на описаниях конкретных объектов.

Примечание

Обратите внимание, что в шаблонах допускаются вложения других шаблонов: какую-то часть параметров можно выделить в отдельный шаблон и повторить его в других описаниях.

Хосты как контролируемые объекты

Любой контролируемый объект в Nagios — компьютер, принтер, коммутатор и т. д. — называется *хостом*. Он должен быть описан специальными инструкциями. Минимально описание хоста может выглядеть так, как показано в листинге 11.4.

Листинг 11.4

```
define host{
host_name myHost        ; имя системы
alias My Best Host      ; полное имя системы
                        ; (можно использовать пробелы и т. п.)
address 192.168.1.254   ; IP-адрес системы
}
```

В описании хоста можно использовать различные опции (подробности нужно уточнить по справочной документации). Например, можно включить параметры, которые будут определять действия, выполняемые при сбоях в работе системы:

```
event_handler server-reboot
check_command check-host-alive
```

В этом случае сервер будет проверять доступность хоста командой `check-host-alive` и, после смены состояния хоста (в недоступное), начнется выполнение программы `server-reboot`. Таким способом можно, например, запускать остановившиеся службы на контролируемых серверах, перезагружать системы и т. п.

> ***Примечание***
>
> Мониторинг событиий позволяет более оперативно восстановить работу систем. Если Nagios не получил ответа о нормальной работе системы, он через период, заданный параметром `retry_interval`, будет повторять контроль до достижения лимита, также определенного настройками (`max_check_attempts`). Событие же обрабатывается сразу после получения первой информации о "ненормальном" состоянии хоста.

Группы в Nagios

Для удобства анализа хосты можно объединять в группы. Для этого необходимо описать группу (листинг 11.5).

Листинг 11.5

```
define hostgroup{
  hostgroup_name  имя_группы
  alias           полное_имя_группы    ; допускаются пробелы и т. д.
}
```

Членство в группе можно определять как в самом описании группы (параметр `hostgroup_members`), перечисляя членов группы через запятую, так и в описании хоста (параметр `hostgroups`).

Использование групп удобно тем, что вы можете настраивать мониторинг не на единичный объект, а сразу на всю группу одним описанием: достаточно вместо опции имени хоста указать опцию имени группы. Кроме того, группы позволяют контролировать систему с большим количеством объектов более удобным способом: например, можно создать группу серверов, выполняющих определенную задачу, и наблюдать за их общим состоянием.

Примечание

Другой способ экономии на описании — возможность перечислять несколько названий хостов в определении службы (через запятую).

Зависимости служб и хостов

В Nagios существует возможность устанавливать отношения зависимости между хостами и службами (dependencies). Делается это для того, чтобы скрыть "лишние" предупреждения. Например, если часть систем находится в локальной сети после маршрутизатора, то в случае его отказа все эти устройства окажутся недоступными. Понятно, что сообщения об их недоступности в таком случае излишни: нужно сначала ликвидировать неисправность маршрутизатора. Настройка зависимости позволяет скрыть предупреждения о недоступности зависимых устройств и не выполнять на них проверку соответствующих служб.

Для того чтобы описать для данного хоста *родительский* (т. е. тот хост, от которого он зависит), необходимо указать имя этого хоста в параметре `parents` (листинг 11.6).

Листинг 11.6

```
define host{
host_name       имя
display_name    отображаемое_имя
address         адрес
parents         имя_родительской_системы
hostgroups      имя_группы
check_command   имя_команды
...
}
```

Настройка зависимостей для служб выполняется аналогичным образом.

Примечание

Параметры зависимостей используются в Nagios для автоматического построения карты контролируемой структуры.

Диапазоны времени

Временные параметры используются в различных конфигурациях: в описаниях хостов (периоды, когда нужно осуществлять мониторинг и отправлять сообщения), служб и контактов (периоды, когда можно отправлять сообщения по хостам и по службам). Синтаксис определения нового периода легко понять из примеров, включенных в файл /usr/local/nagios/etc/objects/timeperiods.cfg.

В описании необходимо перечислить построчно диапазоны времени, которые в него включаются. Причем допустимы названия дней недели, месяцев и порядковые номера (последний/первый понедельник месяца). Периоды времени можно перечислять через запятую. При необходимости из одного шаблона можно исключать

периоды, описанные в другом шаблоне, если указать директиву `exclude` с последующим перечислением периодов времени (через запятую). В листинге 11.7 приведены примеры описания временных диапазонов.

Листинг 11.7

```
monday 09:00-12:00,13:00-18:00
tuesday 00:00-24:00
2009-05-01/7 00:00-24:00   ; Каждый седьмой день, начиная
                           ; с 1 мая 2009 года
day 1-15 00:00-24:00       ; с 1 по 15 число каждого месяца
day 1-15/3 00:00-24:00     ; Каждый третий день
                           ; с 1 по 15 число каждого месяца
february 1 00:00-24:00     ; Каждый последний день февраля
```

Операторы

В системе мониторинга может быть определено любое число операторов. Оператору будут отсылаться предупреждения о состоянии служб (хостов). Операторам можно назначить периоды времени, в течение которых они будут доступны, что позволит точно настроить систему оповещения.

Операторы также могут объединяться в группы для удобства настройки оповещений.

Файлы конфигураций в Nagios

Все упомянутые ранее объекты должны быть описаны в файлах конфигурации. Описание представляет собой обычный текстовый блок, составленный в соответствии с синтаксисом, который можно уточнить по документации Nagios. Кроме того, обычно в качестве образца можно использовать конфигурации, устанавливаемые по умолчанию. Достаточно только откорректировать их по требованиям конкретной системы.

После установки в системе присутствует несколько файлов конфигурации Nagios (табл. 11.2).

Таблица 11.2. *Начальный список конфигурационных файлов Nagios*

Имя файла	Назначение
nagios.cfg	Файл основных настроек конфигурации. Содержит ссылки на файлы конфигурации, импортируемые при старте системы
resource.cfg	Файл описания ресурсов. Содержит синонимы для скрытия путей фактического расположения команд Nagios от конечного пользователя для повышения безопасности
cgi.cfg	Параметры настроек веб-сервера. В этом файле описываются дополнительные пользователи Nagios и предоставленные им права доступа
Папки objects и др.	Папки с отдельными файлами, которые импортируются в конфигурацию при старте Nagios. Эти папки описаны в файле nagios.cfg

Основной файл конфигурации — nagios.cfg. Если открыть его в текстовом редакторе, то в начале файла вы увидите ссылки на другие файлы, которые импортируются при старте программы. Можно ссылаться как на отдельные файлы (cfg_file), так и на папки (cfg_dir), все файлы из которых с расширением cfg будут загружены при старте.

Описания хостов, служб, команд, шаблонов и т. д. могут включаться в любые файлы конфигураций в любом сочетании. Чтобы не запутаться, желательно выработать систему создания описаний, например, все описания операторов можно хранить в одном файле, а описания служб, хостов, соответствующих команд — размещать в папках по типам контролируемого оборудования. Вы можете выбрать любой вариант описания, в любом сочетании — явно указывать на файлы, создать свои автозагружаемые папки и т. п.

Если в каком-либо файле конфигурации допущена ошибка, то служба Nagios не сможет загрузиться. При большом количестве конфигураций найти ошибку не всегда просто. В этом случае нужно выполнить проверку конфигурации следующей командой:

```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

Она покажет ошибку и сообщит имя файла, в котором она допущена.

Мониторинг серверов Windows

Для мониторинга систем на основе Windows разработано несколько различных агентов. Наиболее распространенные из них: NSClient++, NC_NET (**http://sourceforge.net/projects/nc-net**) и OpMonAgent (**http://www.opmon.org/project/opmonagent.zip**). Функционал данных агентов практически идентичен, поэтому мы рассмотрим агента NSClient++, который, на взгляд автора, наиболее популярен.

NSClient++

Агент NSClient++ доступен со страницы **http://trac.nakednuns.org/nscp/**. Эту программу можно загрузить как в виде архива (zip), так и установочным файлом (msi), причем для 32- и 64-битовых платформ предусмотрены различные версии агента. Агент устанавливается в качестве службы Windows.

Перед запуском службы следует *обязательно* настроить параметры ее работы. Для этого откройте файл nsc.ini (в папке установки агента) и снимите комментарий с тех строк, которые соответствуют модулям программы, предполагаемым к использованию для мониторинга системы. Достаточно подробные описания параметров конфигурации приведены в документации плагина на странице **http://trac.nakednuns.org/nscp/wiki/doc/Configuration**.

При настройке конфигурации нужно исходить из принципа, что не следует включать больше опций, чем это необходимо в текущий момент. Например, если вы не планируете получать информацию посредством WMI-запросов, то и не стоит загружать модуль CheckWMI.dll.

Администраторам, не имевшим опыта работы с Nagios, обычно не удается правильно построить строку параметров запроса состояния Windows-системы. Поэтому обратите внимание на возможность запуска агента в диагностическом режиме. При этом вы сможете увидеть потенциальные ошибки в конфигурационном файле и отладить собственные запросы (рис. 11.4).

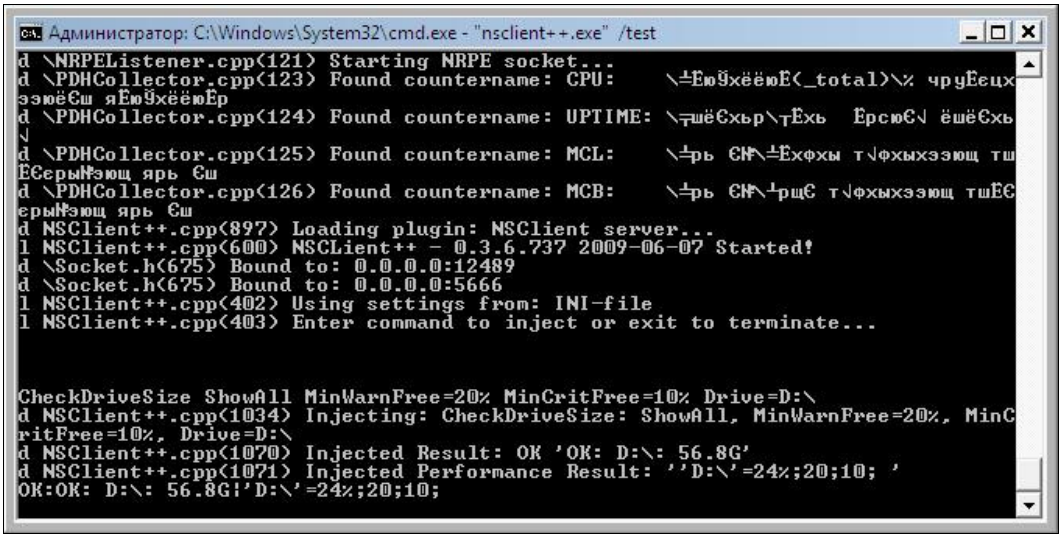


Рис. 11.4. Окно программы NSClient++ в диагностическом режиме

В диагностическом режиме в окне программы отражаются результаты выполнения операций контроля. Здесь вы можете увидеть и проанализировать причины ошибок. Кроме того, в этом окне можно осуществить разовый ручной запуск команды контроля.

Для запуска NSClient++ в диагностическом режиме достаточно выполнить в командной строке

```
NSClient++ /test
```

В окне NSClient++ вы сможете, во-первых, увидеть результаты загрузки всех модулей, а во-вторых, вводить собственные команды и видеть результаты выполнения как запросов со стороны сервера Nagios, так и локальных команд. На рис. 11.4 показано окно отладки плагина, в котором введена команда `CheckDriveSize ShowAll MinWarnFree=20% MinCritFree=10% Drive=D:\` и виден ответ системы.

Плагин NSClient++ позволяет:

- ❒ выполнять встроенные проверки. Перечень проверяемых параметров перечислен в табл. 11.3;
- ❒ запускать сценарии проверки, составленные на различных языках программирования;
- ❒ анализировать журналы системы.

Таблица 11.3. *Параметры, контролируемые NSClient++*

Параметр	Описание
`CheckFileSize`	Контролирует размер файла или папки
`CheckDriveSize`	Контролирует размер свободного или использованного пространства жестких или сменных дисков (тип диска можно выбирать в команде)
`CheckFile`	Контролирует файлы по критериям даты их создания, времени последнего доступа, записи в файл или по размеру файла
`CheckEventLog`	Ищет сообщения об ошибках в файле журнала. Для использования необходимо правильно составить фильтры отбора сообщений
`CheckCPU`	Контролирует загрузку процессора в течение задаваемого периода времени
`CheckUpTime`	Контролирует время работы системы
`CheckServiceState`	Контролирует состояние службы Windows (критическое сообщение формируется в случае несоответствия фактического состояния службы заданному в качестве параметра в команде). Можно контролировать все службы одновременно с заданием исключения. В качестве названия службы нужно указывать то, которое отображается в свойствах службы
`CheckProcState`	Контролирует состояние процессов Windows. Фактически позволяет наблюдать за состоянием процесса, найденного по имени исполняемого файла. Можно контролировать также по числу одновременно запущенных процессов
`CheckMem`	Контролирует состояние виртуальной и физической памяти; доступен параметр количества записанных страниц памяти (commited pages)
`CheckCounter`	Контролирует значения счетчиков производительности. Объекты счетчиков желательно (для удобства использования) задавать в описаниях команд (служб)

`CheckAlwaysOK`
`CheckAlwaysCRITICAL`
`CheckAlwaysWARNING`
`CheckMultiple`
`CheckOK`
`CheckCRITICAL`
`CheckWARNING`
`CheckVersion`
	Так называемые *хэлперы*. Возвращают заранее определенное значение (какое — можно судить по названию команды). Применяются при настройке и отладке системы

Подробности использования команд описаны в технической документации (**http://trac.nakednuns.org/nscp/wiki/CheckCommands**), и по имеющимся примерам легко составить собственные команды контроля состояния Windows.

Стили команд: протоколы NSClient и NPRE

Агент NSClient++ позволяет использовать для контроля системы два протокола: собственный — NSClient и NRPE, традиционно применяемый для Linux-систем. Возможности этих вариантов идентичны, отличается только синтаксис используемых команд. Хотя на взгляд автора, протокол NRPE более гибок в использовании и обеспечивает при работе шифрование данных обмена.

Включаются и выключаются протоколы наличием комментария для соответствующего модуля в файле настроек клиента (nsc.ini). Включать оба протокола обычно не имеет смысла.

Как уже говорилось, синтаксис команд несколько отличается. При использовании NRPE команда строится следующим образом:

```
check_nrpe ... -c <команда> -a <аргументы>
```

Например, проверить доступную физическую память можно так:

```
check_nrpe -H 192.168.0.9 -c CheckMem -a MaxWarn=70% MaxCrit=80% type=physical
```

При работе по протоколу NSClient потребуется другой синтаксис:

```
check_nt ... -v <значение> -w <значение> -c <значение> -l <значение>
```

Проверку памяти, аналогичную описанной, можно было бы осуществить так:

```
check_nt -H 192.168.0.9 -p 12489 -v MEMUSE -w 70 -c 80
```

Обратите внимание, что здесь указана не команда `CheckMem`, которая описана в документации на команды NSClient, а переменная `MEMUSE` (после ключа `-v`). Чтобы узнать, какие переменные можно и нужно указывать в командной строке `check_nt` для контроля соответствующих параметров Windows-системы, необходимо ознакомиться с внутренней справкой команды, доступной при вызове команды с ключом `-h`:

```
check_nt -h
```

> ***Примечание***
>
> Если в параметрах команд проверки необходимо указывать не точные значения порога, а, например, сравнение "больше или равно", то для этого придется разрешить в конфигурации клиента так называемые nasty_meta_chars (для символа < или >). Этот вариант не рекомендуется, предпочтительнее следующие сочетания: `gt` вместо >; `lt` вместо <; `ne` вместо `!=` (или <>).

Контроль счетчиков Windows

Агент NSClient++ позволяет возвращать значения счетчиков Windows. Для этого в параметре команды нужно указать название счетчика. К сожалению, в локализованных версиях Windows названия счетчиков также переведены, причем использовать индекс для выбора нужного счетчика практически нереально (поскольку индексы счетчиков различны для разных систем).

Версия агента не имеет локализации на русский язык. Поэтому необходимо загрузить в файл counters.cfg добавить блок для русского языка (содержимое —

см. **http://www.opennet.ru/opennews/art.shtml?num=17082**), сам файл поместить в папку клиента (этот файл содержит названия основных счетчиков в русской кодовой странице). Кроме того, в командах необходимо указывать точное название счетчика на русском языке. Чтобы его получить, нужно использовать, например, задачу Системный монитор.

Если сервер Nagios развернут на Linux-системе, то в файле описаний команд названия счетчиков должны быть указаны в кодовой странице Windows-1251. Проще всего это реализовать, если редактировать файлы конфигурации в Windows, а потом копировать их на Linux-систему.

У автора возникли сложности при получении параметров счетчиков в русской версии Windows 7. Поэтому в своей работе получение значений счетчиков было настроено с использованием сценария PowerShell. Например, если нужно получить счетчики сетевого интерфейса[1], то можно использовать такой сценарий:

```
Write-Host ("NetIf: OK | 'NetInt'="+([System.Math]::Round((Get-counter -counter
"\Сетевой интерфейс(Realtek PCIe GBE Family Controller)\Всего байт/с" | Select
-expand CounterSamples).CookedValue,0))+"B;")
```

Для запуска сценария на PowerShell в INI-файле агента в разделе `[Script Wrappings]` нужно указать такую строку:

```
ps1=cmd /c echo scripts\%SCRIPT% %ARGS%; exit($lastexitcode) | powershell.exe -
command -
```

Другой способ получить значения счетчиков производительности — воспользоваться командой `typeperf`. Эта команда позволяет отобразить все доступные счетчики (локального или удаленного компьютера). Ее также можно использовать для получения данных о производительности.

Вывод этой команды можно впоследствии передать серверу Nagios. Например, следующая команда выведет на экран значение счетчика сетевого интерфейса:

```
FOR /F "usebackq skip=2 tokens=2 delims=," %I IN (`typeperf "\Сетевой
интерфейс(Realtek PCIe GBE Family Controller)\Всего байт/с" -sc 1`)
DO @echo %~I
```

Мониторинг журналов событий Windows

Существуют две стратегии отбора событий журналов Windows в агенте. Первая предполагает отбор *всех* событий, кроме явно указанных. Это фильтр `out`. При второй стратегии необходимо указывать критерии, по которым будут отбираться желаемые сообщения (фильтр `in`). В обоих случаях необходимо также указывать параметр `filter=new` (это сделано для совместимости с предыдущими версиями).

> ***Примечание***
>
> Один и тот же результат отбора можно получить с помощью как первой, так и второй стратегии. В каждом случае оптимальный вариант нужно выбирать самому администратору.

[1] В сценарии указан конкретный сетевой интерфейс, кроме того, использовано предпочитаемое оформление (округление и добавление единиц изменения в конец вывода). Естественно, что сценарий должен быть модифицирован по конкретным потребностям.

Первая стратегия удобна, если контролируется, например, просто наличие записей о критических событиях в журнале системы. Вторая — если требуется отобрать записи, связанные с конкретным оборудованием или программной службой. Особо следует обратить внимание, что при второй стратегии программа ищет *первую удовлетворяющую условиям поиска запись.* Поэтому крайне важен порядок записи фильтров. Кроме того, обычно для ускорения работы агента рекомендуется сначала записывать те условия, которые *максимально сузят* зону поиска.

Структура фильтра приведена на рис. 11.5. Фильтр начинается всегда с ключевого слова `filter`, потом записывается режим фильтра (`filter mode`), потом — тип фильтра. Далее следует знак "равно", а только после него — оператор. Поэтому в случае, если фильтр задает точное совпадение (=), то в его записи необходимо указать *два* знака равно. Завершают строку фильтра оператор и значение, с которым происходит сравнение.

При определении команды обычно придерживаются такой последовательности: указывают анализируемые журналы (параметр `file`), тип фильтра (два параметра: первый `out` или `in`, второй — `new`), указывают границы для формирования предупреждений, записывают правила фильтрации и определяют дополнительную информацию, которая будет возвращена командой (время генерации, текст сообщений и т. д. — см. справочную документацию).

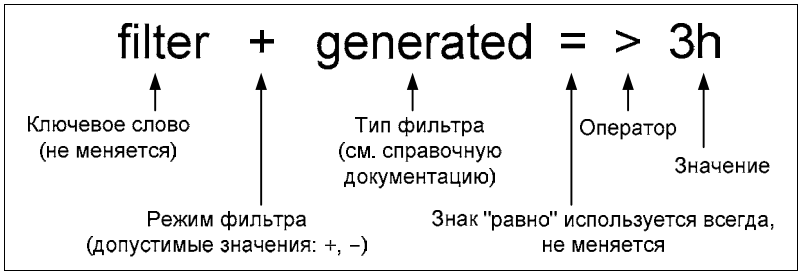


Рис. 11.5. Структура фильтра в Nagios

Основная проблема в реализации контроля журналов событий состоит в некорректном отображении текстов событий при работе с русскоязычными системами. Практически вы ограничены необходимостью работы только с источниками событий, датами, кодами возврата и т. п.

Подробно описание допустимых типов фильтров, опций и т. п. приведено на странице **http://trac.nakednuns.org/nscp/wiki/CheckEventLog/CheckEventLog**.

Использование WMI для мониторинга Windows-систем

В состав NSClient++ входит модуль CheckWMI.dll, позволяющий контролировать Windows-систему с помощью инструментария WMI.

Модуль CheckWMI потребуется в тех случаях, когда предполагается либо анализ строкового параметра, возвращаемого в результате WMI-запроса, либо запрос нескольких значений. При использовании CheckWMI строки запроса несколько

усложняются из-за необходимости применения фильтров. Синтаксис CheckWMI описан на странице **http://nsclient.org/nscp/wiki/CheckWMI/CheckWMI**. По своему построению запросы CheckWMI сходны с фильтрами анализа журналов работы системы, которые описаны ранее.

Модуль CheckWMI фактически состоит из двух подмодулей: CheckWMIValue и CheckWMI. CheckWMIValue оптимизирован для контроля численных значений, например, текущей загруженности процессора (это процент загрузки) или разрешения монитора (количество пикселов) и т. п. В этой команде вы можете просто указать контролируемые параметры и минимальные/максимальные допустимые для них значения, например, так:

```
CheckWMIValue "Query=Select PelsWidth from win32_DisplayConfiguration"
MinCrit=640 MinWarn=800 Check:Width=PelsWidth
```

Приведенная команда составлена для работы в режиме отладки (`nsclient++ /test`). Она запрашивает разрешение дисплея по горизонтали и сообщает о критическом состоянии в случае, если оно равно или менее 640, и выдает предупреждение, если значение не превосходит 800. Из особенностей применения этой команды отметим, что после строки запроса (которая заключена в кавычки) нужно писать параметры минимальных/максимальных значений и только потом указывать название параметра, который контролируется командой (`PelsWidth`). Поясним также опцию `Check`, указанную в командной строке. После `Check` необходимо вписать название параметра, которое будет применяться в системе контроля (можно сохранить и название из описания в WMI, но часто более удобно ввести собственное название), и название, соответствующее объекту класса (то, которое отображается, например, в утилите просмотра WMI Object Browser).

Другие примеры (в том числе в вариантах для конфигурации Nagios) приведены на странице **http://trac.nakednuns.org/nscp/wiki/CheckWMIValue**.

Мониторинг серверов Linux

Работу серверов Linux контролируют с помощью пакета NRPE, причем на сервере Nagios он должен быть установлен как плагин, а на контролируемой системе Linux — в качестве демона. Для установки пригодна как подготовленная версия, так и исходные коды плагина.

Установка плагина NRPE из исходных кодов

Для установки NRPE необходимо скачать его последнюю версию с сайта **http://www.nagios.org/download/addons/**. На момент написания книги последней стабильной версией была NRPE 2.12, процесс установки которой мы и опишем далее.

Поскольку обмен данными с контролируемой системой осуществляется по защищенному каналу, то на сервер с Nagios необходимо предварительно установить OpenSSL. Делается это следующими двумя командами:

```
apt-get install openssl
apt-get install libcurl4-openssl-dev
```

Загруженный с сайта пакет NRPE необходимо распаковать и установить (листинг 11.8; такая установка выполняется на сервере Nagios).

Листинг 11.8

```
tar xzfp nrpe-2.12.tar.gz
cd nrpe-2.12/
./configure
make all
make install-plugin
```

Обратите внимание, чтобы по итогам выполнения команд конфигурирования и установки не было сообщений об ошибках.

Демон NRPE устанавливается аналогично (на всех контролируемых системах), только вместо последней операции (`make install-plugin`) необходимо выполнить (вторая команда позволяет установить демо-конфигурацию, которую можно будет отредактировать для упрощения настройки):

```
make install-daemon
make install-daemon -config
```

Установка плагина NRPE из репозитория

Установка выполняется командой

```
apt-get install nagios-nrpe-plugin
```

Данная команда установит плагин в папку /usr/lib/nagios/plugins/. Именно этот путь и нужно будет указывать в конфигурации для командной строки. Обратите внимание, что синтаксис NRPE несколько отличается от описаний команд в Nagios. Команды необходимо определять в конфигурации по следующему образцу:

```
command[check_users]=<команда>
```

Установка демона NRPE из репозитория

Установка сервера NRPE программой `apt-get` выполняется следующим образом:

```
apt-get install nagios-nrpe-server
```

Успешность установки демона можно проверить командой

```
netstat -an | grep 5666
```

Если NRPE работает, то порт 5666 должен им прослушиваться, о чем вы получите примерно такую информацию:

```
tcp 0 0 0.0.0.0:5666 0.0.0.0:* LISTEN
```

После установки пакета необходимо отредактировать файл настроек. По умолчанию в данном случае настройки хранятся в папке /etc/nagios. В ней находятся два файла: nrpe.cfg и nrpe_local.cfg. Первый файл лучше использовать только для

смены глобальных параметров, а все локальные настройки меняйте в файле nrpe_local.cfg.

Обязательно смените адрес системы, с которой можно контролировать данный хост. Это параметр `allowed_hosts` в файле nrpe.cfg. По умолчанию разрешена только локальная работа (указан адрес 127.0.0.1).

После завершения настроек конфигурации следует перезагрузить демон командой

```
/etc/init.d/nagios-nrpe-server reload
```

Использование прокси-NRPE

Используя NRPE, можно на контролируемом хосте вызвать команду `check_nrpe` для проверки другого хоста. Таким способом можно контролировать некоторую подсеть через один компьютер.

Для этого на хосте, функционирующем в качестве прокси, нужно установить как сервер NRPE, так и плагин.

Мониторинг с использованием протокола SNMP

Nagios позволяет осуществлять контроль систем посредством протокола SNMP. SNMP (Simple Network Management Protocol) — исторически первый протокол управления сетью. Устройства, которые допускают управление по протоколу SNMP, могут принимать из сети команды, выполнять их и передавать информацию о параметрах своей работы. Например, после получения сообщения о пропадании электроэнергии от управляемых аварийных источников питания по протоколу SNMP можно запросить данные об уровне зарядки аккумуляторных батарей и отложить отключение компьютеров до момента практически полной разрядки.

> ***Примечание***
>
> Существуют различные версии протокола SNMP (в настоящее время — первая, вторая и третья). Многие устройства, уже давно эксплуатируемые в сети, предполагают возможность управления только по версии 1.0. Данная версия не предусматривает никакой защиты, имена устройств передаются по сети в открытом виде, что легко позволяет перехватить их снифферами. Поэтому обращайте внимание на то, что имена (*community* в терминологии SNMP) ни в коем случае не должны оставаться в значениях по умолчанию, их следует хотя бы заменить на достаточно длинные и сложные названия. А интерфейсы управления такими устройствами желательно выделить в отдельную виртуальную сеть. Третья версия протокола уже предполагает как аутентификацию при подаче команды, так и шифрование трафика протокола SNMP.

SNMP в первую очередь применяется для управления активным сетевым оборудованием: маршрутизаторами и коммутаторами, аварийными источниками питания, модемами и т. п. Хотя протокол SNMP можно использовать и для контроля компьютеров, если в системе установлена соответствующая служба. Со списком субагентов, доступных для использования в операционных системах Windows, можно ознакомиться, например, на странице **http://support.microsoft.com/kb/237295/ru**.

Все SNMP-совместимые устройства имеют стандартизованную конфигурацию параметров. Эта конфигурация представляет собой некое дерево идентификаторов:

для доступа к какому-либо значению необходимо указать полный путь к нему от самого корня. Например, чтобы получить состояние порта коммутатора, нужно запросить значение для идентификатора .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus.101. Причем обычно разрешено опускать первую часть символов, одинаковых для контролируемых параметров (.iso.org.dod.internet.mgmt.mib-2.). Иными словами, при запросе административного состояния порта коммутатора было бы достаточно только указать interfaces.ifTable.ifEntry.ifOperStatus.101. Существует много ресурсов, на которых можно просмотреть дерево идентификаторов и найти нужный идентификатор, например, OID-repository на сайте **http://www.oid-info.com/**.

> ***Примечание***
>
> Эти идентификаторы называются OID. Структура идентификаторов описывается в специальных файлах, которые называются MIB-файлами. Основная часть структуры стандартизована, но отдельные параметры описаны в проприетарных MIB-файлах (доступны к загрузке с сайтов разработчика оборудования). Интересующиеся читатели могут посетить страницу **http://www.mibdepot.com/index.shtml**, на которой собрано множество MIB, как стандартных, так и разработки отдельных вендоров.

В запросах Nagios допустимы не только символьные, но и численные наименования идентификаторов. Так, указанному ранее параметру соответствует индекс .1.3.6.1.2.1.2.2.1.8.101. Причем именно цифровые идентификаторы рекомендуется применять для повышения производительности системы контроля.

> ***Примечание***
>
> При использовании параметров, специфичных для данного вендора, необходимо загрузить соответствующий MIB-файл (параметр `-m` команды `check_snmp`).

Для работы с SNMP в Nagios должен быть установлен соответствующий плагин. Он включен в состав установки типовых плагинов, но фактически добавляется в систему только в том случае, если предварительно был установлен пакет Net-SNMP. Поэтому если предполагается применение SNMP-модуля, то сначала необходимо установить Net-SNMP с сервера **http://net-snmp.sourceforge.net/** и только после этого устанавливать стандартные плагины.

На сайте **http://net-snmp.sourceforge.net/** необходимый пакет представлен только в исходных кодах или в формате RPM. Если вы не хотите устанавливать пакет из исходных кодов, то можете переконвертировать его с помощью программы alien: `alien -d net-snmp-<`*версия*`>.rmp -scripts`.

После настройки возможности контроля по протоколу SNMP необходимо протестировать работоспособность на простейших запросах, например, проверить длительность работы устройства:

```
/usr/local/nagios/libexec/check_snmp -H <адрес_устройства>
-C <community> -o sysUpTime.0
```

В ответ вы должны получить примерно такое сообщение:

```
SNMP OK — Timeticks: (622339555) 72 days, 0:43:15.55 |
```

Внимание!

В составе пакета Net-SNMP имеются различные утилиты, которые позволяют получить с устройства данные по протоколу SNMP. Например, утилита `snmpwalk` выводит список всех параметров, начиная от указанного OID (или начиная с корня), а утилита `snmpget` возвращает значение указанного параметра по его OID и т. д.

Команда `check_snmp` может запрашивать параметр, принимающий численное значение, и проверять соответствие его значения некоторому диапазону. Так, можно указать значения для состояния предупреждения и критического (ключи `-w` и `-c`) или диапазон значений (через двоеточие).

Внимание!

Обратите внимание, что если вы хотите, чтобы, например, критическим значением интерпретировалось бы возвращаемое число в диапазоне от *a* до *b* (*b* > *a*), то диапазон нужно указывать *b*:*a*. Если указать диапазон в "привычном" виде, как *a*:*b*, то если возвращаемое значение попадает в этот диапазон, результат будет считаться нормальным состоянием, а если не попадает — то как предупреждение или критическое состояние (в зависимости от указанного ключа).

Кроме того, команда может проверять возвращаемое строковое значение (значение, с которым проверяется ответ, следует указать в ключе `-s`) или даже выполнять проверку с использованием регулярных выражений (ключи `-r`, `-R`). Также в запросе можно проверять сразу несколько параметров, перечисляя их OID через запятую, например, так:

```
//usr/local/nagios/libexec/check_snmp -H <адрес> -C <community> -o
.1.3.6.1.2.1.2.2.1.7.101,.1.3.6.1.2.1.2.2.1.7.102,.1.3.6.1.2.1.2.2.1.7.103
SNMP OK — 1 1 1 | iso.3.6.1.2.1.2.2.1.7.101=1 iso.3.6.1.2.1.2.2.1.7.102=
1 iso.3.6.1.2.1.2.2.1.7.103=1
```

`Check_snmp` снабжена подробной справкой (`check_snmp -h`), которая пригодится при составлении запросов к устройству. После того как запрос будет составлен и отлажен, достаточно описать новую команду в файле commands.cfg и добавить нужные службы в файлы описания контролируемых устройств.

Плагины, использующие SNMP-протокол

Плагин `check_snmp` проверяет значение одного параметра. Конечно, можно проверять каждый параметр по отдельности, но в Сети представлено большое количество плагинов, которые осуществляют проверку всего устройства и выдают комплексную оценку.

Например, устройство может содержать несколько вентиляторов, несколько датчиков температуры и т. п. Плагин получает по протоколу SNMP количество соответствующих датчиков, опрашивает всех их и выдает предупреждение, если хотя бы один датчик сообщает параметры вне допустимых пределов.

Так, по адресу **http://wiki.nagios.org/index.php/Howtos:snmp-apc-smart-ups** содержится описание настроек, с помощью которых можно контролировать состояние источников бесперебойного питания от APC (состояние батареи, параметры напряжения, температуру и т. д.).

А по ссылке **http://nagios.manubulon.com/check_snmp_int.pl** можно скачать плагин Snmp interface check, который может проверить сразу несколько интерфейсов коммутатора, сообщить об их состоянии (включен/выключен), об используемой полосе пропускания и количестве ошибок на каждом интерфейсе.

Поэтому перед выполнением индивидуальных настроек обязательно следует провести поиск готовых решений для устройств, применяемых в вашей организации.

Обработка SNMP-трапов

Описанный выше вариант мониторинга системы на основе SNMP-протокола представляет собой случай *активного* контроля: сервер запрашивает состояние устройства. Однако SNMP-управляемые устройства могут быть настроены на самостоятельную отправку сообщений в случае возникновения определенных ситуаций. Такие сообщения принято называть *трапами*.

Для того чтобы устройство отправляло такие сообщения, необходимо предварительно выполнить его настройку. Настройка[1] включает обычно указание событий, при возникновении которых нужно отсылать сообщение, адрес, на который оно должно быть отправлено, и некоторую дополнительную служебную информацию (при необходимости).

Трапы существенно дополняют возможности мониторинга. Во-первых, они отсылаются в момент возникновения события, таким образом администратор может быть оповещен о событии сразу же по его возникновении, а не ждать очередного цикла опроса. Во-вторых, трапы формируются и для тех событий, которые весьма затруднительно зафиксировать иным способом. Например, для попытки неудачного входа в систему, для события сохранения новой конфигурации устройства, для отслеживания ошибок протокола маршрутизации и т. п.

Информация трапа включает адрес устройства, время его непрерывной работы, OID события и некоторую дополнительную информацию (например, индекс интерфейса, который вызвал событие, его состояние и т. п.). Обработка таких сообщений представляет собой нетривиальную задачу, прежде всего потому, что многие события являются уникальными для конкретного оборудования. Иными словами, для каждого оборудования придется выполнять настройку обработки трапов.

Классический способ обработки трапов в Nagios заключается в использовании утилиты `snmptrap`, в настройки которой (snmptrapd.conf) включаются строки реагирования на трапы по следующему образцу:

```
traphandle OID Eventhandler/Programm
```

Этот способ является весьма трудоемким, поскольку такие команды надо формировать для каждого типа трапа. Упростить обработку трапов поможет использование утилиты `snmptt` (**http://www.snmptt.org**). Она предварительно обрабатывает трап, извлекает из него информацию и передает ее сценарию submit_check_result, кото-

[1] Объем настроек определяется моделью оборудования.

рый и сообщает данные о событии в пакет Nagios, используя вариант пассивного контроля.

Установка утилиты достаточно подробно описана на сайте разработчика. Обратите внимание, что для обработки трапов требуется предварительная установка пакета Net-SNMP. Учтите также, что данная утилита может работать как разово запускаемый сценарий, так и в качестве демона. Последний вариант предпочтителен при обработке трапов, поступающих с большой частотой (например, несколько десятков в секунду и более), но более сложен в настройке.

Опишем вариант настройки утилиты в качестве исполняемого сценария. Для такой установки `smnptt` необходимо выполнить следующие шаги:

1. Скопировать файл snmptt в папку /usr/sbin/, предоставить к нему доступ учетной записи nagios и назначить права исполнения (командой `chmod +x snmptt`).
2. Скопировать файл snmptthandler в папку /usr/sbin/, предоставить к нему доступ учетной записи nagios и назначить права исполнения (командой `chmod +x snmptthandler`).
3. Скопировать файл snmptt.ini в папку /etc/snmp/ и отредактировать его опции.
4. Создать папку /var/log/snmptt/.
5. Добавить в файл /etc/snmp/snmptrapd.conf следующую строку:
   `traphandle default /usr/sbin/snmptt`.
6. Настроить ротацию журналов утилиты, скопировав файл snmptt.logrotate в папку /etc/logrotate.d/ под именем snmptt и откорректировав частоту выполнения операций (и другие опции — при желании).
7. Отредактировать сценарий запуска демона snmptrapd (/etc/rc.d/init.d/snmptrapd), включив в строку `OPTION` символы `-On`.
8. В завершение перестартовать службу snmp.

Другие опции (например, настройку в качестве демона или протоколирование — при желании — в базу данных) следует уточнить по документации на сайте разработчика.

Для обработки сообщений трапа в Nagios нужно создать соответствующие службы. Проще всего выполнить это на основе шаблона следующего образца:

```
define service{
name snmptrap-service
use generic-service
register 0
service_description TRAP
is_volatile 1
check_command check-host-alive
active_checks_enabled 0
max_check_attempts 1
normal_check_interval 1
retry_check_interval 1
```

```
passive_checks_enabled 1
check_period none
notification_interval 31536000
contact_groups somegroup
}
```

Обратите внимание на следующие параметры. При создании службы ее параметр `service_description` должен соответствовать названию, которое указывается в сценарии submit_check_result. Команда `check_command` используется для сброса состояния хоста в нормальное (после проверки), но параметр `active_checks_enabled` исключает активные проверки, а `passive_checks_enabled` — разрешает пассивные. Служба установлена в `volative` (параметр `is_volatile` в значении 1), чтобы предупреждение оператору высылалось уже по получению первого сообщения. Параметр `notification_interval` выбран равным одному году, чтобы исключить возможные получения сообщений от предыдущих трапов. На основе этого шаблона нужно создать описания служб для конкретных систем.

После получения трапа он будет обработан демоном snmptrapd, передан в сценарий submit_check_result, который и сообщит данные в службу **Trap**. При просмотре состояния службы в веб-интерфейсе Nagios в строке **Status Information** будет отображена информация, переданная трапом и обработанная утилитой `snmptt`. Одновременно будут направлены сообщения администратору в соответствии с заданными настройками службы.

Чтобы сбросить состояние службы в исходное состояние (состояние меняется в момент получения трапа), достаточно в веб-интерфейсе Nagios перейти по ссылке **Submit passive Check result** для службы **Trap** и указать для параметра **Check Result** значение **OK** (рис. 11.6).

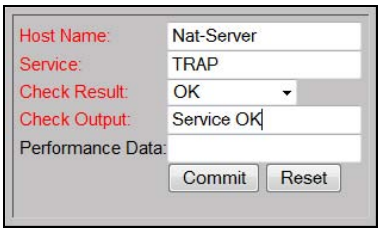


Рис. 11.6. Ручной сброс состояния службы в Nagios

Примечание

Другой вариант сброса — инициировать через веб-интерфейс проверку хоста. В этом случае выполнится команда `check-host-alive`, которая вернет состояние в статус OK.

Главные сложности в настройке `snmptt` заключаются в создании правильной конфигурации, которая должна включать параметры обработки каждого события. Синтаксис конфигурации описан на странице **http://snmptt.sourceforge.net/docs/snmptt.shtml#SNMPTT.CONF-Configuration-file-format**. Простейший пример конфигурации доступен по ссылке **http://projects.debianfr.net/projects/pkg-**

snmptt/browser/trunk/examples/snmptt.conf.generic. Эту конфигурацию можно использовать для настройки и первоначального тестирования обработки трапов.

В файле конфигурации можно включать как описания для конкретных событий, так и для целой группы. В этом случае обработчик, если не найдет точного описания для события, начнет постепенно сокращать цепочку OID до тех пор, пока не найдет совпадения. Если совпадение не будет найдено, то такой трап будет отмечен как неизвестный и сообщение об этом будет помещено в журнал.

> ***Примечание***
>
> В случае проблем обработки трапов можно включить в smnptt.ini режим отладки и уточнить по журналу причины ошибок. Кроме того, можно протестировать обработку на примере образцов трапов из поставки утилиты (`snmptt < sampe-trap`).

Большинство ошибок обработки связано с отсутствием нужных MIB-файлов. Во-первых, в систему нужно загрузить стандартные MIB-файлы. Их можно найти в Интернете (например, на странице **http://www.oidview.com/mibs/0/md-0-1.html**) или же загрузить в Ubuntu путем выполнения команды `apt-get install snmp-mibs-downloader`. Во-вторых, нужно добавить MIB-файлы используемого оборудования, которые нужно найти на сайте изготовителя. Загруженные файлы нужно сохранить в папке /usr/local/share/snmp/mibs (это папка по умолчанию, соответствующий путь можно уточнить командой `net-snmp-config --default-mibdirs`).

Обычно одни MIB-файлы ссылаются на другие (ссылки указаны в начале текста файла), для правильной интерпретации трапа нужно загрузить всю связанную цепочку файлов. Эту операцию приходится выполнять несколькими итерациями, добавляя отсутствующие MIB-файлы. А узнать, что некоторые MIB-файлы отсутствуют, можно, выполнив команды `export MIBS=ALL` и `snmptranslate -Tp`. Первая команда загрузит содержимое всех MIB-файлов, а вторая — отобразит доступную структуру OID и выведет в первых строках информацию об ошибках.

Построение описаний конфигурации существенно облегчает утилита `snmpttconvertmib`. Она обрабатывает MIB-файлы оборудования и добавляет описания трапов в файл конфигурации. В следующем примере в файл конфигурации добавляются события, описанные в файле SNMVv2-MIB (от пакета Net-SNMP; в примере приведены пути размещения файлов по умолчанию):

```
snmpttconvertmib --in=/usr/local/share/snmp/mibs/SNMPv2-MIB.txt --
out=/etc/snmp/snmptt.conf.mib2 --
exec='/usr/local/nagios/libexec/eventhandlers/submit_check_result $r TRAP 1 '
```

В команде в качестве параметров указаны входной и выходной файлы и строка, которая должна быть помещена в качестве имени и параметров исполняемого по данному трапу сценария.

В результате в файле конфигурации будут содержаться примерно такие описания:

```
EVENT warmStart.1.3.6.1.6.3.1.1.5.2 "Status Events" Normal
FORMAT A warmStart trap signifies that the SNMP entity, $*
EXEC /usr/local/nagios/libexec/eventhandlers/submit_check_result $r TRAP 1
"A warmStart trap signifies that the SNMP entity, $*"
```

```
SDESC
A warmStart trap signifies that the SNMP entity,
supporting a notification originator application,
is reinitializing itself such that its configuration
is unaltered.
Variables:
EDESC
```

Обратите внимание, что единичка в строке `EXEC` соответствует событию `WARNING` для Nagios. Если некоторые сообщения (например, включение интерфейса) должны трактоваться как переход в нормальное состояние, то замените 1 на 0. И наоборот, если отдельные события должны соответствовать критическому уровню, тогда смените 1 на 2.

Описания можно редактировать. Можно добавлять собственные команды реагирования (например, операции записи в журнал), изменять статус (вместо критического указать как требующий внимания) и т. п.

Часто приходится включать в конфигурацию обработку различных условий (например, исключить реагирование на события включения сетевых интерфейсов коммутаторов доступа, сохранив оповещения об аналогичных событиях для магистральных каналов и т. п.). Рекомендации по построению подобных правил доступны на указанных выше страницах описания утилиты `snmptt`.

Описания событий удобно иметь в виде отдельных файлов, которые потом импортировать в файл конфигурации, для чего достаточно оформить блок файла snmptt.ini следующим образом:

```
snmptt_conf_files = <<END
/etc/snmp/snmptt.conf
/etc/snmp/snmptt.conf.mib2
END
```

(Третья строка описывает созданный в приведенном выше примере файл.)

Для создания конфигурации проще всего выполнить обработку всех установленных пакетом Net-SNMP MIB-файлов следующим циклом:

```
for i in /usr/local/share/snmp/mibs/*.txt; do
>/usr/local/sbin/snmpttconvertmib -in=$i -out=snmptt.net-snmp.conf
>done
```

и импортировать полученный файл в конфигурацию `snmptt`.

Мониторинг коммутационного оборудования

Активное оборудование сети — коммутаторы, концентраторы, модемы и т. п. контролируются по протоколу SNMP (управляемые модели). Обычно проверяется состояние портов, наличие ошибок, температура устройств, состояние вентиляторов и другие доступные величины.

Однако, кроме указанных параметров, администраторы часто хотят знать фактическое использование полосы пропускания. Эти значения нельзя получить, запрашивая тот или иной параметр состояния оборудования. Их вычисляют на основе анализа периодически получаемых данных.

В Nagios имеются различные способы получения данных об используемой полосе пропускания. Один из них — плагин Snmp interface check мы упоминали ранее. Плагин запрашивает данные от интерфейсов, сохраняет эти значения во временной папке и использует их при очередных запросах для вычисления реально используемой полосы пропускания. Другой — плагин InterfaceTable (**http://www.tontonitch.com/tiki/tiki-index.php?page=Nagios+plugins+-+interfacetable_v3t**). Он не только формирует данные по всем интерфейсам коммутатора, но и подготавливает графики входного и выходного трафика.

> ***Примечание***
>
> Плагин InterfaceTable подготавливает данные для графиков в формат упоминавшейся выше программы PNP4Nagios. Эти настройки должны быть выполнены по соответствующей документации.

Еще одна популярная программа для обработки аналогичных задач — MRTG. Она собирает статистику по протоколу SNMP с активного оборудования, которая при помощи плагина check_mrtgtraf впоследствии передается в Nagios для отображения.

Установить MRTG можно командой `apt-get install mrtg`.

После установки необходимо создать файлы настроек, в которых указать устройства и значения параметров, собираемых программой. Эти настройки записываются в файл /etc/mrtg.conf. Формирование конфигурации MRTG — достаточно сложная задача, поэтому в пакете предусмотрена специальная программа, которая автоматически опросит устройство и сформирует файл конфигурации — `cfgmaker`. При ее запуске в качестве параметров нужно указать строку *`community`* и адрес устройства. Вывод программы следует перенаправить в файл, значения из которого потом мы просто импортируем в файл настроек. В качестве имени такого файла удобно указать имя (или адрес) опрашиваемого устройства:

```
cfgmaker community@адрес > /etc/mrtg/адрес.cfg
```

При формировании конфигурации программа закомментирует блоки, относящиеся к временно отключенным портам. Вы можете потом включить эти блоки, удалив комментарий (символ `#` в начале соответствующих строк).

По итогам работы `cfgmaker` достаточно только оставить в файле конфигурации те блоки данных, которые предполагается анализировать для конкретного устройства. Учитывая, что по информации файла программа создает заголовки и служебные описания на страницах графика, имеет смысл откорректировать названия и описания тех позиций, которые предполагается отображать на графиках. Поскольку анализировать пропускную способность по портам, к которым подключены оконечные устройства (серверы, рабочие станции), не имеет смысла, то целесообразно сохранить мониторинг пропускной способности только для магистральных портов (портов, которые подключены к другим коммутаторам или концентраторам).

После редактирования файла настроек можно запустить программу `mrtg`, указав в качестве параметра конфигурацию устройства. Для систем с кодировкой UTF-8 команда запуска будет выглядеть так:

```
env LANG=C /usr/bin/mrtg /etc/mrtg.cfg
```

При первых двух запусках с новой конфигурацией вы получите предупреждения от команды; это нормально, поскольку в системе не сформированы еще файлы журналов, с которыми работает данная утилита.

При установке пакета MRTG в системе настраивается автоматический сбор информации с коммутаторов раз в пять минут. При желании этот период можно увеличить, если отредактировать соответствующим образом файл /etc/cron.d/mrtg.

Автоматический запуск MRTG осуществляется с конфигурацией, сохраненной в файле /etc/mrtg.cfg. Если вы предварительно тестировали настройки с использованием файла для конкретного устройства, то их необходимо импортировать в /etc/mrtg.cfg. Сделать это можно, например, следующей командой:

```
cat <индивидуальный_файл_настроек> >> /etc/mrtg.cfg
```

По умолчанию MRTG записывает данные, полученные с коммутаторов, в журналы в папке /var/www/mrtg. Имена журналов начинаются с адресов контролируемых устройств, для каждого порта устройства программа создает отдельный файл журнала.

> ***Примечание***
>
> Графики производительности по отдельным портам устройств можно просмотреть, если открыть в обозревателе папку **http://nagiosserver/mrtg/** и выбрать соответствующий файл. При желании с помощью команды `indexmaker` можно сформировать общий индексный файл для упрощения отображения. Необходимые ключи для формирования файла легко уточнить по справочной информации после вызова `indexmaker -h`.

После этих шагов можно собирать данные с устройств командами `Nagios check_mrtg` и `check_mrtgtraf`. Команда `check_mrtgtraf` требует указания следующих параметров:

```
check_mrtgtraf -F <имя_файла_журнала> -a <AVG-MAX> -w входящий,
исходящий -c входящий,исходящий -e период_устаревания
```

В этом примере параметр `-a` указывает, будет ли браться в учет максимальное значение (`MAX`) за период анализа или же программа оценит среднее значение (`AVG`). После ключей `-w` и `-c` указывают пары лимитов для исходящего и входящего трафиков по данному порту. Порт, по которому система будет контролировать данные, определяется выбранным файлом журнала.

На рис. 11.7 приведен пример реального графика, формируемого пакетом mrtg. Помимо отображенных графиков возможен просмотр показателей за периоды с интервалами в 5 минут, 30 минут, 2 часа и сутки.

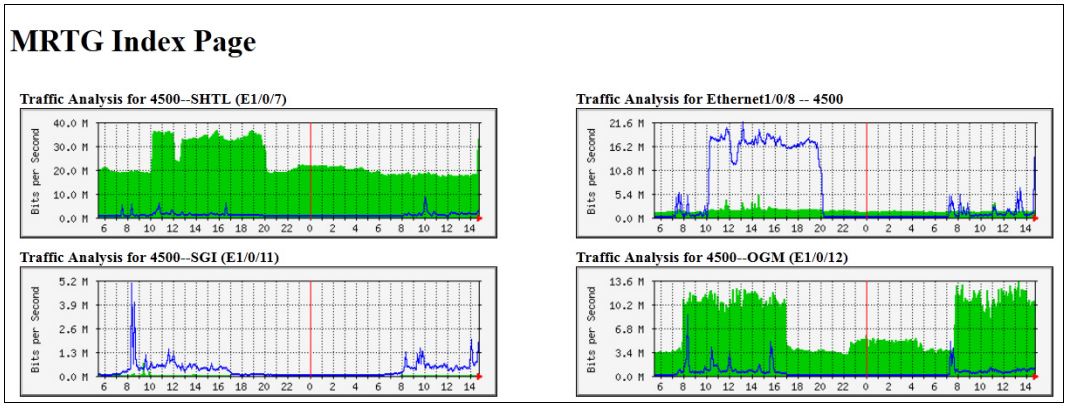


Рис. 11.7. График загрузки порта коммутатора

Использование собственных программ мониторинга

Nagios позволяет легко создать собственные плагины для мониторинга любой системы. Это могут быть любые исполняемые файлы. Необходимо только обеспечить, чтобы они сообщали код завершения работы в соответствии с табл. 11.4.

Таблица 11.4. *Коды возврата программ мониторинга системы для Nagios*

Возвращаемый код	Значение для Nagios
0	Нормально (OK)
1	Предупреждение (Warning)
2	Критическое значение (Critical)
3	Неопределенное значение (Unknown)

Листинг 11.9 иллюстрирует пример сценария для Ubuntu.

Листинг 11.9

```
#!/bin/sh
if <некоторое проверяемое условие>
then
exit 0
else
exit 2
fi
```

В случае создания сценария на Visual Basic под Windows его можно оформить так, как представлено в листинге 11.10.

Листинг 11.10

```
Dim status
status = 0
if <некоторое проверяемое условие> then
wscript.echo <здесь может быть выводимое дополнительно сообщение
предупреждения>
status = 1
elseif <некоторое проверяемое условие> then
wscript.echo <здесь может быть выводимое дополнительно критическое
сообщение>
status = 2
else
status = 0
end if
wscript.quit(status)
```

При создании сценариев необходимо учитывать, что запускаться они будут от имени службы агента мониторинга. По умолчанию в Windows эта служба имеет максимальные права для локальной системы, но не может взаимодействовать с компьютерами сети. Если вы предполагаете с помощью сценариев собирать данные с других компьютеров, то необходимо либо включать технологии имперсонализации, либо запускать агента под другой учетной записью.

Автоматическое реагирование на сбои в работе контролируемых систем

Как уже говорилось ранее, в параметрах конфигурации хоста можно указывать команду, которая должна выполниться при возникновении критической ситуации. По умолчанию Nagios отправляет сообщения по электронной почте (или иным описанным в конфигурации способом) операторам, закрепленным в конфигурации для данного типа хоста. Это сообщение отправляется в случае, когда Nagios окончательно фиксирует состояние аварии. Если вы помните, то в параметрах конфигурации контроля можно задать несколько повторных проверок состояния через некоторый промежуток времени. Именно после выполнения всех проверок и подтверждения состояния предупреждение будет выслано.

Но команда, заданная параметром `event_handler`, будет исполнена уже по получении *первого* результата, свидетельствующего об ошибках в работе систем.

Понятно, что подобные команды реагирования уникальны и должны создаваться индивидуально для каждой контролируемой службы. В качестве примера интересующиеся читатели могут рассмотреть сценарий со страницы **http://vadimszenins.blogspot.com/2008/12/nagios-restart-windows-failed-services.html**, который осуществляет перезапуск остановившейся службы в Windows 2003 Server.

Код сценария содержит все необходимые комментарии по описаниям службы и хоста (строки комментариев начинаются со знаков двоеточия), так что читателю не

составит большого труда разобраться с особенностями использования такого способа реагирования на состояния систем и применить его в собственных системах. Тем не менее, дадим некоторые пояснения.

После проверок синтаксиса вызова сценария программа запрашивает состояние службы с помощью команды `SC` из состава Windows Server 2003 и ищет в ее результатах слово `running`. Если служба не запущена, то сценарий пытается перестартовать ее, выполняя команды останова и запуска службы. Все действия сценария протоколируются в журнале, который сохраняется в папке C:\tools\logs (папка создается при ее отсутствии).

ГЛАВА 12

Защита информации

От информации, хранимой и обрабатываемой в компьютерной системе, все больше и больше зависит судьба организаций. Сбои в доступе к ней, утечки данных и т. п. приводят к значительным убыткам, несут ущерб для имиджа компании.

Опасности, которые нужно учитывать

Существует несколько рисков.

Во-первых, данные могут быть просто потеряны в силу некоторых обстоятельств. Например, случился пожар, повредивший оборудование и носители данных. Или неисправность в блоке питания привела к выходу из строя всех жестких дисков.

Во-вторых, данные могут быть недоступны временно. К примеру, вышло из строя оборудование, в организации есть резервная копия, но на время восстановления информации обслуживание клиентов невозможно, что ведет к убыткам для предприятия.

В-третьих, закрытая информация может стать доступной третьим лицам. Самый простой пример. Увольняющийся менеджер забирает с собой копию списка партнеров организации и продолжает работать с ними в новой компании. Понятно, что в такой ситуации существенная часть клиентов перейдет на обслуживание в новую компанию.

В-четвертых, данные могут быть несанкционированно изменены. Например, сотрудник пытается скрыть хищения и правит с этой целью "сырые" данные в учетной системе так, чтобы недостаток товаров не смог быть обнаружен другими сотрудниками.

В-пятых, в систему может быть заложена информация, которая должна привести к нарушению работы всей компании в заданный момент времени. В последнее время становится известным все большее число случаев, когда в системы управления производством были внедрены закладки, приведшие к аварийным ситуациям.

Понятно, что в каждом конкретном случае значимость каждого риска различна. Если организация осуществляет онлайновые операции, то любой простой сразу

приводит к существенным убыткам. В основной же массе компаний временная недоступность операций с товарно-материальными ценностями переносится достаточно легко.

Причины рисков

Причины возникновения опасностей могут быть различными. Частично они специфичны для каждой организации, но укрупненно могут быть классифицированы, например, следующим образом:

- отказы, возникающие вследствие выхода из строя оборудования, каналов связи и т. п. как в результате естественных причин (износа дисков), так и по причине катастроф, аварий и т. п.;
- риски утечки/изменения/повреждения/утери данных вследствие умышленных или неумышленных действий лиц, не имеющих (или не должных иметь) доступа к соответствующей информации;
- риски утечки/изменения/повреждения/утери данных вследствие умышленных или не умышленных действий лиц, имеющих доступ к соответствующей информации;
- риски неправоправных действий со стороны специалистов, имеющих полные права доступа к информации. Пункт выделен особо в связи с особым риском, с ним связанным.

В каждой организации эти типы рисков должны быть "раскрыты[1]" и для каждой позиции сформированы соответствующие меры противодействия.

Понятно, что добиться 100%-й надежности информации невозможно, а любое приближение к этой цифре будет требовать возрастающих в геометрической прогрессии затрат. Поэтому необходимо выбрать наиболее значимые риски и реализовывать меры защиты только по этим опасностям. Главный критерий такого отбора — стоимость защиты информации должна быть соизмерима с риском потерь. Понятно, что если потенциальный убыток составит 1 тыс. руб., но чтобы защититься от него, нужно потратить 10 тыс. руб., то реализовывать такие мероприятия не имеет смысла.

Конечно, для расчета стоимости ущерба существуют специальные методики. Но на практике такие расчеты обычно не удается выполнить, поскольку, например, невозможно точно оценить вероятности возникновения тех или иных событий и оценки берутся не то чтобы абсолютно "с потолка", но с очень большой погрешностью.

Именно при составлении реальной модели угроз и выделении рисков, по которым будут проводиться мероприятия защиты, и проявляется искусство руководителя и системного администратора.

---

[1] Говорят, что должна быть составлена *модель угроз.*

Порядок организации работ по защите информации

Работы по защите информации следует начинать с инвентаризации существующей системы. Чем точнее она будет описана, тем проще будет проанализировать возможные риски. Очень часто изменения вносятся техническими специалистами, не отражаются в документации, и их просто никто не учитывает.

Следующим шагом вы должны определить для себя модель нарушителя. Кто и как может принести убыток для вашей организации. Например, ценна ли ваша информация настолько, что нужно принимать меры по исключению ее утечки даже через специалистов, имеющих к ней доступ.

Теперь можно соотнести возможные действия нарушителя со структурой информационной системы и зафиксировать потенциальные уязвимости.

В итоге у вас должен получиться некий документ, который будет служить основой для дальнейших конкретных шагов.

> ***Примечание***
> Данный документ нужно обязательно пересматривать на регулярной основе.

Примерные мероприятия по обеспечению защищенности информации

Большинство работ по защите относятся к следующим мероприятиям:

- построение и отслеживание прав доступа пользователей к информации (к компьютерам, к данным на файловом, сетевом уровнях, в приложениях и т. п.);
- обеспечение безопасного подключения к локальной сети как снаружи (межсетевые экраны), так и изнутри (контролируемый доступ в сеть);
- построение системы развертывания обновлений безопасности операционных систем и приложений;
- поддержанием актуальности систем антивирусной защиты;
- контроль неизменности программного кода;
- контроль использования физических носителей, обеспечение физической безопасности компьютерных систем;
- организационные меры по разработке документации по защите информации и внедрению мер контроля их исполнения

  и т. д.

Проактивность мер защиты

На практике обычно руководитель сначала решает, какую систему ему нужно внедрить, а уже после начала эксплуатации задумывается над проблемами обеспечения ее безопасности.

Это порочная практика. Чем раньше вы начнете задумываться над вопросами безопасности, тем дешевле и надежнее будет решение.

Резервное копирование

Про резервное копирование знают все. Поэтому кратко затронем те моменты, которым на практике уделяется мало внимания.

Частоту операций резервного копирования, длительность хранения копий и т. п. должен определять владелец информации. Только он понимает, что и сколько нужно хранить.

Необходимо заранее оговорить допустимые сроки восстановления данных. Невозможно восстановить систему с нуля мгновенно. Учитывайте также, что на практике восстановление данных идет в 2—5 раз медленнее, чем их резервное копирование. Чем больше окно для восстановления, тем дешевле программное обеспечение, которое можно применить при операциях.

Определитесь, нужно ли предоставлять локальным пользователям и администраторам прикладных систем возможность восстановления данных, в том числе выборочного (например, восстановления индивидуального почтового ящика). Это существенно снизит нагрузку на системного администратора предприятия, но, опять же, такой функционал имеют не все программы резервного копирования.

Резервные копии — это вся информация предприятия. Хранить ее нужно так, чтобы никто не смог получить к ней доступ. При сомнениях в обеспечении физической безопасности реализуйте методы шифрования, но учтите, что операции будут выполняться медленнее.

Обязательно планируйте тренировочные операции восстановления. В противном случае велик риск остаться у разбитого корыта.

И едва ли не самое главное. Придерживайтесь правила 3-2-1. У вас должно существовать не менее 3 резервных копий одной информации, в 2-х разных местах, причем хотя бы одна копия должна находиться в другом месте (не на одной площадке).

Теневые копии

Штатное резервное копирование основано в Windows на технологии создания *теневой копии*. Теневая копия представляет собой моментальный снимок данных и может быть использована для копирования данных. Специальные поставщики теневых копий (так называемые *vss-провайдеры*) обеспечивают целостность данных. Например, если на компьютере присутствует vss-провайдер для конкретного сервера баз данных, то он гарантирует, что при создании теневой копии будут завершены все связанные транзакции.

> ***Примечание***
>
> Если такого провайдера нет, то данные приложений могут быть некомплектны.

Теневые копии создаются автоматически на регулярной основе на рабочих станциях и программами резервного копирования на серверах. При удалении данных, да-

же если используются программы безопасной очистки диска (многократная перезапись), данные теневой копии могут быть использованы для доступа к информации.

В Windows 7 открыть теневую копию можно, если вызвать свойства жесткого диска, на вкладке **Предыдущие версии** перейти на желаемую копию и открыть ее (рис. 12.1).

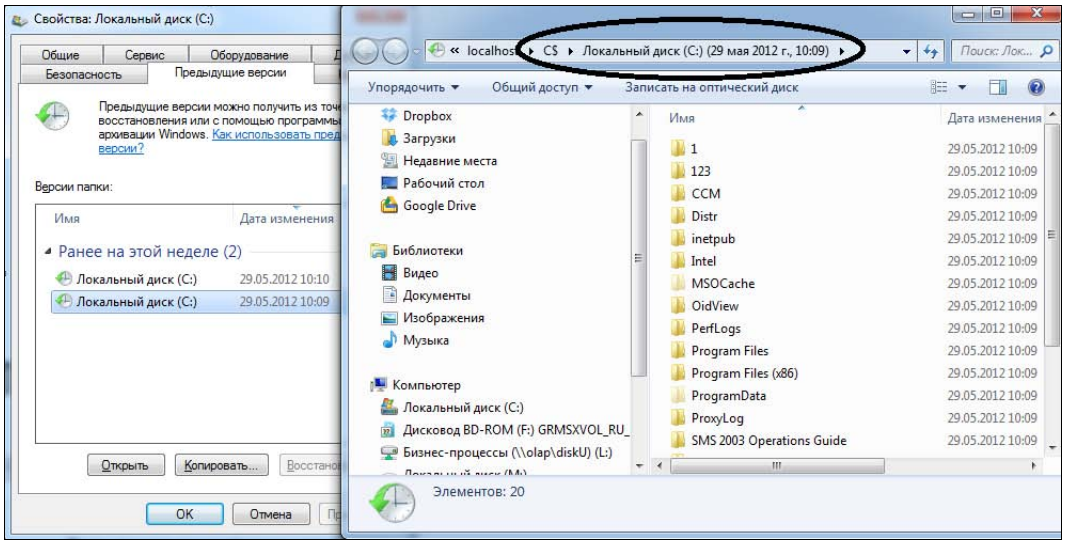


Рис. 12.1. Теневая копия диска в Windows 7

Надпись в строке адреса о дате свидетельствует о том, что вы открыли теневую копию в режиме только для чтения.

Для подключения в командной строке используется команда `vssadmin`. Ее нужно запустить с правами администратора и сначала перечислить имеющиеся копии командой

```
vssadmin list shadows
```

> ***Примечание***
>
> Если на компьютере используется несколько дисков с разными политиками, то следует применить ключ `/for=D:\`, где `D` — имя нужного логического диска.

После того как вы узнаете число копий и их даты, нужно выбрать номер желаемой копии и подключить ее командой

```
mklink /D C:\DDD \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy#\
```

В этом примере *DDD* — имя папки, в которую будет подключена копия (имя произвольно, такая папка должна отсутствовать по подключаемому пути), а # — номер теневой копии для подключения. Обратите внимание, что последний слеш в команде обязателен (при его отсутствии возникнет ошибка).

В серверных ОС для работы с теневыми копиями применяется команда diskshadow. Она позволяет создать копию (ключ create), перечислить их (list shadows), удалить

(delete shadows), подключить теневую копию в качестве нового логического тома (expose *имя_копии диск:*). При вызове этой команды вы попадаете в оболочку, в которой можно вводить соответствующие команды.

> ***Примечание***
>
> Команда может запускать внешний сценарий, позволяющий, например, создать теневую копию, выполнить копирование данных, а потом удалить ставшую ненужной теневую копию. Так, например, можно получить доступ к данным, которые блокированы приложением.

Системы цифровой защиты документов

Самые большие потери организациям наносят люди, имеющие доступ к информации по роду своей деятельности и забирающие ее с собой в случае увольнения (например, базу контактов). В некоторой степени помочь решить эту проблему могут системы защиты цифровых прав документов (системы DRM — **d**igital **r**ight **m**anagement).

Принцип действия такого ПО заключается в следующем. Документ шифруется и хранится в таком виде. Для работы с ним он динамически раскодируется с помощью ключа, выдаваемого сервером. В ключе может содержаться срок автономной работы с документов, что позволит работать с информацией вне офиса. Соответствующий модуль в ПО обеспечивает запрет на операции копирования, пересылки по электронной почте, печать и т. п.

Понятно, что такой принцип не обеспечивает полноценную защиту (документ можно просто переснять с экрана и потом преобразовать в текст, что современные программы делают практически безошибочно). Это средство — только усложнение для злоумышленника несанкционированных действий.

Естественно, что для работы с таким документом должна использоваться соответствующая программа. На сегодня из популярных продуктов возможности DRM включены в офисный пакет от Microsoft, а сам сервер ключей может быть развернут в домене Windows (**http://www.microsoft.com/ru-ru/server-cloud/information-protection/default.aspx**). Профессиональные решения предлагаются также от Oracle — Oracle IRM (**http://www.oracle.com/technology/products/content-management/irm/index.html**), Adobe (h**ttp://www.adobe.com/products/livecycle/rightsmanagement/**), FileOpen (**http://www.fileopen.com/**) и др.

В любом случае нужно учитывать ограниченность использования технологии (защищенные документы могут обращаться только внутри организации, использующей такую технологию, требуется специализированное ПО) и стоимость лицензий.

DLP-решения

Для защиты от утечки данных в крупных компаниях применяются решения DLP, которые анализируют на основании различных технологий и алгоритмов трафик и пытаются найти утечки защищенных данных.

Подобные системы работают, фактически, по итогам: они фиксируют утечку данных. Сама классификация информации (закрытая/открытая) обычно основана на неких статистических критериях. Поэтому технологии перехвата и мониторинг не дают гарантию полной защиты.

Антивирусная защита

Наверное, уже не осталось пользователей, которые не знали бы, что работать на Windows-системе без наличия антивирусной защиты нельзя.

Сегодня разработчики антивирусных программ предлагают большое количество различных средств. Хочется отметить, что сегодня представлены и высококачественные решения Open Source, способные осуществить защиту системы. Упомянем некоторые из них:

- Microsoft Security Essentials (**http://go.microsoft.com/fwlink/p/?LinkId=168949**);
- Panda Cloud Antivirus Free Edition (**http://www.cloudantivirus.com/en/#!/free-antivirus-download**);
- Avira Personal Free Edition (**http://www.avira.com/ru/avira-free-antivirus**);
- Comodo Antivirus Free Edition (**http://antivirus.comodo.com/antivirus.php**);
- Avast Antivirus Free Home Edition (**http://www.avast.com/ru-ru/free-antivirus-download**).

Необходимости использования коммерческих версий для домашних пользователей, небольших и даже средних организаций практически отсутствует. Если говорить о ПО корпоративной защиты, то это, прежде всего, системы защиты хоста, включающие в себя антивирусное ПО и ПО межсетевых экранов, средства контролируемого доступа в сеть, регулирования использования сменных носителей и контроля оборудования и запускаемых программ, различные политики его применения и т. п.

При всем при этом нужно обратить внимание, что в последнее время появились свидетельства того, что программное обеспечение вирусного характера стало разрабатываться серьезными организациями и все более направляется для получения экономических или политических преференций (см., например, ситуации с вирусами Flame, Stuxnet и др., которые широко обсуждались в сообществе). Защитить свою систему от подобных программ практически невозможно. Поэтому имеет смысл переключить внимание на поддержание неизменности программного кода и контроля запускаемых программных модулей.

Восстановление данных с жестких дисков

В Windows не предусмотрено никаких штатных средств для лечения жестких дисков, кроме программы `chkdsk`. Эта утилита позволяет проверить целостность файловой системы, "закрыть" сбойные участки жесткого диска. Но она будет практически бесполезна в случае серьезных повреждений.

Для восстановления информации с жестких дисков чаще всего применяют программы Easy Recovery (Ontrack Data Recovery, Inc., **www.ontrack.com**) и GetDataBack (RunTime Software, **www.runtime.org**).

Эти программы позволяют восстановить данные даже с тех дисков, которые не определяются в BIOS компьютера. Имеется возможность восстановления после форматирования диска, "сборки" файлов на основе их типа и т. п.

Работа с данными программами достаточно очевидна. Сначала анализируется структура жесткого диска, предлагается определить восстанавливаемый раздел и тип файловой системы, после чего начинается поиск информации. Найденный список можно отфильтровать при необходимости по тем или иным критериям (например, восстанавливать только файлы документов), после чего можно выполнить восстановление.

Восстановление всегда производится на другой диск, чтобы не повредить исходные данные. Поэтому при отсутствии сетевых подключений необходимо позаботиться о дополнительном устройстве хранения.

Если возникли дефекты устройства хранения данных (чаще всего переносные устройства, реже — жесткие диски, компакт-диски), то обычно повреждается лишь небольшой участок файла. Но это, как правило, приводит к тому, что соответствующий файл не открывается в программе его редактирования.

Для восстановления таких поврежденных файлов разработано много утилит, которые можно найти в Сети. При этом чем популярнее формат файлов данных, тем больше вероятность того, что для этого типа информации существуют утилиты восстановления. Например, можно перечислить утилиты восстановления для офисных файлов (Microsoft Word, Excel, Access, PowerPoint), для файлов личных папок офиса (pst), для файлов архива (zip), файлов баз данных (dbf) и т. п. Версии этих утилит меняются с модификацией основных программ, поэтому я отошлю читателя к самостоятельному поиску в Интернете.

Принцип работы таких утилит достаточно прост. Они анализируют структуру файла, находят поврежденный блок данных и корректно восстанавливают структуру файла так, чтобы он мог быть открыт в основной программе с минимальными потерями.

ГЛАВА 13

Построение отказоустойчивой системы

Поскольку мы все больше начинаем зависеть от различных информационных систем, то системным администраторам приходится принимать специальные меры, чтобы сервисы были доступны в любое время независимо от возникающих проблем.

Построение высокодоступной информационной системы стоит денег, причем весьма существенных. Поэтому необходимо предварительно правильно выбрать уровень надежности, которого вы собираетесь достичь. И в любом случае нужно соотносить потенциальные потери от отказа в обслуживании с реальными затратами на их предупреждение.

Общие требования к надежной системе

Надежная система — это система, в которой отсутствует единая точка отказа. Иными словами, любой элемент системы должен быть *дублирован*.

Искусство проектировщика состоит даже не только в подборе резервирующих технологий, сколько в способности предугадать потенциальные точки отказа.

В информационных системах обычно дублируют следующие компоненты:

- помещения серверных (центров обработки данных);
- систему электроснабжения;
- систему кондиционирования;
- транспортную инфраструктуру;
- основные сетевые службы (разрешения имен, аутентификации и т. п.);
- собственно прикладные приложения;
- компоненты оборудования: жесткие диски (создание RAID), блоки питания, контроллеры доступа и т. д.

Территориальная распределенность

Если серверы предприятия расположены, например, в одном помещении, то не исключена возможность одновременного выхода их из строя в случае какой-либо аварии и т. п. Если сеть передачи данных построена с дублированием линий связи и частично они проходят по одной трассе, то повреждение этого участка приведет к отказу как основного, так и резервного канала связи. Если резервное копирование проводить на устройство, расположенное в одном шкафу с сервером, то пожар может уничтожить как сам сервер, так и резервную копию.

Известен пример, когда дорогостоящий дублированный центр обработки данных был полностью выведен из строя на несколько дней из-за того, что упавшая во время грозы балка повредила оба (основной и дублирующий) чиллеры системы охлаждения, которые располагались в непосредственной близости один к другому.

Предугадать аналогичные случаи, а тем более предусмотреть соответствующие меры при проектировании очень сложно. Но к этому надо стремиться.

Поэтому, например, серверные желательно размещать на первом этаже, в помещении без окон, без трубопроводов и т. п. Необходимо избегать соседства помещений с материалами, которые могут нанести вред оборудованию (например, трубопроводы над помещением, склады с опасными веществами рядом и т. п.).

При площади серверной свыше 20 $м^2$ по санитарным нормам и правилам требуется применять систему газового пожаротушения. У нас в стране сертифицировано несколько решений; на практике лучше использовать газовую смесь, допускающую вдыхание ее человеком. Проект системы газового пожаротушения не представляет особой сложности, но он должен быть выполнен сертифицированной организацией с последующей приемкой объекта пожарными службами.

Надежность системы электроснабжения

Для серверных небольших предприятий обычно практически невозможно реализовать подключение к двум независимым вводам от подстанций или выбрать более высокий уровень надежности внешнего электроснабжения. Поэтому необходимые требования по отказоустойчивости приходится реализовывать только путем наращивания мощностей оборудования резервного электропитания.

Обратите внимание, что следует выбирать оборудование — серверы, коммутаторы и т. п. — с двумя блоками питания и запитывать их от разных линий. Поскольку источники аварийного питания с несколькими независимыми выходами недоступны по цене небольшим организациям, можно устанавливать для каждой линии независимые устройства.

Для выбора источников бесперебойного питания (ИБП) важно знать потребляемую оборудованием мощность. Этот показатель зависит от комплектации устройства (например, количества установленных жестких дисков) и не совсем верно ориентироваться в таком случае на максимальную мощность его блока питания: это значе-

ние максимально допустимой мощности. Для точного расчета ведущие вендоры предлагают на своих сайтах специальные калькуляторы. Например, для сервера Sun Fire X4800 M2 соответствующее решение доступно по ссылке

http://www.oracle.com/us/products/servers-storage/sun-power-calculators/calc/x4800-m2-power-calculator-405670.html.

Калькулятор учитывает при расчете потребляемой мощности тип процессора, количество памяти, жестких дисков, плат PCIe и т. д. Если вендор не предоставляет подобной услуги, то можно грубо оценить потребление стандартными калькуляторами (например, Power Calculator **http://www.coolermaster.outervision.com/**, Калькулятор мощности **http://www.emacs.ru/calc/**, PSU Watts And Rails Calculator **http://psucalc.tk/** и т. д.).

По рассчитанной мощности нужно выбрать требуемый тип ИБП. При этом помимо значения потребляемой мощности на итоговый выбор сильно влияют значения времени автономной работы и закладываемый на развитие запас мощности.

Обычно трудно обосновать максимальное время автономной работы, на основании которого выбираются ИБП. Часто эта цифра берется "с потолка" или "как у других". При этом даже небольшое увеличение этого времени приводит к существенному удорожанию оборудования. Рекомендуем в качестве критерия оценки использовать время выключения информационной системы с сохранением всех данных. Это значение нужно умножить на 2 или 3.

На резерв принято добавлять примерно 30—50% от полученных расчетных путем показателей. Так вы получите минимальное значение, которое можно использовать при расчете ИБП.

Для выбора ИБП лучше всего обратиться к инструментарию соответствующего вендора. Так, например, APC Schneider Electric предлагает такое средство на странице **http://www.apc.com/tools/ups_selector/**. Вам нужно только ввести желаемые характеристики и получить на выбор несколько вариантов оборудования.

> ***Примечание***
>
> Для серверных помещений лучше выбирать модели ИБП с конфигурацией *N* + 1, несколькими выходами нагрузки с регулируемой возможностью отключения. Это позволит обеспечить надежность ИБП, плавно отключать неответственные серверы и продлить время работы критических подсистем.

Рекомендуем обязательно приобретать устройства, позволяющие настроить программный контроль состояния заряда аккумуляторов, оставшуюся длительность автономной работы и т. д. Лучше всего, если такой контроль будет реализован по сетевым интерфейсам. Такой вариант позволит безопасно выключать оборудование при пропадании электропитания.

> ***Совет***
>
> Не забывайте, что ИБП должно быть снабжено и коммутационное оборудование узлов ядра и распределения. Причем параметры автономной работы этих устройств не должны быть хуже уровня защиты серверного оборудования.

Обеспечение климатических условий эксплуатации

При увеличении температуры окружающей среды экспоненциально снижаются показатели надежности электронного оборудования. Поэтому нормальным условием эксплуатации считается поддержание температуры около 18 °С. Характеристики кондиционеров рассчитываются на основе параметров тепловыделения установленного оборудования. Они обычно входят в состав технических параметров оборудования. Если эксплуатируется "нефирменное" устройство, то его тепловыделение можно рассчитать по потребляемой мощности (формула соответствия доступна в Интернете).

Параметры влажности не являются значимыми, если в серверных не эксплуатируются ленточные библиотеки. Обычно только требуется, чтобы была исключена возможность выпадения росы. Поскольку в помещении серверных не предполагается работа персонала, то требований по воздухообмену обычно не предъявляют.

Так же, как и все остальные системы, оборудование климат-контроля должно быть дублировано. Если организация не может позволить себе установку прецизионных специализированных кондиционеров, то в качестве одного из вариантов может быть установка двух бытовых кондиционеров с разными установленными значениями охлаждения. В этом случае в основном будет работать один кондиционер, а второй будет его подстраховывать и включаться только при отказе первого или сильном повышении внешней температуры. Через некоторый период времени для обеспечения равномерности износа необходимо менять настройки кондиционеров местами.

На кондиционирование расходуется большая часть потребляемой электроэнергии. Причем это электропитание также должно быть резервировано (без охлаждения современные насыщенные оборудованием серверные не могут проработать более 15—20 минут). Поэтому сегодня много внимания уделяется решениям, позволяющим снизить потребление энергии. Например, использование зимой внешнего холодного воздуха для поддержания необходимой температуры внутри помещения. Или создание балластных накопителей, способных некоторое время обеспечить отсутствие охлаждения хладоагента в случае пропадания электроэнергии.

Обеспечение отказоустойчивой среды передачи данных

Необходимое условие надежной работы информационной системы — безотказное функционирование каналов связи. Данная задача решается путем *дублирования* как собственно каналов связи, так и активного оборудования (коммутаторов).

Отказоустойчивая топология сети передачи данных

Для обеспечения отказоустойчивости сети передачи данных необходимо наличие резервных линий, причем пути их прокладки не должны совпадать с основными

кабелями (чтобы случайное повреждение группы кабелей, например, в результате земляных работ, не привело к разрыву как основного, так и дублирующего кабеля). Понятно, что на практике отказоустойчивая конфигурация сети создается только в тех случаях, когда простои в работе информационной системы недопустимы и могут привести к существенным экономическим потерям.

Простое соединение двух коммутаторов двумя кабелями создаст кольцо, которое недопустимо в сети Ethernet. Результатом станет широковещательный шторм и практическая неработоспособность сегмента сети. Поэтому создание отказоустойчивых решений требует первоначальной настройки активного оборудования.

> ***Примечание***
>
> В коммутаторах, предназначенных для работы на уровне доступа, обычно по умолчанию включены протоколы, которые "разорвут" такое кольцо. Коммутаторы уровня ядра не имеют таких настроек, поэтому возникновение кольца быстро приведет к падению сегмента сети.

Существуют два варианта построения сети, в которой присутствуют резервирующие каналы связи. Первый использует протоколы, работающие на втором уровне модели OSI. Второй основан на протоколах маршрутизации (третий уровень модели OSI).

Построение отказоустойчивой сети на основе протоколов второго уровня

Отказоустойчивая конфигурация на протоколах второго уровня обеспечивает самое быстрое восстановление в случае аварии. Сеть может восстановиться за 1—3 с или даже еще быстрее в случае проприетарных протоколов.

Использование протоколов остовного дерева

Протоколы остовного дерева — Spanning Tree Protocol (STP, стандарт 802.1d) и Rapid Spanning Tree (RSTP, стандарт 802.1w) — служат для автоматического построения связей сетевой структуры. Коммутаторы пытаются по определенным алгоритмам вычислить оптимальные маршруты между всеми устройствами и автоматически блокируют (отключают) порты при обнаружении петель. Для определения маршрутов и контроля соединений по специальным алгоритмам постоянно рассылаются служебные пакеты (BPDU, Bridge Protocol Data Units). В случае изменения структуры сети производится ее переконфигурирование. Этот процесс занимает от 30 секунд до нескольких минут в зависимости от размера сети для протокола STP. При использовании RSTP (усовершенствованной версии STP) время перестройки уменьшается до нескольких секунд.

Протоколы могут обеспечить связность сети без каких-либо ручных настроек. Для построения структуры алгоритмы учитывают скорость соединения и количество коммутаторов между точками. Администратору нужно только включить на портах данные протоколы (часто это настройка по умолчанию для коммутаторов уровня доступа). На основании анализа рассылки пакетов BPDU коммутатор определяет

существующие связи и автоматически отключает порты, к которым подключены вторые, резервные каналы.

Для оптимизации дерева связей целесообразно *вручную* назначить приоритеты коммутаторам: устройство в центре сети должно иметь самый малый "вес" (Bridge ID или Bridge Priority), чем дальше от логического центра, тем большие веса нужно назначать коммутаторам. Кроме того, в случае применения протокола RSTP желательно настроить опцию быстрого старта порта (Fast Start) для тех портов, к которым подключены конечные устройства. Это исключит такие порты из процедуры определения маршрутов и ускорит сходимость.

> ***Примечание***
>
> Алгоритм выбора приоритета коммутатора основан на MAC-адресе устройства. Поэтому более *старое* устройство, как имеющее меньший номер MAC, получит приоритет в процедуре выбора корневого коммутатора. На практике обычно происходит с точностью "до наоборот". В центр сети размещают самое новое устройство, как самое производительное.

Протоколы STP/RSTP поддерживаются всеми современными коммутаторами. Однако их серьезный недостаток — отключение резервных связей. Резервные связи не задействуются для передачи данных и включаются только при повреждении основного канала.

> ***Примечание***
>
> Поддержку протокола RSTP (STP) следует включать и не только при наличии избыточных каналов связи. Включение этой функции позволит сохранить функционирование сети в случае случайного или умышленного создания петель, которые без данных протоколов приведут к широковещательному шторму и практическому прекращению функционирования сегмента. Для создания петли достаточно воткнуть один патч-корд в два порта коммутатора (например, пользователь увидел свободный конец патч-корда, не проверил, что другой конец его включен в розетку, и подключил разъем в соседнюю свободную розетку). Обычно протоколы STP/RSTP включаются по умолчанию на коммутаторах уровня доступа.

Использование стандарта MSTP

Стандарт MSTP (Multi Spanning Tree Protocol, описан в 802.1s) является расширением стандарта RSTP на сеть с VLAN.

В отличие от RSTP, MSTP для каждой виртуальной сети строит свое дерево связей. Поэтому предупреждение петель происходит не путем отключения порта коммутатора, а через отключение передачи данных только для определенной VLAN. В результате можно настроить MSTP так, чтобы для части VLAN было заблокировано одно соединение из дублированных ссылок, а для других VLAN — второе. Для этого в настройках протокола администратору вручную нужно назначить каналам различные веса: в одном случае основным будет первый канал, а второй — резервным. Во втором — наоборот. Таким образом, все соединения будут передавать данные. При повреждении канала связи MSTP обнаружит это событие и автоматически перестроит структуру.

Таким образом, MSTP позволяет осуществить *балансировку трафика* по основному и резервному каналам связи.

Главный недостаток решения на протоколе MSTP заключается в сложности настройки такой структуры. Администратор должен четко представлять разбиение системы на VLAN, оценить потоки данных в каждом сегменте и путем ручной настройки добиться примерно равномерной загрузки всех каналов связи.

Также следует учитывать, что во многих моделях коммутаторов (особенно бюджетного ряда) поддержка протокола MSTP не реализована.

Построение отказоустойчивой сети на основе протоколов третьего уровня

Основной практический вариант создания отказоустойчивой конфигурации сети на сегодня — решения, основанные на применении протоколов автоматической маршрутизации. Хотя протоколы маршрутизации имеют несколько худшие показатели времени перестроения сети (например, OSPF может перестроить сеть приблизительно за 3 с), однако трудоемкость настройки структуры сети существенно ниже, чем при использовании, например, протокола второго уровня MSTP.

С точки зрения протоколов маршрутизации сеть с резервными каналами связи представляет собой отдельные подсети с несколькими возможными путями передачи данных из одной подсети в другую. В большинстве случаев администратору достаточно только включить протоколы автоматической маршрутизации, чтобы сеть "заработала". В небольших сетях можно использовать протокол RIP как самый простой в настройке, в средних — протокол OSPF. Рекомендации по настройке этих протоколов приводятся в документации на активное оборудование.

При таком решении переключение на другие пути передачи данных в случае повреждения каналов связи будет происходить за счет изменения таблиц маршрутизации.

Кластеры коммутационного оборудования

Промышленные модели коммутаторов допускают объединение нескольких физических устройств в одно логическое. В этом случае существенно упрощаются все настройки параметров отказоустойчивости структуры.

Подобные решения на сегодня проприетарны, т. е. объединить в один логический можно оборудование только одного вендора. Причем обычно такую совместную работу допускают лишь старшие модели при определенных ограничениях.

Вендоры используют собственные названия таких технологий. Так у Cisco решение носит название Cisco Cluster, у Hewlett-Packard — технологией IRF (Intelligent Resilient Framework) и т. д.

VRRP

При маршрутизации между несколькими VLAN в качестве шлюза по умолчанию для рабочих станций назначается адрес интерфейса коммутатора. Это является

узким местом такого решения, поскольку при выходе из строя коммутатора со шлюзом компьютеры потеряют связь с другими сетями.

Для предупреждения подобных ситуаций необходимо задействовать протокол VRRP (Virtual Routing Redundancy Protocol), который позволяет настроить *два* коммутатора как *один* шлюз. Естественно, что от клиента в таком случае необходимо иметь две линии подключения. Поэтому такой вариант обычно применяется для резервированного подключения коммутаторов уровня доступа к коммутаторам распределения или ядра сети.

> ***Примечание***
>
> Этот протокол реализован далеко не на всех моделях коммутаторов. Как правило, модели, приобретаемые в малых организациях, не имеют поддержки данного протокола VRRP.

Идея создания отказоустойчивого шлюза на базе протокола VRRP состоит в следующем. В сети устанавливают два коммутатора с поддержкой данного протокола. На каждом из них настраивают сетевые интерфейсы и включают протокол VRRP. После чего настраивают интерфейс с одним и тем же IP-адресом на обоих коммутаторах, причем один коммутатор определяется главным, а второй — ведомым. В нормальных условиях работы коммутаторы постоянно обмениваются между собой служебной информацией. Если оба они нормально работают, то по настроенному адресу шлюза "отвечает" только главный коммутатор. Если он выходит из строя, то второй коммутатор начинает принимать данные по адресу шлюза и передавать их в другие сети в соответствии с настройками.

Таким образом обеспечивается отказоустойчивая работа шлюза независимо от состояния отдельного коммутатора или целостности связей.

Протокол VRRP является стандартом. В то же время существуют отдельные модификации его реализации на коммутаторах различных вендоров. Так, из описанного принципа работы VRRP следует, что в "нормальных условиях" передачу данных в другую сеть обеспечивает только главный коммутатор. Хотя физические связи — в целях отказоустойчивости — имеют оба устройства. Поэтому в некоторых коммутаторах реализованы проприетарные расширения функциональности протокола VRRP: оба коммутатора будут работать в качестве шлюза и передавать данные в другие сети. Только при выходе из строя одного из них трафик будет перенаправлен в другой коммутатор. Этим достигается балансировка нагрузки на различные каналы связи и увеличение пропускной способности сети.

Время восстановления структуры сети

Добиться малого времени восстановления передачи данных после единичной аварии очень сложно. На основе использования открытых стандартов реально достичь восстановления обслуживания за период не более 3—5 с.

Проприетарные технологии принципиально способны несколько уменьшить данный период (до величин, менее одной секунды). Однако следует крайне осторожно подходить к подобным прогнозам. Очень часто даже крупные вендоры в маркетин-

говых целях презентуют крайне низкие значения периода восстановления (например, 20 мс), не особо привлекая внимания к тем условиям, при которых получен такой показатель. Если отказ внутри шассийного коммутатора может быть устранен за данное время, то на восстановление после другой неисправности требуется несколько секунд, и сеть в целом будет характеризоваться именно наихудшим показателем.

Что можно посоветовать администраторам? В первую очередь, больше проверять, чем доверять маркетинговым предложениям. Изучать базовые документы по существующим технологиям, читать технические описания оборудования, обращая внимания на любые оговариваемые особенности. Во-вторых, стараться быть в курсе тестов, проводимых независимыми лабораториями, например, Tolly Group (**http://www.tolly.com/**). Хотя и учитывать условия проведения теста.

В-третьих, просчитывать параметры именно для вариантов конфигурации вашей сети. Каждая конфигурация индивидуальна. И не факт, что лучшее решение для идеальной лаборатории окажется таковым в реальной ситуации.

Обеспечение резервированного доступа в Интернет

Если необходимо иметь гарантированный доступ в Сеть, то нужно обеспечить дублирование каналов доступа. При этом следует выбирать услугу, предоставляемую различными сетевыми операторами (чтобы не быть ограниченным единой точкой доступа к магистральным каналам).

Для того чтобы обеспечить отказоустойчивое подключение к двум каналам доступа к Интернету, существуют специальные протоколы маршрутизации. Но для их применения необходимо зарегистрировать IP-адреса организации в качестве *автономной системы* (AS). Автономная система позволяет обеспечить доступность ресурсов организации извне при выходе из строя любого канала доступа. Появление новых AS приводит к увеличению объема таблиц маршрутизации, поэтому необходимо серьезно обосновывать соответствующую заявку.

При наличии двух каналов подключения к Интернету автоматический выбор для исходящего трафика может осуществить маршрутизатор, если на его порту будет информация о состоянии канала. В простейшем случае отказоустойчивый доступ в Интернет можно обеспечить программным способом на Linux-маршрутизаторе, если настроить периодический запуск проверки линии связи (например, командой `ping`) с последующей сменой шлюза по умолчанию в случае падения канала. Пример такого сценария легко можно найти в Сети.

Недостатком такого решения является нерезервированный доступ извне к ресурсам организации. Поскольку адрес, например, веб-сервера зарегистрирован на адрес конкретного провайдера, то при отказе соответствующего канала сервер будет недоступен.

В случае размещения почтового сервера можно создать две MX-записи и переключение в случае повреждения связи будет осуществляться уже на стороне передающего сервера (после неответа почтового сервера, соответствующего MX-записи

с минимальным весом, начнется попытка передачи на следующий адрес, прописанный в DNS-сервере для этого домена).

Примечание

В нормальной ситуации можно задействовать балансировку каналов доступа в Интернет с использованием возможностей `iptables`.

Построение отказоустойчивых сетевых служб

Для базовых сетевых служб — аутентификации, разрешения имен и т. д. — разработаны собственные механизмы обеспечения отказоустойчивости.

Настройка систем аутентификации

При работе в централизованно управляемой сети аутентификация пользователей производится специальными серверами. Если они будут недоступны, то пользователь не сможет работать с сетевыми ресурсами.

Примечание

Станции Windows кэшируют несколько паролей входа пользователей (если этот параметр не отключен групповой политикой). Поэтому при недоступности контроллера домена пользователь, например, сможет войти на сервер удаленных рабочих столов, если он к нему подключался ранее.

Стандартная рекомендация в этом случае заключается в установке не менее двух серверов аутентификации и авторизации (контроллеров домена). В результате при отказе одного контроллера домена второй некоторое время сможет обслуживать сеть.

Длительность обслуживания сети одним контроллером зависит от распределения ролей хозяев операций (если хозяин операций продолжает работу, то срок восстановления второго сервера не критичен) и от интенсивности изменений в службе каталогов (не хозяева ролей имеют некоторый запас идентификаторов для автономной работы, после того, как он будет исчерпан, обслуживать новые запросы контроллер домена не сможет). Поэтому желательно — в случае выхода контроллера домена из строя — принять меры к скорейшему его восстановлению.

Отказоустойчивый DHCP-сервер

В случае отказа DHCP-сервера компьютеры не смогут получить аренду IP-адресов и перейдут на частные диапазоны (169.254.*x*.*x*). В результате работа в сети станет невозможна.

Проблема не очень критична, поскольку, во-первых, основные службы используют статическое разрешение имен, во-вторых, обычно сроки аренды адресов достаточно продолжительные (как правило, составляют от недели и более) и клиенты смогут продолжить работу с уже выделенными адресами.

Однако, поскольку часто состояние данной службы не отслеживают, то системный администратор может просто столкнуться с фактом невозможности работы в сети рабочих станций.

Реализация DHCP на основе сервера Microsoft не позволяет создать полностью отказоустойчивую конфигурацию. Традиционно для обеспечения отказоустойчивости нужно было "поднять" два DHCP-сервера и разделить между ними выдаваемый диапазон адресов. Проблема заключалась в том, что такой способ подходил для небольшого числа компьютеров в сегменте сети: всегда существовала вероятность, что меньший диапазон адресов будет выдан (исчерпан) и в этот момент откажет основной DHCP-сервер.

В Windows Server 2008 появилась возможность настройки совместной работы двух серверов. Выдачу адресов обслуживает основной сервер, чтобы резервный сервер не выдавал в обычных условиях адреса, на нем устанавливается задержка с ответом (в этом случае первым отвечает основной сервер, и он же и выдает адрес). В случае отказа основного сервера на резервном при такой политике должен всегда оставаться свободным некоторый диапазон адресов, поэтому некоторое время второй сервер сможет выдавать адреса.

Такой способ не создает полной отказоустойчивости, но позволяет продолжить нормальную работу системы некоторое время до восстановления DHCP-сервера.

Для настройки разделения областей в Windows Server 2008 нужно открыть консоль управления сервером DHCP и для нужной области в динамическом меню выбрать команду разделения областей. Запустится мастер, который предложит указать второй сервер DHCP для настройки. После проверки доступности этого сервера мастер по умолчанию предложит разделить выдаваемые адреса в пропорции 80 к 20 (рис. 13.1). После указания данного параметра на следующем шаге мастер предложит установить время задержки ответа второго DHCP-сервера. Обычно достаточно согласиться с настройками по умолчанию. После завершения работы мастера вы получите два настроенных DHCP-сервера, разделяющих выдачу адресов одного диапазона.

Если говорить о Linux, то в этих системах существует простой способ объединения двух или более серверов DHCP в отказоустойчивый пул. Оба сервера пула работают синхронно: одновременно обслуживают клиентов и выдают адреса одного и того же диапазона.

> ***Примечание***
>
> Отказоустойчивый сервер DHCP можно создать в Windows, если разместить его на кластере *(см. разд. "Кластерные решения" далее в этой главе)*. Рекомендации описаны на **http://technet.microsoft.com/en-us/library/ee460952%28v=ws.10%29.aspx**.

Настройка отказоустойчивого пула серверов DHCP в Linux выполняется очень легко. Для этого достаточно в конфигурации DHCP описать (определить) отказоустойчивый пул и затем сослаться на него (включить его имя) в настройках каждого выдаваемого блока адресов.

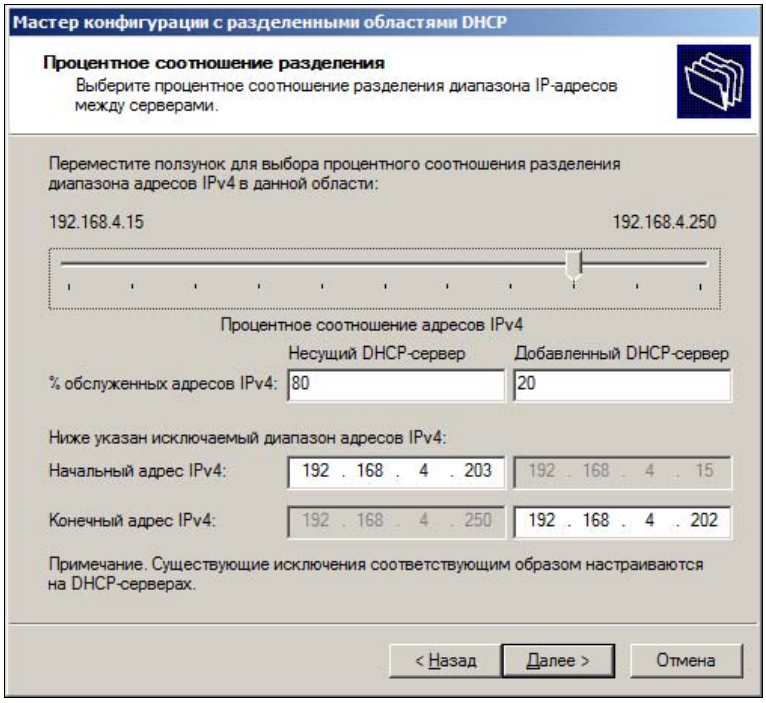


Рис. 13.1. Мастер настройки разделенных областей DHCP

Отказоустойчивый пул описывается следующим образом:

```
failover peer "dhcp-failover" {
primary;
address 10.1.0.1;
port 647;
peer address 10.1.0.2;
peer port 847;
max-response-delay 60;
max-unacked-updates 10;
load balance max seconds 3;
mclt 3600;
split 128;
}
```

Указанные параметры описания пояснены в табл. 13.1.

Таблица 13.1. *Параметры настройки отказоустойчивого пула DHCP*

Параметр	Обозначает
`primary`/`secondary`	Основной или резервный DHCP-сервер
`address`	Адрес сервера. Это может быть как IP-адрес, так и FQDN
`port`	Номер порта, используемого для получения данных от сервера-партнера DHCP

Таблица 13.1 *(окончание)*

Параметр	Обозначает
`peer address`	Адрес сервера DHCP-партнера. Это может быть как IP-адрес, так и FQDNN
`peer port`	Номер порта на сервере-партнере, используемого для отправки сообщений
`max-response-delay`	Параметр определяет, сколько секунд может пройти без получения сообщения от партнера, чтобы сервер оценил связь как прерванную
`max-unacked-updates`	Параметр определяет, сколько служебных сообщений сервер должен отправить партнеру без получения подтверждения, чтобы оценить связь, как прерванную
`mclt`	Максимальное время, в течение которого адрес может быть обновлен данным сервером без контакта с партнером. Действует только на основном сервере
`split`	Параметр определяет балансировку выдаваемых адресов между серверами. Может использоваться в настоящее время только значение 128
`load balance max seconds`	Параметр определяет промежуток времени (после получения от клиента первых сообщений DHCPDISCOVER или DHCPREQUEST), после которого отключается балансировка серверов DHCP

Обычно параметры отказоустойчивого пула можно сохранить в значениях по умолчанию (естественно, кроме самих адресов серверов) так, как указано в приведенном ранее примере.

После определения пула строчку с его именем достаточно включить в блок описания выдаваемых адресов. В следующем примере эта строчка выделена жирным начертанием (последующие строки описания опущены для экономии).

```
subnet 10.1.0.0 netmask 255.255.255.0 {
option domain-name-servers 10.1.0.12;
option routers 10.1.0.1;
pool{
failover peer "dhcp-failover";
range 10.1.0.16 10.1.0.254;
```

Дублирование DNS-сервера

DNS-серверы сегодня являются основой систем разрешения имен. В случае недоступности DNS работа систем в сети практически будет парализована.

Для обеспечения отказоустойчивости в технологиях DNS предусмотрено создание нескольких серверов: *основного* (primary) и одного или нескольких *вторичных* (secondary). Клиенту сообщаются адреса всех серверов DNS. При этом изменения могут вноситься только на основном сервере, остальные серверы синхронизируют данные с первичного.

В домене Windows серверы DNS реализованы на распределенной базе службы каталогов. Данный вариант позволяет распределять нагрузку: каждый сервер может выступать в роли первичного и вносить изменения в данные зоны. При этом основная проблема заключается в клиентах Windows. На практике в случае выхода из строя сервера DNS, который указан в качестве *первой* записи в настройке параметров IP-протокола рабочей станции Windows, последняя не может переключиться на использование второго сервера. Ситуацию спасает перезагрузка рабочей станции, но такое решение недопустимо для систем, требующих непрерывной работы.

Дублирование данных

Одним из способов обеспечения безопасности данных являются различные технологии дублирования. Принцип хранения данных на двух или более серверах во многих случаях оказывается достаточным для требуемого уровня безопасности системы, а реализуются такие решения многими способами, причем часто не требующих дополнительных затрат.

Репликация файловых данных в DFS

Распределенная файловая система позволяет исключить единую точку отказа, позволяя клиентам использовать сетевые пути к данным, а не ссылки, привязанные к конкретным системам.

Кроме того, в таких системах настраивается репликация данных, при помощи которой можно дублировать ресурсы в сети и обеспечивать их идентичность в случае изменений.

Если говорить о Windows-системах, то это *распределенная файловая структура* (Distributed File System, DFS), реализованная на серверах Windows 2000 и старше. Для Linux-систем на сегодня автору не известно бесплатное решение, которое являлось бы лидером в данном классе. Можно упомянуть такие системы, как Ceph (клиентская часть включена в ядро Linux версии старше 2.6.34), XtreemFS, GlusterFS, GFS (Google File System), GPFS (General Parallel File System), Lustre и др. Все это вполне работоспособные решения, которые можно реализовывать в проектах. Соответствующая документация по настройке упомянутых файловых систем легко доступна в Интернете. При этом на Linux-системах легко можно настроить поддержку корней DFS (описание приведено далее в этой главе).

Кроме устранения единой точки отказа использование распределенной файловой системы удобно при администрировании: можно прозрачно для пользователей перемещать совместно используемые файловые ресурсы с одного компьютера на другой без прекращения обслуживания и без перенастроек пользовательских компьютеров, поддерживать идентичность данных центрального офиса и удаленного филиала и т. п.

Особенности создания и настройки DFS описаны в *главе 9*.

Репликация данных средствами СХД

В современных системах хранения данных предусматриваются механизмы, позволяющие создавать копию одной системы на другую. Эти технологии являются проприетарными (могут синхронизировать данные только между изделиями одного вендора) и часто требуют приобретения дополнительной лицензии.

Существуют два варианта совместной работы систем хранения: синхронный и асинхронный режимы. В синхронном режиме запись осуществляется одновременно на обе системы, пока запись не завершится на удаленном устройстве, первая система также не завершит операцию. Синхронный режим гарантирует идентичность данных, но замедляет операции (особенно, если удаленная система подключена не по самому быстрому каналу). При асинхронном режиме операции для удаленной системы ставятся в очередь и выполняются по мере возможности. В результате работа "основной" системы хранения не замедляется, но существует риск несохранения данных на втором устройстве в случае аварии.

Выбор варианта синхронизации определяется в каждом конкретном случае.

Зеркалирование серверов баз данных

Большинство приложений, работающих с систематизированными данными, хранит их на серверах баз данных или SQL-серверах. В связи с распространенностью этой технологии для SQL-серверов разработаны решения, обеспечивающие дублирование данных одного сервера на другом.

> ***Примечание***
>
> Дублирование данных SQL-серверов отличается от копирования обычных файлов, поскольку, например, данные имеют структуру и при дублировании их на новый сервер необходимо обеспечить целостность информации, внести одновременно все взаимосвязанные изменения.

Можно назвать следующие преимущества собственных (для SQL-серверов) методов зеркалирования:

- отсутствие необходимости использования дополнительного оборудования (систем хранения данных), дублирование производится по обычной сети передачи данных;
- зеркалирование можно настроить раздельно для каждой базы (а при использовании, например, кластера из двух систем резервируются все базы сервера);
- нет ограничений по оборудованию (например, для кластера нужно использование однотипных систем);
- зеркалирование может быть настроено в режиме "активный — пассивный" (изменения в данные могут вноситься только на первом сервере, на втором — только копия данных) или "активный — активный" (возможны изменения данных на каждом сервере).

Данные между серверами передаются асинхронно. Основной сервер пересылает на вторую систему данные журнала транзакций (протокол внесенных изменений в

данные), второй сервер обрабатывает их и вносит изменения в свою копию данных. Эти операции выполняются по мере изменений базы, но понятно, что в силу, например, проблем передачи по сети и т. д. подобные невнесенные изменения могут накапливаться. В результате второй сервер гарантирует идентичность данных только при нормальном функционировании обоих серверов и сети передачи данных. Поэтому администратору необходимо постоянно контролировать состояние репликации.

Как уже упоминалось, репликация может настраиваться в двух вариантах: "активный — активный" и "активный — пассивный". В простейшем случае данные могут меняться только на одном сервере. Обычно проблем при таком варианте настроек не возникает.

Проблемы появляются, если требуется настроить репликацию изменений в обе стороны. Если изменения возможны на обоих серверах, то неизбежны конфликты: изменения на одном сервере будут противоречить изменениям на другом. Как следует поступить в таком случае, априори неизвестно, существует несколько алгоритмов разрешения конфликтов, выбор конкретного зависит от многих причин, в том числе и от структуры (схемы) данных. Поэтому настройка двусторонней репликации должна выполняться только подготовленными администраторами баз данных, хорошо представляющими себе внутреннюю структуру системы и прикладных данных.

Собственно настройка зеркалирования, например в MS SQL, не представляет сложностей. Предварительно рекомендуется сделать резервную копию данных и включить полный режим восстановления (Full). После чего вызвать мастер создания подписки (в терминологии MS SQL основной сервер называют издателем, а сервер, на который копируются данные, — подписчиком) и следовать его указаниям (выбрать базу, указать подписчика, выбрать алгоритм и т. д.). Обязательно следует проверить состояние репликации и отсутствие очереди невнесенных изменений в журнале.

Снимки баз данных

Серверы SQL позволяют создавать *снимки данных* — мгновенную копию информации. Снимки часто используются, например, при первичном копировании данных на второй сервер. Эта операция выполняется средствами администрирования сервера и не нуждается в дополнительном пояснении.

Настройка клиентских подключений

Прикладные программы традиционно настраиваются на подключение к одному серверу баз данных. В этом случае при отказе основного сервера баз данных автоматического переключения на второй сервер (с копией базы) не происходит. Пользователь получит ошибку программы, которую можно будет устранить только вручную, указав новую строку для подключения к данным. Конечно, это можно отразить в инструкции, но лучше выполнять перенастройку без привлечения пользователя.

Для автоматического переключения на резервный сервер прикладные программы должны быть запрограммированы специальным образом. В случае если для подключения к данным используются клиенты Native client или ADO.NET, то достаточно дописать второй сервер в строку подключения:

```
"Server=srv1; Failover_Partner=srv2; Database=db1"
```

Если разработчик использует клиентов, не поддерживающих переключение на резервный сервер, то решение должно быть предусмотрено в теле программы.

Сетевая балансировка

Одним из вариантов обеспечения отказоустойчивости является организация параллельной работы серверов. Подобное решение, в первую очередь, направлено на балансировку нагрузки, но может рассматриваться и с точки зрения повышения отказоустойчивости. Такой способ хорошо подходит для совместной работы служб DNS, веб-серверов, узлов удаленных рабочих столов и т. п. — везде, где запросы к одному серверу могут быть направлены на другой.

Для распределения нагрузки между серверами используются различные решения. Есть аппаратные балансировщики, распределяющие нагрузку на основе учета сетевого трафика, есть программные решения, учитывающие загрузку сервера и направляющие новые запросы на менее загруженную систему и т. п.

Самый простой способ организовать параллельную работу — использовать балансировку сетевой нагрузки, решение, реализуемое стандартными средствами Windows-серверов. Такая настройка осуществляется мастером, который создает новый виртуальный интерфейс (со своим адресом). Пакеты, отправляемые на этот интерфейс, будут распределяться по реальным интерфейсам серверов.

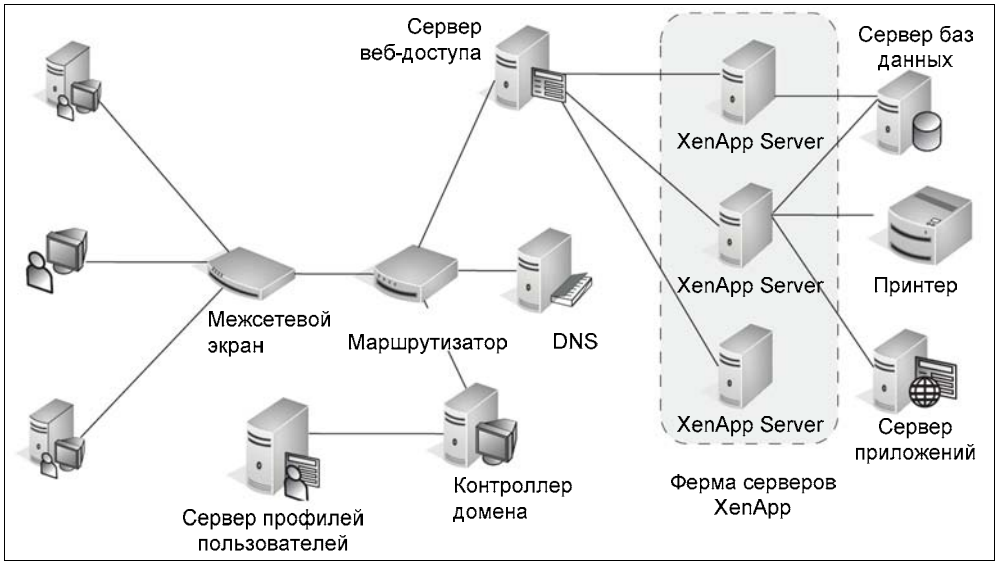


Рис. 13.2. Пример архитектуры фермы серверов Citrix

Настройка веб-фермы реализуется сложнее, поскольку обычно на веб-серверах задействованы различные приложения. Поэтому необходимо уточнить особенности установки по соответствующей документации. Например, установщик для веб-фермы Windows доступен к загрузке с адреса **http://go.microsoft.com/?linkid=9739157**. Как правило, обеспечение серверной фермы требует наличия соответствующей архитектуры системы (на рис. 13.2 показан пример архитектуры серверов Citrix).

Кластерные решения

Кластерные решения на слуху большинства администраторов в качестве основного решения, обеспечивающего отказоустойчивые вычисления. Кластер представляет собой приложение, работающее на нескольких серверах и мигрирующее с одного сервера на другой при возникновении отказа оборудования.

Кластерные решения представлены различными вендорами. Решения во многом сходны, имеют одинаковые преимущества и недостатки. Можно упомянуть Veritas Cluster Server, Fujitsu PRIMECLUSTER, IBM HACMP, HP ServiceGuard, IBM Tivoli System Automation for Multiplatforms (SA MP), Linux-HA, Microsoft Cluster Server (MSCS), NEC ExpressCluster, Red Hat Cluster Suite, SteelEye LifeKeeper и Sun Cluster. Системным администраторам нашей страны, на взгляд автора, наиболее известны решения от Microsoft и Symantec.

Кластер Microsoft

Кластер может быть создан на старших версиях серверов Windows: Windows Server Enterprise Edition или Datacenter. Для создания кластера необходимы два физических сервера (желательно идентичных) и система хранения, позволяющая осуществить одновременное подключение диска к двум серверам. Для подключения системы хранения обычно используется технология FC[1] (fibre channel) или iSCSI. Вообще, к оборудованию, которое предполагается использовать в составе кластера, предъявляются повышенные требования, в общем случае оно должно быть сертифицировано вендором для такого применения (список сертифицированного оборудования доступен через Microsoft Store — **http://go.microsoft.com/fwlink/?LinkID=14201**). Например, для кластеров на основе Windows Server 2003 поддерживалось подключение систем хранения по технологии parallel SCSI, а в версии Windows Server 2008 — только последовательное iSCSI.

Поскольку подключение системы хранения не должно быть единственной точкой отказа, то применяются дублированные подключения. Как правило, для этого необходимы специальные драйверы (например, multipath-драйверы). Рекомендуется также резервирование подключений серверов к сети Ethernet, которое должно быть выполнено по рекомендациям вендора использованных сетевых адаптеров. В результате созданный кластер может выглядеть так, как показано на рис. 13.3.

---

[1] Для передачи данных используется инкапсуляция протокола SCSI в специальный протокол, работающий по волоконному каналу.

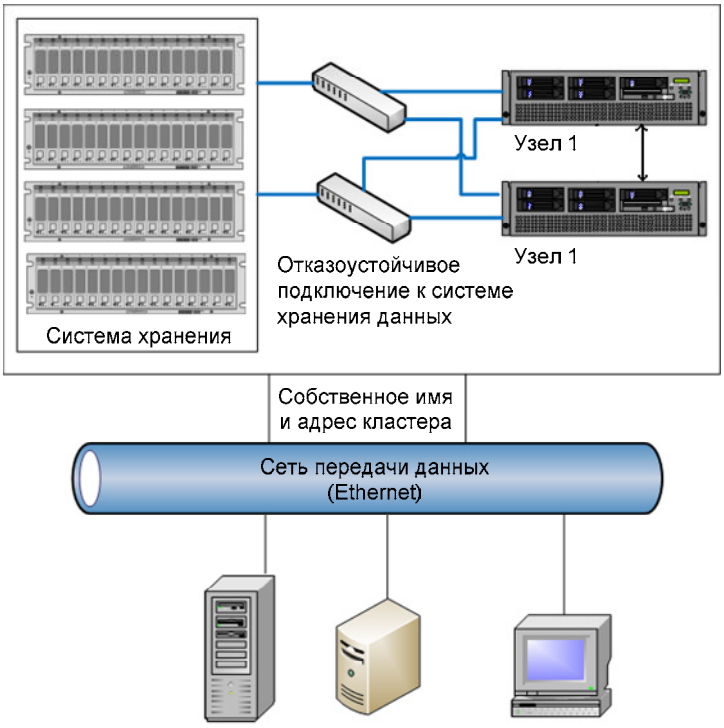


Рис. 13.3. Вариант построения кластера от Microsoft

Серверы, объединяемые в кластер, должны иметь два сетевых интерфейса: один для синхронизации управления (внутренняя сеть, рекомендуется выделять ее в отдельную VLAN), а другой — для полезной нагрузки. Для общего диска, который должен быть создан для кластера, — его называют еще *кворумным диском* (от Quorum, поэтому такому диску принято присваивать букву Q) — достаточно выделить всего 50 Мбайт пространства.

После настройки сетевых интерфейсов и подключения кворумного диска к обоим серверам можно начать создание кластера, запустив соответствующий мастер операций. Особых сложностей эти шаги не вызывают, на серверах создаются службы кластеров, ставятся оснастки управления, кластеру присваивается новое имя и новый сетевой адрес. Именно по этому адресу и имени сервера будут доступны резервированные службы.

Кластер от Microsoft по умолчанию предоставляет резервированные основные службы: общие файлы, службы WINS, DHCP, сертификатов и т. п. Для того чтобы в кластере отказоустойчивым образом работали приложения, они должны быть специально разработаны для кластера. Иными словами, в кластере можно использовать только те приложения, для которых это явно указано. Что касается продуктов Microsoft, то это, в первую очередь, сервер баз данных и почтовый сервер.

При установке приложения в кластер используется специальный вариант запуска программы установки, который создает новый экземпляр сервера (новое имя, но-

вый адрес) и прописывает в настройках службы кластеров параметры резервированных компонентов.

На рис. 13.4 показано окно администратора кластеров с отображением ресурсов программы Symantec NetBackup. Программа установки добавила в кластер ресурсы системы резервного копирования (службы программы, диски для хранения данных и т. д.). В администраторе кластеров можно видеть состояние ресурсов, уточнить узел, на котором в текущий момент работает программа, добавлять или удалять ресурсы и т. п.

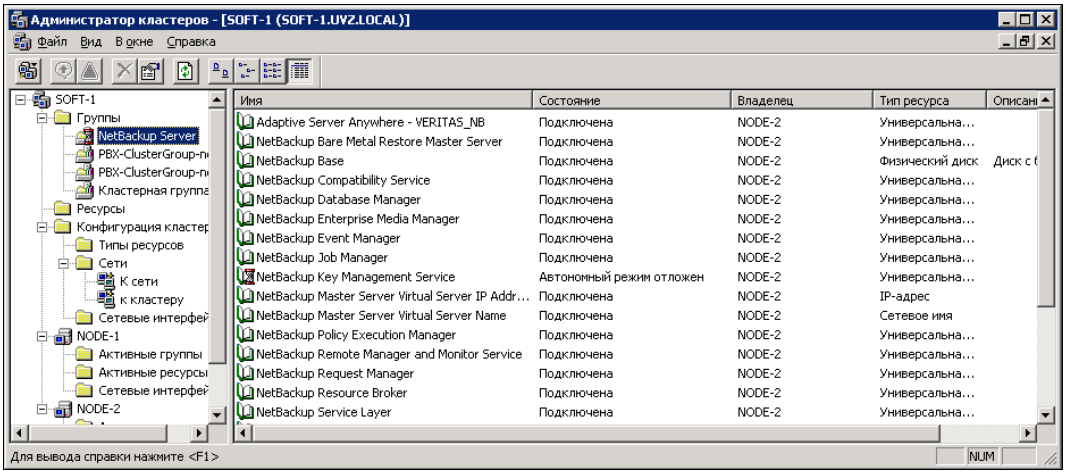


Рис. 13.4. Администратор кластеров для ресурсов NetBackup

В случае отказа узла, к которому подключены ресурсы кластера (выполняется программа), программа запускается на другом узле и все ресурсы мигрируют на него (например, осуществляется переподключение дисков системы хранения).

Понятно, что такое переключение не происходит мгновенно и обслуживание потребителей информационной системы во время этого периода прерывается. Но переключение происходит достаточно быстро (от нескольких секунд до десятков секунд в зависимости от числа ресурсов и сложности приложений), и пользователю обычно достаточно просто повторить операцию, во время которой произошла ошибка.

> ***Совет***
>
> После установки кластера необходимо проверить журналы системы на отсутствие ошибок, проконтролировать состояние ресурсов в консоли администратора и в обязательном порядке протестировать непрерывность обслуживания путем симулирования отказа активного узла кластера.

Veritas Cluster Server

Кластер от Symantec позволяет создавать отказоустойчивые решения не только для Windows, но и для UNIX- и Linux-систем. Это решение широко распростра-

нено у западных пользователей, под него разработано большое количество приложений.

Veritas Cluster Server позволяет создавать как локальные (в пределах локальной сети) кластеры, так и распределенные (в том числе и с подключением только по Интернету). Существуют варианты конфигурации кластера, которые используют разнесенные системы хранения, данные на которых реплицируются средствами самой системы хранения и т. п. (рис. 13.5).

Основное преимущество данного решения — большая распространенность, универсальность и наличие более широкого круга приложений.

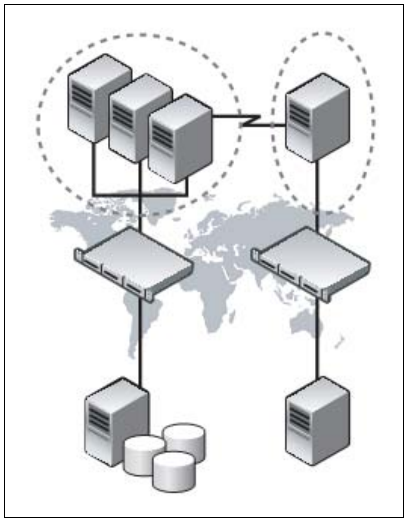


Рис. 13.5. Территориально разнесенный кластер

Территориально распределенные кластеры Microsoft

Кластер на основе серверов Windows можно создать между двумя территориально удаленными площадками. В этом случае на каждой площадке предполагается размещение собственной системы хранения. Приложения будут работать с локальными системами хранения, а данные — реплицироваться между офисами. При этом для синхронизации данных возможно использование различных технологий: собственными ресурсами систем хранения, на файловом уровне (средствами операционной системы) и на уровне приложений (самим приложением, примером такого подхода является сервер Microsoft Exchange).

Решения высокой доступности от Marathon

Примером другого подхода к построению систем высокой доступности являются решения компании Marathon Technologies Corporation, Inc. (**http://www.marathontechnologies.com/**), представившей линейку продуктов everRun. Данный продукт предназначен в первую очередь для построения решений на Microsoft Windows Server, хотя и позволяет защищать XenServer.

Технология everRun предусматривает создание виртуального сервера на основе двух физических серверов (рис. 13.6).

Создание виртуального сервера осуществляет агент everRun, который устанавливается на обычную операционную систему сервера. Оборудование серверов может

отличаться[1], наиболее жесткие требования предъявляются к идентичности процессоров. В отличие от традиционных кластеров решение от Marathon не нуждается в общем файловом ресурсе, однако необходимо наличие нескольких быстрых каналов связи между серверами. Если для "продуктовых" сетевых интерфейсов достаточно линии связи на 100 Мбит, то для межсерверных связей — не менее 1 Гбит, причем задержка при передаче пакета данных не должна составлять более 10 мс. Всего межсерверных каналов должно быть 3: два для синхронизации данных, один для управления. Существует и решение для построения разнесенного виртуального сервера, но оно также предъявляет высокие требования к межсерверному каналу связи.

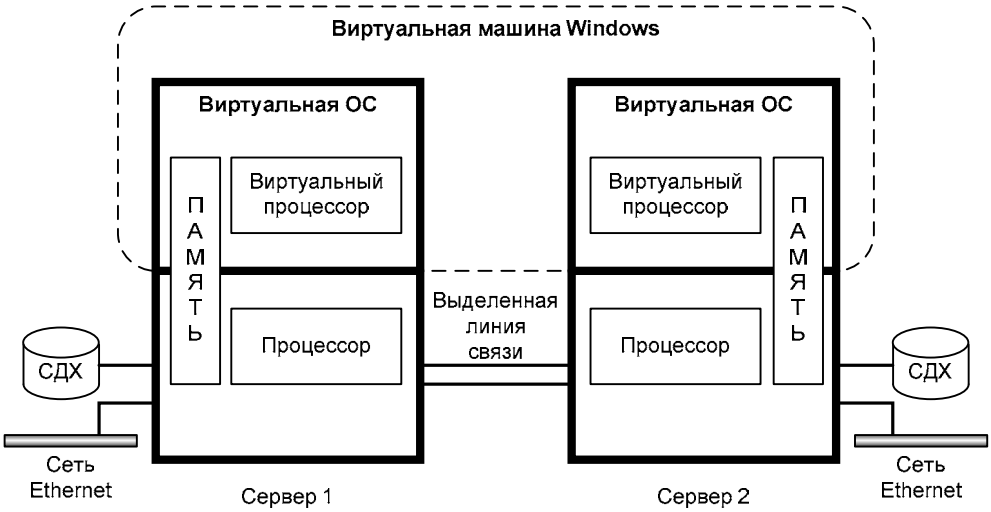


Рис. 13.6. Логическая структура виртуального сервера everRun

Главная особенность технологии состоит в том, как создаются виртуальные компоненты. Они создаются из реальных компонентов на уровне операций. Например, виртуальный диск будет организован из каждого физического диска на каждом сервере на уровне операций ввода-вывода. При выходе из строя одного физического диска виртуальный сервер будет работать с оставшимся диском, а данные будут передаваться на работоспособный диск по межсерверным линиям связи (рис. 13.7 из документации производителя).

Аналогично система будет вести себя при выходе из строя сетевого адаптера и других компонентов. Полный переход вычислений на другой сервер произойдет в случае отказа процессора (оборудования) одного из серверов.

Основное отличие технологий Marathon от традиционных кластеров — это защита не только данных, но и приложений. Если в кластерных решениях будут работать

[1] Например, можно поставить разный объем памяти. Но при этом следует учитывать возможное снижение производительности в случае перехода приложения на резервный сервер из-за недостатков ресурсов оборудования.

только специально разработанные приложения, то технология everRun защитит *любое* приложение Windows. Второй момент: в случае сбоя в традиционном кластере осуществляется откат: приложения стартуют на другом узле с данными, соответствующими моменту перед возникновением отказа. Виртуальный сервер everRun не прерывает вычисления при отказе оборудования.

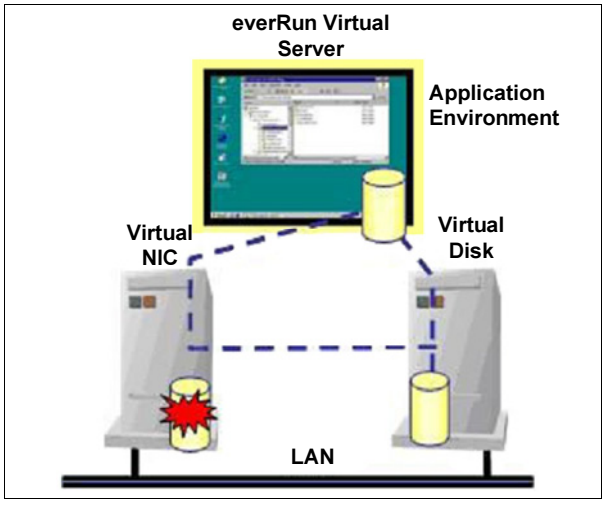


Рис. 13.7. Построение виртуального диска при отказе одного физического диска

Отказоустойчивые решения на виртуальных системах

Кластеры могут быть созданы и из виртуальных систем. Преимущество такого решения состоит в том, что виртуальные машины работают под управлением гипервизора, который может контролировать и управлять их состоянием. В результате появляются такие дополнительные возможности, как миграция виртуальной машины с одного физического сервера на другой *без потери обслуживания*. Такие действия можно осуществить, например, в целях планового обслуживания физического сервера или для экономии электроэнергии (миграция виртуальных машин на один сервер в ночное время с последующим отключением высвобожденных ресурсов) и т. п.

Подобные структуры требуют наличия общей системы хранения, к которой должны иметь доступ как все физические серверы с гипервизорами, так и сервер управления виртуальной структурой. Как правило, компоненты, реализующие такую миграцию, приобретаются за дополнительные деньги.

Ограничения данного решения базируются на требованиях, предъявляемых к таким виртуальным машинам. Это идентичность процессоров (при наличии списка допустимых для внедрения технологий моделей) и наличие аппаратной поддержки виртуализации, необходимость развертывания управляющего центра и создания реше-

ния высокой доступности на существующем кластере высокой доступности, наличие нескольких высокоскоростных сетевых адаптеров (рекомендуется 10 Гбит, но можно использовать и 1 Гбит), наличие системы хранения (диски защищаемых машин автоматически переводятся в "толстый" тип, если они были созданы в режиме "тонких" дисков). Существуют и ограничения по многопроцессорности для систем высокой доступности.

Примечание

Среди особенностей такой технологии от VMware следует отметить, что высокодоступное решение может быть реализовано для любых операционных систем, которые поддерживаются vSphere. А это не только Windows-системы.

ГЛАВА 14

Порядок настройки и определения неисправностей

Эта глава посвящена обслуживанию серверов: от проблем поиска и устранения неисправностей до операций оптимизации системы в целях повышения ее производительности.

Где найти помощь?

Устранение неисправностей в информационной системе практически невозможно без обращения к внешним источникам знаний. Существует несколько ресурсов, где системный администратор может получить "подсказку".

- **Встроенная документация.** Первое, к чему необходимо обратиться при возникновении любой проблемы в работе компьютера, — это встроенная справочная система.
- **Онлайновые базы данных производителей программных продуктов.** Основной объем данных по программным продуктам публикуется на корпоративных сайтах вендоров. К сожалению, размещение документации имеет свои особенности у каждого разработчика. Поэтому лучше изучить структуру сайтов, чтобы в случае возникновения проблем суметь быстро найти нужную информацию.

  Если говорить о документации на продукты Microsoft, то справочная база большей частью локализована — **http://www.microsoft.com/rus/**. Однако без поиска на английском языке, как правило, найти необходимые советы не удается. Примите на заметку еще два ресурса: **http://msdn.microsoft.com/** и **http://technet.microsoft.com/**. На этих ресурсах опубликованы технические статьи о различных продуктах данной компании.
- **Материалы Интернета.** Способы разрешения многих проблем, особенно если таковые случились не только у одного пользователя, можно найти на многочисленных сайтах Интернета. В первую очередь это специализированные сайты, посвященные конкретным прикладным вопросам, сайты известных специалистов, другие серверы, на которых хранятся различные справочные материалы (например, на многих серверах Сети хранятся ответы на типовые вопросы по функционированию системы — FAQ). Такие ресурсы легко находятся при помощи обычных поисковых серверов Интернета.

- **Конференции Интернета.** Если вы не нашли описания своей проблемы на таких узлах Сети, то можно обратиться с соответствующим вопросом в специализированную телеконференцию. Хотя не стоит надеяться, что вы гарантированно получите ответ, но обращение в конференцию является одним из наиболее эффективных способов получения необходимой помощи.

  Примечание

  Подобные конференции обычно поддерживаются как на сайтах разработчиков, так и на других ресурсах, посвященных компьютерной тематике. Определенную помощь может оказать изучение списка конференций, поддерживаемых новостным сервером вашего провайдера.

- **Техническая поддержка производителя.** Крупные производители программного обеспечения имеют специализированные службы для оказания технической поддержки. Обращение в такую службу обычно помогает существенно снизить время решения возникшей проблемы. Особенно, если уровень подготовки технических специалистов на предприятии недостаточен для квалифицированного сопровождения инфраструктуры.

  Обычно подобная поддержка является платной услугой, причем уровень цен не позволяет заказывать ее малым и средним организациям. Постепенно начинает развиваться сервис коммерческого предоставления технической поддержки третьими фирмами. К сожалению, в этом вопросе очень много субъективных факторов, влияющих на качество такого сопровождения. Поэтому решение на приобретение данной поддержки должно приниматься индивидуально с учетом анализа опыта других предприятий.

Неисправность не может не возникнуть

Отказ в обслуживании может возникнуть из-за неисправности любого элемента системы: повреждения кабельной системы, неполадок в работе коммутирующих устройств, выхода из строя узлов компьютера, зависания операционной системы, ошибок программного обеспечения бизнес-уровня и уровня приложений и т. п.

Продумывая меры по обеспечению непрерывной работы информационной системы, следует учитывать все возможности: в реальной жизни происходят самые неожиданные отказы и необходимо встречать их подготовленными.

Будьте готовы к худшему. Будьте готовы к тому, что неисправность произойдет именно тогда, когда вы ее не ждете, и из строя выйдет самый надежный узел или программный продукт.

Общие рекомендации по процедуре решения проблем

Приведем несколько банальных советов, которые все знают, но обычно не спешат выполнять по тем или иным причинам.

Имейте план действий

Для успеха большое значение имеет наличие системности в действиях администратора.

В первую очередь соберите всю доступную информацию о событии. Проверьте кажущиеся очевидными факты: включено ли оборудование, горят ли индикаторы состояния, не появились ли дополнительные шумы и т. п.

Затем систематизируйте информацию о системе:

- ❒ обеспечьте доступ к журналам (журнал событий Windows, syslog для UNIX-систем, журналы приложений);
- ❒ уточните время возникновения проблемы, какие операции выполнялись в этот момент;
- ❒ выясните, проводились ли изменения в настройках системы перед возникновением проблемы, менялось ли оборудование и т. п.;
- ❒ проанализируйте ситуацию: встречались ли наблюдаемые симптомы ранее, были ли сходные отказы, которые могли привести к текущей проблеме, и т. п.;
- ❒ если ошибка наблюдается у пользователя, переговорите с ним, уточните ситуацию, попытайтесь воспроизвести проблему.

Обеспечьте доступность специалистов службы поддержки

Обратите внимание, чтобы пользователи и специалисты знали, куда обратиться со своей проблемой в любое время (даже если работа происходит в выходной день или в режиме удаленного доступа). Например, такую инструкцию можно опубликовать на внутреннем сайте организации и автоматически направлять на нее обозреватели Интернета при их старте, можно включить в первое письмо приветствие, которое будет сформировано при подключении к электронной почте, можно отразить в небольшой инструкции, которая будет выдаваться каждому пользователю при начале работы и т. д.

Формализуйте процесс

Оптимальная работа над решением проблемы должна быть систематизирована. Процесс решения необходимо строить в несколько этапов:

- ❒ сначала нужно четко описать проблему (что случилось);
- ❒ затем проверить ее наличие (подтвердить);
- ❒ после чего следуют собственно анализ причин возникновения ошибки, выработка решения и осуществление необходимых операций;
- ❒ после реализации исправления должна быть проведена проверка: сначала самим администратором, а потом и обратившимся пользователем;
- ❒ завершать инцидент должно его формальное закрытие: если пользователь остается не удовлетворен решением, то работа над его заявкой должна быть продолжена.

Решения администратора должны учитывать текущие задачи пользователя. Например, если проблема возникла с компьютером во время подготовки срочного отчета для руководства и восстановление системы сопряжено со срывом сроков задания, то следует временно предоставить пользователю другой компьютер, перенеся на него вручную исходные файлы, а только потом приступить к ликвидации аварии.

Желательно иметь форму заявки на неисправность, по которой собирать исходную информацию о проблеме. Обычно сбор первичной информации происходит по следующей форме:

- кто обращается с заявкой (имя пользователя, параметры его учетной записи, имя компьютера и место его размещения);
- описание неисправности (когда обнаружена, внешние признаки, есть ли аналогичные проблемы у других пользователей и т. п.);
- какие сообщения о неисправности формирует система, точные их параметры (например, текст предупреждения, выведенного на экран);
- когда в последний раз система правильно выполняла аналогичную операцию;
- какие изменения в системе были проведены с момента последней удачной работы (включая установку новых компонентов оборудования, программных заплаток, операций обновления, любую перенастройку и т. п.);
- критичность возникшей проблемы для пользователя (влияние на соблюдение сроков работы), возможность временных решений.

В зависимости от содержания обращения администратор будет пытаться конкретизировать ответы пользователя или просить сообщить дополнительную информацию. В качестве примера приведем такое обращение:

"Компьютер bla-bla-bla (ОС Windows 7), находящийся в комнате 234, не может печатать документы MS Word 2010 на принтере MP1120 в комнате 230. Вчера проблема отсутствовала. На другой принтер (в комнате 236) печатать можно. В компьютер никакие изменения не вносились. Есть ли проблемы с печатью на этот принтер у других — пользователь не знает".

Из обращения понятно, что проблема не является критичной (вносит только неудобства в работу, документы можно напечатать на другом оборудовании). Администратор может рассказать пользователю о ближайших своих действиях (например, как скоро он выяснит, есть ли проблема у других пользователей) и сообщить первичный срок, когда он может проинформировать о том, как быстро проблема сможет быть устранена.

Для сбора обращений (и последующей организации работы с ними) можно использовать свободные решения ServiceDesk, которые легко найти в Интернете. Это поможет, во-первых, формализовать обращения (точно фиксировать дату обращения, время реакции, устранить лишние эмоции и обвинения и т. д.), во-вторых, даст инструмент контроля качества обслуживания и объективные показатели отчетности по работе администратора.

Примечание

Следует периодически уделять внимание анализу обращений, пытаться выявить те или иные тенденции. Если обращения связаны, например, с некоторыми типовыми ошибками, то, может быть, имеет смысл организовать дополнительное обучение пользователей, изменить какие-либо процедуры и т. п., что в результате снизит нагрузку на администраторов службы поддержки.

Обеспечьте запасные детали

Любая информационная система нуждается в запасных инструментах и принадлежностях (ЗИП). В идеале состав ЗИП должен рассчитываться при создании системы, но обычно для этого не хватает показателей надежности и ЗИП составляется в процентах от объема (например, 10% — значение зависит от практики, принятой на конкретном предприятии), но не менее одного элемента каждого типа.

Следует учесть, что запасные детали к оборудованию, находящемуся на эксплуатации более 3-х лет, приобрести становится весьма сложно. Часто для этого необходимо наличие сервисных контрактов, стоимость которых за 3—5 лет уже начинает превышать стоимость исходного оборудования.

Поэтому при приобретении оборудования нужно одновременно покупать запасные жесткие диски, блоки питания, соединительные кабели и т. п. Не говоря уже о том, что у системного администратора должен быть запас таких расходуемых компонентов, как клавиатуры, мыши, патч-корды и т. д.

Обдумайте заранее свои действия

Администратор должен быть готов к возникновению любой нештатной ситуации и иметь план обеспечения непрерывности функционирования информационной системы.

Подобный план представляет собой перечень мероприятий, которые необходимо осуществить в случае отказа оборудования или в иной нештатной ситуации. В нем должно быть определено, например, на какое оборудование перенести серверы в случае его отказа? Где должны храниться дистрибутивы, чтобы восстановление могло быть проведено дежурным оператором? Какова должна быть процедура восстановления данных? Описав все предполагаемые аварийные ситуации и пути их устранения, вы сможете рассчитать ожидаемое время восстановления системы в каждом случае отказа.

Именно при составлении плана обеспечения непрерывной работы можно оценить стоимость восстановления системы при различных отказах и для некоторых случаев изначально отказаться от возможности оперативного восстановления. Достаточно соотнести затраты на поддержание отказоустойчивости с потенциальными потерями от отказа в обслуживании и принять взвешенное решение.

Если такой план будет утвержден руководством, то, с одной стороны, вы получите защиту от неоправданных требований немедленного восстановления работы, поскольку для каждой ситуации достижимые временные рамки будут четко оговоре-

ны. С другой стороны, этот план станет инструкцией, что нужно делать в аварийной ситуации.

Поиск неисправностей

В персональных версиях Windows постепенно увеличивается количество инструментов, предназначенных для самостоятельного поиска рекомендаций по устранению проблем компьютера.

При настройках по умолчанию, при наличии подключения к Интернету в случае возникновения ошибки система сформирует о ней отчет, автоматически отправит его вендору (запросив ваше согласие) и покажет рекомендации по устранению ошибки, если для аналогичных событий в базе данных имеются нужные описания.

Информация о надежности системы

Программа **Системный монитор** в Windows может быть использована для формирования отчета о надежности компьютера. Для этого необходимо открыть ее, включить отображение панели действий (если она была выключена), отметить в левой части окна программы строку **Средства наблюдения** и в панели действий перейти к **Средства наблюдения | Дополнительные действия | Просмотр сведений о надежности системы**. На экране появится окно Монитора стабильности, в котором схематично будет отображен уровень надежности системы и перечислены основные события (рис. 14.1).

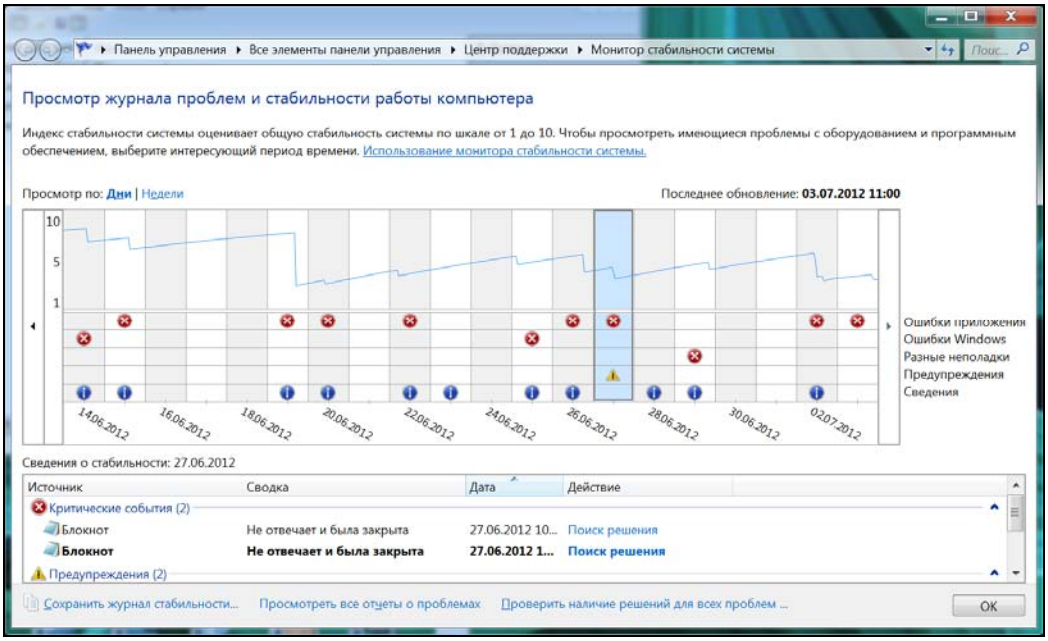


Рис. 14.1. Монитор стабильности системы Windows

Примечание

Другой способ вызова программы — ввести в строке поиска кнопки **Пуск** слово "стабильность" (или "надежность"), в результатах поиска появится строка **Просмотр журнала надежности системы**, по которой можно открыть данную программу.

На графике отображены события, влияющие на надежность системы. Красным цветом отмечены те, которые привели к ее снижению. Отметив желаемое событие на графике, в списке событий вы увидите описания причины снижения уровня надежности и ссылку на дополнительные данные.

Данное средство удобно при качественном анализе состояния компьютера, который не находится под постоянным контролем администратора (например, рабочего места пользователя при возникновении каких-либо проблем).

Монитор ресурсов и производительности

Если попытаться запустить задачу **Системный монитор** с ключом `/report` (`perfmon /report`), то откроется приложение **Монитор ресурсов и производительности**, которое приступит к сбору данных и формированию отчета (рис. 14.2).

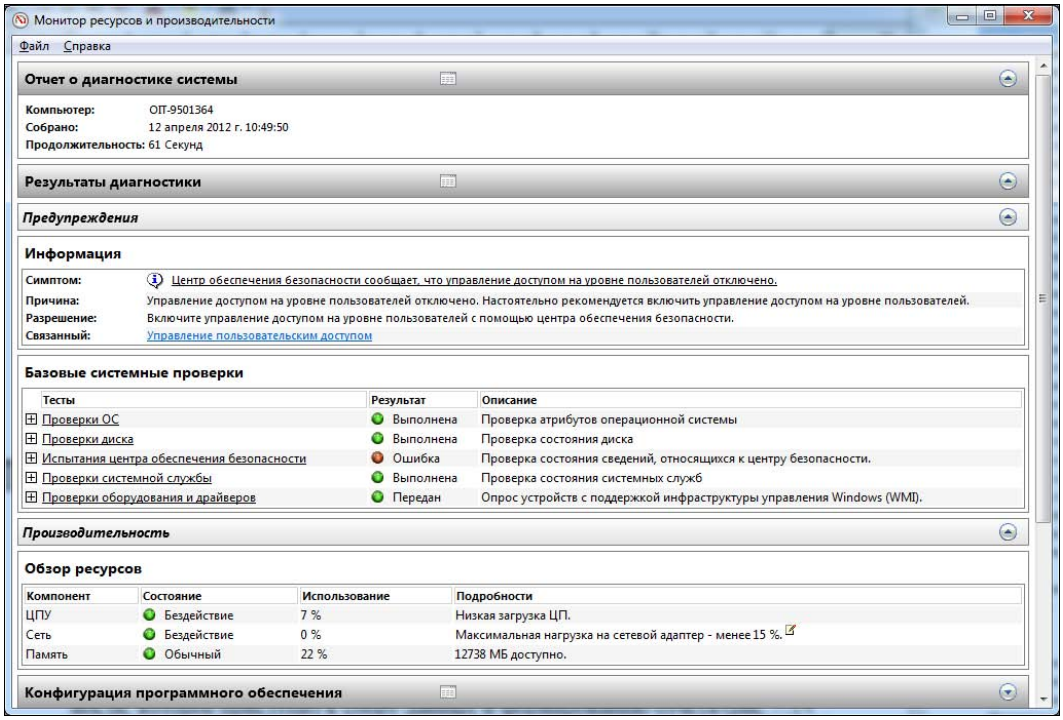


Рис. 14.2. Приложение **Монитор ресурсов и производительности** Windows

В отчете программы представлены анализ результатов диагностики, краткие рекомендации и ссылки, по которым вы можете получить необходимые подсказки.

Подобная информация крайне полезна для первичного знакомства с системой.

Мастер диагностики Windows

В Windows 7 в Панели управления присутствует задача **Устранение неполадок** (рис. 14.3), которая запускает несколько мастеров по диагностике конкретных проблем (сетевого подключения, интерфейса Aero и т. п.).

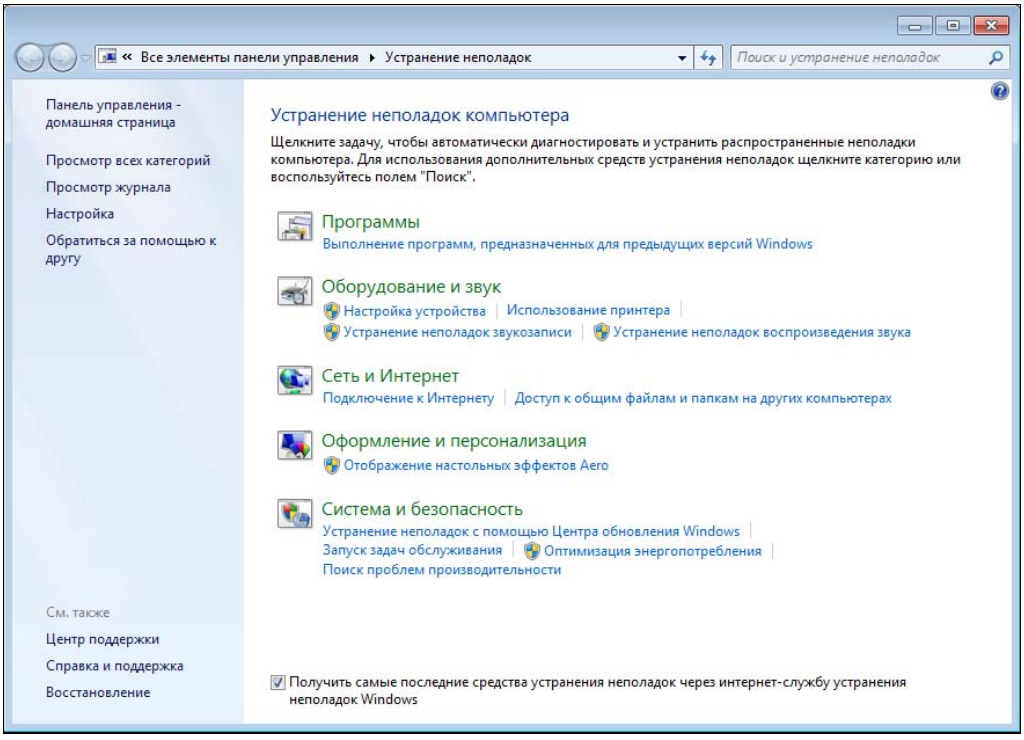


Рис. 14.3. Задача **Устранение неполадок**

Конечно, большинство рекомендаций мастера заключаются в советах, аналогичных фразе *"Проверьте подключение сетевого кабеля"*, но разработчик постоянно обещает расширять функциональность таких мастеров за счет импорта подготовленных пакетов из Интернета.

Запустить мастера диагностики можно и при помощи PowerShell.

> ***Примечание***
>
> Поскольку командлет можно запустить удаленно, это означает возможность выполнить подобную операцию на компьютере пользователя администратором, не отходя от своего рабочего места.

Пакеты диагностики расположены в папке C:\Windows\diagnostics\system, по названию вложенных папок легко определить назначение соответствующего пакета.

Мастер диагностики PowerShell нужно запускать в два этапа: сначала командлетом Get-TroubleshootingPack получить объект устранения неполадки, а потом при помощи Invoke-TroubleshootingPack выполнить диагностику. Приведем краткий при-

мер запуска (выбран вариант запуска диагностики службы поиска; показаны сообщения мастера на первом шаге операций):

```
PS C:\> $a = Get-TroubleshootingPack -path C:\Windows\diagnostics\system\Search
PS C:\> Invoke-TroubleshootingPack -pack $a

Какие проблемы были замечены?
Выберите все подходящие варианты.

[1] Файлы не отображаются в результатах поиска.
[2] Сообщения электронной почты не отображаются в результатах поиска.
[3] Поиск или индексация замедляет работу компьютера.
[4] Проблемы нет в списке (опишите проблему на следующей странице).
[5] Ничего из перечисленного

[?] Справка
[x] Выход
:
```

Некоторые мастера диагностики выполняются без запроса информации от пользователя. Далее приведен пример проверки электропитания, в ходе которого выполняется несколько тестов и просто сообщается итоговый результат:

```
PS C:\> $a = Get-TroubleshootingPack -path
C:\Windows\diagnostics\system\Performance
PS C:\> Invoke-TroubleshootingPack -pack $a
Проверка режима электропитания...
Поиск вошедших в систему пользователей...
Проверка режима программируемого ввода-вывода на диск...
Проверка на наличие нескольких антивирусных программ...
Проверка списка автозагрузки...
Проверка SuperFetch...
Проверка параметров визуальных эффектов...

Проблемы не обнаружены
```

Анализатор соответствия рекомендациям

В состав Windows Server 2008 R2 включен анализатор соответствия рекомендациям (Best Practices Analyzer, BPA), который проверяет настройки сервера на соответствие рекомендациям вендора. Вызов BPA осуществляется из консоли управления сервером. Программа выполняет проверки конфигурации и предлагает советы по устранению найденных недостатков (рис. 14.4).

Программа не вносит никаких изменений в систему, а только выполняет проверку конфигурации. Результаты анализа отображаются в виде списка проблем и рекомендаций по их устранению. Причем рекомендации содержат ссылки на соответствующие инструкции.

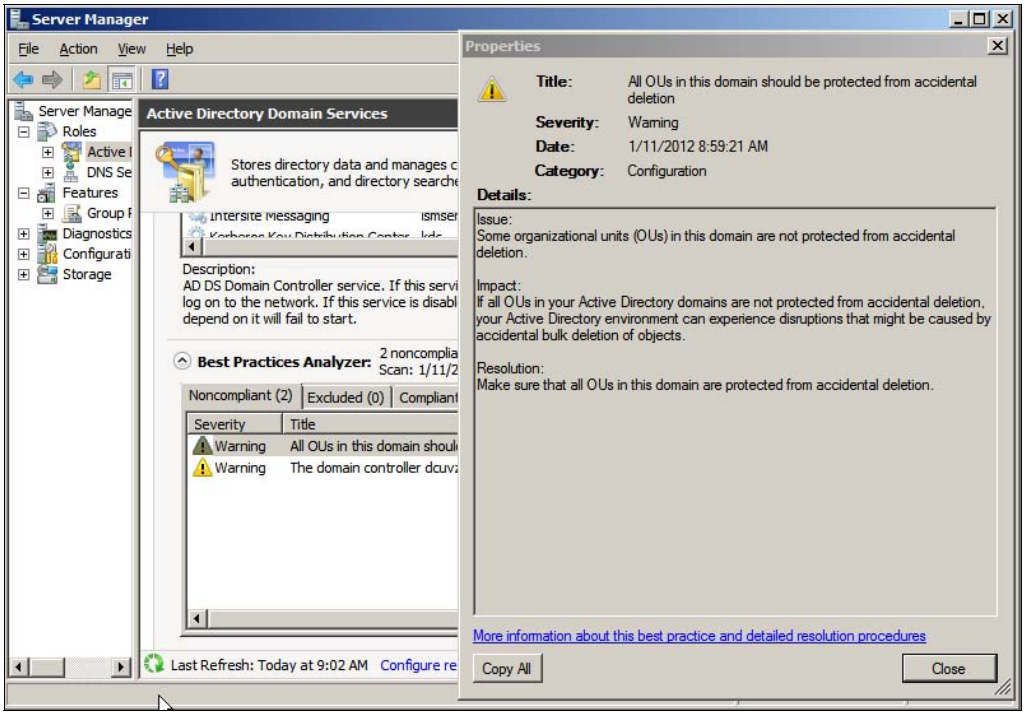


Рис. 14.4. Средство анализа соответствия рекомендациям службы каталогов

Средство анализатора соответствия рекомендациям существует для различных служб: для проверки службы каталогов (как показано на рисунке), серверов DHCP и DNS, файлового сервера, Exchange Server, сервера баз данных (MS SQL), Hyper-V и т. д.

BPA фактически представляет собой сценарии PowerShell. Поэтому это средство можно запускать непосредственно в этой оболочке, в том числе и на удаленных системах. Для работы с BPA применяются два командлета: Get-BPAModel и Invoke-BPAModel. Используются они по такому же принципу, как и локальные мастера диагностики: сначала нужно получить объект, а потом использовать его для анализа. Далее показан пример запуска анализатора, когда производится анализ с использованием всех установленных на компьютере описаний шаблонов:

```
PS C:\> Get-BPAModel -Invoke-BPAModel

ModelId Success Detail
------- ------- ------
Microsoft/Windows/DirectoryServices True (InvokeBpaModelOutputDetail)
Microsoft/Windows/DNSServer True (InvokeBpaModelOutputDetail)
```

Компоненты BPA можно установить и на Windows 7, соответствующие рекомендации можно уточнить при необходимости на сайте вендора операционной системы.

Средства диагностики Windows Server 2008 R2

В Windows Server 2008 R2 встроены средства диагностики основных служб. Запускаются они из консоли управления соответствующими службами и формируют отчет, аналогичный изображенному на рис. 14.5.

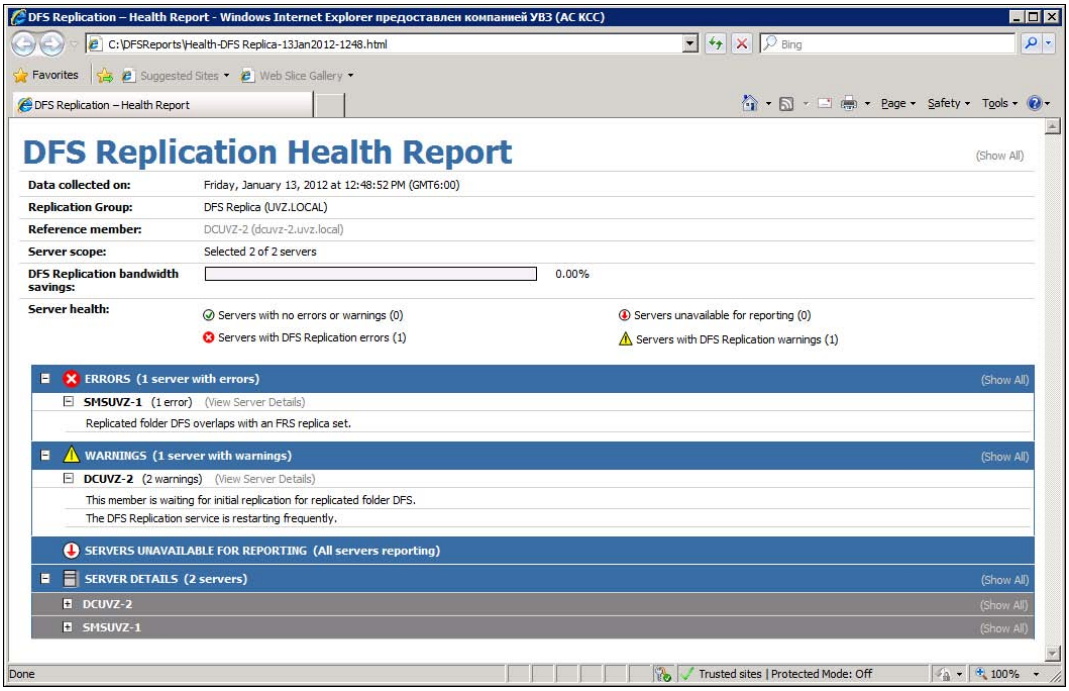


Рис. 14.5. Отчет состояния службы репликации распределенной файловой системы

Fix it

На сайте Microsoft представлен инструмент для устранения типичных ошибок — Fix it (**http://support.microsoft.com/fixit/ru/**, рис. 14.6).

Для его использования нужно зайти на сайт поддержки по указанному адресу, найти соответствующую неисправность и загрузить программу, автоматически восстанавливающую работоспособность системы. При этом решения можно искать как по темам (например, проблемы с Microsoft Office), так и категориям (проблемы с отправкой факсов). В полученном списке решений необходимо найти нужную позицию и запустить ее.

Обратите внимание, что данное решение доступно не только для систем, подключенных к Интернету, но и может быть применено автономно. Имеется версия Microsoft Fix it portable, которая загружает на сменный носитель необходимые для автономной работы данные (около 40 Мбайт). После чего для устранения неполадки достаточно перенести файлы на проблемный компьютер и запустить поиск решений.

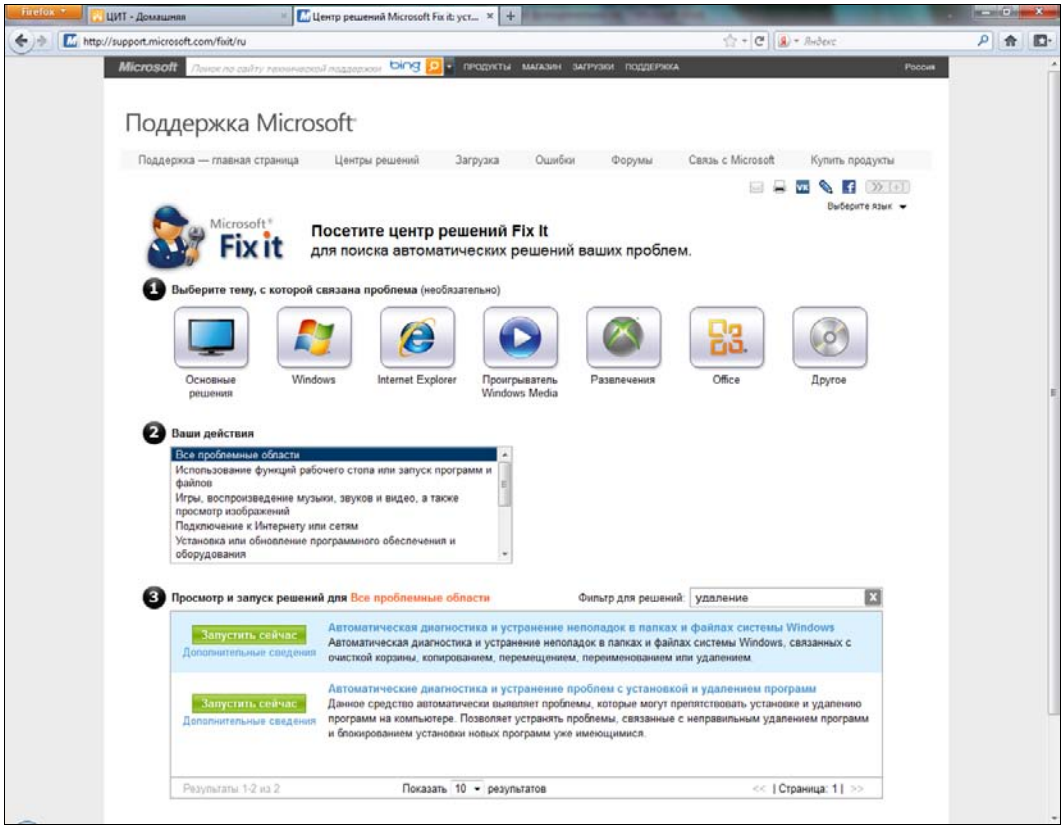


Рис. 14.6. Средство устранения ошибок — Fix it

Анализ журналов системы

Сведения о неисправности как оборудования, так и программного обеспечения практически всегда отражаются в журналах системы или программного обеспечения. Для Windows основные протоколы — это журналы системы, приложений и безопасности, для *nix-систем — журнал syslog и журналы приложений.

Поскольку на ведение журналов затрачиваются вычислительные мощности системы, то по умолчанию (в случае нормальной работы) в журналах фиксируются только основные события и критические оповещения. Часто для анализа причин неисправности такой информации недостаточно, и администраторам приходится настраивать более высокий уровень детализации записываемых событий, задействовать новые журналы.

> ***Примечание***
>
> После устранения неисправности необходимо восстановить исходный уровень детализации журналов, чтобы не использовать нерационально ресурсы системы на запись информации о событиях.

Средства просмотра журналов системы

В Windows для просмотра журналов событий применяется специальная программа **Просмотр событий** (рис. 14.7), вызов которой выполняется через **Панель управления | Административные задачи | Просмотр событий**.

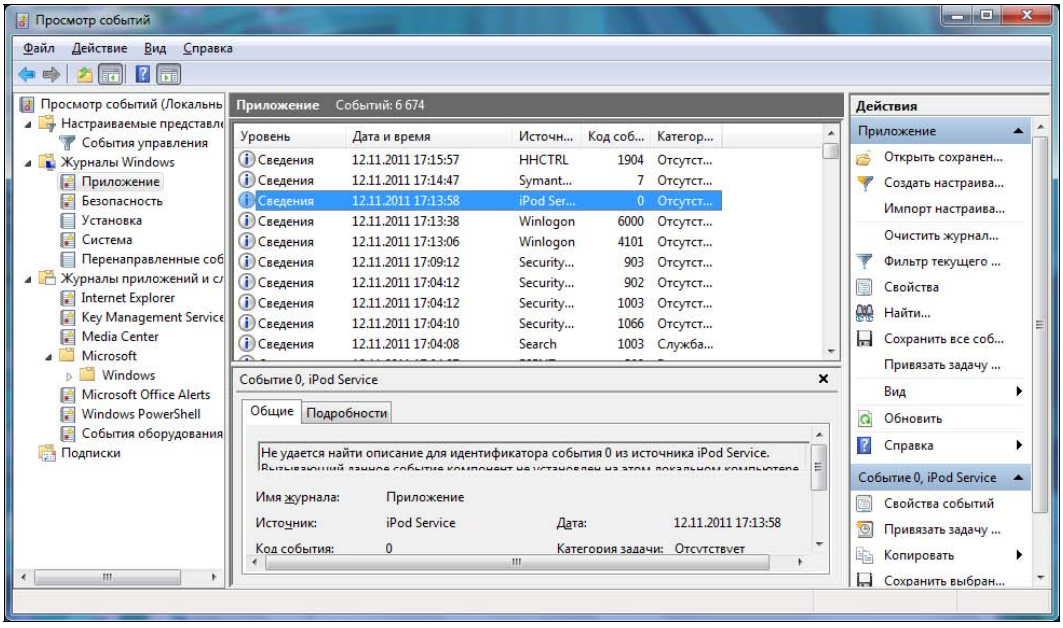


Рис. 14.7. Средство просмотра журнала событий в Windows 7

После запуска программы и выбора нужного журнала в окне будет показан список событий. Описание для каждого события предоставляет краткие характеристики того, что произошло в системе. Дополнительная расшифровка кодов событий приведена в документации Resource Kit, но анализ ситуации в общем случае невозможен без обращения к онлайновой справочной базе Microsoft.

Поскольку в журнале событий могут содержаться десятки тысяч записей, то программа просмотра позволяет отфильтровывать записи по любому критерию и выполнять поиск нужного события. Например, можно отфильтровать события, вызванные только одним процессом или исключить отображение информационных сообщений и т. п.

> ***Примечание***
>
> Информация о событиях в программе просмотра Windows не меняется в режиме реального времени. Для обновления следует выполнить команду **Обновить** (нажать клавишу <F5>).

В *nix-системах события записываются в текстовые файлы. Как правило, журналы создаются в папке /var/log: в самой папке находятся системный журнал syslog, журнал сообщений dmesg, журнал почтового клиента mail и др., некоторые программы

создают свои подпапки, например, веб-сервер (папка apache2), пакет обновлений apt (папка apt) и т. д.

Читать их удобно при помощи команды `tail`, позволяющей отображать события в реальном режиме времени. Для фильтрации событий используется перенаправление потоков в команду `grep`, которая и фильтрует вывод по задаваемым критериям. Так, следующий пример приводит к отображению на экране в реальном режиме времени событий, записанных в системном журнале Ubuntu демоном dhcpd (для удобства приведено только 4 строки вывода):

```
$ tail -f /var/log/syslog | grep dhcpd
Nov 12 21:25:57 test dhcpd: DHCPINFORM from 192.168.10.18 via eth0
Nov 12 21:25:57 test dhcpd: DHCPACK to 192.168.10.18 (00:04:75:c6:8d:ed) via
eth0
Nov 12 21:27:43 test dhcpd: DHCPINFORM from 192.168.10.14 via eth0
Nov 12 21:27:43 test dhcpd: DHCPACK to 192.168.10.14 (00:1e:8c:9b:9c:10) via
eth0
...
```

Чтобы одновременно наблюдать за событиями двух или более журналов в *nix, используется возможность одновременного открытия нескольких консолей: в каждой консоли запускается просмотр одного журнала, а переход к другому реализуется переключением между консолями.

Централизованное ведение журналов

Системным администраторам приходится анализировать данные журналов нескольких серверов. Удобно, если эта операция будет выполняться из одной консоли.

В этих целях в системах Windows 7/Vista/Server 2008 R2 присутствует возможность настройки сбора событий с различных компьютеров. Для этого используется опция **Подписка**.

При создании подписки (рис. 14.8) необходимо указать, с каких систем будут собираться данные, настроить фильтры (какие события копировать), назначить журнал, в который будет осуществляться запись. Так же нужно настроить параметры учетной записи, которая будет иметь доступ к журналу на удаленном компьютере. Кроме того, надо еще выполнить некоторые настройки на удаленной системе (см. онлайновую справку). Подписку можно "оформлять" как для компьютеров домена, так и рабочей группы (особенности настройки в этом случае следует уточнить по справочной документации).

В реальных сетях еще долго будут эксплуатироваться компьютеры с Windows XP или Windows Server 2003, режим подписки с которыми не работает. В этом случае можно использовать сценарий EVENTQUERY.vbs из состава Windows Server 2003, который позволяет вывести события как с локального, так и с удаленных компьютеров, используя необходимые фильтры (по дате, по номеру события, типу и т. п.). Правда, в отличие от режима "Подписка" данный сценарий каждый раз проводит анализ событий на удаленных системах и возвращает отобранные события.

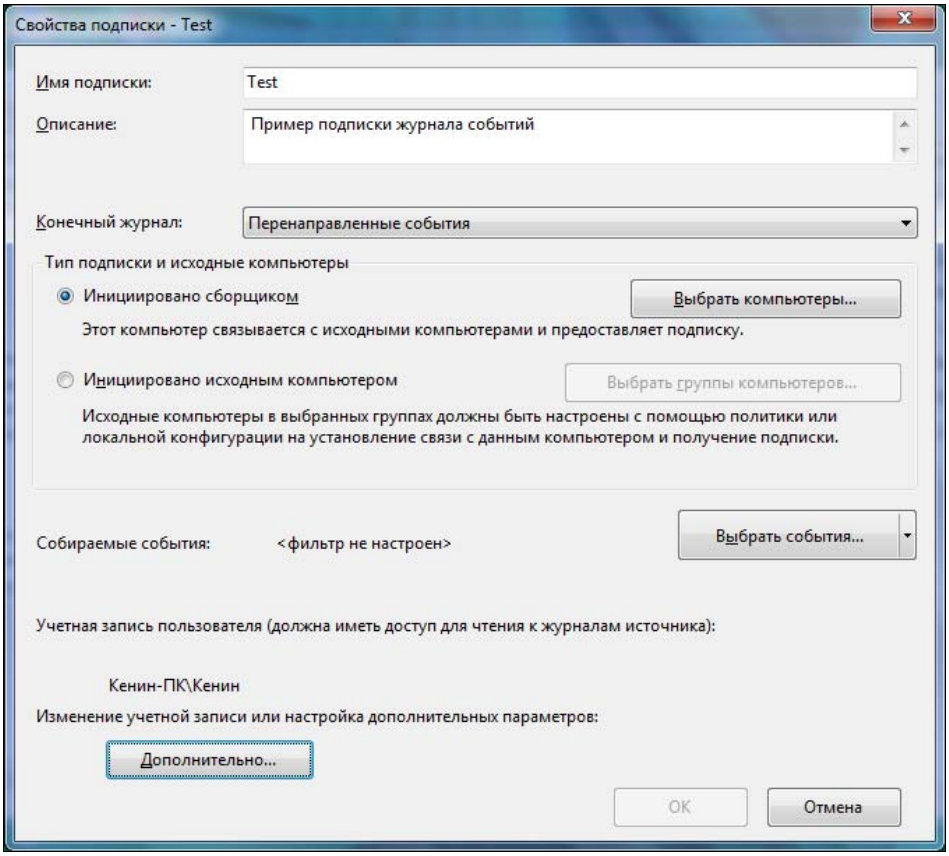


Рис. 14.8. Настройка подписки в Windows 7

При желании использовать графический интерфейс при анализе журналов можно обратиться к специальной утилите — EventCombMT, бесплатно загружаемой с сервера Microsoft (рис. 14.9).

Утилита EventCombMT позволяет просматривать данные протоколов работы сразу нескольких систем. Администратор может задать желаемые условия поиска (номер события, имена компьютеров для анализа, диапазон дат и т. п.). Утилита содержит несколько встроенных описаний условий поиска, например, по ошибкам DNS, FRS, жестких дисков, службы каталогов. Результаты работы программа сохраняет в виде текстовых файлов.

> ***Примечание***
>
> Существует много коммерческих средств, предназначенных для централизации сбора и анализа событий журналов нескольких систем. При желании найти эти решения не составит особого труда.

События журналов важны и в случае разбора инцидентов. Поскольку злоумышленник будет пытаться очистить журналы атакуемой системы, то при предъявлении повышенных требований к хранению событий последние необходимо копировать на выделенный сервер.

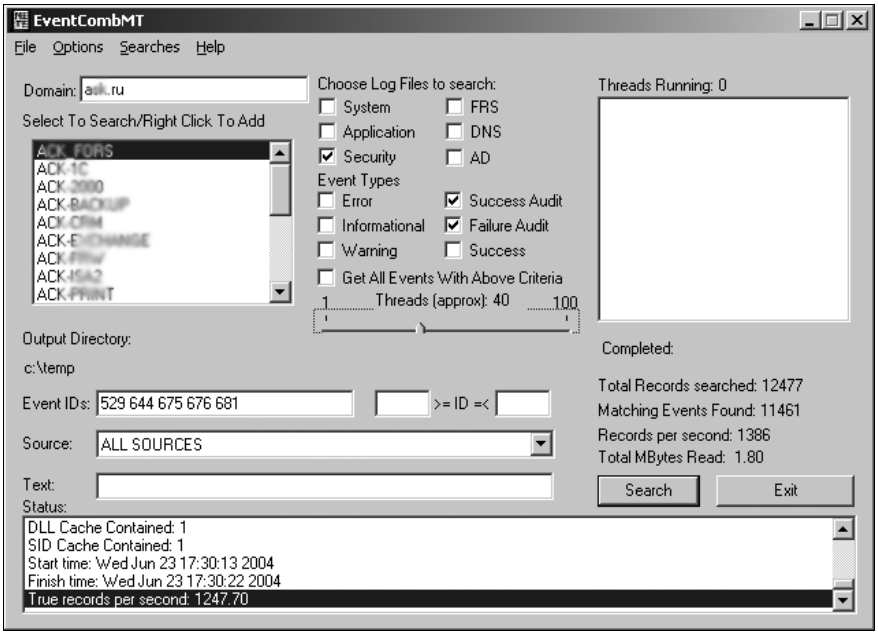


Рис. 14.9. Окно утилиты EventCombMT

При выборе бесплатных решений можно использовать запускаемые по определенному графику специализированные утилиты для чтения журналов. Конечно, удобнее применить коммерческие программы, которые могут централизованно хранить необходимые данные.

На рис. 14.10 представлен пример такой программы — EvenTrigger от компании IS Decisions (**www.eventrigger.com**). Программа позволяет запускать сценарии в соответствии с возникающими событиями, отправлять сообщения на пейджер или по электронной почте, заносить данные в ODBC-базы. С программой поставляется несколько предварительно настроенных триггеров (на события остановки служб, неудачного входа в систему, события печати и т. п.).

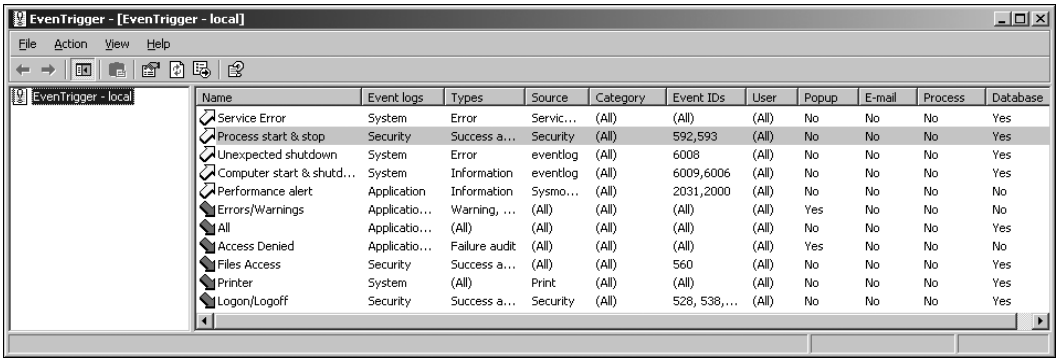


Рис. 14.10. Окно программы EvenTrigger

Подобные функции реализованы и во многих других программах, доступных системным администраторам (GFI LANGuard Security EventLog Monitor, Microsoft Operation Management Server и т. д.).

Изменение детализации протоколирования

Для многих задач (служб) через реестр системы можно изменить детализацию протоколирования, в том числе включить или отключить его полностью. Соответствующие рекомендации, при необходимости, можно найти на сайтах изготовителей программного обеспечения.

> ***Примечание***
>
> Файлы протоколов достаточно сложно анализировать вручную. Существуют различные программы, позволяющие автоматизировать данную операцию, например, отфильтровать и отсортировать записи по каким-либо критериям и т. п. Такие программы легко найти как в свободных ресурсах Интернета, так и у самих разработчиков ПО (например, утилита LogParser от Microsoft).

В *nix-системах детализация протоколирования устанавливается в соответствующих конфигурационных файлах программ. Это текстовые файлы, обычно настроенные на минимум протоколирования. Например, в конфигурации samba[1] присутствует строка `syslog = 0`. Чтобы перейти к более подробной записи, достаточно сменить 0 на большее значение (до 10, чем больше, тем подробнее будет вестись журнал) и перезапустить службу. Рекомендации по изменению уровня протоколирования (какие события будут включены в журнал на каждом уровне) обычно описаны в сопроводительной справочной документации.

Другой способ включения расширенного протоколирования в *nix-системах заключается в запуске соответствующих программ в режиме отладки *(debug)*. Для этого необходимо запустить процесс с определенным ключом и параметром уровня детализации. Сведения о возможности такого старта так же приводятся в справочной документации программы. Например, для упоминавшегося уже демона samba нужно использовать ключ `-d` с последующим указанием уровня протоколирования:

```
smbd -d <уровень>
```

Установка триггеров на события протоколов

Основным способом мониторинга систем на основе Windows является реагирование на события журналов. Подобные настройки можно легко сделать и собственными силами, если представлять контролируемый объем.

В Windows 7/Server 2008 настройку триггеров можно сделать в программе просмотра событий. Достаточно выделить событие, которое будет использовано в качестве образца, и в столбце задач по ссылке **Назначить задачу...** запустить мастер операций (рис. 14.11).

---

[1] Программа samba обеспечивает реализацию общего доступа к файловым ресурсам и принтерам, совместимого с аналогичным в системах Windows.

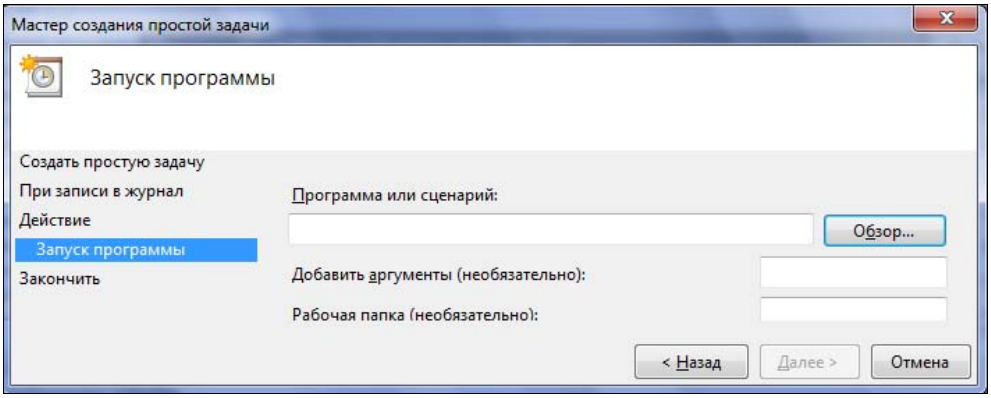


Рис. 14.11. Мастер создания простой задачи на возникновение события в журнале

Мастер позволяет назначить для события отправку сообщения, в том числе и электронной почты, либо произвольную программу.

Для предыдущих версий Windows для создания триггеров можно использовать сценарии. В Windows Server 2003 имеется команда, которая позволяет легко настраивать автоматический запуск любых программ при возникновении заданного события. Это команда `EVENTTRIGGERS`. Справочная система к этой команде подробно описывает, как создать триггер, настроенный на появление определенного события, поэтому мы не будем останавливаться на этом описании.

При помощи сценариев в Windows Server 2003 в журналы можно записать и пользовательские события. Это команда `EVENTCREATE`. Использование утилиты подробно рассмотрено в ее справке (`EVENTCREATE /?`), поэтому мы не будем специально приводить ее описание.

Для систем более ранних, чем Windows Server 2003, администратору, чтобы настроить автоматическое исполнение определенных команд в ответ на заданные события, фиксируемые в журнале, нужно периодически считывать информацию из журналов и самостоятельно ее анализировать. Операция достаточно легко могла быть реализована с помощью сценариев, однако требовала некоторого опыта программирования.

Удаленная помощь пользователю

Одной из задач администрирования информационной системы является оказание технической поддержки пользователей. Обычно в этих целях используются программы доступа к рабочему столу.

Удаленный помощник

Удаленный помощник — режим удаленного подключения к рабочему столу Windows — предназначен для оказания помощи пользователю компьютера, чтобы в случае возникновения проблем в работе он имел возможность обратиться к спе-

циалисту, а последний, подключившись к компьютеру, мог оценить ситуацию, подсказать или показать какие-либо операции.

При подключении удаленного помощника рабочий стол виден одновременно двоим людям: самому пользователю и тому помощнику, который принял приглашение.

Первоначально помощник не может управлять компьютером: ему доступно только наблюдение и возможность обмена мгновенными сообщениями. Можно предоставить удаленному помощнику право на управление компьютером, в этом случае администратор сможет управлять системой так же, как будто он сидит за клавиатурой и мышью. Такое разрешение должен дать локальный пользователь, причем в любой момент он может вернуть себе управление системой.

Чтобы перейти в режим удаленного помощника, предусмотрен специальный механизм отправки приглашений на подключение. Отправить приглашение можно с помощью почтовой программы или программы MSN Messenger. Для этого необходимо выполнить следующие действия: нажать **Пуск | Справка и поддержка** и далее руководствоваться указаниям мастера отправки приглашения. Для осуществления автоматического подключения удаленный помощник должен его принять. В результате специалист сможет наблюдать удаленный рабочий стол, однако управление компьютером остается за локальным пользователем.

Примечание

Параметры вызова помощника могут быть определены централизованно в групповой политике.

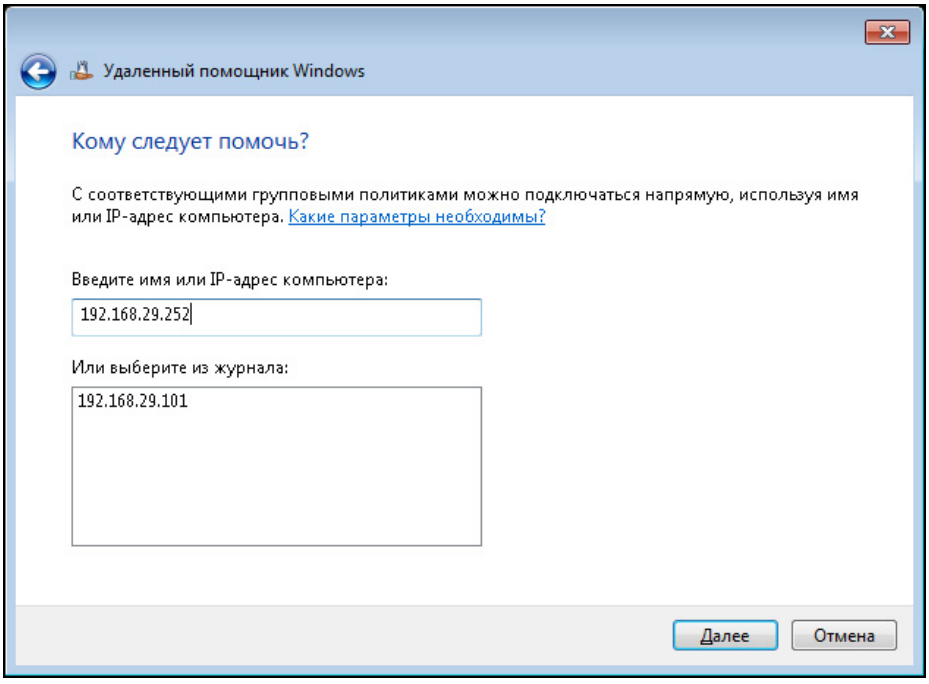


Рис. 14.12. Предложение помощи пользователю от администратора

В случае необходимости (этот вариант доступен в Windows 7) администратор может сам инициировать предложение помощи (рис. 14.12). Команда `msra /offerRA <имя удаленного компьютера>` (ее можно запомнить как аббревиатуру от MS Remote Assistance) позволяет запустить помощника и инициировать сессию на удаленной системе. Такой способ очень удобен при оказании поддержки неопытным пользователям, которым будет сложно объяснить по телефону процедуру запроса помощи. Пользователю достаточно только дать согласие на подключение и предоставить необходимый уровень контроля над своей системой.

Подключение к рабочему столу Windows

Хотя в рабочих станциях с ОС Windows присутствует возможность удаленного подключения к рабочему столу, на практике она редко используется администраторами для оказания помощи пользователям. Основная причина — при подключении администратора текущий пользователь автоматически отключается. Администратор может только посмотреть какие-либо настройки системы, но не показать пользователю, что и как нужно выполнить.

Поэтому администраторы применяют ту или иную программу, позволяющую увидеть удаленный рабочий стол на локальном компьютере и перехватить управление клавиатурой и мышью.

Существует большое количество таких программ: как бесплатные версии (VNC), так и коммерческие (pcAnywhere[1] от компании Symantec, Remote Admin от Famatech Inc., NetOp Remote Control от DanWare Data и т. д.). Выбор конкретной версии определяется возможностями администратора.

В любом случае для управления удаленным компьютером программой такого класса на него должна быть установлена клиентская часть. Эта операция может быть проведена централизованно любым способом. Приведем описание возможностей некоторых программ управления удаленным компьютером.

- **VNC** (**http://sourceforge.net/directory/os:windows/freshness:recently-updated/?q=VNC**). Позволяет удаленно просматривать любые платформы (UNIX, Win32, Mac, мобильные клиенты и т. п.). Это кроссплатформенное приложение может использоваться как в Windows, так и в Linux; имеется вариант на Java, который позволяет управлять рабочим столом из любого обозревателя Интернета.

  Коды программы открыты с 1998 г.; пользователи загрузили более 20 млн ее копий. Программа включена в состав популярной операционной системы Linux. По данным ее сайта, VNC используют все компании, входящие в список Fortune 500 (периодически обновляемый список наиболее успешных компаний).

  Обратите внимание, что сама программа бесплатна, но на ее основе создано много различных программ, в том числе и коммерческих, которые часто ото-

[1] Последняя версия программы позволяет администратору удаленно управлять как системами на основе Windows, так и Linux-компьютерами.

бражаются в начале результатов поиска в Интернете. Поэтому лучше воспользоваться приведенной выше ссылкой на бесплатные ресурсы.

- **Remote Administrator** (RAdmin). Еще одной часто используемой программой удаленного управления для платформы Windows является Radmin (программа коммерческая). Она также позволяет одновременно работать с несколькими удаленными компьютерами с помощью обычного графического интерфейса. Учитывая, что эта задача разработана для Win32, она использует методы аутентификации пользователей, принятые в Windows.
- **TeamViewer** (**www.teamviewer.com/ru/**). Программа объединяет возможности контроля рабочего стола с функционалом общего рабочего пространства, предоставляет возможности проведения совместных конференций. Реализованы возможности подключения через межсетевые экраны. Позволяет показывать свой рабочий стол на удаленные системы.

  Продукт коммерческий, но доступен для бесплатного индивидуального пользования (условия необходимо уточнить по лицензии).

> ***Примечание***
>
> Использование программ удаленного управления в открытых сетях должно сопровождаться особыми мерами безопасности. Целесообразно внимательно следить за обновлениями программ и использовать только последние версии, поскольку каждая новая разработка обычно характеризуется более устойчивой работой и повышенной защищенностью данных сессий.

Средство записи действий по воспроизведению неполадок

Пользоваться удаленным помощником удобно в пределах локальной сети. Если пользователь находится, например, в другой сети за межсетевым экраном, то подключение снаружи к такой системе крайне затруднительно.

В Windows 7 присутствует программа, позволяющая записать действия пользователя в файл и отправить затем его администратору по электронной почте. Это — **Средство записи действий по воспроизведению неполадок**, которое вызывается командой `psr` (от **P**roblem **S**tep **R**ecorder) — рис. 14.13.

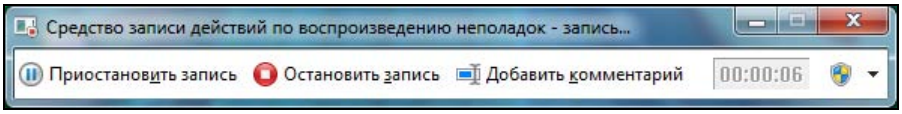


Рис. 14.13. Средство записи действий по воспроизведению неполадок

После запуска программы следует начать запись (нажать кнопку **Начать запись**) и выполнить все шаги, которые приводят к неисправности. После чего остановить запись (нажать кнопку **Приостановить запись**) и указать путь для сохранения записанных действий. При желании можно сразу отправить этот файл по электрон-

ной почте, если нажать на стрелочку справа от знака вопроса в панели утилиты и выбрать команду **Отправить получателю электронной почты**.

В итоге откроется окно нового сообщения электронной почты, в которое будет помещен файл с архивом записи. Сама запись представляет собой MHTML-документ, который можно открыть в Internet Explorer. Файл включает снимки экрана для каждого пользовательского шага и описание выполненных команд (с указанием версий файлов и т. п.).

Конкурентные RDP-сессии рабочей станции

Ограничения на подключения к удаленному рабочему столу рабочей станции являются искусственно наложенными. В Интернете достаточно легко можно найти[1] советы, как превратить рабочую станцию Windows (как версии Windows XP, так и Windows 7) в сервер терминалов. В этом случае возможно подключение к текущему рабочему столу пользователя и параллельное управление сессией (самим пользователем и подключившимся администратором).

Такие решения предполагают замену программной библиотеки на "исправленную". Учтите, что подобный способ является формальным нарушением лицензионного соглашения с разработчиком программного обеспечения.

Интерфейсы удаленного управления

Еще один вариант подключения к удаленному рабочему столу заключается в использовании интерфейсов удаленного управления. Обычно такая функциональность характерна только для серверных материнских плат, но есть и платформы рабочих станций, в которых предусмотрена такая возможность.

Интерфейс удаленного управления, который часто еще называют системой out-of-band-управления, позволяет по отдельному сетевому интерфейсу контролировать состояние аппаратной платформы, включать и выключать питание, программно удаленно монтировать образы CD/DVD и т. д. В том числе имеется опция отображения удаленного рабочего стола и перехват управления клавиатурой и мышью.

На рис. 14.14 показан пример подобного интерфейса удаленного управления.

Как уже говорилось, серверные платы обычно имеют подобный функционал по умолчанию, но есть модели, в которые такая функциональность добавляется путем установки специального модуля. При отсутствии таких возможностей имеется еще вариант использования переключателей KVM over IP.

Переключатели клавиатуры и мыши с управлением по сети TCP/IP позволяют получить доступ к удаленному монитору и клавиатуре. В отличие от интерфейсов удаленного управления данные решения не позволяют включить и выключить питание, увидеть параметры датчиков оборудования и т. п. Поэтому при их использовании не следует забывать о настройке параметров BIOS, например, разрешить

[1] Следует искать на ключевые слова "rdp hack", "concurrent remote desktop session".

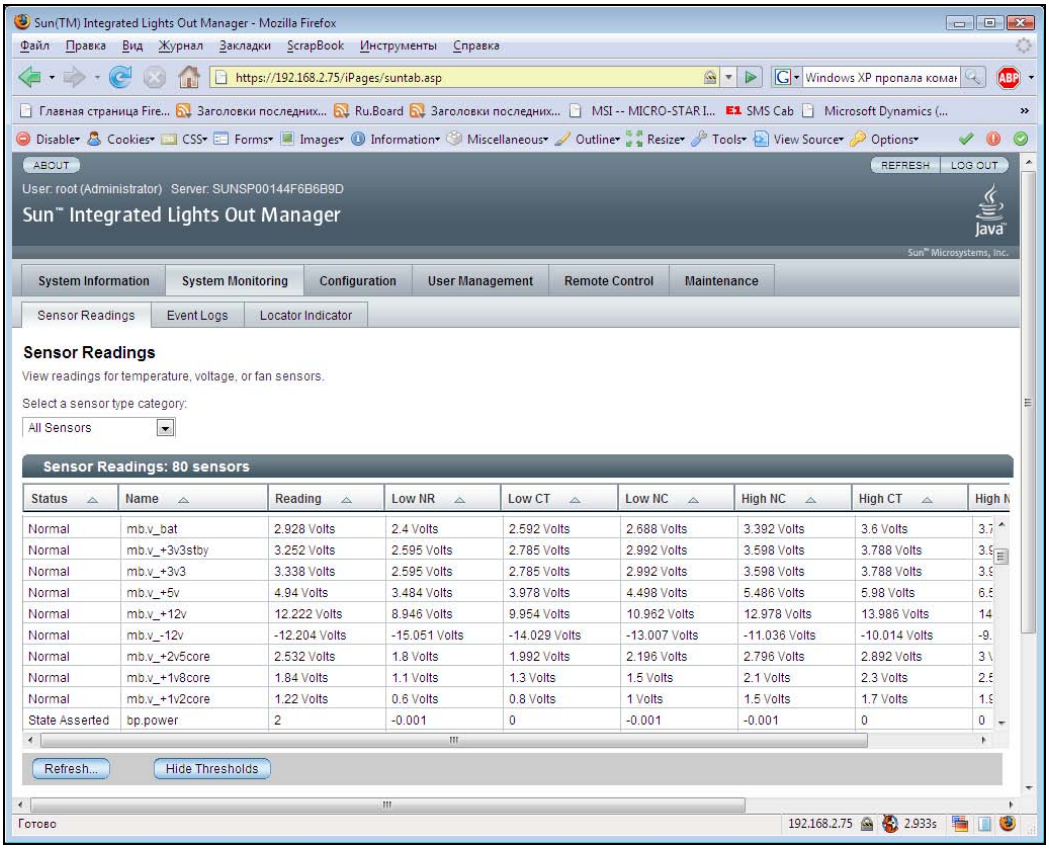


Рис. 14.14. Интерфейс удаленного управления (iLO) сервера Sun

включение системы с клавиатуры, чтобы иметь возможность включить электропитание системы.

Особенности отказов различных компонентов

Отказ в обслуживании может возникнуть вследствие отказа любого элемента информационной системы: повреждения кабелей, неполадок в работе коммутирующих устройств, выхода из строя узлов компьютера, зависания операционной системы, ошибок программного обеспечения бизнес-уровня и уровня приложений и т. п.

Обнаружение неисправностей кабелей передачи данных

Неисправность пассивной инфраструктуры можно определить специальными тестерами. Они с помощью особых тестов проверяют линии связи на соответствие всем требованиям стандарта. Однако такие тестеры достаточно дороги, и далеко не

каждая даже крупная организация их имеет. В большинстве случаев ограничиваются только проверкой наличия соединения (есть контакт — нет контакта), которое выполняется простейшими тестерами. Кабельные тестеры позволяют обнаружить обрыв линии связи, перепутывание проводников и другие типовые неисправности. Тестеры доступны любому администратору, их можно найти по цене менее 1 тыс. рублей.

Если кабель исправен, то нужно проверить состояние портов сетевого интерфейса компьютера и коммутатора. Косвенным признаком исправности может служить индикатор на сетевом порту. Если он горит, то кабель, скорее всего, исправен.

Также нередки случаи выхода из строя сетевых портов. Особенно часто это происходит на длинных (близких к максимальному значению) медных линиях связи после гроз.

> ***Примечание***
>
> Существуют специальные модули защиты от грозовых разрядов. Но как показывает практика, они не обеспечивают гарантированной защиты сетевых портов. Поэтому, с учетом стоимости оборудования, часто предпочитают просто заменять сожженный порт на исправный (с последующей заменой всего коммутатора при выходе из строя всех портов).

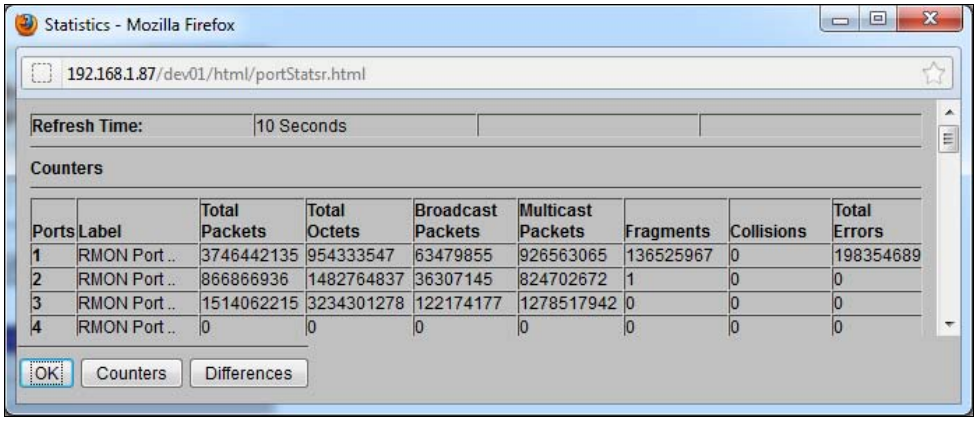
Признаки неисправности кабельной подсистемы

Неисправности на уровне физических носителей могут приводить к ошибкам копирования файлов, "зависанию" приложений, работающих с сетевыми ресурсами, и т. п. Подобные неисправности могут иметь случайный характер (например, при переломе кабеля и восстановлении/пропадании сигнала при незначительном изгибе).

Признаком наличия проблем на уровне кабельной подсистемы могут быть следующие значения счетчиков системы.

- **Число ошибочных пакетов.** При нормальной работе число ошибочных кадров не должно превышать десятых долей процента передаваемой информации. Обычно большой процент ошибок контрольной суммы свидетельствует о низком качестве сети (контакты, помехи в кабеле, неисправности портов оборудования). Неверные длины пакетов — признак неисправности сетевых адаптеров и их драйверов.
- **Величина коллизий.** В нормально работающей сети величина коллизий не должна превышать нескольких процентов. Большая величина — это признак низкого качества сети (локальные коллизии), наличие ошибок адаптеров или неверного проектирования сети. (Late collision — коллизия, обнаруживаемая после передачи первых 64 байтов. Причиной late collision часто бывает большое число повторителей в локальной сети.)

Если у вас сеть построена на управляемых коммутаторах, то статистическую информацию по ошибочным пакетам можно получить от их программ управления (см. пример на рис. 14.15). Если вы заметили подобную статистику на порту коммутатора, то необходимо обязательно выяснить ее причины.



Ports	Label	Total Packets	Total Octets	Broadcast Packets	Multicast Packets	Fragments	Collisions	Total Errors
1	RMON Port ..	3746442135	954333547	63479855	926563065	136525967	0	198354689
2	RMON Port ..	866866936	1482764837	36307145	824702672	1	0	0
3	RMON Port ..	1514062215	3234301278	122174177	1278517942	0	0	0
4	RMON Port ..	0	0	0	0	0	0	0

Рис. 14.15. Данные статистики портов реального коммутатора

Причиной таких ошибок могут быть:

- повреждения кабелей, плохо обжатые разъемы;
- перегрев коммутационного оборудования;
- перегрузка сети (передача значительных объемов данных);
- помехи от СВЧ-печей, люминесцентных ламп, от силового электрооборудования и т. п.

Диагностика IP-протокола

Для диагностики соединения с использованием протокола TCP/IP рекомендуется использовать такую последовательность операций:

1. Проверка параметров настройки IP-протокола.
2. Проверка достижимости ближайших компьютеров сети.
3. Проверка функционирования серверов имен.

> ***Примечание***
>
> В Windows существует специальный мастер диагностики сетевого подключения, который выполняет операции, аналогичные описанным, и выдает результаты соответствующих тестов. Эта программа вызывается из меню утилиты **Сведения о системе** (**Пуск | Все программы | Стандартные | Служебные | Сведения о системе | Сервис | Диагностика сети**).

Проверка параметров настройки IP-протокола

Для отображения параметров IP-протокола используются утилиты `ipconfig` (Windows NT/200*x*/XP/Vista/7), `winipcfg` (Windows 9*x*/ME), `ifconfig` (*nix-системы). Утилиты `ipconfig`, `ifconfig` выполняются в режиме командной строки. Утилита `winipcfg` имеет графический интерфейс.

Утилиты выводят на экран параметры настройки протокола TCP/IP: значения адреса, маски, шлюза. Далее показан пример листинга команды `ifconfig`.

```
kenin@test:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:04:75:c6:8c:18
inet addr:192.168.10.1 Bcast:192.168.10.255 Mask:255.255.255.0
inet6 addr: fe80::204:75ff:fec6:8c18/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:26828665 errors:0 dropped:0 overruns:1 frame:0
TX packets:15577750 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1383752632 (1.3 GB) TX bytes:1068723423 (1.0 GB)
Interrupt:22 Base address:0xa000

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr:::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:63031 errors:0 dropped:0 overruns:0 frame:0
TX packets:63031 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:8932494 (8.9 MB) TX bytes:8932494 (8.9 MB)
```

Программа показывает параметры сетевого интерфейса eth0 и локального интерфейса lo.

Если указанные утилиты покажут, что сетевому адаптеру присвоен адрес 169.254.134.123 (или аналогичный из подсети 169.254.0.0/16), то можно сделать заключение, что в сети недоступен сервер, автоматически присваивающий параметры IP-протокола. Часто причиной подобной ошибки (если ранее компьютер нормально работал в сети) является нарушение контакта в подсоединении сетевого кабеля.

Чтобы инициировать получение параметров адреса в Windows, можно выполнить команду `ipconfig /renew`, для *nix-систем можно просто перезапустить сетевые службы (например, командой `/etc/init.d/networking restart` для Ubuntu). Если параметры адреса не присваиваются автоматически, то следует временно назначить их вручную (соответственно используемому на предприятии диапазону адресов).

Проверка достижимости ближайших компьютеров сети

Для проверки достижимости компьютеров в сети TCP/IP используется команда `ping`. Эта команда посылает на заданный компьютер последовательность символов определенной длины и выводит на экран информацию о времени ответа удаленной системы. Ключами команды можно регулировать количество отсылаемых символов и время ожидания ответа (через этот период выводится сообщение о превышении периода ожидания; если ответ придет позже, то он не будет показан программой).

При тестировании подключения рекомендуется применять нижеприведенную последовательность операций.

1. Сначала проверяется работоспособность протокола TCP/IP путем "пингования" локального интерфейса — адреса 127.0.0.1:

   ```
   ping 127.0.0.1
   ```

   Адрес 127.0.0.1 — это "личный" адрес любого компьютера. Таким образом, эта команда проверяет прохождение сигнала "на самого себя". Она может быть выполнена без наличия какого-либо сетевого подключения.

   Если будет показано сообщение о недостижимости адресата, то это означает ошибку установки протокола IP. В этом случае целесообразно удалить протокол из системы, перезагрузить компьютер и вновь установить поддержку протокола TCP/IP.

2. Следующим шагом необходимо проверить ответ локального компьютера по присвоенному ему IP-адресу. Для этого следует выполнить команду:

   ```
   ping <адрес>
   ```

   Вы должны увидеть ответ от системы.

3. Следующая проверка — это выполнение команды `ping` с указанием IP-адреса любого компьютера в локальном сегменте. Можно использовать любой адрес, относительно которого вы уверены, что он достижим в локальной сети на момент проверки. Например, IP-адрес шлюза или адрес DNS-сервера.

   Для компьютеров локального сегмента проводной сети время отклика на команду `ping` должно составлять не более 1 мс. Наличие такого отклика свидетельствует, что канал связи установлен и работает. Отсутствие ответа обычно говорит либо о повреждении кабельной сети (например, нет контакта в разъеме), либо о неверно установленных параметрах статического адреса (если адрес получается автоматически, то следует обратиться в службу технической поддержки).

   > ***Примечание***
   >
   > При выборе удаленного компьютера для проверки канала связи следует убедиться, что прохождение `ping`-пакетов не запрещено межсетевым экраном.

4. Последняя проверка — это команда `ping`, с указанием в качестве параметра не IP-адреса, а имени какого-либо компьютера (например, имя WWW-сервера вашего провайдера):

   ```
   ping <имя>
   ```

   Если не будет ответа на ввод команды с именем существующего хоста, то это может свидетельствовать либо об ошибке в задании DNS-серверов, либо об их неработоспособности.

Оценка качества аудио- и видеопотоков

Оценка качества передачи аудио- и видеосигналов имеет некоторые отличия. Данные по сети Ethernet передаются, в основном, по протоколу TCP: если пакет по тем или иным причинам теряется или искажается в процессе пересылки, то системы обнаруживают ошибки и повторяют пересылку информации. Мультимедийные по-

токи — для большей скорости — передаются UDP-пакетами, для которых механизма контроля не предусмотрено. Поэтому пакеты могут теряться. Кроме того, может нарушаться последовательность пакетов (из-за наличия программных буферов на активном оборудовании). Программы могут в определенных пределах компенсировать такие ошибки (небольшие потери не замечаются человеком, собственные буфера позволяют восстановить последовательность данных), но эти возможности ограничены.

Выделяются следующие основные показатели:

- задержка при передаче данных;
- джиттер;
- потеря пакетов.

Существуют интегральные показатели качества, например, телефонного разговора по сети Ethernet, но они базируются на указанных ранее критериях.

Способы получения объективных показателей передачи мультимедийных данных

Для формирования объективной оценки качества мультимедийного канала нужно анализировать сами пакеты: время их отправки и получения, порядок пакетов и т. д. Поэтому для анализа необходимо использовать специализированное программное обеспечение. Например, сетевые анализаторы — *снифферы*.

Для анализа состояния инфраструктуры можно использовать программы, предназначенные для мониторинга сетевого трафика. Одна из таких программ — WireShark (**http://www.wireshark.org/**).

Снифферы часто формируют интегральные показатели качества разговора. Например, одним из таких показателей является коэффициент MOS. Этот коэффициент представляет собой экспертную оценку качества: он рассчитывается по определенной методике на основе сравнения группой слушателей полученного сигнала и эталона. Считается, что коэффициент MOS больший 4 соответствует бизнес-качеству разговора, а меньший 2,5 является недопустимым.

Задержка при передаче данных IP-телефонии

Считается, что задержка меньшая 200 мс комфортна для ведения телефонного разговора. Величина большая 700 мс считается неприемлемой для ведения деловых переговоров.

Задержка получается из нескольких величин, но основной вклад вносит задержка при передаче по сети. Обратите внимание, что некоторые каналы, например спутниковые, принципиально имеют большую величину задержки при передаче информации (несмотря на высокую скорость).

Джиттер

Пакеты сигнала принимаются не с одинаковой задержкой: часть приходит раньше, часть позже. Иногда последовательность пакетов нарушается: переданные позже приходят раньше и т. п.

Для компенсации такого "дрожания" времени доставки пакетов используются программные буфера. Понятно, что такая компенсация имеет пределы, после которых искажения уже будут слышны.

Допустимые потери пакетов в телефоном разговоре

Человек может не заметить ухудшение качества разговора при потере пакетов меньшей примерно 5%. Но уже при потере в 10% и более слышно бульканье, речь становится малоразборчивой.

Мониторинг отказоустойчивой структуры

Если в вашей организации реализованы те или иные технологии дублирования, то следует постоянно проверять состояние каждого элемента любым доступным способом. Автору приходилось сталкиваться с ситуациями, когда выходил из строя жесткий диск из состава RAID-массива, сервер пищал длительное время, а его никто не слышал, и неисправность не была выявлена до момента выхода из строя второго диска, что уже привело к потере данных. Аналогично, если вы используете дублированные каналы передачи данных, то можете не заметить выход из строя одного канала и столкнуться с полным отказом, будучи уверенным в том, что ваша система отказоустойчива.

Поэтому следует обеспечить постоянный мониторинг состояния информационной системы.

Неисправности аппаратной части компьютеров

Это весьма тяжело детектируемые неисправности, особенно если происходят достаточно случайно. "Хорошо", если неисправность аппаратной части компьютера приводит к его полной неработоспособности. А выявить "исчезающую" неисправность, обусловленную проблемами "железа", крайне сложно. Как правило, компьютер в таких случаях прекрасно проходит специальное тестирование, но все же постоянно "подвисает" на определенных задачах.

> ***Примечание***
>
> В Linux можно отобразить сообщения о состоянии оборудования во время старта системы командой `dmesg`. Например, чтобы увидеть сообщения о состоянии сетевых карт, нужно отфильтровать вывод команды с помощью `grep`: `dmesg | grep eth`. Другая команда, с помощью которой можно получить информацию об оборудовании — `dmidecode`. Например, чтобы получить информацию о процессоре, нужно выполнить `dmidecode -t 4` (ключи команды, соответствующие типам оборудования, можно уточнить по документации — `man dmidecode`).

Действия при подозрении на неисправность оборудования

При подозрении на аппаратную неисправность необходимо вначале выполнить следующие операции:

- обновить BIOS материнской платы компьютера до последней версии изготовителя;

- выполнить чистую установку операционной системы (без каких-либо "лишних" прикладных программ), после чего установить все обновления от ее изготовителя;
- установить последние версии драйверов для материнской платы, видеоадаптера и т. п. Драйверы оборудования прилагаются к системному блоку. Вам следует обязательно убедиться, что изготовитель не предлагает на сайте новые версии. И если новые версии обнаружены, то скачать и установить именно их. Обратите внимание, что при наличии сертифицированных версий и новых разработок (бета-версии) обязательно следует устанавливать последние сертифицированные варианты;
- если неисправность наблюдается в прикладном программном обеспечении, то следует установить его и все имеющиеся для него обновления.

После выполнения этих операций нужно попытаться воспроизвести неисправность. Если неисправность будет периодически возникать, то такой блок следует передать на техническое обслуживание.

> ***Примечание***
>
> На практике часто встречаются случаи, когда простая замена одних узлов на аналогичные, причем той же модели, часто ликвидировала такие исчезающие неисправности.

Проверка оперативной памяти

Оперативная память является одной из самых частых причин возникновения непонятных сбоев в работе системы. В Windows 7/Server 2008 включена программа проверки оперативной памяти. Запуск ее осуществляется выбором соответствующего пункта загрузки при старте системы. Для предыдущих версий Windows можно использовать утилиту `memtest`, которую легко можно найти на серверах Интернета. Эту утилиту необходимо запускать, загрузившись в режиме командной строки (без подключенных драйверов памяти) с дискеты или компакт-диска (образы загрузочных дисков для различных версий ОС Windows можно, например, загрузить с сайта **http://www.allbootdisks.com/**).

В Linux-системах утилиты проверки памяти часто включаются в комплект установочных дисков. Например, вызов теста памяти в Ubuntu вызывается при загрузке компьютера с установочного компакт-диска в главном меню (на первом экране) — рис. 14.16.

По умолчанию все программы тестирования памяти запускаются в варианте самой простой конфигурации. Если он не показывает ошибку, но при этом есть сомнения в качестве памяти, то следует увеличить время тестирования (число проходов, выбрать более сложный тест и т. д.). Расширенные тесты используют специальные методики проверки, например, разогревая одни области памяти, а потом выполняя проверку смежных участков кристалла. Учитывайте, что для получения качественной оценки модуля памяти длительность тестирования обычно составляет несколько часов.

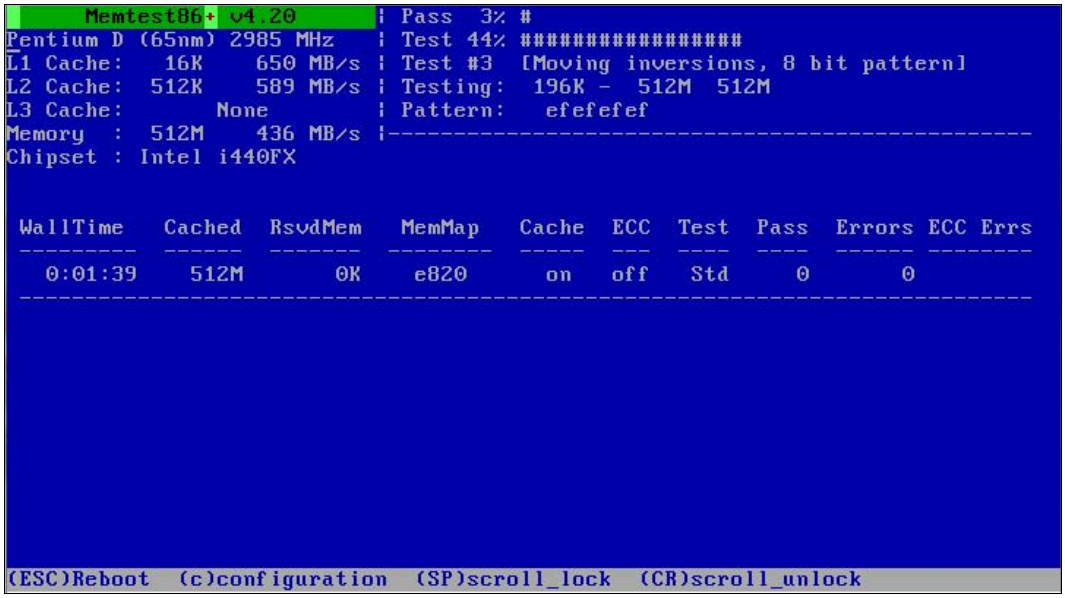


Рис. 14.16. Окно программы проверки памяти в Ubuntu

Контроль жестких дисков

В операционные системы встроены утилиты проверки файловых структур, которые автоматически запускаются во время перегрузки компьютера в случае обнаружения ошибок (например, ошибочных блоков) и, дополнительно в Linux, после длительного периода работы или определенного числа перезагрузок. Это `checkdsk` для Windows и `fsck` для Linux (строго говоря, `fsck` является оболочкой, которая запускает программу проверки, специфичную для используемой в Linux файловой системы).

Программы проверки можно запустить вручную. Обратите внимание, что для исправления ошибок необходимо отключить *(размонтировать)* логический диск. В Windows эта операция может быть осуществлена самой программой (с запросом подтверждения пользователя — кроме системного диска, ошибки на котором можно исправить только при старте операционной системы), в Linux размонтировать диск необходимо вручную.

Поскольку в Linux рекомендуется для проверки также перейти в однопользовательский режим, то для упрощения можно воспользоваться следующими двумя способами включения проверки при очередной перезагрузке. Если планируется перегрузка в текущий момент, то следует выполнить команду `shutdown -rf now` (ключ `f` заставляет выполниться проверку при старте). Если необходимо просто настроить запуск проверки при очередной перезагрузке, то следует создать файл forcefsck в корне (например, командой `touch /forcefsck`, выполняемой от имени суперпользователя).

Контроль теплового режима работы системы

При повышении температуры на несколько градусов вероятность отказа компьютера повышается на десятки процентов. Поэтому контроль теплового режима — важная задача.

Одним из самых ненадежных узлов компьютера являются вентиляторы охлаждения. Они служат для поддержания необходимого теплового режима процессора, видеоадаптера, в блоке питания и т. п. Число вентиляторов варьируется в зависимости от модели компьютера.

Обычно через полтора-два года эксплуатации компьютера дешевые модели вентиляторов снижают скорость вращения лопастей (или даже могут полностью остановиться). Современные материнские платы имеют в поставке программы, которые автоматически контролируют скорость вращения вентиляторов и температурный режим внутри системного блока. При наличии таких программ их следует обязательно установить и своевременно реагировать на их сообщения. При отсутствии средств контроля необходимо периодически (каждый раз, когда вы открываете системный блок) визуально проверять скорость вращения лопастей вентилятора и своевременно заменять неисправные.

Примечания

Допустимо смазывать оси вентиляторов специальной смазкой. Но после такой операции следует проверять данные вентиляторы не реже одного раза в три-четыре месяца.

При отсутствии штатных средств контроля температуры материнской платы компьютера можно воспользоваться бесплатными программами, контролирующими температуру жестких дисков. Одна из таких программ — HDD Thermometer разработки Rdssoft, например, контролирует температуру дисков и может формировать предупреждения администраторам в случае превышения установленных лимитов.

Температура внутри корпуса компьютера может повыситься не только из-за ухудшения качества вентиляторов. Так, причиной перегрева могут стать дополнительные устройства (дополнительные жесткие диски), установленные в компьютер. Вполне возможно, что конструкция корпуса просто не рассчитана на такое количество оборудования. Свою лепту вносят и крайне жаркие дни, которых наблюдается все больше в последние годы.

Все эти причины могут привести к перегреву компьютера и, как следствие, возникновению сбоев в его работе или даже выходу из строя.

Если оборудование установлено в шкафу и температура внутри шкафа измеряется, то для грубой оценки можно ориентироваться на следующие цифры. Температура внутри корпуса компьютера обычно на 15—20 °С превышает температуру окружающей среды. Поэтому администратор должен начать предпринимать срочные меры, если температура внутри серверного шкафа превысит 30 °С.

Резервирование узлов компьютера

Обычно стараются резервировать (с возможностью горячей замены) наиболее часто отказывающие узлы — жесткие диски и блоки питания.

Жесткие диски, как правило, объединяют в RAID-массивы того или иного уровня с возможностью горячей замены. При необходимости серьезной экономии можно создать такие массивы программным способом и использовать SATA-диски. Поскольку RAID обычно конфигурируется с избыточной надежностью, то единичный отказ жесткого диска сохраняет работоспособность устройства хранения. Поэтому администратору необходимо либо постоянно следить за состоянием RAID, либо автоматизировать получение предупреждения о возникновении отказа. Иначе второй отказ может привести к краху системы.

Применение систем с резервированием других узлов (например, памяти) часто экономически не оправдано. Если необходимо обеспечить работоспособность службы при выходе из строя аппаратной части компьютера, обычно применяют кластерные решения (параллельная работа нескольких компьютеров; решение дорогое и не подходит для небольших организаций) или решения высокой доступности для виртуальных систем (также в силу стоимости, практически, доступны только для крупных информационных систем).

Ошибки программного обеспечения

Основная часть отказов Windows-систем связана преимущественно с ошибками в программном обеспечении. Как уже говорилось, это могут быть ошибки самой операционной системы или установленного прикладного продукта.

Если проблема возникала только один раз, то выявить ее причины обычно практически невозможно. Если событие повторилось, то администратору следует тщательно проанализировать всю сопутствующую информацию и выявить события, связанные с инцидентом. Чем тщательнее будет проведен предварительный анализ, тем больше вероятность точного решения. Следует попытаться изолировать данную неисправность от других событий и составить необходимый план действий, предусматривающий возможность операций "отката", если лечение проблемы само вызовет другие отказы.

И естественно, администратор не может не обратиться к поиску аналогичных инцидентов и рекомендаций по их разрешению в той или иной базе знаний.

Выяснение причин катастрофических ошибок в программном обеспечении

При аварийном завершении работы прикладной программы или всей операционной системы часто достаточно сложно определить виновника. Как правило, на компьютере установлено много программ, остались следы от ранее использованных и т. п. Все это может влиять на случившийся отказ программного обеспечения. Существуют специальные продукты, которые могут помочь в таких случаях администратору.

На странице **http://www.microsoft.com/whdc/devtools/debugging/default.mspx/** представлены средства отладки Windows — Debugging Tools for Windows. Понятно, что предназначены они для специалистов, но получить базовую информацию по неисправности можно достаточно простыми способами.

Предварительно надо убедиться, что в системе сохраняются данные из памяти в случае возникновения аварийной ситуации. На рис. 14.17 показано окно, в котором необходимо настроить варианты поведения системы в случае аварийного завершения работы. Обычно достаточно включить автоматическую перезагрузку (это значение по умолчанию) и включить малый дамп памяти (дамп памяти ядра).

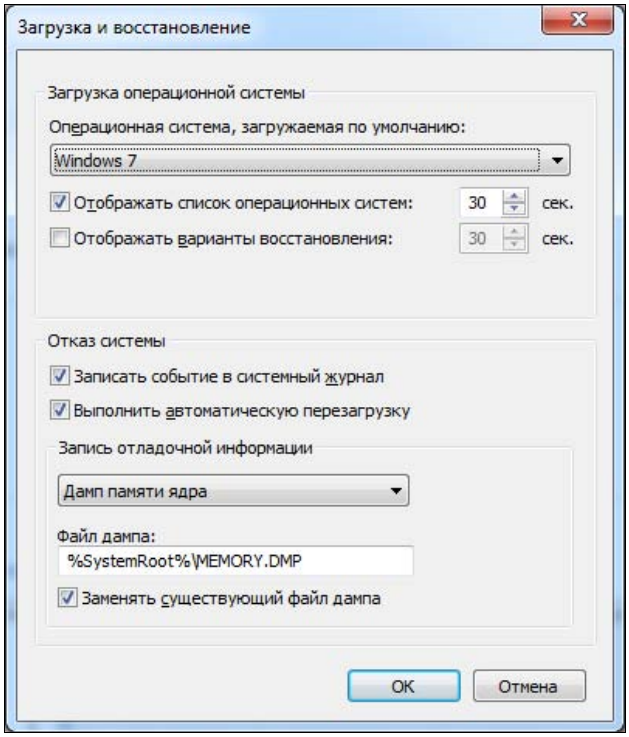


Рис. 14.17. Настройка автоматической перезагрузки и записи отладочной информации в случае аварийных отказов

Для работы со средствами отладки загрузите с сайта их установочные пакеты и, обязательно, наборы символов для вашей операционной системы (наборы символов нужны, чтобы сделать вывод информации более читабельным). Наборы символов отличаются для различных версий Windows, в том числе, необходимо подключать различные наборы для систем с установленными пакетами обновлений и без них. Можно сначала установить средства отладки, а потом, имея подключение к Интернету, загрузить необходимые символы. Но учитывая их объем (несколько сотен мегабайт загрузки и более 1,5 Гбайт в установленном виде), лучше это сделать заблаговременно.

Примечание

Установка символов и самой программы отладчика выполняется независимо. Типовая ошибка начинающих пользователей — отсутствие настройки пути к папке символов в отладчике. Не забудьте при старте программы открыть меню **File** и настроить параметр **Symbol File Path**.

После установки отладчик можно использовать двумя основными способами: открыть для анализа файл дампа памяти или подключиться к работающему процессу (командой **File | Attach to Process...**) и ожидать момента аварийного его завершения.

После получения отладчиком информации об аварии обычно в консоли достаточно ввести команду

```
!Analyze-v
```

и попытаться проанализировать результат. Нужная информация, как правило, представлена в строках `image_name` и `module_name` (рис. 14.18).

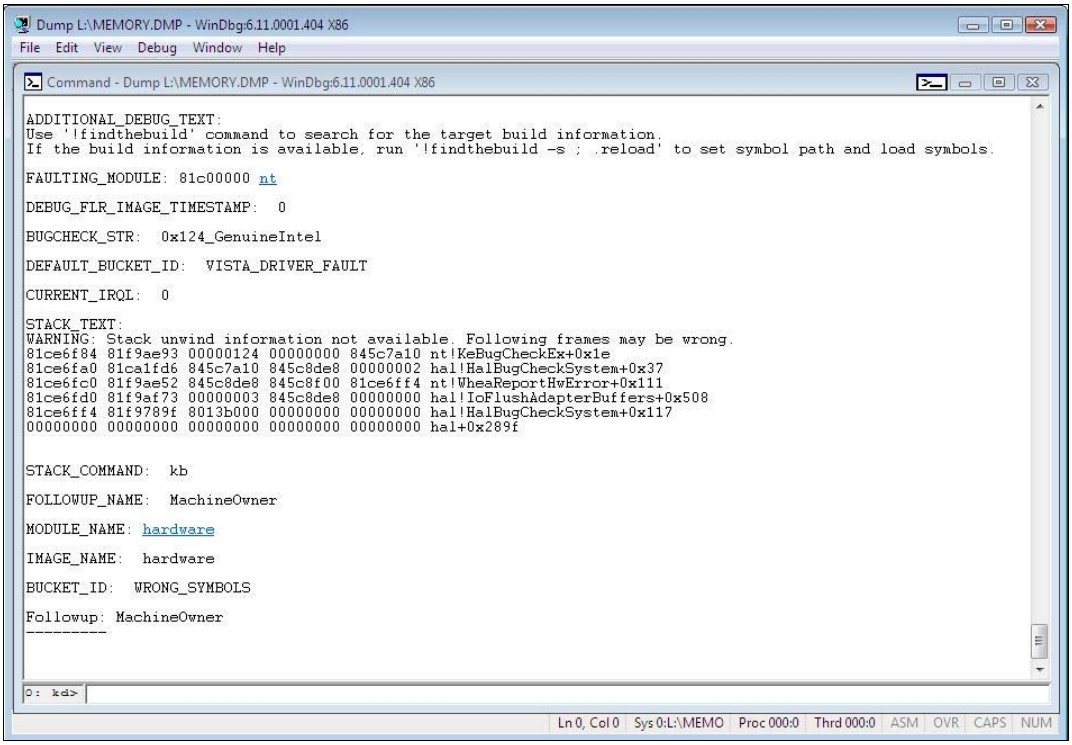


Рис. 14.18. Окно отладчика Windows

На рис. 14.18 показано окно отладчика после выполнения анализа дампа памяти "упавшей" системы. По информации можно сделать вывод, что причина отказа — плохой драйвер оборудования. Исправить именно эту ошибку администратор, естественно, не в силах. Но зато он узнал, что нужно искать новый драйвер оборудования.

Порядок работ по оптимизации системы

Примечание

Существенное влияние на производительность оказывает качество драйверов. При возможности, перед проведением оптимизации следует установить в систему последние имеющиеся версии.

Узким местом производительности информационной системы обычно является один из следующих компонентов:

- процессор;
- оперативная память;
- дисковая подсистема;
- сетевой адаптер (сетевая инфраструктура).

В идеальном случае каждый компонент должен быть равномерно нагружен: не "простаивать", но и не сдерживать работу других частей.

Обычно сначала анализируются суммарные показатели (процессора, памяти, дисковой подсистемы и т. п.). Затем, с учетом полученной оценки, производится более подробный анализ счетчиков, отражающих параметры работы прикладного программного обеспечения.

В табл. 14.1 приведены средние пороговые значения суммарных параметров производительности, по которым можно судить о состоянии системы.

Таблица 14.1. *Показатели производительности*

Параметр	Состояние компьютера	
	оптимальное	перегруженное
Процент загрузки процессора	< 40%	> 80—90%
Средняя длина очереди заданий процессора	< 2	> 4
Процент загрузки процессора обслуживанием системы/процент времени ожидания процессора	< 4%	> 10%
Обмен страниц памяти в секунду	< 500	> 1000
Среднее время операции записи-чтения на логический диск	< 15 мс	> 25 мс
Средняя длина очереди операций записи-чтения на диск	< 0,2	> 0,6
Процент использования полосы пропускания сетевого адаптера	< 40%	> 60%
Очередь на передачу пакетов в сетевом адаптере	0 пакетов	> 2 пакетов

Оценка производительности компонентов системы

Мы постараемся дать далее в этой главе краткую сводку по основным счетчикам операционной системы Windows и по одной из самых распространенных приклад-

ных программ — серверу баз данных. Но сначала кратко опишем базовые показатели оценки каждой подсистемы и особенности интерпретации значений параметров.

> ***Примечание***
>
> При оценке системы нельзя полностью полагаться на приводимые далее критерии. Их следует использовать с учетом специфики вашей информационной системы.

Оценка производительности процессора

> ***Примечание***
>
> Поскольку современные компьютеры имеют возможность снижать скорость своей работы (например, в случае перегрева процессора или просто в режиме простоя), предварительно убедитесь, что высокая загрузка процессора не связана со снижением его тактовой частоты (сравните значения текущей частоты с максимальной).

В современные серверы, как правило, устанавливают не по одному многоядерному процессору. И в условиях "среднего" предприятия увидеть загрузку процессоров компьютера, близкую к 100%, маловероятно. При этом именно процессор может быть узким местом.

Связано это с тем, что показатель производительности подсчитывается усредненно по всем процессорам, а многие расчеты в приложениях не могут быть распараллелены: сначала нужно вычислить одну величину, потом она будет использована в других расчетах и т. д. Поэтому если какой-либо прикладной процесс (например, процесс сервера базы данных) выполняется в одну нить, то соответствующая загрузка процессора будет показываться как 100%/(число процессоров) и распределится (в программе **Производительность**) между всеми ядрами/процессорами.

Поэтому более информативным будет анализ непроизводительных расходов процессора. В случае Windows-систем это будет счетчик **Processor\% Privileged Time**, для Linux-компьютеров нужно оценивать время, затрачиваемое процессором на системные операции и ожидание готовности других устройств. В листинге 14.1 приведен вывод утилиты `iostat`. В строке `avg-cpu` показаны характеристики загрузки процессора: параметр `%system` отображает загрузку системными операциями, `%iowait` — время, затрачиваемое на ожидание завершения операций ввода-вывода на диски.

Листинг 14.1. Вывод утилиты `iostat`

```
kenin@test:~$ iostat
Linux 2.6.32-34-generic-pae (test) 04.11.2011 _i686_ (1 CPU)

avg-cpu: %user %nice %system %iowait %steal %idle
8,10 0,00 1,50 0,96 0,00 89,44

Device: tps Blk_read/s Blk_wrtn/s Blk_read Blk_wrtn
sda 2,08 15,09 109,64 1257276 9133150
```

```
sdb 0,03 0,87 0,00 72700 0
sdc 0,09 2,74 0,00 228062 0
dm-0 14,34 15,05 109,61 1254018 9131104
dm-1 0,01 0,02 0,02 1488 2032
```

Если процент времени, затраченного процессором на служебные цели, составляет 5% и более (примерно), то необходимо принять меры к минимизации этой нагрузки. Возможными причинами могут быть избыточное количество одновременно запущенных программ (время тратится на переключение между процессами), проблемы с оборудованием (увеличенное число прерываний от устройств) и т. д.

- **System\Processor Queue Length (all instances).** Показатель отображает длину очереди заданий, которые необходимо выполнить процессору. Средняя величина очереди заданий, равная двум и выше, свидетельствует о том, что процессор не успевает выполнять все задачи. При этом очень часто средний процент загрузки процессора остается сравнительно небольшим.

  Большая длина очереди может быть обусловлена не только большим количеством одновременно выполняющихся заданий, но и неисправностью какого-либо устройства, например сетевого адаптера, генерирующего большое количество прерываний в единицу времени. Для локализации этой причины следует провести анализ параметра **Processor\Interrupts/sec** *(см. далее)*.

- **Processor\Interrupts/sec.** Счетчик показывает количество запросов к процессору на обработку. Максимальное число прерываний, которое может обработать процессор, зависит от его типа. Для разных процессоров эта величина колеблется от 500 до 2000 прерываний в секунду.

  Поскольку высокое значение данного счетчика может быть следствием неисправности оборудования, следует выяснить, что является источником повышенного количества запросов в единицу времени. Для этого можно задействовать счетчики объекта Thread (Поток), например **%Processor Time**. Эти счетчики отображают в том числе состояние каждого потока, который запускается отдельным процессом. Переключив отображение монитора системы на гистограмму, вы можете увидеть процесс, который монополизирует ресурсы компьютера.

  Примечание

  Бездействие компьютера также относится к процессу. Поэтому для удобства не следует включать отображение этого параметра на графике.

Оценка использования оперативной памяти

Установка дополнительной памяти является часто самым простым способом повышения быстродействия системы. Поэтому важно уметь оценить, действительно ли компьютер нуждается в таком обновлении.

- **Объем свободной памяти.** Современные операционные системы и приложения весьма агрессивно используют оперативную память компьютера, захватывая весь свободный объем. При этом если другим приложениям потребуется допол-

нительный объем оперативной памяти, то система выполняет ее перераспределение. Поэтому судить о достаточности или нехватке оперативной памяти по ее свободному объему не имеет смысла.

Более продуктивным является анализ показателей, отображающих использование файла подкачки.

- **Memory\Pages/sec.** Одним из самых интегральных показателей использования оперативной памяти является счетчик, демонстрирующий количество запросов страниц памяти из файла подкачки на диске. Эти операции проводятся в случае нехватки физической памяти, поэтому большое значение данного показателя свидетельствует о необходимости установки в систему дополнительной памяти. Для современных серверов приемлемым значением считается величина до 200 страниц в секунду. Критическое значение — порядка 1000 страниц в секунду.

> ***Совет***
>
> Обратите внимание, что на некоторых материнских платах частота, на которой работает оперативная память, зависит от конфигурации устанавливаемых модулей. В этом случае добавление новых модулей памяти может привести к снижению скорости работы с ней. Поэтому при необходимости добавления новых модулей надо предварительно изучить рекомендации вендора по оптимальной конфигурации оперативной памяти системы.

Оценка дисковой подсистемы

Дисковая подсистема может существенно снижать производительность компьютера, поскольку она является самым медленным компонентом.

Интегральным показателем оптимальности используемой дисковой подсистемы является длина очереди заданий.

- **LogicalDisk (PhysicalDisk)\Avg. Disk Queue Length.** Счетчик показывает среднюю очередь заданий (операций записи или чтения) для соответствующего диска. Интерпретация данного параметра достаточно проста: если существует очередь на дисковые операции, то это означает, что диски не справляются с записью/чтением информации. Поскольку дисковая подсистема обычно является самым медленным компонентом, а данный счетчик отображает среднее значение, то уже само наличие очереди (значение счетчика, большее примерно 0,5) существенно замедляет скорость вычислений. Поэтому оптимально добиваться минимально возможных значений для данного счетчика (0,1 и менее).
- **% Disk Time.** Счетчик показывает процент времени, в течение которого система "занята" операциями ввода-вывода. Высокие показания (50% и более) могут косвенно свидетельствовать о том, что нужно подумать об использовании более быстрой дисковой подсистемы.
- **Определение источника дисковой активности.** В реальных системах часто причиной повышенной дисковой активности бывают не только "полезные" программы, но те или иные сервисные процессы. Поэтому при оптимизации работы системы с дисками следует проанализировать процессы, инициирующие опера-

ции обмена с дисками, составить перечень файлов, работа с которыми ведется наиболее активно, и т. п.

Определить наиболее активные процессы и узнать, в какие файлы пишутся (читаются) данные, в Windows поможет программа **Монитор ресурсов**. Администратор может отсортировать процессы по желаемому типу активности, отфильтровать информацию и т. д. (рис. 14.19).

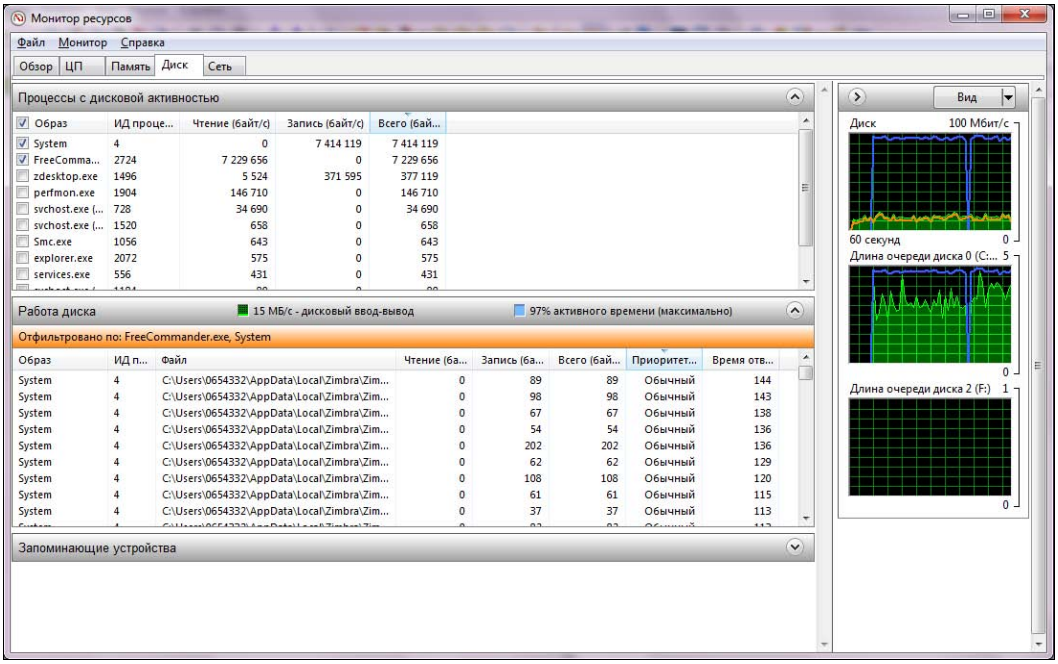


Рис. 14.19. Окно программы **Монитор ресурсов** с отфильтрованными данными дисковой активности

> ***Примечание***
>
> Программа **Монитор ресурсов** доступна только для ОС Windows Vista/Windows 7/Server 2008. Определить причины дисковой активности в предыдущих версиях (например, в Windows XP/Server 2003) значительно труднее. Можно порекомендовать воспользоваться в этом случае утилитами от Sysinternals (FileMonitor, ProcessMonitor) или другими аналогичными средствами.

Для Linux-систем аналогичной функциональностью обладает, например, утилита `iotop`, позволяющая вывести на экран названия процессов с наибольшей дисковой активностью и отобразить соответствующие файлы.

В листинге 14.2 представлены первые строки вывода данной команды.

Листинг 4.2. Фрагмент вывода утилиты `iotop`

```
Total DISK READ: 0.00 B/s | Total DISK WRITE: 102.91 K/s
TID PRIO USER DISK READ DISK WRITE SWAPIN IO> COMMAND
279 be/3 root 0.00 B/s 59.37 K/s 0.00 % 2.05 % [jbd2/dm-0-8]
```

```
2690 be/4 nagios 0.00 B/s 3.96 K/s 0.00 % 0.00 % nagios -d
                                    /usr/local/nagios/etc/nagios.cfg
317 be/4 www-data 0.00 B/s 7.92 K/s 0.00 % 0.00 % apache2 -k start
1 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % init
2 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kthreadd]
......
```

Оценка работы сетевого адаптера

Для оценки работы сетевого адаптера используется тот же подход, что и для подсистемы ввода-вывода системы хранения: использование полосы пропускания должно быть ниже предела скорости передачи и в очереди на отправку пакетов не должно быть.

Обычно считается допустимым среднее значение очереди, равное 1.

Что касается использования полосы пропускания, то для сети, выполненной по стандарту Ethernet, — а это практически все локальные компьютерные сети, — величина утилизации сети равная 60% уже считается критической; на практике следует внимательно проанализировать работу сети при достижении порога утилизации порядка 30—40%.

На практике достаточно редко эти показания снимаются с сетевой карты компьютера. Как правило, используется получение данных с портов управляемых коммутаторов (по протоколу SNMP).

> ***Примечание***
>
> Счетчики отображают объемы передаваемой и принимаемой информации в байтах, тогда как скорость сети указывается в битах (100 Мбит/с, 1 Гбит/с и т. д.). Поэтому, показания счетчика надо умножить на 8, чтобы сравнивать с максимально возможной скоростью передачи данных.

Углубленный анализ производительности системы

Понятно, что суммарные показатели счетчиков дадут достаточно грубую оценку состояния системы. Для анализа причин недостаточной производительности необходимо учесть ряд параметров, описание которых приведено в табл. 14.2.

> ***Примечание***
>
> В таблице указаны счетчики для Windows-систем. Для Linux-систем часть параметров может использоваться в качестве ориентировочных значений.

Перечисленные счетчики характеризуют общее состояние системы. Если на сервер установлено специализированное программное обеспечение, то администратор должен провести анализ показаний счетчиков этого пакета. Понятно, что в рамках издания мы не сможем описать параметры счетчиков даже основных пакетов. С соответствующей документацией необходимо знакомиться самостоятельно.

В качестве примера дадим краткий обзор счетчиков одного из наиболее часто устанавливаемых серверных пакетов — сервера баз данных Microsoft SQL (табл. 14.3).

Таблица 14.2. *Счетчики для быстрой оценки состояния системы*

Счетчик	Описание и пороговые значения оценки
Processor % Privileged Time	Счетчик показывает время работы процессора в привилегированном режиме. В этом режиме осуществляется доступ к дискам, обработка прерываний устройств и т. п. Высокое значение этого показателя может говорить о проблемах в работе сервера. Критическое значение счетчика — примерно 30%, величина для предупреждения — 20%. Высокие значения показателя могут являться следствием проблем использования дисковой подсистемы, сети или высоким значением показателя числа переключений контекста. Поэтому эти счетчики должны быть также исследованы при возникновении проблемной ситуации
Network Interface % Network Utilization	Значение более 50% должно восприниматься, как требующее внимания. Более 80% загрузки сети — критический порог
Network Interface Output Queue Length	Величина очереди пакетов на отправку в сеть. В нормальных условиях очереди быть не должно (сетевой интерфейс должен справляться с нагрузкой). Величина очереди в 1 пакет — состояние предупреждения, в 2 пакета — критическое
System Processor Queue Length — \System\ Processor Queue Length	Показатель данной очереди свидетельствует о числе заданий процессора, которые ждут своего выполнения, поскольку выполняется другое задание. Очередь, более чем в 2 задания, — состояние предупреждения; более чем в 10 — критическое значение. Поскольку это единый показатель для системы, то для многопроцессорной системы указанные значения порогов должны быть разделены на число ядер. Примечание: в зависимости от специфики системы, иногда и величина очереди в 10 заданий на процессор может рассматриваться как допустимое значение. Счетчик должен анализироваться вместе со счетчиками **Processor\% Processor Time**
\System\Context Switches/sec	Показатель числа переключений контекста. Показатель должен анализироваться совместно с параметрами нагрузки процессора. Если число переключений больше 2500 при величине привилегированного времени процессора в 20% или 10 000 переключений при общей загрузке процессора в 50% — состояние предупреждения. При числе переключений более 5000 и 30% привилегированного времени процессора или 20 000 переключений при более чем 70% загрузке процессора — критическое состояние
Process(*)\% Processor Time	Показатель отображает использование процессом ресурсов процессора. В нормальной ситуации ни один процесс не должен монополизировать ресурсы системы (конечно, если сервер не обслуживает исключительно только одну задачу). Значения, после которых параметр нужно оценивать как критический или предупреждение, зависят от конкретной системы. Для оценки как "предупреждение" они могут быть как в пределах 5% для сервера общей направленности, так и 80% — для специализированного
Process Private Bytes — Process(_Total)\Private Bytes	Счетчик может свидетельствовать об утечках памяти. При анализе необходимо следить за трендом: разница в 250 Мбайт между минимальным и максимальным значениями, а также увеличение этого параметра со скоростью более 10 Мбайт в час должно восприниматься как состояние предупреждения. При разнице более 500 Мбайт и скорости роста 100 Мбайт в час состояние оценивается как критическое. Одновременно желательно контролировать параметр доступной памяти

Таблица 14.2 *(продолжение)*

Счетчик	Описание и пороговые значения оценки
Process(*)\Handle Count	Счетчик показывает число потоков процесса и косвенно может свидетельствовать о проблемах утечки ресурсов системы, если разница между минимальным и максимальным значением составляет более 250 и она увеличивается со скоростью более 100 единиц в час. Значения в 500 и 500, соответственно, свидетельствуют уже о критическом состоянии системы. При росте параметра желательно проконтролировать показатели для отдельных процессов, чтобы найти источник роста
Process(_Total)\Thread Count	Счетчик дескрипторов. Высокие показания для какого-либо процесса могут свидетельствовать о проблемах с данным приложением. Значение порядка 250 с ростом в 100 единиц в час должно восприниматься как состояние предупреждения, а 500/500 — как критическое. Желательно при наличии проблем проконтролировать счетчик числа переключений контекста, который может также приблизиться к критическим значениям
Process(*)\Virtual Bytes	Счетчик показывает используемую процессом виртуальную память. Предупреждением является, если объем занимаемой памяти превышает более 75% от выделенного адресного пространства (2 Гбайт для 32-адресных ОС)
Process(*)\IO Data Operations/sec	Счетчик отображает количество операций ввода-вывода для процессов (включая обращения к диску, доступ к сети и другим устройствам). Предупреждением является число операций более 1000 в секунду. В случае высоких значений счетчика необходимо изучить показатели для каждого экземпляра и значения отдельно по операциям доступа к диску и к сети, чтобы найти источник повышенных значений
Process(*)\% Privileged Time	Счетчик показывает время работы процесса в привилегированном режиме. В этом режиме осуществляется доступ к дискам, обработка прерываний устройств и т. п. Высокое значение этого показателя может говорить о проблемах с вводом-выводом для определенных процессов
LogicalDisk(*)\% Free Space	Параметр отображает доступное свободное пространство логического диска. Принято считать, что значение данного параметра менее 5% свидетельствует о критическом состоянии, менее 10% — состояние предупреждения
Processor(*)\% Interrupt Time	Показатель отображает время процессора, используемое для обработки прерываний от устройств (системные часы, мышь, сетевые карты, жесткие диски и т. п.). Обычно такие устройства редко запрашивают внимания процессора (1 раз в 10 мс). Большая величина данного показателя может говорить о неисправности оборудования. Порог предупреждения — 30%, порог критического состояния — 50%
PhysicalDisk(*)\Avg. Disk sec/Read	Отображает время чтения данных с физического диска. Параметр зависит от типа установленных устройств (наличия аппаратных RAID-массивов). Для одиночного диска величина должна быть менее 15 мс, значение более 25 мс — критическое состояние
PhysicalDisk(*)\Avg. Disk sec/Read	Аналогичный параметр, только отображает усредненное значение. Пороговые значения те же

Таблица 14.2 *(продолжение)*

Счетчик	Описание и пороговые значения оценки
PhysicalDisk(*)\Avg. Disk sec/Write	Аналогичный параметр, только для операций записи на диск. Пороговые значения такие же
LogicalDisk(*)\% Idle Time	Параметр косвенно связан с длиной очереди операций с диском. Значение в 0% соответствует постоянному наличию операций ввода-вывода на диске (значение очереди равно 1 и более). Нормальный диапазон — не менее чем 10%
Memory\Free System Page Table Entries	Показывает число страниц памяти, которые не использованы системой. Значение менее 20 000 свидетельствует о наличии проблем. Критическое состояние возникает, если данный показатель меньше 8000
Memory\Pool Nonpaged Bytes	Счетчик отображает значение памяти системы, которая не может быть выгружена (записана на диск в файл виртуальной памяти). Порог предупреждения — 60%, критического значения — 80%. Часто проблемы с пулом невыгружаемой памяти связаны с пользовательскими процессами (библиотеками). Для поиска причин необходимо использовать длительный мониторинг (неделю и более параметров памяти и процессов)
Memory\Pool Paged Bytes	Показатель отображает процент использования пула памяти. Порог для предупреждения — 60%, критического состояния — 80%. В случае высоких значений необходимо отслеживать процессы и память, чтобы найти причины. Возможный вариант устранения нехватки памяти — переход на 64-битные системы
Memory\Pages/sec	Счетчик показывает скорость обмена страниц с виртуальным файлом памяти. Обычно высокий обмен связан с нехваткой оперативной памяти. 1000 страниц в секунду при менее чем 100 Мбайт доступной памяти — предупреждение
Process(_Total)\ Working Set	Параметр характеризует используемую процессом память. При недостатке оперативной памяти она будет изыматься из объема, предоставленного процессам. Этот счетчик имеет значение для качественной оценки вкупе с одновременным контролем показаний свободной памяти. Имеет смысл также контролировать рост данного параметра. Увеличение его более чем на 100 Мбайт за час может свидетельствовать о проблемах работы системы
Memory\System Cache Resident Bytes	Счетчик показывает текущий объем физической памяти, которую система может записать в файл виртуальной памяти. В нормальной ситуации этот объем не должен быть менее 50% объема установленной в системе памяти. Анализ показателей должен проводиться с учетом счетчиков ввода-вывода (поскольку этот кэш может заниматься системой при высокой нагрузке операций ввода-вывода)
Paging File(*)\% Usage	Пороговые значения: 70% для предупреждения, более 90% — критическое
Memory\% Committed Bytes In Use	Счетчик показывает значение процентное используемого объема физической памяти, для которого зарезервирован объем в виртуальной памяти, к сумме значений физической памяти и всех файлов виртуальной памяти. Пороговые значения: 70% для предупреждения, более 90% — критическое. При повышенных значениях достаточно увеличить объем файлов виртуальной памяти

Таблица 14.2 *(окончание)*

Счетчик	Описание и пороговые значения оценки
Server\Pool Nonpaged Failures	Показатель числа ошибок резервирования физической памяти. Говорит о недостатке физической памяти в системе
Memory\Pages Output/sec	Счетчик показывает скорость записей страниц памяти на диск (для освобождения физической памяти). Показатель имеет оценочный характер
Memory\Transition Pages RePurposed/sec	Оценочный показатель. Говорит о вторичном использовании страниц памяти (имеет значение для ускорения операций)
Network Interface(*)\ Packets Outbound Errors	Показывает число пакетов, которые не могут быть отправлены из-за ошибок. Показания данного счетчика в нормальных условиях должны стремиться к нулю
PhysicalDisk(*)\Current Disk Queue Length	Показатель текущего значения очереди операций с диском. В нормальных условиях должен быть менее 2 (см. примечания для счетчиков диска)
LogicalDisk(*)\Avg. Disk Queue Length	Показатель среднего значения очереди операций с диском. В нормальных условиях должен быть менее 2
Processor(*)\% DPC Time	Время, которое процессор тратит на обработку DPC (Deferred Procedure Calls). Обработка этих прерываний выполняется в привилегированном режиме, но с меньшим приоритетом. Пороговые значения для состояния предупреждения — 20%
Processor(*)\DPC Rate	Показатель скорости добавления прерываний DPC в обработку. Пороговые значения: более 10 — предупреждение, более 20 — критическое состояние. Свидетельствует косвенно о неисправности оборудования
Memory\Pages Input/sec	Счетчик показывает число страниц памяти, считанных с жесткого диска, за единицу времени. Пороговое значение предупреждения — 1000
Network Interface(*)\Bytes Total/sec	Показатель суммарной скорости приема и передачи через сетевой адаптер
Processor(*)\% User Time	Процент времени, который затрачивается процессором для работы в режиме пользователя. Зависит от выполняемого приложения. Показатель должен оцениваться в сравнении с показателями привилегированного режима
Cache\Lazy Write Flushes/sec	Счетчик показывает скорость записи изменений файлов на диск (для ускорения операций записи система производит изменения файла в памяти и продолжает работу; затем в фоне производится запись изменений в файл; этот процесс называется Lazy Writing). Значение более 100 свидетельствует о том, что изменения не успевают заноситься на диск
PhysicalDisk(*)\Disk Bytes/sec	Показатель скорости работы с диском. Зависит от конкретной реализации дисковой подсистемы. Для зеркального RAID с дисками 7200 RPM нормальное значение составляет около 20 Мбайт/с

Таблица 14.3. *Счетчики оценки параметров производительности MS SQL-сервера*

Счетчик	Описание и пороговые значения оценки
Process(sqlservr)\% Privileged Time	Пороговые значения: предупреждение — 20%, критическое — 30%. Целесообразно соотнести со значениями счетчиков производительности жесткого диска. Недостаточно быстрые устройства могут вызвать повышение данного параметра. Причины могут быть связаны со значениями ожидания SQL Server (**Latch Waits**, **SQL Server: Wait Statistics**), антивирусными программами, некачественными драйверами и т. п.
SQLServer: Access Methods\Forwarded Records/sec	Данный счетчик должен анализироваться совокупно со счетчиком **\SQLServer:SQL Statistics\Batch Requests/sec**. Значение более 1 пересланного запроса на 10 пакетных запросов должно оцениваться как состояние предупреждения. Пересланные запросы появляются тогда, когда происходят изменения данных на сервере базы и новые данные по размеру превосходят существующие. В результате сервер перемещает данные в новое место. В результате сканирование таблиц данных происходит неоптимально. Параметр может использоваться только в случае отсутствия кластеризованного индекса на таблице
SQLServer: Access Methods\FreeSpace Scans/sec	Данный счетчик должен анализироваться совокупно со счетчиком **\SQLServer:SQL Statistics\Batch Requests/sec**. Значение более 1 сканирования на 10 пакетных запросов должно оцениваться как состояние предупреждения. Вставка данных в таблицу без кластеризованного индекса приводит к операции поиска свободного пространства, что является дополнительными операциями ввода-вывода и снижает полезную производительность сервера: • могут наблюдаться кратковременные тайм-ауты взаимодействия с серверов; • могут быть периоды повышенной нагрузки на процессор и т. д.
SQLServer:Access Methods Full Scans/sec	Счетчик показывает число полных сканирований таблиц или индексов. Причиной могут быть плохие индексы, запрос слишком большого количества данных и т. д. Необходимо анализировать количество полных сканирований по отношению к числу поиска по индексу (**Index Searches/sec**): на 1000 случаев использования индекса должно быть не более 1 полного сканирования. Кроме того, имеет смысл отслеживать и общее число полных сканирований (оно не должно быть большим, например, достигать 1000)
SQLServer:Access Methods Page Splits/sec	Данный счетчик должен анализироваться совокупно со счетчиком **\SQLServer:SQL Statistics\Batch Requests/sec**. Значение более 1 на 20 пакетных запросов должно оцениваться как состояние предупреждения. В любом случае значение этого показателя должно быть минимальным. Разделение таблиц индекса происходит при вставке новых данных в таблицу с заполненным индексом. В этом случае для образования новой записи в индексе его страница должна быть разделена
SQLServer:Access Methods\Scan Point Revalidations/sec	Порог предупреждения — 10 единиц в секунду. Данные события возникают в случае вставки новых значений во время сканирования диапазона данных. В этом случае сервер производит пересканирование, которое называется Scan Point Revalidation. Показатель необходимо оценивать вместе со счетчиками **Range Scans/sec** и счетчиками **Page Latch**. Высокое значение показателя может быть следствием плохого индекса

Таблица 14.3 *(продолжение)*

Счетчик	Описание и пороговые значения оценки
SQLServer:Access Methods Workfiles Created/sec	Данный счетчик должен анализироваться совокупно со счетчиком **\SQLServer:SQL Statistics\Batch Requests/sec**. Значение более 1 создаваемого файла на 20 пакетных запросов должно оцениваться как состояние предупреждения. Workfiles создаются во временной базе для обработки запросов, которые слишком велики для размещения в оперативной памяти. Для уменьшения значения необходим дополнительный анализ базы данных
SQLServer:Access Methods Worktables Created/sec	Порог предупреждения: создание более чем 200 Worktables в секунду. Worktables — это временные таблицы, создаваемые для хранения запросов, курсоров, переменных. Высокое значение показателя может быть свидетельством того, что временная база данных является бутылочным горлышком системы. Высокие значения требуют последующего анализа с использованием SQL Profiler
SQLServer:Buffer Manager Buffer cache hit ratio	Счетчик показывает относительное число страниц памяти с данными, которые использованы сервером без обращения к жесткому диску. Значение должно быть максимально близким к 100%. Порог предупреждения: менее 97%
SQLServer:Buffer Manager Lazy writes/sec	Пороговое значение: 20 для предупреждения. Этот счетчик показывает, как часто устаревшие буфера записываются на диск. Большое значение может свидетельствовать о проблемах с вводом-выводом сервера
SQLServer:Buffer Manager Page life expectancy	Пороговое значение: менее 5 минут (300) для критического состояния. Высокое значение (менее 300) свидетельствует о увеличенном числе операций ввода-вывода. Счетчик отображает один из критических параметров SQL-сервера
SQLServer:Buffer Manager Page lookups/sec	Данный счетчик должен анализироваться совокупно со счетчиком **\SQLServer:SQL Statistics\Batch Requests/sec**. Значение более 100 поисков на каждый пакетный запрос должно оцениваться как состояние предупреждения. Высокое значение свидетельствует о неоптимальной настройке памяти
SQLServer:Buffer Manager Page reads/sec	Пороговое значение: более 90 операций чтения — предупреждение. Значение менее (90—80 и менее) — состояние нормальное
SQLServer:General Statistics Logins/sec SQLServer:General Statistics Logouts/sec	Пороговое значение: более 2 в секунду — предупреждение. Такое значение может свидетельствовать о том, что приложения не настроены на совместное использование подключения
SQLServer:Memory Manager Memory Grants Pending	Счетчик показывает ожидание момента выделения памяти. Значение должно быть близким к нулю, иначе возможны ошибки выполнения запросов (по тайм-ауту)
SQLServer:Memory Manager\Target Server Memory (KB) SQLServer:Memory Manager\Total Server Memory (KB)	Анализироваться должна разница показаний этих двух счетчиков. Обычно объем выделяемой памяти должен соответствовать объему запрашиваемой. Разница более 500 Мбайт является основанием для отнесения ситуации к уровню предупреждения

Таблица 14.3 *(окончание)*

Счетчик	Описание и пороговые значения оценки
SQLServer:SQL Statistics Batch Requests/sec	Счетчик показывает нагрузку сервера баз данных. Значение более 1000 соответствуют крайне загруженному серверу. Примечание: показатель должен корректироваться в зависимости от аппаратной конфигурации сервера
SQLServer:SQL Statistics SQL Compilations/sec	Пороговое значение: 1 компиляция на каждые 100 запросов — предупреждение
SQLServer:SQL Statistics SQL Re-Compilations/sec	Пороговое значение: 1 перекомпиляция на каждые 10 запросов — предупреждение
SQLServer:Locks(*)\Lock Requests/sec	Значение числа блокировок, которые препятствуют мгновенному выполнению задания
SQLServer:Locks(*)\Lock Waits/sec	Суммарное время ожидания завершения блокировок за последнюю секунду

Варианты оптимизации компьютера

Если какой-либо компонент компьютера является узким местом, то надо предпринять меры по его модернизации.

Если не справляется процессор

Заменить процессор в реальной системе маловероятно. Хорошо, если анализируемая система является виртуальной машиной. В этом случае можно добавить еще один виртуальный процессор. Для физических же серверов практически единственным способом разрешения проблем излишней нагрузки на процессор является уменьшение числа решаемых задач.

Если дисковая подсистема недостаточно быстра

Какие могут быть варианты решения проблемы при обнаружении узкого места в дисковой подсистеме?

Самый эффективный путь — добавление жестких дисков в соответствующий RAID-массив, на базе которого создан логический диск. Чем больше жестких дисков объединены в логический, тем более производительным он будет.

Во-вторых, если позволяет устройство хранения, выберите оптимальные для используемого типа данных варианты RAID-массивов. Не забывайте, что самый популярный тип массива — RAID5 — не является самым быстрым.

Проанализируйте дисковую активность и отключите необязательные задачи, ведущие запись информации на диск (например, откажитесь от излишнего протоколирования, перенесите фоновые операции дефрагментирования на периоды минимальной активности и т. п.).

Убедитесь, что в системе установлено достаточно оперативной памяти. Увеличьте ее при нехватке.

Обратите внимание, чтобы на дисках было достаточно свободного места (не менее 20% их объема). Проведите дефрагментацию дисков, уменьшите или исключите использование сжатия и шифрования файлов на тех дисках, на которых выявлена проблема низкой производительности. Для NTFS-дисков можно отключить запись имен файлов в формате 8.3 и запись времени последнего доступа к файлу (для чего в ветви `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Filesystem` надо установить в значение 1 параметры `NtfsDisable8dot3NameCreation` и `NtfsDisableLastAccess` соответственно).

Если эти операции не приведут к успеху, следует искать возможность приобрести более быструю дисковую подсистему.

Примечание

Если позволяют характеристики системы хранения, то можно выполнить точную настройку таких параметров, как размер кластера и т. п. Обычно такие настройки необходимо выполнять до создания логического диска, изменения их можно провести только с уничтожением хранимой информации. Поэтому данные настройки необходимо тщательно планировать на этапе ввода системы хранения в эксплуатацию.

Когда не справляется сетевой адаптер

Улучшить работу сетевого адаптера крайне сложно. Можно порекомендовать обновить его драйвер. Кроме того, иногда бывает, что параметры подключения, которые по умолчанию выставляются в режим *авто*, устанавливаются не на максимальную производительность. Например, вместо полного дуплекса будет использован режим полудуплекса или даже установлена более низкая скорость работы. Выяснить такие "отклонения" можно, если посмотреть состояние сетевого порта коммутатора, к которому подключен данный сетевой адаптер. Если состояние порта не оптимальное, то необходимо вручную сменить настройку и зафиксировать ее в требуемом значении.

Если настройки оптимальны и большой трафик свойственен нормальным условиям работы системы, то необходимо либо добавить еще один сетевой адаптер, либо перейти на сеть с большей скоростью передачи данных.

После установки дополнительного сетевого адаптера данные будут передаваться одновременно по нескольким каналам, в результате чего нагрузка на отдельный канал снизится (примерно пропорционально числу каналов) и будет находиться в приемлемых диапазонах. Такое объединение *(агрегирование)* сетевых адаптеров на серверной стороне канала передачи реализуется программным обеспечением сетевых адаптеров наиболее известных вендоров (например, ProSet для адаптеров изготовления фирмы Intel). Поэтому лучше всего при установке дополнительного адаптера выбирать модель, идентичную уже установленной в сервере. Соответствующие возможности нужно уточнить по документации.

Примечание

В случае особой интенсивности сетевого трафика администраторы могут настроить некоторые параметры TCP/IP-протокола через реестр системы (например, размеры передаваемого окна или число пакетов, после приема которых нужно высылать под-

твержение получения данных). Как правило, эти параметры автоматически настраиваются системой, и устанавливать их вручную имеет смысл только при большом числе сетевых подключений (при массовом обслуживании). Соответствующие настройки следует уточнить по описанию операционной системы.

Аналогично если не хватает полосы пропускания между двумя коммутаторами локальной сети, то следует создать вторую, параллельную линию связи и объединить их (агрегирование каналов средствами коммутационного оборудования). Для регулировки (чтобы минимизировать влияние сетевого трафика одних программ на другие) следует ввести настройки качества обслуживания (установить приоритеты трафика) и ограничения используемой полосы пропускания (так называемый *shaping*).

Дополнительные средства, используемые при анализе показателей производительности

Logman.exe

Команда Logman.exe из состава Windows используется для запуска и прекращения сбора данных файлов журнала на удаленном компьютере.

Для начала записи в журнал производительности нужно выполнить команду

```
logman start название_журнала
```

Кроме того, что с помощью данной команды можно настроить сбор журнала (указать время начала операции и завершения, частоту сбора, определить счетчики и т. д.), в составе ключей есть возможность настройки выполнения внешней команды. Это позволяет, например, отослать созданный файл журнала по электронной почте или передать его по протоколу FTP.

Relog.exe

Средство Relog.exe позволяет преобразовывать файлы журнала (например, журнал Windows NT 4.0 в журнал Windows XP или журнала в двоичном формате (BLG) в формат с разделяющими запятыми (CSV)). При этом можно настраивать выборку счетчиков для такого преобразования, определять временные диапазоны, за которые надо учитывать значения счетчиков и т. п.

Iometer

Средство Iometer используется для тестирования дисковой подсистемы.

Нелишне убедиться, что фактическая производительность дисковой подсистемы соответствует характеристикам оборудования. Диски различных вендоров отличаются по своим параметрам весьма незначительно. Так, для дисков с частотой вращения 7200 об/мин среднее время записи-чтения (без учета кэширования) составляет не более 15 мс. Оно должно быть соответственно меньше с учетом объединения дисков в RAID-массив.

Существует несколько утилит, предназначенных для проверки параметров скорости работы устройств хранения, но наиболее известным и практически профессио-

нальным инструментом является Iometer (**http://sourceforge.net/projects/iometer/files/**) — пакет, первоначально разработанный Intel и впоследствии переданный сообществу Open Source.

Программа позволяет получить реальные параметры работы устройств хранения, однако для получения результата необходимо сначала внимательно ознакомиться с документацией (на что часто не хватает желания у системных администраторов). Причина в том, что в настройках программы необходимо указать большое количество параметров, влияющих на оценку производительности. Например, размер блоков хранения, процент операций записи-чтения и т. д. Причем эти значения будут различны для отличающихся вариантов использования дисков: одни значения необходимо указать для проверки дисков, предназначенных для работы с базами данных, другие — для файловых серверов и т. п. Для упрощения можно использовать вариант параметров, изначально разработанный Intel, который можно загрузить со страницы **http://docs.aboutnetapp.ru/iometer2.icf**. Скопированный с этой страницы текст нужно сохранить в файле и импортировать эти настройки в конфигурацию программы.

Комплект поставки включает два файла. Dinamo используется для управления тестированием на нескольких устройствах, iometer — файл, который следует запустить для проверки. После запуска следует импортировать файл конфигурации как описано ранее, не забыть ограничить размер файла, который создается для тестирования в корне диска (заменить значение **Maximum Disk Size** на допустимое число секторов[1] в файле теста, иначе файл будет создан на всем свободном пространстве

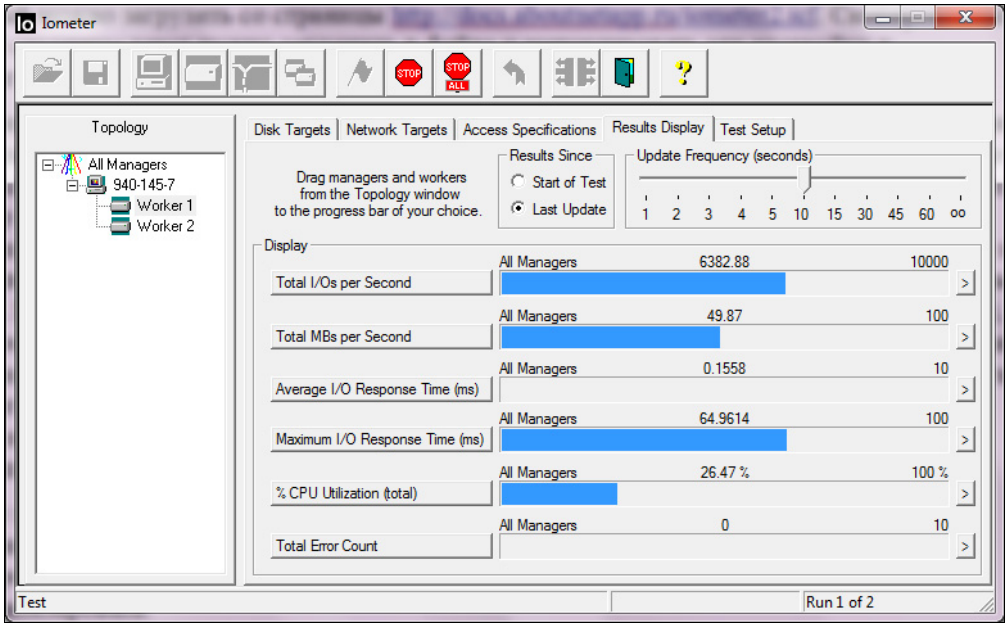


Рис. 14.20. Параметры диска, отображаемые утилитой `iometer`

[1] Не забывайте, что один сектор равен 512 байтам. Соответственно и рассчитывайте размер файла.

диска) и выбрать на вкладке **Access Specifications** необходимые тесты. По умолчанию в программе создается такое число процессов тестирования *(worker)*, которое соответствует числу процессоров в системе. Но их количество можно изменить, как и сменить количество одновременных потоков ввода-вывода *(# of Outstanding IO)*. Простые приложения обычно используют 1—4 потока ввода-вывода, приложения уровня предприятия, например Oracle, могут создавать и до 256 потоков. Из других параметров, которые можно настроить, отметим **Ramp Up Time** (время на разогрев диска перед началом теста) и **Run Time** — максимальное время тестирования (если вы хотите завершить тестирование по истечении заданного периода времени).

После запуска теста на вкладке **Results Display** можно наблюдать за получаемыми значениями (следует только назначить моменты обновления данных — рис. 14.20). Обратите внимание, что набор отображаемых на диаграмме параметров допускает изменения по желанию оператора. Итоговые значения тестирования будут сохранены в CSV-файле, который можно будет впоследствии проанализировать.

PAL

Для операционных систем Windows можно рекомендовать утилиту PAL (Performance Analysis of Logs, доступна с загрузки по ссылке **http://pal.codeplex.com/**). Эта утилита написана на PowerShell, в качестве входного файла использует двоичный журнал счетчиков, в нее включены шаблоны оценок для основных серверов Microsoft (Windows Server, MS SQL, Exchange, SharePoint и т. д.), а результаты анализа могут быть представлены в виде графиков. Программа расширяет возможности отчетов производительности, включенных в систему. Так, при необходимости пользователь может откорректировать шаблоны или создать собственный набор критериев.

На рис. 14.21 показан фрагмент отчета, сформированного PAL по результатам оценки производительности сервера. В верхней части фрагмента перечислены показатели, значения которых выходят за пределы нормального функционирования системы. В нижней части рисунка — график показателя производительности, по которому легко можно определить моменты перехода к критическим значениям.

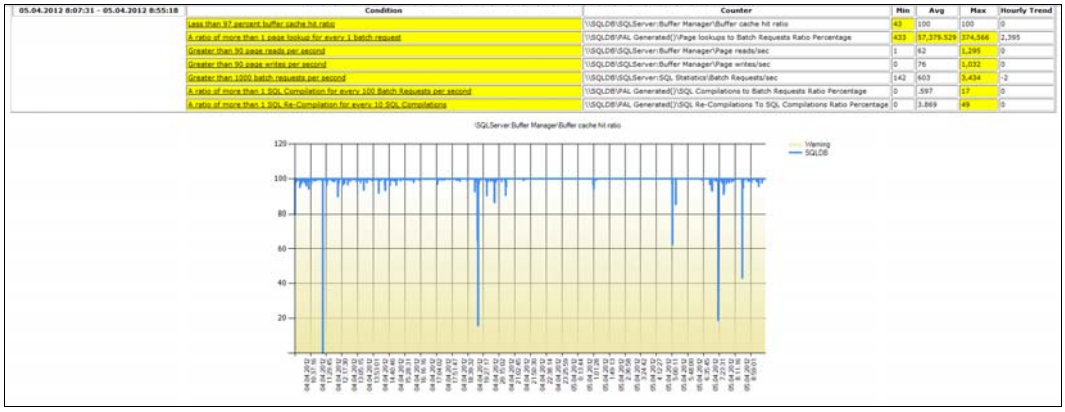


Рис. 14.21. Фрагмент отчета, сформированного PAL

Утилиты настройки параметров дисковой подсистемы Linux

Для тонкой настройки параметров дисковой подсистемы в Linux можно использовать средства hdparm и tune2fs. Описания их использования доступны через справочную систему (man hdparm, man tune2fs). Конечно, можно найти и другие средства, но указанные утилиты имеются в системе по умолчанию.

Следует заметить, что прибегать к ним следует только при наличии определенного опыта и обязательно сохранить первоначальные настройки системы, чтобы можно было восстановить начальные значения.

Предметный указатель

L

M

N

O

P

R

S

T

V

W

О

П

Р

С

Т

У

Ф

Ш