Александр Кенин

САМОУЧИТЕЛЬ СИСТЕМНОГО АДМИНИСТРАТОРА

3-е издание

Санкт-Петербург
«БХВ-Петербург»
2012

УДК 681.3.06
ББК 32.973.26-018.2
К35

Кенин А. М.

К35 Самоучитель системного администратора. — 3-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2012. — 512 с.: ил. — (Системный администратор)

ISBN 978-5-9775-0764-6

Изложены основные задачи системного администрирования, описаны базовые протоколы, даны рекомендации по выбору оборудования и проведению ежедневных рутинных операций. Подробно раскрыты технологии, используемые при построении информационных систем, описаны средства мониторинга и обслуживания как малых, так и распределенных сетей. Рассмотрены методы централизованного управления, основы создания безопасной среды. Даны рекомендации по поиску неисправностей, обеспечению защиты данных. Параллельно рассмотрены решения на основе операционных систем Windows и Linux с использованием как проприетарных, так и открытых технологий. Книга написана на основе многолетнего опыта разработки и практического администрирования информационных систем.

В третье издание включены разделы с описанием новейших технологий, в том числе облачных и систем высокой доступности, рекомендациями по оптимизации производительности, существенно дополнены разделы по настройке систем, поиску неисправностей, виртуализации серверов и рабочих станций.

Для начинающих системных администраторов

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Редактор	*Юрий Рожко*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Виктория Пиотровская*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Марины Дамбиевой*

Подписано в печать 30.03.12.
Формат $70\times100^{1}/_{16}$. Печать офсетная. Усл. печ. л. 41,28.
Тираж 2000 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-5-9775-0764-6

Оглавление

Предисловие

Эта книга написана для всех тех, кто занимается созданием и эксплуатацией информационных систем. Я попытался отойти от конкретных рекомендаций и дать оценку тем или иным технологиям, в большей степени учитывая практический опыт и в меньшей — видение менеджеров по продажам.

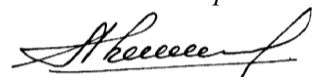
Занимаясь более 20 лет администрированием и развитием компьютерных систем, оказывая техническую поддержку, я постоянно сталкиваюсь с однотипными проблемами и вопросами пользователей и специалистов. И каждый раз я пытаюсь простыми и доходчивыми словами объяснить основы, на которых построена современная информационная система, понимая которые можно успешно контролировать ситуацию.

Возможно, что в некоторых местах я не академически строг. Вероятно, что некоторые читатели критически воспримут рекомендации, которые даются мною на основании, прежде всего, личного опыта. Цель книги заключается и в том, чтобы выработать у пользователя собственную позицию, а не идти на поводу рекламных материалов и заказных статей.

Если вас больше интересуют практические советы, то их можно найти в другой моей книге (см. Практическое руководство системного администратора. — СПб.: БХВ-Петербург, 2010. — 464 с.). Я считаю, что эти книги дополняют друг друга.

Предполагается, что читатель этой книги знаком с основами компьютерных технологий. Свои замечания и предложения вы можете направлять непосредственно мне по электронной почте на адрес **kenin@hotbox.ru** или на адрес издательства "БХВ-Петербург" **mail@bhv.ru** с указанием названия книги и автора.

Ваш Александр Кенин



ГЛАВА 1

Системное администрирование

Специалиста, который объединял компьютеры пользователей в единую сеть и поддерживал работоспособность такой системы, назвали *системным администратором*. В настоящее время увеличивающаяся структуризация сети, появление разнообразных прикладных программ, разработка новых сетевых служб и т. п. все более и более усложняют задачу квалифицированного управления компьютерной системой.

Системный администратор

В нашей стране практически отсутствует понимание места и роли системного администратора. В небольших организациях таковым считают работника, который в одиночку выполняет обязанности по обслуживанию компьютерного парка. В крупных организациях системными администраторами называют как специалистов, которые сопровождают рабочие места пользователей, так и сотрудников, отвечающих за функционирование тех или иных информационных систем предприятия. При этом *технического* специалиста, отвечающего за работу всей системы, как правило, в штате организации нет. Считается, что эти функции выполняют руководители отделов ИТ/ИТ-директора предприятий, но руководство подразделением и системное администрирование — это, как мне кажется, весьма различающиеся направления работы. В результате техническая политика часто отдается на откуп внешним "системным интеграторам", которые в результате проводят линию *вендоров*[1], с которыми у них есть соглашения о партнерстве.

Системный администратор — это специалист, отвечающий за функционирование и развитие информационной системы. Это тот человек, который должен представлять работу всех компонентов в комплексе, в то же время, понимая особенности каждого отдельного элемента. Системный администратор — высшее звено иерархии информационной системы. Он должен координировать работу и специалистов

[1] *Вендор* (от англ. *vendor* — продавец, торговец) — юридическое или физическое лицо, являющееся поставщиком товаров и услуг, объединенных торговой маркой. — *Ред.*

служб технической поддержки, и администраторов подразделений, и руководителей отдельных автоматизированных систем, и офицера информационной безопасности — всех сотрудников "узкой" специализации.

Конечно, знать в совершенстве все технологии, применяемые в современных информационных системах, одному человеку практически невозможно. Как следствие этого на крупных предприятиях создаются целые группы сотрудников, части из которых поручается только поддержание функционирования систем, другой части — развитие и внедрение новых технологий, третьей — взаимодействие с пользователями и т. д. В итоге не остается специалиста, сохраняющего комплексное понимание *всех служб* сети.

Не способствует комплексному подходу и ставший в последнее время популярным *проектный подход*. Небольшие предприятия не могут оплатить проект, а средние предприятия поглощаются крупными. Причем крупные проекты очень привлекательны для различных "распильных" схем, что сильно снижает технический уровень их проработки.

На практике системное администрирование зачастую становится только первой ступенью вхождения в компьютерный бизнес для молодых работников, которые, освоив первичные функции управления компьютерными системами, без особых раздумий о безопасности данных, надежности информации, предупреждении отказов, комфортности пользователей и т. д. — "лишь бы работало", стараются при первом же удобном случае перейти в группы разработки ИТ-проектов или стать продавцами программ и компьютеров. А предприятия остаются без системного администратора, вновь и вновь сталкиваясь с проблемами функционирования компьютерной системы.

Хороший системный администратор "созревает" не за один год. Многое невозможно узнать только по технической документации или по итогам специализированных курсов. Необходим опыт и, прежде всего, комплексный взгляд на систему, не затуманенный всепоглощающей рекламой того или иного производителя программного обеспечения. Нужен именно *системный* подход к *системному администрированию*.

Эта книга написана в помощь тем системным администраторам, которые дорожат своей работой, любят свою систему и хотят получить от своей деятельности максимум эффекта. В книге не делается акцент на последовательности выполнения той или иной операции: это хорошо описано в технической документации. Я попытаюсь объяснить основные принципы, заложенные в основу тех или иных технологий, управлять которыми приходится системному администратору, а также попробую дать свое видение различных вариантов решений, с которым читатель волен согласиться или нет.

Регламент работы

Деятельность администратора — это непрерывный процесс возникновения проблем, их решения, появления новых вопросов и т. д. Качество же работы практически пропорционально его "незаметности": чем стабильнее работает система (нет

проблем у пользователей) и чем быстрее разрешаются инциденты, тем профессиональнее специалист, обслуживающий такую систему.

Стабильная работа информационной системы не получается сама собой. Обычно она является результатом планомерной работы системного администратора по обслуживанию оборудования и программных средств, по анализу возникающих событий и выработкой решений, предупреждающих тот или иной отказ (так называемый, *проактивный мониторинг*).

Попытка привести пример возможных плановых операций системного администратора приведена в *главе 12*. Описания средств мониторинга даны в *главе 7*. Некоторые способы повышения отказоустойчивости информационной системы администраторы смогу почерпнуть из материалов *главы 10*. Также имеет смысл регламентировать порядок разрешения возможных инцидентов. Например, можно определить время ввода в эксплуатацию нового компьютера, срок восстановления системы из резервной копии на новом оборудовании и т. п. Чем более подробно будут классифицированы возможные ситуации, тем меньше претензий потенциально возникнет у пользователей в отношении уровня их обслуживания.

Не стоит оценивать факт наличия подобного регламента лишь с точки зрения контроля над системным администратором. Данный документ может служить аргументом, например, для переноса сроков завершения работ в случае одновременного возникновения нескольких неисправностей. Кроме того, подобный регламент может быть основанием для решений руководителей: или они должны согласиться на несколько суток простоя в случае катастрофического отказа, либо должны будут изыскивать средства для приобретения оборудования холодного резерва.

Неплохо, если вы сможете развернуть ту или иную автоматизированную форму для фиксирования обращений пользователей и контроля их исполнения. Эта же программа может сослужить хорошую службу администраторам, только приступающим к работе в организации, в качестве базы знаний данного предприятия, по которой можно осуществлять предварительное обучение нового специалиста. Подобрать подобный продукт не составляет особого труда, поскольку большинство требований, предъявляемых на малых и средних предприятиях к данному классу ПО, реализовано в программах с открытым кодом. Достаточно выполнить поиск на сайте SourceForge.net (**http://www.sourceforge.net/**) и выбрать наиболее подходящий вариант из нескольких десятков проектов.

Выбор операционной системы

Воспитанные на домашних Windows-рабочих станциях, многие пользователи пытаются перенести свои знания только одной операционной системы в реальную жизнь. Однако современные системы, как правило, объединяют решения на различных операционных средах. В первую очередь учитываются вопросы производительности, факторы надежности, экономические аспекты решений и т. д.

Windows-системы отличаются удобным пользовательским интерфейсом, широким спектром прикладных программ, большой армией разработчиков. В результате

Windows фактически является доминирующей программой на конечных пользовательских местах, особенно в организациях и предприятиях, где выполняемые операции не всегда фиксированы четко.

В то же время большинство офисных задач, решаемых на компьютерах, относятся к работе с документацией, электронной почтой, серфингом Интернета. Эти задачи великолепно решаются и в бесплатных приложениях, за которые не нужно платить лицензионные отчисления. Поэтому в организациях, в которых начинают считать деньги и оценивать эффективность работы, постепенно начинают внедряться решения на открытых кодах и на персональных рабочих местах. Если говорить о бесплатных операционных системах, то в первую очередь следует назвать проект Ubuntu, в рамках которого выходят как серверные версии, так и пользовательские. Эти операционные системы поддерживаются крупными компаниями: OEM-партнерами являются ARM, Asus, Dell, Hewlett Packard, Lenovo, много компаний разрабатывают прикладное программное обеспечение и т. д. Группа разработчиков постоянно выпускает обновления, заплатки безопасности, гарантируется техническая поддержка специальных серверных версий длительного срока эксплуатации (5 лет) и т. д. Создается и российская бесплатная операционная система. Насколько известно, она выполнена на другом клоне Linux — Mandriva. Оценить ее можно будет после выпуска и начала эксплуатации. Принципиального значения выбор того или иного дистрибутива не имеет, главное — общая направленность процесса на неуклонное расширение решений открытого кода.

Информатизация все больше приходит и на производство. В производственных информационных системах эксплуатируются "тяжелые" приложения, исторически созданные для Unix-систем. На средних предприятиях такие решения переходят на ту или иную версию Linux. Среди наиболее известных можно упомянуть HP AIX, Oracle Solaris, RedHat.

*nix-системы отличаются, прежде всего, надежностью и стабильностью работы, возможностями тонкой настройки. Приложения, будучи запущены, не прерывают работы в течение многих месяцев.

> ***Примечание***
>
> Обозначение UNIX-подобной операционной системы, которая образовалась под влиянием UNIX, иногда сокращается до обозначения "*nix-система".

Стоимость владения

Выбор операционной системы, в том числе, зависит и от стоимости ее владения. Абстрактной стоимости владения не существует. В каждом конкретном случае она должна оцениваться для условий конкретного предприятия. Не верьте тому, что администратора Linux надо обучать, а администратор Windows уже подготовлен "по определению". На первичном уровне администрирования любой специалист, имеющий некоторое знакомство с информационными системами, достаточно быстро сможет начать управлять как Linux, так и Windows. А если возникает необходимость серьезной подготовки, то без обучения не обойтись как одному, так и другому специалисту.

Примечание

Для оценки: в зарубежных проектах на стоимость сопровождения программного обеспечения закладываются суммы, примерно в размере 1/5 общей стоимости продукта.

Открытые стандарты

На практике большинство информационных систем включает в себя компьютеры с различными операционными системами и прикладными программами. На каждом участке применяется наиболее оптимальное решение. Гарантом их работоспособности являются единые стандарты взаимодействия.

Страница Интернета может быть просмотрена в любом обозревателе — Firefox, Internet Explorer, Opera и т. д. Отсутствуют проблемы взаимной аутентификации пользователей Windows — Linux. В Windows реализован открытый стандарт Kerberos, а для взаимодействия по протоколам NTLM и т. п. имеется бесплатный продукт Samba, входящий в состав всех дистрибутивов Linux. Объединение каналов при передаче информации осуществляется на основе стандарта 803.2ad независимо от конкретной модели сетевого оборудования, установленного в сети передачи данных. Документы, подготовленные в MS Office, открываются в OpenOffice (бесплатная офисная система, предназначенная для Linux), и наоборот.

Подобных примеров можно привести много.

В то же время многие фирмы предлагают собственные уникальные технологии для реализации в информационной системе. Применять их или нет — серьезная проблема в каждом конкретном случае. Если вы используете уникальную технологию, то обычно получаете более высокую производительность, чем при типовом решении, но оказываетесь привязанными к конкретному вендору. При этом перспектива дальнейшей поддержки технической части решения производителем часто бывает не очевидной, если, конечно, очистить предложения от рекламных слоганов.

В любом случае я бы советовал ориентироваться в первую очередь на использование решений, описанных в открытых стандартах. И только в случае невозможности такого выбора применять *проприетарные* технологии и разработки.

Примечание

Проприетарным (от англ. proprietary — частное, патентованное) называют программное обеспечение, являющееся собственностью автора, сохраняющего за собой монопольное право на использование, распространение, копирование и аналогичные операции. Проприетарное программное обеспечение также может иметь открытый (опубликованный) код, но его лицензия включает контроль собственника над продуктом.

Конкурсы

Внедрение новых технических решений часто происходит на основе открытого конкурса. Системные администраторы могут оказать серьезное влияние на результаты конкурса путем формулирования технических требований, причем в открытом конкурсе можно практически заранее выбрать победителя, если конкретизировать

требования до такой степени, что они могут быть выполнены только определенной моделью оборудования[1]. А можно сформулировать лишь основные, принципиальные требования проекта, рассмотреть полученные в итоге конкурса подходы к решению проблемы и выбрать оптимальный вариант.

Переход на новые версии программного обеспечения

"В крови" большинства системных администраторов живет желание применить новую версию ПО сразу же после его выпуска. Желание понятное, хотя в большинстве реальных ситуаций конечные пользователи не получат от такого перехода никаких дополнительных преимуществ. Подумайте, какие новые функции эксплуатируются в офисных программах? Подавляющему большинству пользователей достаточно только тех возможностей, которые им были доступны, например, уже в MS Office 97.

В любом случае необходимо оценить выгоды, которые вы надеетесь получить от перехода на новую версию программного обеспечения, и сравнить их с затратами на эту операцию (стоимость обновления версий ПО, стоимость модернизации оборудования и т. п.). Оказывается, что очень часто можно следовать старому доброму совету: если программа работает, то не надо ее трогать.

> ***Примечание***
>
> Конечно, большое количество версий ПО, одновременно находящихся в *эксплуатации*, усложняет работу администратора. Например, необходимо следить за обновлениями всего парка ПО, устанавливать вместо одного патча два или три, загружая их из Интернета. Но обычно серьезных проблем такая ситуация не создает.

Сертификация системных администраторов

Если некоторое время назад в чести были трудовые династии, то сейчас смена работы через 2—3 года стала реальным способом увеличения заработной платы. При этом посредниками между работниками и работодателями выступают кадровые агентства, а работник зачастую оценивается только по формальным признакам. Почти повсеместно подбором и приемом персонала занимаются менеджеры, не являющиеся специалистами по кадровой работе, а оценивающие "бумажную" составляющую резюме.

Поскольку такие "правила игры" реально существуют, то системному администратору следует не забывать во время своей работы получать необходимые сертификаты. Если руководство согласно оплатить курсы обучения, на которых готовят

---

[1] С учетом того, что вендоры предоставляют специальные скидки для конкурсов, то предприятие-партнер может предложить такие цены, которые позволят выиграть конкурс при прочих равных условиях. На практике автору не один раз приходилось сталкиваться с условиями конкурса, составленными подобным образом.

к сдаче экзамена на такие сертификаты, — хорошо. В противном случае следует найти собственные средства для оплаты сертификации в какой-либо области.

Сертификат — то же, что и права на вождение автомобиля. Он не подтверждает, что вы *хорошо* водите машину, однако является документом, который свидетельствует в вашу пользу. Хотя — по данным специализированных исследований — доверие к сертификатам со стороны линейных руководителей на Западе падает, для большинства сотрудников кадровых служб количество имеющихся у вас сертификатов пропорционально возможности положительного решения, тогда как их отсутствие может стать поводом для отказа.

> ***Примечание***
>
> И наоборот, наличие сертификата часто отнюдь не свидетельствует об уровне специалиста. Например, автору неоднократно приходилось отказывать в приеме на работу лицам, предоставлявшим многочисленные сертификаты, но в процессе собеседования не подтверждавшим указанные в них практические навыки управления системой.

Вопросы, на которые необходимо ответить во время сдачи сертификационного экзамена, составлены на основе зарубежной практики. Очень часто с ситуациями, по которым они составлены, администратору, работающему в наших организациях, сталкиваться не приходится. Поэтому наличие даже большого опыта практической работы не позволит вам сдать экзамены с первого захода. Целесообразно найти в Интернете (или магазинах) учебные пособия для подготовки к тестам и после их изучения потренироваться на реальных вопросах. С этой целью, во-первых, можно познакомиться с материалами, публикуемыми на таком сайте, как **http://www.braindumpcentral.com/**. Во-вторых, не очень сложно найти экзаменационные программы, пусть даже и не последней версии, на которых следует потренироваться в сдаче теста. Кроме того, для многих тестов доступны электронные учебники — см., в частности, **http://www.ebuki.apvs.ru/** (выполните, например, поиск по строке "exam").

Немного этики

По роду своей деятельности системный администратор имеет потенциальный доступ практически ко всей информации, хранящейся на предприятии в электронном виде. И именно барьеры этического плана должны удерживать его от соблазна узнать чужую зарплату или прочесть чью-либо корреспонденцию. Корректность также имеет большое значение в работе системного администратора. Например, многим администраторам приходится применять программы, перехватывающие экран и клавиатуру компьютера пользователя. У автора данная программа настроена таким образом, что при удаленном подключении на экране пользователя *всегда* выводится соответствующее предупреждение. Я специально акцентирую на этом внимание, поскольку встречал в прессе высказывания "специалиста" о том, как ему нравится наблюдать за реакцией пользователей при удаленном перехвате управления, когда компьютер переставал "слушаться" владельца.

В немалой степени от системного администратора зависят способы реализации корпоративных политик в области безопасности. С одной стороны, это желание руководителей осуществлять полный контроль над деятельностью подчиненных (перлюстрация корпоративной электронной почты, контроль посещения страниц Интернета и т. п.), с другой — право каждого на личную тайну. По данным статистики, желание полностью контролировать сотрудников чаще всего возникает у руководителей малых предприятий.

Системный администратор *вынужден* быть дипломатом и поддерживать хорошие отношения как с руководством, так и с коллективом сотрудников, находя компромиссные решения противоречивых ситуаций.

О мистике

И в заключение. Автор неоднократно замечал взаимосвязь между своим внутренним состоянием и стабильностью работы системы. Если вы садитесь за компьютер в плохом настроении, то не ждите, что он ответит вам "полным пониманием". Если вы не станете дружески относиться к своим системам, то будьте готовы к постоянным неожиданностям.

ГЛАВА 2

Выбор оборудования и программного обеспечения

Эксплуатация в составе информационной системы накладывает ряд дополнительных требований на применяемое оборудование и программное обеспечение.

Требования к оборудованию информационных систем

На рынке представлено много аналогичного оборудования, и выбор конкретных моделей часто представляет нелегкую задачу.

Выбор вендора

Лично я рекомендую всем покупать оборудование среднего ценового диапазона. Топовые модели обычно обладают функционалом, который не будет востребован во время эксплуатации. Самые дешевые — часто работают не так стабильно, как хотелось бы.

Этот принцип можно распространить и на выбор вендора. Как правило, информацию о ранжировании вендоров получить достаточно легко. И лучше выбирать опять же фирмы из середины списка. Наиболее известные вендоры часто завышают стоимость оборудования, пользуясь известностью своей марки. Следует не поддаваться на рекламные обещания: крупные компании выделяют на маркетинговые цели весьма существенный процент от стоимости оборудования. Например, один из вендоров коммутационного оборудования только на посреднические цели — партнерам — выделяет от 30 до 40% от стоимости проданного оборудования. Естественно, что партнеры всячески будут способствовать продвижению именно такой линейки и убеждать в ее исключительности.

Имеет смысл комплектовать однотипное оборудование моделями одного вендора. Как правило, вендоры поставляют совместно с оборудованием некоторые дополнительные опции, которые позволяют упростить администрирование. Например, это может быть программное обеспечение централизованного администрирования серверов или проприетарные протоколы коммутационного оборудования.

Сервисные контракты

Чем дороже оборудование, тем, как правило, больше задач оно решает в информационной системе. И тем к большим потерям приведет его простой на время ремонта или обслуживания. Поэтому целесообразно заключать сервисные контракты, которые гарантируют восстановление оборудования в течении оговоренного срока.

Возможность заключения сервисного контракта с заданным уровнем обслуживания (временем поставки вышедшего из строя компонента) следует учитывать при выборе оборудования. Особенно если предприятие расположено вдалеке от региональных центров. Перед принятием решения обязательно уточните наличие региональных складов, время доставки на предприятие детали с такого склада, наличие в регионе сертифицированных вендором специалистов, которым разрешено проводить обслуживание и ремонт предполагаемого к покупке оборудования.

Запасные элементы

Постарайтесь приобрести запасные части к приобретаемому оборудованию. Обычно сервисные контракты после 3—4 лет эксплуатации становятся очень дорогими, а приобрести детали становится невозможным, поскольку они перестают выпускаться в связи с переходом на новые модели.

Например, для серверов необходимо приобрести запасные жесткие диски и блоки питания. Эти детали чаще всего отказывают во время эксплуатации.

Дополнительные требования к компьютерам

Оборудование должно удовлетворять ряду российских стандартов (санитарные правила, по электробезопасности и т. п.). Эти требования будут удовлетворяться, если оборудование будет иметь сертификат РОСТЕСТа.

Параметры компьютеров обычно должны быть определены в проектной документации. Как правило, оговариваются минимальные требования к процессору (тип, число процессоров/ядер, частота), памяти, дисковой подсистеме.

Выбор процессора

Серверы начального уровня выбираются обычно с x86-процессорами. Для более мощных систем возможно использование процессоров другой архитектуры, но этот выбор обычно диктуется приложением (задачи SAP обычно реализуют на мощных вычислительных процессорах серии Power, серверы баз данных Oracle оптимизированы под собственные серверы с процессорами архитектуры RISC и т. д.).

Число ядер, частота и т. д. выбирается на основе требований проекта. В случае планирования виртуализации необходимо улучшать конфигурацию примерно на 20%.

Выбор шасси

Серверы обычно устанавливают в стойку и шкаф. Соответственно, они должны поставляться в шассийном исполнении и должны быть снабжены креплениями (*рельсами*) для установки в шкаф с возможностью выдвижения для обслуживания.

Для обеспечения возможности резервирования электропитания шасси должно иметь два блока питания, допускающих их "горячую" замену.

Выбор материнской платы

Сервер должен быть укомплектован системой out-of-band-управления. Эта система позволяет по отдельному сетевому интерфейсу мониторить состояние сервера, включать и выключать его, программно удаленно монтировать образы CD/DVD и т. д. Обычно серверные платы включают данную опцию по умолчанию, но есть модели, в которых она является дополнительным компонентом. На рис. 2.1 показан пример подобного интерфейса удаленного управления.

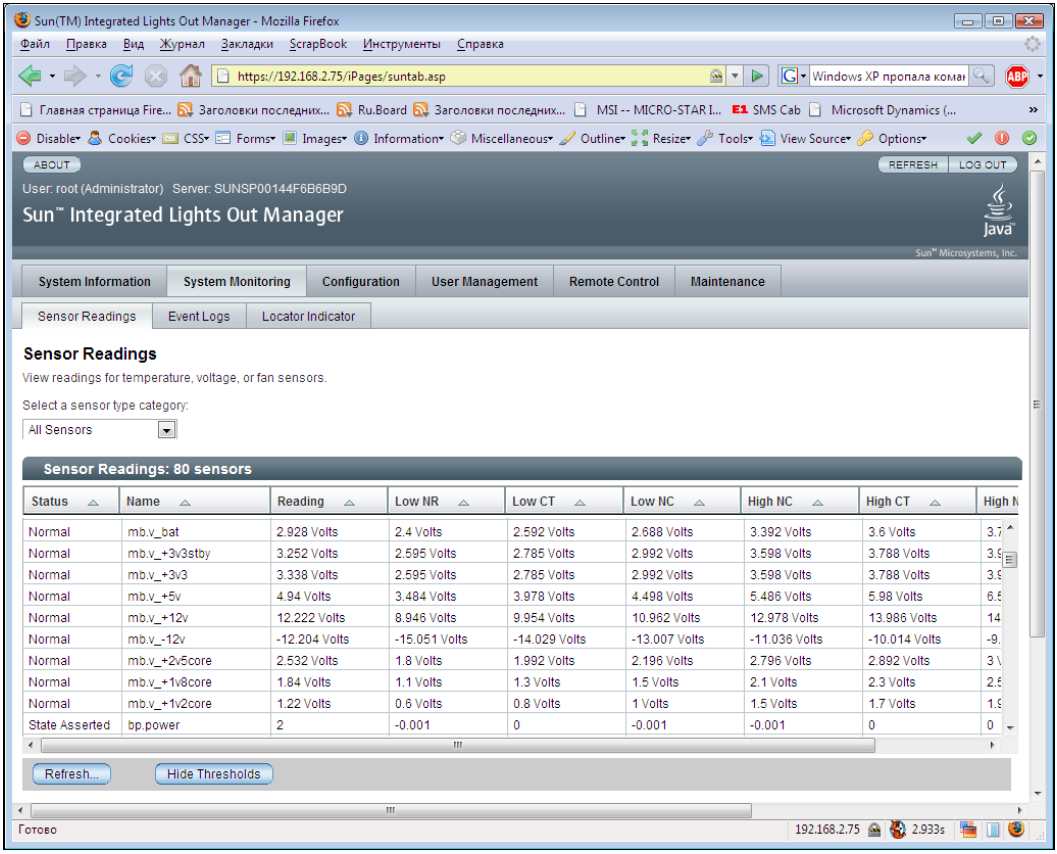


Рис. 2.1. Интерфейс удаленного управления (iLO) сервера Sun

Программные средства мониторинга, существующие для данной модели, должны быть совместимы с той системой контроля, которая используется на предприятии.

Для упрощения инвентаризации желательно, чтобы серийный номер шасси/сервера был доступен программным способом.

Сервер должен иметь аппаратный RAID-контроллер для создания отказоустойчивого массива из устанавливаемых дисков.

Выбор дисков

Желательно хранить и обрабатывать данные на специализированных устройствах — *системах хранения данных* (СХД). На рынке представлено много моделей таких устройств, доступных или дорогих, с большим или меньшим функционалом. Можно купить платформу с большим числом жестких дисков и установить на нее программное обеспечение серверов хранения данных (в том числе, и бесплатное). Вариантов много, в любом случае переход на СХД позволит более рационально использовать дисковое пространство и повысить надежность системы.

Поэтому в сервере лучше оставить только два небольших, но быстрых диска для построения отказоустойчивого массива (зеркала) и размещения на нем операционной системы.

Если данные будут храниться локально, то изначально нужно установить в сервер максимальное число дисков. Это повысит производительность дисковой подсистемы. При этом нужно продумать, как будут сформированы массивы. Обычно создают RAID (Redundant Array of Independent Disks — избыточный (резервный) массив независимых дисков) 5-го уровня из всех дисков сервера, который потом разбивают (или не разбивают) на несколько логических. Это самый экономичный вариант отказоустойчивого массива, но не самый оптимальный. Например, тип массива должен быть различным для размещения журналов сервера баз данных и для файлов самой базы.

Поэтому до покупки сервера следует ознакомиться с рекомендациями по размещению данных приложений: какой тип массива рекомендуется, под какой размер блока данных должен быть отформатирован диск и т. п.

Выбор параметров устройства для хранения данных является одним из самых сложных вопросов конфигурации компьютера. Проблем несколько. Во-первых, редко когда сервер используется только для одной задачи, а разные приложения отличаются характеристиками операций ввода/вывода. Во-вторых, даже если планируется обслуживать только одну задачу, никто, даже разработчики соответствующего программного обеспечения, обычно не могут дать оценку по числу операций ввода/вывода в секунду, соотношению операций чтения-записи и т. д. Даже если цифры и называются, то они весьма приблизительные, как экстраполированные результаты приложения в примерно "сходной" конфигурации на другом предприятии.

Скорость работы устройств хранения обычно характеризуют параметрами *IOPS* (Input/Output operations Per Second — число операций ввода/вывода в секунду) и максимальной скоростью записи/чтения. Параметры хотя и взаимосвязаны, но характеризуют различные "стороны" устройства хранения. Например, в программном обеспечении баз данных обычно используется размер блока для операций записи/чтения в 8 Кбайт. Для файловых серверов обмен данных ведется для 60% случаев блоками по 4 Кбайта (см. **http://blog.aboutnetapp.ru/archives/475**), 10% — по 65 Кбайт и т. п. Естественно, что показатель IOPS при записи больших блоков данных будет существенно ниже, чем в случае 4-килобайтного блока.

Показатели IOPS, в основном, определяются скоростью вращения жесткого диска и не столь существенно отличаются у разных производителей. Для грубой оценки можно использовать следующие значения (табл. 2.1).

Таблица 2.1. *Средние значения IOPS в зависимости от скорости вращения шпинделя диска*

Число оборотов в минуту (RPM)	IOPS
15 000	170
10 000	120
7 500	70

Для ускорения обмена данными операции записи/чтения проводят сразу с несколькими жесткими дисками — объединяют диски в RAID. Существуют различные варианты RAID-массивов, отличающихся вариантами записи данных (см. **http://ru.wikipedia.org/wiki/RAID**). Если оценивать RAID-массивы по скорости работы, то следует учитывать, что разным типам RAID присуще различное количество дополнительных операций для реализации функций отказоустойчивости и т. п. Поэтому объединяя три диска в RAID 5, мы не получим трехкратного увеличения скорости работы.

В результате, для разных типов приложений необходимо выбирать свои варианты создания RAID-массивов. Существуют специальные формулы, позволяющие вычислить ожидаемое теоретическое увеличение производительности, но проще воспользоваться бесплатными он-лайновыми ресурсами — калькуляторами IOPS:

- **http://www.wmarow.com/storage/strcalc.html**;
- **http://www.storage-expert.ru/index.php/section-table/42-disk-array-faq/63-online-iops-calc**

  и др. (рис. 2.2).

Такие расчеты дадут оценочные параметры для простых систем хранения и для массивов, собранных из жестких дисков сервера. Современные системы хранения используют дополнительные способы увеличения производительности, например, кэширование данных в оперативной памяти контроллеров СХД, использование быстродействующих твердотельных дисков (SSD-диски) для временного размещения данных и т. д. Если предполагается использовать подобное оборудование, то нужно обратиться к специализированным калькуляторам и техническим спецификациям, которые предоставляют соответствующие вендоры.

Выбор памяти

Часто специалисты пытаются дополнить рекомендованную конфигурацию системы модулями оперативной памяти. Желание объяснимое, но не следует упускать из виду тот факт, что скорость работы с памятью может зависеть от ее конфигура-

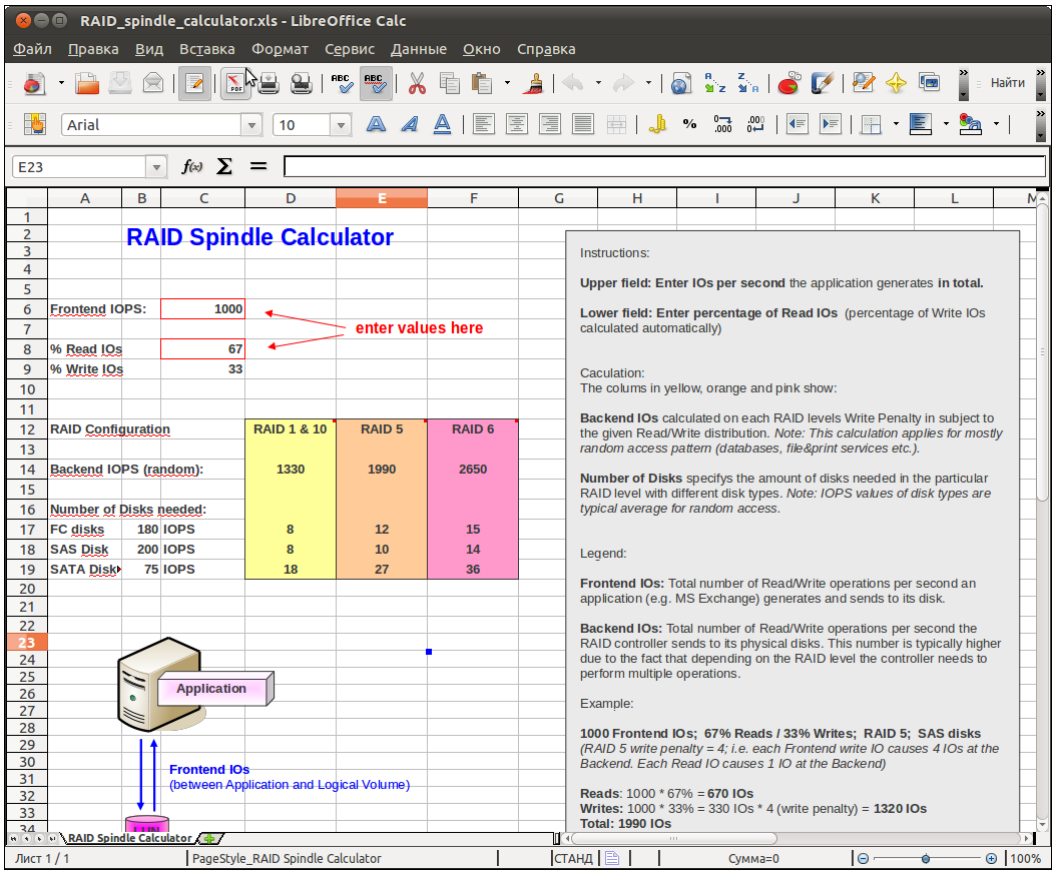


Рис. 2.2. Образец калькулятора RAID

ции — числа установленных модулей. Легко может оказаться так, что, добавив новые модули памяти, вы одновременно снизили вдвое скорость обмена данными с ней.

Обычно в документации на сервер (материнскую плату) присутствуют рекомендации по конфигурации модулей памяти. Некоторые вендоры предлагают даже мастера выбора памяти, можно обратиться к техническим специалистам вендора и т. п. В общем, нужно только воспользоваться предлагаемыми возможностями.

Совместимость компонентов

И последнее. Все компоненты сервера должны быть совместимы. Учесть все требования, чтобы исключить ошибки, достаточно сложно. Поэтому вендоры предлагают специальные конфигураторы, с помощью которых можно сформировать желаемый сервер. Этими конфигураторами пользуются как сами специалисты вендоров, так они доступны и для рядовых покупателей. На рис. 2.3 показан пример такого конфигуратора для серверов Hewlett Packard.

Рис. 2.3. Пример онлайнового конфигуратора сервера от Hewlett Packard

Дополнительные требования к коммутационному оборудованию

Коммутационное оборудование выбирается с учетом поддержки технологий, использованных при построении инфраструктуры. Желательно использовать только стандартизованные решения, поскольку это позволит в дальнейшем сочетать оборудование различных вендоров.

Оборудование без возможности сетевого управления (без поддержки протокола *SNMP* (Simple Network Management Protocol — простой протокол сетевого управления)) можно выбирать только для малых организаций.

Поскольку в практику все более внедряются решения по передаче голосового и видеотрафика по сети, нужно, чтобы все оборудование поддерживало приоритезацию трафика с числом очередей не менее 4, а оборудование уровня распределения и ядра позволяло ограничивать (регулировать) полосы пропускания для различного трафика.

Если организация занимает несколько комнат и порты сети не находятся под постоянным контролем, необходимо выбирать оборудование с поддержкой протокола 802.1x.

Дополнительные требования к аварийным источникам питания

Источники аварийного питания (UPS) (Uninterruptible Power Supply — источник бесперебойного питания) должны быть резервированы, если оборудование не имеет независимых выходов, то следует приобретать по 2 UPS на один узел.

Источники аварийного питания должны быть снабжены сетевыми интерфейсами, по которым можно получать данные о состоянии батарей, уровне зарядки, оставшемся времени автономной работы.

Состав программного обеспечения типовой организации

Любая информационная система включает в себя инфраструктурные службы — службы и программы, необходимые для поддержания работы системы и выполнения типовых функций, а также собственно "полезное" программное обеспечение — приложения, выполняющие расчеты в целях обеспечения производства данной организации.

Если прикладное программное обеспечение весьма разнообразно и общие рекомендации дать достаточно сложно, то инфраструктурные решения во многом схожи.

В любой информационной системе представлены следующие классы программ и приложений:

- операционные системы;
- подсистемы разрешения имен;
- подсистемы авторизации, аутентификации и контроля доступа;
- службы файловых сервисов;
- средства доступа к глобальной сети (Интернету) и просмотра внешних ресурсов;
- программное обеспечение защиты хоста (антивирусное ПО и ПО межсетевых экранов, контроля приложений и т. п.);
- подсистема резервного копирования;

- программное обеспечение офиса (текстовый редактор, редактор электронных таблиц и т. д.);
- подсистема обмена сообщениями электронной почты.

Можно перечислить еще много типовых служб, которые свойственны информационным системам, но указанный выше список можно найти на любом предприятии.

Операционные системы были упомянуты в *главе 1*, далее попытаемся дать оценки оставшихся компонент.

Службы разрешения имен

Используемые на практике службы разрешения имен, операции по настройке и использованию подробно рассмотрены в *главе 3*.

Система авторизации, аутентификации и контроля доступа

При увеличении числа совместно работающих систем для снижения затрат на их администрирование используют централизованное управление. В этом случае параметры учетной записи пользователей хранят на серверах, на серверах осуществляется проверка правильности введенных данных и принимается решение на доступ к ресурсам.

В сетях Windows в качестве централизованного хранилища используется служба каталогов — *Active Directory*. Для Linux-систем обычно применяется проект OpenLDAP. Поскольку оба этих каталога используют открытые стандарты, то возможны решения, когда Linux-клиенты проходят проверку на серверах домена Windows, а Windows-системы — в домене, контроллерами которого являются серверы Linux.

Подключение Linux к домену (Kerberos)

Для подключения Linux-систем к домену Windows можно использовать различные технологии. Либо на основе NTLM[1]-аутентификации (традиционный вариант, совместим с доменами Windows NT), либо на основе Kerberos (поддерживается в доменах Windows 200*x*). Поскольку система безопасности Windows в нормальном режиме использует протоколы Kerberos, то рекомендуется именно так и подключать клиентов Linux.

В следующем примере мы опишем последовательность операций для ОС Red Hat Linux, в других клонах ОС Linux действия могут незначительно отличаться.

> ***Примечание***
>
> Red Hat Linux имеет настройки Security Level Configuration. Если выбран уровень безопасности системы High или Medium, то аутентификация в домене Windows будет не-

[1] NTLM (NT LAN Manager) — протокол сетевой аутентификации, разработанный фирмой Microsoft для ОС Windows NT. — *Ред.*

возможна. Поэтому включите вариант No Firewall (с помощью команды меню **Main | System Settings** или в режиме терминала командой `redhat-config-securitylevel`).

Протокол Kerberos будет работать только в том случае, если рассогласование времени между компьютером пользователя и контроллером домена составляет меньше 5 минут. Поэтому перед началом операций необходимо синхронизировать время на компьютерах и проверить идентичность установленных часовых поясов.

Для подключения к домену нужно выполнить три шага:

1. Отредактировать конфигурацию клиента Kerberos и nsswitch;
2. Получить билет Kerberos для учетной записи администратора;
3. Выполнить команду подключения к домену.

Настройка конфигурации клиента Kerberos

Настройки Kerberos можно выполнить с помощью имеющихся в системе графических утилит (рис. 2.4), но проще вручную отредактировать файл конфигурации, расположенный по следующему пути: /etc/krb5.conf. В этом файле достаточно отредактировать только параметры доменной области (realm) и центра выдачи ключей (KDC)[1] (Key Distribution Center — центр распределения ключей — служба Kerberos):

```
[realms]
LOCAL.DOMAIN = {
kdc = tcp/dc1.local.domain:88 tcp/dc2.local.domain:88
admin_server = dc1.local.domain
default_domain = local.domain
}
[domain_realm]
.local.domain = LOCAL.DOMAIN
local.domain = LOCAL.DOMAIN

[kdc]
enable-kerberos4 = false
```

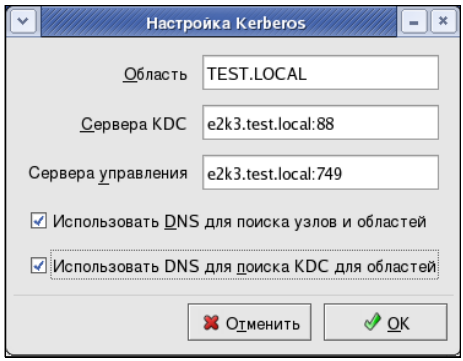


Рис. 2.4. Настройка параметров Kerberos в графическом режиме в Red Hat

[1] В данном примере DNS-имя домена — local.domain, а контроллеры домена имеют имена dc1 и dc2.

Назначения параметров видны по их названиям. Можно использовать также пример, содержащийся в исходном файле krb5.conf.

> ***Примечание***
>
> Записи в этом файле *чувствительны к регистру*. Рекомендуется вводить имена *только* в верхнем регистре, именно так, как это сделано в данном примере.

Настройка nsswitch.conf

В файле /etc/nsswitch.conf определяется, какие источники будут использованы для получения данных о пользователях. Иногда настройки по умолчанию ограничиваются только локальными параметрами (в строках упомянуто только `files`). Поэтому проверьте, чтобы содержимое файла /etc/nsswitch.conf включало параметры как `files`, так и `winbind`. Например, так:

```
group: files winbind
hosts: files dns nis winbind
networks: files winbind
passwd: files winbind
shadow: files winbind
shells: files winbind
```

Получение билета Kerberos для учетной записи администратора

После того как вы отредактируете конфигурацию, необходимо получить билет Kerberos на Linux-компьютере для учетной записи администратора домена. Для этого выполните следующую команду:

```
kinit administrator@LOCAL.DOMAIN
```

Обратите внимание, что имя домена должно быть набрано прописными буквами, а слева от знака "`@`" указана учетная запись администратора этого домена.

Команда должна отработать без ошибок. Самая распространенная ошибка возникает в случае, если время системы Linux отличается от времени контроллера домена. В этом случае синхронизируйте время и повторите команду.

Проверить полученный билет можно, выполнив команду:

```
klist
```

Эта команда должна показать параметры полученного билета (имя учетной записи, срок действия билета).

Подключение к домену

Для включения компьютера с Linux в домен Windows по протоколу Kerberos необходимо выполнить следующую команду (подключение происходит к домену, указанному в параметрах по умолчанию — конфигурации клиента Kerberos):

```
net ads join -U administrator%password
```

Обратите внимание, что используется ключ `ads`, говорящий о подключении к службе каталогов по протоколу Kerberos. Не забудьте сменить имя пользователя

`administrator` и пароль `password` на реальное имя пользователя, имеющего право подключения компьютеров к домену (лучше всего, если это будет администратор домена), и его пароль. В ответ вы должны получить сообщение об удачном выполнении операции.

Проверка подключения

После подключения к домену в списке компьютеров-членов домена можно будет увидеть Linux-систему.

Проверить наличие подключения можно, попытавшись отразить информацию об учетных записях и их паролях в домене. Сначала проверьте наличие безопасного подключения с помощью следующей команды:

```
wbinfo –t
```

На экране должно появиться аналогичное приведенному далее:

```
[root@linux ~]# wbinfo –t
checking the trust secret via RPC calls succeeded
```

Командой `wbinfo –u` можно отобразить список пользователей, а применив ее с ключом `–g` — список групп.

Проверьте, что служба winbind успешно получает пароли с контроллера домена. Для этого выполните команду:

```
getent passwd
```

В списке паролей вы должны увидеть записи, относящиеся к домену (имена пользователей будут показаны в начале строки в виде: `домен\пользователь`).

Сервер Linux в качестве контроллера домена

Сервер Linux может выступать в качестве контроллера домена Windows. Можно настроить сервер Kerberos, но обычно создают NTLM-домен с помощью демона Samba. Для этого нужно внести всего несколько строк в конфигурационный файл и снова стартовать службу smbd.

Необходимые изменения документированы в самом файле конфигурации, комментарии легко найти в Интернете, поэтому мы не будем специально останавливаться на этом.

В качестве контроллера домена сервер Linux хранит учетные записи пользователей. При этом вы можете применять сценарии, исполняемые при входе пользователей в домен, однако вам недоступны групповые политики, активно используемые при управлении доменом Windows 200*x*. Групповые политики предполагается реализовать в версии Samba 4, которая в настоящее время проходит тестирование. Хотя пользователи, работавшие с этой версией, отмечают полную ее работоспособность в их конфигурации, в том числе и применение групповых политик.

Возможный выход в такой ситуации заключается в применении дополнительных пакетов для реализации необходимых функций. Например, для автоматизации

установки и удаления программ Windows можно применить программу WPKG (**http://wpkg.org**).

Совместные документарные ресурсы

Сеть любой организации не обходится без общих папок с документами или приложениями. В сетях Windows общие папки и принтеры предоставляются по протоколу SMB (Server Message Block — блок серверных сообщений (протокол, разработанный Microsoft, Intel и IBM)). Компьютеры с ОС Linux также могут подключаться к этим ресурсам и даже предоставлять свои ресурсы для клиентов Windows. Для этого используется специальная служба Samba.

Проект Samba входит в состав всех Linux-дистрибутивов. Недавно к разработке данного проекта официально подключилась корпорация Microsoft, что дополнительно свидетельствует о важности этого направления и качестве его разработки.

Сама операция предоставления ресурса в общий доступ в Windows сложности не вызывает. Достаточно выполнить соответствующую команду из свойств объекта, дать сетевое имя и назначить права доступа.

При работе в составе домена доступ предоставляется по доменным учетным записям. В рабочей группе необходимо либо создавать одноименные учетные записи на всех компьютерах с одинаковыми паролями, либо разрешать доступ для всех. Последнее не очень хорошо с точки зрения безопасности, но оптимально для группы из нескольких компьютеров.

Документы можно предоставлять и путем размещения их на порталах. Это более трудоемкая операция, зато легко организовать обсуждения материалов, версионность документа, предоставить пользователям возможность самостоятельно создавать ресурсы.

Существует расширение технологии общих папок — *распределенная файловая система*. Она более подробно рассмотрена в *главе 10*.

Учетная запись для анонимного доступа

В случае предоставления ресурсов в общий доступ для всех, операционная система не контролирует права доступа и использует в этом случае специальную учетную запись.

В Windows это учетная запись Гость. Она по умолчанию заблокирована в системе, поэтому при желании использования анонимного доступа необходимо ее разблокировать. Соответственно, и настройки файлов на диске должны позволять этой учетной записи чтение или запись информации.

Учетной записи Гость в ОС Linux соответствует учетная запись nobody. По умолчанию анонимный доступ к ресурсам Linux также запрещен. Если вы хотите его разрешить, то удостоверьтесь в существовании в системе учетной записи nobody и откорректируйте конфигурацию Samba по следующему образцу:

```
[global]
  security = user
  map to guest = Bad Password

 [share_definition]
  guest ok = yes
```

Другой способ состоит в использовании параметра `security = share`. В этом случае доступ к ресурсу будет осуществляться только с параметрами гостевой учетной записи.

Портальные решения

Помимо размещения документов в общих папках возможен вариант общего доступа к ним по веб-технологиям. Это создание порталов. *Портал* представляет собой веб-сервер, группирующий информацию нескольких источников. Обычно размещение информации на портале доступно самим пользователям. Пользователи могут создавать собственные странички (на основе шаблонов), добавлять в них органы управления, реализовывать функциональность контроля движения документов и т. п. На страницах можно хранить документы, согласовывать графики и поручения, настраивать поиск по определенной тематике.

Существуют как бесплатные, так и коммерческие версии порталов. Среди серверных продуктов Microsoft — это сервер SharePoint. Строго говоря, есть базовая функциональность портала, которая называется *SharePoint Foundation*. Этот компонент входит в состав новых версий серверов и может быть бесплатно загружен для предыдущих выпусков. На SharePoint Foundation также можно создать корпоративные веб-сайты. Сервер SharePoint добавляет к базисному функционалу некоторые дополнительные элементы управления, возможность создания распределенного на несколько серверов портала и т. д. Поэтому начинать использование портала вполне можно именно с базисного варианта.

Среди бесплатных продуктов наибольшей функциональностью отличается портал Liferay. Для установки и базового администрирования этого портала не требуются навыки программирования. Liferay разработан на Java и работает на любой вычислительной платформе в среде Java Runtime Environment и сервере приложений.

Поиск по сетевым ресурсам

При большом количестве документов на общем ресурсе работать с ними становится крайне сложно. Даже если и принята система наименований документов, то все равно поиск нужного файла часто занимает много времени.

Существует вариант бесплатного поискового сервера от Microsoft — SearchServer Express, который позволяет индексировать документы в общих папках. В результате документ можно легко найти по ключевым словам. Сервер индексирует документы офиса, PDF и текстовые файлы.

Сервер базируется на технологии SharePoint, результаты поиска выводятся на вебстраничку.

Работа с Windows-ресурсами в Linux

Для работы в составе домена Windows (использование единой базы учетных записей пользователей, подключение/предоставление общих ресурсов и т. п.) предусмотрен пакет Samba. Этот пакет входит во все дистрибутивы Linux, и обычно нет необходимости загружать инсталляционные файлы с сайта **www.samba.org**.

Установка

Пакет Samba должен быть установлен по правилам используемой версии Linux. Для тех, кто привык работать в графической среде (при ее установке), есть средства настройки параметров основных сетевых служб (рис. 2.5), в которых можно включить эту службу.

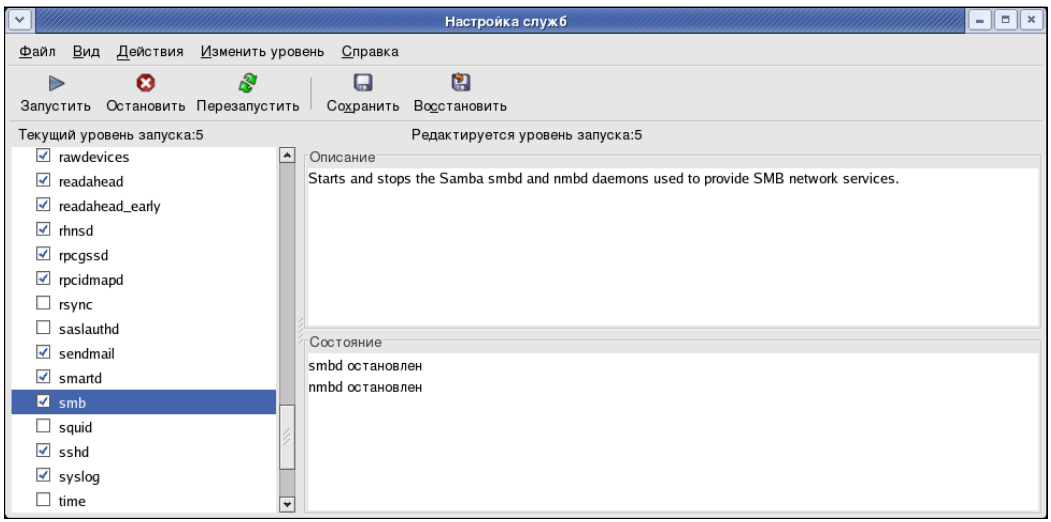


Рис. 2.5. Настройка автоматического запуска Samba графическими средствами

Проверить, работает ли демон Samba, можно, перечислив все активные процессы и отфильтровав вывод команды по названию службы:

```
ps -A | grep smb
```

Настройки Samba

Настройки Samba содержатся в файле конфигурации, который расположен по следующему пути: /usr/samba/lib/smb.conf.

Файл состоит из нескольких разделов: `[globals]` — глобальные настройки, `[homes]` — домашние папки пользователей, `[printers]` — настройки печати и пользовательских разделов, в которых определяются сетевые папки. Имена разделов заключаются в квадратные скобки, параметры определяются в виде `key = value`. Файл конфигурации снабжен комментариями, так что для вас не составит особого труда разобраться с правилами его редактирования. Вы можете просто снять ком-

ментарии с тех строк, которые описывают наиболее подходящую конфигурацию сервера, и настроить по образцу совместный доступ к ресурсам.

> ***Примечание***
>
> Отсутствие ошибок в файле можно проверить с помощью команды `testparm`. Если она сообщит об ошибке, следует перепроверить внесенные настройки.

Предоставление ресурсов в общий доступ

Операцию можно осуществить как с использованием графического интерфейса (рис. 2.6), так и путем правки конфигурации программы. Приведенный ниже краткий пример иллюстрирует основные параметры предоставления ресурса в общий доступ:

```
[Documents]
   comment = Архив документов
   path = /usr/local/docs
   valid users = @"domain\domain users" domain\user1
   admin users = @ domain\group2
   writable=yes
   browseable=yes
```

Необходимые дополнительные параметры (настройку протоколирования доступа, корзины, варианты предоставления ресурса с произвольной маской доступа и т. п.) легко уточнить по справочной документации.

Обратите внимание, что в секции `[global]` файла конфигурации можно установить, для каких диапазонов адресов будут предоставляться в совместное использование ресурсы, максимальное число одновременно открытых файлов и т. п.

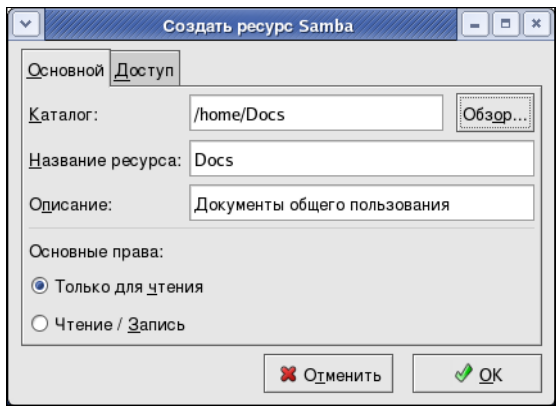


Рис. 2.6. Графический интерфейс управления службой Samba

При предоставлении ресурсов в доступ пользователям домена следует учитывать, что пользователь, подключающийся к ресурсу, будет иметь на компьютере личную папку.

Подключение к общим ресурсам

Подключение к общим ресурсам ОС Windows, предоставленных ОС Linux, осуществляется обычным способом (либо из меню командой подключения к общей папке, либо из командной строки с помощью `net use`).

Для подключения ресурсов Windows на *nix-компьютере используется команда `smbmount`. Нужно указать, какой ресурс и в какую точку монтируется, ввести параметры учетной записи. Например, так:

```
smbmount //servername/sharename /mountdirectory -o
username=mywindowsusername,password=mywindowspassword
```

Подключение сохранится до перезагрузки системы.

Команда `smbmount` фактически является сокращением команды `smbclient`:

```
smbclient  //hostname/service <ключи и параметры>
```

Указывая соответствующие ключи, можно выполнить различные операции, например, копирование данных, удаление файла на Windows-системе, создание архива и т. д.

> ***Примечание***
>
> Команда `smbclient` позволяет отобразить список всех ресурсов, предоставленных в совместное использование с компьютера: `smbclient -L hostname`

Обозреватели Интернета

В сетях, имеющих доступ в Интернет, скорость и качество работы обозревателей имеют важное значение.

В составе Windows поставляются обозреватели Internet Explorer. Поскольку обозреватели Интернета являются одной из самых часто обновляемых программ, то системному администратору следует позаботиться об установке на клиентские системы самой последней версии. Это обеспечит правильное отображение страниц и безопасность работы.

Существует много бесплатных обозревателей. Это Mozilla Firefox, Google Chrome, Opera и др. Выбор любого продукта во многом определяется личными пристрастиями, хотя автор предпочитает серфинг Интернета при помощи Firefox.

Во-первых, он легко дополняется бесплатными модулями. Например, на моем компьютере установлены блокировщик рекламы, переводчик, переключатель в режим Internet Explorer, локальная записная книжка (для сохранения участков страниц Интернета) и др.

Во-вторых, Firefox у меня установлен на нескольких компьютерах, и параметры работы в Интернете, закладки, пароли доступа синхронизированы между домашней, рабочей и мобильной системой.

Ну и в-третьих, он просто нравится.

Защита хоста

Каждый сервер или рабочая станция должны быть защищены от вредоносного программного обеспечения, от попыток сетевых атак и т. п. Поэтому наличие программ защиты хоста является крайней необходимостью.

Вопросам защиты информации посвящена *глава 9* этой книги. В этом разделе отметим только то, что к функциям программ защиты хоста обычно относят:

- антивирусную защиту, защиту от вредоносного кода;
- контроль доступа к компьютеру из сети и контроль трафика изнутри наружу (межсетевой экран);
- защиту от сетевых атак (анализ передаваемых по сети пакетов);
- контроль устройств и приложений (разрешение/запуск приложений, блокировка/доступ к устройствам).

Функции межсетевого экрана в настоящее время встроены во все операционные системы. Можно говорить о разном уровне функциональности, удобства управления и т. д., использовать дополнительное ПО, но это уже определяется требованиями к уровню безопасности и опытом администратора.

Иностранные пользователи в основном используют бесплатные версии антивирусного программного обеспечения. К сожалению, в нашей стране практика иная, хотя имеющиеся бесплатные продукты и обеспечивают необходимый уровень защиты. Можно упомянуть бесплатные антивирусы Microsoft Security Essentials, Avast!, AVG, Avira AntiVir и многие другие.

Функции защиты от сетевых атак обычно необходима в корпоративных сетях. Индивидуальные персональные компьютеры достаточно просто закрыть от любого входящего трафика средствами межсетевого экрана.

Аналогично, контроль устройств и приложений востребован системными администраторами. На рис. 2.7 показано сообщение системы в ответ на попытку пользователя подключить запрещенное устройство.

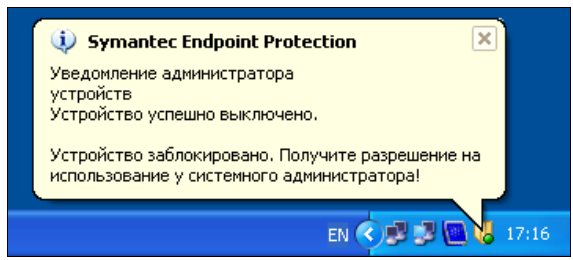


Рис. 2.7. Блокировка устройств с помощью Symantec Endpoint Protection

Обратите внимание, при выборе решения необходимо искать приложения, которые позволяют блокировать все устройства по типу (например, все USB-сменные носители) и разрешать при этом подключение по серийному номеру. В противном случае пользователи найдут способ обойти эти ограничения.

Средства резервного копирования

Наличие подсистемы резервного копирования и соблюдение регламентов операций создания копий данных является требованием к каждой информационной системе. Программы резервного копирования, включаемые в состав операционной системы, большей частью пригодны только для защиты данных личных документов и аналогичной информации.

Какой же опционал должен быть включен в программное обеспечение резервного копирования? Можно назвать следующие возможности:

- Возможность восстановления всей системы с нуля и на новое оборудование.

  Программа резервного копирования должна позволить администратору быстро и путем простых операций подготовить и восстановить систему на новом оборудовании. Понятно, что подобные ситуации не будут встречаться часто, но эта возможность сведет к минимуму возможные простои. На рис. 2.8 показано одно из окон настройки конфигурации восстановления системы на новое оборудование в программе резервного копирования Symantec NetBackup. Администратору достаточно просто добавить в предложенном окне новые драйверы оборудования к имеющейся конфигурации.

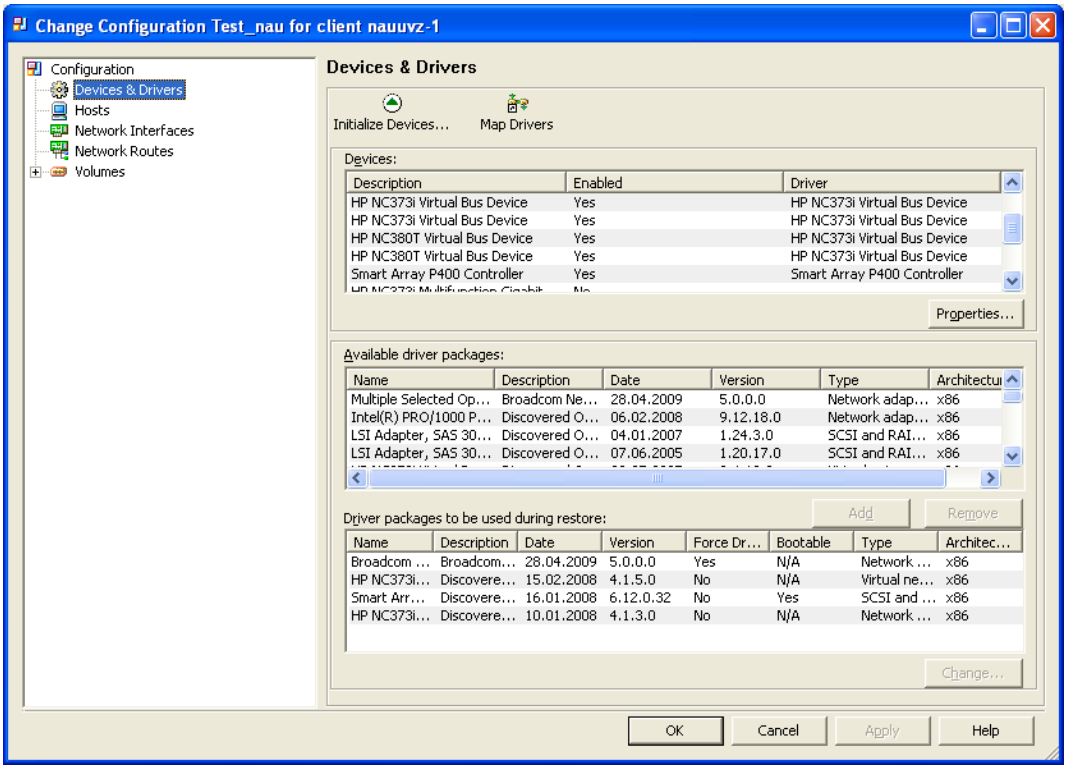


Рис. 2.8. Окно настройки параметров конфигурации для восстановления системы

- Поддержка прикладных программ, эксплуатируемых в организации.

  Корпоративная программа резервного копирования должна выполнять задачу сохранения данных для всех программ, которые используются в организации. Это касается серверов баз данных, почтовых программ различных производителей, ERP-систем, если таковые присутствуют в системе, и т. д.

  > ***Примечание***
  >
  > *ERP-система* (англ. Enterprise Resource Planning System — система планирования ресурсов предприятия) — это интегрированная система на базе ИТ для управления внутренними и внешними ресурсами предприятия.

- Программа резервного копирования должна позволять создавать гибкий график операций.

  Администратор должен достаточно просто настраивать график полного и частичного резервного копирования для каждого продукта и быть уверенным, что в случае сбоя (например, временной недоступности сервера) операция будет повторена через заданные промежутки времени.

  Кроме того, администратор не должен выполнять несколько последовательных операций при восстановлении данных: программа должна самостоятельно объединить полные и промежуточные копии на требуемый момент времени.

- Возможность гранулярного восстановления.

  На практике резервные копии данных часто используются для того, чтобы восстановить случайно удаленные пользователями отдельные файлы или вернуть информацию к предыдущему состоянию.

  Удобно, если такая функциональность доступна самим пользователям, чтобы они не привлекали администраторов для решения указанных задач (конечно, с необходимым контролем прав доступа).

- Развитая отчетность.

  Отчетность по результатам выполнения операций является немаловажным свойством. Быстрое получение сведений об ошибках операций, о составе резервных копий, об использовании объемов устройств хранения и т. п. помогает администратору принимать верные решения по управлению системой.

- Поддержка ленточных библиотек (опционально).

  В большей части организаций операция резервного копирования выполняется на дисковые устройства. Это быстро, достаточно дешево. Но если требуется хранить данные годами, то в такой ситуации конкурентов у ленты нет и сегодня. Но магнитная лента требует и особого обращения к себе: специальных условий хранения, периодических перемоток и т. п. Поэтому ленточные библиотеки применяются только в крупных организациях или в специализированных целях.

- Дедупликация данных (опционально).

  Технология дедупликации подразумевает исключение дублирования хранимых данных. Данные разбиваются на блоки, для них вычисляется хэш-функция.

И если выполняется попытка записи нового блока, который уже совпадает с тем, что хранится в системе (совпадают значения хэш-функций), то вместо повторной записи всех данных блока записывается только указатель на существующие в системы блоки.

Дедупликация может сократить размер хранимых данных, особенно если по регламенту резервного копирования организации должно создаваться и храниться много промежуточных копий (например, если требуется сохранять ежедневные копии в течение месяца).

> ***Примечание***
>
> Разработано несколько технических решений дедупликации, например, для блоков данных постоянной длины и переменной (последнее более приспособлено к небольшим изменениям данных). Но это не имеет принципиального значения при данном рассмотрении.

Уменьшая объемы хранения данных, технология резко повышает требования к надежности систем хранения. Если при "обычных" копиях выход из строя одного блока данных приводил к ошибке в одном файле, то при использовании дедупликации такая ошибка может привести к гораздо серьезным последствиям.

Дедупликация полезна и в том случае, если резервное копирование выполняется по медленным каналам (например, удаленных клиентов по сети Интернета). В таких ситуациях может помочь выполнение дедупликации на стороне клиента: на систему хранения в таком случае будут передаваться только уникальные блоки и информация по дедуплицированным.

- Возможности резервного копирования виртуальных машин (опционально).

  Современные программы резервного копирования позволяют сохранять данные с виртуальных машин с помощью агента, устанавливаемого на гипервизор, без установки агентов резервного копирования на каждую виртуальную машину.

  Если администратор хочет использовать такую возможность, то он должен предварительно уточнить, для каких операционных систем и приложений подобная функциональность поддерживается, и сравнить стоимость лицензий такого решения с суммарной стоимостью лицензий агентов на каждой виртуальной машине.

- Дополнительные корпоративные функции (опционально).

  Программы резервного копирования могут включать дополнительные функции, позволяющие снизить нагрузку на производственные системы во время операций или имеющие какой-либо дополнительный функционал. Например, при наличии в информационной системе устройств хранения, подключенных по сети *SAN*, на таком устройстве могут создаваться мгновенные снимки данных, которые будут копироваться на устройство резервного копирования по линиям FC (fiber channel — оптоволоконный канал), а выполнять само копирование — для разгрузки производственного сервера — можно с другого сервера.

Примечание

SAN (англ. Storage Area Network — сеть хранения данных) — представляет собой архитектурное решение для подключения внешних устройств хранения данных, таких как дисковые массивы, ленточные библиотеки, оптические приводы к серверам таким образом, чтобы операционная система распознала подключенные ресурсы как локальные.

Такие возможности специфичны для каждого продукта.

Электронный офис

Наличие программ текстового редактора, электронных таблиц и т. п. стало фактическим стандартом для персонального компьютера. Большинство пользователей не задумываются о требуемой функциональности от этих продуктов и той цене, которую приходится платить за эти программы.

Можно уверенно сказать, что подавляющая часть пользователей не использует возможности, заложенные в последних версиях продуктов. Для текущей работы с документами полностью достаточно той функциональности, которая присутствует в бесплатных версиях.

Наиболее известной версией бесплатного офисного пакета является OpenOffice.

Примечание

В связи с тем, что компания Sun Microsystems вошла в состав Oracle, у сообщества были опасения в сохранении для этого продукта статуса бесплатного. В итоге появился продукт LibreOffice, по сути это клон OpenOffice, но с публичной лицензией. Через некоторое время Oracle передал открытому сообществу права на OpenOffice. Таким образом, это решение остается бесплатным для использования.

OpenOffice бесплатен для применения. В его состав входят:

- текстовый процессор OpenOffice.org.Writer (аналог Microsoft Word);
- редактор формул OpenOffice.org.Math (в пакете Microsoft Office используется как встроенный объект);
- редактор рисунков OpenOffice.org.Draw;
- редактор электронных таблиц OpenOffice.org.Calc (аналог Microsoft Excel);
- редактор презентаций OpenOffice.org.Impress (аналог Microsoft PowerPoint).

Интерфейс программы полностью напоминает Microsoft Office в том варианте, который был до появления ленточного интерфейса (рис. 2.9). Лично автору этот интерфейс более удобен в работе, чем новый, но это, конечно, дело вкуса.

OpenOffice позволяет редактировать документы Microsoft Office (в том числе и последних версий — .docx и аналогичных), свой же собственный формат документов стандартизован в нашей стране.

Продукт локализован. Можно скачать базовый дистрибутив с сайта **http://download.openoffice.org/** и использовать его совершенно свободно и бесплатно.

Обратите внимание, что есть и сборка продукта от Инфра-ресурс (**http://i-rs.ru/download**), являющаяся коммерческим продуктом. Как написано на сайте,

"*InfraOffice.pro генерирует предупреждения при подписи, сохранении или отправке документа со скрытой информацией (правки, комментарии, поля и т. п.) и/или персональными данными, предоставляя средства автоматизации для их удаления*". Если вам нужна эта функциональность, то вы можете заплатить за такой продукт, но лично я не вижу смысла в такой версии. Базовый продукт удовлетворяет обычно полностью всем потребностям пользователей.

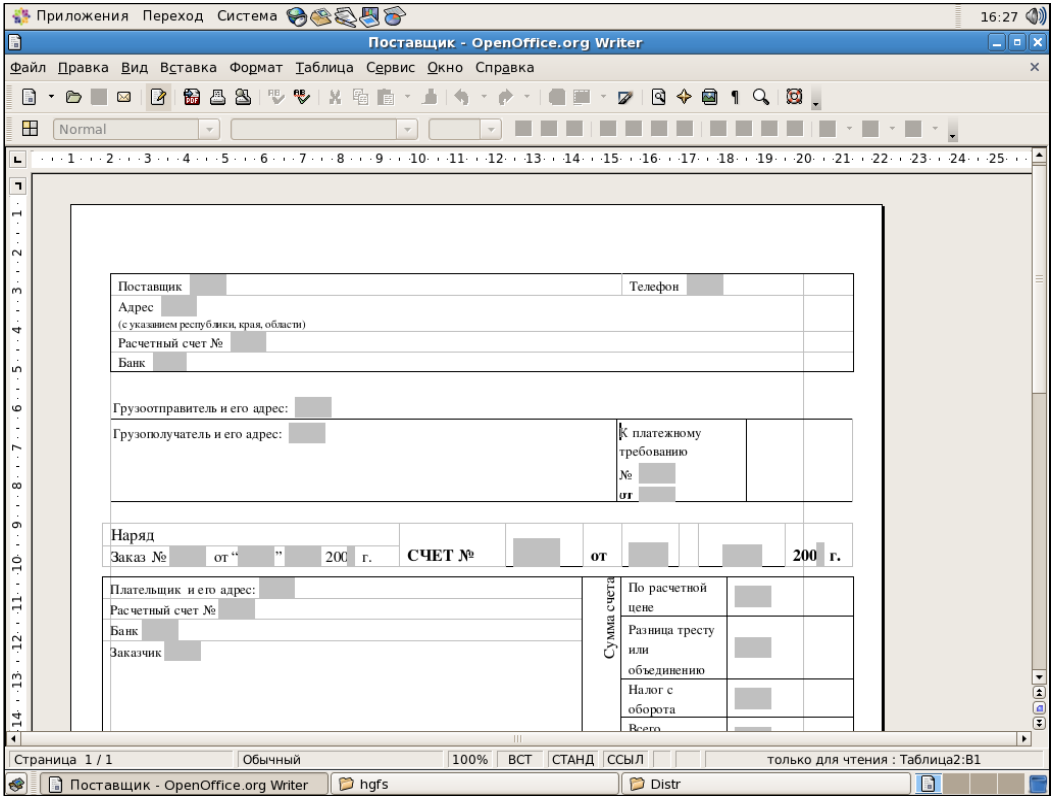


Рис. 2.9. Окно документа Microsoft Office в программе OpenOffice. На рисунке показан счет, созданный на основе шаблона Microsoft Office (доступен для загрузки в качестве образца с сайта Microsoft по адресу **http://office.microsoft.com/ru-ru/templates/TC010700121049.aspx?CategoryID=CT101172551049**) и открытый в пакете OpenOffice в среде Linux (операционная система CentOS). Нетрудно убедиться, что, несмотря на сложную структуру документа, его оформление сохранилось при открытии в OpenOffice

OpenOffice может быть использован на предприятиях с централизованным управлением по групповым политикам. Рекомендации по разворачиванию групповых политик для OpenOffice подробно описаны на сайте **http://openofficetechnology.com/**.

Причины сохранить Microsoft Office, конечно, могут быть. Например, часть прикладного программного обеспечения осуществляет экспорт информации в документы Microsoft Word. Сложности сформировать документы OpenOffice нет, однако это просто не предусмотрено в программе. Или часть бухгалтерских отчетов формируется в Microsoft Excel, причем шаблоны поставляются внешней организа-

цией и содержат сценарии на VisualBasic, при преобразованиях которых часто возникают проблемы.

Электронная почта

Если для индивидуального пользователя часто достаточно почтового ящика на любом из бесплатных серверов Интернета, то серьезность организации проявляется и в наличии собственного почтового домена, когда в правой части адреса указывается имя собственного домена организации.

Самый простой способ организации подобного почтового обслуживания заключается в размещении сервера на ресурсах Интернет-провайдера. После регистрации собственного доменного имени достаточно доплатить еще небольшую сумму и оформить услугу почтового обслуживания. Преимущества такого варианта: надежность (решения провайдера выполнены в отказоустойчивом варианте), доступность из любой точки Интернета, возможность простейшей обработки сообщений (например, фильтрация спама и т. п. — зависит от конкретных условий).

Однако в последнее время от почтового сервера ждут не только обмена сообщениями, но и поддержки функциональности организации групповой работы: наличие календаря и планирования встреч, общих папок хранения сообщений и документов, единых списков контактов и т. п. Частично данный функционал можно реализовать и на бесплатных почтовых ящиках, например, в Gmail можно вести календарь, а если в качестве клиента использовать обозреватель Chrome, то и получать оповещения на рабочий стол о предстоящих событиях и т. п. Однако более функциональными являются локальные решения, которые можно выбрать и настроить под конкретные пожелания.

> ***Примечание***
>
> *Gmail* (от Google Mail) — бесплатная услуга электронной почты от американской компании Google. Предоставляет доступ к почтовым ящикам через веб-интерфейс и по протоколам POP3, SMTP и IMAP.
>
> *Chrome* — браузер, разработанный компанией Google на основе свободного браузера.

Среди коммерческих решений корпоративной работы можно отметить Lotus от IBM и Exchange Server от Microsoft.

Сервер и клиенты Lotus присутствуют в версиях как для Linux-систем, так и для Windows. Отличительной особенностью Lotus является построение продукта как распределенной базы данных. В результате, используя Lotus как транспортную систему, легко реализуются такие приложения, как, например, учет и регистрация входящей корреспонденции, заявлений и т. п.

Exchange Server можно установить только на серверы Windows, а основной клиент — Microsoft Outlook — так же предназначен для стационарных и мобильных Windows-систем. Преимущество данного варианта организации корпоративного обслуживания — в интеграции всей линейки продуктов Microsoft. Единый интерфейс всех продуктов офиса, типовое управление, легкость обмена данными.

Эти перечисленные чуть ранее продукты являются коммерческими, и их внедрение часто не по карману небольшим организациям. В то же время существует ряд бесплатных продуктов, которые поддерживают возможности групповой работы, в частности:

- eGroupware (**http://www.egroupware**.org/);
- Group-Office (**http://www.group-office.com**);
- Open-Xchange (**http://mirror.open-xchange.org/ox/EN/community/**);
- Scalix (**http://www.scalix.com**, бесплатная версия имеет некоторые ограничения функциональности по сравнению с коммерческим вариантом);
- Kolab (**http://www.kolab.org**);
- OGo-OpenGroupware (**http://www.opengroupware.org/**);
- Zimbra (**http://www.zimbra.com/**);
- Open Source Outlook MAPI Connector (**http://www.openconnector.org**/).

Так, автор уже много лет эксплуатирует в различных организациях систему корпоративной работы Zimbra Collaboration Suite Open Source Edition (*ZCS*). Архитектура этого продукта представлена на рис. 2.10.

В Zimbra Collaboration Suite Open Source Edition реализованы, например, следующие возможности:

- *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.
- Функция "*Адресная книга*", позволяющая создавать собственные списки контактов и использовать контакты пользователей из службы каталогов домена Windows.
- 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.
- Функция "*Папки документов*", позволяющая хранить в почтовом ящике документы пользователя и предоставлять их в совместный доступ с назначением прав для конкретных пользователей.
- Функция "*Портфель*", позволяющая создавать документы средствами ZCS и т. д.

Отметим также, что все почтовые сообщения в ZCS проверяются на сервере антивирусной программой и программой блокировки спама. И весь этот комплект функций абсолютно бесплатен!

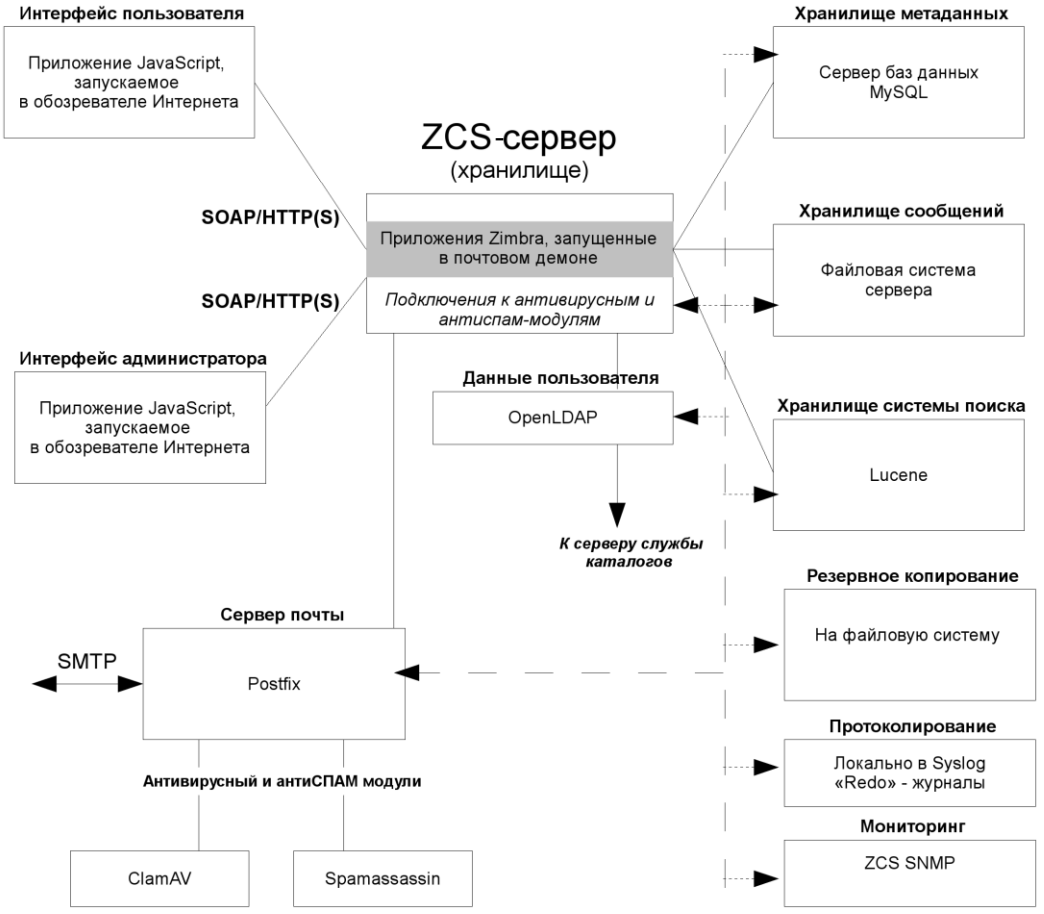


Рис. 2.10. Архитектура ZCS

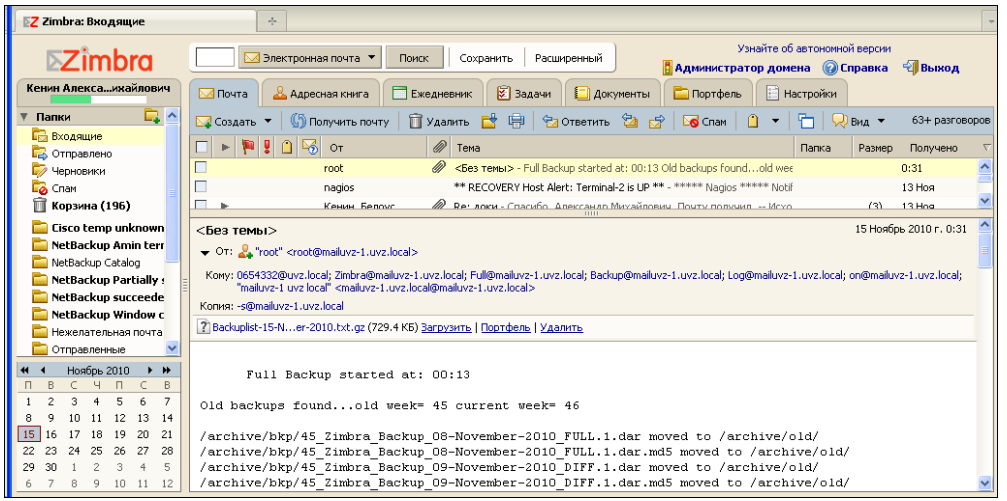


Рис. 2.11. Пример веб-интерфейса ZCS

Для работы с ZCS по стандартным почтовым протоколам (POP3, IMAP, HTTP/HTTPS, SMTP/SMTPS) можно использовать любые почтовые клиенты. Корпоративная функциональность доступна либо в собственном бесплатном клиенте, либо при использовании веб-интерфейса (рис. 2.11).

Свободное программное обеспечение

Типовые задачи в настоящее время успешно можно решать только при помощи бесплатного программного обеспечения. Список доступных программ постоянно пополняется. Поэтому следующую таблицу (табл. 2.2) приведу, скорее, как некую стартовую точку, которая должна показать существующие возможности.

Таблица 2.2. *Перечень некоторых бесплатных программ для Windows*

Название и соответствующий сайт	**Примечание**
OpenOffice (**http://www.openoffice.org/**)	Пакет программ офиса, включает текстовый процессор, программы для работы с электронными таблицами, базами данных, презентациями. Форматы документов совместимы с продуктами Microsoft Office
Firefox (**http://www.firefox.com/**) Google Chrome (**http://www.google.ru/chrome?hl=ru**)	Обозреватели Интернета. Особенность этих программ в том, что для них созданы тысячи различных дополнений, расширяющих функциональность обозревателя: различные записные книжки, блокировщики рекламы, переводчики и т. п. Поэтому не ограничивайтесь загрузкой самой программы, а обязательно расширьте ее возможности установкой дополнений. Интерфейс русский
GIMP (**http://www.gimp.org/**)	Графический редактор — в некотором смысле аналог Adobe Photoshop. Работает со слоями, содержит множество инструментов и фильтров для обработки изображений, различные кисти и т. п. Интерфейс русский
ImageBurn (**http://www.imgburn.com/**) InfraRecorder (**http://infrarecorder.org/**)	Программы для записи, копирования CD- и DVD-дисков. Работают с аудио-, видеодисками и дисками с данными и с их образами. Русский интерфейс загружается дополнительно
NanoCAD (**http://www.nanocad.ru/**)	Базовая САПР-платформа для различных отраслей. Свободно распространяемая
FreeCommander (**http://www.freecommander.com/**)	Файловый менеджер. Для тех, кто привык работать с панелями Norton'a. Интерфейс русский
7Zip (**http://www.7-zip.org/**)	Архиватор. Может распаковать архивы форматов ARJ, CAB, CHM, CPIO, DEB, DMG, HFS, ISO, LZH, LZMA, MSI, NSIS, RAR, RPM, UDF, WIM, XAR и Z. Есть русскоязычный интерфейс

Таблица 2.2 *(продолжение)*

Название и соответствующий сайт	Примечание
CCleaner (**http://www.ccleaner.com/**)	Мощная программа для чистки реестра системы. Интерфейс англоязычный
Avast! (**http://www.avast.com/**) AVG (**http://free.avg.com/**) Avira (**http://www.free-av.com/**) PCTools Antivirus (**http://www.pctools.com/free-antivirus/**)	Некоторые антивирусные программы, лицензия которых предусматривает бесплатное применение в некоммерческих целях. В коммерческих целях можно использовать ClamWin (**http://www.clamwin.com/**), но он не содержит антивирусного монитора в реальном режиме времени (позволяет сканировать файлы). В то же время на его основе созданы антивирусные серверы, сканирующие весь входящий трафик организации (как почтовый — см. раздел "*Zimbra Collaboration Suite*", так и трафик Интернета (см. *"Антивирусная проверка HTTP-трафика"*)
ZoneAlarm (**http://www.zonealarm.com/**)	Персональный межсетевой экран
COMODO (Internet Security (**http://www.personalfirewall.comodo.com/**)	Система персональной защиты, включающая межсетевой экран и антивирусную проверку
PC Tools Firewall Plus (**http://www.pctools.com/firewall/**)	Межсетевой экран для Windows, включая версии Windows 7 и 2008, как 32-битной, так и 64-битной архитектуры
Ad-Aware Free (**http://lavasoft.element5.com/**)	Программа для защиты от вредоносных кодов (SpyWare, mailware и т. д.)
PDF creator (**http://sourceforge.net/projects/pdfcreator/**) PDF converter (**http://www.dopdf.com//**)	Утилиты устанавливают в системе PDF-принтер: печать на этот принтер создает документы в формате PDF (исключается необходимость в программе Adobe Acrobat)
Foxit Reader (**http://www.foxitsoftware.com/**)	Легкая альтернатива Acrobat Reader (то же бесплатной программы)
Babiloo (**http://babiloo-project.org/**) GoldenDict (**http://goldendict.org/**)	Программы-переводчики
Inkscape (**http://www.inkscape.org/**)	Редактор векторной графики, сходный по возможностям с Illustrator, Freehand, CorelDraw
Cuneiform (**http://www.cuneiform.ru/**)	Программа оптического распознавания символов
Codendi (**http://www.codendi.com**) Collabtive (**http://collabtive.o-dyn.de**) dotProject (**http://www.dotproject.net**) eGroupWare (**http://www.egroupware.org**) KForge (**http://www.kforgeproject.com/**) и др.	Программное обеспечение управления проектами, основанное на Web-интерфейсе. Поддерживает обычно управление ресурсами, контакты, систему обмена сообщения, отслеживания событий, управления документами и т. д. Сравнительную характеристику продуктов можно уточнить на странице **http://en.wikipedia.org/wiki/List_of_project_management_software**

Таблица 2.2 *(окончание)*

Название и соответствующий сайт	Примечание
SugarCRM (**http://www.sugarcrm.com/crm/community/sugarcrm-community.html**)	Бесплатная версия коммерческого пакета управления отношениями с клиентами (CRM)
Alfresco (**http://www.alfresco.com/**)	Система управления документами (Enterprise Content Management)

Базовые сведения о работе в *nix-системах

Информационные системы предприятий не мыслятся сегодня без серверов, работающих на одном из клонов *nix-систем.

Linux-мифы

Бесплатные операционные системы и прикладные программы являются серьезным конкурентом коммерческим продуктам. На большинстве рабочих мест можно безболезненно перейти на программы с открытым кодом. Естественно, что вокруг этой проблемы существует много рекламных спекуляций, призванных внушить пользователям и руководителям определенные представления о "правильном" пути.

Автор не ставит целью дать подробную инструкцию по работе с Linux-системами. Открытых источников очень много, и во многом они лучше того, что я смог бы предложить читателю. Постараемся просто объективно сравнить основные характеристики коммерческого и бесплатного продуктов и познакомить читателей с другим классом операционных систем, чтобы каждый смог самостоятельно составить собственное мнение о быстро развивающихся продуктах.

Современные операционные системы и прикладные программы, особенно самые массовые, строятся, прежде всего, на стандартах. Как Linux, так и Windows могут использовать одинаковые сетевые протоколы, единую пользовательскую базу (сервер с учетными записями пользователей может быть как на основе Linux, так и Windows) и т. п.

Естественно, что полной тождественности различных продуктов быть не может. Возникающие проблемы носят, прежде всего, психологический характер. Когда я решил сменить обозреватель Интернета (в то время это был вынужденный шаг, поскольку производительности моего компьютера не хватало для работы в Internet Explorer), то несколько дней меня не покидало чувство дискомфорта и желание вернуться в привычную среду. Сейчас я уже ни за что не откажусь от работы в Firefox: эта программа мне кажется более удобной и предоставляет большие возможности. Существенно меньшие неудобства были связаны с переходом к OpenOffice.

Сегодня в распоряжении пользователей большое количество разнообразных дистрибутивов Linux на любой вкус. Их легко найти и скачать из сети Интернет. Дистрибутивы для серверов и рабочих станций отличаются только набором программ, вы легко можете установить дополнительные пакеты и использовать, например, рабочую станцию в качестве сервера.

Для работы сервера Linux графический интерфейс излишен. И администраторы, приобретшие даже незначительный опыт работы, стараются выполнять большинство операций именно в режиме командной строки. Тем не менее, графический интерфейс в данной операционной системе также присутствует, и вы можете использовать его для настроек так же, как делали это в Windows.

В то же время, использование командной строки имеет ряд преимуществ. Во-первых, команды очень легко автоматизировать, используя пакетные файлы. Во-вторых, графический интерфейс сам может быть причиной ошибок, кроме того, на оформление затрачиваются серьезные ресурсы системы. В-третьих, использование текстовых файлов конфигурации программ позволяет очень легко переносить настройки с одной системы на другую, а для резервирования системы в большинстве случаев достаточно сохранить несколько текстовых файлов.

Примечание

Не случайно, что и базовая функциональность нового сервера от Microsoft — Windows Server 2008 — предполагает отказ от графического интерфейса и работу исключительно в режиме командной строки.

Безопасность в Linux и Windows

Очень много разговоров ведется о безопасности работы в операционных системах. При этом приводятся различные данные, которые должны показать преимущество той или иной операционной системы. Сейчас очень популярны цифры о количестве обнаруженных уязвимостей и сроках их устранения, причем в зависимости от критериев оценки лидером "становится" то одна, то другая система. Можно рассматривать количество обнаруженных уязвимостей, можно оценивать степень их опасности и сроки реагирования разработчика. Любая такая оценка будет объективной, но насколько она отражает реальную жизнь?

Я бы советовал больше прислушиваться к мнению практикующих администраторов, сопровождающих системы на Linux. Для однажды установленной операционной системы и запущенного на ней программного обеспечения сам факт перезагрузки уже является нештатной ситуацией. Компьютер с Linux просто всегда работает и выполняет возложенные на него задачи.

Примечание

При освоении Linux необходимо сразу заставить себя отказаться от практики перезагрузок компьютера: в отличие от Windows, это не приносит никакого эффекта. Причины практически любых проблем нужно искать в системных настройках.

Несколько моментов, о которых следует знать пользователям Linux

В Интернете представлен весьма большой объем документации по настройке Linux, и если возникла та или иная проблема, скорее всего, вы найдете необходимые рекомендации простым поиском в Сети. Здесь упомянем только несколько основных моментов, которые нужно учесть администраторам, имеющим опыт работы только в Windows.

Собственно сам Linux — это только *ядро*. Остальное — это приложения и службы, которые вы устанавливаете. Нечетные номера версий — экспериментальные, четные (2.8 и т. п.) представляют собой стабильные сборки.

В Linux не принято хранить файлы "где придется". Есть достаточно четкая структура размещения информации (см. табл. 2.3 в *разд. "Структура папок Linux" далее в этой главе*), поэтому, например, все пользовательские данные будут находиться только в папке соответствующего личного профиля.

При работе в консоли система позволяет автоматически дополнять ввод с клавиатуры по нажатию клавиши <Tab>. Например, если требуется скопировать файл, то достаточно набрать команду (`cp`), первые символы имени файла и нажать клавишу <Tab>. Если первые символы однозначно определяют имя файла или команды, то система автоматически допишет полное название. В противном случае никаких изменений на экране не будет, а повторное нажатие клавиши <Tab> выведет на экран полный перечень имен, начинающихся с введенных символов.

> ***Примечание***
>
> Состав доступных команд зависит от учетной записи, под которой выполнен вход в систему. Если вы не видите в списке требуемой команды, попробуйте переключиться на учетную запись root.

Как правило, пользовательская работа в Linux ведется при помощи графического интерфейса, однако в любой момент можно начать работу в нескольких *консолях*. Для этого достаточно запустить новый сеанс с помощью нажатия клавиш <Ctrl>+<Alt>+<F1>, <Ctrl>+<Alt>+<F2>[1] и т. д. (графическому интерфейсу соответствует сочетание клавиш <Alt>+<F7>).

Работу в консоли существенно облегчит использование программы *MidNight Commander — mc* (рис. 2.12). Программа практически повторяет интерфейс и возможности Norton Commander, с которого начиналась вся работа на компьютерах под управлением операционной системы DOS. При помощи программы mc можно осуществлять любые файловые операции (копировать, переименовывать, удалять, создавать папки и т. д.), редактировать файлы, просматривать архивы, установочные пакеты и т. п. MidNight Commander по умолчанию не устанавливается, но

[1] Клавиша <Ctrl> требуется только при запуске команды в графическом режиме. После переключения в режим консоли переходить в другой сеанс можно нажатием клавиш <Alt>+<F*n*>, возврат в графический режим также будет выполняться нажатием сочетания клавиш <Alt>+<F7>.

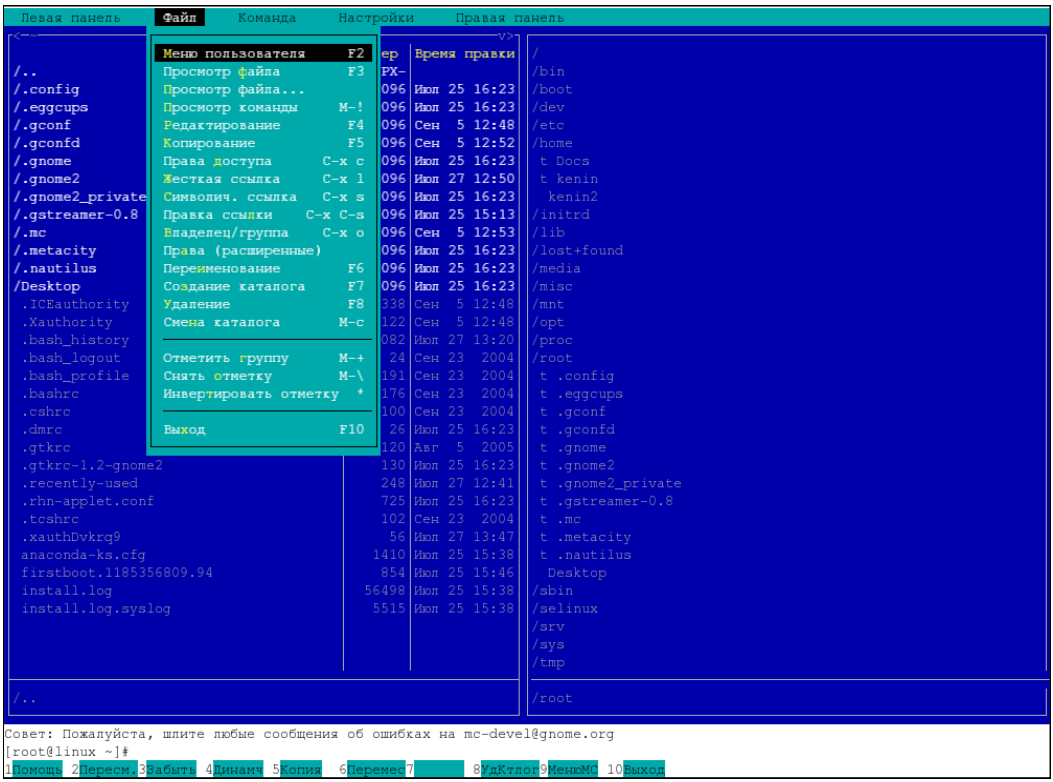


Рис. 2.12. Программа MidNight Commander

входит в большинство дистрибутивов Linux. Думаю, что вы не пожалеете, если будете использовать возможности данной программы.

В Linux расширения имен файлов не используются для ассоциации выполняемых операций. Исполняемым может быть *любой* файл, необходимо только предоставить ему соответствующее разрешение. Кстати, это повышает безопасность системы.

Команды в Linux чувствительны к регистру. Например, ключи `R` и `r` могут обозначать различные операции.

В Linux не принято подключать жесткие диски под именами логических дисков (C, D, E и т. д.). Обычно диски *монтируются*: добавляются в качестве новой папки в определенное место файловой структуры.

Так же, как и в Windows, в Linux создаются пользователи, которых можно объединять в группы. Учетные записи могут быть как локальными, так и храниться централизованно (и использоваться на нескольких компьютерах). В Linux есть один "суперпользователь", которому разрешено все. Его имя — root. Работа от имени этой учетной записи не приветствуется. Текущие операции выполняются с правами обычного пользователя, в случае операции, требующей административных прав, система запрашивает пароль учетной записи root (и обычно сохраняет его некоторое время в памяти для удобства последующих административных операций).

Права доступа обычно отображаются в виде последовательности символов `-rwxr-x--x`. Первый символ указывает тип файла (`-` — обычный файл, `d` — папка, возможны также псевдофайлы), следующие три символа определяют права владельца файла, следующие три — права группы, к которой принадлежит владелец, и последние три обозначают права для всех остальных пользователей. В каждой тройке первый символ свидетельствует о наличии права чтения (`r`) или его отсутствии (дефис), 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`.

Структура папок Linux

Linux предполагает четкую структуру расположения папок и файлов. В табл. 2.3 приведены наиболее "значимые" папки системы.

Таблица 2.3. *Типовая структура папок в Linux*

Папка	**Назначение**
/sbin	Папка с программами редактирования и проверки структуры диска, а также изменения состояния системы
/dev	Содержит записи, соответствующие устройствам, подключенным к системе
/usr/bin	Папка программ работы с учетными записями. В этой же папке хранятся программы демонов
/etc	В этой папке находится основная часть файлов локальной конфигурации системы
/etc/init.d	Скрипты запуска системы. Часто указывают, в свою очередь, на папки /etc/rc?.d (? — цифра от 0 до 6, соответствует уровню запуска)
/home/*username*	Домашняя папка пользователя *username*
/usr	Папка с общими программами; доступна только для чтения
/usr/local	В эту папку должны устанавливаться прикладные программы
/usr/share/doc	Папка, в которую обычно копируется справочная документация по установленным программам
/lib	Папка с программными библиотеками
/mnt	Обычно используется для подключения устройств (диски, CD-ROM и т. д.)
/opt	Папка, в которой обычно размещаются устанавливаемые программы, имеющие большой объем
/proc	Папка для хранения специальных файлов, формируемых ядром системы
/var	Папка для изменяемых данных. Содержит, в том числе, папки журналов системы

Текстовый редактор vi

Если используется графическая оболочка, то для редактирования файлов применяются программы типа OpenOffice, Gedit и аналогичные, работающие в графическом режиме. Однако в аварийных ситуациях, когда нужно восстанавливать систему, а обычно такие операции выполняются в нервной обстановке и при отсутствии времени, работать можно только в консоли.

В Linux существует очень мощный текстовый редактор, который запускается командой `vi` (в терминале). Умение пользоваться им может оказаться очень полезным.

Редактор можно запустить сразу с открытием файла. Для этого после vi нужно через пробел указать имя файла.

Текстовый редактор vi имеет два режима работы: командный и редактирования. При открытии файла вы попадаете в командный режим, в котором можно выполнять такие операции, как поиск, замена, сохранение файла, вызов внешней команды и т. п.

Чтобы начать ввод текста, следует перейти в режим редактирования. Например, чтобы ввести символ в текущей позиции, надо нажать сначала на клавишу `i` и только потом начать набор. Если нажать клавишу `a`, то символы будут вводиться справа от позиции курсора и т. п. Обычной ошибкой пользователей, начинающих работу в vi, является попытка удаления символов или перемещения курсора в режиме редактирования. В этом случае редактор набирает спецсимволы, поэтому приходится выходить в командный режим, удалять ошибочный ввод, перемещаться в нужную точку текста и снова входить в режим редактирования.

Чтобы вернуться из режима редактирования в командный режим, следует нажать клавишу <Esc>.

В редакторе доступно много команд, они подробно описаны в Интернете. Упомяну лишь самые основные, которые позволят выполнить простейшие операции с текстом (табл. 2.4).

Таблица 2.4. *Команды текстового редактора vi*

Команда	Действие
`a`	*Добавить*. Переход в режим ввода текста *справа* от курсора
`i`	*Вставить*. Переход в режим ввода текста *слева* от курсора
Клавиши перемещения курсора	Перемещение курсора по документу. Для перемещения курсора используются также четыре расположенные в ряд клавиши <h> (влево), <j> (вниз), <k> (вверх) и <l> (вправо). Можно использовать их вместе с цифрами: например, ввод команды `9k` переместит курсор на 9 строк вверх
<Ctrl>+<F>/<Ctrl>+<B>	Перемещение на одну страницу вперед/назад
`G`	Переход на последнюю строку документа
`nG`	Переход на строку с номером *n*

Таблица 2.4 *(окончание)*

Команда	Действие
x	Удаление символа над курсором
X	Удаление слова, в котором находится курсор
dw	Удаление символов, начиная с текущего, до конца слова; ввод команды 4dw приведет к удалению *четырех* слов
d$	Удаление символов, начиная с текущего, до конца строки
yw	Копирует текущее слово в буфер
yy	Копирует текущую строку в буфер
p	Вставляет содержимое буфера после курсора
/слово	Поиск символов *слово* вперед
?слово	Поиск символов *слово* назад
:g/поиск/s/замена/g	Замена сочетания символов, указанного в строке *поиск*, на сочетание, указанное в строке *замена*, во всем тексте документа
u	Отмена последней операции (можно отменить несколько шагов)
<Ctrl>+<R>	Восстановление последней отмененной операции
:w	Сохранение файла
:wq	Сохранение файла и выход из режима редактирования
ZZ	То же, что и :wq — сохранение файла и выход
:q	Выход из редактора (операция выполнится, только если все внесенные изменения сохранены)
:q!	Выход без сохранения изменений
:! command	Выполнение внешней команды (*command*)
<Ctrl>+<G>	Вывод информации об имени редактируемого файла и текущей позиции в нем

Выполнение команд с правами другого пользователя

Для выполнения программ с правами другого пользователя служит команда su. При выполнении команды[1]

```
su -
```

система запросит пароль. Введите пароль пользователя root, и вы получите его права (обратите внимание, что при этом изменяется символ приветствия).

Для возвращения введите команду exit или нажмите клавиши <Ctrl>+<D>.

[1] Можно не использовать дефис в качестве параметра: в этом случае вы также получите права администратора, но параметры окружения (например, текущая папка) останутся прежними. При вводе дефиса команда переведет вас в новое окружение.

Помимо переключения на суперпользователя эта же команда, введенная с указанием какой-либо другой учетной записи в качестве параметра, позволяет переключиться на нее, если далее по запросу системы ввести ее имя и пароль:

```
su — user1
```

> ***Примечание***
>
> При переходе от суперпользователя к другому пользователю пароль вводить не требуется.

Прикладные программы в Linux

Операционная система — это только "основа", позволяющая работать в прикладных программах, ради которых и включают компьютер. Сегодняшний Linux включает в себя большое количество бесплатного прикладного программного обеспечения. Это текстовые и графические редакторы, аудио- и видеопроигрыватели, утилиты записи CD/DVD, почтовые клиенты и обозреватели Интернета, серверы баз данных и т. п.

Программы для Linux доступны обычно в двух вариантах: в исходных кодах и в пакетах, полностью подготовленных для автоматической установки. При наличии предварительно скомпилированного пакета именно его и устанавливают. Преимущество этого варианта в том, что при установке автоматически добавляются и необходимые библиотеки (те, которые должны быть установлены для нормальной работы программы, иначе называют зависимостями).

Установочные пакеты хранятся в *депозитариях*. Для того чтобы добавить новую программу в систему, достаточно выполнить простейшую команду. Например, для установки программы в Ubuntu:

```
apt-get install программа
```

Эта команда загрузит из Интернета необходимый установочный пакет и все зависимости и выполнит установку.

Установочные пакеты не всегда существуют для конкретной версии Linux. В этом случае нужно выполнить установку из исходных кодов. Этот процесс несколько более трудоемкий, поскольку требует ручной установки отсутствующих библиотек и предварительной установки программного обеспечения для компиляции.

На портале **http://SourceForge.net** вы можете найти тысячи проектов, среди которых есть и программы управления предприятием (ERP-системы), CRM-системы, системы электронного документооборота и т. п.

Среди коммерческого программного обеспечения можно отметить тенденцию постоянного увеличения числа вендоров, разрабатывающих свои продукты как для систем на основе Windows, так и для использования в Linux. Если примерами крупных западных разработчиков уже вряд ли кого удивишь (например, для системы документооборота Documentum можно выбрать любую платформу и клиента, причем ее версия для Linux характеризуется большей надежностью и повышенной

производительностью), то пример российской фирмы 1С, выпустившей версию своей программы для Linux, говорит о многом.

Кроссплатформенный запуск программ

Существуют как коммерческие, так и бесплатные проекты, позволяющие запускать Windows-программы на Linux-системах. Наиболее известный бесплатный пакет — это Wine (**www.winehq.org**).

Под Wine работают не все программы. Но пользователям в свое время удавалось запустить в этом пакете даже программу 1С.

Второе решение запуска Windows-программ состоит в использовании виртуальной машины. Вы устанавливаете виртуальную машину, в которой запускаете операционную систему Windows и проблемное приложение. Данный способ гарантированно позволит продолжать использовать прикладную программу, но потребует приобретения лицензионной копии Windows.

Существует возможность запускать и Linux-программы под Windows. Интересующихся читателей можно отослать к ресурсам Интернета.

Установка Linux

Установка Linux и ее первоначальная настройка не составляют никакой сложности. Операции выполняются в графической среде при помощи мастера установки (рис. 2.13), который в процессе инсталляции запрашивает основные параметры

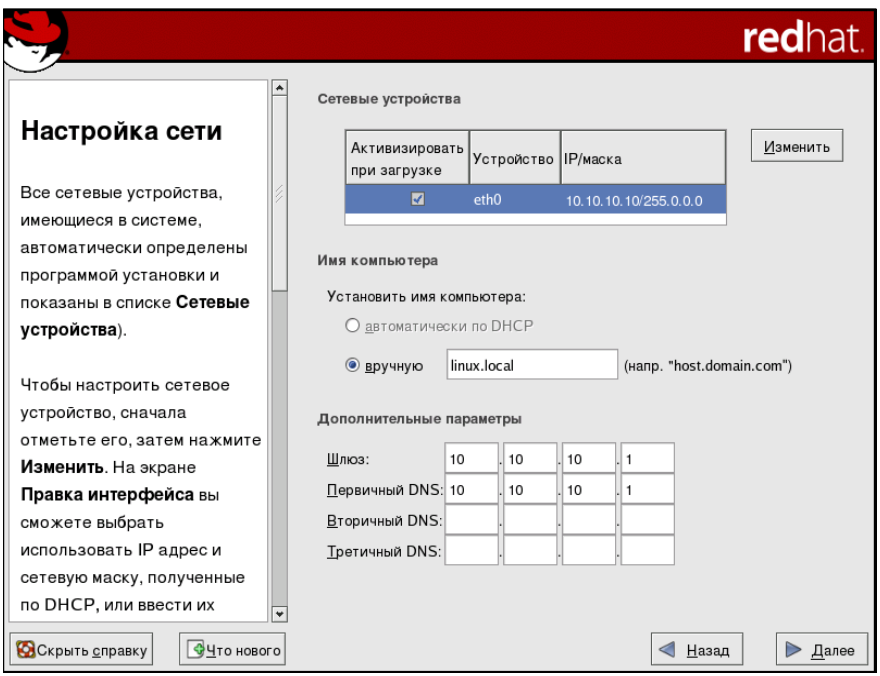


Рис. 2.13. Установка Linux происходит в графическом режиме

(часовой пояс, раскладку клавиатуры, путь установки и т. п.). Если какие-то параметры вам не понятны, можно просто согласиться с вариантом, предложенным мастером по умолчанию.

Многовариантная загрузка

На одном компьютере можно использовать несколько операционных систем. Лучше всего устанавливать их на различные логические диски. Но часто желание попробовать новую операционную систему возникает, когда компьютер уже используется и свободных дисков нет.

Можно воспользоваться возможностями Windows 7 и уменьшить разделы жесткого диска для того, чтобы создать новый раздел и установить систему на него. Но установщики Linux позволяют сами изменить конфигурацию разделов существующей системы *без потери данных*. Мастер установки предложит создать на существующем диске новый раздел, при этом вы можете указать желаемый объем нового раздела (по умолчанию обычно предлагается использовать половину имеющегося свободного пространства). Операция займет некоторое время (зависит от объема жесткого диска), после чего установка Linux продолжится.

Естественно, что подобный вариант действий возможен только тогда, когда первой установленной системой была Windows. Современные установщики Linux "знают" практически все используемые операционные системы других вендоров.

> ***Примечание***
>
> После установки Linux на раздел Windows и последующей загрузки Windows система предупредит о возможных неисправностях диска и предложит выполнить его проверку. При этом возможна и перезагрузка Windows (после установки новых устройств). Это стандартная реакция системы на изменение раздела диска. Данные не потеряны, надо просто один раз согласиться на выполнение предложенных шагов.

Тестирование Linux на виртуальной машине

Если вы хотите предварительно протестировать систему Linux и ознакомиться с ней, то можно воспользоваться ее установкой на виртуальную машину. Можно, конечно, использовать виртуальную машину от Microsoft, но это не самый лучший вариант для Linux-гостевой системы. Я бы рекомендовал проводить эксперименты в среде Oracle VirtualBox.

ГЛАВА 3

Структура сети

Информационная система предприятия начинается с соединений между различными устройствами. От качества этих каналов связи не в последнюю очередь зависит стабильность и надежность работы бизнес-приложений.

Структурированные кабельные сети

Согласно действующим правилам, *структурированные кабельные сети* (СКС) должны проектироваться и монтироваться специализированными организациями, имеющими государственную лицензию на данный вид деятельности. Однако на практике в силу высокой стоимости данных работ монтаж СКС в небольших организациях обычно выполняется собственными силами. Провода прокладываются вдоль плинтусов, а по стенам, в основном по эстетическим соображениям, устанавливаются специализированные короба. При этом далеко не всегда выполняются требования, предъявляемые стандартами СКС.

Действующими стандартами СКС в России являются ГОСТ Р 53245-2008 "Информационные технологии. Системы кабельные структурированные. Монтаж основных узлов системы. Методы испытания" (**http://protect.gost.ru/document.aspx?control=7&baseC=6&page=0&month=11&year=2009&search=53245&id=174298**) и ГОСТ Р 53246-2008 "Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования" (**http://protect.gost.ru/document.aspx?control=7&baseC=6&page=0&month=11&year=2009&search=53246&id=174287**).

> ***Примечание***
>
> Тексты этих документов содержат опечатки, поэтому они должны применяться с осторожностью.

Категории СКС

Кабельные системы характеризуются *категорией*, определяющей качество линии связи (табл. 3.1).

Таблица 3.1. *Категории кабельных систем*

Категория	Максимальная частота сигнала, МГц	Область применения
3	16	Телефонные каналы, локальные сети Ethernet 10Base-T
5	100	Локальные сети со скоростью передачи до 100 Мбит/с
5e	100	Локальные сети со скоростью передачи до 1000 Мбит/с
6	250	Локальные сети со скоростью передачи до 1000 Мбит/с
7	600	Локальные сети со скоростью передачи до 1000 Мбит/с, сети ATM, кабельное телевидение

Кабельную сеть можно отнести к определенной категории, только если при ее создании использованы элементы (розетки, разъемы, кабели и т. п.), удовлетворяющие требованиям данной или более высокой категории, а проектирование и монтаж выполнены в соответствии с требованиями стандартов (ограничения на длины, число точек коммутации и т. д.).

В настоящее время большинство эксплуатируемых кабельных систем относятся к категории 5, которая допускает передачу данных по сети со скоростью до 100 Мбит/с. Категория 5e вводит небольшие дополнительные ограничения, которые позволяют использовать каналы передачи данных с гигабитными сетевыми картами. На практике аккуратно выполненная проводка на элементах категории 5 позволяет осуществлять передачу на скорости до 1 Гбит/с.

Волоконно-оптические сети

При построении кабельной системы предприятия часто возникает необходимость подключения устройств, разнесенных на большие расстояния (100 и более метров). В этом случае успешно применяются волоконно-оптические линии связи.

Обычно одно волокно кабеля используется для передачи сигнала, другое — для приема. Существует оборудование, позволяющее за счет использования различных диапазонов излучения передавать и принимать данные по одному волокну, но оно применяется не часто: обычно оптические кабели проектируются с большим запасом по числу волокон.

При расстояниях 100—200 м применяются *многомодовые* оптические кабели. Стоимость прокладки и эксплуатации такой линии практически соизмерима со стоимостью линии на витой паре. При длинах соединений свыше 200 м используется *одномодовый* оптический кабель. Соответствующее оборудование (приемники и передатчики оптического сигнала) по стоимости в несколько раз дороже, чем модели для многомодового кабеля.

Примечание

Существуют технологии оптического уплотнения (CWDM — Coarse Wavelength-division multiplexing, грубое мультиплексирование с разделением по длине волны, и DWDM — Dense Wavelength Division Multiplexing, плотное спектральное мультиплексирование),

позволяющие по одному волокну передавать несколько каналов данных. Но они оправданы только в случае сверхдлинных линий связи и не применяются на уровне предприятий.

Если расстояние, на которое предполагается передавать данные, измеряется десятками километров, то необходимо использовать передатчики повышенной мощности (они присутствуют в линейках продукции практически всех изготовителей).

Для подключения волоконно-оптических линий применяются специальные модули. Существуют различные модели такого оборудования, на практике в последнее время наиболее распространены SFP-модули, подключаемые в соответствующие порты активного оборудования (рис. 3.1). Но поскольку на практике эксплуатируются различные технологии, при проектировании расширения сети следует обращать внимание на совместимость используемых решений. Например, следует учитывать типы оптических разъемов, которые могут отличаться на оборудовании различных вендоров, принимать во внимание тип оптического кабеля (выпускаются более чем по 5 стандартам), длину волны и т. п.

Примечание

SFP (small form-factor pluggable) — компактный сменный приемопередатчик, регламентирован международным стандартом. В конструктиве SFP выпускаются модули для подключения как витой пары, так и оптических каналов (одномодовых и многомодовых) на различные частоты линии связи.

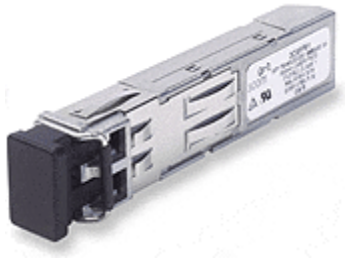


Рис. 3.1. SFP-модуль для подключения оптического канала связи

Эксплуатация волоконно-оптических каналов связи требует повышенной аккуратности со стороны пользователей. Не допускается резко изгибать кабель, следует оберегать оптические поверхности от засорения (не трогать их руками, всегда закрывать концы кабеля и гнезда в модуле подключения специальными заглушками и т. д.). В случае повреждения кабеля обычно требуется приглашение монтажных фирм, поскольку приобретение оборудования для поиска и определения мест неисправности (рефлектометры и т. п.) доступно только специализированным организациям.

Сети 10G

Увеличение объемов информации заставляет постоянно повышать скорости передачи данных. Внедрение мультимедийных приложений (IP-телефония, видеоконференции, системы видеонаблюдения и т. п.) приводит к тому, что величина скоро-

сти передачи в 1 Гбит/с становится недостаточной для магистральных каналов предприятия. Объединение каналов *(см. разд. "Использование "агрегированных" каналов" в главе 10)* не позволяет увеличить это значение на порядок.

Результатом усилий ряда предприятий стала технология передачи на частоте 10 Гбит/с. В настоящее время стандартизовано использование в данных целях как медного кабеля (витой пары), предназначенного для небольших расстояний, так и оптического. На практике соединения 10G применяются для связи коммутаторов уровня ядра предприятия или при оснащении дата-центров, где имеют место самые высокие требования к объемам и скорости передачи данных.

Схема разъема RJ-45

Для подключения компьютера к коммутатору обычно используется расшивка разъема, показанная на рис. 3.2.

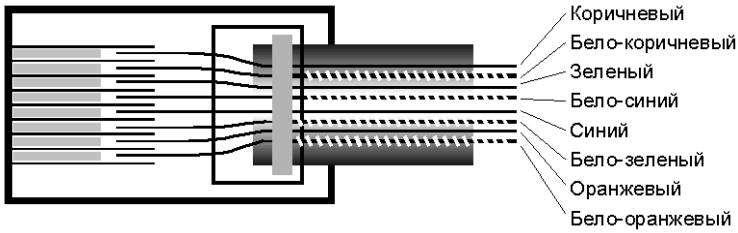


Рис. 3.2. Расшивка разъема RJ-45

На практике применяются два варианта расшивки кабеля — A и B. Один (B, показан на рисунке) используется в основном в странах Америки, другой — A — в странах Европы. Варианты отличаются только "переменой мест" зеленой и оранжевой пар.

Однако даже в условиях одной организации можно встретить оба варианта разделки разъема, например, вследствие выполнения работ разными исполнителями или в результате поставок патч-кордов различных исполнений. Вообще говоря, разделка разъема не сказывается на работе оборудования за исключением случая, когда один конец кабеля разделан по варианту A, а другой — по варианту B. На практике такая ситуация чаще всего возникает при использовании розеток и кросс-шкафов (когда разводку в шкафу делает один человек, а розеток — другой) или при укорачивании существующего кабеля (если исполнитель не проверит тип расшивки отрезаемого разъема).

Для передачи сигналов на линиях связи 100 Мбит/с используются только две пары из четырех (в Gigabit Ethernet на скорости 1000 Мбит/с задействованы все четыре пары), имеющихся в кабеле. Хотя это и не разрешается стандартами, администратор может задействовать оставшиеся пары, например, использовать средние контакты (пара *голубой — бело-голубой* провода) под телефон, а коричневую пару в качестве замены одной из сигнальных при обнаружении обрыва в кабеле. Следует

учитывать, что для питания устройств поверх сети Ethernet (PoE) используется центральная пара проводников и что в гигабитных каналах задействованы все проводники.

Два компьютера можно соединить витой парой *без коммутатора*. Для этого необходима специальная расшивка разъема, которая называется *перекрещенной* (crossover). При такой расшивке на одной из сторон кабеля меняются местами входные и выходные провода (первая и третья пары, см. табл. 3.2). К использованию перекрещенных кабелей приходится прибегать не только в случае соединения "компьютер — компьютер", но и, например, при подключении ADSL-модема непосредственно к сетевой плате компьютера или соединении двух коммутаторов ранних моделей выпуска (ADSL-модемы, как правило, имеют порты, предназначенные для подключения к коммутаторам локальной сети).

Итоговая расшивка такого кабеля представлена в табл. 3.2.

Таблица 3.2. *Перекрещенная схема расшивки разъемов RJ-45*

Разъем 1: цвет жилы	Разъем 2: цвет жилы
Бело-оранжевый	Бело-зеленый
Оранжевый	Зеленый
Бело-зеленый	Бело-оранжевый
Синий	Синий
Бело-синий	Бело-синий
Зеленый	Оранжевый
Бело-коричневый	Бело-коричневый
Коричневый	Коричневый

Примечание

Современные модели коммутаторов обладают возможностью определения типа расшивки кабеля и автоматически переключаются на нужный вариант. У ранее выпускавшихся моделей такой функции нет, поэтому, например, для соединения двух таких устройств между собой также необходимо использовать crossover-кабель. На некоторых моделях имеется либо кнопка переключения типа одного из портов, либо два разъема для одного порта, соответствующих тому или иному варианту подключения (называемых MDI и MDIX).

Варианты исполнения СКС

Кабельная система предприятия может быть выполнена различными способами: по технологии скрытой проводки, в накладных каналах, в пространстве под фальшполом или над навесным потолком и т. п. Собственными силами прокладка кабелей обычно выполняется без трудоемких строительных работ — в накладных каналах, при этом переходы между отдельными помещениями осуществляются либо через отверстия в стенах, либо над накладным потолком коридора.

Внимание: патч-корды

Часто в условиях предприятия экономят на кабелях, при помощи которых осуществляется подключение компьютера в розетку кабельной сети. Следует отметить, что эти кабели, называемые *патч-кордами*, часто являются причиной снижения скорости передачи данных. Они подвергаются наибольшему механическому воздействию, в то время как бывают изготовлены специалистом недостаточной квалификации. С течением времени их параметры ухудшаются, что приводит к периодическим ошибкам передачи данных.

Обратите внимание, что, по данным одного из производителей патч-кордов, две трети их не проходят тестирования после изготовления в промышленных условиях. Трудно ожидать стабильности характеристик от изделий, изготовленных в кустарных условиях, поэтому стоит комплектовать рабочие места только профессионально выполненными патч-кордами.

Составные линии

Стандарты СКС не предусматривают возможности составления линий передачи данных из нескольких участков. Это значит, что соединение компьютера с коммутатором должно состоять из патч-корда, информационной розетки, кабеля, коммутационной панели (на которую "расшит" кабель), патч-корда до разъема на коммутаторе. Если по каким-либо причинам длины кабеля недостаточно (кабель поврежден или сотруднику выделено другое место), то наращивать его *нельзя*.

Однако на практике достаточно часто приходится сталкиваться с необходимостью удлинения кабеля. Ни в коем случае не рекомендуя применять на практике нижесказанное, должен отметить, что на 100-мегабитных сетях кабели вполне удовлетворительно функционируют при наличии скрутки (или, что еще лучше, паяного соединения) двух кусков. При этом следует минимизировать длину участка кабеля, на котором нарушен шаг витой пары. И, поскольку качество контактов скрутки может существенно снизиться через некоторый промежуток времени из-за воздействия внешних условий (например, окисления под воздействием влаги), следует позаботиться о надежной изоляции такого соединения.

Прокладка силовых кабелей

Каждое рабочее место пользователя должно быть оборудовано розеткой электропитания с заземлением и информационными розетками. В небольших организациях обычно используют розетки существующей электропроводки. При этом следует учитывать, что расстояние между силовой и информационной розетками одного рабочего места по стандарту не должно превышать 1 м. Кроме того, в целях снижения уровня помех и повышения пожароустойчивости в стандартах определяется минимальное расстояние между силовым и информационными кабелями: оно зависит от потребляемой мощности, но обычно можно ориентироваться на значение в 10—15 см. На практике редко удается выдержать такие расстояния, поэтому, чтобы минимизировать влияние силового кабеля, часто используют специальные кабели с экранированием.

При размещении большого числа пользователей в помещении, не оборудованном достаточным количеством силовых розеток, часто осуществляется проводка силовых и информационных кабелей до рабочего места в одном канале. Согласно стандарту, если оба кабеля прокладываются в общем канале, то должна быть предусмотрена сплошная перегородка между силовыми и информационным отсеками.

Примечание

Одним из мощных источников электропомех являются люминесцентные лампы. При прокладке информационных кабелей часто не обращают внимания на их близость к таким лампам, например, при монтаже новых трасс над фальшпотолком. Для снижения влияния данного источника помех не следует допускать прокладку информационного кабеля ближе 15 см от люминесцентной лампы.

Питание по сети Ethernet

Современное оборудование, подключаемое к компьютерным сетям, часто потребляет совсем немного мощности. Учитывая, что в стандартах передачи данных 10/100 Мбит/с используются только две пары проводников витой пары из четырех имеющихся, часто можно существенно сэкономить на прокладке кабелей, если применить технологию *питания оборудования по кабелю Ethernet* (Power over Ethernet, PoE).

Какое оборудование запитывают по технологии PoE? Обычно это IP-телефоны, точки беспроводного доступа, камеры видеонаблюдения и т. п.

Существует несколько вариантов обеспечения PoE. Первый состоит в использовании специальных коммутаторов либо уже имеющих функцию PoE, либо поддерживающих ее (коммутаторы допускают установку дополнительного блока питания, после чего обеспечивается предоставление услуги PoE). Данный способ применяется при наличии значительного числа портов с функцией PoE, например, при эксплуатации в организации IP-телефонов.

Примечание

Администраторы могут использовать управление портами PoE для того, чтобы, например, перезагрузить зависшее устройство: достаточно снять напряжение с соответствующего порта, а потом снова подать его при помощи команд управления коммутатором.

Второй способ подачи питания через сеть Ethernet заключается в приобретении специальных блоков питания, включаемых в "разрыв" сетевого кабеля (для подачи напряжения 48 В используется коричневая пара проводников). Такое решение оправдано при подключении единичных устройств.

В PoE-коммутаторах применяется специальная технология для проверки порта. Перед подачей питания на порт выполняется специальное тестирование, замеряются параметры подключенного оборудования и, если оно соответствует требованиям технологии PoE, коммутатор включает питание. Таким образом, в порты PoE можно безопасно включать обычные устройства. При использовании же "врезных" блоков питания, особенно самых дешевых их вариантов, следует исключить возможность случайного подключения другого оборудования.

В соответствии со стандартом 802.3af максимальная мощность, которая может быть получена устройством с PoE-порта, составляет 12,95 Вт (при этом порт должен обеспечить мощность до 15,4 Вт). Подключаемые устройства часто потребляют меньшую мощность, например, типовая точка беспроводного доступа потребляет около 11 Вт, IP-телефоны — от 2 до 14 Вт в зависимости от модели. В целях экономии на большинстве моделей коммутаторов суммарно допустимая мощность питания по портам Ethernet меньше величины 15,4 × <*количество портов*> в ваттах (Вт). В случае превышения допустимого значения потребляемой мощности коммутатор начинает *отключать* питание отдельных портов, учитывая *приоритеты* портов для PoE, которые администратору необходимо назначить вручную в соответствии с предназначением подключенного оборудования.

Требования пожарной безопасности

Основные требования пожарной безопасности при прокладке кабелей в офисе заключаются в следующем:

- кабели, каналы, розетки и т. п. должны соответствовать определенной категории пожароустойчивости; обычно это выполняется при помощи современных элементов СКС;
- силовые и информационные кабели при прокладке в одном канале должны быть разделены сплошной перегородкой. Минимальное расстояние от силовых кабелей до информационных определяется по специальным нормативам в зависимости от нагрузки, но обычно не должно быть менее 12—15 см;
- отверстия, выполненные для прокладки кабелей между помещениями, должны быть закрыты легкоудаляемым негорючим материалом, например, цементом или гипсом низкой прочности, минеральной ватой и т. п.;
- при прокладке кабелей в пространстве над навесным потолком недопустимо использовать горючие материалы.

В случае монтажа кабельной системы под фальшполом нормативами налагаются более строгие ограничения. Например, разделение пространства под фальшполом на зоны, отделяемые друг от друга несгораемыми материалами и т. п.

Топология сети

Под топологией понимают схему расположения и соединения устройств сети. Обычно выделяют две топологии: *физическую*, которая описывает реальное расположение устройств и наличие каналов связи между ними, и *логическую*, создаваемую поверх физической и описывающей пути передачи данных.

Размеры сегментов сети на витой паре

Длина 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. 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 возрастает уровень помех, возникающих при отражении высокочастотных сигналов от точки соединения кабеля и розетки. Это может привести к увеличению числа ошибок в линии.

Для локальной 10-мегабитной сети, построенной на *концентраторах*, существует "правило 5/4": между любыми двумя сетевыми устройствами должно быть не более 5 сегментов сети с четырьмя концентраторами *(хабами)*. Это требование ограничивает размер сети диаметром 500 м, построенной на концентраторах и с использованием витой пары. Ограничение на длины обусловлено самой природой Ethernet, принципами, на которых строится такая сеть, и не зависит от совершенствования элементной базы. В сети Ethernet каждая система может начать передачу данных в произвольный момент времени, независимо от других устройств. Если во время передачи система обнаруживает чужую посылку данных, то эта ситуация (одновременная передача информации несколькими системами называется *коллизией*) детектируется, и данные будут повторно переданы каждой из этих систем через некоторый случайный промежуток времени. При больших размерах участка сети такая коллизия может быть не обнаружена (система "не услышит" чужой пакет во время попытки своей передачи), что приведет к потере данных, повторам передачи и результирующему снижению пропускной способности сети.

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

Типовая структура сети предприятия

На практике существует два подхода к построению каналов передачи данных. В первом случае развитие начинается от комнаты системного администратора, в которой устанавливается коммутирующее оборудование, становящееся центром сети. В дальнейшем, по мере увеличения числа рабочих мест, к сети подключаются новые коммутаторы, и структура сети принимает достаточно хаотичный вид (рис. 3.3).

Подобная сеть, хотя и обеспечивает текущее функционирование сетевых приложений, не является отказоустойчивой и часто не позволяет внедрить современные решения, критичные к параметрам инфраструктуры.

Если предприятие въезжает в новый офис, то, как правило, структура сети проектируется "с нуля". Для структуры сети принято выделять несколько *уровней*.

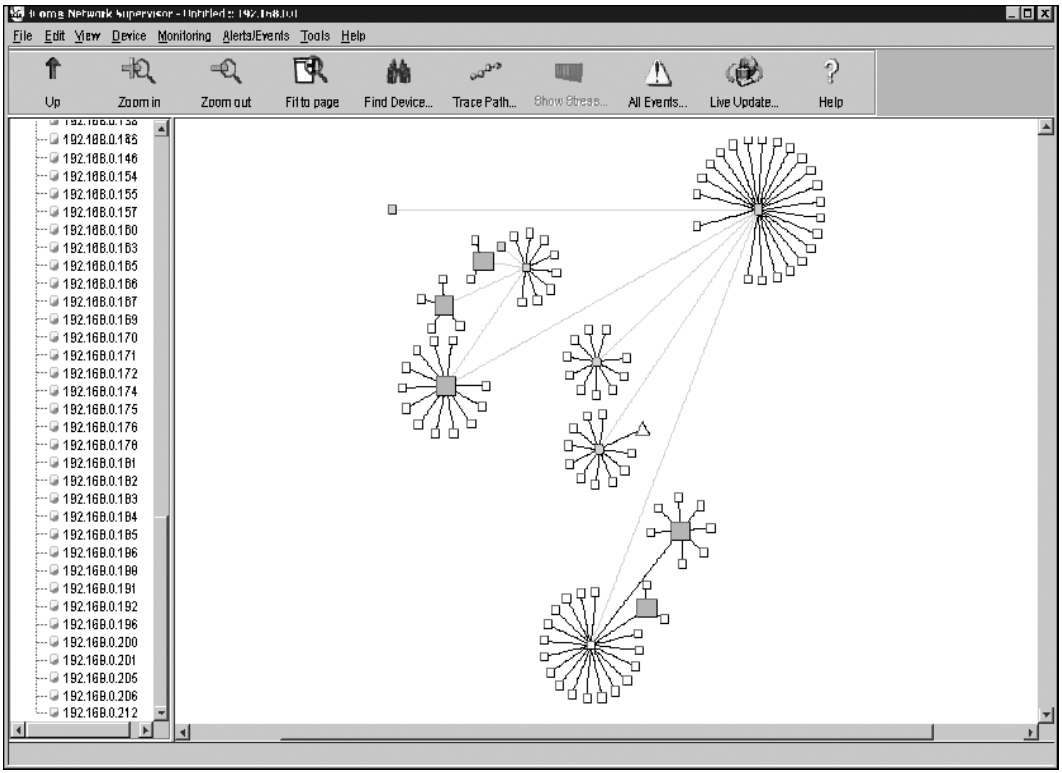


Рис. 3.3. Структура локальной сети небольшого предприятия после некоторого периода неуправляемого развития

Уровни ядра, распределения и доступа

Современная сеть создается на основе трех уровней: *ядра* (core), *распределения* (distribution) и *доступа* (access), как это показано на рис. 3.4. На уровне доступа обеспечивается подключение конечных рабочих станций. На уровне распределения реализуется маршрутизация пакетов и их фильтрация (на основе списков доступа и т. п.). Задача оборудования уровня ядра — максимально быстро передать трафик между оборудованием уровня распределения.

Если рассматривать типовую сеть небольшой организации, занимающей несколько этажей одного здания, то уровень распределения будет соответствовать оборудованию, объединяющему коммутаторы каждого этажа, а уровень ядра — активному оборудованию, размещаемому обычно в главной серверной.

Это классическая схема иерархической структуры, которая на практике часто модифицируется с учетом специфики организации, оборудования и т. д. Так, в зависимости от размеров предприятия, может отсутствовать какой-либо уровень, и структура сети станет двухуровневой. Маршрутизацию данных можно реализовать на уровне ядра, а оборудование уровня распределения будет только пересылать данные внутри сегмента сети. Все зависит от решаемых задач, распределения потоков информации и предъявляемых к информационной системе требований.

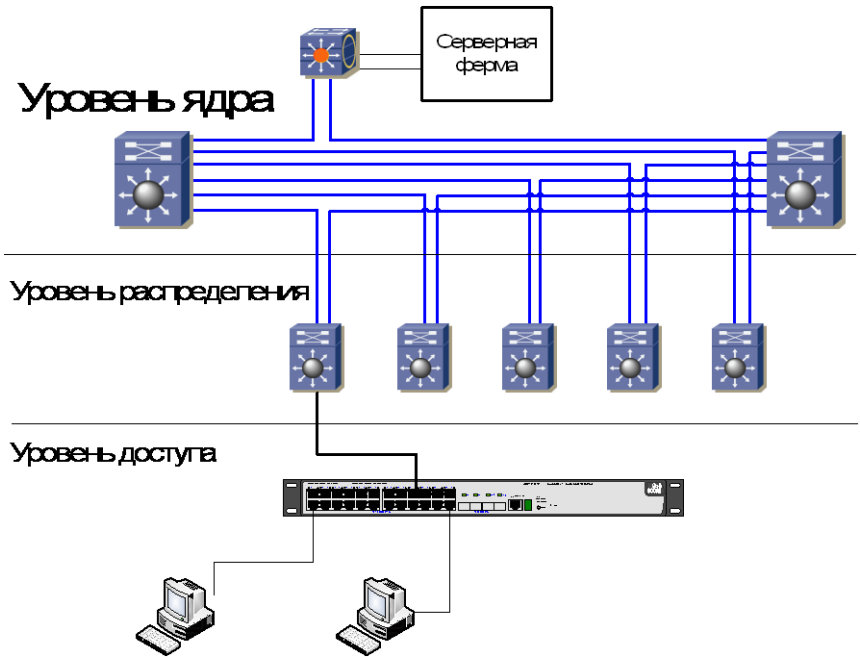


Рис. 3.4. Трехуровневая структура сети

Часто в схеме сети выделяют *серверную ферму*. Принципиально серверная ферма представляет собой обычный узел распределения, но реализованный на быстродействующем оборудовании и, как правило, со 100%-м резервированным решением. В малых организациях часто практикуется подключение серверов непосредственно к ядру сети передачи данных.

На практике структуру сети администраторам обычно приходится "примерять" на уже существующие линии связи, ограничиваться возможностями по созданию новых соединений (учитывая, по какой трассе можно проложить линию связи собственными силами) и т. д. Поэтому одной из основных рекомендаций при изменении топологии сети должна быть минимизация количества коммутаторов между любыми двумя точками подключения компьютеров.

Топология каналов сети распределенного предприятия

Если при построении сети внутри здания обычно удается придерживаться иерархии связей "здание — этаж — рабочее место", то в случае размещения предприятия в нескольких зданиях структура сети в значительной степени определяется возможностями прокладки внешних кабелей. Наличие кабельной канализации, воздушных линий связи, кабельных эстакад и т. п. достаточно жестко определяют возможные направления каналов передачи данных.

Поскольку стоимость прокладки кабелей между зданиями достаточно высока, обычно прокладывается лишь минимум связей, которые обеспечат отказоустойчи-

вость сетевой структуры. При этом весьма часто используется *кольцевая* структура, иногда снабжаемая "перемычкой" для снижения числа промежуточных узлов между двумя узлами распределения. На рис. 3.5 приведен вариант подобной структуры сети крупного распределенного предприятия.

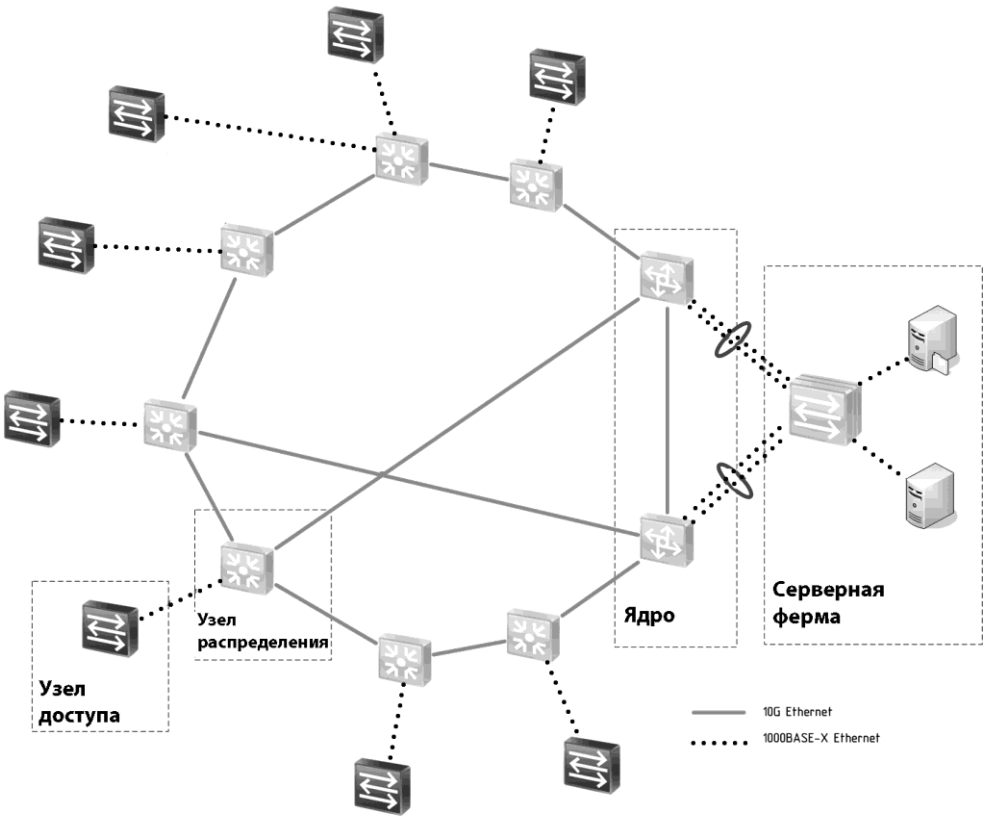


Рис. 3.5. Вариант структурной схемы связей территориально распределенной информационной системы

Сеть управления

Для сохранения управляемости оборудованием сети рекомендуется строить отдельную сеть для подключения интерфейсов управления. Имеется в виду, что эта сеть должна быть собрана на физически других линиях связи, чем те, которые используются для передачи данных. Например, это будут отдельные концентраторы[1],

[1] Именно концентраторы, причем можно использовать оборудование, предназначенное для 10-мегабитных сетей. Поскольку это самые надежные устройства, а сеть управления не требует высокой скорости передачи данных.

к которым подключены активные устройства; связи между различными площадками можно выполнить при помощи модемов по телефонным линиям связи и т. п.

Главное, чтобы эта сеть продолжала функционировать в случае повреждения каналов передачи данных, чтобы администратор не потерял доступ к устройствам и имел возможность контролировать структуру.

Примечание

Если транспортная сеть полностью резервирована, то можно не создавать выделенную сеть управления. В любом случае, высокая доступность интерфейсов управления должна быть рассмотрена специально.

Документирование структуры каналов связи

Традиционной проблемой большинства организаций является документирование своей кабельной подсистемы. Специализированные программные продукты, позволяющие поддерживать схемы сети с учетом вносимых в нее изменений в актуальном состоянии, стоят весьма дорого, а исходная документация быстро становится неактуальной после нескольких перемещений сотрудников и прокладки дополнительных каналов связи.

Существует много программ, которые позволяют автоматически воспроизвести структуру сети. Топология, изображенная на рис. 3.3, выполнена с помощью одной из таких программ. С помощью данных, собираемых программой, легко находить точки подключения компьютеров к коммутаторам, обнаруживать те или иные неисправности конкретной конфигурации.

Для сбора первичных данных подобные программы используют протокол SNMP. В случае эксплуатации неуправляемых устройств администратор должен составлять такие диаграммы вручную.

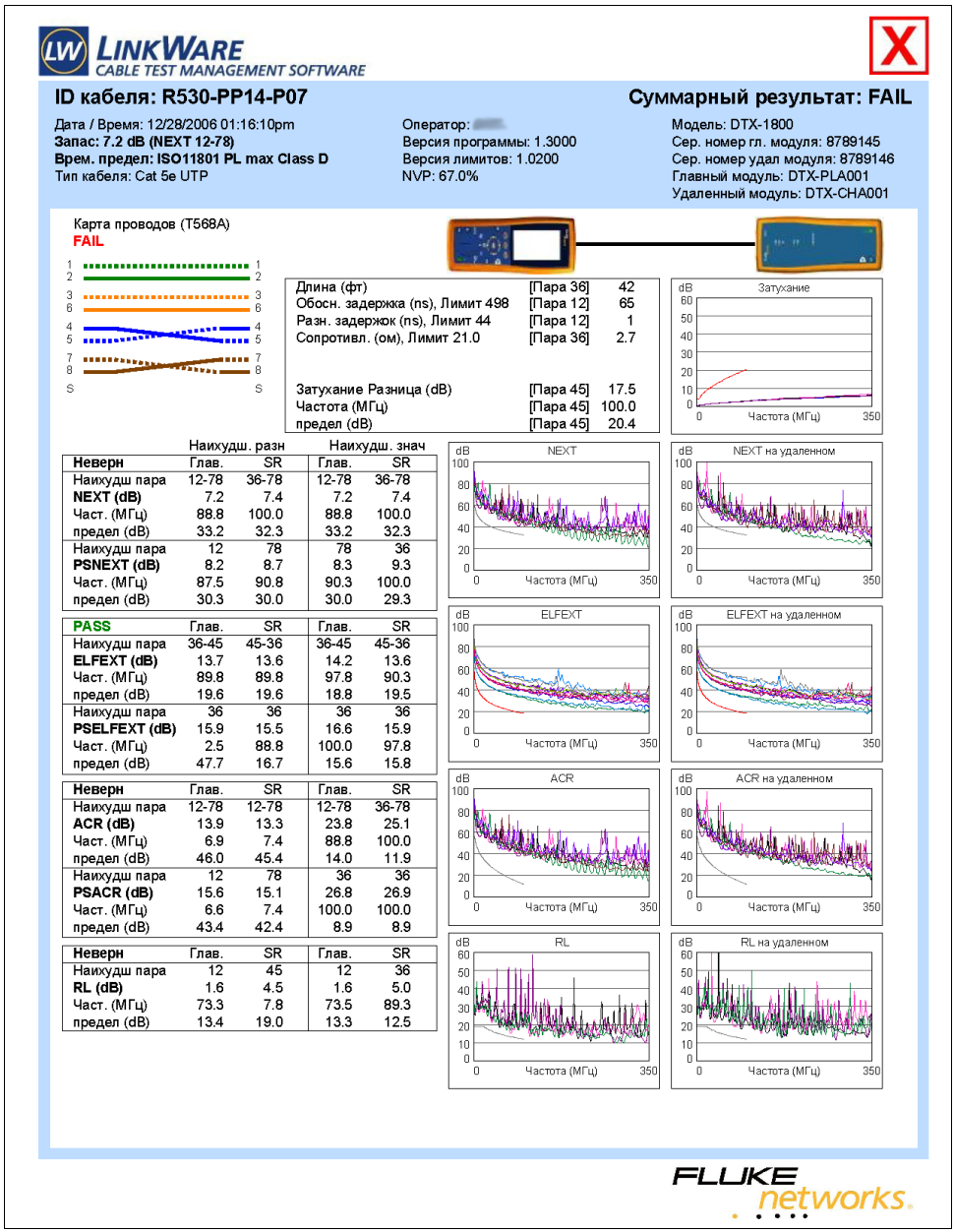
Качество сетей связи предприятия

Администратор должен быть уверен, что эксплуатируемые линии связи не создают никаких проблем в работе информационной системы.

Тестирование кабельной системы

Качество информационной системы начинается с качества комплектующих, использованных при построении сети. Несмотря на доступность инструментов для расшивки кабеля и монтажа элементов СКС, желательно привлечь к работам фирмы, которые имеют опыт работы на этом рынке и обладают необходимым уровнем компетенции. Например, даже такая мелочь, как лишний перехлест пары проводников при расшивании гигабитного соединения, может привести к тому, что линия связи по своим параметрам не будет соответствовать заданной категории.

Все линии связи должны быть протестированы сертифицированным оборудованием. Это позволит не только выявить ошибки, но и обнаружить ухудшение парамет-



	Наихудш. разн		Наихудш. знач	
Неверн	Глав.	SR	Глав.	SR
Наихудш пара	12-78	36-78	12-78	36-78
NEXT (dB)	7.2	7.4	7.2	7.4
Част. (МГц)	88.8	100.0	88.8	100.0
предел (dB)	33.2	32.3	33.2	32.3
Наихудш пара	12	78	78	36
PSNEXT (dB)	8.2	8.7	8.3	9.3
Част. (МГц)	87.5	90.8	90.3	100.0
предел (dB)	30.3	30.0	30.0	29.3

PASS	Глав.	SR	Глав.	SR
Наихудш пара	36-45	45-36	36-45	45-36
ELFEXT (dB)	13.7	13.6	14.2	13.6
Част. (МГц)	89.8	89.8	97.8	90.3
предел (dB)	19.6	19.6	18.8	19.5
Наихудш пара	36	36	36	36
PSELFEXT (dB)	15.9	15.5	16.6	15.9
Част. (МГц)	2.5	88.8	100.0	97.8
предел (dB)	47.7	16.7	15.6	15.8

Неверн	Глав.	SR	Глав.	SR
Наихудш пара	12-78	12-78	12-78	36-78
ACR (dB)	13.9	13.3	23.8	25.1
Част. (МГц)	6.9	7.4	88.8	100.0
предел (dB)	46.0	45.4	14.0	11.9
Наихудш пара	12	78	36	36
PSACR (dB)	15.6	15.1	26.8	26.9
Част. (МГц)	6.6	7.4	100.0	100.0
предел (dB)	43.4	42.4	8.9	8.9

Неверн	Глав.	SR	Глав.	SR
Наихудш пара	12	45	12	36
RL (dB)	1.6	4.5	1.6	5.0
Част. (МГц)	73.3	7.8	73.5	89.3
предел (dB)	13.4	19.0	13.3	12.5

Рис. 3.6. Протокол испытания качества линии связи специализированным оборудованием

ров линии, которое может привести к отказам только после некоторого периода эксплуатации. Наличие подобных тестов позволит быть уверенным в качестве построенной СКС, в том, что линия будет надежно работать как на момент создания, так и через несколько лет эксплуатации.

На рис. 3.6 в качестве примера представлен результат тестирования одной линии связи на соответствие требованиям категории 5e. Линия не прошла тест, поскольку

в ней было перепутано подключение проводников. Подобные тесты должны быть проведены для всей кабельной системы, а их результаты — храниться в архиве администратора.

Тестирование качества передачи данных

На действующей инфраструктуре о качестве передачи информации по каналам связи можно судить по показаниям счетчиков коммутационного оборудования. Понятно, что такие показания можно получить только на управляемых устройствах, простейшие — так называемые, *офисные* модели — такой функциональностью не обладают. Правда, они и дешевле...

О том, по каким показаниям счетчиков и как судить о качестве передаче данных, мы поговорим в *главе 11*. Сейчас же рассмотрим возможности повышения качества обслуживания с использованием возможностей регулирования трафика.

Приоритезация трафика

Построить сеть, которая гарантированно пропускала бы весь трафик в случае активной сетевой работы всех пользователей, практически нереально. Параметры пропускной способности рассчитываются по усредненным показателям с учетом предположений о характере использования сети (типы задач, наличие голосового и мультимедийного трафика и т. п.).

В большинстве сетей малых и средних предприятий пропускная способность сети используется менее чем на 10%, и ограничения в передаче данных из-за исчерпания полосы пропускания кажутся маловероятными. Но все каналы связи имеют свои пределы. С увеличением интенсивности использования сетевых приложений, повсеместном внедрении мультимедийных решений вероятность кратковременной перегрузки сети будет только повышаться.

Сама сеть *не гарантирует* доставку информации. Если пакет с данными не может быть передан, он просто теряется. Большинство приложений корректно обработает факты потери части передаваемых данных и запросит их повторно. Однако есть задачи, для которых любая потеря пакетов недопустима. Например, при передаче голоса подобная ситуация приведет к возникновению "провалов", "бульканья" речи. В этом случае можно решить проблему, если предоставить передаче голоса более привилегированные условия, чем, например, протоколу пересылки почтовых сообщений. Ничего не случится, если почтовое сообщение будет доставлено чуть позже; это даже не будет замечено пользователями.

Задача приоритезации трафика решается путем присвоения передаваемым по сети пакетам определенного *класса* обслуживания и обеспечения для каждого класса соответствующего *качества* обслуживания. Часто для простоты все эти технологии называют QoS — Quality of Service. Обращаю внимание читателя, что настраивать QoS имеет смысл только при возникновении подобных ситуаций. В случае достаточности полосы пропускания никаких дополнительных действий предпринимать не нужно. В общем случае данная задача является весьма сложной и решается поразному для локальной и магистральных сетей. Подумайте хотя бы над теми пара-

метрами, которые нужно обеспечить для качественной передачи данных. Это может быть и гарантия полосы пропускания, и отсутствие задержек пакетов более определенной величины, и максимально допустимый процент потери пакетов. Разные задачи будут определять отличающиеся требования. Далее мы опишем основные подходы, используемые для решения задачи приоритезации трафика.

Варианты приоритезации: QoS, ToS, DiffServ

Существует несколько возможностей определения необходимого качества обслуживания. На уровне кадров Ethernet (второй уровень модели OSI) существует возможность включения поля TAG, значение которого определяет требуемый уровень обслуживания. Поскольку протокол IP работает не только в сетях Ethernet, но и в сетях WAN, которые не обязательно основаны на кадре Ethernet, то и в IP-пакете было предусмотрено специальное поле ToS, принимающее данные о требуемом уровне обслуживания. Впоследствии был разработан новый протокол Differentiated Services (DS или *DiffServ*), который и используется в настоящее время для маркировки IP-пакетов в соответствии с уровнем обслуживания.

Коммутаторы, используемые на малых и средних предприятиях, а также коммутаторы уровня доступа в больших сетях обычно используют для приоритезации только поле QoS Ethernet-кадра. Коммутаторы уровня предприятия могут приоритезировать трафик с учетом всех действующих стандартов. Так, на рис. 3.7 показано

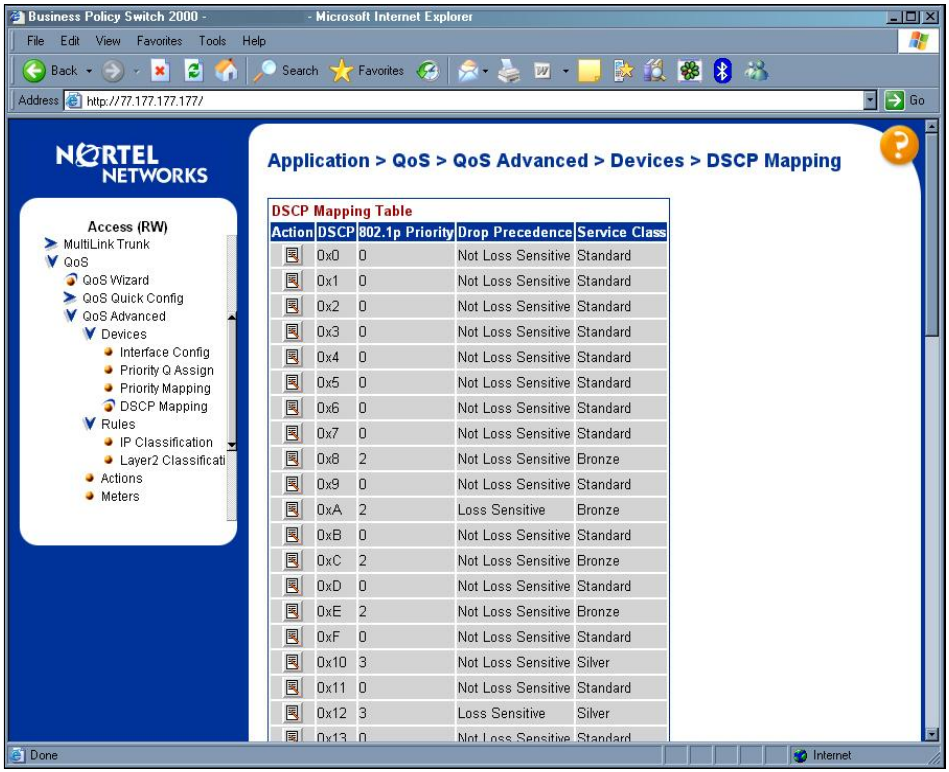


Рис. 3.7. Скриншот окна управления коммутатора фирмы Nortel

окно настройки параметров качества обслуживания коммутатора фирмы Nortel, в котором можно "подстроить" метки DSCP к значениям приоритетов 802.1p.

Пакеты данных в соответствии с протоколом 802.1p (точнее, само поле определено в протоколе 802.1q, но назначение битов приоритета описано в протоколе 802.1p) имеют специальное поле приоритета из трех битов. Таким образом, данные в локальной сети могут быть промаркированы одним из восьми *классов* обслуживания. Приоритет пакету должна "ставить" программа, создающая данный трафик, но его значение может быть изменено по пути следования (например, на некоторых моделях коммутаторов). Существуют различные программы, позволяющие менять параметры качества обслуживания и назначать данным желаемые классы (приоритеты). Так, в состав пакета Resource Kit для сервера Windows входит программа Traffic Control, позволяющая назначать классы обслуживания на основе собственных фильтров и переопределять параметры качества обслуживания.

В протоколе DiffServ на описание приоритета выделено 6 бит, что позволяет иметь до 64 возможных классификаций приоритезации. Реально используется существенно меньше уровней сервиса. В табл. 3.3 приведены основные применяемые на практике уровни сервиса DiffServ.

Таблица 3.3. *Часто используемые на практике уровни сервиса DiffServ*

Класс	**PHB (Per Hop Behavior)**	**Описание**	**Область применения**
Default	—	—	—
Class-Selector	—	Используется для обратной совместимости с ToS	—
Expedited Forwarding (EF)	EF	Используется при необходимости минимизации варьирующихся задержек и потери пакетов. Предполагает гарантированную полосу пропускания	Передача голоса
Assured Forwarding (AF)	AF11 High Priority Low Drop Precedence	Рекомендован для особо важных приложений	Сетевые службы, программы управления производством (SAP и т. п.)
	AF21 Medium Priority Low Drop Precedence		Службы обеспечения безопасности
	AF22 Medium Priority Medium Drop Precedence		Сообщения электронной почты
	AF22 Medium Priority High Drop Precedence		Фоновая репликация данных
	AF31 Low Priority Low Drop Precedence		HTTP

Классификация, маркировка, приоритезация

Для настройки приоритезации трафика необходимо выполнить несколько шагов. Во-первых, следует создать правила, по которым можно выделить часть трафика, требующую особых условий при передаче. Этот процесс называется *классификацией*. Например, вы хотите предоставить льготные условия для передачи данных какому-то приложению. Если оно работает по какому-либо протоколу, не используемому другими приложениями, то достаточно создать правило классификации на основе протокола. Можно определить правило, которое будет выделять трафик, отправленный устройством А устройству Б с 8 часов утра до 12 часов дня каждый понедельник (возможности классификации зависят, в первую очередь, от используемого оборудования) и т. д.

После того как данные классифицированы, передаваемый пакет следует *маркировать*. Поскольку по стандарту Ethernet реально существует восемь приоритетов, то вам необходимо составить правила, которые поставят в соответствие каждый описанный — *маркированный* — тип трафика одному из существующих уровней. Часто в целях удешевления модели коммутаторы, предназначенные для использования на уровне доступа, имеют меньше 8 очередей, используемых при приоритезации трафика. Соответственно сузятся ваши возможности по детализации процесса приоритезации. Промаркированный пакет будет готов к применению правил приоритезации.

Классификацию с последующей маркировкой пакетов можно проводить на любом коммутаторе, поддерживающем управление приоритезацией. В том числе допускается и выполнение *перемаркировки* трафика, т. е. повторного назначения приоритетов на основании других правил. Однако более рационален иной подход: маркировку трафика следует выполнять там, где такой трафик *создается*, иными словами — на коммутаторах уровня доступа. Коммутаторы уровня распределения и ядра используют уже назначенную маркировку и на основании ее выполняют приоритезацию трафика по заданным на них правилам. Это оптимизирует нагрузку на активное оборудование сети, разгружая центральные коммутаторы от дополнительной работы по анализу трафика.

После того как выполнены классификация и маркировка, необходимо применить *правила приоритезации*. Стандарт предусматривает восемь уровней приоритета, но не описывает правила, которые могут быть применены к каждому из них. В этом отношении имеются только общие рекомендации, поэтому вам придется сформировать правила приоритезации самостоятельно. Например, вы можете создать правило, которое будет блокировать весь трафик, соответствующий определенному классу.

Реально процессы обеспечения различного уровня качества передачи реализуются путем направления пакетов на различные *очереди* в коммутаторе.

Как работает приоритезация: очереди

Процесс приоритезированной передачи пакетов реализуется следующим образом. На коммутаторе создаются буферы для временного хранения пакетов на каждом порту. Их принято называть *очередью*.

Количество буферов — это количество очередей, которые поддерживает коммутатор. В идеале количество очередей должно быть равно количеству уровней приоритезации, а именно восьми. Меньшее их количество не позволит использовать все возможности протокола, большее — не имеет смысла за пределами данного коммутатора, хотя и позволяет более точно приоритезировать передачу трафика в конкретном коммутаторе. Размеры буфера обычно не одинаковы для разных очередей: чем выше приоритет очереди, тем больше памяти отводится для хранения ее пакетов. Качество коммутатора определяется в том числе и объемом памяти, выделяемой для очередей: более дорогие модели имеют большие размеры буферов. Обычно расширенными настройками коммутатора можно распределять выделенную память между очередями по собственным критериям, однако на практике эти параметры по умолчанию обычно не изменяют.

Если канал связи свободен, то пакет данных сразу же передается по назначению. Если такой возможности нет, то коммутатор помещает пакет на временное хранение в соответствующую очередь. Как только линия связи освободится, коммутатор начнет передачу пакетов из очередей. Существует несколько алгоритмов выбора данных из очередей для последующей передачи по сети (администратор может выбирать алгоритмы и настраивать их параметры). Наиболее популярны два алгоритма: Strict Priority Queuing (SPQ) и Weighted Round Robin (WRR).

При использовании алгоритма SPQ сначала передаются пакеты из очереди, имеющей максимальный приоритет, и только когда она полностью освободится, коммутатор начнет передачу данных из следующей по приоритету. Данный алгоритм обеспечивает практически гарантированную доставку пакетов максимального приоритета, однако при существенном объеме высокоприоритетной информации другие пакеты могут теряться (коммутатор вообще не сможет приступить к обслуживанию очереди с низким приоритетом).

Алгоритм WRR использует специальные взвешенные процедуры для отправки пакетов. Каждой очереди выделяется определенный лимит для передачи: чем выше приоритет очереди, тем больше пакетов из нее передается, но в любом случае будут опрошены все очереди в порядке снижения приоритета: после истечения выделенного периода обслуживания одной очереди коммутатор перейдет к обработке пакетов очереди, следующей по приоритету. Данный алгоритм обеспечивает передачу *всех* типов пакетов.

Иногда используют смешанные алгоритмы. Например, самые критичные очереди (обычно имеющие приоритет 1 или 2) обслуживают на основе алгоритма SPQ, а для всех остальных применяют вариант WRR.

Ограничение полосы пропускания трафика (Traffic shaping)

Коммутаторы, на которых реализована возможность приоритезации трафика, часто имеют возможность ограничивать полосу пропускания для того или иного типа данных. Например, можно ограничить выделяемую полосу для загрузки данных по протоколу FTP или для протоколов видеопросмотра в рабочее время значением,

обеспечивающим достаточный свободный объем для основных производственных приложений.

Данная настройка выполняется в соответствии с правилами конфигурирования конкретной модели коммутатора.

Беспроводные сети

Выполнение полного цикла работ по проектированию и монтажу структурированной кабельной сети (СКС) является весьма затратной операцией. Стоимость проектирования, стоимость самих материалов, оплата монтажных работ — эти расходы могут составить весьма значительную сумму. Даже в небольших организациях для создания сети необходимо приобрести несколько сотен метров кабеля. Для средних и крупных организаций счет уже ведется на тонны "меди". Кроме того, достаточно велики стоимости розеток, каналов и других элементов. При этом в силу большой трудоемкости в проекты обычно закладываются необходимые резервы, рабочие места, которые только могут быть созданы в перспективе, и т. п.

Для небольших офисов существует решение, которое уже сейчас успешно конкурирует с существующими кабельными сетями — *беспроводные линии связи*.

Для создания такой сети каждый компьютер должен быть оборудован беспроводным адаптером, а в офисе необходимо установить специальные устройства — так называемые *точки доступа*, выполняющие, кроме того, роль хабов сети.

В настоящее время большая часть ноутбуков комплектуется устройствами доступа к беспроводной сети, а стоимость адаптера, устанавливаемого в "обычный" компьютер, сравнима со стоимостью стандартной сетевой платы. Если учесть, что стоимость точки доступа аналогична стоимости небольшого коммутатора, то переход на беспроводную сеть может быть экономически оправдан для многих организаций, а в некоторых случаях (например, аренда помещения без права выполнения монтажно-строительных работ, наличие мобильных сотрудников, к примеру, официанты могут использовать мобильные компьютеры для приема заказов, врачи иметь с собой ноутбуки при проведении обхода и т. д.) использование беспроводной сети может стать и единственным приемлемым решением.

Стандарты беспроводной сети

В настоящее время устройства для беспроводной сети выпускаются на основе нескольких стандартов, некоторые параметры которых приведены в табл. 3.4.

Таблица 3.4. *Некоторые параметры стандартов беспроводной сети*

Параметр	Стандарт		
	802.11a	802.11b	802.11g
Диапазон частот, ГГц	5	2,4	2,4
Число каналов	8	3	3

Таблица 3.4 *(окончание)*

Параметр	Стандарт		
	802.11a	**802.11b**	**802.11g**
Максимальная скорость передачи, Мбит/с	54	11	54 (108 с аппаратным сжатием)
Совместимость	—	802.11.g	802.11.b

На практике лучше выбрать один стандарт беспроводного оборудования, а при необходимости использования совместимых режимов — проверять наличие сертификации соответствующего решения.

Проектирование беспроводной сети предприятия

С помощью беспроводных технологий можно соединять компьютеры (по принципу "точка — точка"), отдельные сегменты сетей и т. п. Наиболее часто в локальных сетях устройства беспроводного доступа ставятся в качестве *точки доступа (Wireless Access Point, AP)*. В этом случае персональные компьютеры подключаются к точкам доступа, через которые осуществляют доступ как в локальную сеть организации, так и в Интернет, при этом точка доступа выступает аналогом концентратора локальной сети.

После выбора стандарта беспроводной сети следует определить *зоны покрытия*. Одно стандартное устройство AP "покрывает" зону радиусом около 75—100 м. Хотя существуют различные оценки для расчетов диаграмм зон покрытия, эти величины существенно зависят от конкретных условий: планировки помещений, материала стен и т. п. Лучшим способом является проведение тестовых измерений на местности с использованием соответствующего оборудования. На рис. 3.8 приведен пример такой программы, которая анализирует замеры параметров радиочастотного сигнала в реальных условиях и формирует карту зоны покрытия (с привязкой к карте с помощью глобальных систем позиционирования).

Как правило, это весьма дорогостоящая операция, поэтому часто ограничиваются тестированием уровня сигнала встроенными средствами беспроводного адаптера (штатными средствами Windows). При этом следует учесть, что существующее на предприятии оборудование при своей работе может создать помехи беспроводной сети, и предусмотреть необходимые технологические резервы. И даже при отсутствии постоянных помех используемые в беспроводной сети программы должны быть устойчивы к кратковременному исчезновению связи. Например, при работе в 1С могут наблюдаться случаи аварийного завершения программы из-за кратковременной потери связи с сервером.

На количество устанавливаемых точек доступа будут влиять также требования к скорости передачи данных. Указанные в табл. 3.4 значения скорости передачи данных являются максимальными, а полоса пропускания *делится* между всеми устройствами, которые подключены к данному каналу. Также следует учитывать, что

скорость передачи данных снижается на максимальных расстояниях при слабом уровне сигнала. Установка дополнительных точек доступа позволит распределить между ними пользователей и повысить скорость обмена данными. В связи с этим обычно рекомендуется устанавливать одну точку доступа приблизительно на 10 клиентов, хотя технический предел подключений беспроводных устройств, как правило, составляет не одну сотню систем.

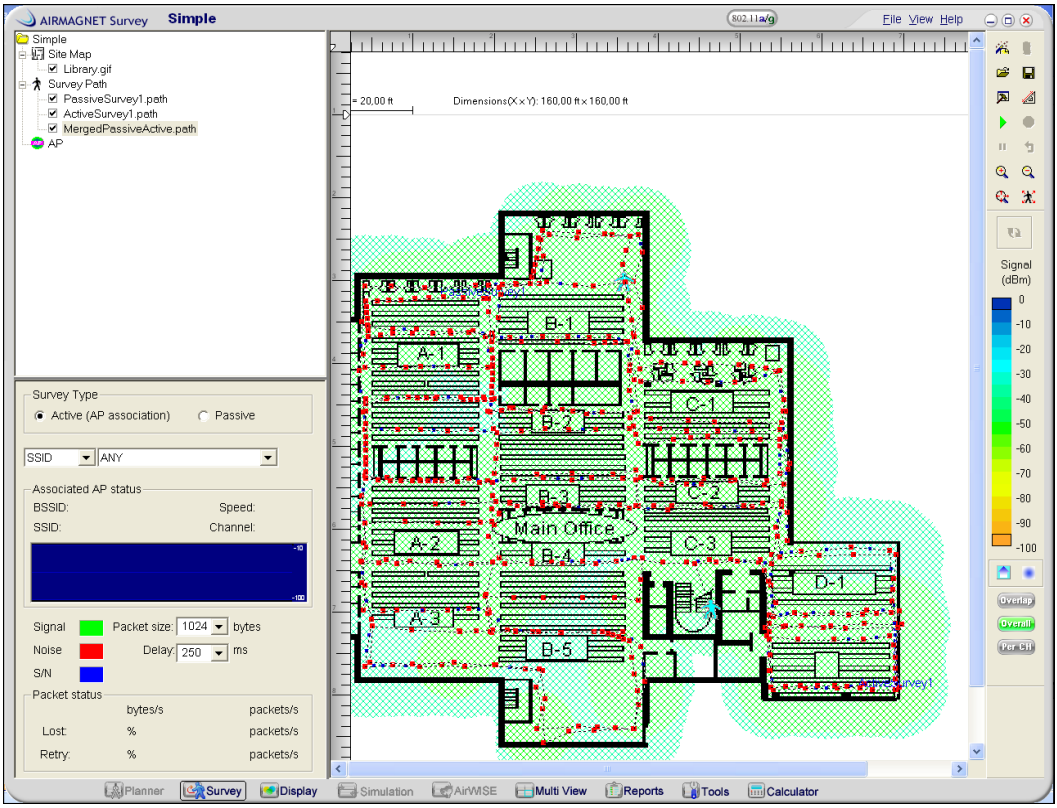


Рис. 3.8. Проектирование установки беспроводных точек доступа.
Для обеспечения работы в любой точке здания в беспроводной сети необходимо учесть многие факторы. Специализированное программное обеспечение позволяет построить возможные зоны покрытия на основе замеров и анализа параметров радиосигнала.
На рисунке представлен пример от AirMagnet, Inc.

Беспроводные решения могут помочь соединить, например, два здания. Для этого созданы специализированные беспроводные *мосты* и направленные антенны.

Примечание

Если режим работы системы предполагает мобильность устройств (постоянное перемещение их во время работы с системой с переключением между различными точками доступа), то для исключения прерывания сессий необходимо использовать специальное программное обеспечение.

Безопасность беспроводной сети

Точку доступа можно сравнить с концентратором локальной сети, который поставлен в общедоступное помещение. Любой может "подключиться" к данному сегменту и прослушивать передаваемую информацию. Поэтому правильной настройке подключения клиентов необходимо уделить особое внимание.

Шифрование трафика беспроводной сети

Для защиты передаваемой по беспроводной сети информации все данные *шифруются*. Исторически первый стандарт безопасности для Wi-Fi — протокол WEP (Wired Equivalent Privacy или Wireless Encryption Protocol, протокол шифрования в беспроводной связи) — предусматривает шифрование с помощью статичного ключа, известного как пользователю, так и администратору точки доступа. К сожалению, в практической реализации этого документа были найдены ошибки, которые позволяют за короткое время (порядка нескольких часов) вычислить данный ключ. Поэтому протоколы WEP, даже с увеличенной длиной ключа, не могут считаться безопасными при создании корпоративной беспроводной сети.

> ***Примечание***
>
> Если примененные при создании беспроводной сети устройства не поддерживают новых протоколов безопасности, то администраторы могут защитить передаваемую информацию путем создания виртуальных частных сетей (VPN) поверх беспроводных каналов связи.

Новый стандарт безопасности WPA (Wi-Fi Protected Access) предусматривает как использование динамических (изменяемых) ключей шифрования, так и аутентификацию пользователя при входе в беспроводную сеть. Проектируя беспроводной сегмент сети, следует приобретать только устройства, удовлетворяющие данному стандарту.

Аутентификация пользователей и устройств Wi-Fi

В беспроводных сетях применяются два способа проверки пользователей и устройств при их подключении. Первый — это проверка MAC-адресов устройств, подключаемых к данной точке доступа. В этом случае администратор вручную должен настроить для *каждой* точки доступа соответствующий список MAC-адресов устройств, которым разрешено беспроводное подключение.

Способ не может считаться безопасным, поскольку MAC-адреса легко определяются при прослушивании беспроводного сегмента, а "подмена" MAC-адреса не представляет никакой сложности даже для не совсем опытного пользователя.

Второй способ основан на протоколе двухточечного соединения с надежной аутентификацией — EAP (Extensible Authentication Protocol). Для предприятий следует рекомендовать аутентификацию на основе стандарта 802.1x с использованием сервера RADIUS.

Наиболее безопасен способ, при котором для аутентификации вместо паролей используются сертификаты. Однако он требует наличия на предприятии настроенной

системы *PKI* (Public Key Infrastructure, инфраструктура открытых ключей) *(см. главу 9)*. Настройка беспроводных устройств для аутентификации с использованием сертификатов по протоколу 802.1x практически идентична примеру, описанному в *главе 9* в *разд. "Настройка протокола 802.1x"*. Единственное отличие заключается в выборе шаблона политики, используемой на сервере RADIUS (рис. 3.9).

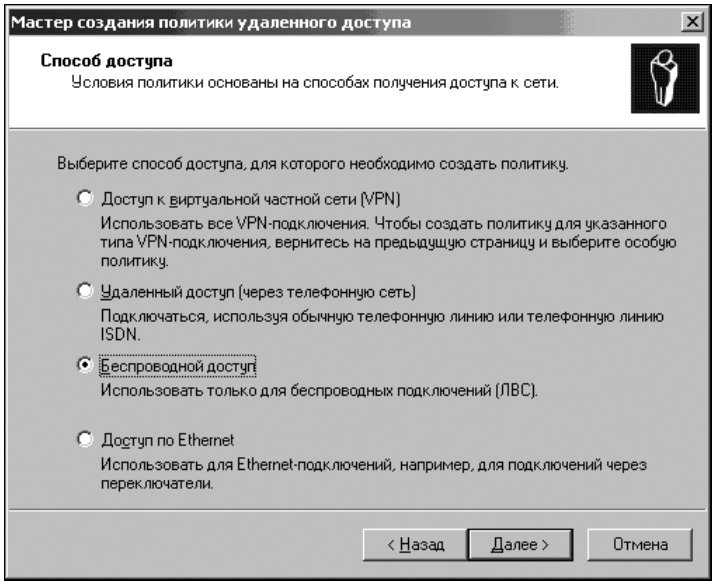


Рис. 3.9. Создание политики RADIUS-сервера для беспроводной сети. При создании политики удаленного доступа для сервера RADIUS должен быть выбран шаблон **Беспроводной доступ**

Примечание

При такой настройке клиенты, ранее не работавшие в составе домена, не могут быть подключены к нему по беспроводной сети, поскольку на них не установлены необходимые сертификаты. Вам следует либо заранее осуществить подсоединение компьютера к домену с помощью проводной сети, либо настроить особую политику для временного подключения гостевых записей (введя в этом случае временные ограничения сессии в политике подключения сервера RADIUS). При краткосрочном подключении к сети клиент получит сертификат и в дальнейшем будет работать в соответствии с постоянной политикой беспроводного доступа.

Безопасность клиента

При подключении компьютера к публичной беспроводной сети следует принимать те же меры безопасности, что и при работе в Интернете. Прежде всего следует обязательно защитить подключение брандмауэром (например, встроенный брандмауэр Windows — опция **Защитить подключение к Интернету** в свойствах беспроводного подключения). Этим вы блокируете доступ к данным, хранимым на локальном компьютере, из внешней сети.

Обратите внимание, что в целях безопасности необходимо *в обязательном порядке* запретить допущенные разработчиком по умолчанию разрешения доступа к компьютеру извне (осуществляется через настройку брандмауэра отключением исключений, рис. 3.10).

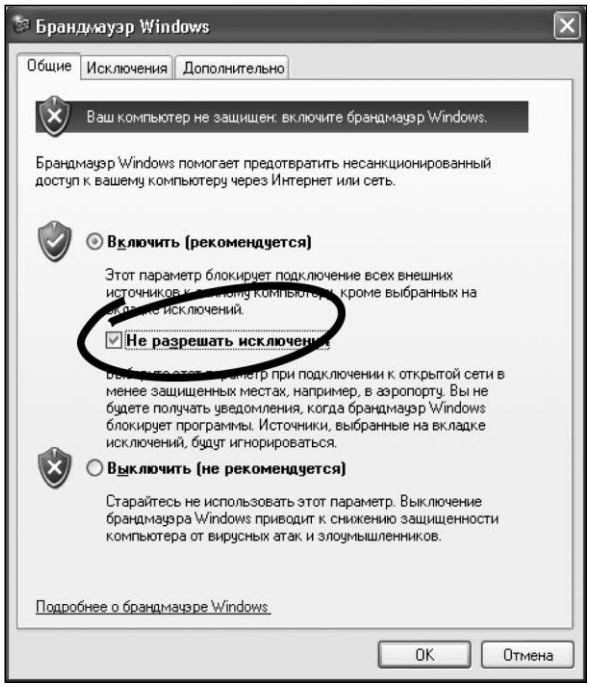


Рис. 3.10. Настройка брандмауэра Windows.
В межсетевом экране Windows XP имеются так называемые исключения, предназначенные для работы в локальной доверенной сети, которые позволяют подключиться к защищенному компьютеру извне. Не нужно забывать, что в публичных сетях допущенные по умолчанию исключения должны быть *запрещены* (выделено на рисунке)

Настройка транспортных протоколов

Протоколы

Сетевой протокол — это набор программно реализованных правил общения компьютеров, подключенных к сети. Практически это "язык", на котором компьютеры разговаривают друг с другом. В настоящее время стандартом стало использование *только* протокола TCP/IP. В предыдущих версиях Windows по умолчанию устанавливалось несколько протоколов, обычно это NetBEUI, NWLink IPX/SPX, TCP/IP.

- **NetBEUI.**

  Компактный и эффективный протокол для взаимодействия в малых сетях (до 200 компьютеров). Используется в самых разнообразных системах: Microsoft LAN Manager, Windows 3.1/3.11 for Workgroups/95/98/NT 4.0, IBM PCLAN, LAN

Server и т. п. В Windows 2000 и старше применяется новая спецификация этого протокола, которая получила название *NetBIOS Frame Protocol (NBFP)*. NetBEUI (NBFP) не требует никаких дополнительных настроек. Если нужно быстро создать сеть и вы не чувствуете себя уверенными в понимании дополнительных настроек, которых, например, требует протокол TCP/IP, то включите протокол NBFP. Вы получите простую и весьма быстро функционирующую локальную сеть.

- **NWLink IPX/SPX.**

  Если в сети есть серверы Novell NetWare (в последних версиях Netware по умолчанию используется протокол TCP/IP), то этот протокол необходим для организации с ними связи. В противном случае данный протокол следует исключить из числа используемых в системе.

- **TCP/IP.**

  Основной рекомендуемый протокол как для больших сетей предприятий и малых офисов, так и для соединения домашних компьютеров в частную сеть. В отличие от других протоколов требует ряда предварительных настроек.

> ***Примечание***
>
> Не следует использовать в сети больше служб и протоколов, чем требуется для нормальной работы в конкретной ситуации. Во-первых, при этом будут непроизводительно использоваться ресурсы компьютера. Во-вторых, любая дополнительная служба и неиспользуемый протокол — это еще один "вход" в систему, который надо защищать. Поэтому проще не предоставлять дополнительных возможностей хакерам, чем постоянно следить за обнаруживаемыми в этих службах уязвимостями, устанавливать необходимые обновления и т. п.

Модель OSI

С целью систематизации часто используется *модель OSI (Open Systems Interconnection model, модель взаимодействия открытых систем)*, условно разбивающая сетевое взаимодействие на семь уровней (табл. 3.5).

Знание уровней OSI обычно требуется при сдаче тех или иных сертификационных экзаменов, но на практике такое деление потеряло свое значение. Если первые три уровня еще можно достаточно хорошо вычленить при анализе того или иного сетевого проекта, то классифицировать функциональность оборудования по остальным уровням достаточно сложно. В маркетинговых целях часто указывают в описаниях коммутаторов, что они работают, например, на уровне 4 или 7. На практике это означает только, что при реализации определенного функционала в коммутаторах осуществляется анализ пакета данных по характеристикам, относящимся к соответствующим уровням. Например, это происходит при операциях маршрутизации группового трафика (коммутатор анализирует пакет на принадлежность той или иной программе), приоритезации пакетов и т. п.

Таблица 3.5. *Модель OSI*

Уровень OSI	Назначение	Примеры	Необходимое сетевое оборудование
Application (7)	Обеспечение служб сетевых приложений	Протоколы SMTP, HTTP, FTP и т. п.	—
Presentation (6)	Службы кодирования и преобразования данных, используемых на уровне приложений	Стандарты кодирования изображений (GIF, JPEG, TIFF и т. п.), аудио и видео (MPEG) и т. п.	—
Session (5)	Обеспечение коммуникаций между приложениями более высокого уровня (согласование, поддержка, завершение сессий)	Session Control Protocol (SPC) Remote Procedure Call Zone Information Protocol (AppleTalk)	—
Transport (4)	Обеспечивает передачу данных от одной точки до другой	TCP (используются соединения) UDP (передача данных без создания соединения)	—
Network (3)	Обеспечивает логическую структуру сети (сетевые адреса)	IP	Маршрутизаторы Маршрутизирующие коммутаторы
Data Link (2)	Обеспечивает передачу данных по тем или иным *физическим* каналам связи	Ethernet Token Ring FDDI Point-to-Point Protocol Frame Relay	Коммутаторы Мосты
Physical (1)	Определяет физические, механические, электрические и другие параметры физических каналов связи (напряжение, частота, максимальные длины участков и т. п.)	LAN категории 3 LAN категории 5 V.35	Концентраторы

Стек протоколов TCP/IP

Когда говорят о TCP/IP, то обычно подразумевают под этим именем множество различных протоколов, использующих в своей основе TCP/IP. Существует большое количество различных стандартов, которые определяют те или иные варианты взаимодействия в сети с использованием протоколов TCP/IP.

Так, есть правила, по которым осуществляется обмен сообщениями между почтовыми серверами, и есть правила, по которым конечные пользователи могут получать в свой ящик письма. Имеются правила для проведения широковещательных видео- и аудиотрансляций, правила для организации телефонных переговоров по Интернету. Существуют правила, которые определяют поведение участников передачи данных в случае возникновения ошибки и т. п.

Логично, что при разработке правил пересылки файла никто не создает новых механизмов пересылки единичного пакета данных и что протокол пересылки файлов основан на более простом протоколе передачи пакетов.

Поэтому принято говорить, что существуют уровни протокола IP, а на каждом уровне — различные варианты специальных протоколов. Весь этот набор протоколов называют *стеком протоколов TCP/IP*.

Протоколы UPD, TCP, ICMP

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

IPv6

Бурное развитие Интернета привело к тому, что параметры, заложенные при создании протоколов IP, стали сдерживать дальнейшее развитие глобальной сети. Так появился протокол *IPv6*.

К основным особенностям IPv6 относятся:

- сохранение неизменными основных действующих принципов построения протокола IP;
- использование более длинных адресов (128-битные);
- применение встроенного 64-битного алгоритма шифрования;
- учет механизма резервирования пропускной способности протокола (ранее проблема решалась введением классов обслуживания);
- наличие больших возможностей дальнейшего расширения функций: строго описана только часть характеристик, остальные допускают дальнейшее развитие.

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 (рассматривается в *главе 5*), 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 организа-

ции, когда вся инфраструктура находится под контролем и управлением, нужно учитывать все нюансы (например, система разрешения имен в DirectAccess построена через сервер корпорации Microsoft).

Параметры TCP/IP-протокола

Здесь и далее мы будем рассматривать характеристики протокола IPv4.

IP-адрес

Каждый компьютер, работающий по протоколу TCP/IP, обязательно имеет *IP-адрес* — 32-битное число, используемое 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 уникальны. Это значит, что каждый компьютер имеет свое сочетание цифр, и в сети не может быть двух компьютеров с одинаковыми адресами. IP-адреса распределяются централизованно. Интернет-провайдеры делают заявки в национальные центры в соответствии со своими потребностями. Полученные провайдерами диапазоны адресов распределяются далее между клиентами. Клиенты сами могут выступать в роли интернет-провайдера и распределять полученные IP-адреса между субклиентами и т. д. При таком способе распределения IP-адресов компьютерная система точно знает "расположение" компьютера, имеющего уникальный IP-адрес; ей достаточно переслать данные в сеть "владельца". Провайдер в свою очередь проанализирует пункт назначения и, зная, кому отдана эта часть адресов, отправит информацию следующему владельцу поддиапазона IP-адресов, пока данные не поступят на компьютер назначения.

Для построения *локальных сетей* организаций выделены специальные диапазоны адресов. Это адреса 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) через Интернет, поэтому в различных локальных сетях компьютеры могут иметь совпадающие адреса из указанных диапазонов. Такие адреса часто называют *серыми* адресами.

Для пересылки информации с таких компьютеров в Интернет и обратно используются 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* и более подробно описана в *главе 5*.

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 может использование *групповых рассылок (IP Multicast Addressing)*.

Для этого компьютеру присваивается еще один IP-адрес из специального диапазона: с 224.0.0.0 по 239.255.255.255[1], причем диапазоны 224.0.0.0—224.0.0.255 и 239.0.0.0—239.255.255.255 не могут быть использованы 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) и т. п. Назначение адресов групповой рассылки производится соответствующим программным обеспечением.

Групповая рассылка поступает *одновременно на все* подключенные устройства. В результате сетевой трафик может быть существенно снижен по сравнению с вариантом передачи таких данных каждому устройству сети независимо.

По умолчанию рассылки передаются на все порты, даже если к ним не подключены устройства, подписавшиеся на эту рассылку. Чтобы исключить такой паразитный трафик, используются специальные возможности коммутаторов — поддержка IGMP snoophing (прослушивание протокола IGMP), PIM DM/PIM SM (PIM-DM — Protocol Independent Multicast Dense Mode и PIM-SM — Protocol Independent Multicast Sparse Mode — протоколы маршрутизации многоадресных сообщений). При включении и настройке этого функционала (поддерживается не всеми моделями оборудования) данные будут передаваться только на нужные порты.

Распределение IP-адресов сети малого офиса

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

Статические адреса закрепляются:

- за шлюзом, для которого обычно используют адрес xxx.xxx.xxx.1, но это традиция, а не правило;
- за серверами DNS, DHCP, WINS;
- за контроллерами домена;
- за серверами сети (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 используют *динамические адреса*. Удобно часть динамических адресов выдавать для локального использования, а часть — для внешних клиентов, "гостей" сети. Это позволит проще настраивать ограничения доступа к внутренним ресурсам сети для сторонних систем.

---

[1] Multicast-адрес присваивается динамически. Это делает соответствующая программа, использующая многоадресную рассылку.

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

Маска адреса

Понятие *подсети* введено, чтобы можно было выделить часть IP-адресов одной организации, часть другой и т. д. 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 к ним применяются специальные правила для вычисления маршрута пересылки из одной сети в другую. Поэтому при использовании протокола TCP/IP важно знать, к какой сети принадлежит получатель информации: к локальной или удаленной.

Маска адреса — 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. При этом 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[1]) может содержать хосты с адресами от 192.168.0.1 до 192.168.0.254. 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 используется при этом в качестве широковещательного).

На практике сети с небольшим возможным числом хостов используются 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 C. Сеть класса C имеет маску адреса 255.255.255.0 и может содержать до 254 хостов. Применение сетей класса C при разбиении на подсети VLAN в условиях предприятия связано с тем, что протоколы автоматической маршрутизации используют именно такие подсети.

При создании подсетей в организации рекомендуется придерживаться следующего правила: подсети, относящиеся к определенному узлу распределения, должны входить в одну сеть. Это упрощает таблицы маршрутизации и экономит ресурсы ком-

[1] 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.

мутаторов. 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.

Эта рекомендация несущественна для сетей малых и средних организаций, поскольку ресурсов современных коммутаторов достаточно для хранения настроек такого объема.

> ***Примечание***
>
> 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.globalstrata.com/services/network/bscnetcalc.asp**.

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 глобальной сети, необходимо знать правила, куда пересылать информацию для внешней сети. Для этого служит такая характеристика IP-протокола, как адрес шлюза.

Шлюз (Gateway, default gateway)

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 для доступа в Интернет используется прокси-сервер, то компьютерам локальной сети адрес шлюза также может не назначаться.

Для индивидуальных пользователей, подключающихся к Интернету, или для небольших предприятий, имеющих единственный канал подключения, в системе должен быть только один адрес шлюза — это 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 используется таблица маршрутизации.

Таблицы маршрутизации

Организация может иметь несколько точек подключения к Интернету (например, в целях резервирования каналов передачи данных или использования более дешевых каналов и т. п.) или содержать в своей структуре несколько IP-сетей. В этом случае, чтобы система "знала", каким путем (через какой шлюз) посылать ту или иную информацию, используются *таблицы маршрутизации* (routing table). В таблицах маршрутизации для каждого шлюза указывают те подсети Интернета, для которых через них 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 в случае его выхода из строя по тем или иным причинам автоматически будет использоваться следующее наиболее "дешевое" подсоединение.

Таблицы маршрутизации имеются на каждом устройстве, использующем протокол IP. Администраторы в основном работают с таблицами маршрутизации коммутирующего оборудования. Настройка таблиц маршрутизации компьютеров имеет смысл только в случае наличия нескольких сетевых адаптеров, подключенных к различным сегментам сети. Если у компьютера есть только 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).

Просмотреть таблицу маршрутизации протокола TCP/IP можно при помощи команды `route print` для Windows или `route` — в Linux. С помощью команды `route` можно также добавить новый статический маршрут (`route add`) или постоянный маршрут — `route add -p` (маршрут сохраняется в настройках после перезагрузки системы).

Покажем на примере, как можно использовать модификации таблицы маршрутизации. Предположим, что на Windows-компьютере имеются две сетевые карты, одна из которых непосредственно подключена к Интернету (имеет реальный адрес), а вторая используется для работы во внутренней сети (локальный адрес). Доступ в Интернет осуществляется по умолчанию через шлюз в локальной сети. В этом случае таблица маршрутизации, отображаемая по команде `route print`, выглядит примерно так:

```
Активные маршруты:
Сетевой адрес    Маска сети       Адрес шлюза    Интерфейс   Метрика
0.0.0.0          0.0.0.0          192.168.0.4    192.168.0.29   1
127.0.0.0        255.0.0.0        127.0.0.1      127.0.0.1      1
192.168.0.0      255.255.255.0    192.168.0.29   192.168.0.29   1
192.168.0.29     255.255.255.255  127.0.0.1      127.0.0.1      1
192.168.0.255    255.255.255.255  192.168.0.29   192.168.0.29   1
195.161.192.0    255.255.255.224  195.161.192.2  195.161.192.2  1
195.161.192.2    255.255.255.255  127.0.0.1      127.0.0.1      1
195.161.192.255  255.255.255.255  195.161.192.2  195.161.192.2  1
224.0.0.0        240.0.0.0        192.168.0.29   192.168.0.29   1
224.0.0.0        240.0.0.0        195.161.192.2  195.161.192.2  1
255.255.255.255  255.255.255.255  192.168.0.29   192.168.0.29   1
255.255.255.255  255.255.255.255  195.161.192.2  195.161.192.2  1
Основной шлюз:         192.168.0.4
===================================
Постоянные маршруты: Отсутствует
```

Проверим путь прохождения пакетов на адрес Интернета, например 109.84.231.210, с помощью команды `tracert`:

```
tracert 109.84.231.210 -d
```

Ключ `-d` в команде использован для ускорения операции, чтобы отключить запросы DNS-имен тех хостов, через которые передается пакет данных.

В итоге получаем примерно такую картину (листинг ограничен первыми четырьмя узлами):

```
Трассировка маршрута к 109.84.231.210 с максимальным числом прыжков 30
1    <1 мс    <1 мс    <1 мс   192.168.0.4
2    <1 мс    <1 мс     1 ms   195.12.72.145
3    15 ms     1 ms     1 ms   195.12.75.245
4    40 ms    57 ms    41 ms   195.12.75.241
...
```

Предположим, что мы хотим изменить путь прохождения пакетов к выбранному нами хосту, направив информацию через вторую сетевую карту (а не через шлюз по умолчанию). Для этого с помощью команды `route add` нужно добавить желаемый нами маршрут:

```
route add 109.84.231.210 mask 255.255.255.255 195.161.192.2
```

В команде мы указали, что хотим назначить новый маршрут не для диапазона адресов, а только для конкретного значения (поэтому маска — 255.255.255.255). Кроме того, явно указали адрес сетевого интерфейса, через который нужно пересылать пакеты.

После выполнения данной команды (на экран система не выводит никаких итогов операции) можно просмотреть новую таблицу маршрутизации:

```
Активные маршруты:
Сетевой адрес    Маска сети       Адрес шлюза    Интерфейс     Метрика
...
109.84.231.210   255.255.255.255  195.161.192.2  195.161.192.2    1
...
Основной шлюз:         192.168.0.4
===================================
Постоянные маршруты: Отсутствует
```

По сравнению с исходным вариантом таблица маршрутизации дополнилась одной строкой, которая приведена в данном примере (остальные строки не изменились и опущены для наглядности).

Проверяем новый путь прохождения сигналов:

```
Трассировка маршрута к 109.84.231.210 с максимальным числом прыжков 30
1     1 ms     1 ms     1 ms     195.161.192.1
2    23 ms    22 ms    23 ms     195.161.94.137
3    23 ms    23 ms    23 ms     195.161.94.5
...
```

Видно, что пакеты пересылаются уже через *другой* интерфейс.

Эти изменения маршрутизации действуют до перезагрузки системы или до подачи обратной команды: удаления записей маршрутизации. Для восстановления пара-

метров маршрутизации достаточно подать команду, указав тот маршрут, который требуется удалить:

```
route delete 109.84.231.210
```

Если подобные изменения необходимы постоянно, то следует использовать запуск команды с ключом `-p`, после чего добавленный маршрут будет отображен также в строке `Постоянные маршруты`. При этом обычно можно не указывать параметры маски и интерфейса (если они однозначно определяются по вводимому в команде адресу).

> ***Примечание***
>
> На практике автор встречался с ситуациями, когда изменение параметров маршрутизации в операционной системе Windows не сразу "отрабатывалось" корректно. Иногда после операций над таблицей маршрутизации для достижения успеха нужно было программно отключить и вновь включить тот сетевой интерфейс, для которого выполнялась настройка.

Понимание правил маршрутизации важно не только при построении маршрутов в Интернете, — задаче, которую вряд ли придется решать администраторам сетей некрупных предприятий. На практике для выделения обособленных участков локальной сети (например, по соображениям безопасности) достаточно широко используются виртуальные сети. А для того чтобы обеспечить доступ в такие сети, администраторы должны уметь написать правильную таблицу маршрутизации для соответствующей VLAN или создать список доступа — ACL (access control list), в котором правила записываются аналогично правилам маршрутизации.

Автоматическое присвоение параметров IP-протокола

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

Серверы DHCP

В локальных сетях администраторы 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. Причем администраторы могут с помощью сервера DHCP сообщать клиенту различные настройки: адреса WINS- и DNS-серверов, серверов времени, указывать расположение данных автоматической настройки прокси-клиентов и т. п.

> ***Примечание***
>
> На практике возможны различные варианты настройки DHCP. Так, автор неоднократно на практике сталкивался с ситуацией, когда адреса клиентам назначались фактически "по статике" (путем резервирования по MAC-адресам), а остальные параметры TCP/IP-протокола определялись динамически.

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.

При добавлении IP-протокола в операционную систему его настройки по умолчанию предусматривают автоматическое получение параметров. Если в сети есть настроенный DHCP-сервер, то от пользователя локального компьютера в этом случае не потребуется никаких дополнительных действий по настройке TCP/IP-протокола.

Адресация APIPA

Для облегчения построения небольших сетей предусмотрена возможность самостоятельного назначения адресов. Если в сети нет сервера DHCP, а протокол IP установлен с параметрами автоматического получения значений, то Windows присвоит сетевой плате адрес из диапазона от 169.254.0.1 по 169.254.255.254 (маска подсети 255.255.0.0), предварительно проверив, не используется ли уже такой адрес в системе. Данный механизм позволяет применять IP-протокол в небольших сетях при минимальных ручных настройках — компьютеры увидят друг друга в локальной сети. Естественно, что никаких дополнительных параметров настройки операционная система в этом случае не получает. Например, она не будет знать, куда посылать запросы, чтобы получить данные с серверов Интернета. А если будет отключен протокол NetBIOS поверх TCP/IP, то системы не смогут разрешить имена других компьютеров сети и т. п.

> ***Примечание***
>
> Использование адреса из указанного ранее диапазона (проверяется командами `ipconfig` или `winipcfg`) при наличии в сети сервера DHCP свидетельствует либо о неисправности последнего, либо о проблемах кабельного подключения данного компьютера.

Назначение адресов при совместном использовании подключения к Интернету

Особая ситуация возникает при настройке совместного использования подключения к Интернету. В этом случае тот компьютер, на котором создается данное подключение, начинает выполнять роль сервера DHCP с единственным ограничением: 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 использования подключения присутствует как на серверных системах, так и на рабочих станциях, то такое решение является наиболее оптимальным для небольших организаций. Настройте подключение к Интернету, включите его совместное использование — и вы получите у себя в сети корректное назначение параметров TCP/IP-протокола для компьютерных систем.

> ***Примечание***
>
> Из-за того, что в данной технологии используется один и тот же диапазон адресов, организовать канал соединения двух таких локальных сетей невозможно.

Порт

При передаче данных кроме IP-адресов отправителя и получателя пакет информации содержит в себе номера портов. *Порт* — это некое число, которое используется 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—65535 могут быть использованы 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 используют 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. Однако 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, а используют некоторый диапазон значений. Один из возможных вариантов настройки брандмауэров для недокументированных программ — это анализ их реального трафика с помощью какой-либо программы для перехвата передаваемых по сети пакетов.

Увидеть, какие порты реально задействованы на компьютере, можно с помощью команды `netstat`. В зависимости от версии операционной системы данная команда имеет различный набор ключей, позволяющих детализировать отчет (например, указать программы или процессы, использующие конкретные порты). В общем случае достаточно запустить команду `netstat` с ключом `-a`:

```
>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 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.

> ***Примечание***
>
> Для получения информации по удаленному компьютеру используются специальные программы *сканирования портов*. Наиболее известный бесплатный продукт — *nmap*. Данные по отдельному порту можно получить штатными средствами системы (например, с помощью команды telnet или утилиты *PortQry* из состава Support Tools). Обратите внимание, что хотя использование подобных программ не запрещено стандартами, тем не менее многие системы оценивают сканирование портов как попытку вторжения и блокируют источник на некоторый период времени.

Протокол ARP

Пакеты, пересылаемые в сети Ethernet, адресуются компьютерам не по их именам и не на IP-адрес. Пакет предназначается устройству с конкретным MAC-адресом.

MAC-адрес — это уникальный адрес сетевого устройства, который заложен в него изготовителем оборудования. Первая половина MAC-адреса представляет собой идентификатор изготовителя, вторая — уникальный номер данного устройства.

> ***Примечание***
>
> MAC-адрес часто используется для идентификации систем, например, при создании фильтров допуска в Интернет. Однако следует знать, что этот способ не является полностью надежным: хотя MAC-адрес должен быть уникальным и является неотъемлемой характеристикой устройства, существуют способы его изменения. Например, в новых операционных системах его можно сменить даже через штатные свойства сетевого адаптера, поэтому хакеру для обхода такого фильтра доступа достаточно вывести из строя действующую систему (или выбрать момент ее выключения) и продолжить работу от ее адреса.

Для получения MAC-адреса используется протокол *ARP* (Address Resolution Protocol, протокол разрешения адресов). В системе имеется специальная утилита, которая позволяет отобразить кэш известных данному компьютеру MAC-адресов — arp.

Утилита arp может быть использована, например, при создании резервированных адресов DHCP-сервера. Для такой настройки администратору необходимо ввести MAC-адрес соответствующей системы. Чтобы его узнать, достаточно выполнить команду ping на имя данной системы, после чего просмотреть кэш ARP (командой arp -a) и скопировать значение MAC-адреса в настройки DHCP.

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 компьютеры могут иметь два имени: это NetBIOS-имя компьютера и имя *хоста* (DNS-имя). Обычно имя хоста и NetBIOS-имя совпадают, и к этому следует стремиться. Но принципиально эти имена могут быть разными. Например, длина NetBIOS-имени ограничена 15 символами, а хосту может быть присвоено более длинное название. Или, если при создании домена вы пытаетесь дать ему имя, совпадающее с именем будущего контроллера, то программа установки предложит выбрать другое имя данному хосту.

Имя хоста 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, 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.

На практике под *именем домена* понимают всю группу символов справа от полного имени компьютера. В зависимости от того, сколько групп символов входит в доменное имя, различают домены первого, второго, третьего и т. д. уровней.

> ***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 дать домену Windows имя вида ***<название_организации>*.local**.

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***
>
> Иногда употребляют термин *FQDN* — fully qualified domain name (обычно эту аббревиатуру употребляют без перевода; русский термин звучит как *полное имя узла*). Под FQDN понимают полную цепочку имен системы: от имени хоста до имени корневого домена. Чтобы подчеркнуть, что имеется в виду *полное* имя, в конце его ставят *точку*, которую принято считать *именем корневого домена*. Например, FQDN для Web-сайта будет писаться следующим образом: **www.ask.ru.** (последняя точка включается в имя).

Имена хостов внутри широковещательного домена Windows должны быть уникальны. При попытке запуска системы, имеющей такое же имя, как и у другого работающего компьютера, вы получите сообщение об ошибке.

Доменные имена Интернета

В Интернете за уникальностью присваиваемых имен следит организация (физическое лицо), отвечающая за домен, в рамках которого выдается имя. При присвоении

имен используется принцип: если данное доменное имя свободно, то его можно получить. Приобретение доменного имени — это платная услуга, кроме того, необходимо ежегодно продлевать действие имени. "Отобрать" выданное доменное имя практически невозможно.

Такой способ гарантирует уникальность полного доменного имени компьютера и в то же время требует проверки на уникальность желаемого имени только в одном месте.

Организации и физические лица, регистрирующие для себя доменные имена, обычно стараются создать такое доменное имя, которое легко запоминается пользователем, при этом часто используется юридическое название. Сравните: Белый дом (США) — **whitehouse.gov**, корпорация Microsoft — **microsoft.com**, и т. д.

Существуют два направления создания доменных имен. Одно — по географическому принципу (каждая страна имеет свой домен первого уровня, в рамках которого создаются все имена компьютеров), второе — по типу деятельности организации. В России "географические" домены имеют имена ru и рф (последний — для названий домена на кириллице). Сохранился также домен su, закрепленный ранее за СССР.

Функции технического сопровождения системы регистрации и DNS-серверов зоны ru осуществляет Российский НИИ развития общественных сетей (РосНИИРОС). Со списком организаций, осуществляющих регистрацию в домене ru, можно ознакомиться на странице **http://www.ripn.net:8080/nic/dns/registry-all/reg_list.html**.

Второе направление — это присвоение имени на основе типа деятельности. Среди подобных имен наиболее известен домен com для коммерческих организаций. Другие популярные домены — это edu (учебные организации), gov (правительственные), net (сетевые ресурсы), org (некоммерческие организации), info и т. п.

В настоящее время список доменов "по типу деятельности" существенно расширен, в том числе введено много доменов, в которых можно бесплатно зарегистрировать имя для общественных проектов.

Соотношение доменных имен и IP-адресов компьютеров

Каждый компьютер в глобальной сети должен иметь уникальный IP-адрес. Без наличия такого адреса работа просто невозможна. Наличие доменного имени для работы не обязательно. При необходимости в строках адреса программ, предназначенных для работы в Интернете, можно набирать IP-адрес.

Доменное имя может существовать, но не иметь IP-адреса (естественно, работа с такими узлами невозможна). Такая ситуация может возникнуть, если, например, организация заранее зарегистрировала за собой доменное имя, но не располагает в настоящий момент какими-либо ресурсами в сети Интернет. В этом случае говорят, что домен *не делегирован*.

Одно доменное имя может иметь несколько IP-адресов. Обычно это практикуется на популярных узлах Интернета, что позволяет с помощью специальных решений распределить нагрузку с одного компьютера на несколько. Аналогично несколько

доменных имен могут соответствовать одному IP-адресу (например, при размещении на компьютере нескольких веб-серверов, соответствующих различным организациям).

IP-адреса, соответствующие данному доменному имени, могут меняться. Например, организация переезжает или меняет интернет-провайдера. Сохранение "за собой" доменного имени позволяет не беспокоиться, что в подобных случаях придется нести затраты на "раскрутку" нового имени.

Серверы доменных имен (DNS)

NetBIOS-имя компьютера определяется при установке операционной системы. По умолчанию это же имя будет использовано в качестве имени хоста при получении IP-адреса, хотя в Windows можно назначить разные имена NetBIOS и DNS.

Для поиска компьютера в локальной сети по имени ранее использовались широковещательные запросы: система рассылает запрос на определение имени всем станциям и ждет ответа. Увеличение размеров сети заставляет отказаться от данного метода, поскольку он приводит к значительному росту подобного широковещательного трафика. В распределенных сетях на основе протокола TCP/IP для разрешения имен используются специальные серверы — DNS-серверы (Domain Name System).

Серверы DNS обеспечивают получение доменного имени по запросу на основе IP-адреса, и наоборот. Поэтому указание адреса сервера DNS является одной из основных настроек протокола TCP/IP, необходимых для работы в Интернете. Если в настройках не указан IP-адрес сервера DNS, то пользователь не сможет полноценно работать в Интернете, поскольку ему будет не доступен переход по ссылкам, в которых использовано доменное имя, а это практически все ссылки на информационных серверах.

Адрес сервера DNS обычно сообщается 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.

WINS

Служба регистрации имен в сети Windows (Windows Internet Naming Service, WINS) использовалась для регистрации сетевых имен компьютеров в локальных сетях до Windows 2000. Служба WINS позволяла корректно разрешать имена в сетях с наличием маршрутизаторов. Маршрутизаторы не пропускают широковещательные пакеты, поэтому сегменты локальной сети оказываются изолированными друг от друга при операциях просмотра без использования WINS.

> ***Примечание***
>
> Хотя в настоящее время WINS-сервер в локальных сетях необходим станциям на базе Windows 3.1/9*x*/NT, однако и часть современных служб использует NetBIOS. Поэтому целесообразно сохранить WINS в составе локальной сети.

При начале работы в сети компьютер "сообщает" серверу WINS свое имя и IP-адрес. Эти параметры заносятся в специальную базу и используются для поиска имени компьютера на основе его адреса, и наоборот. Поэтому, чтобы узнать имя компьютера в локальной сети (или его адрес), достаточно сформировать запрос к WINS.

Адрес WINS обычно автоматически сообщается клиентам с помощью DHCP-сервера при получении параметров TCP/IP.

Статическое задание имен

В небольшой локальной сети для задания соответствия "IP-адрес — сетевое имя" можно использовать статические записи, формируемые вручную. Это позволяет обеспечить функционирование сети без использования серверов WINS, 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:

- 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 используется для загрузки специальных NetBIOS-имен (указания сервера домена, серверов приложений и т. п.). Файлы находятся в папке %systemroot%/system32/drivers/etc. При установке системы обычно создаются примеры (имеют расширение sam), по образцу которых и следует редактировать необходимые файлы.

Изменять файлы можно в любом текстовом редакторе, однако для этого необходимы права администратора. Запись должна начинаться с первой позиции строки, а столбцы могут отделяться любым числом пробелов. Операция трудоемкая, особенно при добавлении в сеть новых компьютеров, поскольку это потребует внесения изменений в данные файлы для *всех* уже имеющихся в сети систем.

Последовательность разрешения имен

На практике вы можете столкнуться с тем, что часть систем "видит" одно число компьютеров в сети, а другая — иное. Одни компьютеры успешно работают в сети, а на других отображается сообщение, что вход в сеть не может быть осуществлен, т. к. система не находит контроллер домена. Эти ситуации обусловлены различными используемыми методами *разрешения имен*.

Разрешение имен применяется для того, чтобы найти компьютер (определить IP-адрес) по его имени и получить информацию о сетевых службах, например, узнать адреса контроллеров домена.

Основное отличие методов разрешения имен различных версий Windows состоит в том, что системы до Windows 2000 использовали для разрешения имен NetBIOS, а Windows 2000 и старше (Windows 200*x*/XP/7) нуждаются в информации DNS.

При необходимости разрешения имени сначала предпринимается попытка его поиска в локальных ресурсах. Прежде всего, это локальный кэш имен, который для увеличения производительности создают все системы (кэш имен NetBIOS или кэш имен DNS). Если нужное имя компьютера не найдено, то система пытается найти его в host-файлах. Если и эта попытка неудачна, то системы с ОС Windows 2000 и старше обращаются к серверу DNS, определенному в параметрах настройки протокола TCP/IP их сетевого адаптера. Если сервер DNS недоступен или не смог вернуть имя, то на этом попытки прекращаются и сообщается, что имя не найдено.

Системы Windows NT 4.0 в зависимости от параметров настройки NetBIOS либо рассылают широковещательные запросы на определение имени, либо обращаются к серверу WINS. Информация DNS используется только в том случае, если это явно указано в настройках сетевого адаптера.

С помощью DNS системы на базе Windows 200*x*/XP/7 находят и расположение служб. Например, адрес контроллера домена может быть узнан по имени _ldap._tcp.dc._msdcs.<имя_домена>, адрес службы Gatekeeper (используется при передаче IP-телефонии, видеоконференций и т. п. по каналам связи) определяется по результатам запроса на имя Q931._tcp.<имя_домена> и т. д.

При использовании NetBIOS-станции, регистрируясь в сети, сообщают свое имя и имена служб, которые на них запущены. Эти имена можно просмотреть, например, при помощи команды `nbtstat –a <имя_компьютера>`. В результате будет отображена приблизительно такая информация:

```
>nbtstat -a test
Internal:
Адрес IP узла: [192.168.0.29] Код области: []

Таблица NetBIOS-имен удаленных компьютеров
Имя                    Тип          Состояние
---------------------------------------------------
TEST           <00>    Уникальный   Зарегистрирован
ACK            <1C>    Группа       Зарегистрирован
ACK            <00>    Группа       Зарегистрирован
TEST           <20>    Уникальный   Зарегистрирован
ACK            <1B>    Уникальный   Зарегистрирован
ACK            <1E>    Группа       Зарегистрирован
ACK            <1D>    Уникальный   Зарегистрирован
__MSBROWSE__.  <01>    Группа       Зарегистрирован
MP_ACK         <1A>    Уникальный   Зарегистрирован

Адрес платы (MAC) = 00-02-B3-4F-F9-E9
```

В нашем примере компьютер TEST зарегистрировал имя рабочей станции TEST (первая строка). Типы служб, соответствующих сообщаемым командой кодам, можно посмотреть, например, по адресу **http://www.microsoft.com/technet/prodtechnol/winntas/support/ sur_apph.mspx**. Запись `ACK <1C>` свидетельствует о том, что этот компьютер является контроллером домена ACK, `ACK <00>` — это имя домена компьютера, `TEST <20>` свидетельствует о том, что на компьютере запущена служба *сервер*. Строка `ACK <1B>` говорит о том, что компьютер является мастер-просмотрщиком сети и т. п.

Эти имена сохраняются на компьютерах, выполняющих роли просмотра сети, а также на сервере WINS, с которых они могут быть получены по запросам клиентов.

Настройка серверов WINS, DHCP, DNS

Службы серверов WINS, DHCP, DNS должны быть установлены на компьютер со статическим IP-адресом.

Установка и настройка WINS

Установка WINS крайне проста: достаточно указать эту службу в составе устанавливаемых компонентов Windows Server. Какой-либо последующей специальной настройки служба WINS не требует. Вам необходимо при "раздаче" клиентам настроек протокола TCP/IP указать только адрес сервера со службой WINS, после чего системы при старте автоматически будут регистрироваться в базе WINS. В случае необходимости (она возникает крайне редко) соответствующие записи можно занести вручную, если воспользоваться консолью управления WINS (статические записи).

Если в системе установлено *несколько* WINS-серверов, то необходимо настроить синхронизацию их баз данных. Для этого на каждом WINS-сервере следует указать адрес другого WINS-сервера, с которым нужно проводить синхронизацию данных.

> ***Примечание***
>
> Если маршрутизаторы сети пропускают широковещательные сообщения, серверы WINS можно настроить на автоматическое обнаружение партнеров по синхронизации. Для этого достаточно отметить соответствующую опцию на вкладке дополнительных свойств настройки WINS.

WINS-прокси

Компьютеры используют данные базы WINS только в том случае, если соответствующие настройки определены в их параметрах TCP/IP-протокола. Если вы хотите, чтобы все NetBIOS-компьютеры сети могли воспользоваться WINS для разрешения имен, то следует создать в каждом сегменте сети WINS-прокси.

Компьютеры, не использующие WINS, для разрешения имен рассылают широковещательные пакеты. WINS-прокси, обнаружив такой пакет, пытается разрешить имя в своем кэше и при неудаче передает запрос на тот WINS-сервер, который зарегистрирован для данной системы. Если сервер WINS возвращает имя, то WINS-

прокси передает эти данные той системе, которая отправила широковещательный запрос.

Для включения режима прокси необходимо установить в 1 параметр `EnableProxy` в разделе `HKLM\System\CurrentControlSet\Services\NetBT\Parameters` реестра компьютера, который предполагается использовать в роли WINS-прокси.

Настройка DHCP

Использование DHCP-сервера требует от администратора обязательного определения ряда параметров. Для установки службы достаточно отметить ее в перечне параметров Windows Server, но после установки необходимо выполнить (в Windows 2008 Server указанные шаги предлагает выполнить мастер установки роли) как минимум следующие действия:

- ❒ создать и настроить зону;
- ❒ авторизовать DHCP-сервер.

> ***Примечание***
>
> При наличии в сети двух DHCP-серверов клиент "возьмет" настройки IP-протокола от того сервера, ответ от которого будет получен первым *(см. разд. "Порядок получения IP-адресов клиентами DHCP" далее в этой главе)*.

Создание и настройка зоны

Сервер начнет раздавать адреса только после того, как вы зададите диапазон этих адресов и определите необходимые параметры протокола. Делается это путем создания новой области (scope).

> ***Примечание***
>
> Название области может быть задано произвольно; диапазон адресов менять в процессе работы допустимо, но значение маски подсети, определенное при создании области, изменить *невозможно*. Можно только удалить область и создать новую с иным значением.

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

Желательно в параметрах DHCP-сервера указать, чтобы он проверял IP-адрес перед его выдачей клиенту. Это позволит предупредить конфликты, возникающие при самостоятельном присваивании IP-адресов у клиентов, а также облегчит ситуацию восстановления сервера (например, после полной очистки его баз).

> ***Примечание***
>
> Если в сети предприятия есть компьютеры с операционной системой до Windows 2000, то целесообразно установить в настройках DHCP обязательную регистрацию выдаваемого адреса на сервере DNS независимо от того, установлена данная опция у клиента или нет.

Авторизация DHCP-сервера

DHCP-серверы на операционных системах Windows 200*x*, работающих в составе домена Windows, должны быть *авторизованы*. Если DHCP-сервер не авторизован в службе каталогов, то он не будет выдавать IP-адреса. Чтобы авторизовать сервер, пользователю с правами администратора предприятия необходимо в меню консоли управления DHCP-сервером выбрать пункт **Авторизовать сервер**. 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.

Если в вашей сети установлен DHCP-сервер на другой операционной системе, например на платформе Windows NT 4.0 Server или на Linux, то он будет обслуживать клиентов *независимо от авторизации в службе каталогов*.

Настройка параметров области

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

Для этого необходимо определить *опции* области.

> ***Примечание***
>
> В последних версиях операционных систем мастер создания области автоматически предлагает заполнить основные параметры. При этом могут быть определены как параметры всего сервера, так и параметры области. Обратите внимание, что в случае конфликта параметров клиентам будут сообщаться параметры не сервера, а области.

Вы можете определить любые параметры области (как минимум, необходимо указать те величины, которые запрашиваются мастером создания новой зоны), а при необходимости — и создать собственные. Описание дополнительных параметров обычно включаются в документацию прикладного программного обеспечения, которому необходимы дополнительные настройки DHCP.

Резервирование адресов

DHCP-сервер можно настроить так, чтобы он выдавал клиентам не случайный, а заранее определенный адрес.

> ***Примечание***
>
> Автор достаточно часто сталкивался с ситуацией, когда все адреса в локальной сети раздавались на основе резервирования. Администраторы осуществляли такую статическую настройку адресов для того, чтобы сочетать закрепление адресов, свойственное статическому распределению, с возможностью легкой смены таких параметров, как адрес DNS-сервера.

Чтобы настроить резервирование адреса, необходимо знать *MAC-адрес сетевого адаптера* соответствующего клиента, причем для новых сетевых адаптеров MAC-адрес может быть определен по их упаковке (вторая часть адреса — это серийный номер адаптера). Этот адрес достаточно просто определить, если сначала подключить клиента к сети любым способом (например, назначить адрес вручную или автоматически), после чего воспользоваться утилитой arp *(см. разд. "Протокол ARP" ранее в этой главе)*.

Сам процесс резервирования не представляет сложности: достаточно в оснастке управления DHCP-сервером ввести в окне операции резервирования имя клиента и его MAC-адрес.

> ***Примечание***
>
> Обратите внимание, что для резервированного клиента DHCP-сервер позволяет установить свои, индивидуальные параметры протокола TCP/IP, отличные от параметров области.

"Подстройка" DHCP под группы клиентов

Очень часто администраторы сети хотели бы, чтобы часть клиентов получала IP-адреса из одного диапазона, а часть — из другого, возможно, с отличающимися параметрами настройки протокола TCP/IP.

Существует всего несколько возможностей "выделить" различных клиентов, но только для получения отличающихся параметров области (scope option).

Первая возможность — это резервирование клиентов. Для резервированных клиентов можно определить собственные параметры области. Но для создания такого клиента нужно точно знать его MAC-адрес.

Вторая возможность — это разделение клиентов по *классам*: классу вендоров (vendor class) и классу пользователей (user class). Для клиентов класса администратор может настраивать индивидуальные опции DHCP-сервера. Например, в DHCP вендором считается производитель соответствующего программного обеспечения операционной системы. В результате можно разделить клиентов с операционными системами разных версий и вендоров.

> ***Примечание***
>
> Администраторы могут добавлять описания классов вендоров в параметры DHCP-сервера, но для этого придется узнать по технической документации необходимые настройки соответствующего производителя.

Использование *пользовательских классов* доступно в серверах DHCP Microsoft, начиная с версии 2000 и выше. Основное отличие от вендорского класса состоит в том, что устанавливать принадлежность к классу могут сами пользователи (с помощью команды `ipconfig /setclassid <имя_подключения> <класс>`). Например, можно применить пользовательские классы для осуществления различной настройки TCP/IP-протокола мобильных и стационарных компьютеров.

Конечно, в больших организациях подобную настройку можно включить в образы операционной системы, которая потом будет тиражироваться раздельно по струк-

турам предприятия. Но для малых организаций применение пользовательских классов обычно не востребовано.

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.

> ***Примечание***
>
> Для соединения сегментов могут использоваться RFC-1542-совместимые маршрутизаторы, которые имеют возможность пропускать пакеты с запросом аренды адреса. Однако обычно такая настройка достаточно трудоемка, требует внимательного анализа конфигурации сети и нечасто применяется на практике.

Создание областей с различными диапазонами IP-адресов выполняется типовым образом: вы создаете область и определяете для нее любой желаемый диапазон адресов. Однако раздавать из области адреса, не соответствующие диапазону собственной подсети, DHCP-сервер *не будет*, пока не получит адресованного ему запроса из другого сегмента.

Такие запросы может формировать специальный агент — агент ретрансляции DHCP (DHCP Relay Agent). Обычно используется агент ретрансляции, установленный на коммутационном оборудовании. Но можно задействовать и агент, входящий в состав сервера маршрутизации и удаленного доступа (Routing and Remote Access Server, RRAS).

Принцип работы агента ретрансляции DHCP достаточно прост. Агент прослушивает сеть на наличие пакетов запроса аренды адреса. Если такой пакет получен, то агент ожидает некоторое время (на случай, если в данном сегменте сети есть свой DHCP-сервер, который и обслужит клиента; таким образом можно повысить отказоустойчивость данного сегмента сети, дублируя локальный DHCP-сервер соответствующей областью на удаленном DHCP-сервере). Если запрос клиента остается необслуженным, то агент ретранслирует запрос в соседние сегменты сети. Если в соседних сегментах есть DHCP-сервер, то он получает данный запрос и, поскольку запрос отправлен с адреса другого сегмента сети, предоставляет в аренду адрес именно того диапазона, из которого пришел запрос.

Для установки программного агента ретрансляции достаточно в настройках IP-маршрутизации (**IP Routing**, пункт **General**) соответствующего сервера RRAS выбрать команду создания нового протокола маршрутизации и указать **DHCP Relay Agent**. В настройках агента ретрансляции следует указать IP-адрес DHCP-сервера, на который будут ретранслироваться запросы аренды адреса.

Далее нужно добавить в агент ретрансляции интерфейс (или несколько интерфейсов, если компьютер подключен к нескольким сегментам сети), через который будут пересылаться запросы аренды. Затем при необходимости следует отрегулировать *порог ожидания* (*boot threshold*) — время, в течение которого будет ожидаться

ответ локального DHCP-сервера, и *hop-count threshold* — максимальное количество маршрутизаторов, через которые может пройти этот пакет.

Порядок получения IP-адресов клиентами DHCP

Во многих случаях знание процедуры аренды IP-адреса может помочь в диагностике неисправностей сети.

Первичное получение адреса

При включении компьютера клиент, настроенный на динамическое получение адреса, передает широковещательную рассылку с запросом IP-адреса (запрос идет от адреса 0.0.0.0 с маской 255.255.255.255). Это сообщение называется *DHCPDISCOVER*. На этот запрос отвечают *все* DHCP-серверы сегмента сети, предлагая IP-адрес. Соответствующее сообщение называется DHCPOFFER. Выделяемые для аренды адреса на некоторый период резервируются и не предлагаются другим клиентам.

Клиент ждет предложения по адресу от сервера DHCP одну секунду. Если оно не приходит ни от одного сервера, то запрос аренды повторяется еще пять раз (через увеличивающиеся промежутки времени приблизительно в течение 30 сек). Если ответ от DHCP-сервера так и не получен, то клиент получает адрес по технологии APIPA *(см. разд. "Адресация APIPA" ранее в этой главе)*.

На *первое* полученное предложение от DHCP-сервера клиент отвечает широковещательным сообщением (DHCPREQUEST), в котором содержится IP-адрес сервера, выдавшего это предложение. После получения такого сообщения *другие* DHCP-серверы освобождают зарезервированные ими IP-адреса, а сервер, предложение которого принято, высылает подтверждение (DHCPACK). Только после получения этого подтверждения клиент полностью инициализирует TCP/IP-протокол своего сетевого адаптера.

Продление аренды

Запрос на продление аренды IP-адреса высылается после истечения половины периода аренды и при каждой перезагрузке системы. Для этого на сервер, выдавший адрес, отправляется DHCPREQUEST-запрос. Если подтверждение получено (DHCPACK), то клиент продолжает использовать текущие параметры конфигурации. Если ответ не получен, то запросы на данный сервер повторяются. Перед окончанием срока аренды и при отсутствии ответа от выдавшего IP-адрес DHCP-сервера клиент высылает уже широковещательные запросы DHCPDISCOVER, пытаясь получить адрес от *любого* DHCP-сервера.

> ***Примечание***
>
> При отказе в аренде DHCP-сервером высылается специальный пакет DHCPNACK.

Если срок аренды закончился, а клиент не смог ни получить подтверждения от "своего" DHCP-сервера, ни запросить новый IP-адрес, то *текущие настройки IP-протокола освобождаются*, а клиент получает адрес по APIPA.

Если при перезагрузке операционной системы попытка обновления аренды адреса неудачна и клиент не может установить связь со шлюзом по умолчанию, то теку-

щие настройки IP-адреса также освобождаются. Такая ситуация может свидетельствовать о переносе компьютера в другой сегмент сети, поэтому он освобождает свой адрес.

Диагностика и обслуживание DHCP-сервера

Обычно никаких проблем с использованием DHCP-сервера не возникает. В противном случае следует включить протоколирование его работы (опция на одной из вкладок консоли управления сервером). После выявления причин неисправностей для повышения производительности системы ведение журнала работы DHCP-сервера следует отключить.

Сервер проводит фоновую дефрагментацию базы данных клиентов. Ручная *(офлайновая)* дефрагментация имеет смысл только в случае большой нагрузки на серверы (более 1000 записей клиентов). При меньшем числе клиентов ручную дефрагментацию (она проводится при помощи программы `jetpack`; которая требует предварительной остановки DHCP-сервера) рекомендуется проводить раз в несколько месяцев или еще реже.

При возникновении ошибок в базе достаточно просто исполнить операцию `reconcile` для соответствующей области или всего сервера. При серьезных проблемах допустимо остановить DHCP-сервер и удалить все файлы баз из его каталога. После старта они будут воссозданы с пустыми значениями, которые потом снова заполнятся по получении запросов.

DNS

В доменах Windows информация о необходимых для работы систем службах хранит DNS. И основное количество проблем функционирования домена (службы каталогов) связано именно с неверной настройкой администраторами службы DNS. Поэтому стоит рассмотреть сервер DNS более подробно.

Термины DNS

DNS (Domain Name System, система доменных имен) — это служба разрешения имен в сетях на основе протокола TCP/IP.

- **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 *прямой* и *обратной* 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 зарегистрировано и обратное.

Примечание

Отсутствие обратного разрешения имени является достаточно частой ошибкой в Интернете. Обычно владельцами прямой зоны данного домена и обратной зоны, которая соответствует этому имени, являются разные люди (организации), поэтому в процессе регистрации новых DNS-записей часто забывают создать соответствующую запись обратной зоны.

Фактически прямые зоны соответствуют доменам некоторого уровня. Например, зона ask.ru позволяет разрешить все запросы имен, относящихся к домену ask.ru.

Для разрешения обратных имен в домене самого верхнего уровня создана зона in-addr.arpa. Названия зон обратного просмотра формируются добавлением к этому имени 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.

В большинстве случаев отсутствие регистрации в обратной зоне не мешает нормальной работе в Сети. Однако оно может и привести к ошибкам в тех случаях, когда необходимо установить по IP-адресу имя сервера. Например, при обмене почтовыми сообщениями в настоящее время принято проверять принадлежность сервера к тому домену, от имени которого он передает почту. Если обратное разрешение имени не будет проведено, то система может получить отказ в приеме почты.

- **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 зонами. 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. 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. Обычно в настройках DNS-серверов предусматриваются специальные механизмы оповещений, которые обеспечивают синхронность записей первичной зоны и ее копий на вторичных серверах. Но, если это не запрещено настройками DNS-сервера, вы можете создать на своем сервере вторичную зону, обновления которой будут осуществляться по некоему графику. В результате записи такой копии могут оказаться неактуальны. Поэтому принято для домена определять серверы имен, информация которых "официальна". Такие серверы называют NS-записями соответствующего домена. Обычно для каждого домена создается два или три NS-сервера. Если ответ на запрос разрешения имени получен от NS-сервера, то он считается авторизованным, другие серверы возвращают неавторизованные ответы.

Примечание

Это не значит, что в этом случае возвращаются неверные данные. DNS-сервер разрешит запрос клиента на основании данных своей копии только в том случае, если эти данные не устарели. Но если срок жизни записей на сервере имен был установлен, например, равным неделе, то в случае внесения изменений в первичную зону необходимо быть готовым к тому, что еще до недели после смены информации на NS-сервере другие серверы DNS могут возвращать старые значения. То есть вы столкнетесь с ситуацией, когда часть систем уже получила правильные данные об имени, а часть — нет. Поэтому перед предполагаемой сменой записей DNS необходимо уменьшить время их жизни и выждать период, равный старому времени жизни. Это позволит сократить период такой неопределенности в разрешении имен. После выполнения операции настройки следует вернуться к старым величинам, чтобы снизить нагрузку на сеть и DNS-серверы.

Если вы предполагаете, что копия DNS-записей на сервере DNS неактуальна, то следует выполнить операцию *очистки кэша* для соответствующей зоны. Для этого необходимо в консоли управления сервером включить опцию отображения дополнительных параметров, найти нужную зону среди структуры кэша и выполнить для нее очистку. При следующем запросе данных из этой зоны сервер загрузит копию с того сервера DNS, на который настроена пересылка запросов. Поэтому и эта операция также не гарантирует получение актуальной копии записей. При рассмотрении проблемных ситуаций следует выяснить на официальных ресурсах адреса NS-серверов данного домена и проверить записи с помощью утилиты `nslookup`, подключаясь к соответствующему NS-серверу *(см. разд. "Обслуживание и диагностика неисправностей DNS-сервера" далее в этой главе)*.

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 передача зон обычно разрешается только на заранее определенный администратором системы список IP-адресов DNS-серверов. Если операция передачи зоны запрещена, то вы не сможете создать на своем DNS-сервере вторичную зону для данного домена.

- **Делегирование зон.**

  Если на DSN-сервере создана, например, прямая зона для домена test.local, то запись о домене третьего уровня level3.test.local должна содержаться 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, для чего используется процесс делегирования зоны. При делегировании зоны DNS-сервер создает у себя запись, указывающую, что запросы разрешения имени для этой зоны должны перенаправляться на другой DNS-сервер, на который проведено делегирование зоны.

- **Stub-зона (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 сменить и записи NS-сервера. Если соответствующее изменение не будет внесено на сервер, который осуществляет делегирование, то процесс разрешения имен будет нарушен (основной сервер по-прежнему будет отправлять запросы на уже не существующий адрес, и в результате будет формироваться неверный ответ).

  Для исправления подобной ситуации в DNS-сервере Windows Server 2003 введены *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 я уже указывал ранее, принято называть именем "точка". Если в DNS создать зону "точка" (зона с таким именем создается при установке службы каталогов с одновременной установкой и настройкой сервера DNS), то это будет фактически означать, что данный сервер является корневым в структуре DNS *(см. следующий раздел)*, т. е. он должен разрешать самостоятельно любые запросы имен. Если этот DNS-сервер не может разрешить имя, то его ответ будет сообщать, что такого хоста не существует.

> ***Примечание***
>
> При необходимости пересылки запросов DNS на другие серверы зону "точка" следует удалить, после чего появится возможность настройки пересылки запросов DNS.

Порядок разрешения имен в DNS

Для разрешения имен в DNS предусмотрено два типа запросов: итеративный и рекурсивный.

Итеративный запрос служит для получения от DNS-сервера, которому он направлен, наилучшего ответа, который может быть получен *без обращения* к другим DNS-серверам. *Рекурсивный запрос* предполагает, что сервер DNS должен выполнить все операции для разрешения имени. Обычно для этой цели необходимо выполнить несколько запросов к различным серверам DNS.

Процесс определения имени с использованием итеративных запросов весьма трудоемок. Нужно найти NS-сервер для данного домена и затем запросить от него данные по требуемому имени. Обычно клиенты все эти операции "возлагают" на DNS-серверы, отправляя им рекурсивный запрос.

DNS-сервер после получения рекурсивного запроса просматривает собственный кэш имен. Если он находит нужную запись и она еще не устарела, то это значение возвращается клиенту. Если записи нет, то сервер предпринимает попытку поиска сервера имен для домена, содержащегося в запросе. Чтобы найти такой сервер, запрос *всегда* отправляется на корневой сервер, а от него получают информацию по

домену первого уровня, запросом на домен первого уровня получают информацию о NS-серверах домена второго уровня и т. д. После этого отправляется итеративный запрос на NS-сервер соответствующего домена. Естественно, что большинство информации от корневых доменов уже кэшировано на данном сервере. Этим резко снижается нагрузка на сеть и уменьшается время ответа на запрос. В результате запросы "не доходят" до корневых серверов, но сама цепочка разрешения имени *всегда выполняется от корня* до текущего домена.

Обычно администраторы локальных DNS-серверов настраивают свой сервер на пересылку (forwarding) запросов разрешения имен на тот или иной сервер DNS (обычно это DNS-сервер провайдера). Тем самым вся процедура разрешения имен будет выполняться уже другим сервером. Поскольку мощные серверы Интернета обычно имеют существенно больший кэш и лучший канал подключения к глобальной сети, то таким способом достигается уменьшение времени ответа и снижение трафика.

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: 20110810.

- **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 в случае возникновения каких-либо вопросов по домену организации у специалистов были реальные контактные данные. Обратите внимание, что символ "`@`" адреса электронной почты заменяется на точку.

- **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 базе DNS для домена должна быть обязательно создана MX-запись. В целях резервирования может быть создано несколько MX-записей, причем 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 другими весами в порядке их возрастания.

- **SRV** (Запись службы).

  Специальный тип записи, используемый для обнаружения в домене служб (например, службы IP-телефонии и т. п.). Записи о системных службах Windows автоматически создаются службой каталогов. Ручное добавление записей осуществляется при настройке дополнительных продуктов в соответствии с прилагаемой технической документацией.

> ***Примечание***
>
> Кроме описанных существуют и другие типы записей, предназначенные, например, для DNSSEC, IPv6 и т. п., но мы не будем их касаться в этой книге.

Установка сервера DNS

Сервер DNS можно установить только на компьютер со статическим IP-адресом. При этом удостоверьтесь, что сервер DNS, который предназначается для обслуживания организации, может правильно разрешать *неполные* имена. То есть 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, статически устанавливаемых для сетевого адаптера сервера DNS.

Для установки службы DNS-сервера достаточно выбрать соответствующую опцию среди добавляемых компонентов (выбрать роль). В целях отказоустойчивости информационная система должна быть настроена на использование нескольких серверов DNS.

После запуска службы DNS следует уточнить некоторые параметры настройки. Во-первых, если сервер должен разрешать имена сети Интернет, то следует удалить зону "точка" (если такая создана при установке) и указать IP-адреса тех серверов DNS, на которые будут пересылаться запросы разрешения имен. Обычно в качестве таковых указываются DNS-серверы провайдера.

Далее следует создать на сервере DNS необходимые зоны. Эта операция выполняется при помощи соответствующего мастера. 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 фактически будет являться первичной (допускать внесение изменений), а сами данные — безопасными (при работе с зоной будет применена действующая в Windows система безопасности).

Интегрированная в службу каталогов система имен реплицируется в Windows 200*x* по всем контроллерам домена. Начиная с ОС 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. Создание такого раздела выполняется из оснастки управления DNS-сервером (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.

После установки и настройки основных параметров DNS-сервера необходимо выполнить его первичную проверку. Для этого следует в свойствах сервера на вкладке мониторинга включить опции проверки как работы самого сервера, так и правильности перенаправления запросов и провести тест, после чего проверить корректность разрешения имен как внутренней сети, так и внешней (если сервер DNS используется и для разрешения имен Интернета) с помощью команды `nslookup` *(см. разд. "Обслуживание и диагностика неисправностей DNS-сервера" далее в этой главе)*.

> ***Примечание***
>
> При создании домена одновременно с установкой DNS прямая зона создается автоматически. Зону обратного разрешения следует создать вручную.

Записи домена Windows

Если на сервере DNS зарегистрирована зона, соответствующая домену Windows, то в этой зоне должны присутствовать специализированные записи, которые определяют нахождение служб каталогов домена. Данные записи создаются автоматически через некоторое время после установки службы каталогов.

Разделение DNS

Все большее число сотрудников начинают использовать мобильные компьютеры для доступа к ресурсам организации как изнутри локальной сети, так и из Интернета. В целях 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. 3.11).

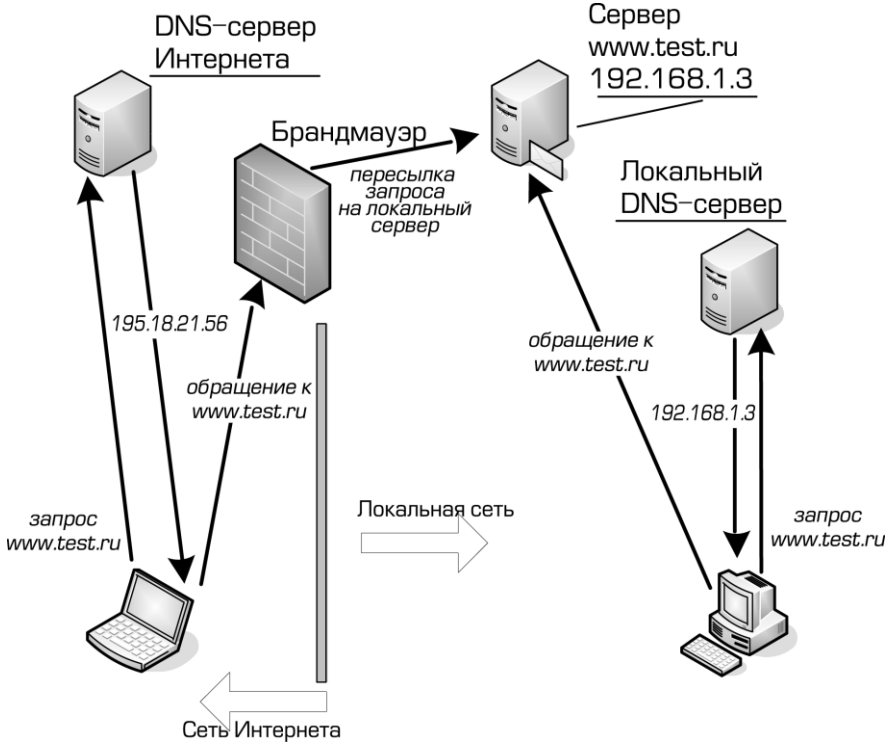


Рис. 3.11. Разделение DNS

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 использовании технологии разделения DNS клиент локальной сети и компьютер Интернета при разрешении одного и того же имени будут обращаться к различным DNS-серверам. В результате локальный клиент будет обращаться по локальному адресу, а клиент Интернета перешлет запрос на брандмауэр организации, который и перенаправит его на локальный адрес запрашиваемого ресурса.

- **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. Далее в этой зоне следует создать записи, соответствующие именам систем, предоставляющих необходимые службы (естественно, что изменение записей этой зоны должно выполняться только вручную), причем в качестве IP-адресов этих записей должны быть указаны *локальные* IP-адреса систем. Таким образом, на внутренних DNS-серверах будет по две зоны: зона, соответствующая "внутреннему" домену Windows (реальные внутренние названия компьютеров локальной сети), и зона с "внешним" именем (фактически содержащая 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.

Настройка DNS в удаленных офисах

Возможны различные варианты конфигурации разрешения имен для удаленных офисов. В наиболее часто используемом случае подключения удаленного офиса к основному через Интернет по VPN-каналу можно реализовать следующую настройку DNS. DNS-сервер удаленного офиса настроить на пересылку запросов разрешения имени на DNS-сервер интернет-провайдера, а пересылку запросов на

разрешение внутренних имен настроить на DNS-сервер центрального офиса. Такая конфигурация легко реализуется на DNS-серверах Windows Server 2003/2008.

Примечание

Ресурсом, для которого наиболее часто приходится реализовывать подключение пользователей как изнутри организации, так и снаружи, является почтовая система. 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 использует 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 KB 833401). Обратите внимание, что одновременно следует настроить и клиента Outlook так, чтобы по умолчанию для подключения к почтовому серверу Exchange использовался вариант RPC over HTTP (статья "Configuring Outlook 2003 for RPC over HTTP").

Обслуживание и диагностика неисправностей DNS-сервера

Самый простой способ проверить работоспособность сервера — 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.

Сервер DNS ведет протокол своих основных событий в специальном журнале — DNS-сервер (доступен с помощью программы Просмотр событий). В этом журнале по умолчанию фиксируются только основные события (старт или остановка службы, серьезные ошибки: невозможность передачи зоны и т. п.). Если необходимо подробно проанализировать работу сервера, то можно включить крайне детализированный протокол — установить опции *ведения журнала отладки* на соответствующей вкладке консоли управления сервером DNS. Но использовать эту возможность следует *только* на период отладки. В журнал по умолчанию заносится вся информация (подробно — все данные пакетов), что негативно сказывается на производительности сервера.

Универсальная утилита, которую можно использовать для получения данных с любого DNS-сервера (и, соответственно, проверки его работоспособности), — это nslookup, которая вызывается одноименной командой. 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 используется 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 использования программы `nslookup` (строки, вводимые пользователем, в начале строки отмечены знаком >).

```
>nslookup
Default Server: ack
Address: 192.168.0.10
```

Примечание

После запуска программа выдала сообщение, что подключена к DNS-серверу ack с IP-адресом 192.168.0.10.

```
>server ns.unets.ru
Default Server: ns.unets.ru
Address: 195.161.15.19
```

Примечание

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.

```
>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
```

Примечание

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**.

```
>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
```

Примечание

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,** приоритет 10 и **relay.utnet.ru**, приоритет 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**.

Для проверки разрешения имен DNS почтового сервера MS Exchange используется специальная утилита, которую необходимо загрузить с сайта Microsoft — dnsdiag. Эта программа должна быть запущена на компьютере почтового сервера из папки информационного сервера (IIS) с помощью команды `dnsdiag`.

Выходная информация программы полностью соответствует тем данным, которые получает почтовый сервер в процессе разрешения имен. Эта информация может помочь в диагностике проблемных ситуаций.

Рассмотрим пример использования утилиты dnsdiag.

Примечание

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).

```
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.

Перенос записей зон

Информация зон DNS домена может быть экспортирована в обычный текстовый файл. Таким способом можно легко вручную перенести зону DNS с одного сервера на другой (например, при модернизации платформы или после какого-либо восстановления).

ГЛАВА 4

Информационные системы предприятия

Построение информационной системы зависит от многих параметров, в том числе, от численности сотрудников, от распределенности офисов, от решаемых задач и т. п.

Домашние сети

В малых предприятиях с небольшим числом компьютеров к функционированию сети не предъявляется особых требований. Обычно нужно получить доступ к файлам на диске другого компьютера, распечатать документ на общем принтере и выйти в Интернет. Сотрудники хорошо знают друг друга, и не возникает необходимости разделения прав доступа к каким-либо ресурсам и т. п. Такие сети принято называть *домашними*.

Создаются такие системы крайне просто. Необходимо только осуществить прокладку локальной сети, установить рабочие станции и предоставить ресурсы для совместного использования. Обычно все эти шаги не вызывают сложностей даже у не очень подготовленного пользователя.

Для работы в Интернете, конечно, можно использовать и вариант совместного доступа, предусмотренный в Windows, но лучше приобрести небольшой аппаратный маршрутизатор. Эти устройства дешевы, обеспечивают подключение компьютеров локальной сети к Интернету, надежно защищают внутреннюю сеть от внешних атак, включают в себя сервисы *DHCP* (Dynamic Host Configuration Protocol — протокол динамической конфигурации хоста) и точки беспроводного доступа (Wi-Fi).

Такая сеть имеет некоторые особенности настройки.

Первая заключается в особенностях группы *Все*. Если ресурсы предоставляются с рабочей станции Windows для совместного использования *всем*, то это означает не *всех* в житейском понимании этого слова, а для всех учетных записей, которые зарегистрированы на локальном компьютере. Иными словами, в системе должны быть созданы пользователи, соответствующие текущим пользователям *каждой* рабочей станции сети (идентичные имена и пароли). Если в Windows нет учетной

записи с именем и паролем пользователя, пытающегося подключиться с другой станции (а обычно операция производится от имени того, кто работает на компьютере), то в подключении будет отказано. То есть если на одном компьютере работает пользователь `Иванов` с паролем `пароль`, на втором — `Петров` с паролем `пароль2`, то необходимо создать пользователей `Иванов` и `Петров` с соответствующими значениями паролей на той станции Windows, ресурсы которой предоставляются для совместного использования. Причем при необходимости смены паролей они должны изменяться синхронно. На практике на малых предприятиях в этом случае на всех компьютерах прописывается один и тот же пользователь с одинаковым ненулевым паролем.

Более удобный в этом случае вариант для малой сети — это разрешить анонимный доступ. Делается это включением учетной записи Гость, которая по умолчанию заблокирована. Это самый простой способ, но он не позволяет выборочно контролировать или как-то ограничивать доступ к ресурсам, поскольку все подключения к компьютеру будут осуществляться от имени одной учетной записи. Если ресурс будет предоставлен в общее пользование, то он станет доступен любому пользователю.

Вторая проблема — это ограничения, искусственно введенные в рабочие станции Windows. Прежде всего, это максимальное количество подключений пользователей по сети — 10. Это ограничение не мешает подключиться одиннадцатому пользователю, но при этом автоматически разорвется одно из имеющихся неактивных соединений. Кроме того, существуют ограничения по количеству одновременно открытых по сети файлов. К сожалению, это условие становится критичным при использовании популярной программы 1С:Предприятие (в комплексной версии или при работе уже 3—4 сотрудников в обычной конфигурации).

Самый простой и бесплатный способ обойти подобные ограничения Windows — установить Linux-систему и организовать с нее предоставление ресурсов для Windows-клиентов (см. *главу 2*).

Одноранговые сети

Описанная в предыдущем разделе сеть является частным случаем *одноранговой сети*, в которой каждый компьютер управляется автономно и отсутствуют какие-либо централизованно реализуемые правила. Все управление ресурсами компьютера остается за локальным администратором. Кстати, по такому принципу реализован и Интернет.

Для объединения компьютеров в одноранговую сеть достаточно только создать структуру сети (провести кабели или купить беспроводные точки доступа, поставить коммутаторы и т. п.). Компьютер подключается к сети и настраивается на использование ресурсов других систем. В свою очередь администратор каждого компьютера должен определить, какие ресурсы локальной системы предоставляются в общее пользование и с какими правами, и осуществить необходимые настройки.

Одноранговая сеть удобна, если число компьютеров не превышает одного-двух десятков. С увеличением числа компьютерных систем осуществлять автономное

управление каждой по единым требованиям предприятия администратору становится слишком затруднительно. Поэтому при росте локальной сети вводится то или иное централизованное управление. Конкретный критерий смены варианта управления сети определяется спецификой функционирования каждой организации.

Для сетей небольших организаций в качестве операционной системы рабочих станций может быть использована любая программа. Учитывая, что большинство пользователей имеют на домашних компьютерах ту или иную версию Windows и что обычно на таких предприятиях не существует серьезных производственных задач, можно рекомендовать построение небольшой локальной сети на основе Windows.

Не стоит приобретать топовые версии операционной системы. Для работы на малых предприятиях прекрасно подойдет версия Windows 7 Home Edition, стоимость которой существенно ниже профессионального варианта. Различие между этими системами касается в основном вопросов безопасности при работе в составе домена и не существенно в данном случае.

Также не имеет смысла обновлять версии операционных систем: прежде чем тратить средства на такое обновление, следует тщательно оценить, какие преимущества принесет эта операция и будут ли оправданы затраты.

> ***Примечание***
>
> Определенным стимулом для западных пользователей является наличие поддержки операционных систем изготовителем. Однако, учитывая, что российские пользователи практически не прибегают к такому сервису, данный факт не может быть серьезным основанием для замены операционных систем новыми версиями.

Сеть с централизованным управлением

В средних и больших организациях для упрощения управления сетью создают систему централизованного управления. Для этого параметры учетных записей хранят централизованно (службы каталогов), а на всех системах производят регистрацию общих групп пользователей.

В случае Windows — централизованное управление реализуется путем создания *доменов Windows*.

В доменах Windows каждый компьютер "теряет" свою автономность, он начинает управляться не только локальным администратором, но и администратором домена.

Управление локальными ресурсами

Для того чтобы централизованно управлять компьютером, на нем необходимо осуществить ряд настроек. Эти операции выполняются при *включении компьютера в домен*. Их можно выполнить как для рабочих станций с операционной системой Windows, так и с Linux.

Обычно систему добавляют в домен с локальной консоли. Данная операция включена в меню свойств компьютера на вкладке сетевой идентификации. Она должна

выполняться с правами локального администратора. Кроме того, необходимо знать идентификационные данные (имя пользователя и пароль) учетной записи, которая имеет право добавлять компьютеры в домен.

> ***Примечание***
>
> Операцию можно выполнить из командной строки с помощью утилиты `netdom` (`netdom join ComputerName /Domain DomainName /UserD DomainUserUPN /PasswordD * /User0 ComputerAdminUser /Password0 * /Reboot`). Эта программа позволяет осуществить операцию подключения и *удаленно*. Однако первоначальная установка Windows имеет политику безопасности, разрешающую *только* локальное выполнение данной операции.

Возможность добавлять рабочие станции в домен

Начиная с ОС Windows 2000, право добавлять рабочие станции в домен предоставлено обычным пользователям домена. Но с ограничением — не более десяти станций. В некоторых случаях желательно разрешить пользователю превысить этот лимит.

Обычные рекомендации для изменения такого лимита сводятся к тому, чтобы отредактировать права доступа к объекту Подразделение (Organization Unit, OU): предоставить конкретному пользователю право создания объектов типа "компьютер" и модификации его атрибутов. Операция легко выполняется настройкой соответствующих свойств безопасности для OU в оснастке управления AD (Active Directory, служба каталогов). Но это не единственная возможность и далеко не лучшая.

Если необходимо изменить лимит, установленный для *всех* пользователей, то следует модифицировать атрибуты объекта службы каталогов. Количество рабочих

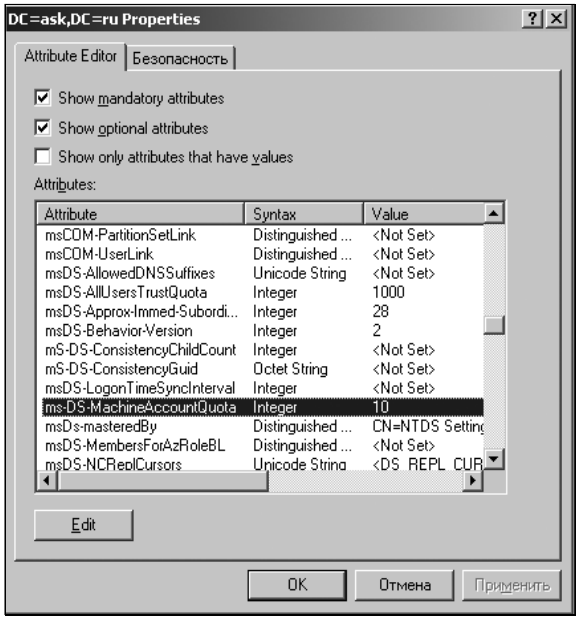


Рис. 4.1. Изменение квоты на добавление компьютеров в домен

станций, которое пользователь может добавить в домен, определяется атрибутом ms-DS-MachineAccountQuota объекта "домен". Для его изменения достаточно воспользоваться программой ADSI Edit и установить желаемое значение (рис. 4.1). Установка значения этого параметра в 0 предоставляет пользователям право добавлять в домен *неограниченное* количество компьютеров.

Более целесообразно не пускать создание новых систем в домене "на самотек". Администратору следует создать объекты типа "компьютер" в службе каталогов и предоставить право подключения данных компьютеров в домен соответствующим пользователям, для чего следует в момент их создания выбрать опцию **Изменить** и определить пользователя, которому будет предоставлено такое право (рис. 4.2).

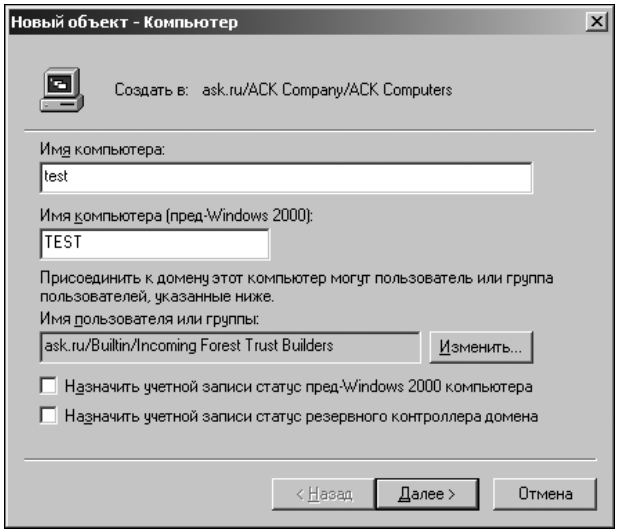


Рис. 4.2. Создание объекта "компьютер" с делегированием его подключения к домену

Удаление устаревших записей о компьютерах и пользователях

В процессе эксплуатации старые компьютеры заменяют новыми путем простого добавления в домен новой системы. При этом учетные записи старых компьютеров продолжают храниться в службе каталогов. Аналогичная ситуация и с учетными записями пользователей: для новых работников создаются учетные записи, но при увольнении сотрудников блокировка (с последующим удалением) их учетной записей не выполняется.

Определить такие устаревшие записи легко: в службе каталогов хранится информация о последнем входе соответствующей учетной записи в домен. Нужно просто выбрать из всего списка те записи, у которых период неактивности больше некоторого значения.

Удобно сделать это с помощью утилиты dsquery, команда запуска которой имеет специальный ключ — `inactive`. Например, так можно вывести на экран список пользователей, не работавших в течение последних 4 недель:

```
dsquery user -inactive 4
```

Примечание

При большом числе устаревших объектов для автоматизации процесса вывод данной команды можно направить по конвейеру на команду удаления из службы каталогов. Хотя, мне кажется, лучше контролировать такие операции вручную.

Изменения настроек системы при подключении ее к домену

При добавлении станции в состав домена производится ряд изменений настроек Windows.

Во-первых, назначаются новые ресурсы для совместного использования. Предоставляются для совместного использования корневые каталоги локальных дисков (под именами C$, D$ и т. д.), каталог установки системы (ADMIN$), создается совместный ресурс IPC$ (используется для установки соединений по именованному каналу — *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 ресурсы совместного использования, имя которых заканчивается знаком $). Если вы попытаетесь удалить их, то после перезагрузки системы они вновь восстановятся. Настройкой реестра системы эти ресурсы можно отключить.

Во-вторых, 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.

Примечание

При входе пользователей домена на рабочую станцию система использует данные учетных записей (имя, пароль, установленные ограничения и т. п.), хранимые на контроллерах домена. Обычно политикой безопасности разрешено кэширование нескольких паролей пользователя, что позволяет последнему войти в систему даже при отсутствии связи с контроллером домена, используя параметры последнего входа. Если работу начинает локальный пользователь, то данные берутся из локальной базы учетных записей.

"Кто кого": локальный или доменный администратор

Централизованное управление порой вызывает у некоторых пользователей негативную реакцию. При этом опытные пользователи вполне могут наложить ограничения на реализацию тех или иных функций управления. Рассмотрим некоторые такие возможности.

Примечание

Опытный пользователь, работающий на локальном компьютере, всегда может получить пароль локального администратора, необходимый для выполнения описываемых операций, использовав, например, способы восстановления пароля администратора.

- **Исключение компьютера из домена.**

  Один из самых эффективных способов блокирования централизованного управления — это исключение локальной системы из домена. Достаточно отключить компьютер от сети, в свойствах системы изменить ее сетевую идентификацию — вместо домена указать *одноименную* рабочую группу. Мастер идентификации выдаст сообщение о невозможности удаления учетной записи компьютера в домене, но успешно завершит все локальные операции.

  После чего необходимо создать локального пользователя, имя которого и пароль *совпадают* с данными пользователя домена. В результате пользователь сохранит практически всю функциональность работы в сети, но исключит любое централизованное управление.

  "Технически" противостоять такому решению весьма сложно. Ограничения, которые может накладывать администратор домена для исключения такого варианта, должны основываться на анализе членства *учетной записи компьютера* в домене. Практически единственный способ — это включение политики ipsec и настройка ее на разрешение сессий *только* с членами домена. Однако такой вариант неприменим в случае наличия в сети рабочих станций с операционными системами предыдущих версий, которые также не являются членами домена.

- **Отключение совместного использования административных ресурсов.**

  Локальный пользователь может отключить создание административных ресурсов, если добавит параметр

  ```
  AutoShareWks : DWORD = 0
  ```

  в ветвь реестра

  ```
  HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
  ```

  (Для восстановления необходимо удалить этот параметр.)

  Следует учитывать, что отключение этих ресурсов может нарушить работу имеющейся в домене системы управления.

- **Исключение администратора домена из группы локальных администраторов.**

  Поскольку локальный администратор имеет полные права над своей системой, то он может ограничить администратора предприятия, исключив его из группы локальных администраторов. В системах с Windows NT 4.0 против такого решения практически не было "противоядия". С Windows 2000 и далее появилась возможность регулировать членство в группах с помощью групповых политик. Хотя практика контроля состава групп локальных администраторов вызывает крайнее недовольство рядовыми пользователями, но администратор предприятия может самостоятельно определить список членов этой группы.

  Блокировать такой вариант можно, только приняв меры по недопущению применения групповой политики для данной системы (блокировав порты на

транспортном уровне), но работа полученной системы будет существенно затруднена.

- **Блокировка администратора домена на уровне файловой системы.**

  С помощью ограничений доступа к файлам локального компьютера можно запретить, например, конкретным администраторам домена локальный вход в систему. Для этого следует установить для учетной записи такого администратора запрет доступа к файлам nddagnt.exe, userinit.exe, win.com, wowexec.exe. Выполнять операцию следует внимательно, чтобы случайно не запретить доступ, например, самому себе.

  Примечание

  Данная рекомендация может быть использована также при приеме на работу нового администратора. Поскольку в системе нет штатных средств ограничения локального входа администратора, то это, по сути, единственный способ защиты наиболее ответственных участков от непрофессиональных действий нового, непроверенного работника.

Конечно, данное ограничение нельзя рассматривать всерьез, поскольку, например, групповой политикой (если не заблокировать ее) администратор домена может восстановить права доступа к значениям по умолчанию.

- **Блокирование групповой политики.**

  Поскольку основное управление осуществляется через применение групповых политик, то целью локального администратора может являться изменение ограничений, налагаемых групповой политикой, или полная ее блокировка.

  Примечание

  В доменах Windows 2003 по умолчанию групповая политика не загружалась на медленных каналах связи. А поскольку для определения скорости канала использовалась оценка времени ответа на команду `ping`, то блокировка таких пакетов была самым простым методом отключения применения групповой политики. Во-первых, локальный администратор может переопределить параметры, установленные групповой политикой. Групповая политика для компьютера применяется при старте системы, а для пользователя — в момент его входа в сеть. Впоследствии система периодически проверяет изменения настроек групповой политики и применяет *только* обнаруженные *изменения* в групповой политике. Конечно, можно задать периодическое применение *всех* параметров групповой политики. В этом случае параметры, занесенные локальным администратором, будут вновь переписаны на централизованные. Но администраторы домена редко используют такие настройки, поскольку это существенно увеличивает нагрузку на контроллеры домена.

  Поэтому если параметр настройки доступен для изменения локальным администратором, то он будет сохраняться в этом измененном состоянии фактически *до следующей перезагрузки системы*. А компьютер можно не перезагружать весьма долго...

  Во-вторых, можно заблокировать применение *всех* политик, сохранив членство компьютера в домене. Например, поскольку групповые политики копируются в виде файлов с контроллеров домена (из папок SYSVOL), то можно создать такую настройку ipsec, которая будет блокировать SMB-трафик с контроллеров домена ("закрыть" порты 137, 139, 445).

Способы, к которым может прибегнуть локальный администратор для ограничения возможностей своего доменного коллеги, можно перечислять еще долго. Данная проблема имеет только одно принципиальное решение — это организационные меры, когда подобные действия локального администратора повлекут за собой "воспитательные меры" руководителей подразделений.

Проблема аудитора

Серьезные проблемы безопасности в Windows создает наличие у администратора (как локального, так и всей сети в целом) полных и единоличных прав над своей системой. Поэтому он может выполнить какие-либо операции в системе, а потом попытаться их скрыть, замаскировав тем или иным способом. Например, переписав журнал протокола. Это создает потенциальные бреши в системе безопасности. Для исключения подобных действий в сетевых системах (например, в сетях Novell) обычно имеется специальный *аудитор* — пользователь, который не имеет административных прав, но может протоколировать *любые* действия. Причем даже администратор не имеет технической возможности изменить состояние файлов протоколов. Иными словами, скрыть свои операции.

Возможный вариант решения данной проблемы в рамках систем, построенных исключительно на Windows, — это сбор данных протоколов работы компьютеров в реальном времени на отдельную, изолированную рабочую станцию. В этом случае принципиально останется возможность сравнения данных работающих систем и архивов аудита. Администратору доступно много программ, реализующих данную функцию, найти которые в Интернете не предоставляет особого труда.

Методы управления локальной системой

После добавления рабочей станции в домен администратор домена получает над ней фактически неограниченную власть.

Какие возможности управления есть у администратора?

Во-первых, имеющиеся в системе оснастки (например, Управление компьютером) позволяют — при наличии соответствующих прав — управлять не только локальной системой, но и любой удаленной. Так, администратор может останавливать и запускать службы, просматривать протоколы работы системы, создавать удаленных локальных пользователей и менять их членство в группах и т. п. Операции достаточно понятные и не требуют особого объяснения. Нужно только выполнить подключение соответствующей оснастки к удаленному компьютеру (рис. 4.3).

На практике подобные инструменты администратора используются только для индивидуальных настроек. Применение их нерационально, если настройки надо выполнить, например, с десятком компьютеров.

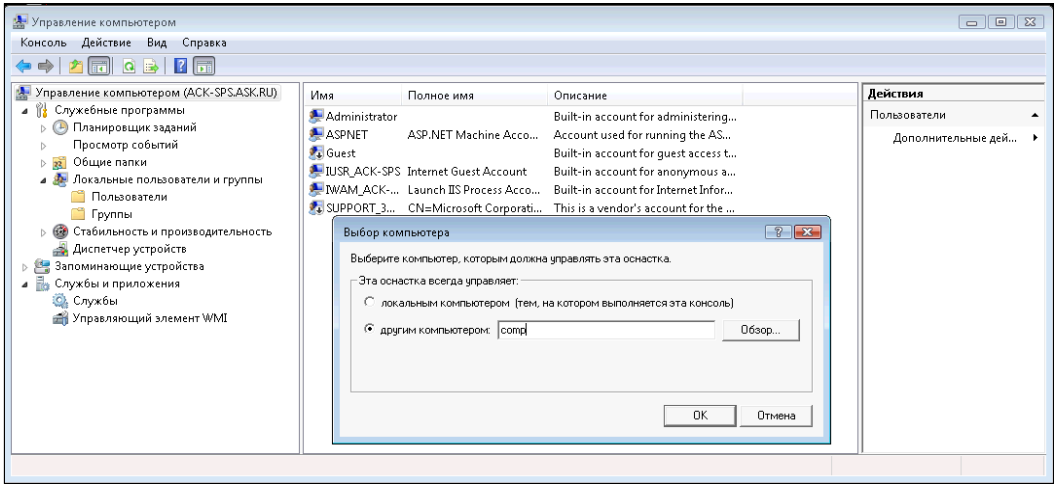


Рис. 4.3. Подключение оснастки управления к удаленному компьютеру

Во-вторых, каждый пользователь при регистрации в домене на компьютере — члене домена[1] вызывает исполнение *сценария входа в систему*. Необходимость выполнения сценариев определяется в свойствах учетной записи пользователя на вкладке **Профиль**. Достаточно создать желаемый сценарий, который должен выполняться при начале работы пользователя, сохранить его в папке Scripts на контроллере домена и назначить пользователям.

В Windows NT 4.0 пользователь мог прервать выполнение сценария входа в систему (например, во время исполнения пакетного файла нажать комбинацию клавиш <Ctrl>+<C>). Начиная с Windows 2000, выполнение сценария по умолчанию осуществляется скрыто. Хотя администратор может с помощью групповой политики включить отображение выполнения команд (**Конфигурация Windows | Административные шаблоны | Система | Сценарии**) и выбрать синхронный (пока сценарий не будет выполнен до конца, пользователь не начнет работу в системе) или асинхронный вариант выполнения сценария.

Поскольку в последних версиях Windows возможности управления из командной строки существенно расширены, то с помощью подобных сценариев можно выполнять практически любые действия: подключать сетевые диски в зависимости от членства пользователя в группе безопасности или в OU, переопределять принтеры, осуществлять копирование файлов и т. п.

Преимущество этого способа управления — выполнение сценария при каждом входе в систему и максимальная простота настройки (например, создали один сценарий и настроили его выполнение для всех пользователей). Недостаток — сценарии выполняются от имени учетной записи пользователя. Если пользователь не

[1] Групповые политики позволяют задать выполнение сценария входа для *компьютера*. Но на практике автор не встречался с использованием таких сценариев, поскольку обычно администраторы больше используют сценарии входа пользователей и групповые политики.

имеет административных прав, то в сценарии не будут выполняться команды, требующие наличия прав на управление системой.

Третий способ управления — самый распространенный — использование групповых политик для Windows 200*x*/XP/7. Число настроек, которыми можно управлять с помощью групповых политик, исчисляется тысячами. При этом можно настраивать не только параметры операционной системы, но и основных приложений. Можно осуществлять контроль запуска приложений, настраивать параметры безопасности транспортного протокола, распространять параметры приложений по умолчанию и т. п.

Примечание

Использование групповых политик будет рассмотрено в *главе 6*.

В-четвертых, для управления компьютерами администратор может создавать собственные программы. Конечно, для этого требуется некоторые познания в программировании и опыт, но так можно, например, собрать и проанализировать любые данные, выполнить желаемую настройку на любом числе компьютеров. Преимуществом способа является и полный контроль над ходом выполнения: вы запускаете программы в то время, когда это необходимо.

Проще всего использовать для создания собственных программ имеющиеся в системе средства программирования. Можно выполнять задания в командной строке. Но функционал этих команд ограничен. Большие возможности предоставляют Visual Basic, WMI и PowerShell. С помощью этих средств администратор легко может составить желаемые *сценарии*.

Чтобы сценарии выполнились на компьютере, на нем должна быть установлена соответствующая система. Например, для запуска Visual Basic — Windows Scripting Host, для сценариев ps — оболочка PowerShell. Не все операционные системы поддерживают этот функционал при установке с параметрами по умолчанию.

Примечание

Некоторые основы составления сценариев описаны в *главе 6*.

Служба каталогов

Информационные системы обычно создаются для организаций, обладающих четкой структурой. При реализации тех или иных бизнес-действий в обязательном порядке должны учитываться права пользователей, их подчиненность и т. п. Поэтому структура компьютерной информационной системы, как правило, должна создаваться по образу и подобию организационной структуры предприятия.

Средством описания такой структуры являются *каталоги*. Фактически каталоги — это базы данных. Объектами такой базы данных являются пользователи, компьютеры, подразделения, территории, предприятия и т. п. Каждый объект описывается многими 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 с такими

объектами осуществляется 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*.

Стандарты позволяют создавать структуру каталога так, чтобы наиболее полно удовлетворить потребности каждого конкретного случая. Существуют каталоги разработки различных фирм. Но все каталоги поддерживают единые правила взаимодействия с ними. Это протокол *LDAP* (Lightweight Directory Access Protocol, протокол облегченного доступа к каталогам).

Применяя любую утилиту, которая реализует протокол LDAP, пользователь (программа) может соединиться с каталогом и, используя предоставленные права, запросить или записать информацию, выполнить другие допустимые операции. При этом изменения, вносимые в каталог, могут привести к существенной перестройке всей структуры компьютерной сети. Так, перемещение одного объекта `Подразделение` может привести к изменению десятков и сотен характеристик подчиненных объектов (вложенных подразделений, компьютеров, пользователей).

Служба каталогов Windows (Active Directory)

Описанный ранее каталог реализован в Windows (начиная с Windows 2000) как *служба каталогов* (Active Directory, AD). Служба каталогов Windows имеет в своей структуре такие единицы, как:

- ❒ лес;
- ❒ дерево;
- ❒ домен;
- ❒ организационное подразделение (Organization Unit, OU);
- ❒ сайты.

Хотя многие методы управления сетью в Windows базируются на службе каталогов (например, групповые политики), все же существенная часть операций унаследована исторически. Например, группы безопасности существуют отдельно от подразделений. И если вы меняете членство пользователя в подразделении, то для последующей коррекции его прав доступа необходимо дополнительно вручную изменить группу безопасности, в которую входит пользователь.

Служба каталогов хранит много информации, которая может быть полезной администратору, но не доступна явно в графических средствах управления. Оснастка Active Directory (AD) включает возможность поиска по службе каталогов. Например, можно найти рабочие станции, установленные средствами разворачивания образов, или пользователей, для которых установлен неограниченный срок действия пароля, и т. п. Каждый раз составлять заново строку поиска[1] неудобно, проще сохранить

[1] Например, даже простой поиск сотрудников, которым разрешен удаленный доступ в сеть, требует ввода запроса (&(&(objectclass=person)(msNPAllowDialin=TRUE))).

часто используемые запросы в самой оснастке и вызывать их по названию. На рис. 4.4 показан пример оснастки с сохраненными запросами (в примере — запрос по системам, развернутым средствами централизованной установки).

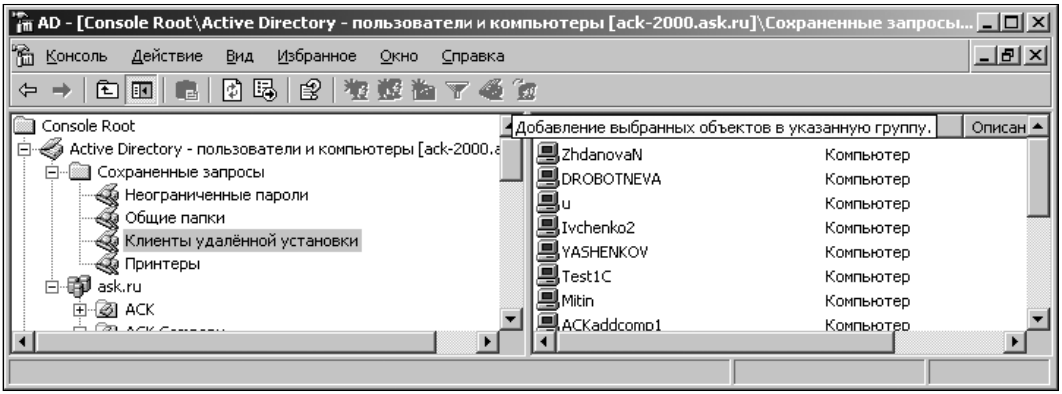


Рис. 4.4. Сохраненные поисковые запросы оснастки службы каталогов

Домены Windows

Исторически иерархические сети на основе Windows создавались на базе *доменов*.

В локальных сетях на базе Windows понятие "домен" используется для обозначения совокупности пользователей и компьютеров, объединенных общими правилами безопасности (централизованная регистрация нового пользователя, единые правила доступа к совместно используемым ресурсам, единые требования по ограничениям времени работы в сети и т. п.). Единая политика безопасности в доменах Windows обеспечивается специально выделенными компьютерами сети — *контроллерами домена*.

> ***Примечание***
>
> Не следует путать термины "домен Windows" и "домен Интернета". Хотя внешне доменная структура Windows и строится аналогично системе имен Интернета, но, говоря о домене Windows, в первую очередь имеют в виду не единую систему имен, а единую политику управления и безопасности.

В одной организации может существовать *несколько* доменов. Это могут быть как *вложенные* домены, так и домены с различными пространствами имен.

> ***Примечание***
>
> *Пространство имен* — это совокупность уникальных имен. В данном пространстве имен по конкретному имени однозначно может быть определен соответствующий ему объект. Типичный пример — структура DNS (Domain Name System, система доменных имен). Например, в пространстве имен различных доменов могут существовать компьютеры с одинаковым именем хоста: test.primer.org и test.primer2.org. Однако в пространстве имен NetBIOS одинаковых наименований компьютеров быть не может. Поэтому при объединении таких компьютеров в единую локальную сеть вам необходимо будет дать им различающиеся NetBIOS-имена.

Наличие в одной организации доменов с отличающимися именами характерно для транснациональных организаций. Например, головное предприятие может иметь домен testorg.ru, а его подразделение в другой стране — testorg.cs.

В то же время создание *вложенных* доменов не имеет особого смысла при проектировании информационной структуры предприятия. Подобная структура оправдана только для доменов Windows 2003 в том случае, если для некоторого подразделения необходима иная политика паролей учетных записей (например, более строгие требования к составу пароля, наличие блокировок и т. п.; в Windows 2008 свойства паролей стали полностью управляться групповой политикой). Все другие настройки могут быть выполнены политиками подразделений.

Подразделение

Домены Windows (начиная с версии Windows 2000) могут содержать *подразделения* (Organization Unit, OU). OU — это своеобразный контейнер, в который можно помещать как компьютеры, так и пользователей (очевидно, что речь идет о соответствующих логических объектах).

Основная причина создания OU для администраторов системы — это возможность применения к объектам OU *групповых политик (см. главу 5)*. Повторюсь, что групповые политики — это основное средство управления компьютерной сетью. С их помощью можно автоматически устанавливать на заданные компьютеры программное обеспечение, выполнять настройку прикладных программ, менять параметры безопасности сегмента сети, разрешать или запрещать запуск конкретных программ и т. п.

Каждое OU может, в свою очередь, содержать внутри себя любое количество вложенных OU, учетные записи компьютеров и пользователей, группы (пользователей). Если попробовать изобразить графически такую структуру — домен с несколькими вложенными доменами со структурой OU, пользователями и компьютерами, то такой рисунок будет напоминать *дерево* с вершиной, ветвями, листьями. Этот термин и сохранен для описания такой структуры.

> ***Примечание***
>
> Обратите внимание, что при удалении OU будут удалены и содержащиеся в нем объекты (например, учетные записи компьютеров — компьютеры уже не будут членами домена).

Лес

Если на одном предприятии существуют 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 200x, объединенных общей схемой, конфигурацией и двусторонними транзитивными доверительными отношениями.

Обратите внимание, что деревья в таком лесу не самостоятельны. Все эти деревья создаются *внутри одной организации* и управляются централизованно администра-

торами предприятия. Говоря терминами логической организации сети, между любыми доменами внутри предприятия существуют *доверительные двусторонние отношения*.

Практически это означает, что администратор предприятия является "начальником" администратора любого домена, а пользователь, прошедший аутентификацию в одном домене, уже "известен" в другом домене предприятия.

> ***Примечание***
>
> Многие администраторы доменов в структуре леса заблуждаются, считая что только они могут управлять безопасностью объектов. Даже если они явно запретили доступ каким-либо пользователям, то владелец корневого домена (леса) Windows *всегда* имеет возможность получить доступ к объектам и назначить собственные права. Иными словами, в сети с централизованным управлением необходимо полностью доверять тем администраторам, которым принадлежат корневые права.

Сайты

Если домены и OU описывают логическую организацию, то *сайты* (Sites) предназначены для описания *территориальных делений*. Считается, что *внутри одного сайта* присутствуют скоростные каналы связи (обычно компьютеры сайта находятся 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 используемый протокол (IP или путем приема/передачи сообщений по протоколу SMTP) и т. п.

Соотношение территориальной и логической структуры выбирается из конкретной конфигурации предприятия. Например, можно создать несколько сайтов в одном домене или сформировать в каждом сайте свой домен и т. п.

> ***Примечание***
>
> Поскольку алгоритм выбора контроллера домена рабочей станцией использует структуру сайтов, то создание дополнительных сайтов может быть способом балансировки нагрузки между контроллерами домена.

Режимы совместимости доменов и леса

Домены Windows могут обслуживаться контроллерами на базе операционных систем Windows NT 4.0 Server или Windows 200*x*. Более новая операционная система обеспечивает большие возможности в управлении доменами и большую безопасность. Однако в целях обратной совместимости домены Windows могут работать в различных *режимах* (mode). Если в вашей сети нет контроллеров на базе предыдущих версий ОС, то следует перевести домен в режим наибольшей безопасности.

Данная операция доступна в свойствах домена в оснастке управления, а для леса — в соответствующей оснастке управления сайтами и службами (в свойствах соответствующего объекта).

DN, RDN

Для успешной работы с каталогами необходимо ориентироваться в терминах DN (Distinguished Name, отличительное имя) и RDN (Relative Distinguished Name, относительное отличительное имя).

Объекты каталога хранятся в иерархической структуре. Условно можно сравнить такую структуру со структурой файловой системы. Есть корневой каталог, есть вложенные в него каталоги, в них, в свою очередь, могут храниться как сами файлы, так и другие папки. В этой аналогии термин DN подобен *полному пути имени файла*. В DN приводится полный путь к объекту, начиная с самой "верхней" точки иерархии каталога.

RDN подобен *относительному* пути к файлу. Это может быть только само имя файла (обычный RDN) или относительный путь (многоатрибутный RDN). Например, в организации может быть заведен пользователь `Иванов`. Если в организации в разных отделах работают два Иванова, то только по фамилии невозможно будет определить конкретного работника. Но если использовать многоатрибутный RDN, состоящий, например, из фамилии и названия отдела, то работник будет обозначен точно:

```
cn = Иванов + ou = Бухгалтерия
```

Управление структурой домена предприятия

При проектировании логической структуры компьютерной сети организации следует учитывать многие факторы: решаемые задачи, требования безопасности, количество офисов, квалификацию обслуживающего персонала и т. п.

В небольших организациях не имеет особого смысла создание разветвленной логической структуры сети, поскольку обычно внутри организации применяются только одна или две групповые политики. С увеличением численности компьютерных систем структура становится все более сложной.

В большинстве случаев логическая структура домена будет "следовать" за организационной структурой предприятия. На малых и средних предприятиях обычно не возникает задача оптимизации количества и размещения контроллеров домена (ситуация с удаленным офисом будет обсуждена в *главе 5*). Если исходить из критериев мощности компьютера, то производительности одного сервера обычно вполне достаточно для обслуживания нескольких сотен рабочих станций. Однако в целях резервирования целесообразно иметь в сети не менее двух контроллеров, чтобы временные неисправности на одном из них не отразились на функционировании предприятия.

Создание нового домена

Для создания нового домена необходимо запустить утилиту dcpromo (ее можно стартовать также из задачи управления сервером, выбрав в меню пункт создания контроллера домена). 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.

> ***Примечание***
>
> Естественно, что для выполнения операций пользователь должен обладать соответствующими правами. Так, для создания нового дерева доменов предприятия операцию необходимо выполнять с правами администратора предприятия.

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. 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. Ничто не запрещает вам избрать для внутреннего домена имя, которое не соответствует реальным доменам Интернета, например, дать название myorg.local.

> ***Примечание***
>
> Проследите, 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. Если сервер DNS не настроен, по умолчанию программа установки предлагает создать и настроить сервер DNS локально. В общем случае служба каталогов не требует обязательного использования 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.

> ***Примечание***
>
> SRV-запись на сервере DNS позволяет клиенту узнать расположение сервера, обслуживающего соответствующую службу. SRV-записи для Microsoft-доменов строятся по форме _Service ._ Protocol . DnsDomainName. Например, адреса LDAP-серверов домена могут быть запрошены по имени _ldap._tcp.*имя_домена*, а адрес сервера глобального каталога конкретного леса в домене — как _ gc._tcp.*имя_леса*.

Особенности создания дополнительного удаленного контроллера в домене Windows

После создания нового контроллера домена программа пытается выполнить его синхронизацию с другими контроллерами. Объем данных, передаваемый в этой операции по сети, обычно составляет десятки мегабайт, а в средних организациях может превышать и несколько сотен мегабайт. Поэтому установку контроллеров

для филиалов, подключенных через медленные каналы связи, лучше выполнять непосредственно в центральном офисе. После первоначальной синхронизации компьютер можно выключить и перевезти на удаленную площадку. Объем синхронизуемых данных, которые будут переданы после включения компьютера в удаленном офисе, в этом случае будет существенно ниже объема первоначальной синхронизации и не создаст критической нагрузки на каналы связи.

В Windows 2003 введена новая возможность при создании контроллера домена — это выполнение первоначальной синхронизации из файлов резервного копирования.

Для создания нового контроллера необходимо сначала выполнить резервное копирование состояния (system state) любого контроллера домена, после чего полученные файлы резервной копии любым способом передать в удаленный офис (например, нарезать на CD-матрицы). В удаленном офисе следует восстановить эти данные *в другое место* (выбрать папку для восстановления при запуске операции). Затем запустить утилиту dcpromo с помощью одноименной команды `dcpromo` с ключом `/adv`. При таком варианте ее запуска на одном из шагов появится дополнительная опция, запрашивающая место, откуда следует провести загрузку первичных данных (рис. 4.5). Вам достаточно указать папку, в которую было проведено восстановление данных с контроллера домена. В завершение операции система проведет синхронизацию последних изменений службы каталогов.

Эта возможность позволяет существенно сократить объем реплицируемых по каналам связи данных.

Примечание

Для проведения операции создания нового контроллера домена при *любом варианте* необходимо иметь связь с действующими контроллерами домена (для проверки прав и внесения необходимых изменений в схему организации).

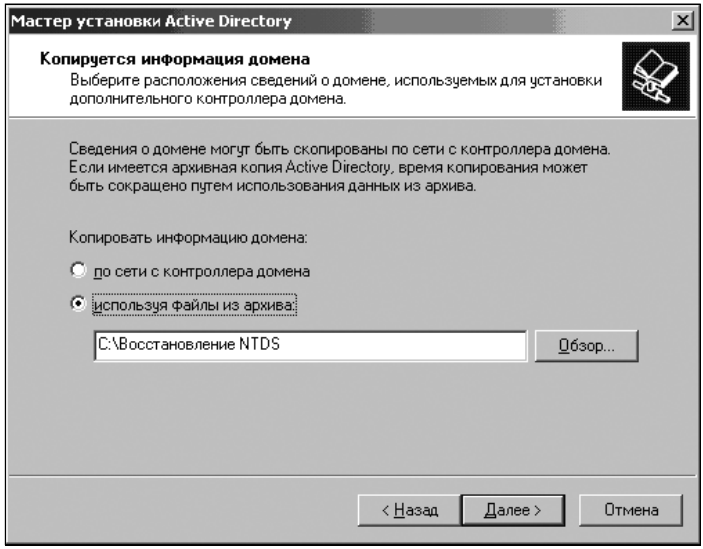


Рис. 4.5. Копирование данных контроллера домена из архивной копии

Создание контроллеров домена "только для чтения"

В удаленных филиалах могут быть установлены *контроллеры домена* Windows 2008 *только для чтения* (RODC — Read Only Domain Controller). Данный вариант позволяет снизить риск дискредитации данных всего домена в случае доступа злоумышленника к контроллеру в филиале.

Способы создания RODC описаны в *главе 5*.

Удаление контроллера домена

Штатное удаление контроллера домена производится с помощью той же утилиты dcpromo. Ее следует запустить на компьютере, роль которого предполагается понизить до обычного сервера. Указав необходимые параметры операции (например, пароль будущего локального администратора), администратору нужно только дождаться сообщения о требуемой перезагрузке системы. Для успешного завершения операции компьютер должен иметь связь с другими контроллерами (если это не последний контроллер домена).

Бывают ситуации, когда контроллер выходит из строя, например из-за неполадок в оборудовании, и его не планируется восстанавливать из резервной копии. В таком случае необходимо удалить из службы каталогов все записи, которые связаны с этим контроллером. Для этого штатно используется утилита ntdsutil.

> ***Примечание***
>
> В новых версиях Windows Server графические утилиты пополнены опциями удаления контроллера, однако описываемый в тексте способ может пригодиться при работе в доменах предыдущих режимов.

Опишем последовательность шагов, которые необходимо выполнить в данной утилите для удаления отсутствующего контроллера домена.

1. После запуска утилиты на экране появится окно ее интерфейса. Вам необходимо перейти к опции **metadata cleanup**.
2. Теперь нужно подключиться к работающему контроллеру домена (**connections | connect to server <*имя*>**), на котором мы будем выполнять операцию удаления метаданных.
3. После подключения к контроллеру снова возвращаемся в режим **metadata cleanup**. На этом шаге необходимо выбрать тот контроллер, данные о котором предполагается удалить.
4. Набираем команду **Select operation target**, после перехода в этот режим последовательно подключаемся к ресурсам организации. Например, чтобы указать на конкретный сервер, сначала нужно будет просмотреть список сайтов (**List sites**), после чего подключиться к нужному сайту (**Select site <*номер, полученный на предыдущем шаге*>**). Затем просмотреть список доменов и подключиться к нужному и т. д. В завершение после выполнения команды `List servers for domain in site` вы увидите нумерованный список серверов. Вам нужно выбрать тот сервер, который предполагается удалить (**Select server <*номер*>**), и вернуться в меню **metadata cleanup**.

5. В меню **metadata cleanup** дать команду на удаление параметров выбранного сервера (**Remove selected server**).

Переименование домена

Имя домена Windows невозможно сменить для доменов на основе операционных систем Windows NT 4.0 Server/Windows 2000 Server. Для доменов, работающих в режиме Windows 2003 и старше, такая возможность появилась, и автору приходилось ее выполнять. Но эта операция весьма ответственна и не всегда в ходе ее осуществления могут быть изменены все наименования. Например, сертификаты, выданные на старые имена, окажутся недействительны, придется менять настройки почтового сервера и т. п.

Операция переименования требует тщательной подготовки. Последовательность действий администратора для переименования домена изложена в документе Introduction to Administering Active Directory Domain Rename технической библиотеки Microsoft по адресу **http://technet.microsoft.com/en-us/library/cc816848%28WS.10%29.aspx**.

Утилиты управления объектами службы каталогов

Управление доменом может проводиться не только с серверов Windows. При наличии соответствующих прав большинство операций может быть выполнено удаленно с рабочих станций. Для этого необходимо установить пакет администрирования.

Пакет администрирования Adminpak.msi для серверов Windows 2003 поставлялся с дистрибутивом сервера и мог быть установлен на рабочие станции Windows XP. Для серверов Windows 2008 средства удаленного управления стали называться Remote Server Administration Tools for Windows 7 и доступны к загрузке со страницы **http://go.microsoft.com/fwlink/?LinkID=137379**. Особенности установки пакета подробно описаны в технической библиотеке в документе **http://technet.microsoft.com/en-us/library/ee449483%28WS.10%29.aspx**.

Стандартные средства для удаленного управления структурой службы каталогов повторяют возможности оснасток управления на сервере — это оснастки управления пользователями и компьютерами, доменами и доверием, сайтами и службами. Как в случае любой графической утилиты, этими программами удобно и быстро можно выполнять типовые операции, для которых они были разработаны. В нашем случае — это операции создания пользователей и подразделений, назначение им свойств, перемещение пользователей, компьютеров и подразделений между различными контейнерами и т. п.

Выполнение данных операций с помощью указанных оснасток достаточно прозрачно, все проблемы администратор легко решит с помощью справочной системы.

Утилиты запросов командной строки службы каталогов

В системе присутствует несколько утилит, которые позволяют в режиме командной строки выполнить простейшие операции со службой каталогов Windows: поиск

объектов по заданным критериям, добавление и удаление объектов, их перемещение и т. п. Это команды `dsquery` (выполняет поисковые запросы к службе каталогов), `dsadd` (добавляет новые объекты), `dsget` (отображает параметры объектов), `dsmod` (изменяет параметры объектов), `dsmove` (перемещает объекты), `dsrm` (удаляет объекты).

Например, с помощью команды `dsquery` можно легко получить список компьютеров, не работавших в сети в течение какого-либо периода времени:

```
dsquery computer -inactive 5
```

где 5 — число недель, в течение которых компьютер не входил в сеть.

Утилита *csvde* позволяет импортировать/экспортировать объекты в формате CSV. Этот формат удобен для последующего анализа, например, в Excel. Синтаксис команды аналогичен описываемому далее для Ldifde. Особенность использования команды `csvde` состоит в том, что с ее помощью можно добавлять объекты, но нельзя изменять их атрибуты или удалять существующие объекты.

LDAP-управление

Служба каталогов Windows представляет собой иерархическую структуру, управление которой может осуществляться не только оснастками, но и с использованием различных способов прямого доступа к данным. Например, администратор может получить доступ к объектам службы каталогов с использованием сценариев на Visual Basic, применяя запросы ADO и т. п.

Поскольку служба каталогов поддерживает протокол LDAP, ставший стандартом для доступа к подобным службам, то для управления структурой домена удобно применять утилиты, реализующие подключение по этому протоколу.

Подключаемся к каталогу по протоколу LDAP

Во-первых, можно использовать оснастку ADSI Edit (рис. 4.6). С помощью этой оснастки можно подключиться к любому узлу структуры службы каталогов, увидеть его атрибуты, при необходимости отредактировать их и установить желаемые права доступа. Оснастка позволяет создавать новые объекты в структуре каталогов, удалять существующие, перемещать их и т. п.

> ***Примечание***
>
> Обратите внимание, что с помощью этой оснастки можно подключиться к любой точке структуры каталогов, а не только к элементам Domain, Configuration, Schema. Достаточно указать соответствующие параметры в меню программы.

Во-вторых, при установке Support Tools в систему добавляется утилита ldp.exe, которая позволяет подключаться к службам по протоколу LDAP, добавлять и удалять объекты, редактировать их, выполнять поиск. Утилита несколько необычна в использовании, поскольку предполагает первоначальные знания администратором структуры каталогов. При ее запуске следует выполнить подключение к службе в нужной точке *(connect)* и зарегистрироваться *(bind)*.

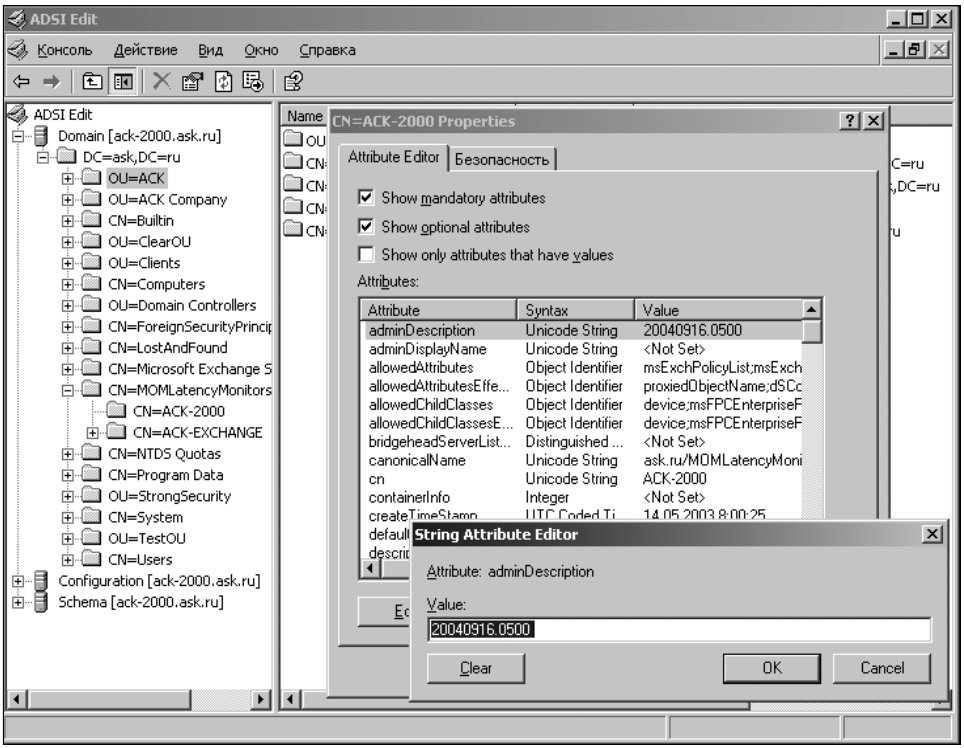


Рис. 4.6. Утилита ADSI Edit

Конечно, применять утилиту ldp.exe в случаях, когда можно, например, использовать графические оснастки, не имеет смысла. Но эта утилита позволяет выполнять операции *с объектами* службы каталогов с использованием синтаксиса LDAP-протокола. Например, первоначально ldp.exe являлась единственным бесплатным вариантом восстановления удаленных объектов каталога.

Ну и в-третьих, в Сети доступно много средств, в которых реализованы возможности подключения и управления системой по протоколу LDAP и которые могут оказаться для администратора более удобны в применении.

Синтаксис поисковых запросов LDAP

Чтобы правильно составить запрос к службе каталогов, необходимо изучить основы LDAP-синтиксиса.

В службе каталогов информация хранится в виде объектов. Для обозначения *свойств* объектов (по терминологии Microsoft) в стандартах LDAP применяется термин *атрибуты*.

Чтобы выбрать нужные данные из службы каталогов, необходимо составить *фильтр*. В LDAP используются специальные конструкции для фильтров, в которых оператор ставится *до* самих величин. Например, если вам необходимо найти всех пользователей с фамилией Иванов, то фильтр следовало бы записать по следующей

форме: `(И(тип=пользователь)(фамилия=Иванов))`. То есть два условия объединены требованием `И`, которое записано *до* условий.

В фильтрах допустимы операторы, перечисленные в табл. 4.1.

Таблица 4.1. *Допустимые операторы фильтров*

Оператор	Описание
=	Равно
~=	Приблизительно равно
<=	Меньше или равно
>=	Больше или равно
&	И
|	ИЛИ
!	НЕТ

Примечание

Некоторые объекты допускают использование поиска по маске (`*`); в общем случае наличие такой возможности следует уточнить по документации.

Если в запросе необходимо использовать символы: "`(`", "`)`", "`*`" и `NUL`, то они должны быть записаны через escape-последовательность так, как указано в табл. 4.2.

Таблица 4.2. *Escape-последовательности*

Символ	Записывается как
*	\2a
(	\28
)	\29
\	\5c
NUL	\00

Примечание

Аналогично через escape-последовательность записываются двоичные данные с разбиением по два байта.

Определенную сложность при первых обращениях к операциям поиска вызывает знание необходимого атрибута, который должен быть использован в операции. Можно порекомендовать просмотреть все атрибуты объекта этого же типа, выбрать нужное свойство и использовать его в запросе. Это можно сделать и в самой программе ldp.exe, если включить отображение вывода в результате поиска *всех* атрибутов. Для этого следует открыть окно поиска, нажать кнопку **Option** и в строку перечня атрибутов ввести звездочку (`*`).

Примечание

Чтобы вернуться к выводу сокращенного списка атрибутов, следует в данной строке перечислить (через точку с запятой) названия тех атрибутов, которые должны отображаться на экране по результатам поиска.

Покажем на небольшом примере, как можно быстро в домене найти пользователя по второму почтовому адресу.

Дополнительные адреса электронной почты, которые присвоены пользователю, перечисляются в атрибуте `proxyaddresses`. Дополним перечень отображаемых атрибутов этим значением (допишем его в строку `Attributes` после точки с запятой) и снимем флажок в параметре `Attributes`, чтобы программа поиска вывела на экран значения атрибутов. Установим в окне настройки фильтра поиска в качестве начальной точки имя нашего домена, а критерием поиска выберем следующую строку:

`(&((objectclass=user)(proxyaddresses=*`*адрес*`*)))`

Она означает, что мы хотим искать только пользователей, у которых один из адресов электронной почты содержит символы `адрес` (в любом месте адреса). Выберем зону поиска по всей базе (SubTree). Выполнив поиск, мы получим на экране необходимые сведения.

Команда *ldifde*

Большая часть системных администраторов предпочитает использовать для конфигурирования серверов текстовые файлы, поскольку с ними удобнее работать, чем с двоичной информацией. Для каталогов существует стандарт LDIF (LDAP Interchange Format, определен в документе RFC 2849), который определяет правила представления данных каталога в текстовом файле.

LDIF-файл представляет собой текстовые строки, в которых приведены атрибуты объектов, их значения и директивы, описывающие способы обработки этой информации. В Windows имеется утилита ldifde (запускаемая одноименной командой), которая выполняет такое преобразование данных из службы каталогов, используемой в Windows, в текст и обратно. Ключи утилиты позволяют уточнить точку подключения, глубину выборки, указать фильтры операции и т. п.

На эту утилиту обычно обращается мало внимания, хотя она может существенно упростить многие административные задачи. Обычно с помощью ldif-файлов выполняется модификация схемы каталога при установке новых приложений.

Предположим, что вам необходимо откорректировать параметры пользовательских учетных записей, например, указать для всех работников некоторого подразделения в свойствах учетных записей название их отдела. Выполнение операции "в лоб" — последовательное открытие учетных записей и вставка нужного описания в соответствующее поле — весьма трудоемко и нерационально при значительном числе сотрудников.

С помощью же данной утилиты можно выполнить экспорт в текстовый файл параметров учетных записей пользователей *только* для заданного подразделения (уста-

новив фильтр по данному OU), после чего с помощью обычного текстового редактора одной операцией поиска и замены откорректировать значения нужных атрибутов. В завершение достаточно выполнить импорт полученного файла. В результате атрибуты для *всех* записей будут откорректированы практически за несколько шагов.

> ***Примечание***
>
> Такая операция также весьма просто выполняется с помощью сценария Visual Basic. Достаточно подключиться к нужному контейнеру, установить фильтр для выборки только объектов типа "пользователь" и запустить цикл для каждого элемента данного типа в этом контейнере. Однако приведенная схема не требует от администратора знания сценариев и может быть выполнена буквально в течение нескольких минут.

Ранее мы рассматривали пример, как с помощью команды `dsquery` получить список компьютеров, длительное время не работавших в составе сети. Приведем второй способ, как можно получить в файл такой список с помощью команды `ldifde`:

```
ldifde -f <имя_файла>.txt -n -d "dc=<имя_домена>,dc=ru" -r
"(&(objectcategory=computer)(|(lastlogon<=127296891259257277)(!lastlogon=*)))" -
p SubTree -l lastlogon
```

В фильтре использовано представление даты в машинном формате. Такие значения легко можно получить при помощи простых операций, например:

```
Dim Time1 As System.DateTime = System.DateTime.Now().AddMonths(-2)
Dim FileTime1 = Time1.ToFileTime
```

Переменная `FileTime1` будет иметь значение, соответствующее дате двухмесячной давности. Необходимо учитывать, что компьютеры, которые не перезагружались в течение этого периода, также будут иметь "старые" значения времени входа в систему. Фильтр также выводит имена компьютеров, для которых отсутствует значение параметра времени входа в систему.

Представленный пример несколько искусственен, поскольку результат может быть получен более простым способом. Но он приведен именно для того, чтобы проиллюстрировать существование различных возможных вариантов действий администраторов.

Делегирование прав

Традиционно системный администратор объединял в себе все текущие функции управления доменом. Он создавал и удалял пользователей, добавлял компьютеры в домен, следил за членством в группах и т. п. Большинство таких рутинных операций без ущерба для функционирования сети может быть переложено на других сотрудников. Например, новые учетные записи пользователей в соответствующем подразделении могут создаваться сотрудником кадровой службы при оформлении приема на работу; компьютеры в домен добавляться сотрудниками технической службы сервиса; разработка групповых политик, предусматривающих установку специализированных программ, вестись техническими специалистами соответствующего отдела; добавление пользователей в группы безопасности — сотрудника-

ми подразделений безопасности и т. п. При этом за администратором предприятия сохранились бы все руководящие функции для возможных экстренных вмешательств, но "освободились руки" для подготовки и реализации стратегических решений.

Для того чтобы осуществить на практике такую передачу прав, которую принято называть *делегированием*, администратору достаточно изменить разрешения безопасности на соответствующий контейнер. Так, если необходимо делегировать кому-либо право создания пользователей, то этому сотруднику следует дать право на создание объекта типа "пользователь" в заданном подразделении. При этом перечень возможных прав доступа для контейнера является настолько подробным, что администратор без труда может настроить объем делегирования (например, дать право добавления в домен компьютеров, но лишить возможности изменения или удаления таких объектов).

Делегирование прав создания учетных записей позволит более тесно "связать" кадровые записи и записи служб каталогов. Учетная запись в этом случае может иметь только минимальные начальные права для входа в систему. Предоставление дальнейших прав по доступу к ресурсам (изменение членства в группах) могут осуществлять менеджеры соответствующих групп.

Большинство утилит графического управления объектами службы каталогов содержат в меню команду *делегирования прав*. Эта команда вызывает мастер, который меняет список прав доступа (рис. 4.7). Запуск данного мастера является самым простым способом делегирования прав на объекты. Но при этом администратору следует учитывать два момента.

Во-первых, всегда можно более точно откорректировать права доступа, если обратиться к редактированию параметров безопасности контейнера *напрямик*.

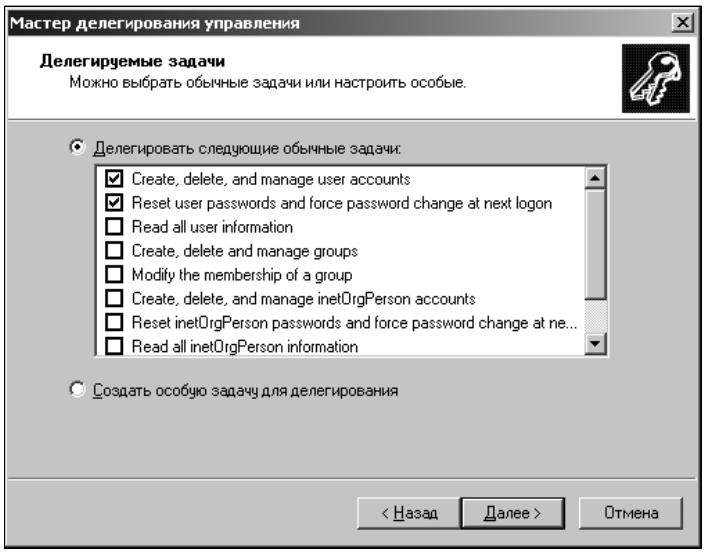


Рис. 4.7. Мастер операций предлагает определить объем делегирования прав

Во-вторых, хотя мастер делегирования прав присутствует в системе, но мастера *отзыва прав* не предусмотрено. Иными словами, если, например, необходимо передать право управления от одного сотрудника другому, то администратору придется вначале *вручную* исключить первого из списка доступа.

Просмотр и восстановление удаленных объектов каталога

Удаленные объекты каталога (например, учетная запись пользователя или компьютера) в домене Windows сначала помещаются в специальный контейнер (аналог Корзины), в котором они сохраняются по умолчанию 60 суток. В течение этого времени данные объекты можно *восстановить*.

> ***Примечание***
>
> Этот интервал можно изменить, если ввести, например с помощью ADSI Edit, новое значение атрибута `tombstoneLifetime` для объекта `cn=Directory Service, cn=Windows NT,cn=Services, cn=Configuration,<DN_корня_леса>`.

Администратор может использовать и утилиту для автоматического восстановления удаленных объектов каталога (см. **http://www.sysinternals.com/Utilities/AdRestore.html**).

Учетные записи и права

Безопасность в операционных системах базируется на понятиях учетной записи и предоставляемых ей прав.

Понятие учетной записи

Программа, которая выполняется на компьютере с установленной операционной системой Windows, 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 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 (Система). 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. 4.8), которые добавляют 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 (см., например, *группы по запросу*).

Стандартные учетные записи имеют 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
```

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 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.

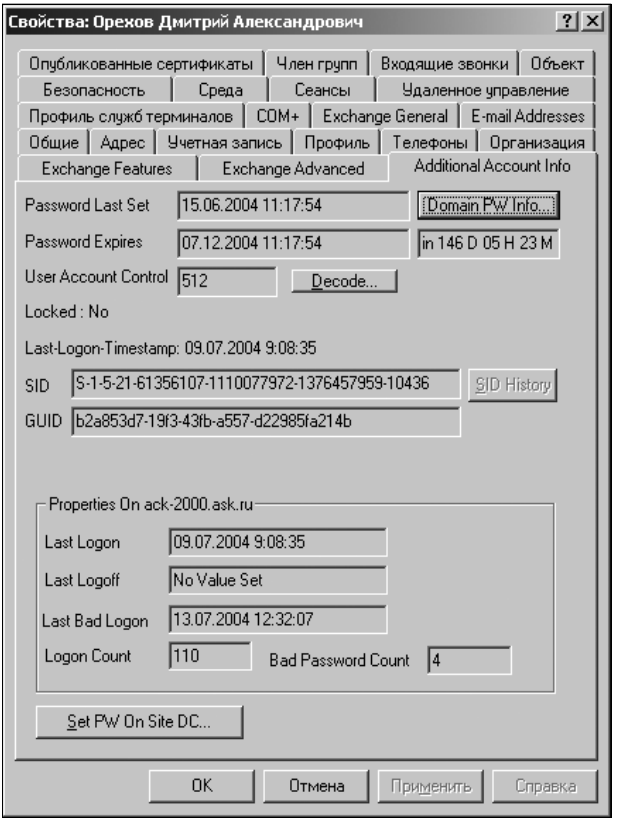


Рис. 4.8. Дополнительные параметры учетной записи

После установки пакета Account Lockout and Management Tools в свойствах учетной записи отображается вкладка, на которой администратор может увидеть в том числе и количество неудачных попыток входа в систему (**Bad Password Count**) (рис. 4.8). Данную информацию можно получить и выполнив непосредственный запрос к службе каталогов. В качестве фильтра можно указать следующую строку:

```
(&(objectclass=user)(!(objectclass =computer))(!(badPwdCount=0))
(badPwdCount=*))
```

При необходимости вы можете создать такой запрос, сохранить его в оснастке управления AD и получать сведения о результатах подключения к домену без установки упомянутого пакета.

Группы пользователей

Разные пользователи должны иметь разные 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. Поскольку книга посвящена, в первую очередь, работе в составе компьютерной сети, уделим особое внимание именно группам, создаваемым в доменах Windows.

Исторически сложилось так, что существует несколько типов групп. 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`).

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. 4.3).

Таблица 4.3. *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 с 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.

Ролевое управление

Современные прикладные программы предусматривают работу с данными пользователей с различающимися функциональными обязанностями. Для регулирования прав доступа к возможностям программы принято использовать *ролевое управление*. Роль представляет собой предварительно настроенный набор прав пользователя, выполняющего определенные обязанности (директор, главный бухгалтер, кассир и т. п.). При подключении нового пользователя такой системы администратору достаточно предоставить ему тот или иной предварительно подготовленный набор прав.

Прикладные программы могут создавать роли как группы безопасности в домене, так и как локальные группы на том компьютере, где работает программа. Администратору остается только включить необходимых пользователей (или группу пользователей, если таковая уже создана) в состав соответствующей роли.

Результирующее право: разрешить или запретить?

При назначении прав можно определить как *разрешение*, так и *запрещение* на выполнение какой-либо операции. Если пользователь входит в несколько групп, то каждая из них может иметь свой набор разрешений и запретов для данной операции. Как формируется итоговое разрешение, особенно если разрешения различных групп противоречат друг другу?

Первоначально проверяется, существуют ли *запреты* на выполнение операций для какой-либо из групп, в которые входит пользователь, и для самой учетной записи. Если хотя бы для одной группы определен запрет доступа, то система сформирует отказ в операции. Затем проверяется наличие разрешений на *доступ*. Если хотя бы для одной группы будет найдено разрешение, то пользователь получит право выполнения желаемого действия.

В соответствии с описанным правилом обработки, если пользователь как член одной группы имеет разрешение на выполнение действия, а как член другой группы — запрет, то результатом явится отказ в выполнении операции.

Следует быть крайне осторожным при назначении явных запретов. Очень легко (если на компьютере используется сложная структура групп) запретить даже самому себе выполнение тех или иных операций.

> ***Примечание***
>
> Существует единственное отступление от данного принципа преимущества запрета перед разрешением, известное автору. Это определение итогового разрешения на основе *наследуемых* и *явно указанных* прав, которое описано в *разд. "Наследуемые разрешения: будьте внимательны" далее в этой главе*.

Разрешения общего доступа и разрешения безопасности

Для объектов, 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 и проверяется *независимо* от разрешений общего доступа. Иными словами, если пользователю разрешено подключаться к этому ресурсу по сети, но доступ к файлам запрещен разрешениями безопасности, 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. 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 различных 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.

Наследуемые разрешения: будьте внимательны

По умолчанию вновь создаваемые ресурсы наследуют свои разрешения безопасности от родителей. Так, при сохранении нового файла его разрешения будут установлены по разрешениям той папки, в которой создается файл.

При необходимости изменения прав внутри такой структуры наследования легко можно добавить новые права для любых учетных записей. С исключением дело обстоит несколько сложнее. Сначала необходимо *разорвать* цепочку наследования (в диалоговом окне, открывающемся при нажатии кнопки **Дополнительно** в свойствах безопасности, снять флажок **Разрешить наследование разрешений от родительского объекта...**) и отредактировать список установленных прав.

Назначение разрешений файловой системы обычно не представляет особой сложности. При этом наиболее частый вопрос, который возникает у пользователей, — это изменение прав доступа, когда в свойствах объекта они отображаются квадратиками с серым фоном.

Такое отображение свидетельствует о том, что разрешения на данный объект *наследуются* от родительского. Для того чтобы изменить их, необходимо данную связь разорвать. Эта операция выполняется через кнопку **Дополнительно** — достаточно снять уже упоминавшийся флажок **Разрешить наследование...**.

Разрешения, которые добавлены к списку унаследованных, называют *явно установленными*. Явно установленные разрешения имеют *преимущество* перед унаследованными. При этом не работает принцип верховенства запрета. Если унаследовано право запрета на доступ, а явно задано разрешение, то в результате пользователь *сможет* выполнять операции с файлами (рис. 4.9).

В свойствах файла отмечены как запреты (унаследованы от родительской папки, выделены серым фоном флажка выбора), так и явно назначенные полные права владения. В этом случае будет действовать *явное назначение прав*. Пользователь сможет выполнять с файлом любые операции, несмотря на наличие запрета.

В такой ситуации результирующие права неверно отображались самой системой: было показано полное отсутствие прав, несмотря на наличие разрешения полного доступа.

> ***Примечание***
>
> Администратору следует внимательно отнестись к такому правилу, поскольку это может привести к неучитываемым возможностям доступа к данным. Причем на компьютере автора окно отображения результирующих прав доступа неверно показывало существующие разрешения: права доступа к файлу не были показаны, хотя они фактически имелись.

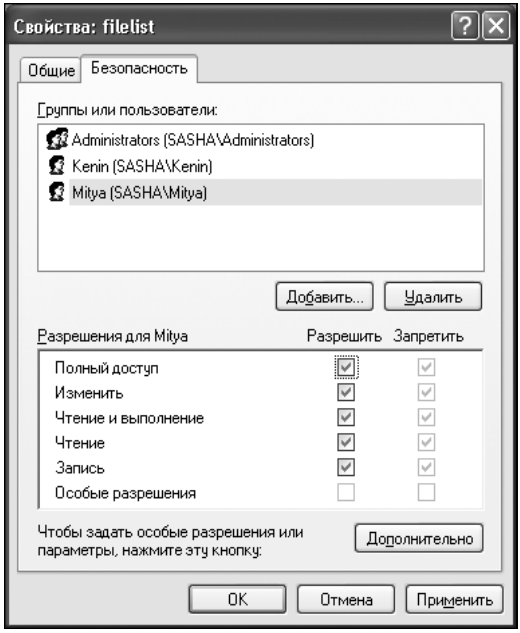


Рис. 4.9. Наследованные и явно заданные разрешения противоречат друг другу

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.

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.

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[1] 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 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

[1] Такое поведение было свойственно Windows XP, в последующих версиях система выдает предупреждение, что файл после копирования или перемещения будет уже незашифрованным.

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 **Безопасность** нажать кнопку **Дополнительно** и выбрать вкладку **Действующие разрешения**. После чего необходимо выбрать пользователя, для которого будут определяться действующие права, и посмотреть итоговый результат (рис. 4.10).

> ***Примечание***
>
> Средствами групповой политики администратор имеет возможность отключения просмотра результирующих прав.

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.

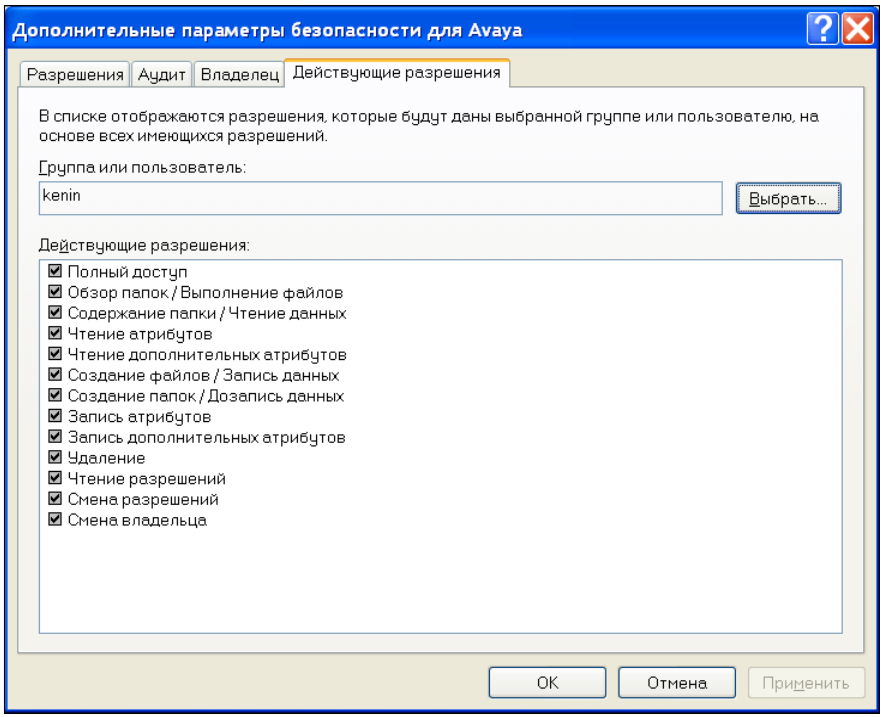


Рис. 4.10. Отображение действующих прав доступа к файлу для выбранного пользователя

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.

Создание и удаление учетных записей

После установки операционной системы 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.

Примечание

Обратите внимание, что после использования мастера установки Windows XP в режиме отображения страницы приветствий во время входа в систему название учетной записи администратора не показано на экране. Однако эта учетная запись может быть

применена для работы с системой, причем обычно администраторы забывают о необходимости установки для нее пароля, что позволяет легко локально зайти в систему с правами администратора, предъявив "пустой" пароль.

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 (рис. 4.11): управления компьютером в локальном случае и оснастка управления AD Пользователи и компьютеры при создании доменных пользователей.

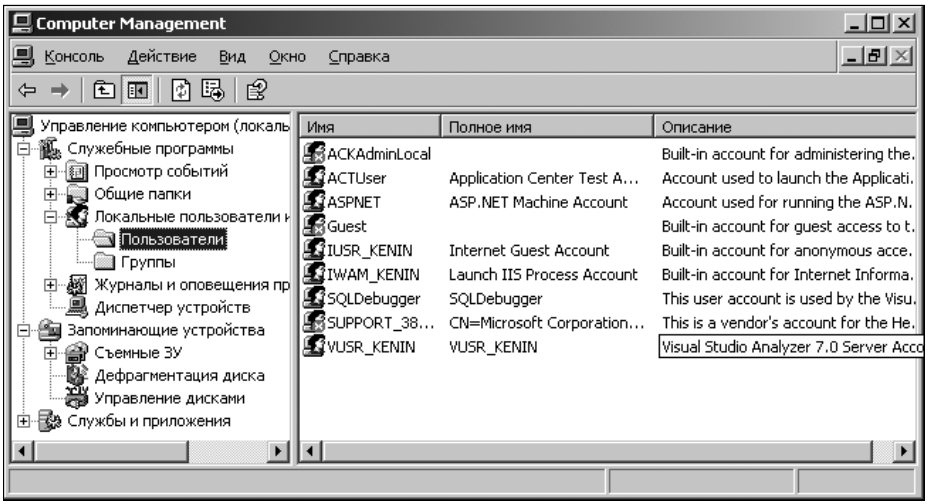


Рис. 4.11. Добавление нового пользователя локальной системы

При создании новых пользователей домена рекомендуется устанавливать для них требование смены пароля при первом входе в сеть.

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. Эти учетные записи можно использовать для контроля доступа к сетевым ресурсам.

Если в организации используются дополнительные параметры учетной записи (название отдела, адрес и т. п.), то более удобно 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.

Дополнительные параметры учетной записи

Каждая учетная запись имеет существенное количество дополнительных параметров, значения которых могут быть использованы в работе организации. Это дает администратору возможность объединять пользователей в группы, учитывая содержимое того или иного поля. Например, можно создать группу, объединяющую пользователей, находящихся в определенном офисе, и присвоить ей почтовый адрес.

Поля учетной записи могут заполняться с помощью окна свойств, вызываемого из оснастки управления службой каталогов (или управления компьютером — при правке локальных пользователей). Эти свойства можно запрашивать и устанавливать с помощью достаточно простых сценариев, однако более удобно выполнять соответствующие операции поиска и изменения данных на основе протокола LDAP *(см. разд. "LDAP-управление" ранее в данной главе)*, при этом администратору доступны практически любые критерии поиска необходимых записей.

Права учетной записи

Кроме разрешений доступа к файлам, пользователь 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.

Права пользователей в системе назначаются через оснастку Локальная политика безопасности, расположенную в группе административных задач (рис. 4.12). 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.

Восстановление параметров безопасности по умолчанию

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 устанавли-

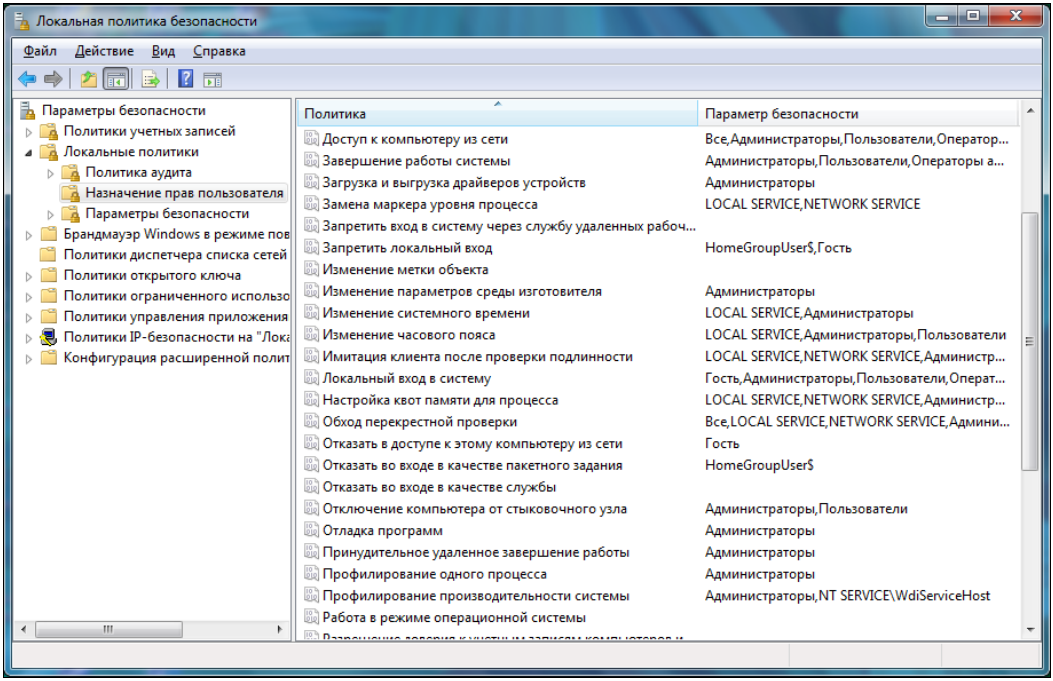


Рис. 4.12. Окно настройки прав пользователя в системе

ваемой 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: политика паролей, политика блокировки учетных записей и политика Kerberos;
- Локальные политики: политика 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;
- Файловая система: 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.

Автоматически создаваемые учетные записи

При установке операционной системы автоматически создается несколько учетных записей пользователей. Ранее мы упоминали учетную запись *Администратор*. Эта учетная запись особая. 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 Windows 7 учетная запись Администратор как бы разделилась на две: одна учетная запись соответствует той, с которой вы входите в систему, другая — учетная запись, которая используется, если вызывается команда **Запустить от имени ад-**

[1] В версиях, более ранних чем Windows XP. В новых версиях Windows упомянутые операции допустимы.

министратора. С этим связаны некоторые ошибки, когда пользователи не могут понять, почему не выполняется сценарий, исполняемый от имени Администратор. 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, то 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 учетных записи. Это *IUSR_*имя_компьютера и *IWAM_*имя_компьютера. Учетная запись IUSR_*имя_компьютера* применяется при предоставлении Web-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 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. Учетная запись Система 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 Системы. Поэтому для использования

при запуске служб введены еще две учетных 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 большими 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.

Встроенные группы

При установке операционной системы 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 создается 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 копи-

рования, управлять принтерами, журналами безопасности и протоколами аудита системы.

- *Операторы резервного копирования* (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.

  Примечание

  Учетная запись 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 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.

  Примечание

  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.

- *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.

- *HeplSevicesGroup*.

  Группа предоставляет типовой набор прав, необходимый специалистам службы техподдержки. Не следует включать в нее других членов, кроме учетной записи, созданной по умолчанию.

- *Remote Desktop Users*.

  Ее члены могут осуществлять удаленное подключение к рабочему столу компьютера. Иными словами, если вы хотите иметь возможность удаленно подклю-

читься 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 только на просмотр параметров настройки служб DHCP (или WINS). Применяются при делегировании прав техническому персоналу (например, для сбора информации о состоянии сервисов).

- *Network Configuration Operators*.

  Пользователи группы имеют право изменения TCP/IP-параметров. По умолчанию группа не содержит членов.

- *Print Operators*.

  Члены группы могут управлять принтерами и очередью печати.

В системе присутствуют и другие группы, на описании которых мы не будем особо останавливаться (Account Operators, Pre-Windows 2000 Compatible Access, Server Operators и т. д.).

Специальные группы

В операционной системе 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 ком-

пьютере. 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 использовать 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.

Рекомендации по использованию операции *Запуск от имени...*

По соображениям безопасности не рекомендуется использовать для текущей работы учетную запись, обладающую административными правами. Смысл этого требования очень прост. Если на компьютере работает неопытный пользователь, то он не сможет что-либо испортить в настройках системы и привести ее в нерабочее состояние. Кроме того, в повседневной практике очень легко встретиться с какой-либо скрытой вредоносной программой. Если при запуске такой программы она не будет обладать административными правами, то возможностей нанести вред компьютеру у нее будет существенно меньше.

Однако на практике пользователям периодически приходится выполнять различные административные действия. Например, установить драйвер для нового внешнего устройства хранения информации, на котором вы принесли для просмотра взятый у приятеля видеофильм, и т. п. Понятно, что несмотря на все рекомендации, большинство пользователей для удобства работали с правами учетной записи администратора.

В операционных системах Windows 7 по умолчанию максимальные права не предоставлены и администратору. Чтобы выполнить действия, меняющие системные настройки, предусмотрен специальный механизм для быстрого запуска программ с использованием административных прав. Это операция **Запуск от имени Администратора**.

Эта команда доступна в динамическом меню соответствующего ярлыка. Кроме того, если при запуске программы система обнаружила попытку выполнения действий, для которых требуется подобная эскалация прав, то пользователь увидит на экране запрос на продолжение, который он должен подтвердить (или отказаться, если подобная операция не планировалась).

Примечание

Обратите внимание, что учетная запись Администратор и учетная запись, которая используется при запуске от имени администратора, — это различные учетные записи. Если не учитывать данный момент, то это может привести к неожиданным результатам, например, при выполнении сценариев входа в домен.

ГЛАВА 5

Работа в глобальной сети

Работая в глобальной сети, необходимо решать несколько задач:

- обеспечить доступ к внешним ресурсам Интернета;
- защитить внутренние ресурсы организации от внешних и внутренних угроз (предотвратить потери и утечки данных);
- организовать связь между центральным офисом и филиалами и наладить доступ к эксплуатируемым приложениям;
- предоставить доступ мобильным сотрудникам к ресурсам организации.

Организация доступа к ресурсам Интернета

Во внутренней сети можно использовать реальные адреса Интернета, но такой вариант является скорее исключением, чем правилом. Обычно на организацию выделяется небольшое число реальных адресов, внутри периметра распределяются серые адреса *(см. главу 3)*.

Для *преобразования сетевых адресов* применяется, в том или ином варианте, технология трансляции адресов — Network Address Translator (NAT).

NAT

Технология трансляции адресов (NAT) позволяет осуществить подключение к Интернету практически любого числа компьютеров, используя 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 на исходный. Если NAT не находит у себя записи о перенумерованном порте, то пакет отбрасывается.

Таким образом, 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 о IP-адресах в своих данных, поэтому для корректной работы таких протоколов NAT модифицирует и сами TCP-последовательности. Так, в ОС 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 в операционной системе не предусмотрено, то работа через NAT будет невозможна без использования для такой системы реального адреса.

Из описания работы NAT видно, что он защищает сеть предприятия от злоумышленника, "принимая" только *ответы* на запросы из локальной сети. Если же вам 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 активируются внешними запросами. Например, почтовый клиент MS Outlook при работе с сервером MS Exchange использует протокол RPC (*Remote Procedure Call*, вызов удаленных процедур). 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 межсетевой экран блокирует эти пакеты. Поэтому в данном примере клиент не будет получать автоматические сообщения о приходе новой почты, хотя сможет принимать и отправлять сообщения по команде пользователя.

Реализация NAT средствами службы маршрутизации Windows

Для серверных систем настройка NAT осуществляется через оснастку службы маршрутизации и удаленного доступа. Для настройки NAT следует добавить интерфейсы подключения к Интернету и локальной сети к протоколу маршрутизации NAT, для чего на вкладке **Общие** (General) свойств интернет-интерфейса надо 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 использовании одного адреса подключения к Интернету нужно уста-

новить переключатель **Преобразовать TCP/UDP-заголовки** (Translate TCP/UDP headers) для свойств интернет-интерфейса.

Примечание

NAT от Windows Server может осуществлять трансляцию как на частные адреса локальной сети, так и на реальные адреса. Если доступно несколько реальных адресов, то NAT сопоставляет частный IP-адрес с реальным. В этом случае трансляция портов не осуществляется. При исчерпании реальных адресов NAT включает трансляцию портов.

Реализация NAT при совместном использовании подключения к Интернету

NAT применяется в Windows при включении совместного использования подключения к Интернету. Эта функциональность присутствует как в рабочих станциях, так и в серверных операционных системах.

Организовать совместное использование подключения к Интернету можно при любом способе связи, будь это подключение через модем или локальную сеть (если провайдером проложен к вам выделенный канал). Соответствующую настройку легко выполнить аналогично описываемому далее примеру подключения к Интернету с использованием 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 в Интернет поставьте соответствующий флажок.

Примечание

Если вы не хотите, чтобы соединение с Интернетом автоматически устанавливалось каждый раз, когда кто-либо из локальной сети обращается к Сети (пытается открыть страницу Интернета, принять почту и т. п.), то уберите соответствующий флажок в опциях настройки.

При выборе совместного использования 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 настройка протокола TCP/IP должна быть выполнена 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 использовании подключения достаточно создать соответствующее правило. Покажем на примере, как выполнить публикацию внутреннего FTP-сервера в сети Интернет при совместном использовании подключения.

1. Откройте свойства соединения с Интернетом, для которого организовано совместное использование, перейдите на вкладку **Дополнительно** и нажмите кнопку **Настройки**. Появится окно с перечнем типовых сервисов Интернета, которым разрешен доступ во внутреннюю сеть 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 изменялся впоследствии, поскольку стандартно при совместном использовании подключения к Интернету адреса компьютерам выдаются динамически и могут изменяться. После завершения операций закройте все окна настройки, нажав кнопку **OK**.

В результате подобных настроек, например, на FTP-запрос, поступающий из внешней сети, будет отвечать не непосредственно подключенный к Интернету компьютер, а указанный вами при описанных ранее операциях.

Использование соединения может быть протоколировано (записаны пропущенные или отклоненные пакеты, рис. 5.1), однако в связи с большим объемом файла протокола для его анализа необходимо использовать программные продукты других разработчиков.

Таким же 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 введении нового сервиса необходимо указать тип используемого протокола 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 используете 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.

Ограничения совместного использования подключения к Интернету

Из технических особенностей реализации совместного использования подключения к Интернету вытекают ограничения его применения.

Совместное использование подключения позволяет быстро и с минимальными затратами обеспечить работу компьютеров локальной сети в Интернете через одну точку подключения. Однако такое решение применимо только для домашней сети или сети малого офиса, потому что данный вариант подключения создает неконтролируемый доступ в Интернет для *всех* компьютеров локальной сети. В сети организации необходимо вести контроль доступа к ресурсам Интернета, иметь возможность выборочно предоставлять доступ одним сотрудникам и запрещать

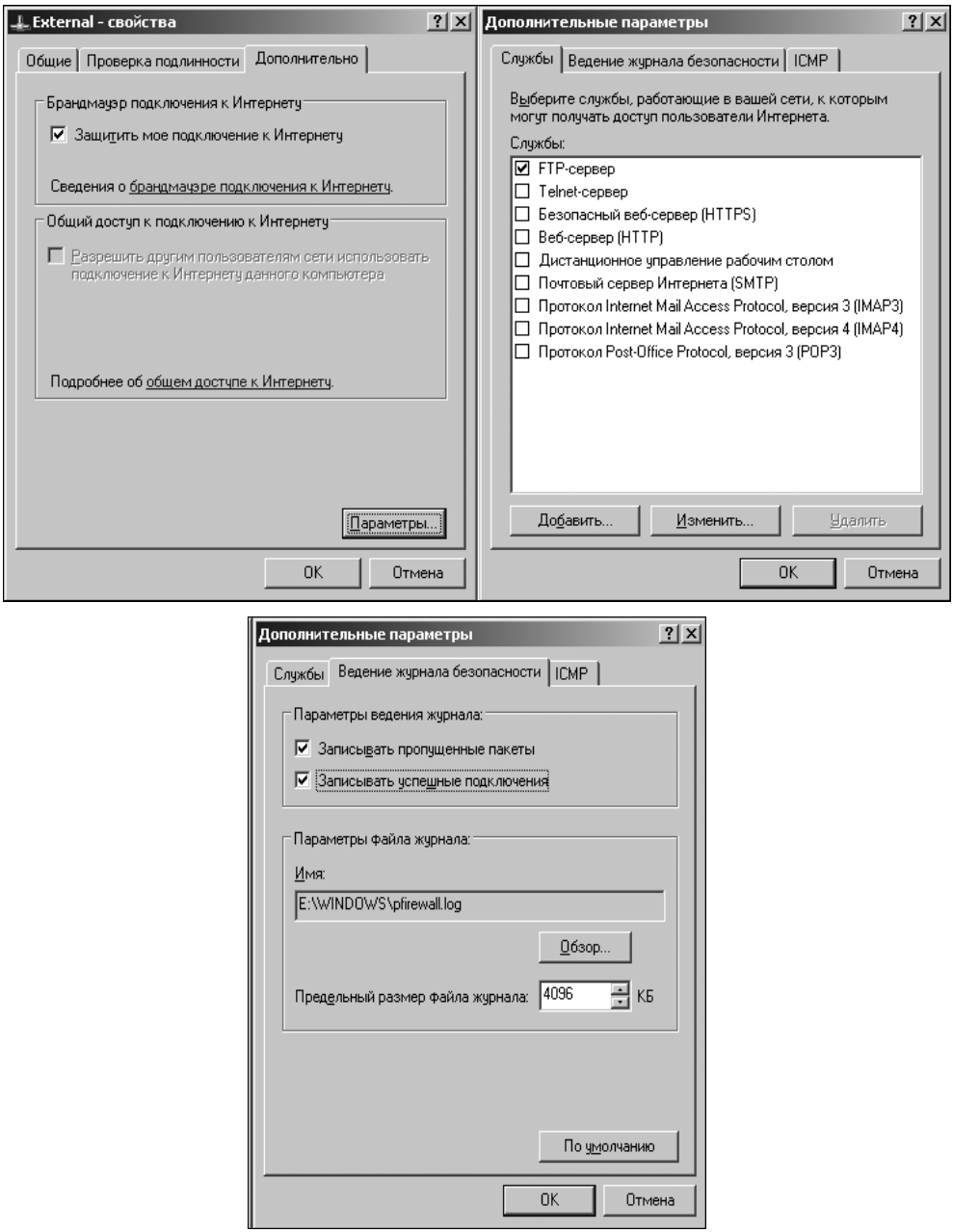


Рис. 5.1. Настройка параметров совместно используемого подключения

другим и т. п., в связи с чем в средних и крупных организациях применяются серверные решения, позволяющие реализовывать принятую политику предоставления доступа в Интернет.

Кроме того, можно использовать в локальной сети только диапазон адресов 192.168.0.0/24, причем адрес 192.168.0.1 может быть только у компьютера, обеспе-

чивающего 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 совпадения диапазонов адресов локальных сетей).

Аппаратный NAT

Для небольших организаций подключение к Интернету удобнее всего организовать с помощью аппаратных маршрутизаторов. Эти устройства дешевы (стоимость порядка 100$ в зависимости от модели), оборудованы несколькими внутренними портами (обычно 2—4), функционалом Wi-Fi-точки доступа. Устройство содержит настраиваемый сервер DHCP для автоматической настройки компьютеров локальной сети. Поддерживаемые решения по подключению к интернет-провайдеру обеспечивают работу в российских условиях.

Выполнены эти маршрутизаторы на Linux-операционной системе, настраиваются через веб-интерфейс и не требуют вмешательства пользователя в процессе эксплуатации.

Реализация NAT средствами Linux

Настройка NAT в Linux осуществляется крайне просто. Делается это одной командой утилиты iptables.

Пусть eth0 — это интерфейс Интернета, а eth1 — интерфейс локальной сети.

После этого в настройку iptables достаточно добавить только строчку:

```
iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
```

> ***Примечание***
>
> Кроме указанного правила не следует забывать о необходимости других правил фильтрации. Например, правил контроля пересылаемых пакетов, фильтрации доступа к системе из внутренней сети и т. п.

Фильтрация трафика

В современной информационной системе объединяются различные задачи с отличающимися категориями информации, а опасность часто исходит не из-за периметра организации, а от имеющих доступ пользователей. Поэтому *каждая* автоматизированная система в составе общей информационной системы должна быть защищена межсетевым экраном.

Демилитаризованная зона

Традиционно существовало понятие *демилитаризованной зоны* (*Demilitarized zone, DMZ*), которым обозначали компьютеры, чьи ресурсы должны быть опубликованы в Интернете.

DMZ представляет собой специально организованную подсеть локальной сети, которая отделена межсетевыми экранами как от Интернета, так и от компьютеров

локальной сети (рис. 5.2). При такой конфигурации сети злоумышленнику, сумевшему взломать компьютер с опубликованной службой, крайне сложно, если не совсем невозможно получить доступ к другим локальным ресурсам.

DMZ-зону можно создать с использованием двух межсетевых экранов (рис. 5.2, *а*) или одного, но имеющего три сетевых адаптера (рис. 5.2, *б*). Второй вариант хотя и несколько дешевле, но более трудоемок в настройке и требует повышенного внимания администратора.

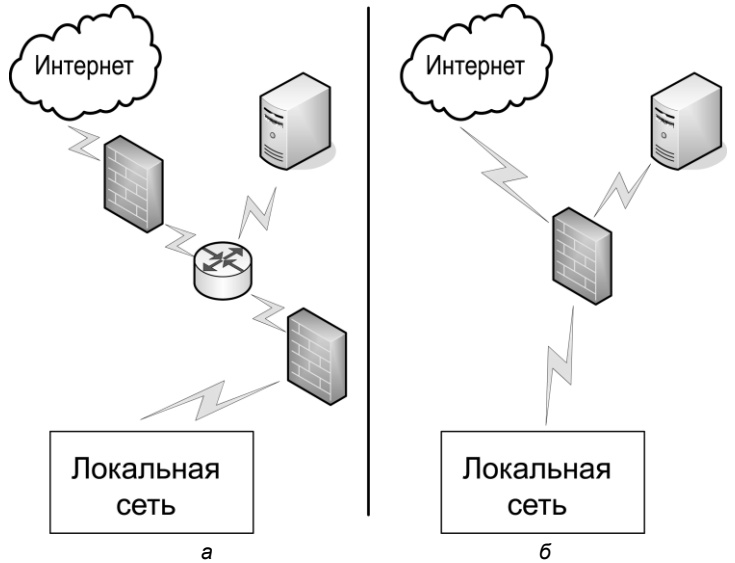


Рис. 5.2. Варианты создания демилитаризованной зоны:
а — с использованием двух межсетевых экранов; *б* — с использованием одного межсетевого экрана

Понятие демилитаризованной зоны имеет сегодня, скорее, академическое значение. Защищать межсетевыми экранами необходимо не только системы, к которым есть доступ из внешней сети, но все серверы и рабочие станции.

Межсетевой экран (брандмауэр)

Межсетевой экран (МСЭ), или *брандмауэр* (firewall), — это комплекс технических, программных и организационных мер по безопасному подключению одной сети к другой. В зависимости от решаемых задач и конфиденциальности защищаемой информации это может быть просто небольшая программа, установленная на компьютере, или же специализированные аппаратные средства, реализующие требования конкретной организации.

Обычно по общим соображениям безопасности в качестве межсетевого экрана рекомендуется использовать автономное устройство. Иными словами, в случае программной реализации брандмауэра на этот компьютер не следует возлагать решение никаких других задач.

Что может межсетевой экран и чего не стоит от него ожидать?

Межсетевой экран осуществляет фильтрацию как передаваемых данных, так и принимаемой информации. Он позволяет отсечь те пакеты, которые нежелательны для данной сети, и направлять внешний трафик только к назначенным компьютерам. Межсетевые экраны скрывают внутреннюю структуру локальной сети.

В то же время межсетевой экран никоим образом не защищает от "дыр", которые могут быть в разрешенных сервисах и которыми может воспользоваться злоумышленник для проникновения в локальную сеть. Так, широко известен пример, когда в одну из версий популярного бесплатного FTP-сервера был встроен троянский вирус, позволяющий перехватывать управление сервером. Пример подключения к ресурсам локальной сети через межсетевой экран приведен также в *разд. "Доступ из-за межсетевого экрана" далее в этой главе.*

Учитываемые параметры фильтрации

В зависимости от конкретной системы межсетевого экрана могут быть реализованы различные варианты фильтрации проходящих данных, в частности, возможно:

- открывать или запрещать прохождение данных в зависимости от времени суток и дней недели;
- разрешать прохождение явно заданных протоколов;
- фильтровать информацию в зависимости от адреса отправителя/адреса получателя;

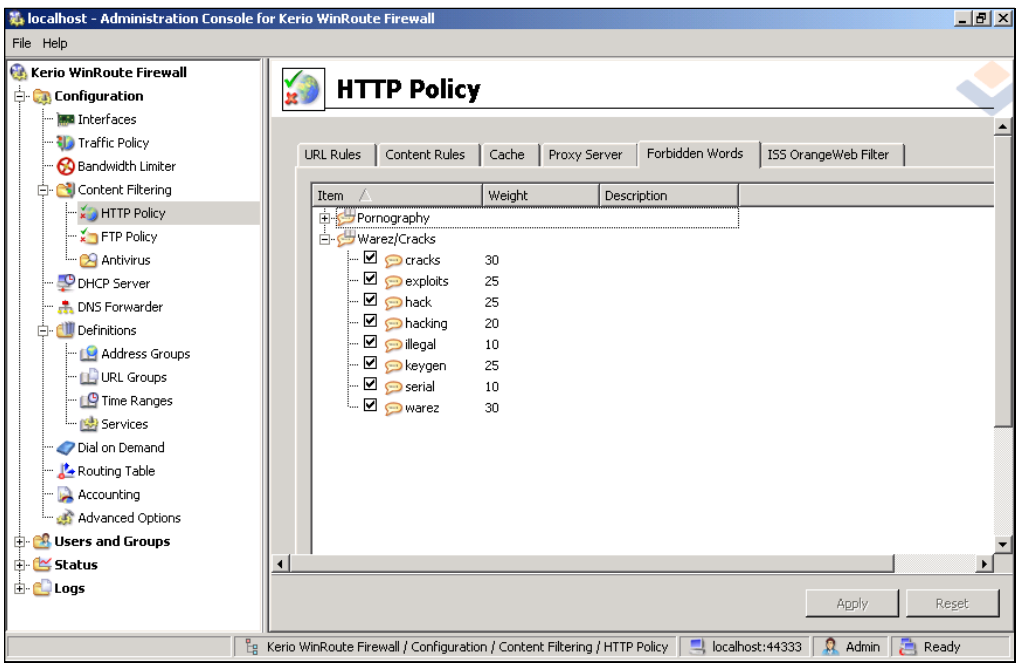


Рис. 5.3. Фильтрация контента средствами межсетевого экрана

- разрешать передачу данных в зависимости от результатов аутентификации отправителя;
- фильтровать получение данных в зависимости от содержания информации.

Возможны различные комбинации этих параметров: можно запретить работу с определенным перечнем хостов Интернета некоторому кругу сотрудников в рабочее время или заменить рекламу, формируемую баннерными системами, "пустыми" местами на страницах. В качестве примера на рис. 5.3 представлено окно настройки параметров межсетевого экрана Kerio WinRoute Firewall, в котором определяются ключевые слова, по которым будут блокированы запросы к страницам Интернета.

Кроме того, обычно межсетевые экраны имеют ряд дополнительных сервисных возможностей: позволяют организовать протоколирование работы (учет трафика Интернета по пользователям, адресам, объему и т. п.), выявлять атаки со стороны внешней сети и направлять сообщения об этом администратору для принятия соответствующих мер, управлять используемой полосой доступа в Интернет и т. п.

Варианты организации межсетевых экранов

Все способы фильтрации, применяемые в традиционных межсетевых экранах, условно можно разделить на фильтрацию пакетов и использование шлюзов уровня сессии или уровня приложения. В большинстве случаев реальные системы комбинируют эти варианты.

Фильтрация пакетов

При фильтрации пакетов разрешения на прием/передачу данных выдаются только на основе анализа IP-адреса и номера порта источника пакета и его назначения. Данный вариант является самым простым и быстрым способом реализации межсетевого экрана.

> ***Примечание***
>
> Принципиально существуют возможности "обмануть" такой межсетевой экран, например, фальсифицируя адреса в пакетах.

Шлюзы

Шлюзы уровня сессии организуют временные соединения между клиентом и хостом Интернета на основе некоторых заданных правил. После создания такого канала вся информация, передаваемая по нему, свободно пропускается. После завершения сессии канал уничтожается.

Более совершенным считается другой способ организации шлюзов — шлюзы уровня приложения (часто называют *прокси-серверами*). Прокси-серверы обычно принимают запросы (как извне сети, так и изнутри), аутентифицируют пользователя, анализируют запросы и перенаправляют их в зависимости от содержимого (например, заблокируют определенный запрос на внутренний веб-сервер, а другой отошлют на соответствующее устройство). Фактически между клиентом и хостом Ин-

тернета образуется цепочка из двух соединений: от клиента до прокси и от прокси до хоста Интернета. Таким образом, запрещается прямой доступ к внутренним ресурсам организации, а весь трафик считается исходящим (входящим) от имени прокси-сервера.

Прокси-серверы имеют развитые возможности аутентификации пользователей, хорошие механизмы протоколирования своей работы и обеспечивают наибольший уровень защиты локальной сети.

Intrusion Prevention Systems

Описанные выше способы фильтрации трафика в конечном итоге разрешают по тем или иным правилам доступ "хорошим" пользователям (или службам) и запрещают "плохим". Такая практика постепенно теряет свою эффективность, поскольку вредоносные коды все больше и больше "подстраиваются" под существующие методы защиты. Например, что мешает какой-либо программе воспользоваться разрешением доступа в Интернет для передачи "подсмотренных" на компьютере данных на какой-либо сервер глобальной сети, маскируясь при этом под обычную работу пользователя? А если деятельность компании тесно связана с глобальной сетью, то сетевые атаки на ее серверы, имеющие целью вызвать отказ в обслуживании клиентов, могут повлечь за собой миллионные убытки.

Для предотвращения подобных вторжений в инфраструктуру предприятия стали применяться аппаратные и программные решения, *контролирующие содержание* передаваемых по сети пакетов с целью обнаружения подозрительной активности. Первоначально такие системы контролировали сеть параллельно основным устройствам и выдавали сигналы опасности при обнаружении подозрительных данных. Они получили название Intrusion Detection Systems (IDS).

Современные системы предотвращения атак — Intrusion Prevention Systems (IPS) — выполняют активную функцию. Они не только обнаруживают атаку, но и сразу же блокируют подозрительный трафик. Подобные системы могут обнаружить подготовку DoS-атаки, блокировать трафик программ, используемых для передачи данных между пользователями (типа Kazaa, Gnutella, ICQ и т. п.), обнаруживать сетевые черви, активность эксплойтов и т. п. (рис. 5.4).

Принцип действия IPS основан, прежде всего, на сравнении информации, передаваемой по сети, с заранее известными сигнатурами, которые присутствуют в пакетах, передаваемых червями, в пакетах программ, использующих те или иные уязвимости программного обеспечения, и т. п. Состав сигнатур постоянно обновляется с сайтов разработчиков IPS. Кроме того, IPS могут обнаруживать аномальные изменения трафика (например, резкое увеличение пакетов определенного типа) и сохранять пропускную способность канала для "полезных" данных.

Понятно, что с увеличением количества сигнатур, учитываемых при анализе содержимого пакета данных, растет нагрузка на устройство и, в конечном итоге, снижается его пропускная способность, поэтому надежно защитить весь сетевой трафик организации практически невозможно. Например, функция Cisco Intrusion Detection Systems включена в ПО коммутаторов Cisco, начиная с IOS Software

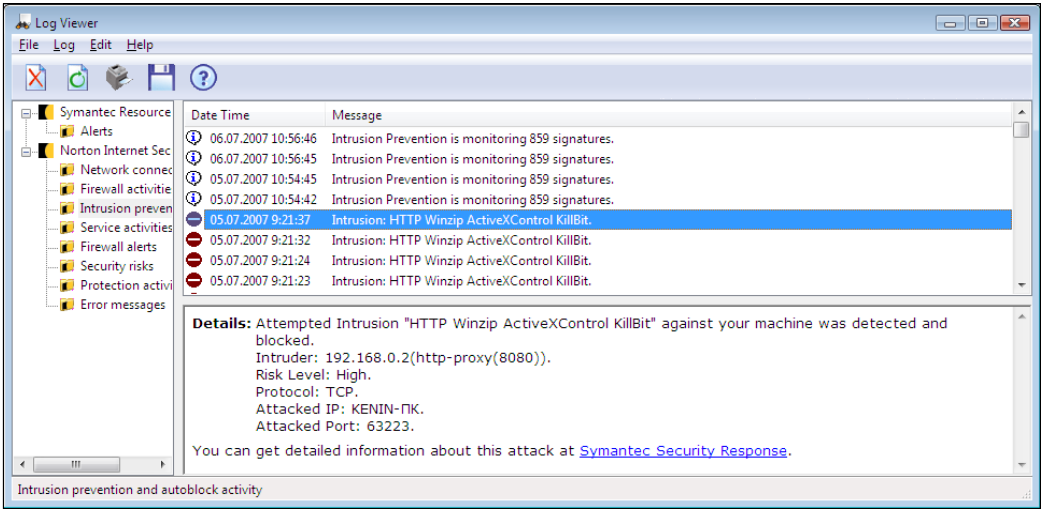


Рис. 5.4. Программа Norton Internet Security
блокировала вторжение на пользовательский компьютер

Release 12.0.(5), но производитель предупреждает о снижении производительности устройства при увеличении числа сигнатур в используемых политиках предотвращения атак. IPS применяют в пограничных точках: на стыке Интернета и локальной сети организации, между серверным сегментом и пользовательской частью.

Как уже говорилось, технологии предотвращения атак могут быть программными или аппаратно-программными. Можно отметить, например, новое поколение *Check Point* — межсетевой экран, используемый большинством крупнейших компаний мира для защиты своих ресурсов, который включает в себя технологию *SmartDefense*, предназначенную для анализа проходящего трафика. Существуют и специализированные решения от Tipping Point (**www.tippingpoint.com**), Internet Security Systems (**www.iss.net**), Radware (**www.radware.com**), TopLayer (**www.toplayer.com**) и др.

Использование решений данного класса чувствительно увеличивает расходы предприятия с одной стороны и предъявляет повышенные требования к уровню подготовки администратора с другой стороны. Поскольку подобные дополнительные расходы для небольших предприятий обычно не оправданы, то в них используются традиционные программы брандмауэров. В то же время данная функциональность стала включаться в антивирусное программное обеспечение ведущих вендоров, занимающихся вопросами безопасности.

Варианты межсетевых экранов

В распоряжении администраторов имеются как *аппаратные* межсетевые экраны, так и *программные* решения. Различие между этими двумя вариантами достаточно условно. Аппаратный модуль — это фактически специализированная под опреде-

ленную задачу та или иная вычислительная система. Обычно для него создается операционная система (например, IOS у Cisco) или используется бесплатная версия Linux.

Программные варианты предполагают установку на типовые операционные системы, например: на Linux, операционные системы от Microsoft и т. п.

Аппаратные решения

На сегодня для малых предприятий наиболее дешевым решением являются аппаратные межсетевые экраны (стоимость их менее $200).

Такие модели выпускают практически все производители коммутационного оборудования. Имеются комплексные решения, например ADSL-модем и межсетевой экран в одном корпусе.

В зависимости от сложности устройства доступны различные уровни защиты сети. Но даже самые дешевые модели включают в себя такие функции, как статическую фильтрацию пакетов, наличие DMZ-портов, возможность создания VPN-подключений, NAT-трансляцию с сервером DHCP, средства предупреждения администратора (отправка e-mail и т. п.).

Встроенный межсетевой экран Windows XP/7/Server 2003/2008

В операционных системах Windows имеется встроенный межсетевой экран.

По сравнению с Windows XP, в Windows 7 расширены возможности фильтрации трафика встроенными средствами. Теперь пользователи могут создавать правила не только для входящего, но и для *исходящего* трафика. Кроме того, в системе существуют три *профиля* межсетевого экрана. Один соответствует подключению к частной сети, другой — к публичной сети, третий используется при работе в составе домена Windows. Профили представляют собой наборы правил, оптимизированные для работы в условиях соответствующей сети (профиль выбирается в зависимости от характеристик сети, в которой в текущий момент работает компьютер). Количество профилей изменить нельзя, но пользователь может изменить состав и настройку правил, составляющих тот или иной профиль.

Каждый профиль имеет правила по умолчанию для входящего и исходящего трафиков. Они применяются в случае отсутствия для пакета данных явно определенного правила. Для исходящего трафика правило по умолчанию для всех профилей разрешает все, для входящего трафика — все блокирует. Вы можете изменить эти установки, например, запретить передачу данных из компьютера в сеть. В этом случае необходимо создать разрешающее правило для передачи необходимых данных вовне.

По умолчанию в профиле созданы наборы разрешающих правил, которые обеспечивают работу компьютера в составе сети Microsoft. Наборы правил довольно объемны, но на начальных этапах настройки Windows можно сохранить предложенные изготовителем настройки.

Операции выполняются под руководством мастера (рис. 5.5); их выполнение не представляет особой сложности.

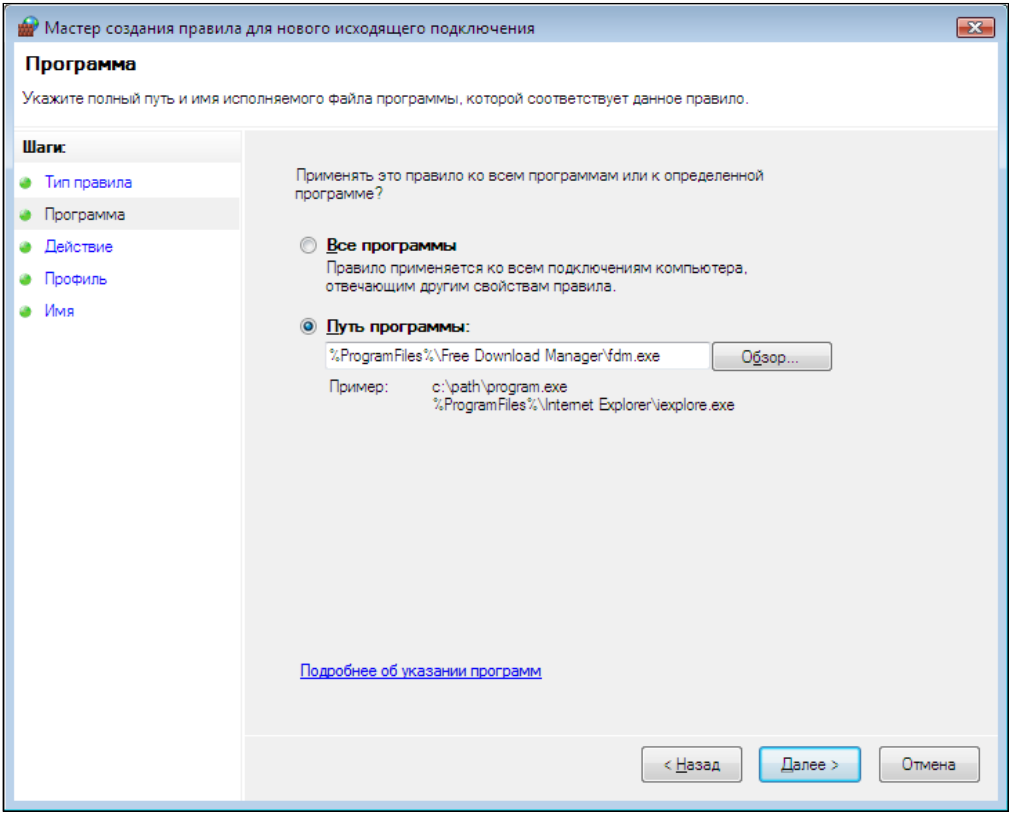


Рис. 5.5. Мастер создания правила для *исходящего* трафика в Windows Vista

Хотелось бы обратить особое внимание на следующие моменты.

Правило можно создать для программы, службы или порта. Если есть возможность, нужно выбирать программу или службу. Дело в том, что порт открывается созданным правилом на все время работы межсетевого экрана, а если правило создано для программы, то порт будет открыт только в период активности соответствующей программы. Это более безопасная ситуация.

> ***Примечание***
>
> Межсетевой экран может использовать эти настройки только для программ, работающих через Windows Socket. Поскольку особенности построения конкретной программы заранее не известны, то после создания правила следует проверить его работоспособность и при наличии ошибок выполнить настройку на основе протокола (порта).

Выбор настраиваемого правила необходимо сделать, если предполагается фильтровать трафик в зависимости от адресов источника и назначения. Правило позволяет определить как один адрес, так и диапазон IP-адресов. Кроме того, можно указать в правиле группу компьютеров по их функциональному назначению: WINS-, DHCP- или DNS-серверы, шлюз или локальная подсеть. Такое назначение позволяет более точно настроить правила с учетом возможного переноса данных ролей на другие компьютеры сети.

Программные комплексы

На рынке существует большое количество предложений межсетевых экранов. Администратор имеет возможность выбрать решения, обладающие большей или меньшей функциональностью. В любом случае перед тем, как внедрять решение, администратор должен тщательно взвесить желаемые требования и возможные стоимостные оценки реализации.

В Сети существует большое количество программ, предназначенных для защиты индивидуальных компьютеров. Например, можно отметить такие персональные межсетевые экраны, как AtGuard, BlackICE Defender, Jammer, Kerio Personal Firewall, Outpost Firewall, Sygate Personal Firewall, Tiny personal firewall, Zone Alarm и др. Часть этих продуктов — коммерческие программы, часть имеет версии, доступные для бесплатного использования.

Обычно такие программы сочетают в себе возможности блокировки трафика с дополнительными сервисами: например, запрет всплывающих окон, отсечение рекламных баннеров, фильтрация по вызывающему приложению и т. п. Часто программы имеют так называемый *режим обучения*, позволяющий неопытному пользователю осуществить точную настройку защиты. В этом режиме программа сообщает обо всех попытках передачи информации в Интернет. Анализируя представленную межсетевым экраном информацию, пользователь принимает решение о полной блокировке передачи, о разовом или постоянном разрешении. Таким образом, можно в результате обучения создать нужную конфигурацию доступа в Интернет.

Продукты, предназначенные для использования на уровне предприятий (Microsoft Forefront Threat Management Gateway, Check Point, Trend Micro Internet Gateway и т. п.), обычно носят комплексный характер: с их помощью можно создавать правила, фильтровать контент, предотвращать атаки определенного типа и т. д.

Фильтрация пакетов средствами операционной системы

В Windows предусмотрена возможность фильтрации пакетов. Например, с помощью фильтров легко защитить специализированный сервер (почтовый или аналогичный), разрешив прохождение пакетов только на определенный порт от конкретных устройств.

При помощи настройки фильтров политики IPSec легко создать правила, запрещающие или разрешающие трафик на конкретные узлы сети (рис. 5.6). При этом политики IPSec могут быть распространены на компьютеры сети с помощью групповой политики. Таким способом штатными средствами можно создать инструмент быстрого повышения уровня безопасности системы: достаточно предварительно разработать групповые политики IPSec, сводящие к минимуму сетевое взаимодействие, и включить их в случае вирусной атаки или признаков вторжения в сеть.

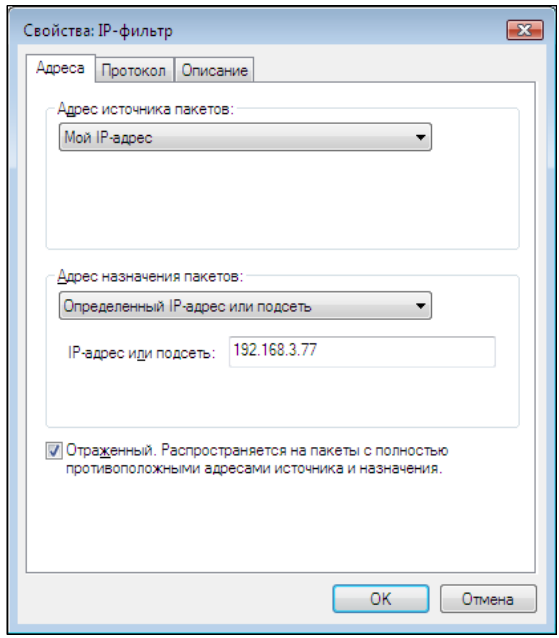


Рис. 5.6. Фильтры IPSec позволяют очень точно настроить разрешения на передачу того или иного трафика системы

Настройка параметров межсетевого экрана при помощи групповой политики

Версии Windows с последними обновлениями безопасности предусматривают включение межсетевого экрана по умолчанию. При этом используются параметры, оптимальные для некоторого "среднего" варианта: защита активна, но задействованы исключения, обеспечивающие работу компьютера в локальной сети. Это, с одной стороны, неудобно в локальной сети с развернутыми системами управления: межсетевой экран (МСЭ) блокирует доступ таких программ к компьютерам, а с другой, — не обеспечивает должного уровня защиты в публичных сетях. Поэтому встроенные межсетевые экраны Windows нуждаются в централизованной настройке с помощью групповых политик.

Групповые политики межсетевого экрана

Параметры настройки групповой политики межсетевого экрана Windows расположены по следующему пути: **Конфигурация компьютера | Административные шаблоны | Сеть | Сетевые подключения | Брандмауэр Windows** (рис. 5.7). Настройки снабжены подробным пояснением, поэтому обратим внимание только на основные моменты конфигурирования.

В политике предусмотрено два контейнера: *профиль домена* и *стандартный профиль*. Параметры профиля домена используются в случае работы компьютера в сети домена (работа в составе домена определяется по параметрам сетевого адреса и

доступности контроллера домена). Если компьютер, например ноутбук, включен в другую сеть, то настройки межсетевого экрана будут выполнены согласно параметрам, содержащимся в контейнере стандартного профиля.

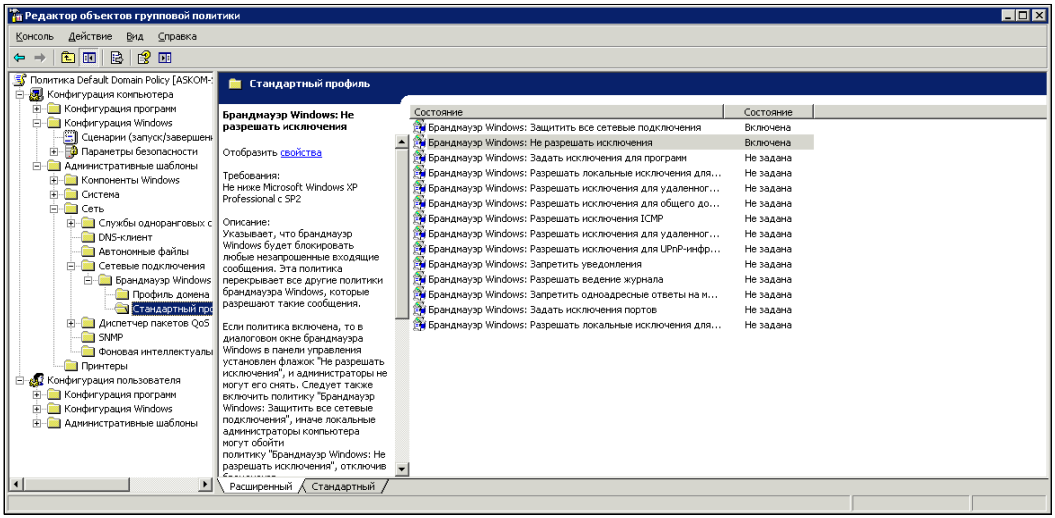


Рис. 5.7. Настройка параметров МСЭ при помощи групповых политик

Какие настройки могут быть рекомендованы для применения в обоих случаях? Во-первых, наиболее безопасным вариантом является использование межсетевого экрана как в условиях работы в домене, так и в публичной сети. Во-вторых, должна быть определена политика исключений защиты. При работе в домене, естественно, должны быть включены правила, относящиеся к работе в локальной сети. Кроме того, необходимо *создать* исключения и отразить их в групповой политике для тех программ управления, которые эксплуатируются на предприятии. Например, если вы используете корпоративную антивирусную программу, то должны разрешить доступ к компьютерам по тем портам, которые она использует (например, для антивируса от Symantec используемые порты описаны в документе **http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2005033011582148?OpenDocument&src=ent_hot&dtype=corp&seg=ent&prod=Symantec%20Client%20Firewall&ver=8.0&tpre=**).

А если на предприятии внедрена система удаленного мониторинга, то должны быть открыты порты для данной программы или включена опция **Разрешать исключения для удаленного управления** для возможности управления через удаленную консоль. В каждом конкретном случае перечень таких исключений индивидуален, а их количество должно быть минимально разумным.

Для стандартного профиля правилом должен стать *запрет* использования всех исключений межсетевого экрана, поскольку такой вариант наиболее безопасен для публичной сети.

В табл. 5.1 приведены возможные настройки параметров групповой политики для межсетевого экрана Windows.

Таблица 5.1. *Рекомендуемые параметры настройки МСЭ*

Параметр	**Рекомендуется для профиля**	
	домена	**стандартного**
Защитить все сетевые подключения	Включен	Включен
Не разрешать исключения	Не задан	Включен, и настроены исключения для используемых программ
Задать исключения для программ	Включен, и настроены исключения для используемых программ	Включен, и настроены исключения для используемых программ
Разрешать локальные исключения для программ	Отключен	Отключен
Разрешать исключения для удаленного управления	Отключен	Отключен
Разрешать исключения для общего доступа к файлам и принтерам	Отключен	Отключен
Разрешать исключения ICMP	Отключен	Отключен
Разрешать исключения для удаленного рабочего стола	Включен	Включен
Разрешать исключения для UPnP-инфраструктуры	Отключен	Отключен
Запретить уведомления	Отключен	Отключен
Разрешать ведение журнала	Не задан	Не задан
Запретить одноадресные ответы на многоадресные или широковещательные запросы	Включен	Включен
Задать исключения портов	Отключен	Отключен
Разрешать локальные исключения для портов	Отключен	Отключен

Межсетевой экран Linux

Операционные системы Linux содержат развитые функции управления сетевым трафиком. Наиболее широко используется межсетевой экран iptables. Программа позволяет осуществить настройки фильтрации пакетов существенно более точно, чем межсетевые экраны в Windows. Это объясняется тем, что в Linux имеется больше возможностей управления трафиком на низком уровне, чем доступно пользователям Windows.

Настройки запуска

Межсетевой экран iptables входит в состав практически всех современных выпусков Linux. Обычно при установке операционной системы задается вопрос, хотите

ли вы задействовать сетевой экран по умолчанию или нет. В зависимости от вашего выбора, программа будет либо запущена, либо выключена. Для того чтобы узнать, работает программа межсетевого экрана или нет, достаточно вывести на экран список процессов командой `ps -A` и отфильтровать его по названию службы командой `grep`. При этом набор правил фильтрации пакетов по умолчанию запретит доступ к ресурсам компьютера извне и ограничит некоторые функции работы в локальной сети.

Запуск межсетевого экрана в Red Hat можно осуществить командой:

```
/sbin/service iptables start
```

Для остановки демона в качестве параметра следует указать `stop`, для перезапуска (необходимо после редактирования конфигурации) — `restart`.

Для автоматического запуска программы межсетевого экрана при каждом старте системы достаточно выполнить команду

```
/sbin/chkconfig --level 345 iptables on
```

Примечание

В Linux существует несколько вариантов (уровней) загрузки. Они определяют, будет система стартовать в однопользовательском режиме, надо ли загружать графическую среду и т. п. Нормальному режиму работы соответствуют уровни 3 и 5; отличие между ними состоит только в том, что на уровне 3 не загружается графическая подсистема.

Примечание

В зависимости от используемого дистрибутива вы можете выполнить настройку служб специальными утилитами. Например, на рис. 5.8 представлен вариант настройки запуска службы утилитой `ntsysv` в Red Hat.

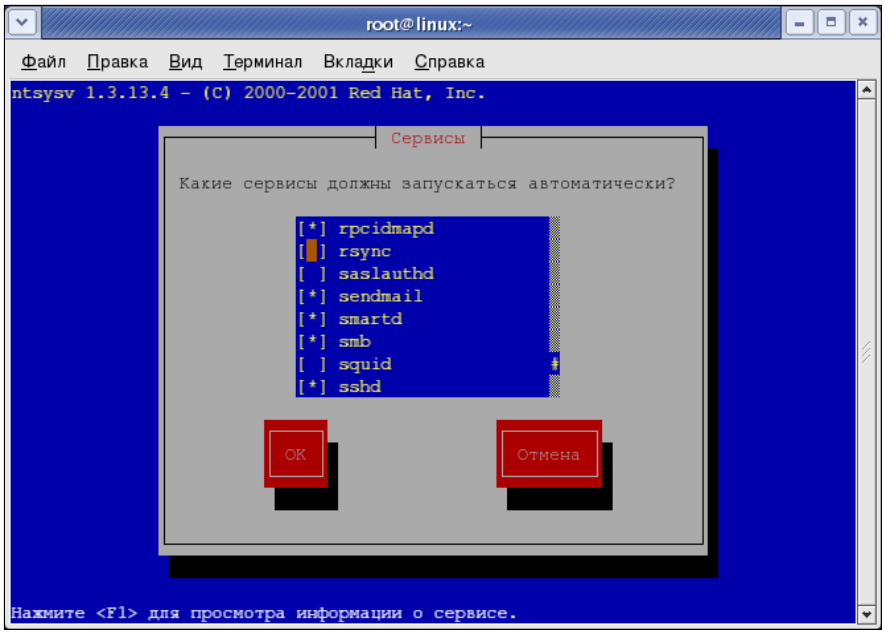


Рис. 5.8. Утилита для настройки параметров служб, работающая в текстовом режиме

Использование *iptables* в Ubuntu

Ubuntu является одним из наиболее популярных клонов Linux, поддерживаемым многими вендорами. В Ubuntu основным является упрощенный вариант межсетевого экрана, поэтому в системе нет сценария автозапуска программы iptables, отсутствуют соответствующие файлы настроек. Для использования iptables необходимо выполнить специальные шаги:

1. Создать необходимые правила фильтрации трафика с использованием команды `iptables`;
2. Экспортировать настройки в какой-либо 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:

```
pre-up iptables-restore < /etc/iptables.rules
post-down iptables-save -c > /etc/iptables.rules2
```

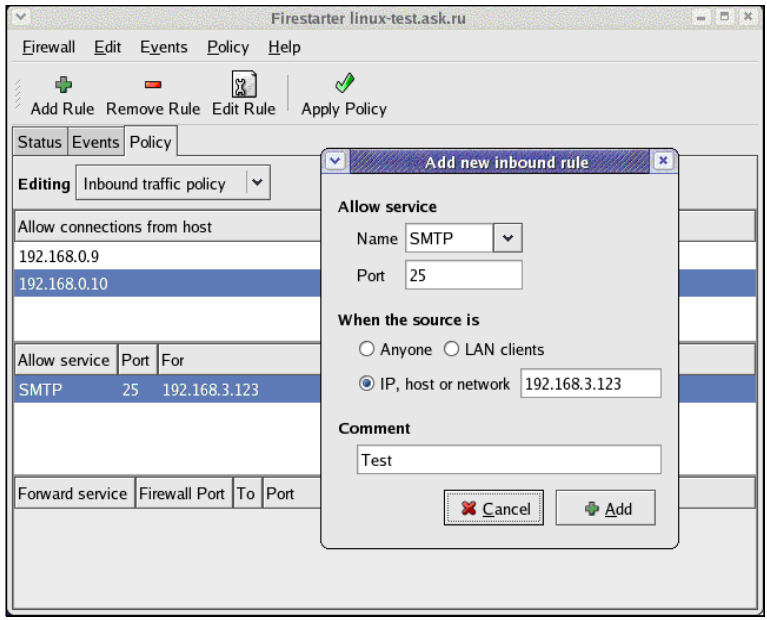
Эти команды будут выполняться каждый раз при включении и выключении сетевого интерфейса и активировать созданные ранее правила (сохранять в файл действующие настройки).

Обратите внимание, чтобы файл /etc/iptables.rules существовал перед перезагрузкой системы, в противном случае сетевой интерфейс не будет включен.

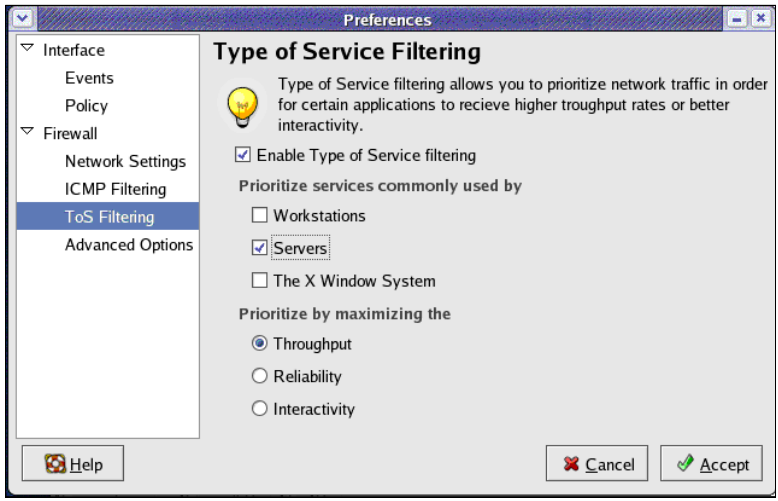
Программы графического управления *iptables*

Для точной настройки межсетевого экрана требуется обращение к командной строке и добавление соответствующих правил с полным набором параметров — условий, которым должен удовлетворять пакет, чтобы к нему было применено данное правило. Для пользователя, только начинающего работать в Linux, подобная настройка может вызвать существенные затруднения.

В большинстве случаев, чтобы обеспечить необходимый уровень безопасной работы в сети, достаточно применить стандартные ограничения. В таких ситуациях можно рекомендовать использовать для настройки межсетевого экрана графические утилиты. Их легко найти среди бесплатного программного обеспечения на сайте Surceforge.net. В качестве примера на рис. 5.9 показан интерфейс одной из таких программ.



а



б

Рис. 5.9. Графическая настройка параметров межсетевого экрана

На рисунке представлены экраны программы FireStarter. С ее помощью легко настроить часто используемые на практике параметры межсетевого экрана в графическом режиме. На рис. 5.9, *а* показано окно настройки правила публикации службы, а на рис. 5.9, *б* — включение возможностей приоритезации трафика. Программа позволяет наблюдать события межсетевого экрана, создавать правила входящего и исходящего трафика, настраивать режим совместного использования подключения и т. п.

Принципы работы *iptables*

Любой пакет несколько раз анализируется на соответствие некоторым условиям каждым сетевым интерфейсом компьютера. При удовлетворении условиям к пакету применяется соответствующее правило, и дальнейший анализ на данном этапе не проводится. Если ни одно из правил не содержит условий, соответствующих пакету, к нему применяются правила по умолчанию. Подобные наборы правил носят названия *таблиц*.

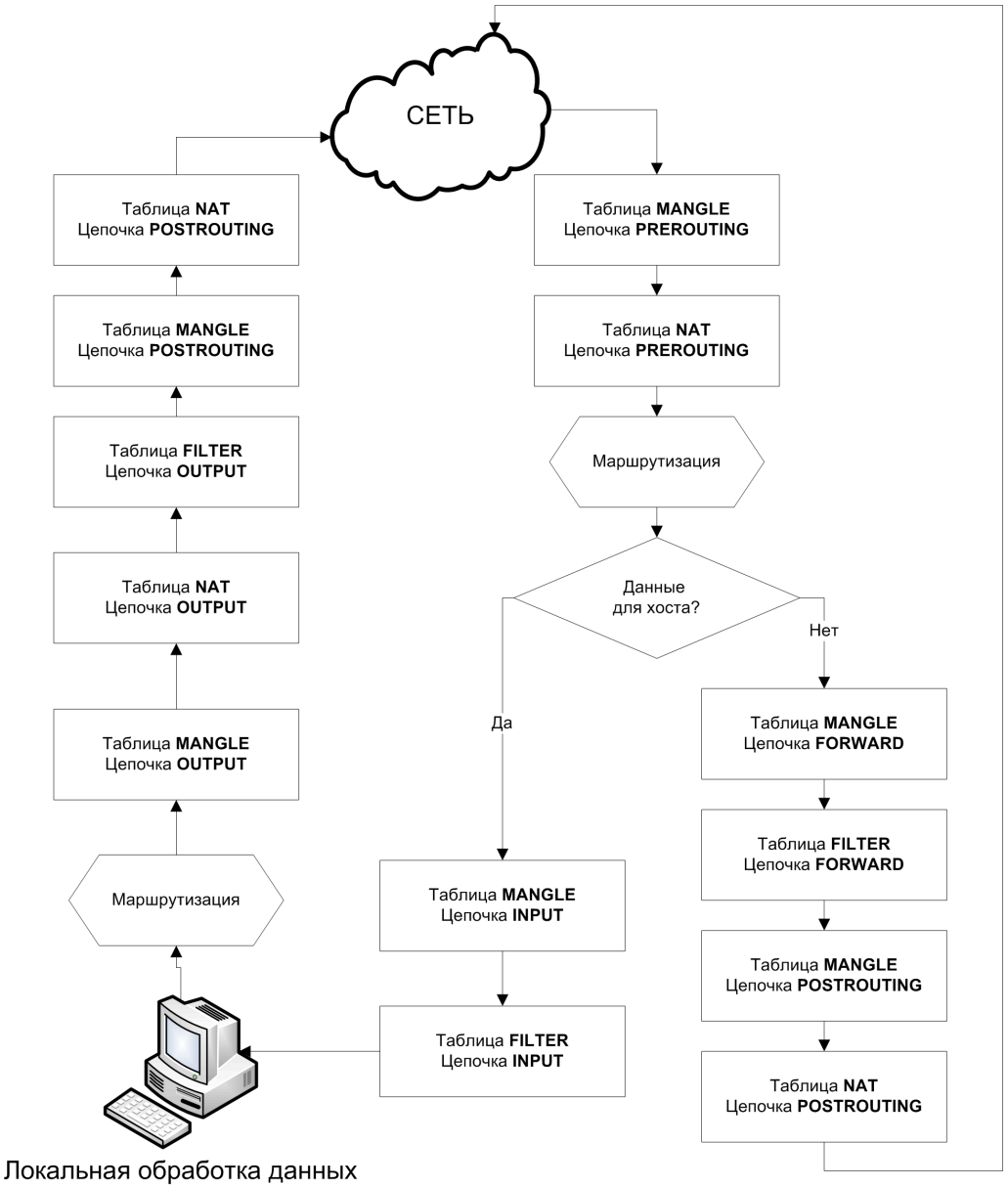


Рис. 5.10. Последовательность анализа пакета данных в фильтрах iptables

Существует три таблицы правил: filter — основная таблица, nat — используется для пакетов, создающих новое подключение (можно менять адреса источника и назначения пакета), и mangle, применяемая для специального типа пакетов.

На рис. 5.10 показана последовательность анализа пакета при его приеме или отправке. Для настройки межсетевого экрана следует создать правило по пути следования пакетов. Например, для фильтрации входящего трафика правила нужно создавать в цепочке INPUT, исходящего — OUPTUT. В цепочке FORWARD можно фильтровать трафик, маршрутизируемый системой (*проходящий* через сервер), PREROUTING используется для маршрутизации внешнего трафика на опубликованный внутренний ресурс и т. д.

> ***Примечание***
>
> Правила исполняются в порядке их списка. Поэтому обращайте внимание на их последовательность (команда `A` добавляет правило в конец списка, `I <номер>` — помещает в заданную позицию списка).

К пакетам, удовлетворяющим условиям фильтров, можно применить несколько действий: они могут быть пропущены (ACCEPT), удалены с сообщением источнику об ошибке передачи данных (REJECT) или уничтожены без оповещения (DROP). Существует также возможность настройки и применения пользовательского варианта обработки (QUEUE).

Создание правил межсетевого экрана

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. `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.

Описания параметров команды легко можно найти в Интернете. Более подробно процесс настройки iptables приведен в моей другой книге (см. Практическое руководство системного администратора. — СПб.: БХВ-Петербург, 2010. — 464 с.). Здесь же кратко рассмотрим пример команд, выполняющих минимальную настройку Linux-системы для работы в сети Интернета:

```
iptables -A INPUT -i eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth0 -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i eth1 -p tcp -m tcp --dport 22 -j ACCEPT
iptables -P INPUT DROP
iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to-source xxx.xxx.xxx.xxx
```

Первое правило разрешает внешнему интерфейсу (eth1) прием пакетов, которые являются ответом на исходящий трафик (состояние RELATED и ESTABLISHED).

Второе и третье правила разрешают весь входящий трафик по внутреннему и локальному интерфейсам.

Четвертое правило разрешает подключение из Интернета к серверу для управления по протоколу ssh (на практике желательно разрешать доступ не со всех систем, а только с конкретных адресов). Пятое правило переключает политику по умолчанию на DROP: никакие пакеты, кроме явно перечисленных ранее, не будут пропускаться.

Последнее правило включает режим NAT для внешнего интерфейса с явным указанием адреса, от которого должен проходить обмен с внешними системами.

Аутентификация доступа в Интернет

Встроенные межсетевые экраны Linux позволяют очень точно настроить правила фильтрации, но они не работают на уровне сессии. Поэтому в случае использования такой защиты в корпоративной среде у злоумышленников остается возможность присвоения себе адресов других компьютеров для обхода защиты. Выходом в такой ситуации является аутентификация *любой* попытки доступа в Интернет.

Подобные межсетевые экраны предлагают, как правило, коммерческие клиенты для систем на основе Windows. Вы можете приобрести такой продукт, но существуют и иные способы решения.

Один из них основан на подключении пользователя домена к совместно используемому ресурсу на межсетевом экране (такое подключение может быть легко настроено в сценариях входа в домен). Наличие подключения и его параметры используются в сценариях обработки запросов.

Другой способ заключается в предоставлении доступа к Интернету путем организации VPN-подключения к межсетевому экрану. Такой подход часто используется небольшими интернет-провайдерами, поскольку дает возможность легко подсчитать объем трафика каждого клиента.

Оптимизация доступа в Интернет

Большинство организаций пользуются выделенным каналом доступа в Интернет. Если этот канал безлимитный и скорость работы в Сети удовлетворяет пользователей, то дополнительных действий не требуется. В противном случае необходимо попытаться оптимизировать использование канала, для чего можно выполнить следующие пункты.

- **Установить локальный прокси-сервер и увеличить объем для кэширования файлов.**

  Практика показывает, что, например, картинки, использованные при оформлении сайта, меняются редко. А пользователи посещают в основном одни и те же ресурсы. Поэтому кэширование страниц Интернета на локальном сервере — *прокси-сервере* — может сэкономить при правильных настройках от трети до половины всего трафика. Поскольку запросы на эти ресурсы уже не будут отсы-

латься в Сеть, то страницы будут открываться быстрее, а полоса пропускания канала освободится для других действий.

- **Распределить полосу пропускания.**

  Если какой-то пользователь начнет загрузку большого файла (например, фильма с близлежащего сервера), то у всех остальных работа в Интернете практически замрет. В большинстве случаев можно ограничить полосу пропускания для больших по объему файлов, сохранив возможность быстрого открытия страниц Интернета. В результате закачка файла будет длиться чуть дольше, но все остальные сотрудники не почувствуют неудобства в работе. Подобную нарезку полосы пропускания могут делать современные прокси-серверы.

- **Блокировать рекламные ресурсы.**

  Объем рекламы (если считать по размеру файлов оформления на странице сайта) часто превышает размер полезной информации. Если отсечь эту рекламу на уровне шлюза в Интернет, то полезное использование канала существенно улучшится.

- **Настроить маршрутизацию внешнего трафика в зависимости от тарифов провайдера.**

  Если стоимость трафика через прокси-сервер провайдера выше расценок городского трафика и ниже междугороднего, то вы имеете возможность настроить маршрутизацию так, чтобы городской трафик "шел" напрямик, а междугородный использовал подключение к прокси-серверу провайдера.

  Примечание

  Объем трафика с местных сайтов, конечно, зависит от города, специфики организации и т. п. В среднем его доля может достигать 10% от общего объема трафика.

- **Осуществить организационные меры.**

  В случае платного канала обычно наиболее эффективны организационные меры снижения трафика Интернета, например, установление лимитов работы с последующей оплатой превышения трафика или отключением мультимедийного содержимого (пользователь сможет получить информацию из Интернета, но без картинок и т. п.).

Прокси-сервер

На прокси-сервере автоматически сохраняется на некоторый срок вся проходящая через него информация. Если прокси-сервер обнаружит запрос данных, уже имеющихся на нем в копии, 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.

Кроме того, современные прокси-серверы имеют развитые средства управления трафиком: на них можно блокировать содержимое по тем или иными критериям, нарезать полосы пропускания для пользователей и т. п.

Прокси-сервер сохраняет данные страниц в соответствии с теми показателями, которые заложены при их проектировании. Бывает, что разработчики не указывают такие значения и прокси-сервер использует свои настройки по умолчанию: в этом случае он может выдать пользователю устаревшие данные. Чтобы обновить страницу и загрузить последние данные, следует выполнить команду **Обновить** в меню программы просмотра. В этом случае прокси-сервер должен запросить актуальные данные из Интернета. Часто бывает и обратная ситуация. Администраторы увеличивают настройки сроков хранения некоторых типов файлов в кэше (например, иллюстраций), чтобы повысить эффективность работы прокси-сервера.

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. Важно соблюдать баланс: увеличение объема файлового кэша повышает нагрузку на процессор сервера (а обычно в качестве прокси-серверов администраторы настраивают не самые быстрые системы) и на его диски, что может привести к увеличению времени отклика.

На рис. 5.11 приведена реальная диаграмма использования кэша прокси-сервера по итогам работы за месяц (получена по анализу журналов работы). Хотя конкретные показатели будут отличаться в различных организациях, видно, что работа через прокси существенно снижает трафик интернет-организации.

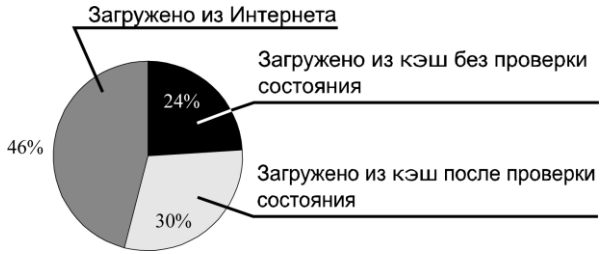


Рис. 5.11. Статистика использования кэша прокси-сервера

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. Так, в домене Windows настройки прокси-сервера могут распространяться через групповую политику.

Для автоматической конфигурации параметров использования прокси-сервера предназначен специальный сценарий. По умолчанию такой сценарий должен иметь

имя wpad.dat и публиковаться по протоколу HTTP на сервере с доменным именем WPAD.

Сценарий автообнаружения прокси написан на языке макропрограммирования. В случае необходимости его можно откорректировать. Например, при наличии двух точек доступа к Интернету сценарий может содержать функции случайного использования 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.

> ***Примечание***
>
> Обратите внимание, что если обозреватель получит из данного сценария параметры нефункционирующего прокси-сервера, то просмотр Интернета окажется невозможным.

Если вы имеете подобный сценарий (он, например, создается автоматически при установке прокси-сервера Microsoft ISA Server, другие примеры легко найти в Сети), то необходимо создать на DNS-сервере запись, которая указывала бы на хост WPAD (например, можно создать запись-синоним — CNAME).

Параметры сценария могут сообщаться также и сервером 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
```

В параметрах DHCP можно указывать и номер порта, на котором публикуется сценарий. В случае DNS-записей допустима публикация только по стандартному порту HTTP — 80.

"Прозрачный" прокси

Администратор может так настроить систему, что все интернет-запросы будут автоматически перенаправляться через прокси. При этом на пользовательском компьютере никакой настройки не выполняется. Причем все это будет происходить незаметно для пользователя, прозрачно (*transparent*).

Основное ограничение такого режима — прокси-сервер должен пропускать все запросы, поэтому никакой аутентификации пользователей (для разграничения доступа в Интернет) организовать не получится.

Особой настройки такой режим не требует. Прокси-сервер настраивается на пропуск анонимного трафика. А трафик организации в Интернет перенаправляется на вход прокси-сервера. В случае маршрутизатора на базе Linux подобное перенаправление можно сделать одной командой:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to squid:3128
```

В этом примере пакеты протокола TCP, приходящие на интерфейс eth0 на порт 80, перенаправляются на адрес *squid* и порт 3128 (порт по умолчанию для прокси-сервера Squid).

Настройка использования полосы пропускания

Существуют различные технологии регулирования полосы пропускания. Проще всего, на взгляд автора, это сделать, используя *прокси-сервер Squid*. Этот прокси-сервер бесплатен, существует в версиях как для Linux, так и для Windows и является фактическим стандартом прокси-серверов Интернета.

Для регулировки полосы пропускания удобнее всего применять следующий подход. Во-первых, можно назначить групповые лимиты для пользователей. Например, задать, что работники рекламы могут занимать не более 60% полосы пропускания, работники производственного отдела — 50% и т. п. Можно сделать структуру групп пользователей иерархической. В результате работники данного подразделения не смогут занять весь канал. При этом выделенная им полоса будет делиться между всеми поровну: много пользователей будут одновременно работать — будет низкая скорость, один пользователь получит весь лимит.

Во-вторых, можно назначить различную скорость загрузки файлов в зависимости от их размеров. В этом случае первая часть файла (до заданного объема) загружается на максимально настроенной скорости, а для последующей вступают в силу ограничения. Таким образом можно обеспечить всем сотрудникам максимально быструю работу с сайтами (поскольку оформление веб-страниц обычно не занимает большого объема и поэтому будет загружено на максимальной скорости) и сохранить возможность загрузки файлов большого размера (они будут загружаться, но со скоростью, которая не будет мешать остальным сотрудникам).

Чтобы включить управление полосой пропускания в Squid, нужно настроить пулы задержек, создать списки доступа, которые будут определять 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 позволяет 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 0. В конфигурации Squid сначала нужно определить число создаваемых пулов, а потом указать, какой пул к какому классу относится:

```
delay_pools 4 # Будет создано 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
```

Параметры лимитирования полосы пропускания определяются 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* (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 в 8 Кбайт. Обозначение `-1/-1` применяется в случае отсутствия лимитирования. Далее приведен пример конфигурации настроек в предположении, 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, потом — для класса 3. При этом последней командой для каждого пула должен быть включен запрет для всех, чтобы программа вышла из анализа по данному классу:

```
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.

В организации имеет смысл наладить фильтрацию контента интернет-трафика, например, запретив скачивание рекламы, порносайтов и т. п. Конечно, делать это нужно на основании распоряжения руководителя, но подготовить его системному администратору не составит труда.

Сегодня нет надежных алгоритмов определения типа содержимого. Например, сообщалось о разработке фильтров, анализирующих изображения на рисунках и позволяющих выявить порнографические фотографии, но о реальной эксплуатации таких технологий пока информации нет.

На практике применяется два подхода. Это блокировка сайта по ключевым словам (если на странице встретилось слово, занесенное в черный список, то загрузка такого содержимого будет блокирована) или по черным спискам (список сайтов, для которых известно, что они хранят определенное содержимое). Не стоит обольщаться, что такими списками будут "закрыты", например, все порносайты. Число порно-

сайтов превышает по разным оценкам несколько миллионов, и блокировать их тем или иным списком доступа просто нереально.

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, лучше использовать ограничения по доменам назначения, чем применять 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/** (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), 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 используйте 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 нужно использовать типы acl *url_regex, urlpath_regex, dstdom_regex* — в зависимости от того, какой вариант вы имеете.

После чего 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, попадаются ресурсы, случайно попавшие в такой список и нужные для текущей работы. Кроме того, некоторая часть, например, рекламы не будет отфильтрована. Такие случаи надо отследить по файлам журнала работы Squid и добавить новые условия фильтрации.

Удаленная работа

С повышением мобильности пользователей все чаще возникает необходимость обеспечить удаленный доступ к определенным ресурсам и реализовать полноцен-

ную работу в составе корпоративной сети. При этом администратору приходится решить несколько задач:

- обеспечить безопасное подключение к компьютерной сети организации (через публичные сети — Интернет или через модем);
- обеспечить приемлемую производительность для удаленных пользователей при работе по достаточно медленным каналам связи.

Удаленное подключение пользователей

Удаленный пользователь может подключиться к корпоративной сети двумя способами: через модемное подключение к одному из компьютеров сети или через общедоступные сети (Интернет). В обоих случаях это решение реализуется через настройку *сервера удаленного доступа и маршрутизации* (RRAS). При модемном подключении пользователь создает физический канал связи с RRAS, при работе из Интернета реализуется *логическое* подключение к RRAS через VPN (Virtual Private Network, виртуальная частная сеть).

Прием входящих подключений

Обеспечить подключение внешнего пользователя к системе можно как для рабочей станции, так и для сервера. Обычно практическое значение имеют два варианта: подключение через сеть Интернет и подключение через модем на данном компьютере.

Настройка рабочей станции

На прием входящих модемных соединений можно настроить рабочие станции Windows. Например, если вы хотите скопировать файлы с компьютера своего приятеля или поиграть с ним в сетевую игру, то совсем не обязательно создавать такое подключение через провайдера Интернета: достаточно один компьютер настроить для приема входящих соединений, а на другом использовать обычный вариант подключения к внешней сети.

Для создания входящего соединения следует запустить мастер создания новых подключений и выбрать опцию **Установить прямое подключение к другому компьютеру**. На следующем шаге необходимо включить опцию **Принимать входящие соединения** и отметить устройство, через которое будет осуществляться подключение. На завершающем этапе следует установить разрешения для тех пользователей, которые будут подключаться к данной системе.

Настройка сервера

При наличии подключенного модема после активизации сервера RRAS никаких дополнительных настроек администратора не требуется. Необходимые порты подключения модема создаются автоматически. Возможность доступа пользователей во внутреннюю сеть при таком подключении определяется политиками сервера RRAS (или службы RADIUS) — *см. разд. "Политики подключений" далее в этой главе*.

VPN

VPN (Virtual Private Network, виртуальная частная сеть) представляет собой способ расширения локальной компьютерной сети за счет включения в нее удаленных компьютеров через общедоступные сети. При подключении по VPN удаленный компьютер становится как бы участником локальной сети. Данные, которые должны быть переданы по VPN через открытые каналы связи, предварительно шифруются, "вкладываются" (инкапсулируются) в обычные пакеты и пересылаются серверу корпоративной сети. Все эти процессы происходят незаметно для пользователя. Внешнее впечатление такое, что создан специальный канал связи с корпоративной сетью и компьютер напрямик подключен к локальной сети.

Такой канал связи, предусматривающий инкапсулирование данных и их шифрование в процессе передачи, называется *VPN-соединением*. При работе по VPN на компьютере создается новое подключение к сети со своими параметрами настройки IP-протокола: IP-адрес из состава корпоративной (локальной) сети, данные внутренних DNS-, WINS-серверов и т. п. В качестве шлюза по умолчанию для компьютера при этом указывается шлюз удаленной локальной сети.

На практике используются различные варианты организации VPN-каналов. Вы можете просто купить "готовый канал VPN" (такие услуги предлагаются провайдерами, но они весьма дороги и используются только при подключении офисов) или использовать встроенные опции маршрутизаторов (если оборудование доступа в Интернет позволяет создавать входящие VPN-подключения). Однако наиболее простым и дешевым вариантом является создание программных VPN-подключений на базе операционных систем Linux или Windows.

> ***Примечание***
>
> VPN-канал можно применять в рамках одной локальной сети при подключении отделов, работающих с особо конфиденциальной информацией. Так, можно связать, например, отдел кадров и бухгалтерию для передачи данных о доходах сотрудников.

Настройки входящих VPN-подключений для Windows

Входящее VPN-подключение можно создать как для рабочей станции Windows, так и для серверной операционной системы. Следует отметить, что на рабочей станции одновременно может быть задействовано *только одно подключение*.

Настройка VPN-подключения на базе операционной системы рабочей станции

В качестве примера рассмотрим процесс настройки операционной системы Windows для организации возможности приема удаленных VPN-подключений. Можно выполнить одно подключение по любому из следующих интерфейсов: модемное соединение (рис. 5.12), инфракрасный порт, параллельный порт.

Создание VPN-подключения выполняется при помощи мастера новых подключений в следующей последовательности:

1. В мастере создания новых подключений выберите вариант **Установить прямое подключение к другому компьютеру**.

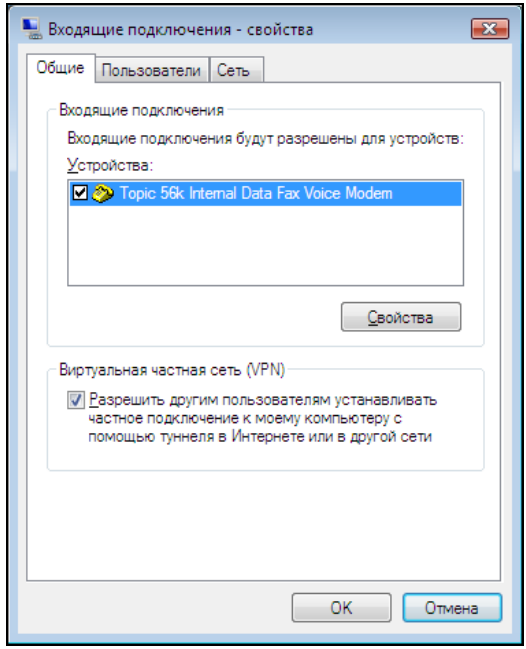


Рис. 5.12. Настройка параметров входящего подключения в Windows

2. Отметьте, что соединение должно обрабатывать входящие соединения (опция **Принимать входящие подключения**).
3. На вкладке о VPN-подключениях укажите, что вы хотите разрешить VPN-подключение, и выберите пользователей, которым будет разрешено использовать данное подключение.
4. На вкладке программного обеспечения в меню определения свойств IP-протокола настройте опции подключения удаленных пользователей к локальной сети: либо только к данному компьютеру (нужно снять флажок **Разрешить звонящим доступ к локальной сети**), либо ко всем компьютерам локальной сети (флажок установить). Также нужно определить параметры TCP/IP-протокола, которые будут использованы внешним клиентом. Адрес, получаемый VPN-клиентом, должен входить в подмножество адресов внутренней сети; как правило, на компьютерах сети в качестве шлюза используется адрес сетевой карты внутреннего интерфейса VPN-сервера.

Настройка VPN-подключений на базе серверной операционной системы

VPN-доступ в серверных операционных системах реализуется через службу RRAS. Администратору необходимо добавить столько портов для VPN-подключений, сколько потребуется в работе организации. Эта операция выполняется либо с помощью мастера настройки RRAS, либо вручную — простым добавлением нужного числа портов.

На практике обычно совмещают межсетевой экран и сервер входящих подключений по VPN. И создание входящих сессий в этом случае производится по правилам программного обеспечения межсетевого экрана.

VPN-подключения и межсетевые экраны

На практике могут быть реализованы различные варианты расположения VPN-сервера и межсетевого экрана организации. Можно расположить VPN-сервер за межсетевым экраном, внутри локальной сети, тогда МСЭ будет перенаправлять весь VPN-поток на локальную систему. Это является безопасным решением, поскольку на сервере VPN производится аутентификация пользователя и несанкционированные данные просто отбрасываются.

Если расположить VPN-сервер *перед* межсетевым экраном, то необходимо выполнить настройку МСЭ, разрешающую пересылку пакетов с VPN-сервера внутрь локальной сети.

Фильтрация трафика VPN

В системах Windows VPN-канал создается службой маршрутизации и удаленного доступа. Поскольку RRAS проводит аутентификацию пользователя, то весь VPN-трафик безопасно может быть перенаправлен на такой сервер. Для обеспечения безопасности сервера (предотвращения атак на другие службы) в этом случае достаточно установить фильтры, которые пропускают к нему *только* трафик VPN и отсекают иные пакеты.

Подобную настройку легко выполнить штатными средствами, не устанавливая дополнительно программы межсетевого экрана. Следует настроить следующие фильтры на интернет-интерфейсе сервера:

- *для подключения по протоколу PPTP*:
  - по умолчанию игнорировать все пакеты, кроме явно разрешенных (drop all packets except those that meet the criteria below);
  - разрешить IP-протокол на порт 1723 (разрешает передачу управляющего трафика PPTP);
  - разрешить IP-протокол с идентификатором 47 (разрешает передачу данных по PPTP);
  - разрешить IP-протокол на порт 1723 в варианте **TCP [established]** (настройка нужна, если инициатором соединения выступает сам VPN-сервер);
- *для подключения по протоколу L2TP*:
  - по умолчанию игнорировать все пакеты, кроме явно разрешенных;
  - разрешить пакеты на UDP-порт номер 500;
  - разрешить прохождение протокола с идентификатором 50;
  - разрешить пакеты на UDP-порт номер 1701.

Не забывайте, что для обоих фильтров необходимо разрешить прохождение как *входных* пакетов, так и соответствующих симметричных *выходных*.

Настройки клиентов для подключения по VPN

Настроить VPN-подключение к сети предприятия можно в любых операционных системах клиента. Но, например, каждая версия Windows имеет некоторые отличия

по созданию VPN-канала. В последних версиях (Windows XP, Windows 2000) данная операция выполняется с помощью мастера подключений.

Чтобы создать VPN-подключение к удаленной сети организации, достаточно вызвать задачу создания нового подключения и в мастере установок отметить вариант подключения к корпоративной сети, после чего просто ответить на запросы мастера.

> ***Примечание***
>
> Если параллельно с работой в корпоративной сети необходимо организовать использование Интернета (или доступ в иные сети) *не через сеть организации*, то в дополнительных настройках параметров подключения по VPN следует *отключить* применение *шлюза по умолчанию* из сети организации.

Действующий канал VPN будет отображаться пиктограммой еще одного сетевого соединения.

Политики подключений

Администраторы имеют возможность регулировать параметры доступа удаленных клиентов в локальную сеть.

> ***Примечание***
>
> Описываемые политики доступа определяют одновременно как возможность подключения по модему, так и создание VPN-подключения.

При использовании RRAS настройки доступа выполняются путем задания расписания входящих соединений (когда можно и когда нельзя устанавливать подключение) и путем *политики подключений*. На каждом сервере RRAS применяются свои политики доступа. При этом в домене не существует возможности централизации этих настроек. Точнее, администратор не может централизованно управлять политиками доступа RRAS. Но он может создать на каждом сервере RRAS одинаковые политики, определяющие права доступа к локальной сети в зависимости от членства в доменных группах, после чего централизованно настраивать доступ путем изменения состава этих групп. То есть если в организации имеется несколько точек доступа, то настраивать каждую из них следует индивидуально.

Возможный выход — это установка службы IAS (Internet Authentication Service). IAS — это реализация сервера RADIUS (Remote Authentication Dial-In User Service) на платформе Microsoft. RADIUS традиционно используется многими интернет-провайдерами для аутентификации подключаемых к сети пользователей. После установки IAS достаточно в настройках каждого сервера RRAS указать использование этой службы (в целях резервирования обычно настраиваются основной и резервный серверы IAS). Таким образом, *все серверы* удаленного доступа при попытках подключения пользователей будут обращаться к одному серверу IAS, а настраивать одну политику доступа гораздо удобнее, чем постоянно заботиться об идентичности параметров различных серверов.

Варианты аутентификации пользователей

Существуют различные варианты проверки данных пользователей, пытающихся осуществить подключение к локальной сети. По умолчанию используются безо-

пасные методы, предполагающие как шифрование пароля пользователя, так и шифрование передаваемых данных. Вряд ли администратору придется разрешать менее безопасные варианты, предусмотренные в целях совместимости с предыдущими версиями клиентов.

Самым безопасным способом аутентификации пользователя является использование *смарт-карт* (или их аналогов). Если имеется техническая возможность, следует использовать только этот вариант подключения, для чего в политике RRAS (или IAS) указать среди вариантов аутентификации пользователей *только протокол расширенной проверки подлинности* (*Extensible Authentication Protocol, EAP*).

Разрешения на подключения

По умолчанию политика RRAS не разрешает подключения к сети предприятия ни одному пользователю. В этом случае используются права доступа, прописанные в настройках каждого пользователя, а по умолчанию пользователи создаются *без наличия права* создания подключения.

Если администратор сохраняет политику подключения по умолчанию, то он должен *индивидуально* выдать разрешения пользователям на подключение к локальной сети. Для этого необходимо установить параметр разрешения доступа на вкладке настройки входных звонков профиля пользователя.

Другой способ разрешения состоит в создании собственных политик доступа, в которых право подключения предоставляется либо определенным пользователям, либо их группам. Создание и редактирование новой политики подключения не представляет никакой сложности и легко может быть выполнено любым специалистом.

Удаленное подключение к Linux

Linux изначально является многопользовательской системой с возможностью удаленного подключения и исполнения команд. Для него не требуется никаких дополнительных программ или режимов.

Наиболее безопасным способом удаленной работы с Linux является использование протокола OpenSSH. Создаваемое подключение в этом случае шифруется и данные недоступны для злоумышленника.

Чтобы иметь возможность такого подключения, на Linux должен быть запущен OpenSSH-сервер, а само подключение следует выполнять любым клиентом, поддерживающим SSH-протокол.

OpenSSH-сервер

OpenSSH-сервер входит в поставку операционной системы. Вам необходимо убедиться, что сервер SSH установлен и находится в режиме автоматической загрузки. Обычно установка SSH-сервера выбирается на этапе первичной инсталляции системы, так что администратору необходимо только уточнить параметры, используемые для подключения (как правило, более ужесточить по сравнению с параметрами по умолчанию).

Настройки сервера следует провести в соответствии с особенностями используемого вами дистрибутива Linux. Более никаких специальных действий выполнять не требуется.

Подключение SSH-клиента

Существуют различные версии SSH-клиентов, разработанных как для Linux, так и для Windows. Использование SSH в принципе не отличается от работы в режиме telnet, но выполняется по шифрованному каналу.

При первом подключении к Linux программа запросит вашего согласия на включение удаленного хоста в число доверенных систем. При желании вы можете предварительно скопировать ключ хоста Linux для использования в программе SSH-клиента. В этом случае можно при подключении использовать вместо пароля этот ключ.

Использование графических утилит для подключения к Linux

SSH-подключение обеспечивает работу с Linux-системой в режиме консоли (командной строки). Опытным администраторам этого достаточно для управления. Но можно подключиться к системе так же, как к терминальному серверу.

Если на Linux установлена графическая оболочка, то существуют программы, позволяющие работать в ней на удаленном компьютере. Наиболее распространенным средством такого подключения является применение кроссплатформенного пакета

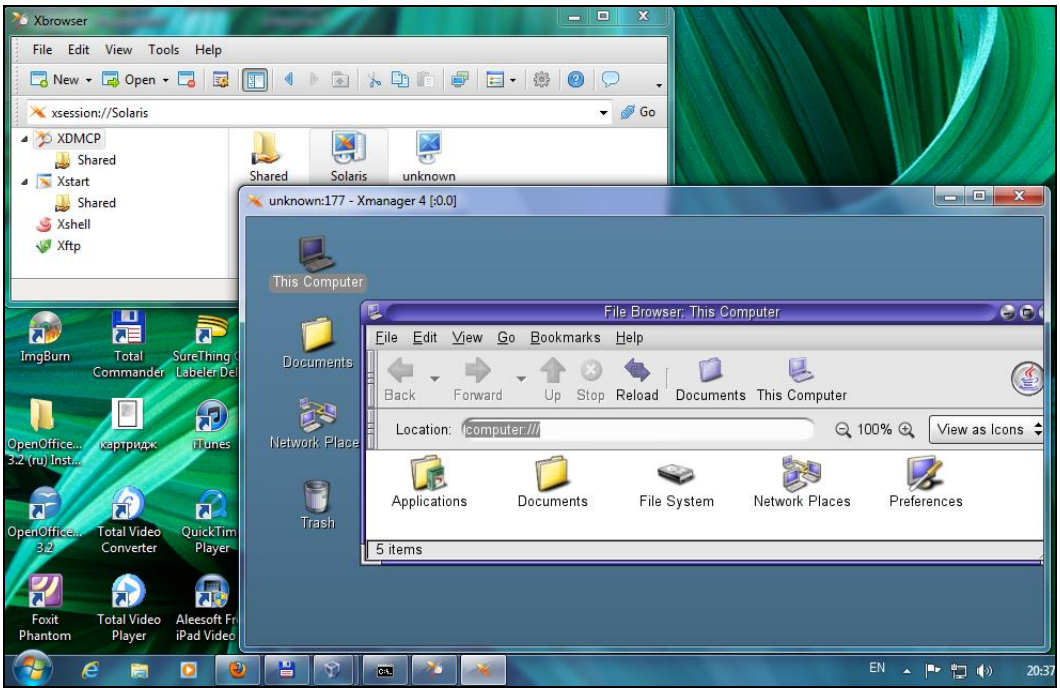


Рис. 5.13. Подключение к серверу Solaris с помощью Xmanager в среде Windows 7

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).

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

При числе одновременных подключений не более 2-х пользователей бесплатен и вариант NoMachine NX (**http://www.nomachine.com/**). Существуют и другие, коммерческие решения. Например, на рис. 5.13 показано пример подключения к серверу Oracle Solaris в срезе Windows 7 при помощи программы Netsarang Xmanager.

Подключения филиалов

Многие организации имеют несколько территориально разделенных площадок, которые должны работать в составе единой компьютерной сети. В этом случае локальные сети организаций должны быть соединены *туннелем*.

В настоящее время появилось много доступных моделей маршрутизаторов, с помощью которых можно как осуществить безопасный доступ организации в Интернет, так и настроить VPN-подключение к другому коммутатору. В результате между коммутаторами создается туннель, по которому осуществляется обмен данными между двумя локальными сетями. Преимущество такого решения — надежность (решения, заложенные в маршрутизаторы хорошо отработаны), стабильность работы (в маршрутизаторах используются Unix-подобные операционные системы), быстрота восстановления канала в случае обрыва связи и т. д.

Если покупка маршрутизатора представляется невозможной, то создать канал между локальными сетями можно и программно. По сути нужно создать те же VPN-подключения, но с некоторыми особенностями.

Во-первых, такое подключение должно устанавливаться автоматически и автоматически же восстанавливаться в случае разрыва. Во-вторых, через такое соединение должны передаваться пакеты не только на компьютер, осуществивший подключение, но и для всей удаленной сети (нужно, чтобы между сетями было установлено соединение).

Туннель между Linux-системами

Проще всего создать безопасное объединение локальных сетей, если в качестве пограничных компьютеров используются Linux-системы. Для создания такого подключения сначала организуется безопасное соединение сетей, после чего настраивается туннель и правила фильтрации трафика.

Возможны различные варианты безопасного подключения. Например, если с другой стороны канала имеется компьютер с установленной ОС Windows, то следует

настраивать VPN-подключение, а соединения между Linux-компьютерами легко выполняются с использованием протокола SSH.

Для того чтобы настройка осуществлялась без запроса пароля, в случае VPN он сохраняется в программе или записывается в файл (для Linux, доступ к файлу предоставляется только учетной записи, от которой выполняется подключение), а для SSH-подключения используются пары ключей учетной записи, что позволяет создавать соединение без запроса параметров учетной записи.

Настройка выполняется несколькими командами. Рекомендации по настройке широко представлены в Интернете, поэтому мы не будет особо останавливаться на них.

Постоянное подключение к серверу Windows

Описанный ранее вариант подключения удаленного офиса в случае реализации на ОС Windows носит название *интерфейса по требованию* (dial-in-интерфейса).

Создание интерфейса по требованию осуществляется мастером в задаче **Маршрутизация и удаленный доступ**. Достаточно выбрать в меню опцию создания нового интерфейса по требованию, дать ему имя, указать параметры учетной записи, с помощью которых будет осуществляться подключение к другому серверу, и ввести параметры удаленной сети для создания статической маршрутизации.

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*. То есть 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`.

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 сервером маршрутизации и удаленного доступа.

В случае разрыва канала...

В филиале может быть установлен контроллер домена только для чтения (RODC, описан *далее в этой главе*). Но в небольших предприятиях филиалы часто укомплектованы всего лишь несколькими компьютерами. В этом случае размещение в удаленном офисе контроллера домена не оправдано экономически.

При этом перед администраторами стоит задача обеспечить совместную работу филиала с центральным офисом. Достаточно часто качество канала связи с центральным офисом (Интернетом) оставляет желать лучшего; в результате при обрыве связи удаленные пользователи теряют возможность доступа к ресурсам не только 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*.

Существуют два возможных пути 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. В этом случае 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 синхронизировать 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 совместно используемым папкам на других компьютерах (к которым ранее не подключался) будет невозможно.

> ***Примечание***
>
> Кэширование паролей может быть отключено групповой политикой. В таком случае описанный режим будет недоступен.

Карантин клиентов удаленного подключения

> ***Примечание***
>
> Данная возможность присутствует в Windows 2003 Server. В Windows 2008 используется несколько другая технология — NAP (описана в *главе 9*).

Если компьютеры локальной сети находятся "под присмотром" администратора, то о состоянии систем, подключаемых средствами удаленного доступа, можно только предполагать. В результате, например, спамеры начинают активно использовать такие компьютеры: на них существенно проще установить программу-троян и заставить почтовую систему организации пересылать спам. Поскольку удаленный пользователь успешно регистрируется в системе, то почтовый сервер будет принимать от него для рассылки любую корреспонденцию. Поэтому естественно желание администраторов каким-то образом проконтролировать удаленную систему перед подключением.

В сервере маршрутизации и удаленного доступа присутствует возможность такой проверки. Происходит это следующим образом: при подключении удаленного клиента сервер проверяет политику доступа, и если установлены требования проверки клиента, то подключает систему и временно помещает ее *в карантин*. На клиенте в это время запускается программа, проверяющая выполнение определенных администратором условий. Результат проверки сообщается серверу удаленного доступа, который принимает решение отключить клиента или предоставить ему полный доступ в сеть.

Для выполнения таких действий необходимо установить службу карантина, которая входит в состав пакета Resource Kit Tools для Windows Server 2003 (бесплатно

загружается с сервера Microsoft). Установка выполняется запуском файла rqs_setup.bat, который создает на компьютере службу Remote Access Quarantine Service. После установки службы необходимо добавить в реестр параметр `AllowedSet` (тип `REG_MULTI_SZ`) со значением в виде версий сценариев, которые будут запускаться на клиентах.

Далее следует создать сценарий *(профиль)* удаленного входа клиента. Удобно использовать компонент Connection Manager Administration Kit (CMAK), входящий в состав сервера (установка через компоненты Windows в составе Management and Monitoring Tools). После запуска CMAK следует выбрать опцию создания нового профиля, дать ему имя[1] и создать New Custom Action. Именно эта настройка будет описывать параметры карантина.

В окне настройки **New Custom Action** следует указать программу (сценарий), который будет запускаться на клиенте. Эта программа может использовать ряд переменных, которые будут ей переданы системой (полный список доступен в онлайновой справке CMAK). Минимально в строке **Parameters** нужно указать:

- %DialRasEntry% (имя удаленного подключения/службы);
- %TunnelRasEntry% (имя туннельного подключения);
- %Domain% (название домена, к которому осуществляется подключение);
- %UserName% (имя пользователя);
- %ServiceDir% (путь к папке профиля).

Параметр **Action Type** следует установить в значение **Post-connect**, а **Run this custom action for:** — в значение **All connections**. Далее проверить, что установлены (отмечены флажками) параметры **Include the custom action program with this service profile** и **Program interacts with the user**, и сохранить изменения. Затем на вкладке **Additional Files** следует указать те файлы, которые необходимо иметь пользователю. Это, во-первых, программа карантина для клиента (rqc.exe), во-вторых — та программа (сценарий), которая будет запускаться на стороне пользователя.

После завершения работы мастер настроит профиль CMAK. Полученные в результате файлы будут сохранены в папке %SYSTEMDRIVE%\Program Files\CMAK\Profiles*<имя профиля, данное при его создании>*. Файл с именем, указанным вами при настройке CMAK, и с расширением exe необходимо передать пользователям, которые должны будут запустить его у себя для создания профиля подключения.

После настройки параметров подключения для клиента администратору системы необходимо создать политику удаленного доступа, которая определит параметры карантина, а именно: назначить время карантина (период ожидания сервером ответа от клиента перед его отключением) и IP-фильтры, которые должны ограничить доступ клиента к ресурсам сети во время карантина.

---

[1] Имя следует давать по требованиям названий файлов типа 8.3, поскольку это название станет именем исполняемого файла на клиенте (к нему автоматически будет добавлено расширение exe).

Настройка времени ожидания выполняется в меню редактирования профиля политики в разделе **Advanced**. В этом окне следует добавить атрибут с вендором Microsoft и названием **MS-Quarantine-Session-Timeout**. Значение этого параметра следует установить равным максимально допустимому периоду ожидания в секундах.

Второй возможный атрибут — это **MS-Quarantine-IPFilter**. После его добавления в свойствах следует выбрать те фильтры, которые должны быть активизированы на время карантина. Минимально необходимо разрешить входящий и исходящий трафик по порту 7252 (TCP). Этот порт по умолчанию используют программы карантина rqc/rqs. Необходимость открытия других портов определяется администратором (например, если нужно разрешить в это время использование DNS, то следует разрешить UDP 53 и т. п.).

Примечание

Network Access Quarantine Control (NAQC) может использоваться при подключении операционных систем Windows 98 SE/ME/2000/XP/Server 2003.

Контроллер домена только для чтения

Многие компании территориально размещены по нескольким офисам, будь то 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 в случае нестабильного канала 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 2008 Server 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 т. п. 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 2003 Server, 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*.

DirectAccess

В операционных системах Windows 7 Профессиональный/Максимальный выпуск и Windows 2008 R2 (данная технология требует также домен режима Windows 2008 Server, наличия развернутой структуры сертификатов) появилась возможность подключения к ресурсам внутренней сети предприятия без операций создания VPN (при подключении используются возможности безопасности протокола IPv6). Пример структуры подобного подключения представлен на рис. 5.14 (рисунок из библиотеки TechNet).

Преимущества решения DirectAccess — в отсутствии каких-либо пользовательских операций для подключения к локальной сети. Например, ноутбук из локальной сети переносится в глобальную сеть и по-прежнему продолжает работать с внутренним ресурсом. Если говорить "технически", то при работе в Интернете автоматически создается туннель к ресурсам локальной сети.

Настройка DirectAccess предполагает выполнение ряда операций. Подробно об этом можно прочесть в руководстве по адресу **http://technet.microsoft.com/ru-**

ru/library/dd630627%28WS.10%29.aspx (главная страница технологии доступна по адресу **http://www.microsoft.com/en-us/server-cloud/windows-server/directaccess.aspx**).

Особенностью технологии DirectAccess является постоянный контроль над клиентской системой со стороны IT-служб предприятия. Поскольку компьютер-клиент DirectAccess должен быть членом домена, а туннель подключения к домену всегда работает при наличии доступа в Интернет, то к компьютеру постоянно применяются действующие в организации технологии управления: выполняются групповые политики, обновляются антивирусные базы данных и т. п.

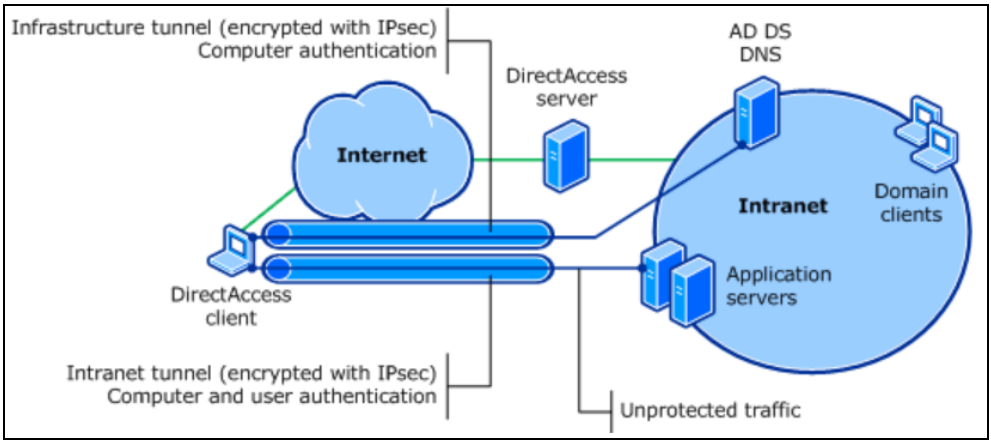


Рис. 5.14. Пример подключения к локальной сети с использованием DirectAccess

Сегодня технология DirectAccess пока не нашла широкого распространения в нашей стране. Причин несколько.

Во-первых, технология доступна только для клиентов указанных версий. Сегодня на предприятиях и в организациях продолжает эксплуатироваться большое количество систем Windows XP/2003, к ресурсам которых DirectAccess не позволяет подключиться.

Во-вторых, DirectAccess основано на возможностях протокола IPv6. Данный протокол реализован не в полной мере на предыдущих версиях Windows, что не позволяет подключиться к ресурсам, предоставляемым системами Windows XP/2003. Кроме того, при отсутствии инфраструктуры IP6 необходимо выполнить операции по настройке туннелирования протокола IPv4 в IP6.

В-третьих, технологии авторизации и аутентификации, применяемые в DirectAccess, существенно ограничивают круг межсетевых экранов. Рекомендуемым межсетевым экраном является продукт Microsoft, а для других решений требуется наличие сертификации Microsoft. В то же время исторически большинство организаций для доступа в Интернет применяет решения других вендоров.

Терминальный доступ

При удаленном подключении к офису пользователи хотят воспользоваться всеми сервисами, которые реализованы в локальной сети. Однако недостаточное качество каналов связи зачастую не позволяет эффективно работать во многих приложениях. Одним из вариантов решения данной проблемы является использование *терминальных служб*.

Принцип действия терминальных служб состоит в том, что все вычисления производятся на мощном удаленном компьютере (его называют *терминальным сервером*), а пользовательский компьютер является "удаленной консолью". Данные и команды, которые пользователь вводит (с клавиатуры, мышью), передаются на терминальный сервер, где они обрабатываются, а пользователю возвращаются лишь графические изменения в интерфейсе. Иными словами, пользовательский компьютер практически использует только монитор, клавиатуру, мышь.

В результате при работе в типовой офисной программе терминальный клиент в среднем передает по сети около 500 байт данных в секунду, что позволяет полноценно работать с удаленным компьютером, используя модемные соединения или медленные каналы связи.

Терминальные серверы от Microsoft

В 1995 г. компания Citrix выпустила продукт под названием Winframe, который стал первым терминальным сервером на базе Windows NT. После договора между Microsoft и Citrix о кросс-лицензировании в 1998 г. вышли версии Windows NT Server Terminal Server Edition и Citrix MetaFrame (продукт Citrix расширял возможности терминального сервера Windows NT TSE). В "поколении W2K" терминальные службы включены в поставку всей линейки серверов Windows 200*x* Server.

Терминальные клиенты

В качестве клиентов терминала могут служить практически любые компьютеры, в том числе и классов 386/486/Pentium, причем сами терминалы *не нуждаются в модернизации*. Поскольку все вычисления выполняются на сервере, то при необходимости нужно наращивать или обновлять *только* его мощности.

Одновременно использование терминалов снижает административные затраты на сопровождение. У пользователя становится меньше возможностей повлиять на стабильность работы системы, а администраторы начинают управлять "всем в одном месте". Терминальные системы более безопасны, поскольку устранение уязвимости на сервере ведет к аналогичному результату для всех его клиентов, и практически не оставляют никаких "вольностей" пользователю — ведь контролю администратора поддается практически все.

Кроме того, стоимость терминальных устройств существенно ниже полнофункциональных компьютеров. Терминалы могут быть выполнены на бездисковой основе (Linux-терминалы, которые можно загрузить по сети с сервера), так и на основе за-

грузки с тех или иных аналогов жесткого диска (например, DiskOnModule и т. п. — объем ядра Linux вместе с программой подключения к RDP-серверу составляет менее 8 Мбайт).

> ***Примечание***
>
> Тонкие клиенты на базе Linux обычно содержат в себе возможности подключения к различным терминальным службам (по протоколам Citrix ICA, RDP, Tarantella, X, telnet, tn5250 и т. д.). Пользователи могут бесплатно загрузить как исходные коды, так и готовые образы программ для любого варианта загрузки — с диска или дискеты, CD, по сети и т. п. (см., например, **http://thinstation.sourceforge.net/**).

Если в качестве клиента терминального сервера используется Windows XP/ Windows 7, то необходимое программное обеспечение для подключения к серверу уже установлено. Это программа Подключение к удаленному рабочему столу (вызов из меню **Пуск | Стандартные | Связь**). Однако желательно обновить ее до последней версии (например, с выпуском Windows 2008 сменилась версия протокола подключения). Имеющиеся версии можно продолжать использовать, но все же лучше бесплатно загрузить обновления с сайта вендора.

Обратите внимание, что для подключения к терминалу необходимо быть на нем либо администратором, либо членом группы Пользователи удаленного рабочего стола. Поскольку эта группа первоначально пуста, то в нее нужно добавить соответствующих пользователей.

Еще одно место, где контролируется право работы в терминале, — это параметр учетной записи пользователя, разрешающий такое подключение. По умолчанию это право *включено* для каждой учетной записи. Но администраторы могут задействовать этот параметр для индивидуальных запретов или разрешений.

Режимы терминальных служб

Существует два варианта подключения к рабочему столу удаленного компьютера.

- **Подключение к рабочему столу** (ранее *административный режим*) используется *только* для удаленного управления сервером или рабочей станцией. При подключении к рабочему столу сервера[1] одновременно могут работать не более двух человек, причем обладающих административными правами на данном сервере. В этом режиме не требуется дополнительных лицензий.
- В **терминальном режиме** (ранее назывался *режим приложений*) для подключения необходимы дополнительные специальные лицензии, но количество одновременных подключений не ограничено, причем работать на сервере могут и пользователи с обычными, не административными правами.

[1] К рабочей станции можно удаленно подключиться только одному администратору, при этом текущий пользователь отключается от рабочего стола. Ограничение это, скорее, лицензионное, поскольку в Интернете можно найти решения, снимающие ограничения на количество удаленных сессий и фактически превращающие рабочую станцию в терминальный сервер.

Лицензирование терминальных служб

Для использования *терминальных служб* необходимы специальные лицензии, которые приобретаются отдельно от сервера. Существуют различные схемы лицензирования, на которых мы не будем останавливаться. Лицензии достаточно дороги для того, чтобы обеспечить благожелательное отношение к вам продавца при обращении за консультациями.

Лицензии специфичны для каждого выпуска, иными словами, лицензии от сервера Windows 2003 не подойдут для Windows 2008. Лицензии должны покупаться для каждого подключения, независимо от того, подключается ли рабочая станция Windows 7 Ultimate или бездисковая Linux-система.

"Технически" необходимость выдачи лицензий предполагает установку в локальной сети (и активацию) специального *сервера лицензий*. При работе в составе домена Windows сервер лицензий необходимо устанавливать на контроллере домена. Если использовать вариант установки **Enterprise**, то сервер терминальных лицензий будет обнаруживаться клиентами автоматически (используя службу каталогов) в любом домене леса, но только в пределах данного сайта.

Сервер лицензий обязательно должен быть активирован через сайт изготовителя. Также активируются клиентские лицензии. В случае необходимости администраторы легко найдут в Сети любые рекомендации по выполнению данной операции. Без активации лицензий сервер создает временные лицензии, которые можно использовать в течение 90 дней. Но и постоянные лицензии также не выдаются клиентам на неограниченный срок: они периодически обновляются, чтобы восстановить лицензии, "отданные" компьютерам, которые уже больше не работают в сети (например, вышли из строя).

> ***Примечание***
>
> После установки лицензий имеет смысл выполнить резервное копирование сервера, чтобы можно было восстановить лицензии.

Особенности использования приложений на терминальном сервере

Режим терминального сервера не предназначен для использования программ, вызывающих интенсивную нагрузку на процессор. Не рекомендуется использовать этот режим для мультимедийных и аналогичных приложений. Такие задачи целесообразнее решать на локальных системах. Терминальный сервер предназначен прежде всего для "обычных" офисных программ.

Установка прикладных программ в режиме приложений должна использовать специальные условия. Эти условия реализуются автоматически при запуске установки через утилиту установки и удаления программ, расположенную в Панели управления (или когда установка производится файлом setup или install).

После установки приложения имеет смысл проанализировать внесенные изменения в автозагрузку. Например, многие программы выводят в системной области панели задач некие индикаторы. Так, антивирусная программа показывает наличие и со-

стояние защиты на компьютере. В большинстве случаев такие индикаторы только отнимают лишние ресурсы системы и могут быть отключены в целях повышения производительности.

Для корректной работы приложений в режиме терминального сервера должен выполняться ряд условий (отсутствие записи данных в каталоги самой программы и т. д.). Эти требования стали предъявляться и программам, предназначенным для установки в Windows 7/Windows 2008, поэтому такие условия обычно выполняются. Но на практике можно встретить любую ситуацию. Исправить ее можно включением специальных сценариев (подробности можно уточнить в сопроводительной документации).

Безопасность терминальных сессий

Терминальный сервер, как сервер публичного доступа, обычно нуждается в более строгих ограничениях, чем персональный компьютер пользователя.

> ***Примечание***
>
> Конечно, как и при всяких настройках, администратору нужно представлять возможные опасности и разумно реализовывать только необходимые ограничения. Если вы включите *все* те ограничения, параметры которых присутствуют в групповых политиках для терминального сервера от Microsoft, то нормально работать в терминальной сессии не сможет ни один пользователь.

Поскольку терминальный сервер предоставляется многим пользователям, то крайне важно администратору сохранить его работоспособность, не давая пользователям устанавливать лишние 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. Администратору нужно найти золотую середину.

В частности, пользователей нужно ограничить применением только заданного перечня программ. Следует запретить им доступ к локальным ресурсам сервера, ограничить в выполнении ресурсоемких операций, лишить права устанавливать новые программы и т. п. Приведу небольшой список возможных ограничений.

> ***Примечание***
>
> Желательно создать специальное подразделение в службе каталогов (OU, Organization Unit), в которое переместить терминальный сервер. Для этого OU следует назначить собственную групповую политику, в которой и определить необходимые ограничения.

- Ограничить список программ, которые разрешено запускать пользователям терминала.
- Ограничить перечень устройств, к которым предоставляется доступ пользователю терминала. Например, исключить доступ к CD-ROM, сменным дискам и т. д.
- Без необходимости не стоит разрешать пользователю подключать как диски своего компьютера, так и с любых других систем (для исключения запуска программ с этих носителей).

- Желательно отключить возможность установки пользователем программ с использованием Windows Installer.
- Рекомендуется запретить просмотр и поиск *любых* ресурсов (например, просмотр сети, поиск принтеров, поиск файлов и т. п.).
- Желательно настроить административные шаблоны для таких задач, как: Проводник, меню **Пуск**, Панель управления и т. д., ограничив состав возможностей только необходимыми функциями.

> ***Примечание***
>
> Операцию поиска в Проводнике можно вызвать быстрыми клавишами <Ctrl>+<E>. Чтобы заблокировать эту возможность, создайте файл с некоторым поясняющим текстом (например, текстовый или в формате HTML) и установите следующие значения реестра системы: `HKLM\SOFTWARE\Microsoft\Internet Explorer\Search` параметры `SearchAssistant=REG_SZ: <путь к файлу>` и `CustomizeSearch=REG_SZ: <путь к файлу>`. Теперь при попытке выполнить операцию поиска пользователь увидит только содержание данного файла.

В общем случае следует руководствоваться принципом: чем более публичным является терминальный сервер, тем большие ограничения должны налагаться на его использование в целях предупреждения не всегда разумных инициатив пользователей.

Подключение к консоли терминального сервера

Если вы работали за консолью сервера, войдя в систему локально с клавиатуры, а потом попытались подключиться для удаленного управления, то по умолчанию будет создана новая сессия, со своим экраном, а не тем, который вы оставили. Это не всегда удобно для администраторов: иногда необходимо увидеть сообщения, которые отображаются после старта системы (например, сообщения от системы контроля серверной платформой или предупреждения о неудачном запуске службы), или использовать задачи управления, доступ к которым сохранен на локальном столе, или просто продолжить работу с документом, который остался открыт, когда вам неожиданно пришлось уйти с рабочего места.

Для работы с экраном консоли нужно запустить клиента подключения к удаленному рабочему столу с ключом `/console`:

```
MSTSC /console
```

Этот ключ можно указать в параметрах (свойствах) ярлыка подключения. Кроме того, есть возможность переключиться в консольную сессию, уже работая в терминале. Среди команд терминала есть утилита SHADOW, позволяющая подключиться к любой терминальной сессии. Сессия консоли всегда имеет нулевой номер, поэтому достаточно выполнить команду:

```
SHADOW 0
```

В отличие от запуска подключения с ключом (`MSTSC /console`), данная команда не сможет подключить к консоли, если с последней предварительно не был выполнен вход в систему.

Подключение администратора к сессии пользователя

Администратор терминального сервера (точнее, тот пользователь, которому такое право дано протоколом RDP; по умолчанию это только администраторы терминального сервера, но при необходимости данное значение можно изменить, воспользовавшись оснасткой управления параметрами RDP-протокола) имеет возможность подключиться к пользовательской сессии. Данный режим обычно служит для оказания помощи пользователям терминального сервера: администратор получает возможность наблюдать за чужим экраном и демонстрировать выполнение операций.

Операция выполняется через задачу управления терминальными сессиями исполнением соответствующей команды меню свойств. По умолчанию для выполнения данной операции система запрашивает подтверждение пользователя. Однако можно легко установить настройки, позволяющие выполнить операцию и без такого согласия. Иными словами, администратор может подсмотреть таким способом за пользователем, причем последний не будет подозревать о наличии такого контроля.

Эти настройки определяются в параметрах по умолчанию для терминальной сессии.

Публикация приложений в терминале

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. Публикация приложения позволяет работать в нужной программе без ее установки на локальную систему.

Для терминалов Microsoft можно реализовать такие настройки подключения, которые внешне соответствуют подключению к одной задаче. В версии терминальных серверов Windows 2000/Windows 2003 достаточно в свойствах подключения на вкладке **Программы** указать параметры вызываемой задачи (рис. 5.15). После этого при подключении пользователя к терминальному серверу автоматически запускалась указанное приложение. Если пользователь завершал работу в приложении, то вслед за его закрытием прерывалось и подключение к терминальному серверу.

Настройку запускаемого приложения обычно администраторы использовали для таких пользователей, как бухгалтеры: подключение к терминальному серверу для них воспринималось просто как запуск программы 1С.

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

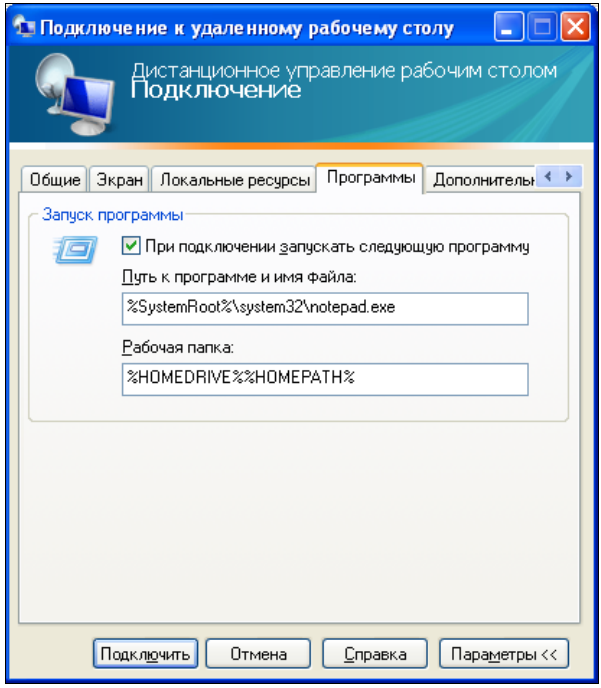


Рис. 5.15. Настройка запуска в терминальной сессии заданного приложения

терминального сервера — параметры настройки подключаемого приложения будут просто проигнорированы.

Удаленные приложения (RemoteApp) в Windows 2008 настраиваются через **Диспетчер удаленных приложений (RemoteApp) 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. 5.16).

Данная оснастка позволяет из одного места настраивать основные параметры терминального сервера. Панель навигации в правой части окна отображает операции, доступные для каждого выделяемого объекта.

Перенос настроек приложения в параметры подключения предоставил администраторам дополнительные возможности. Удаленное приложение стало возможным *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.

> ***Примечание***
>
> Существует возможность разрешать запуск на терминале только приложений, публикуемых через список *RemoteApp*.

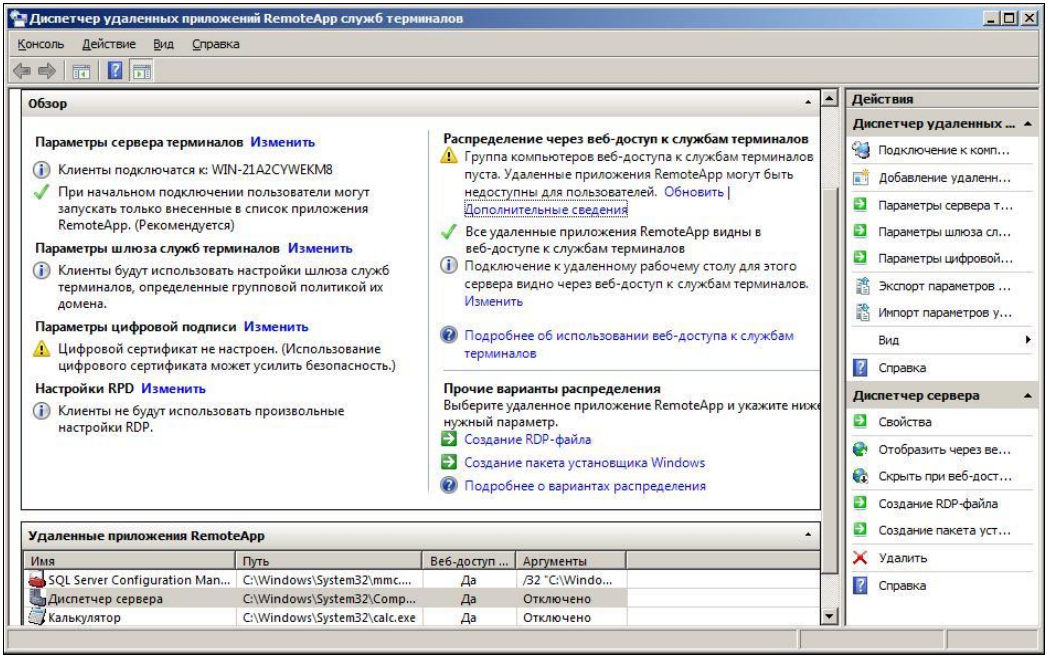


Рис. 5.16. Диспетчер удаленных подключений

Веб-доступ к терминальному серверу

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, использовать для работы можно только Internet Explorer и необходимо иметь права и разрешающие настройки обозревателя для установки ActiveX. Реальное подключение к терминальной сессии осуществляется по протоколу RDP (Remote Display Protocol, протокол для удаленных дисплеев), что требует и открытого порта 3389.

Веб-доступ в версии Windows 2008 несколько изменился. Теперь на исходной странице публикуются не только ссылки на доступ к терминальной сессии, но и перечень опубликованных приложений (рис. 5.17).

По умолчанию веб-интерфейс доступен по пути **http://<*имя_сервера*>/ts**.

Веб-интерфейс удобно использовать для разового доступа к необходимому приложению не с компьютеров локальной сети. При постоянном использовании рациональнее ссылку на такое приложение сохранить на локальном компьютере. Администраторы могут настроить веб-интерфейс таким образом, что на нем будут опубликованы приложения с различных терминальных серверов внутри организации. Но это, конечно, решение уже для крупных предприятий.

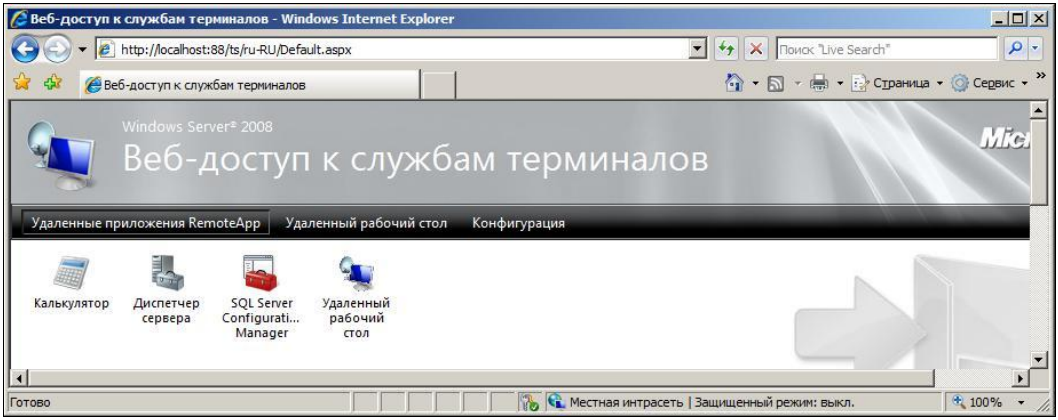


Рис. 5.17. Веб-интерфейс терминального сервера

Шлюз терминалов

Если необходимо обеспечить подключение пользователей, работающих в Интернете, к ресурсам, расположенным на различных терминальных серверах внутри локальной сети организации, то администраторы должны были настраивать публикацию для каждого терминала, а пользователи — вручную создавать несколько подключений, для каждого ресурса отдельно.

В Windows 2008 Server появилась функциональность шлюза терминалов. Шлюз терминалов позволяет публиковать в Интернет по одному адресу несколько внутренних терминальных серверов.

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. Регулируется доступ к внутренним терминалам обычным способом, с помощью политик.

Настройка шлюза терминалов не представляет особой сложности, и мы специально останавливаться на ней не будем.

Создание локальных копий данных

Пользователю, удаленно работающему с ресурсами организации, хочется выполнять работу так же быстро, как если бы он находился в офисе, и иметь возможность завершения работы независимо от наличия удаленного доступа к офису. Выходом в такой ситуации является создание копий данных на мобильном устройстве с последующей их синхронизацией с сервером. Такое решение позволяет пользователю продолжать работу полностью в автономном режиме.

Примечание

Первой программой Windows, предназначенной для синхронизации данных двух источников, была программа Портфель. Данная программа сохранена и в текущих вер-

сиях ОС, однако она является *индивидуальным* решением. Пользователь должен вручную помещать в Портфель файлы, с которыми он предполагает работать в другом месте, а потом также вручную проводить синхронизацию изменений. С основами работы в данной программе легко разобраться, воспользовавшись интерактивной справочной системой.

BranchCache

Технология BranchCache предназначена для ускорения работы с документами в филиалах за счет их кэширования. Технология появилась только в Windows 7/Windows 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 серверов Windows 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).

Существует 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, 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), т. е. его хэш-функцию. 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, получив 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

[1] Поэтому компьютеры должны находиться в пределах локального сегмента сети.

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. Дополнительно желательно — для повышения уровня защищенности данных — настроить для серверов использование сертификатов (описание доступно в документации по технологии).

Автономные файлы

В Windows предусмотрена возможность кэшировать сетевые ресурсы на локальный компьютер. 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.

Сделать файлы сетевой папки доступными в автономном режиме можно, разрешив ее кэширование (рис. 5.18). 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.

Работа с файлом при наличии подключения к сетевому ресурсу будет проводиться именно с сетевой копией. Операции синхронизации (с учетом их настроек) сделают обе копии файлов идентичными.

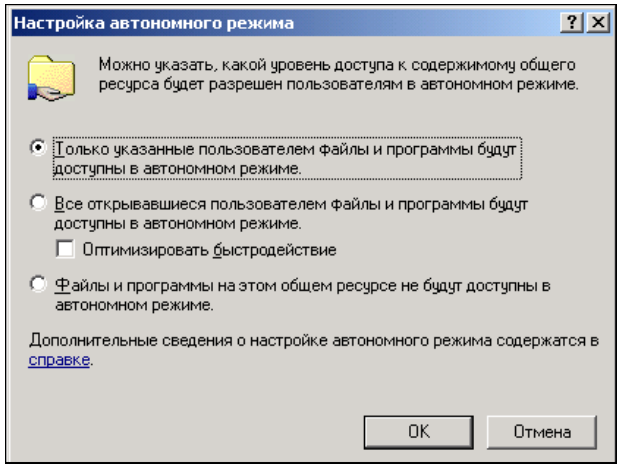


Рис. 5.18. Включение и настройка автономных файлов

Существует несколько вариантов кэширования файлов. При *ручном способе* на локальный диск копируются только файлы, явно отмеченные пользователем. Если выбрать вариант *автоматического кэширования документов*, то на локальном диске будут создаваться автономные копии тех документов, которые открывались пользователем.

Опция **Создать ярлык папки автономных файлов на рабочем столе** позволяет вывести на рабочий стол ярлык к папке, в которой хранятся автономные копии файлов. Эта опция удобна, если вы предполагаете продолжить работу с файлами в автономном режиме.

Для автоматического кэширования файлов выделяется по умолчанию 10% объема жесткого диска. Эта величина может быть изменена в настройках опций автономных файлов. Если объем автономных файлов превышает заданный лимит, то система автоматически удаляет самые старые версии. Таким образом, в автоматических режимах нет гарантии, что все необходимые файлы будут доступны автономно. Система может удалить часть из них, если будет достигнут порог допустимого использования жесткого диска. Обратите внимание, что объем автономных файлов, которые были кэшированы в ручном режиме, не учитывается в данном лимите, т. е. выбранные *вручную* файлы *всегда будут доступны автономно*.

Варианты синхронизации автономных файлов

Существуют различные варианты синхронизации автономных файлов с сетевыми ресурсами. Вы можете установить синхронизацию при входе и/или выходе из системы, по заданному времени или в период нахождения компьютера в ждущем режиме (рис. 5.19).

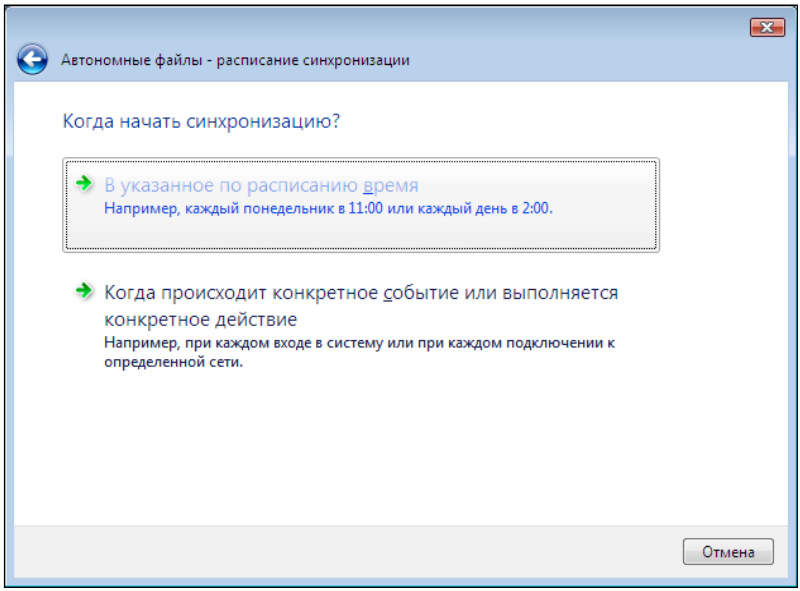


Рис. 5.19. Настройка вариантов синхронизации автономных файлов в Windows

Настройки синхронизации устанавливаются в программе Синхронизовать, которая расположена в меню **Пуск | Стандартные**. Заметьте, что синхронизация может быть проведена только в то время, когда пользователь совершил вход в компьютерную сеть.

Разрешение конфликтов

В случае работы с автономными копиями файлов возможно возникновение ситуаций, когда документ редактировался как автономно, так 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 200*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 из-за межсетевого экрана

Заблуждением является мнение, что межсетевой экран препятствует любой попытке подключения извне к персональному компьютеру. 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 любом пользователю. На рис. 5.20 (из руководства LogMeIn) доходчиво объясняется обычному пользователю про его возможности подключения к данным локальной системы из любой точки Сети.

Идея доступа к локальному компьютеру извне заключается в следующем. На компьютер устанавливается программа, которая инициирует подключение к заданному 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 нему осуществляется через сервер соответствующей программы. Обычно в этих целях применяется обозреватель Интернета (поскольку эта программа доступна в любых интернет-кафе и других публичных точках).

Подобных решений существует много. Можно упомянуть LogMeIn (бесплатное решение, **https://secure.logmein.com/solutions/personal/**), 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.

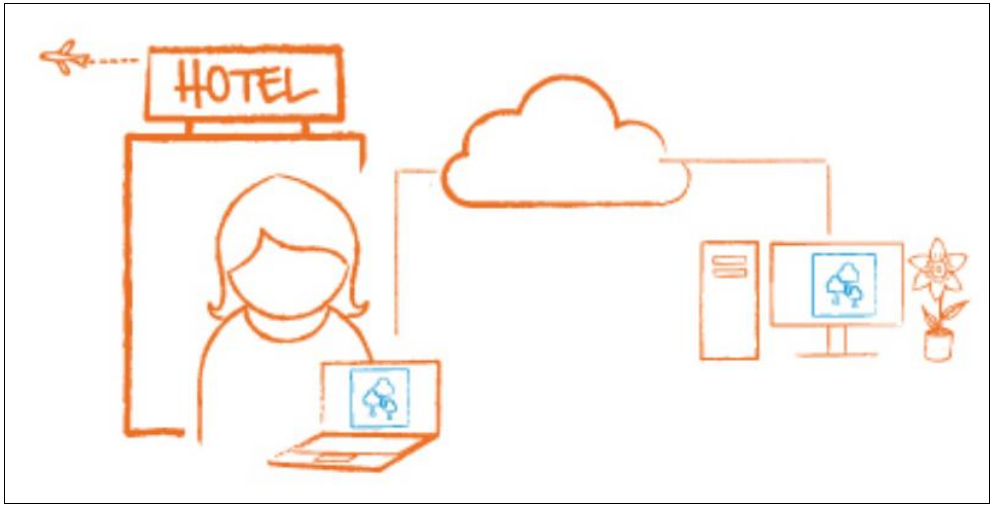


Рис. 5.20. Подключение к данным компьютера возможно из любой точки Интернета

Предотвратить описанный способ нарушения безопасности информационной системы можно, если полностью исключить возможность установки пользователем приложений (тотальным контролем запускаемого программного обеспечения).

ГЛАВА 6

Управление информационной системой

Деятельность по управлению компьютерной информационной системой нуждается в инструментах, которые помогут администратору выполнять многие рутинные операции. В текущей работе администратору информационной системы обычно нужно:

- ❒ знать состав информационной системы;
- ❒ контролировать функционирование ее компонентов;
- ❒ обеспечивать единые параметры приложений;
- ❒ иметь инструменты централизованного управления.

Инвентаризация

Часто документированию информационной системы уделяется недостаточное внимание, поэтому новому администратору приходится тратить много усилий на проведение инвентаризации: построение схемы сети, составление списка компьютеров, используемого программного обеспечения и т. п.

Построение топологии существующей СКС

Для устранения неисправностей линий связи необходимо знать, как соединено активное оборудование, к какому порту подключен конкретный компьютер. Администратор должен иметь комплект документации, в которой были бы описаны линии связи, приведены журналы кроссировок (помимо тех таблиц, которые обычно наклеиваются на коммутационные шкафы), хранились бы результаты приемочных тестов и сведения о проведенных ремонтах и т. п.

Сведения о топологии реальной сети, информацию о портах и подключенном к ним оборудовании можно собрать автоматически, если структурированная кабельная сеть (СКС) построена на *управляемых* коммутаторах.

Для построения подобных схем соединения существуют различные программы. В случае "простых" схем применимы и бесплатные версии. Так, на рис. 3.3 *(см. гла-*

ву 3) представлена схема соединений реальной сети, автоматически составленная одной из таких бесплатных программ.

Если сеть разбита на отдельные сегменты (виртуальные сети) и в ней присутствуют резервные каналы связи и т. п., то возможностей бесплатных версий оказывается недостаточно. В этом случае для составления схемы, если она не была составлена прежним администратором, можно воспользоваться триальными версиями программ, впоследствии вручную отслеживая вносимые изменения.

Примечание

После построения структуры сети программными средствами не забудьте перенести на схему номера соответствующих портов (так, как они нанесены на шильдики оборудования), патч-кордов (они должны иметь бирки с каждой стороны), номера кабелей (по проектной документации и как они фактически промаркированы) и т. п.

Инвентаризация физических каналов связи

Инвентаризация кабельной инфраструктуры является одной из самых сложных задач при наличии разветвленной сети предприятия. В лучшем случае у администратора есть кабельные журналы, в которых приведен перечень кабелей и списки соединений, выполненных на коммутационных панелях. Часто эти списки не актуальны, а реальные подключения знает только сам администратор.

Если у администратора нет полной инвентаризации, начиная от расположения кабелей, назначения портов коммутационных панелей и заканчивая списком установленного программного обеспечения, то на устранение повреждений, от которых никто не застрахован, может потребоваться длительный промежуток времени, в течение которого предприятие будет нести убытки из-за непредоставления услуг информационной системой. Чем более подробно будет составлена соответствующая документация, чем тщательнее она поддерживается в актуальном состоянии, тем легче сориентироваться в аварийной ситуации.

Существуют специальные программы, ведущие учет рабочих мест, соединительных кабелей и другого оборудования, которые позволяют в случае необходимости быстро вывести всю информацию о пути соединения точки "А" и точки "Б", а именно: номер розетки, кабель, номера коммутационных панелей и портов, на которые разделены кабели, и другую информацию. Первоначальный ввод данных в такие программы, т. е. данных о размещении на чертежах рабочих мест и коммутационного оборудования, а так же занесение данных о соединении портов и т. п., выполняется вручную на основании реализованного проекта СКС.

В последнее время производители оборудования СКС начинают предлагать различные решения *автоматизированного* управления кабельной инфраструктурой. Эти решения основаны, как правило, на внедрении дополнительного служебного *(девятого)* проводника в коммутационных шнурах. Коммутационные панели оснащаются дополнительными контактными площадками, специальные модули осуществляют сбор сведений о фактических подключениях и передают их в отдельную систему контроля (решения PatchView компании RiT Technologies, технология

Itracks, система iPatch Real Time Infrastructure Management от компании SYSTIMAX Solutions и др.). Такой подход позволяет построить схему подключений в автоматическом режиме и, самое главное, отслеживать ее изменения в реальном режиме времени.

Стоимость дополнительных проводников, новых контактных площадок и другого аналогичного оборудования относительно невелика. Данные технологии могут быть легко внедрены и в существующих проектах. Однако стоимость модулей анализаторов, сервера контроля и собственно самого программного обеспечения пока не позволяют широко использовать подобные средства интеллектуального управления СКС.

Учет компьютеров и программ

Автоматическая инвентаризация программного обеспечения и оборудования для функционирующих систем не представляет большой сложности. Современные операционные системы позволяют собрать такие данные различными способами (через объекты операционной системы, через командный интерпретатор специального назначения *WMIC* (Windows Management Instrumentation Command-line) — см. далее в этой главе — и т. д.).

Данные о параметрах оборудования и программного обеспечения легко собрать централизованно при наличии прав доступа к соответствующему компьютеру (рис. 6.1). В домене с этой целью обычно используются учетные записи, включенные в группу администраторов домена. В рабочей группе придется указывать параметры учетных записей каждой системы. Администратору доступно большое

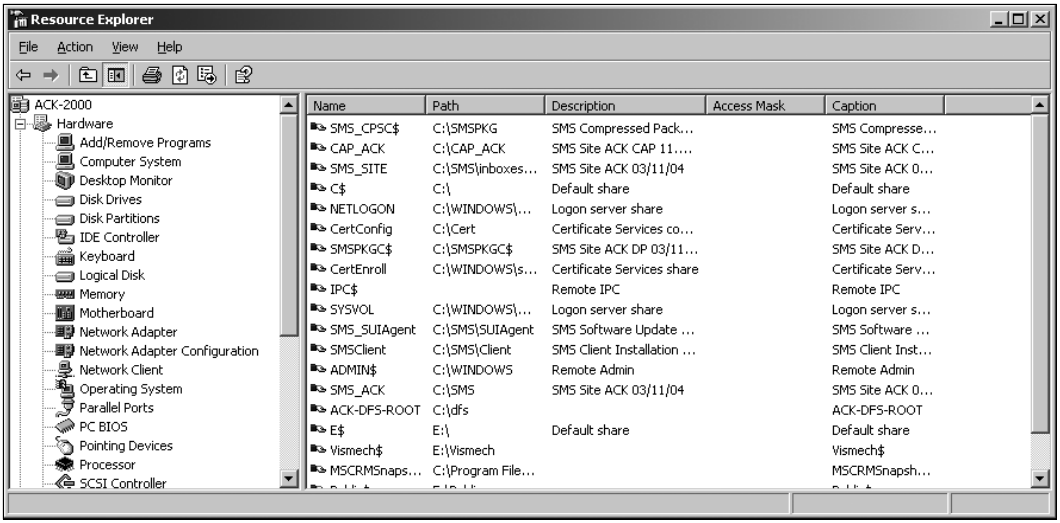


Рис. 6.1. Результаты инвентаризации ресурсов с использованием специализированного ПО. Собранные данные хранятся в базе, поэтому администратор легко может сформировать необходимый запрос и получить ответ, например, на скольких компьютерах используется данный программный продукт

число программ, реализующих данный функционал (в том числе и бесплатных), поэтому значение при выборе инструмента имеют личные предпочтения и, возможно, дополнительные особые требования, такие как необходимость периодической инвентаризации в больших организациях или требования интеграции с бухгалтерскими учетными системами.

Контроль функционирования ПО

В повседневной практике для администратора очень важно своевременно получить информацию о возникновении того или иного сбоя в работе информационной системы. Еще лучше — получить предупреждение заблаговременно.

О некоторых специализированных продуктах, предназначенных для своевременного предупреждения администратора о событиях в информационной системе, будет рассказано в *главе 7*.

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. Опишем 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 не-

возможно из-за введенных ограничений. В каждой конкретной организации перечень параметров управления должен определяться индивидуально. Чтобы применение групповых политик, прежде всего, облегчало работу как пользователя, так 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 котором 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 2008R2 содержится в документах, которые можно загрузить со страницы **http://go.microsoft.com/fwlink/?LinkId=131389**.

Групповые политики в различных версиях операционных систем

Групповые политики появились практически с доменами Windows, правда назывались они тогда *системными политиками* (system policy), а возможности их были крайне ограниченными.

В каждом выпуске Windows количество параметров, которые можно было установить при помощи групповой политики, существенно увеличивалось. Частично менялись технологии (например, в Windows 2003 Server родительским процессом для обработки групповой политики был netlogon, а с Windows 7/2008 была введена специальная служба — *Group Policy Client*, обеспечивающая повышенную устойчивость процесса, изменились технологии обнаружения медленных каналов связи и т. п.), менялись сами средства создания и редактирования политик, появлялись новые форматы (XML в шаблонах ADMX) и т. д.

Чтобы не разбираться подробно с каждым внесенным изменением и не нарушить работу групповых политик, стоит воспользоваться простым принципом: групповые политики должны соответствовать выпуску операционной системы и редактироваться только со станции соответствующего выпуска (например, политики Windows 2008 нужно редактировать только с сервера Windows 2008 или с рабочей станции Windows 7).

Примечание

В других случаях, например, при желании использовать шаблоны ADMX с контроллерами домена Windows 2003, нужно обратиться к технической библиотеке вендора.

И второе. Групповые политики, созданные для новых версий Windows, не будут применяться к предыдущим выпускам. Точнее, будут, но в существенно меньшем объеме. Поэтому администратору придется комбинировать управление устаревшими ОС, используя наряду с групповыми политиками и другие технологии, частично освещенные в этой главе.

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 2008/Windows 7 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. 6.2);

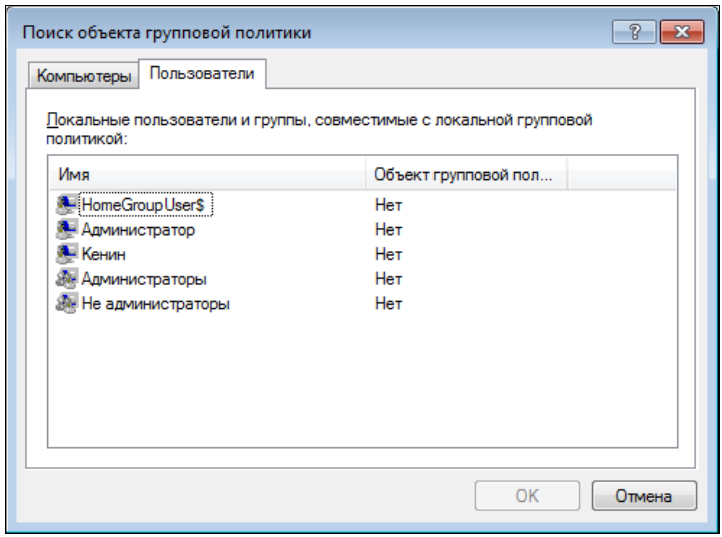


Рис. 6.2. Множественные объекты групповой политики

3. Локальная политика пользователя (если имеется);
4. Групповые политики домена по иерархии контейнеров (сайт, домен, подразделение и т. п.).

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 *компьютер* и *пользователь* 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.

Кроме того, хранятся административные шаблоны — ADMX-файлы, представляющие собой XML-файлы 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 использовать дополнительный 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*.

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 2008 (R2), так и с рабочих станций Windows 7.

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 (*RSAT* — Remote Server Administration Tool), 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** появляется 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. 6.3 показан пример окна моделирования политики (для отображения конкретных значений параметров нужно перейти по ссылкам **показать**).

Групповая политика изменяется в Редакторе управления групповыми политиками (рис. 6.4), для этого достаточно выбрать соответствующую команду в меню. Новую групповую политику можно создать либо 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 оставлять на экране только те параметры, которые действуют для конкретной опе-

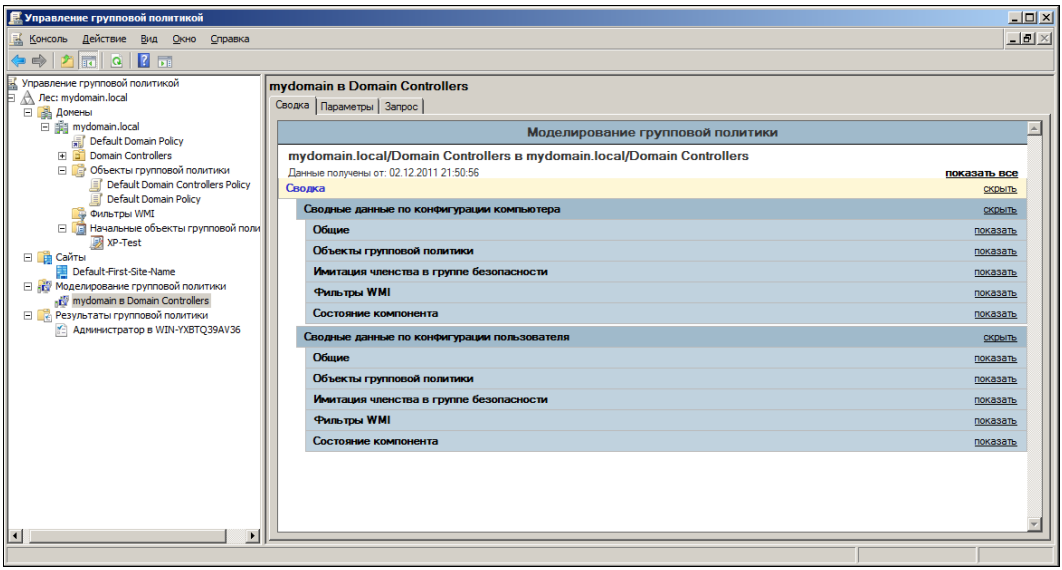


Рис. 6.3. Консоль управления групповой политикой (режим моделирования)

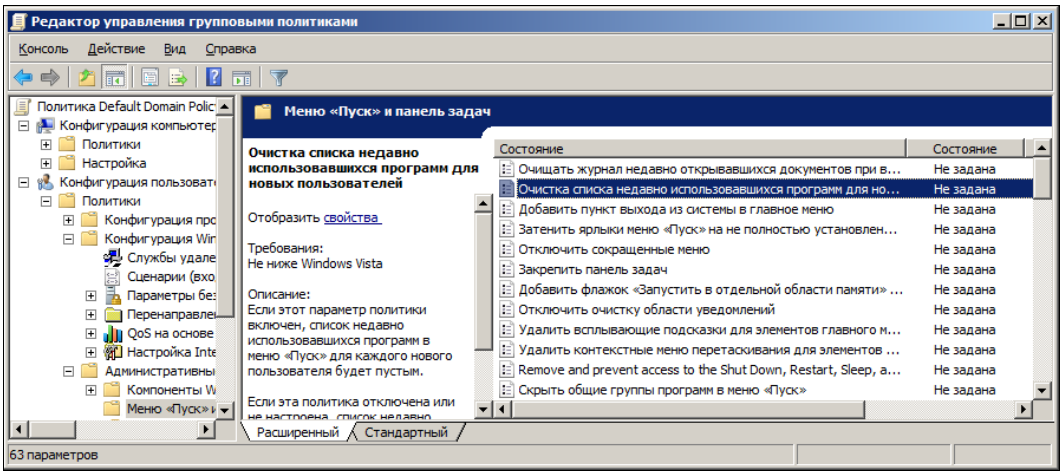


Рис. 6.4. Редактор управления групповыми политиками

рационной системы. Для этого используется специальный фильтр (рис. 6.5), в котором нужно установить необходимые параметры для отбора.

Чтобы применить созданную политику, достаточно установить для нее связь (link) на соответствующий объект службы каталогов в оснастке Управление групповыми политиками.

Хуже, если применение политики привело к ошибкам работоспособности системы *(см. разд. "Последствия отключений политик" ранее в этой главе)*. В некоторых ситуациях может помочь возвращение групповой политики к параметрам по умолчанию. На ПК с ОС Windows 2003/2008 это можно сделать с помощью утилиты dcgpofix. Подробности запуска можно получить, запустив команду `dcgpofix /?`

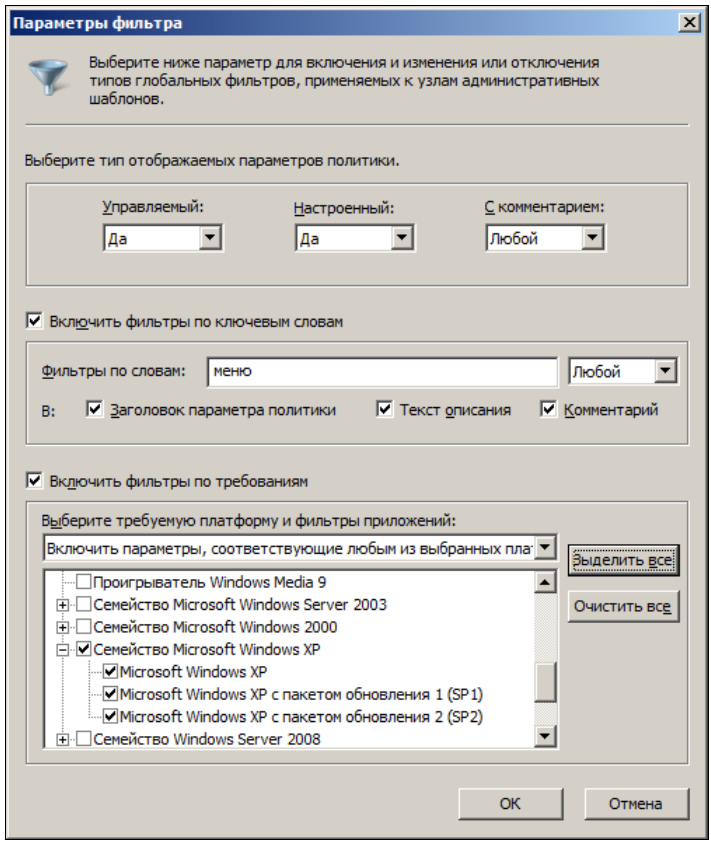


Рис. 6.5. Настройка параметров фильтра редактора групповой политики

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 2008R2/Windows 7 с RSAT (параметры этих политик — только для чтения, они предназначены для импорта в групповые политики).

Начальные объекты групповой политики предназначены 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, появившемся в управлении групповыми политиками после приобретения очередной компании, стала возможность расширенного управления групповыми политиками — 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, которая контролирует 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 групповыми политиками появляется новый контейнер — *Изменение управления*. Операции над групповой политикой можно теперь контролировать (рис. 6.6).

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 администраторы, вносящие изменения в

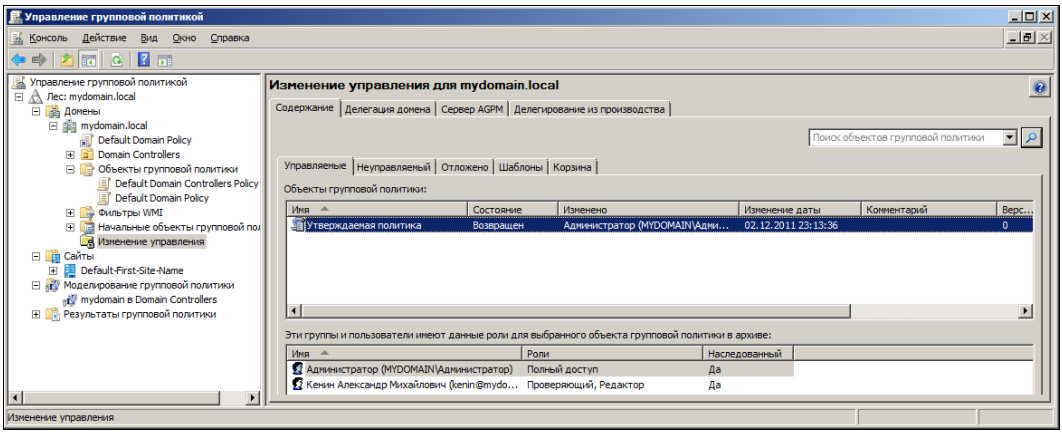


Рис. 6.6. AGPM: контролируемая политика

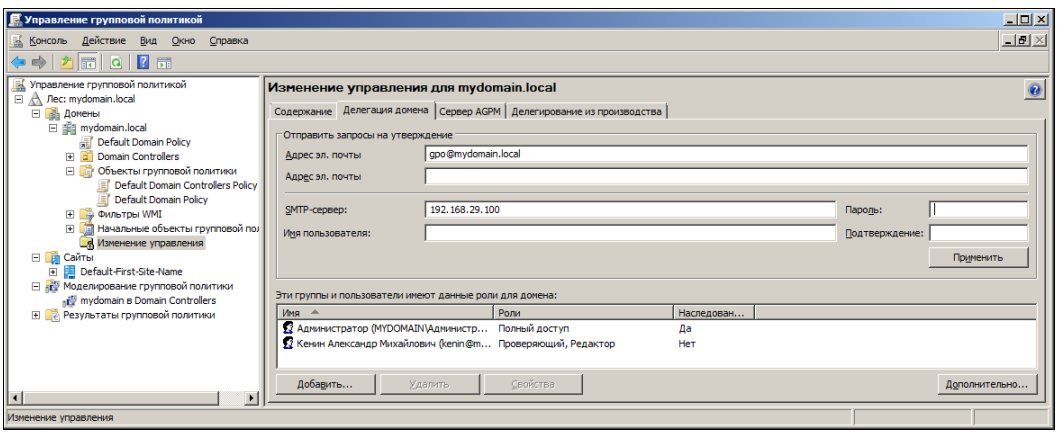


Рис. 6.7. Назначения прав администраторов по управлению групповыми политиками

групповую политику, не будут доступны функции публикаций изменений в реальной структуре, несмотря на то, что они также могут обладать правами администраторов домена (рис. 6.7).

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.

"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**.

Фильтрация при помощи WMI-запросов

Существует возможность уточнять область применения политики на основе WMI-фильтров. Администратор, знакомый с основами программирования и использования WMI *(см. разд. "Windows Management Interface" далее в этой главе)*, 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.

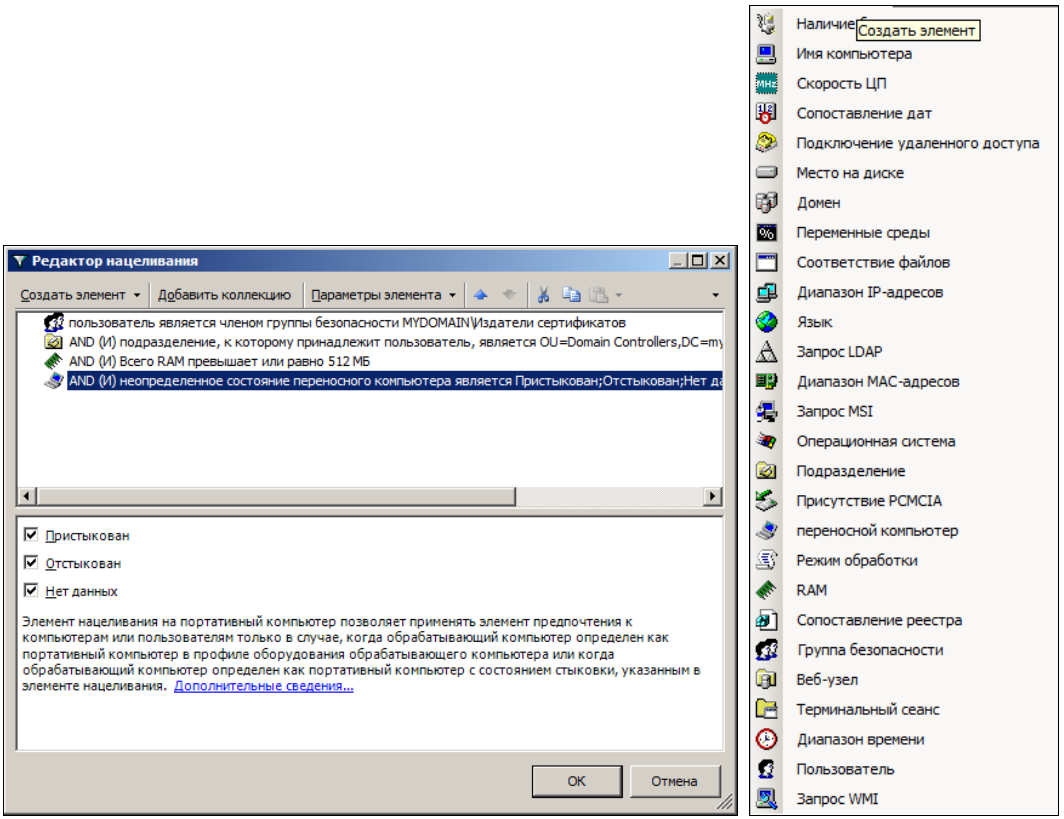
Метод не требует дополнительных разъяснений. Но фактически при его использовании мы вместо усложнения структуры каталогов создаем соответствующую структуру групп безопасности.

Предпочтения групповых политик

В групповых политиках Windows 2008 появился дополнительный раздел — **Предпочтения**. Параметры этого раздела позволяют управлять подключением дисков, параметрами реестра, локальными пользователями и группами, службами, файлами и папками.

Главное преимущество раздела **Предпочтения** — легкость назначения параметров без обращения к каким-либо сценариям, составлению сложных запросов и т. д. Это позволяет, с одной стороны, облегчить настройку групповой политики, с другой — упростить структуру службы каталогов, поскольку не нужно будет создавать дополнительных контейнеров для выборки компьютеров.

Для использования раздела **Предпочтения** не нужно знать языки программирования, правила составления запросов в них и т. п. Все операции проводятся при помощи графического интерфейса. При этом возможности отбора крайне велики.



а *б*

Рис. 6.8. Редактор нацеливания (слева) и список учитываемых параметров (справа)

На рис. 6.8, *а* показан пример окна фильтра Предпочтений, а на рис. 6.8, *б* — список тех параметров, которые можно использовать при отборе.

Покажем на примере возможность подключения сетевых дисков с использованием предпочтений групповых политик.

Откроем для редактирования групповую политику и перейдем к разделу **Конфигурация пользователя | Настройка | Конфигурация Windows | Сопоставления дисков**. Из динамического меню выберем команду **Создать | Сопоставляемый диск**.

В появившемся окне **Свойства: Диск** укажем сетевой ресурс, к которому хотим подключиться, параметры учетной записи (если необходимо), букву, под которой будет смонтирован ресурс и т. д. После чего перейдем на закладку **Общие параметры** (рис. 6.9).

Установим флажки в нужных позициях и флажок ***Нацеливание на уровень элемента***. После чего нужно нажать на кнопку **Нацеливание**, откроется окно редактора (рис. 6.8, *а*), в котором достаточно вызвать команду **Создать элемент**, из открывшегося списка (рис. 6.8, *б*) с помощью мыши надо добавить необходимые

условия отбора. Условий может быть несколько, столько, сколько нужно для выбора конкретных систем(ы).

После завершения операций сопоставление диска будет осуществлено групповой политикой только для тех систем, которые удовлетворяют заданным условиям отбора.

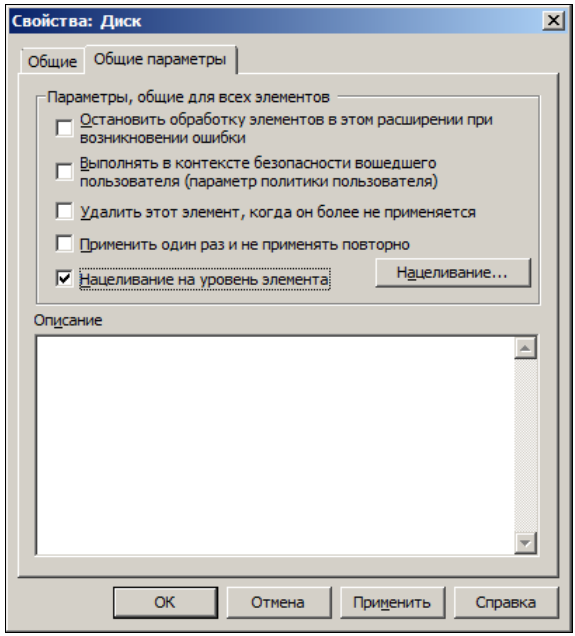


Рис. 6.9. Нацеливание на уровень элемента

Рекомендации по применению политик

Главная рекомендация состоит в том, чтобы *не изменять политику по умолчанию*. Не стоит вносить изменений в действующую политику по умолчанию. Если возникнет какая-либо серьезная ошибка в политике, то возврат к начальному состоянию приведет к удалению не только последних настроек, но и всех других параметров, тщательно настраиваемых в течение долгого времени.

Поэтому создавайте *новые политики* для основных административных действий по управлению системой. В результате для изменения настроек вам необходимо только отключать/включать привязку политик к организационной структуре.

При настройке параметров политик ориентируйтесь на рекомендуемые значения для конфигураций предприятия (см. *разд. "Начальные объекты групповой политики" ранее в этой главе*).

Обработка одной политики с большим числом назначенных параметров практически не отличается по времени от обработки нескольких политик, в каждой из которых назначается только часть этих параметров. Поэтому удобнее создавать несколько политик, чем включать все изменения в одну.

Не удаляйте созданные ранее групповые политики. Просто отключите привязку их от объектов службы каталогов. Они могут понадобиться для анализа ситуации в случае обнаружения каких-либо проблем в дальнейшем.

Если ваши настройки относятся только к параметрам компьютера или только к пользователю, то не забывайте устанавливать признак применения лишь соответствующей части политики. Это повысит скорость обработки.

Некоторые особенности политики ограниченного использования программ

Работа с групповыми политиками, определяющими параметры настройки оборудования или программ, обычно не вызывает сложностей. Параметры хорошо комментированы, поэтому эффект от их включения вполне предсказуем. Сложности обычно вызывает использование групповых политик для ограничения запуска прикладных программ.

Политики ограниченного использования программ, кроме реализации корпоративной политики в части "запрещенных" и "разрешенных" программ, позволяют эффективно защищать компьютеры от троянских коней и других вирусов, блокируя запуск неизвестных кодов.

> ***Примечание***
>
> В корпоративных версиях Windows 7 вместо политик ограниченного использования программ должны использоваться политики управления приложениями (AppLocker). Правила политик использования программ могут быть импортированы в AppLocker, но состав контролируемых параметров в этой технологии несколько другой (издатель, путь, хэш). Настройка правил в AppLocker осуществляется при помощи мастера и не представляет особой сложности.
>
> Среди особенностей AppLocker можно отметить более тонкую настройку (правило создается не для всех, а для конкретной группы или пользователя), улучшенное протоколирование, поддержку Powershell, возможность использования только в режиме наблюдений (аудита).

Политика ограниченного использования программ состоит из двух частей: *политики по умолчанию* и *политики исключений*.

Политика по умолчанию определяет поведение системы в случае отсутствия явных указаний: либо все запрещать, либо все разрешать. Если администратор компьютера заранее знает перечень программ, с которыми будет работать пользователь, то удобнее использовать запрет по умолчанию и явно разрешить запуск программ по списку. В противном случае следует разрешить запуск программ по умолчанию и запретить запуск "подозрительного" или нежелательного для организации ПО.

Варианты политик ограниченного использования

Разрешения/запреты на запуск конкретных программ могут формироваться на основе следующих критериев.

Примечание

В качестве исполняемых файлов в правилах могут указываться не только файлы программ, но и все файлы с расширениями, зарегистрированными для автоматического запуска программ на основе ассоциаций. Этот перечень можно видоизменить при формировании политики ограничений программного обеспечения.

- **Хэш.**

  При старте программы проверяется хэш ее программного кода и сравнивается со значением, записанным во время создания правила. В случае совпадения запуск программы разрешается (или запрещается, если правило создается для блокировки), иначе — блокируется (соответственно разрешается).

  Данное правило жестко регулирует возможности использования ПО и не разрешает пользователю "собственными силами" обойти это ограничение. Например, запрет на основе хэш-правила не даст использовать программу даже в случае переименования ее исполняемого файла, копирования его в другую папку и т. д.

  Недостаток критерия — некоторое замедление *каждого* запуска программы из-за подсчета ее хэша и сравнения полученного значения с контрольным. Кроме того, в случае обновления версии программного обеспечения администратору придется переопределять данное правило (поскольку хэш запускаемого файла новой версии программы будет отличен от прежнего).

- **Сертификат.**

  В этом случае система при попытке запуска программы проверяет наличие у нее цифровой подписи — соответствующего сертификата от доверенного удостоверяющего центра. Так же, как и в случае использования правила контроля хэша, система затрачивает некоторые ресурсы при запуске программы. Однако данный подход более гибок, поскольку позволяет администратору выполнять обновления программного обеспечения при условии наличия у новых программ цифровых подписей.

- **Путь.**

  Правило, создаваемое на основе указания пути к исполняемому файлу, является самым удобным в использовании, но одновременно и самым "ненадежным".

  При создании правила необходимо указать путь к программным файлам. Причем возможно указание как пути к папке (в этом случае правило будет действовать для всех файлов в этой папке и во всех вложенных в нее каталогах), так и к конкретному файлу. Допускается указание UNC-путей и использование в записи масок и переменных. Кроме того, правило допускает указание в качестве переменной пути ветви реестра. Так, переменная

  ```
  %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
  ProgramFilesDir%
  ```

  указывает на папку, в которую по умолчанию выполняется установка программ.

  Эти переменные используются, например, при создании правил запуска для тех программ, путь установки которых выбирает пользователь, а система использует при запуске информацию из реестра (программы Microsoft Office и т. д.).

Примечание

Переменная реестра записывается следующим образом: `%[Registry Hive]\[Registry Key Name]\[Value Name]%`. При использовании переменных реестра не допускаются сокращения (например, вместо `HKEY_LOCAL_MACHINE` — `HKLM`); после переменной (знака `%`) не может сразу следовать символ `\`. Кроме того, при указании правила пути реестра можно использовать только значения `REG_SZ` или `REG_EXPAND_SZ`.

Контроль выполнения данного правила совершенно не сказывается на производительности системы, однако у опытного пользователя имеются многочисленные возможности для "обхода" контроля. Во-первых, пользователь может копировать и переименовывать исполняемые файлы программ, чтобы обойти ограничения запрета по конкретному пути. Во-вторых, используя возможности переопределения переменных, можно также обойти наложенные ограничения.

- **Зона Интернета.**

  Одно из самых неудачных, на взгляд автора, правил, которое вводит ограничения на запуск программ в зависимости от того, из какой зоны проведена установка. На момент подготовки книги данное правило могло устанавливаться только для msi-пакетов (Windows Installer Packages).

  В правиле используется типовой для систем Windows перечень зон безопасности: **Интернет**, **Местная интрасеть**, **Ограниченные узлы**, **Надежные узлы**, **Мой компьютер**.

Опции настройки применения политик ограниченного использования программ

Существует несколько дополнительных опций настройки применения политик ограничения программного обеспечения. Прежде всего, это возможность применения политик к библиотекам программ (DLL Checking). В обычной практике применение такой проверки не имеет смысла, поскольку приводит к существенной деградации производительности компьютера[1], а эффект может быть наложен ограничениями только на собственно исполняемые файлы. Использование данной возможности оправдано только в тех случаях, когда администраторам необходимо осуществлять проверку целостности библиотек программ.

Опция **Для всех пользователей, кроме администраторов** позволяет не применять политики ограничения для администраторов локальных компьютеров. Необходимость ее использования определяется конкретной ситуацией.

Опция разрешения всем пользователям включать сертификаты в список доверенных, хотя и установлена по умолчанию, является не лучшим выбором. Предпочтительнее при работе в составе управляемой сети передать эти функции администраторам того или иного уровня.

Опция **Назначенные типы файлов** позволяет регулировать перечень расширений имен файлов, для которых будут применяться политики ограничения. Обычно этот

[1] Обычно при запуске одной программы загружается несколько десятков библиотек, причем одна и та же библиотека может вызываться несколько раз.

список включает наиболее распространенные типы файлов, которые могут быть использованы для запуска программного кода.

Когда ограничения не действуют

Разработка политики ограничения ПО обычно не бывает без ошибок. Поэтому важно знать, как можно "вернуть" возможность управления системой администратору, если в результате применения неверной политики у него отсутствует возможность запуска программ.

> ***Примечание***
>
> Следует учитывать, что правила ограниченного использования программ применяются не ко всем клиентам (только к Windows XP SP2 и старше).

Правила ограничения программного обеспечения не применяются в безопасном режиме, поэтому достаточно перезагрузить систему, нажать клавишу <F8>, выбрать безопасный режим и выполнить необходимые действия.

Имейте также в виду, что правила ограничений программного обеспечения не применяются для программ, запускаемых от имени учетной записи **Система**.

Следует также учитывать, что правила ограничений не применяются при запуске драйверов (и вообще всех процессов уровня ядра системы), любых макросов в составе документов MS Office, а также программ, созданных с учетом Code Access Security Policy (на основе common language runtime).

Последовательность применения политик ограниченного использования программ

Порядок применения политик ограниченного использования программ имеет некоторые особенности. При наличии явных противоречий между правилами двух наследуемых политик (одна политика запрещает запуск данной программы, а другая — разрешает) используется типовая последовательность применения настроек. Однако политики ограниченного использования программ могут содержать различные правила: например, одно разрешает запуск *всех* программ для данной папки, а другое — запрещает загрузку *определенных* типов файлов. В этих случаях правила применяются в соответствии с их *старшинством*.

Во-первых, "старшинство" требований устанавливается в зависимости от типа правил (причем правило, написанное в первой строке, превалирует над правилом второй строки и т. д.):

- хэш-правило;
- правило на основе сертификата;
- правило "пути";
- правило на основе зоны Интернета;
- правило по умолчанию.

Во-вторых, правила пути могут описывать требования к различным папкам, в которых находится исполняемый файл программы. В этом случае превалирует то правило, которое относится к *наиболее конкретному указанию пути*. Далее приведены примеры правил ограничений, расположенные *от наиболее конкретного к наиболее общему*:

- C:\Мои документы\Отчеты\Отчет за май.doc;
- C:\Мои документы\Отчеты*.doc;
- *.doc;
- C:\Мои документы\Отчеты\;
- C:\Мои документы\.

> ***Примечание***
>
> При отличающихся значениях необходимости применения политики ограниченного использования программ к административным учетным записям в политиках компьютера и пользователя применяется значение, определенное политикой компьютера.

Некоторые рекомендации применения политик ограниченного использования программ

Составление политик ограниченного использования программ требует от администратора определенного опыта. Кроме тщательного продумывания вариантов политик, администратору необходимо принимать во внимание различные факторы.

Так, запуск конкретной программы может зависеть от другого исполняемого файла, и если на этот файл будет наложено ограничение, то запуск основной программы станет невозможным. Внимательно следует изучить ситуацию, когда необходимо использовать пути к папкам, а когда — пути с переменными реестра. Необходимо учесть такие факторы, как разрешение сценариев входа в систему, не заблокировать случайно запуск антивирусного программного обеспечения и т. п. Поэтому имеет смысл предварительно проанализировать на компьютерах сети состав автоматически загружаемого программного обеспечения.

Сведения о пути к исполняемым файлам проще всего получить, если запустить желаемую программу и открыть задачу **Сведения о системе** (**Программы | Стандартные | Служебные**). Можно также набрать в командной строке `wmic` и нажать клавишу <Enter>, а потом в появившемся окне ввести `process` и нажать клавишу <Enter>. Вы увидите пути к исполняемым файлам запущенных в текущий момент программ.

> ***Примечание***
>
> Более подробно использование технологии WMI и ее командного интерпретатора `wmic` описано далее в этой *главе*.

Определить *зависимые* программы в общем случае достаточно тяжело. Обычно приходится экспериментировать. Можно только посоветовать внимательно просмотреть файлы из папки установки соответствующей программы и файлы из папки %ProgramFiles%\Common Files.

Нельзя забывать и то, что "благодаря" защите системных файлов на компьютере в папке %windir%system32\dllcache хранятся копии исполняемых служебных файлов и пользователь, которому запрещено запускать исходные файлы по исходному пути, может воспользоваться их копиями, указав точный путь к данной папке.

Некоторые особенности политики установки программного обеспечения

С помощью групповых политик можно устанавливать программы на локальные системы. Использование таких возможностей интуитивно понятно. Необходимо создать соответствующий пакет установки и включить его в групповую политику.

Что необходимо учесть администратору при работе с такими политиками.

Во-первых, в качестве установочного пакета можно использовать файл либо в формате MSI, либо в формате ZAP. 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]
; Only FriendlyName and SetupCommand are required,
; everything else is optional.

; FriendlyName is the name of the program that
; will appear in the software installation snap-in
; and the Add/Remove Programs tool.
; REQUIRED
FriendlyName = "Microsoft Excel 97"

; SetupCommand is the command line used to
; run the program's Setup. With Windows Server 2003
; and later you must specify the fully qualified
; path containing the setup program.
; Long file name paths need to be quoted. For example:
; SetupCommand = "\\server\share\long _ ; folder\setup.exe" /unattend
; REQUIRED SetupCommand = "\\server\share\setup.exe"

; Version of the program that will appear
; in the software installation snap-in and the
; Add/Remove Programs tool.
; OPTIONAL
DisplayVersion = 8.0

; Version of the program that will appear
; in the software installation snap-in and the
; Add/Remove Programs tool.
```

```
; OPTIONAL
Publisher = Microsoft
```

Во-вторых, установка программы должна проводиться в "тихом" режиме, т. е. без диалога с пользователем. Например, не должен запрашиваться серийный номер продукта. Подготовка такого инсталляционного пакета в общем случае является далеко не тривиальной задачей.

В-третьих, 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** *(см. разд. "„Обход" параметров пользователя" ранее в этой главе)* 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).

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 которого осуществляется установка соответствующего программного обеспечения.

Административные шаблоны

Количество регулируемых групповой политикой параметров можно менять. Проще всего добавлять настройки различных значений реестра системы. Для этого используются *административные шаблоны*.

> ***Примечание***
>
> По образцу файлов шаблонов администратор легко может создать свои дополнительные настройки, которые он сможет распространить при помощи групповой политики. Понятно, что для создания такого файла администратору необходимы соответствующие знания, которые он может получить из технической документации на операционные системы и настраиваемое программное обеспечение.

Обычно административные шаблоны копируются на локальный диск после установки соответствующего программного обеспечения. Поэтому администратору для

добавления нового шаблона достаточно открыть для изменения групповую политику (с компьютера, на котором установлено приложение) и выполнить операцию добавления нового шаблона. Другой способ — загрузить административные шаблоны с сайта разработчика (если они там предоставлены) и импортировать их в политику.

В завершение следует настроить необходимые параметры и привязать групповую политику к соответствующему подразделению.

Утилиты группового управления

Несмотря на большое количество утилит, входящих в состав операционной системы и пакетов Resource Kit, администраторы обычно предпочитают иметь в запасе продукты третьих фирм, которые хорошо зарекомендовали себя при разрешении тех или иных проблем.

Профессиональные продукты управления большими сетями — HP Open View, Unicenter и др. — обычно недоступны администраторам малых и средних сетей из-за высокой стоимости: их базовые комплекты оцениваются в 20—30 тыс. долларов без стоимости клиентских лицензий. Поэтому в таких организациях управление сетью строится на использовании отдельных, не интегрированных друг с другом комплектов.

Существует много средств, облегчающих выполнение административных задач. Часть из них мы упомянем в этой книге. Но, естественно, что каждый системный администратор будет применять только продукты, оптимально подходящие для конфигурации его парка оборудования. Читатель должен понимать, что в объеме одной книги невозможно даже привести перечень всех таких продуктов. Автор пытается показать, прежде всего, спектр таких программ, основываясь на некотором опыте работы с ними.

Средства поддержки пользователей

Одной из задач администрирования информационной системы является оказание технической поддержки пользователей. Обычно в этих целях используются программы доступа к рабочему столу.

> ***Примечание***
>
> Технологии, описываемые в следующих разделах, могут быть использованы только на *работоспособной операционной системе*.

"Удаленный помощник"

Удаленный помощник — режим удаленного подключения к рабочему столу — предназначен для оказания помощи пользователю компьютера, чтобы в случае возникновения проблем в работе он имел возможность обратиться к специалисту, а последний, подключившись к компьютеру, оперативно оказать посильную помощь.

Параметры вызова помощника могут быть определены централизованно в групповой политике.

Чтобы перейти в этот режим, предусмотрен специальный механизм отправки приглашений на удаленное подключение. 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. Предоставить удаленному помощнику право на управление компьютером должен текущий пользователь, причем он может в любой момент вернуть себе управление системой.

Отправить приглашение можно с помощью почтовой программы или программы MSN Messenger. Для отправки приглашения необходимо выполнить следующие действия: нажать кнопку **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.

В случае необходимости (этот вариант доступен в Windows Vista/Windows 7) администратор может сам инициировать предложение помощи (рис. 6.10). Команда `msra /offerRA <имя удаленного компьютера>` (ее можно запомнить как аббревиатуру от MS Remote Assistance) позволяет запустить помощника и инициировать сессию

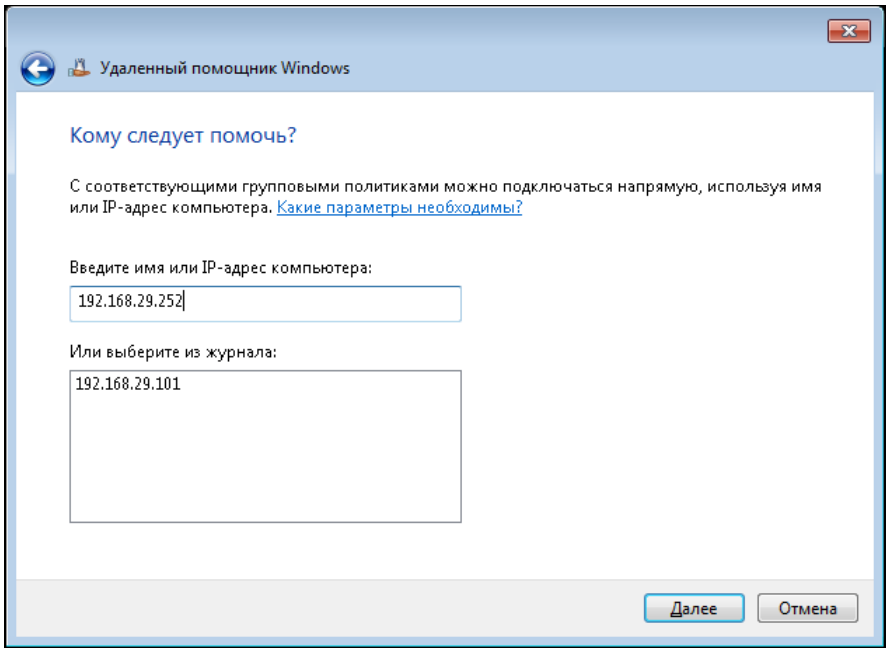


Рис. 6.10. Предложение помощи пользователю от администратора

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.

Если удаленному специалисту необходимо "перехватить" управление компьютером, то он может обратиться к пользователю путем обмена мгновенными сообщениями. Если пользователь даст такое согласие, то дальнейшая работа удаленного пользователя ничем не будет отличаться от обычной терминальной сессии, кроме возможности локального пользователя в любой момент вернуть себе управление компьютером.

Утилиты подключения к рабочему столу

Хотя в рабочих станциях с ОС Windows присутствует возможность удаленного подключения к рабочему столу, на практике она редко используется администраторами. Во-первых, соответствующие опции должны быть предварительно включены в настройках клиентского компьютера (это, конечно, можно сделать и централизованно), во-вторых, при попытке удаленного подключения текущий пользователь отключается от экрана. Администратор может только посмотреть, 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* (Virtual Network Computing, **www.realvnc.com**).

  VNC позволяет удаленно просматривать любые платформы (UNIX, Win32, Mac, мобильные клиенты и т. п.). Это кроссплатформенное приложение; 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).

[1] Последняя версия программы позволяет администратору удаленно управлять как системами на основе Windows, так и Linux-компьютерами.

- *Hidden Administrator*.

  Hidden Administrator[1] (**www.hidadmin.ru**) — программа российского автора. Подобно другим программам она обеспечивает полный доступ к ресурсам удаленного компьютера, предоставляет администратору возможности скрытого наблюдения и управления, обмена файлами и т. п. Отметим также наличие опции удаленного включения системы (Wake on LAN).

- *Remote Administrator* (RAdmin).

  Еще одной часто используемой программой удаленного управления для платформы Windows является RAdmin. 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.

> ***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.

Средства автоматизации — сценарии

Управление в режиме консоли, хотя и требует от администратора наличия опыта работы, привлекательно тем, что позволяет полностью автоматизировать процесс, например, выполнять заданные операции по расписанию.

При изучении правил использования сценариев могут помочь следующие ресурсы:

- Script Center (**http://technet.microsoft.com/en-us/scriptcenter/default**)
- Центр технологий Windows PowerShell (**http://go.microsoft.com/fwlink/?LinkID=102372**)
- Блог Windows PowerShell (**http://go.microsoft.com/fwlink/?LinkID=128557**)
- Windows PowerShell Script Repository (**http://go.microsoft.com/fwlink/?LinkId=169615**)

Использование командной строки

Несмотря на то, что командная оболочка включает не так уж и много операций, с ее помощью опытный администратор может автоматизировать многие процессы. Чаще всего командные сценарии используются администраторами для настройки параметров входа в систему.

---

[1] Следует учитывать, что часть антивирусных программ рассматривает утилиты удаленного управления в качестве вредоносного кода.

Обратите внимание, что командный интерпретатор может выполнять циклы, анализировать условия, "разбирать" текстовые файлы и т. д. Если среди команд нет тех, которые выполняют нужные операции, можно использовать внешние утилиты и обрабатывать код их завершения. Например, для анализа членства пользователя в группе службы каталогов можно применить утилиту ifmember (доступно с сайта Microsoft) и проанализировать ее результат. Приведем пример такого блока сценария командной строки:

```
:sales
ifmember "sales"
if not errorlevel 1 goto ops
net use q: \\server\share
GoTo NextSection
```

Примеры использования командных сценариев доступны в Интернете.

Сценарии Visual Basic

В Windows возможно выполнение сценариев, написанных на таких языках программирования, как VBScript, JScript и JScript.NET. Использование этих языков программирования оправдано в тех случаях, когда нужно проанализировать параметры приложений, членство в группах, создать файлы отчетов, создать интерфейс программы и т. п. Иными словами, с их помощью создается новая программа компьютера.

Для исполнения программного кода сценария на компьютере должна присутствовать система, которая интерпретирует этот код и обеспечивает взаимодействие с другими программами. Обеспечивает такую функциональность специальный *сервер сценариев* — Windows Script Host (WSH).

> ***Примечание***
>
> Кроме упомянутых языков программирования администраторы могут применять и другие технологии, такие как Perl, TCL, REXX, Python и др. Для этого необходимо установить соответствующие модули интерпретаторов разработки третьих фирм.

WSH встроен в операционные системы Windows 98/ME/2000 и старше. Для Windows 95 можно бесплатно установить WSH, загрузив соответствующий файл с информационного сервера разработчика.

Каждая последующая версия WSH существенно функциональнее предыдущей, поэтому для систем, находящихся в эксплуатации, целесообразно обновить эту службу до последней версии.

Как правило, администраторы редко создают нужные сценарии "с нуля". Обычно ищется подходящий пример, который лишь незначительно модернизируется. Подобные коды достаточно широко представлены в Сети, а на сайте разработчика ОС можно воспользоваться ресурсами Центра сценариев по адресу **http://technet.microsoft.com/ru-ru/scriptcenter/default.aspx**.

На рис. 6.11 представлено окно одной из коллекций, свободно доступных с сайта разработчика (Portable Script Center, **www.microsoft.com**).

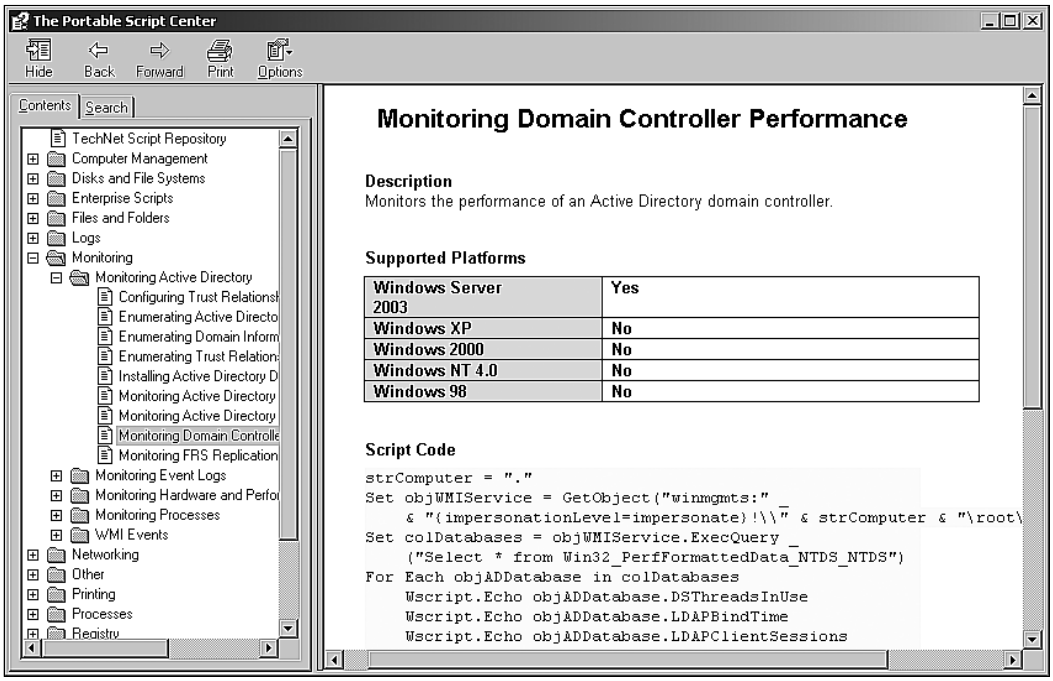


Рис. 6.11. Script Center

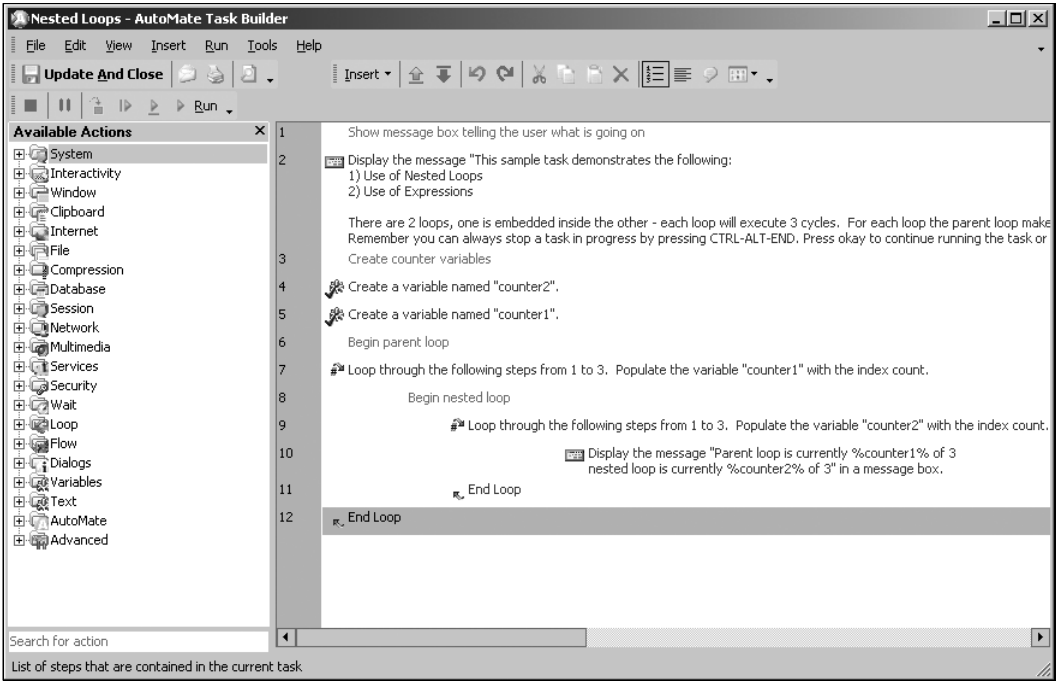


Рис. 6.12. Мастер создания автоматического сценария управления системой

Многие администраторы чувствуют себя недостаточно уверенно при составлении сценариев. В то же время применение сценариев существенно облегчает администраторские функции. В таких ситуациях могут помочь специальные продукты, которые позволяют составить сценарий в визуальном режиме, просто добавляя необходимые шаги (проверки, условия, действия и т. п.) путем перетаскивания мышью и задания необходимых характеристик каждого шага.

Один из таких продуктов приведен на рис. 6.12. Это программа AutoMate от компании Network Automation, Incorporated (NAI) (**www.networkautomation.com**).

Intelligent Platform Management Interface

Существует стандарт, который описывает требования по управлению компьютерными платформами — спецификация IPMI (Intelligent Platform Management Interface). Серверы, удовлетворяющие данной спецификации, могут управляться удаленно с консоли. В число действий, доступных администратору, входит:

- удаленное включение, выключение и перезагрузка сервера независимо от состояния операционной системы;
- обновление BIOS;
- просмотр параметров состояния сервера (температура, уровни напряжения, состояние датчиков, установленных на сервере), в том числе получение автоматического оповещения о событиях в работе системы по сети.

Подсистема удаленного управления не входит в состав всех платформ. В некоторых случаях такая возможность уже встроена в оборудование, в других можно дооснастить сервер специальной платой, реализующей необходимые функции.

Windows Management Interface

Windows Management Interface (WMI) — это технология управления Windows-компьютерами, реализующая стандарты Web-управления предприятием (WBEM, Web-based Enterprise Management. WBEM разработан компанией 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.

Технология используется, преимущественно, для доступа к оборудованию (получению данных о составе оборудования, его параметрах, состоянии и т. п.).

Стандартами WBEM предусмотрена типовая схема управляемых объектов — Common Information Model (CIM). Эта схема реализована в WMI как пространство имен Cimv2. В этом пространстве имен по умолчанию выполняются WMI-команды.

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 в целях контроля системы нужно знать, какие классы и пространства имен доступны для использования, 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[1] (рис. 6.13).

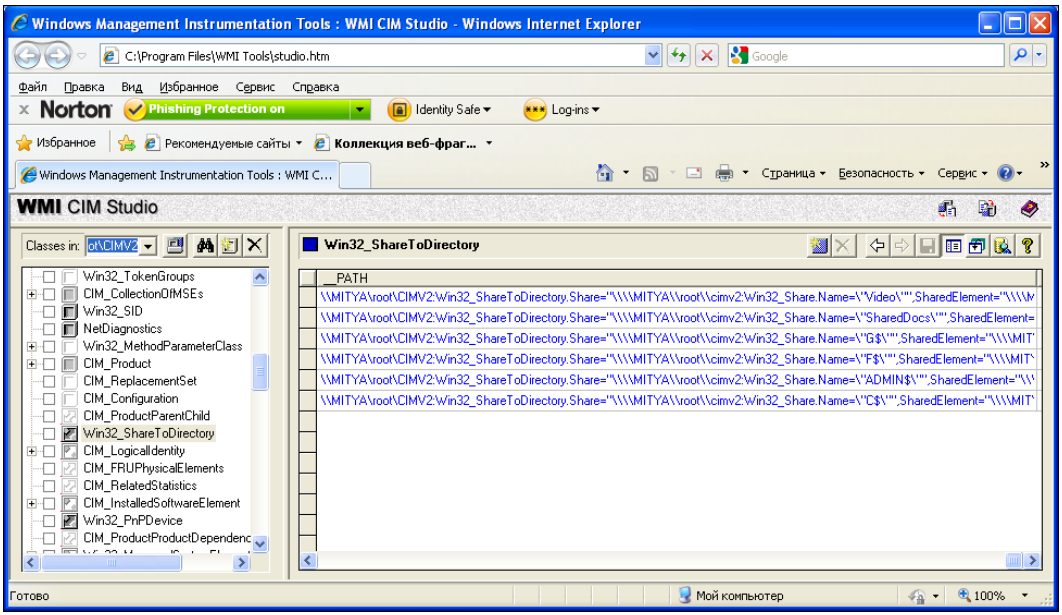


Рис. 6.13. Один из экранов WMI Administrative Tools

Для использования WMI необходимо знание иерархической структуры объектов системы. Запомнить ее практически невозможно, поэтому при составлении запросов могут помочь такие продукты, как WMI CIM Studio. С помощью данной программы 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. Средства среды разработки WMI Administrative Tools удобны тем, что наряду с просмотром существующих на компьютере классов WMI-администратор может

[1] Эти программы бесплатно можно загрузить с сайта Microsoft.

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 (также бесплатно доступна к загрузке с сайта Microsoft).

Программа содержит большую подборку готовых сценариев, которые можно использовать для составления необходимых запросов.

Утилита Scriptomatic (рис. 6.14) позволяет найти сценарий, с помощью которого можно получить желаемые сведения о работе системы, и на его основе составить WQL-запрос.

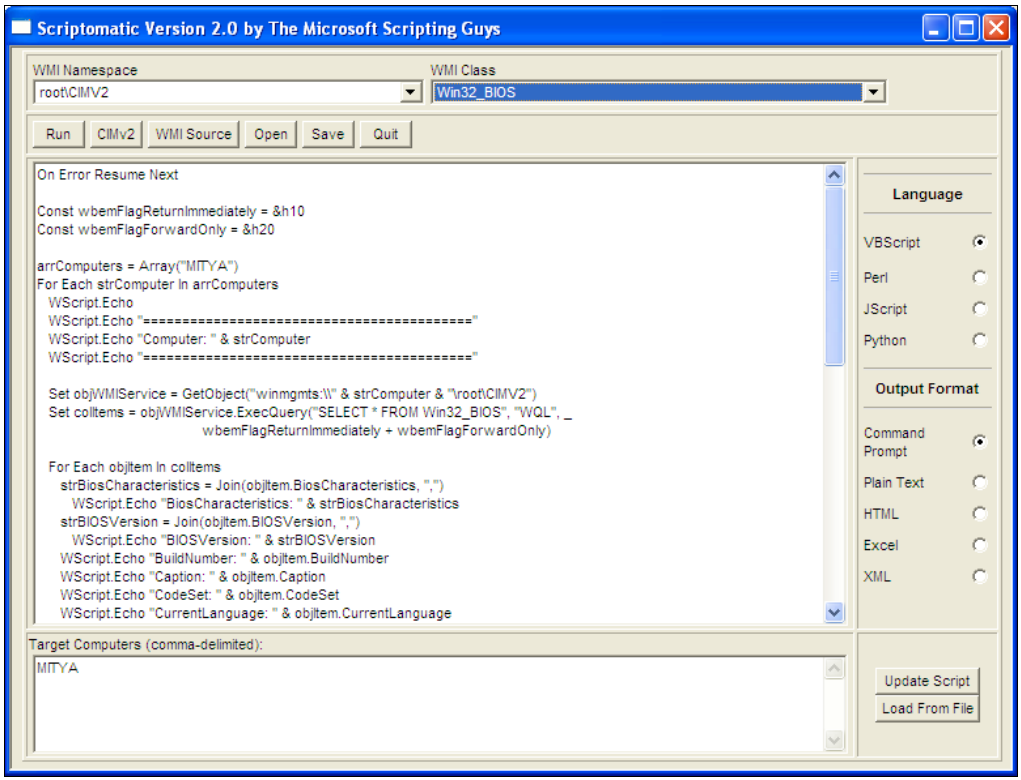


Рис. 6.14. Утилита Scriptomatic 2.0

WMI Query Language

Практическое использование интерфейса WMI для получения данных о состоянии оборудования или программной среды во многом напоминает работу с базой данных: вам необходимо указать, какие параметры должны быть получены от какого

объекта и при каких ограничениях (фильтрах). Язык запросов для WMI так и называют — WMI Query Language (WQL). Даже команды WQL принято называть *запросами*. Запросы WMI обрабатываются в специальном интерпретаторе — wmic (WMI Command-line tool). Объекты WMI доступны и для использования в Visual Basic, что позволяет составлять любые сценарии.

После запуска интерпретатора на экране появляется окно, аналогичное окну командной строки, в котором следует вводить необходимые команды. В этой утилите доступна объемная подсказка, вызываемая по ключу `/?`. Однако для успешной работы в этом режиме необходимо четко представлять, в каком классе находится объект, характеристики которого вы хотите получить или в настройки которого предполагается внести изменения.

Язык WQL может быть использован только для получения той или иной информации. Запросы WQL не позволяют добавить данные или изменить определенные параметры. Если вам необходимо выполнить какие-либо настройки, то сначала следует получить (выбрать) с помощью запросов WQL соответствующий объект, а затем, используя допустимые для данного элемента методы управления, провести желаемые изменения.

Варианты применения WMI

Существуют различные методы использования возможностей интерфейса WMI.

Для автоматизации управления компьютерными системами доступ к WMI может быть реализован через Windows Scripting Host. Это позволяет администратору создавать сценарии управления системами. Вы можете запросить характеристики какого-либо объекта с помощью языка WQL и изменить значения некоторых из них, присвоив новые величины параметрам выбранного объекта.

Определенную помощь в представлении о структуре классов WMI может оказать программа WBEMTest.exe, имеющаяся на каждом компьютере с установленным WMI. Используя программу WBEMTest.exe, можно перечислить классы WMI и отобразить характеристики отдельных элементов. Утилита позволяет выполнить WQL-запрос и увидеть его результат на экране. Хотя утилита предназначена для поддержки и имеет ограниченные возможности, но она может помочь разобраться с WMI-классами.

Для тех, кто предполагает использовать управление системами через WMI, целесообразно установить на компьютер какую-либо программу просмотра WMI. Например, весьма неплохими возможностями обладает программа CIM Studio, которая может быть свободно загружена с сайта Microsoft (рис. 6.13).

Для использования WMI необходимо знание иерархической структуры объектов системы. Запомнить ее практически невозможно, поэтому при составлении запросов могут помочь такие продукты, как WMI CIM Studio. С помощью данной программы администратор имеет возможность подключиться к любому пространству имен, зарегистрированному в системе, отобразить существующие классы объектов, увидеть свойства класса (характеристики, которые можно получить при исполнении запроса) и методы (параметры, которые можно установить в команде). Здесь

же можно открыть окно, в котором попробовать создать собственный WMI-запрос и сразу увидеть его результаты.

> ***Примечание***
>
> Те, кто использует в своей работе Microsoft Visual Studio.NET, могут применять входящие в ее состав утилиты. Если ни одна из перечисленных программ по каким-либо причинам вас не устраивает, то в Интернете легко можно найти и другие утилиты.

Примеры

Большинство практических WMI-сценариев создается на основе того или иного примера, который найден в Интернете. Приведу несколько возможных вариантов WMI-сценариев.

- **Перечисление логических дисков системы.**

  Следующий сценарий на Visual Basic выводит на экран наименования логических дисков, присутствующих в системе.

```
for each Disk in GetObject("winmgmts:").InstancesOf _
  ("CIM_LogicalDisk")
    WScript.Echo "Instance:", Disk.Path_.Relpath
Next
```

  При выполнении цикла переменной `Disk` поочередно присваиваются все элементы класса "логический диск". Затем сценарий (третья его строчка) выводит на экран сообщение с логическим именем этого диска.

- **Перезапуск остановившихся служб системы.**

  Следующий пример кода на Visual Basic может быть использован для перезапуска остановленных служб системы:

```
Set colListOfServices = GetObject("winmgmts:").ExecQuery _
("Select * from Win32_Service Where State = 'Stopped' and _
  StartMode = 'Automatic'")
For Each strService in colListOfServices
  strService.StartService()
Next
```

  Первая строка кода создает коллекцию объектов, удовлетворяющих условию выборки, заданному в WQL-запросе. Этот запрос выбирает все службы, для которых установлен автоматический режим запуска и которые в настоящий момент остановлены. Пятая строка кода организует цикл, выполняющий метод запуска служб, найденных на предыдущем этапе.

  Для данного сценария можно установить автоматический запуск через определенные промежутки времени, чтобы гарантировать работу всех служб компьютера. В свойствах службы есть опция восстановления, в которой можно задать параметры перезапуска службы после ее аварийной остановки. Однако если служба по тем или иным причинам не стартовала при запуске системы или была

остановлена вручную, то автоматически она также не будет запущена. Приведенный в примере код позволяет автоматически находить такие службы и запускать их.

PowerShell

PowerShell представляет собой средство, разработанное Microsoft для автоматизации различных задач и состоящее из интерпретатора и языка высокого уровня. PowerShell входит в состав Windows 7/Windows 2008 и может быть загружен для предыдущих версий. Язык реализован на Microsoft .NET Framework, интегрирует в себя доступ к WMI, COM, ADSI.

Сценарии PowerShell составляются из *командлетов* (cmdlet). Командлет объединяет в себе команду и объект, над которым она выполняется, и обычно называется по принципу глагол-объект. Например, командлет `Get-Content` возвратит (get) содержимое (content) того элемента, который будет указан в параметрах: Так, `Get-Content c:\test.txt` выведет на экран содержимое файла c:\test.txt.

PowerShell поддерживает перенаправление вывода, которое получило в его интерпретаторе название конвейера. Поддерживаются регулярные выражения, обработка условий — в общем, все те функции, которые присущи современным языкам программирования.

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. 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 данную команду настроить на автоматическое выполнение.

Помимо командной строки интерпретатора в последних версиях PowerShell появилась и графическая среда — интегрированная среда сценариев (ISE — Integrated Script Environment) Windows PowerShell. Это приложение, в котором можно выполнять команды PowerShell, создавать, тестировать и отлаживать скрипты с использованием удобного графического интерфейса с цветовым кодированием (рис. 6.15).

Следует иметь в виду, что в примере рис. 6.15 применен объект WMI. Это широко используемая практика в PowerShell для доступа к параметрам оборудования компьютера.

Обратите внимание, что при начале работы с PowerShell желательно настроить личный профиль — сценарий, который исполняется при каждом открытии интерпретатора. В этом профиле можно определить такие настройки, как локальный

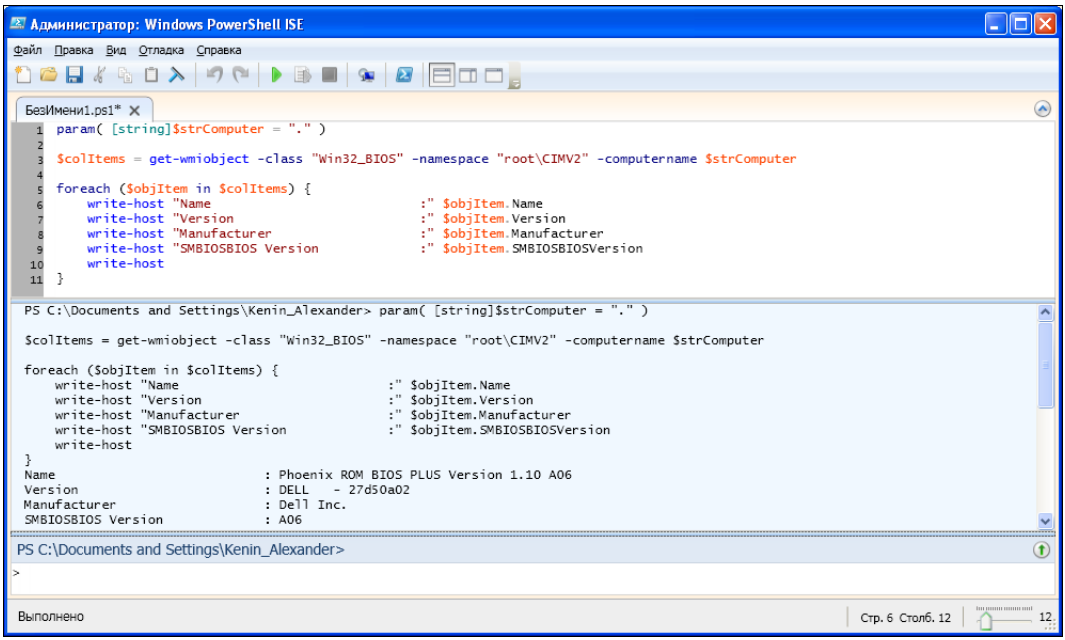


Рис. 6.15. Интегрированная среда сценариев PowerShell

путь, параметры безопасности, синонимы (сокращения для часто употребляемых команд) и т. п.

Отдельные утилиты администрирования третьих фирм

Администраторы весьма часто пополняют свой арсенал продуктами, выпущенными независимыми разработчиками программного обеспечения.

Приведем несколько ссылок на подобные продукты.

Утилиты от компании 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, 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 програм-

ма, отображающая все запущенные в системе процессы с указанием их иерархии. А утилита Diskview 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.

Средства восстановления системы

Администратору необходимо иметь средства, позволяющие выполнить загрузку со сменного носителя и получить доступ к жесткому диску компьютера. Обычно на такие диски записывают еще программы проверки структуры диска, программы восстановления таблицы разбиений, восстановления файлов, добавляют функционал перехода к существующей в системе точке восстановления, предусматривают команды сброса административного пароля и т. п.

Существует различные сборки таких дисков. Так, средство создания такого загрузочного диска включено в пакет Microsoft Desktop Optimization Pack (программа ERD Comander), отметим также диски восстановления от компании Acronis.

Подобные диски несложно найти в Интернете. Главное, что подобная утилита должна быть в наборе инструментов системного администратора.

Снифферы

Хотя администратору и не нужно разбираться в тонкостях сетевых протоколов, но он должен уметь на базовом уровне использовать тот или иной вариант программы сетевого анализатора *(сниффера)*. Сниффер (sniffer) может быть использован для оценки основных параметров функционирования сети: процента использования полосы пропускания, оценки используемых протоколов, количества пакетов с ошибками и т. п. Кроме того, сниффер позволяет обнаружить отклонения в работе устройств: избыточное количество пакетов того или иного типа, что может быть признаком заражения какой-либо системы вирусом или готовящейся атаки.

Также сниффер незаменим для настройки работы брандмауэра со специализированными недокументированными приложениями (обнаружение реально используемых приложением портов). Программы-анализаторы сетевого трафика обычно имеют развитые средства его анализа; это позволяет автоматически выявлять те или иные отклонения в работе сетевых устройств (рис. 6.16).

Я советую установить ту или иную программу анализа и мониторинга сетевого трафика и проанализировать трафик систем при обычных условиях. Это позволит приобрести некоторый опыт, чтобы в случае необходимости оперативно оценить, откуда идут пакеты, отфильтровать ненужный для анализа в конкретном случае трафик, поставить триггер на запуск анализатора по конкретным событиям и т. д.

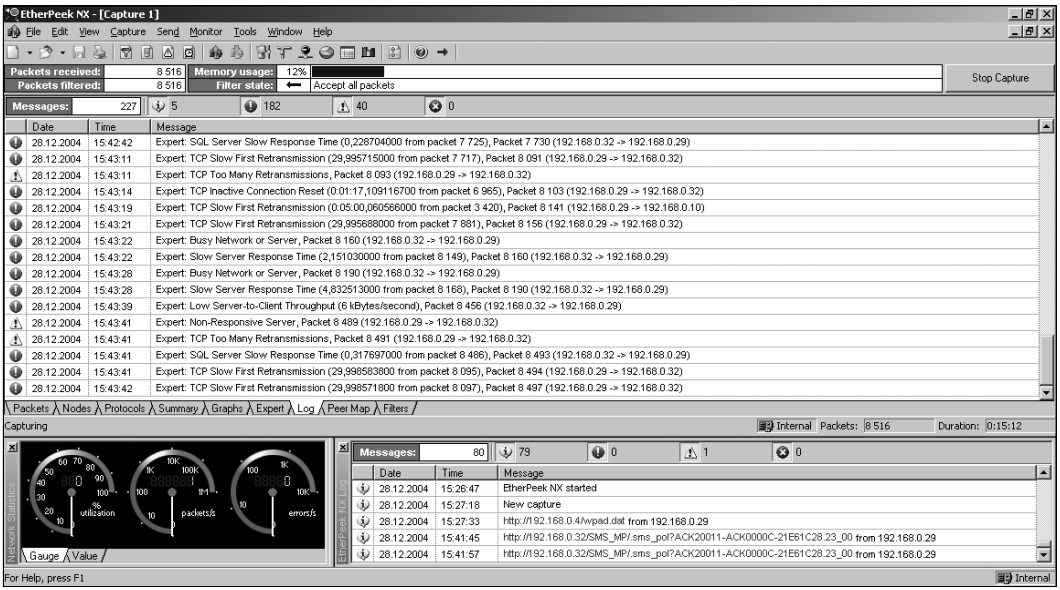


Рис. 6.16. Окно анализатора сетевых пакетов EtherPeek NX (**http://www.wildpackets.com/**)

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

Еще один популярный пакет (**http://www.systemtools.com/hyena/index.html**) для каждодневного администрирования Windows-систем.

Автоматизация установки программного обеспечения

Системному администратору постоянно приходится вводить в эксплуатацию новые рабочие места, а так же модернизировать существующие. Администратору обычно необходимо либо полностью подготовить компьютер (начиная от установки операционной системы и заканчивая прикладными программами и всеми обновлениями),

либо только установить прикладные программы (если компьютер поставлен с OEM-версией Windows).

В первом случае нужно использовать либо варианты разворачивания операционных систем, либо операции из дублирования. В случае только установки прикладного программного обеспечения на новую систему можно воспользоваться средствами группового управления (сценариями входа в систему или групповыми политиками) для распространения программного обеспечения. Но при этом установочные пакеты должны быть специально подготовлены: в них должны быть включены настройки, принятые для данной организации, и исключены запросы к пользователю (для полной автоматизации процесса).

Развертывание Windows 7 при помощи WAIK

Для автоматизации разворачивания Windows 7 вендор создал пакет WAIK — Windows Automated Installation Kit. Этот пакет свободно доступен для загрузки с сайта Microsoft и поможет создать образы системы для последующего автоматического разворачивания по требованиям конкретного рабочего места.

Следует сразу сказать, что такой подготовительный процесс для создания образов Windows 7 весьма трудоемок. В результате на практике применяют его только в тех организациях, где разворачивание Windows является повседневной задачей или же в случае массовой миграции на новую операционную систему.

Поэтому читателя, решившего внедрить данную технологию, отошлем к онлайновой технической библиотеке изготовителя.

Клонирование систем

Самый быстрый способ подготовить новую систему к эксплуатации — сделать ее *копией* уже существующей, т. е. *клонировать*. *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 прибегают при обновлении аппаратной части рабочего места (новый системный блок), при создании новых рабочих мест и т. д.

Существуют различные способы клонирования. Новый образ можно скопировать на жесткий диск, загрузившись со сменного носителя и перенеся данные со сменного устройства или по сети с сервера, если обеспечить удаленную загрузку новой рабочей станции. Первый вариант более прост в настройке и использовании, второй — более гибок, поскольку на сервере можно хранить образы для различных вариантов установки, но и требует установки серверной части.

Администратор выбирает тот вариант, который оптимальным образом подходит для его системы.

Подводные камни процесса клонирования

При кажущейся простоте операции при дублировании системы администратора ждет много проблем.

Первая группа трудностей связана с возможным различием оборудования на старой и новой системе. Для новой платформы могут понадобиться новые драйвера и система не сможет работать с программным обеспечением тех устройств, на которые была настроена исходная система. Критичными для переноса являются два момента: HAL в операционной системе Windows и отличия в устройствах хранения, с которых запускается операционная система.

> ***Примечание***
>
> *HAL — hardware abstraction layer*, представляет собой программный код, позволяющий операционной системе без изменений работать с различным аппаратным обеспечением. Условно HAL можно представить себе как драйвер материнской платы компьютера.

В обоих случаях такого расхождения загрузка клонированной системы может завершиться так называемым "голубым экраном смерти".

> ***Примечание***
>
> Существует способ добавить в систему драйверы основных устройств так, чтобы система смогла стартовать на новом оборудовании. Этот способ описан в *разд. "Снятие образа физического сервера" главы 8*.

Причиной второй части проблем является наличие в системе уникальных параметров, которые были созданы одной из установленных программ. Самый известный пример из этой области — уникальный идентификатор безопасности, который присваивается каждому компьютеру при включении его в домен. Поскольку в домене не может быть двух компьютеров с уникальным идентификатором безопасности, то простое дублирование диска приведет в таком случае к ошибке в работе.

Другие уникальные характеристики настройки компьютера — это его имя, параметры сетевой настройки (IP-адрес) и т. п. В зависимости от установленного программного обеспечения на компьютере могут присутствовать и другие уникальные идентификаторы (например, идентификатор для систем мониторинга или централизованного управления. Заранее предвидеть все такие параметры практически невозможно. Поэтому администратору необходимо быть готовым к поиску решений возникающих проблем.

Еще одни сложности, которые могут возникнуть при клонировании системы, это наличие зашифрованных файлов (папок). Поскольку при шифровании данных применяется уникальный идентификатор безопасности, который заменяется программами дублирования диска (иными словами, на новой системе данные уже не прочесть), то для сохранности информации *все зашифрованные файлы необходимо расшифровать перед клонированием*.

Существует специальный способ подготовки жесткого диска к дублированию, рекомендованный вендором. Это использование утилиты sysprep.

Утилита *sysprep*

Рекомендуемый вариант подготовки жесткого диска к установке на другом компьютере состоит в использовании утилиты sysprep, поставляемой в составе дистрибутива системы. Версии утилиты отличаются для различных операционных систем. При возможности следует всегда использовать наиболее свежие версии. Например, начиная с версии 1.1, добавлена возможность обнаружения при завершении установки новых драйверов IDE-дисков. Проверить наличие новых версий необходимо на сайте изготовителя.

В Windows 2008 утилита находится в папке Windows, в других версиях ее нужно искать в Support\Tools\ установочного компакт-диска системы в архиве deploy.cab.

Программа sysprep практически "возвращает" программу установки на несколько шагов назад, при этом допустимо использовать 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".

Создание установочного образа системы при помощи утилиты *sysprep*

Для создания установочного образа системы при помощи утилиты sysprep нужно выполнить следующие действия:

1. Установите на типовой компьютер желаемую версию операционной системы, последние обновления безопасности, все прикладное программное обеспечение (офис, антивирусное ПО, обозреватели Интернета третьих фирм и т. п.).
2. Создайте на диске (в корне) папку SYSPREP, запишите в нее утилиты Sysprep.exe и Setupcl.exe (эта папка после установки системы будет автоматически удалена).
3. Чтобы исключить запросы дополнительной информации после переноса диска на новый компьютер (например, запроса серийного номера Windows), создайте в папке SYSPREP файл ответов. Проще всего воспользоваться программой диспетчера установки (Setupmgr.exe). После генерации файла ответов желательно просмотреть его и включить дополнительные параметры, если это необходимо.
4. После сохранения файла ответов запустите программу sysprep. По завершению ее работы можно перенести жесткий диск в новую систему и включить компьютер. Обычно через несколько минут система завершит процесс установки и будет полностью работоспособна.

Примечание

Если предполагается наличие не PnP-устройств (это обычно относится к установке на устаревшее оборудование), то при запуске программы sysprep используйте ключ `-pnp`. Это позволит обнаружить такие устройства на новом компьютере, но может существенно (до 20 минут) увеличить процесс установки.

Подготовка диска для существенно отличающейся системы

Если аппаратная платформа, на которую предполагается установить клонированный образ жесткого диска, содержит устройства, драйверы которых не включены в состав дистрибутива операционной системы, то нужно предпринять дополнительные шаги. В первую очередь это относится к платформам с аппаратным RAID-массивом.

В этом случае необходимо специальным образом подготовить жесткий диск *перед* операцией клонирования[1].

1. Чтобы команда `sysprep` "заставила" программу установки протестировать на новой системе все типы жестких дисков, следует включить в файл ответов такие строки:

```
[Sysprep]
BuildMassStorageSection = Yes
[SysprepMassStorage]
```

2. Чтобы добавить новые драйверы устройств, которые отсутствуют в дистрибутиве Windows, внутри[2] папки SYSPREP создайте папку с названием, например, Drivers. Для удобства можно сделать структуру папки разветвленной, например создать папки Drivers\Video, Drivers\Net и т. п. Скопируйте в эти папки OEM-драйверы устройств компьютеров вашей сети.

Примечание

По умолчанию драйверы должны содержать цифровую подпись изготовителя. В противном случае их установка будет отложена до первого входа администратора в систему. Если необходимо разрешить установку драйверов без цифровой подписи, то следует включить в секцию `[Unattended]` файла ответов строку `DriverSigningPolicy = Ignore` (как при использовании программы *sysprep*, так и RIS).

3. Дополните файл ответов Sysprep.inf в разделе `[Unattended]` ссылками на папку с драйверами по следующему образцу:

```
OemPnPDriversPath = <путь_к_папке_драйверов>;<путь_к_папке_драйверов>
```

Папки должны быть перечислены через точку с запятой. Например:

```
OemPnPDriversPath = "sysprep\Drivers\net; sysprep\Drivers\Video"
```

---

[1] Можно воспользоваться утилитами редактирования файла образа диска, добавить в него необходимые папки и изменить соответствующим образом файлы настроек.

[2] Можно разместить драйверы и в другом месте, соответственно подправив путь к ним в файле ответов. Например, в корневой папке жесткого диска. Причина размещения драйверов именно в папке SYSPREP — это автоматическое ее удаление после завершения установки системы.

Желательно включить в образ максимальное число драйверов, чтобы обеспечить его универсальность.

После завершения этих операций запустите утилиту sysprep.

Дублирование жесткого диска

После завершения операций утилиты sysprep необходимо этот жесткий диск использовать как образец для создания новых. Существует много средств, позволяющих сделать копию жесткого диска.

Наиболее простой вариант создания копии данной системы заключается в дублировании структуры жесткого диска. Наиболее популярна программа GHost от компании Symantec, часто используют также 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 использовать этот файл для последующего создания копий дисков. Особенно удобно использовать вариант сетевого разворачивания образа диска при одновременной подготовке нескольких систем. В этом случае запись диска будет вестись одновременно на все компьютеры.

Разворачивание по сети требует установки соответствующего сервера. Загрузка систем в этом случае будет происходить либо по сети (используя PXE-вариант загрузки), либо со специально подготовленного загрузочного диска (если сетевая

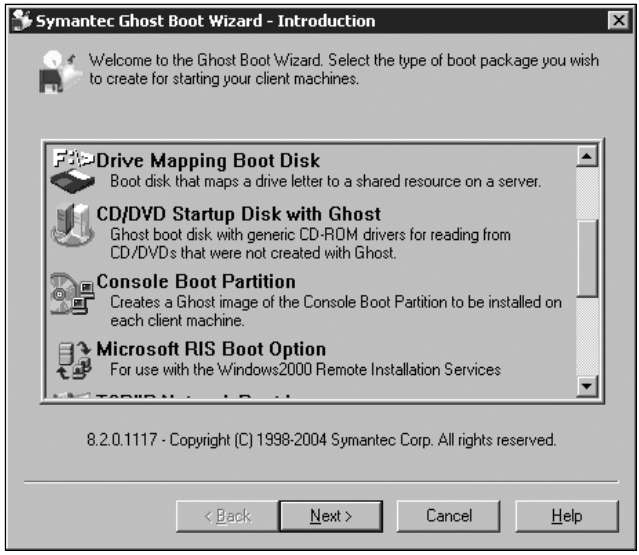


Рис. 6.17. Мастер создания загрузочного диска.
Мастер помогает создать дискету, после загрузки с которой можно осуществить дублирование жесткого диска с подключением к другому компьютеру. В случае необходимости создается индивидуальный образ с использованием драйверов сетевого адаптера от изготовителя оборудования

карта не поддерживает режим *PXE*[1]). Функция подготовки такого диска включается в корпоративные версии соответствующих программ (рис. 6.17). Замечу, что корпоративные версии программ предлагают и иные специальные варианты выполнения операции. Например Symantec GHost Solution Suite позволяет автоматически создавать виртуальные разделы, после загрузки с которых программа дублирования получает полный доступ как к жесткому диску, так и к различным сетевым устройствам с файлами-образами дисков.

Образы клонируемого диска и их модификация

Вместо дублирования подготовленного диска можно создать его *образ* и сохранить такой файл на сервере. Практически все программы клонирования дисков позволяют формировать 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.

После подготовки диска программой sysprep при включении новой системы начинается просмотр специальных папок. В эти папки можно включить сценарии (и соответствующие файлы программ установки), которые будут выполнены автоматически при включении системы. Таким образом можно легко добавлять в образы новые программы и возможности.

Описание правил добавления автозапускаемых сценариев можно найти в справке утилиты sysprep. А для редактирования файла образа легко найти соответствующую утилиту.

Клонирование компьютеров-членов домена

Программа sysprep не позволяет клонировать системы, являющиеся членами домена. Необходимо сначала перевести компьютер в рабочую группу, после чего клонировать диски и добавить новые станции в домен.

Обратите внимание, что некоторые программы имеют специальные функции для клонирования дисков со станций, являющихся членами домена. Например, упоминавшаяся ранее программа Symantec GHost CE. При установке такой программы учетная запись, от имени которой она будет запускаться, наделяется правом добавления рабочих станций в домен. В результате появляется возможность клонирования диска и последующего автоматического добавления системы в домен за одну операцию. Пользователем данная операция воспринимается как клонирование станции-члена домена.

---

[1] *PXE* (от англ. Preboot eXecution Environment) представляет собой среду для загрузки компьютеров с помощью сетевой карты без использования жестких дисков и других аналогичных устройств. PXE-код, находящийся в сетевой карте, загружает из сети исполняемый файл, которому и передает управление для дальнейшей работы системы.

Подготовка программ для тихой установки

При установке прикладных программ часто приходится вводить много ответов, указывая путь установки, состав выбранных функций и т. п. Необходимость таких операций, с одной стороны, снижает скорость установки программного обеспечения, с другой — осложняет выполнение операций установки в автоматическом режиме.

> ***Примечание***
>
> Для тихой установки следует использовать *корпоративные* версии программ. Если программа требует, например, ввода индивидуального серийного номера, то такие действия крайне сложно автоматизировать.

Существуют разные способы подготовки программ к установке без запросов к пользователю.

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 (рис. 6.18), 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.

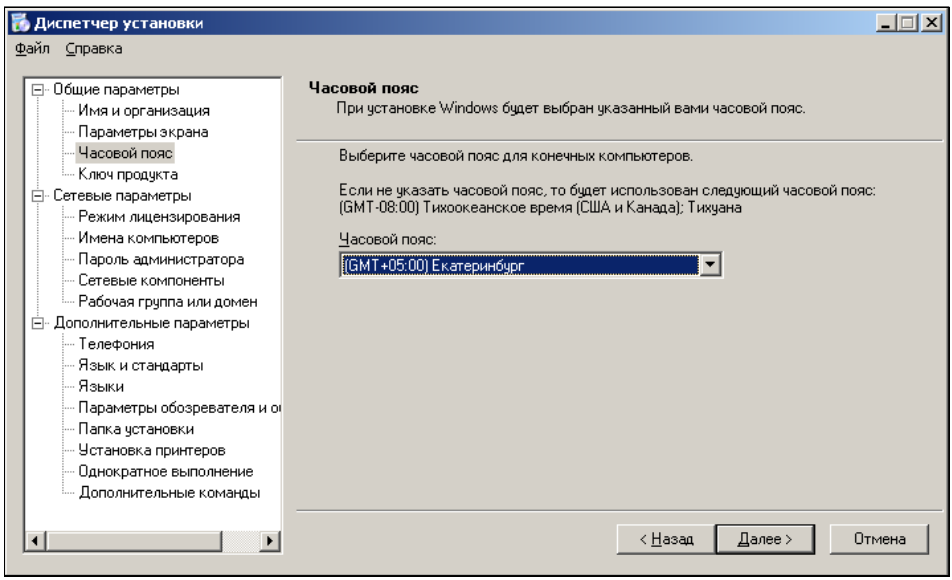


Рис. 6.18. Программа формирования файла ответов для автоматизированной установки

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.

Если не удается найти инструкции по составлению трансформаций у изготовителя продукта, то можно воспользоваться программами для редактирования установочных файлов (рис. 6.19) (не забывайте, что есть программы, преобразующие исполняемые файлы установки (setup.exe) к виду *.msi). Как правило, эти программы либо записывают ответы пользователя во время тестовой установки, либо позволяют отобразить структуру MSI-файла, назначить необходимые параметры, скрыть диалоговые окна и т. п.

Примечание

Если в процессе подготовки файлов трансформаций не были заданы все параметры, то могут возникнуть ситуации, когда программа выведет диалоговое окно для получения дополнительной информации установки. Если установка должна выполняться скрытно и не от имени учетной записи текущего пользователя, то подобная ситуация может привести к сохранению остановившейся программы в памяти системы сколь угодно долго. Поэтому подготовленные к установке пакеты должны быть обязательно протестированы.

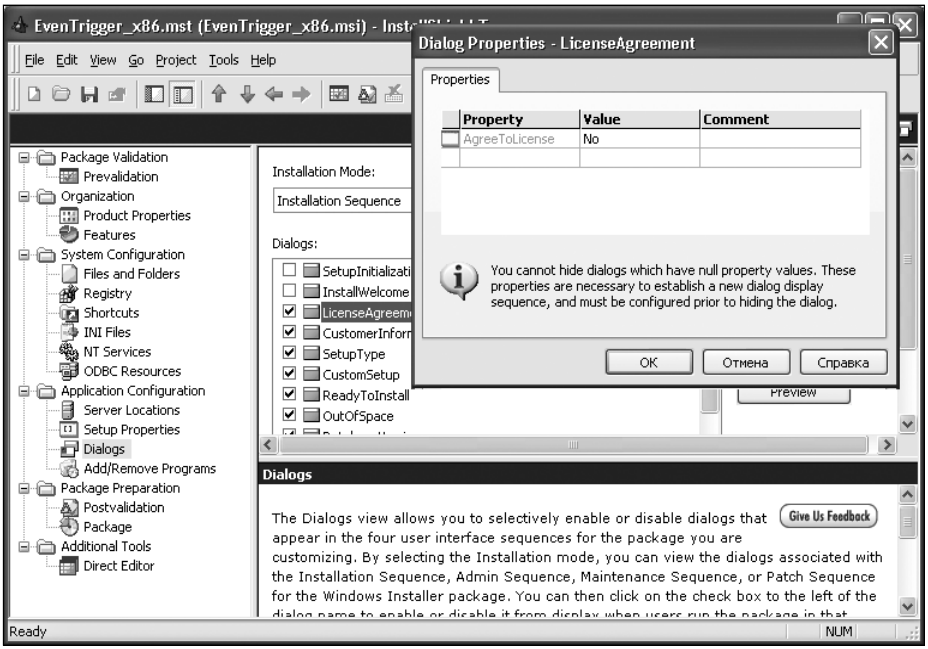


Рис. 6.19. Редактирование установочного файла с помощью специализированной программы

Использование ключей тихой установки

"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.

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.

> ***Примечание***
>
> Если в процессе установки с выбранным ключом возникла ситуация, требующая введения пользователем дополнительной информации, то программа покажет соответствующее диалоговое окно.

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 использовать 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 будет иметь имя *setup.iss*. Аналогично, если вы не используете для файла ответов имя по умолчанию, то его необходимо указать с ключом `/f1` при запуске тихой установки.

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 установ-

ки, 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. В этом процессе от администратора требуется меньшее вмешательство: достаточно

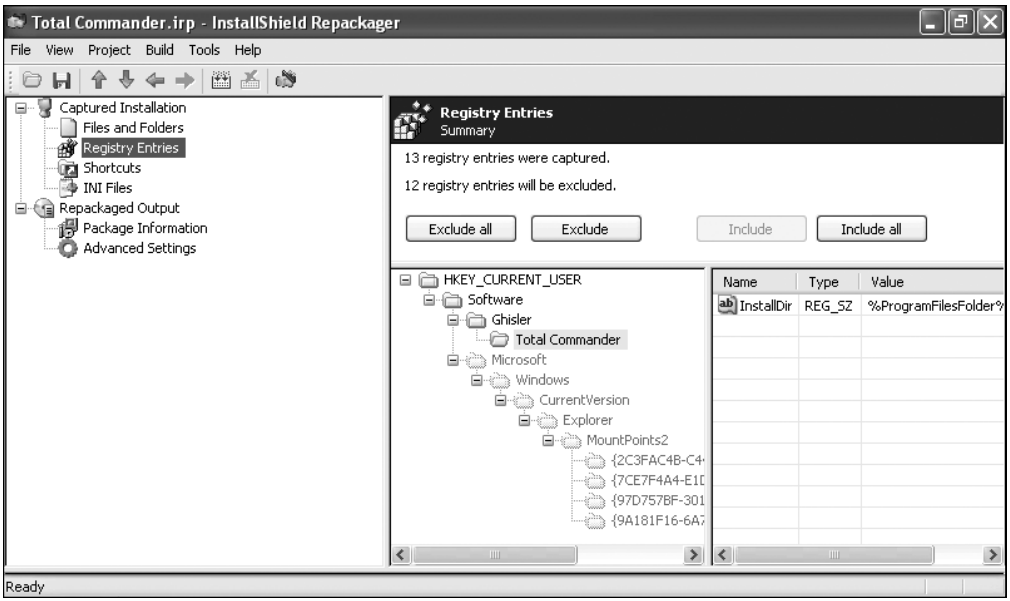


Рис. 6.20. Программа показывает изменения, которые вносит программа установки в настройки системы

проконтролировать зафиксированный перечень изменений и отказаться от шагов, которые могли быть вызваны фоновой активностью системы (рис. 6.20).

Переупаковка позволяет включить в один дистрибутив несколько последовательно устанавливаемых продуктов. Достаточно запустить до второго сканирования системы необходимое число программ. 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.

Административная установка

В организациях часто используют *административную установку*. Административная установка подразумевает перенос дистрибутивных файлов продукта в какую-либо сетевую папку с одновременным внесением настроек, специфичных для данной организации. Так, многие программы имеют функцию установки отдельных компонентов "по требованию" (при первом обращении). Вы можете включить в административную установку указание на несколько сетевых путей, где будут храниться файлы дистрибутива. В результате при попытке добавления компонента инсталлятор проверит несколько сетевых папок и не сообщит об ошибке, если одна из них недоступна в текущий момент. Вы также можете включить в установку, например, указание параметров подключения почтового клиента к серверу Exchange. Таким образом пользователи, первый раз запускающие Outlook, автоматически увидят свой почтовый ящик без необходимости промежуточных шагов настройки подключения.

Административная установка выполняется с помощью ключа `/a`. При этом следует применять файлы трансформаций.

ГЛАВА 7

Мониторинг информационной системы

Чтобы работать не только по фактам инцидентов, а предупреждать возможные отказы, системный администратор существенную часть своего рабочего времени должен затрачивать на оценку состояния оборудования и программных средств, просмотр протоколов работы различных служб и т. п. Анализ получаемой информации обычно требует высокой квалификации, являясь при этом весьма рутинной операцией. Даже если администратор и не пренебрегает этой частью своих повседневных обязанностей, тем не менее, все эти усилия не могут гарантировать контроль функционирования компонентов в реальном режиме времени.

Поэтому наличие той или иной системы мониторинга системы является требованием к современной информационной системе.

Основные способы контроля

Для мониторинга системы традиционно используются:

- анализ сообщений в журналах системы;
- SNMP-протокол (для контроля активного оборудования);
- имитация запросов к системе (например, тестовый запрос к базе данных);
- специальные агенты, дополнительно устанавливаемые в системы (для расширенного мониторинга).

Журналы системы и программ

Во время работы все программы записывают в журналы основные события. Поэтому основным способом контроля работоспособности программ является анализ журналов в операционной системе.

Если говорить о Windows-системах, то это системные журналы приложений, безопасности и системы, а также журналы приложений. В Linux-компьютерах это системный журнал (syslog) и также журналы приложений (обычно создаются в папках

каталога var). Журналы можно анализировать локально или же перенаправлять события на другой компьютер. В Windows в этих целях применяются возможности подписки на события журналов (доступно с выпуска Vista), для Linux можно легко установить централизованный Syslog-сервер, на который будет направлены сообщения локальных систем.

Протокол SNMP

Оборудование информационных систем обычно контролируется по протоколу SNMP (описан далее в этой главе). Кроме того, в программное обеспечение встраивается функционал отправки предупреждений о событиях на заданный адрес. Конечно, не все оборудование обладает такими возможностями. Устройства, предназначенные для небольших организаций, снабжаются только простейшими веб-интерфейсами управления, на которых только можно увидеть информацию о состоянии. В лучшем случае, можно настроить оповещения по электронной почте.

Контроль ответов служб

Если можно сгенерировать тестовый запрос к приложению и получить на него ответ, который доступен для анализа, то это будет лучшим способом контроля работоспособности службы.

По такому способу организован так называемый *безагентный* мониторинг. Так можно проверять сетевые службы (сервер DHCP, DNS и аналогичные), доступность веб-серверов, электронной почты и т. п. При этом при контроле работы проверяется не только сам факт ответа, но и его содержимое. Например, для веб-сервера можно проконтролировать наличие в ответе сервера определенной строки, для электронной почты — проверить в ответе имя почтового узла и т. п.

Таким же методом можно проверять и серверы баз данных — путем генерации SQL-запроса к тестовой таблице и проверке содержимого ответа.

Главное преимущество данного способа — это абсолютное невмешательство в работу контролируемой системы, проверка производится извне системы, на нее нет дополнительной нагрузки за счет работы программ контроля (количество контрольных запросов в производственной системе обычно на несколько порядков меньше числа запросов полезной нагрузки).

> ***Примечание***
>
> В современных операционных системах объем информации, доступный для внешних программ без установки локального агента, существенно увеличен. Это относится к той информации, которая доступна по стандартным протоколам (WMI и аналогичным). Понятно, что при получении такой информации внешняя программа должна предъявить соответствующие полномочия.

Мониторинг с использованием агентов

Данный способ предполагает установку на контролируемую систему некоторой программы (ее принято называть *агентом*), который либо самостоятельно выпол-

няет проверки по заданному графику, либо обеспечивает выполнение задания контроля, получаемого с сервера. Результаты проверки агентом возвращаются на сервер мониторинга. Преимущество данного способа контроля заключается в том, что наблюдению доступны практически любые параметры как оборудования, так и программной среды. Недостатки — необходимость предварительной установки агентов, затраты производительности на исполнение агентов (эта производительность отнимается 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.

Simple Network Management Protocol

Для сбора информации от оборудования, подключенного к сети, и управления им используется специальный протокол SNMP (Simple Network Management Protocol, простой протокол управления сетью). Устройства[1], которые допускают управление по данному протоколу, могут принимать из сети команды, выполнять их и передавать информацию о параметрах своей работы. Например, после получения сообщения о прекращении поступления электроэнергии от управляемых аварийных источников программа может запросить данные об уровне зарядки аккумуляторных батарей и отложить отключение компьютеров до момента практически полной разрядки.

SNMP-протокол использует отправку сообщений по протоколу UDP (т. е. без установления соединений и контроля доставки сообщения).

> ***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 сообществ передаются по сети в открытом виде, что легко позволяет перехватить их снифферами. Поэтому обращайте внимание на то, что имена сообществ (community в терминологии протокола SNMP) ни в коем случае не должны сохранять значения по умолчанию, их следует заменить на достаточно длинные и сложные названия. А интерфейсы управления такими устройствами желательно выделить в отдельную виртуальную сеть.

В системах мониторинга SNMP-протокол используется для активного сетевого оборудования: маршрутизаторов и коммутаторов, аварийных источников питания, модемов и т. п.

Существует две возможности мониторинга по протоколу SNMP.

Первая технология заключается в периодическом опросе параметров работы, анализу их (с генерацией предупреждений в случае выхода значений за пределы нормального функционирования) и сохранению полученных данных в электронной

[1] Цена управляемых устройств выше неуправляемых конструкций, в связи с чем в малых организациях чаще используют неуправляемое оборудование.

таблице или базе данных (для возможной последующей оценки администратором трендов).

Второй вариант — настройка генерации предупреждений на самом устройстве. В этом случае сообщение о событии будет послано самим устройством. Такие сообщения в терминах SNMP принято называть *трапами*.

> ***Примечание***
>
> В целях безопасности современное активное оборудование в настройках по умолчанию не использует протокол SNMP, его надо включить соответствующими командами управления и настроить (выбрать уровень, ввести параметры безопасности и т. п.).

SNMP-управление отличается относительной простотой реализации. Каждый настраиваемый или контролируемый параметр имеет уникальный номер. Для получения информации о состоянии устройства достаточно к нему отправить команду с указанием номера параметра, а для управления — команду установки параметра с его номером и значением (мы не рассматриваем в этом контексте вопросы аутентификации и авторизации протокола SNMP). Чтобы настроить трапы, следует указать, для каких событий они должны быть включены, и определить адреса системы, на которую будут отправляться сообщения.

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. Такие идентификаторы называются *OID* (Object Identifier). Структура идентификаторов описывается в специальных файлах, которые называются *MIB-файлами* (Management Information Base). Основная часть структуры стандартизована, но отдельные параметры описываются в проприетарных MIB-файлах (доступны к загрузке с сайтов разработчика оборудования).

> ***Примечание***
>
> *Проприетарные* (от англ. *proprietary*) — частные, патентованные, разработанные внутри компании для собственных целей (о программных или аппаратных средствах).

MIB-файл позволяет также вместо цифровых индексов использовать их символьные обозначения. Это может быть более удобно для администратора (запрос по цифровому идентификатору можно выполнить всегда, для использования символьного обозначения в программу должен быть импортирован соответствующий MIB-файл). Например, чтобы получить состояние порта коммутатора, надо 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.

Интересующиеся читатели могут посетить страницу **http://www.mibdepot.com/index.shtml**, на которой собрано большое количество MIB как стандартных, так и разработки отдельных вендоров. Также можно воспользоваться любой из доступ-

ных утилит-просмотрщиков MIB-файлов, которые позволяют легко найти нужный параметр и/или идентификатор (рис. 7.1).

В запросах можно использовать как символьные, так и численные наименования идентификаторов. Так, указанному ранее параметру соответствует индекс .1.3.6.1.2.1.2.2.1.8.101. Для повышения производительности системы контроля рекомендуется использовать именно численные значения, поскольку программе не приходится искать соответствие в файлах настроек. Хотя в случае символьного написания сами команды более удобочитаемы.

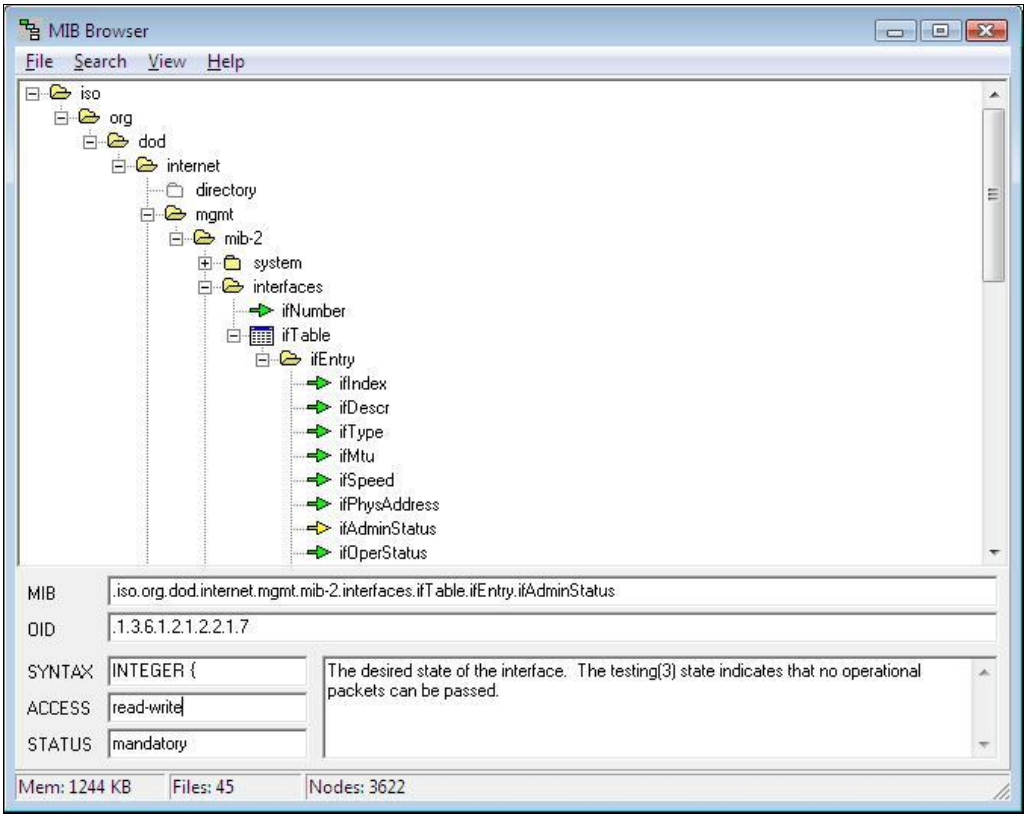


Рис. 7.1. MIB-browser.
На рисунке показан интерфейс одной из программ просмотра MIB. С помощью таких программ можно найти название и цифровой индекс того параметра, значение которого предполагается контролировать в системе мониторинга

В большинстве случаев достаточно использовать стандартные параметры. То, какие из них соответствуют желаемой информации, легко найти в Сети по ключевым словам "mib browser". Например, на странице **http://support.ipmonitor.com/mibs_byoidtree.aspx** (рис. 7.2) можно увидеть все дерево параметров и найти нужную ветвь.

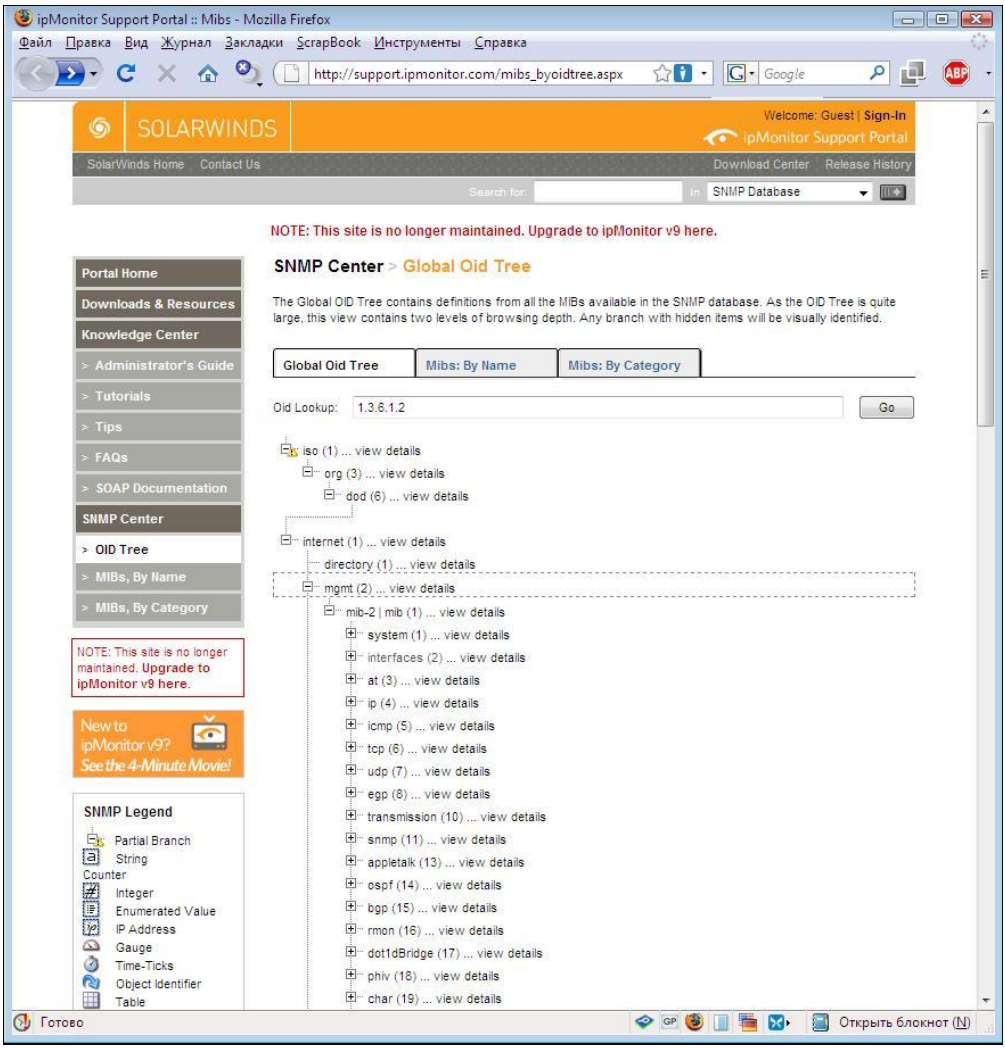


Рис. 7.2. Глобальная структура MIB.
На рисунке показана страница одного из сайтов с отображением глобальной структуры MIB. Такие источники помогают правильно выбрать контролируемые параметры

Простейшие варианты мониторинга

Профессиональные системы мониторинга не дешевы. В то же время потребности небольших систем легко удовлетворить подручными средствами.

Контроль журналов Windows

Операционная система постоянно фиксирует состояние выполнения тех или иных операций в *журналах*. Записи в журналах являются для администратора "первой ласточкой", предупреждающей о неполадках в работе. Однако при увеличении чис-

ла обслуживаемых администратором систем своевременно прочитывать информацию журналов на всех компьютерах у администратора не хватает времени.

В этом случае необходимо использовать специальные возможности оснастки просмотра журналов в Windows 7/Windows 2008.

Привязка задачи

Администратор может настроить автоматический запуск какого-либо задания в случае возникновения события в журнале. Можно это сделать, явно указывая параметры события при создании задания, но удобнее перенести параметры из сообщения журнала.

Выделите сообщение, по появлению которого нужно выполнять некие действия, и перейдите по ссылке **Привязать задачу** (рис. 7.3). Дальнейшие шаги будут происходить под управлением мастера операций. Вы можете назначить отсылку сообщения (в том числе по электронной почте) или запустить любую задачу.

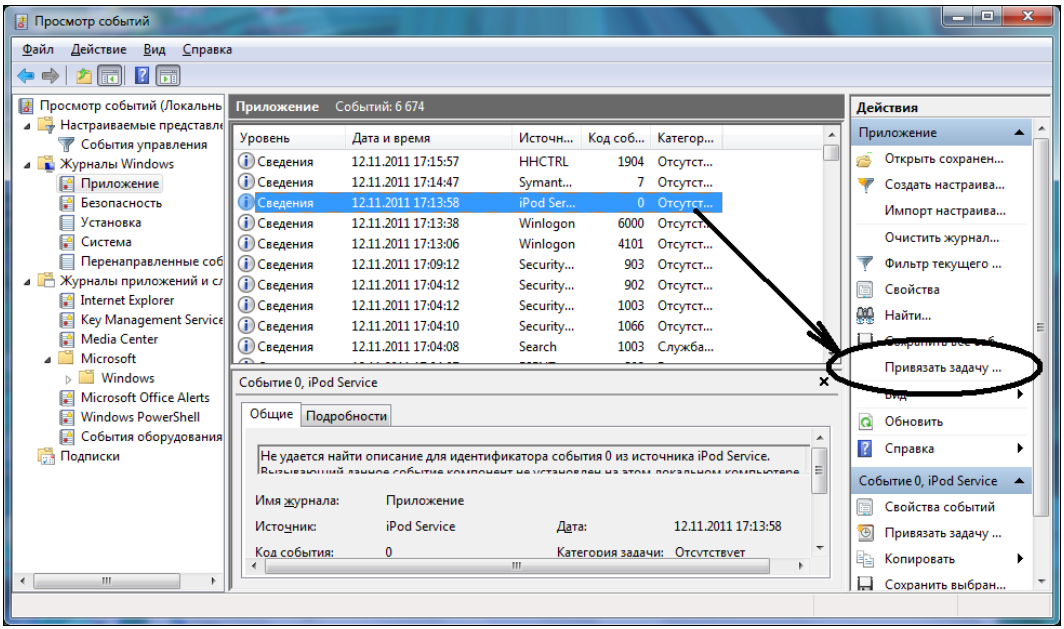


Рис. 7.3. Окно программы просмотра журнала событий

После настройки правила реагирования на события появятся как задания в журнале планировщика (рис. 7.4).

В сервере Windows 2003 возможности в привязке задачи нет. Но можно воспользоваться специальным сценарием — `EVENTTRIGGERS`, который позволяет настроить автоматические действия системы на то или иное событие. Справочная система к этой команде подробно описывает, как следует создать триггер, настроенный на появление определенного события. Поэтому мы не будем останавливаться на этом описании.

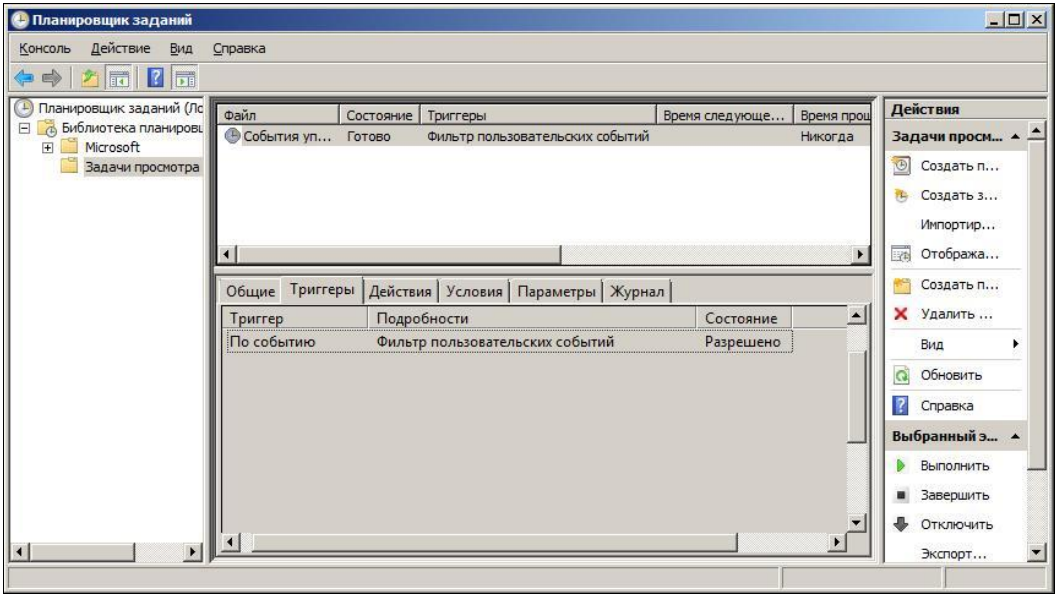


Рис. 7.4. Планировщик заданий Windows 2008.
Это задание отсылает сообщение по электронной почте на указанный адрес в случае появления нового сообщения в созданном администраторе, настраиваемом представлении журнала событий

Подписка на события

Оснастка просмотра события позволяет собирать сообщения с других компьютеров. Для этого достаточно настроить *подписку* (рис. 7.5). При настройке подписки вы также указываете правила сбора сообщений (фильтрации), определяете компьютеры, с которых ведется сбор данных и т. д. Обычно все собранные таким образом сообщения направляют в журнал **Пересланные события**, который можно использовать при создании собственных настраиваемых сообщений.

В серверах Windows 2000/2003 подобная функциональность в оснастке просмотра событий отсутствует. Но вы можете воспользоваться бесплатной утилитой EventCombMT из состава Resource Kit для сбора событий с нескольких систем. Утилита входит в состав Account Lockouts Tools (см. документ KB824209) и позволяет собирать события с учетом фильтрации по номеру (точное совпадение, диапазон номеров и т. п.), по источнику события, по тексту сообщения, по времени события и т. д. (рис. 7.6). В составе утилиты присутствует подробная справка, которая помогает составить любой необходимый фильтр поиска сообщений.

Другой возможный способ для систем Windows XP/Windows 2003 — это использование сценария EVENTQUERY.vbs, который позволяет вывести события как с локального, так и с удаленных компьютеров, используя необходимые фильтры (по дате, по номеру события, типу и т. п.). Кроме того, анализировать журнал событий можно и другими средствами. Так, утилита LogParser позволяет в том числе подключаться к журналам событий различных компьютеров и осуществлять произвольные выборки сообщений.

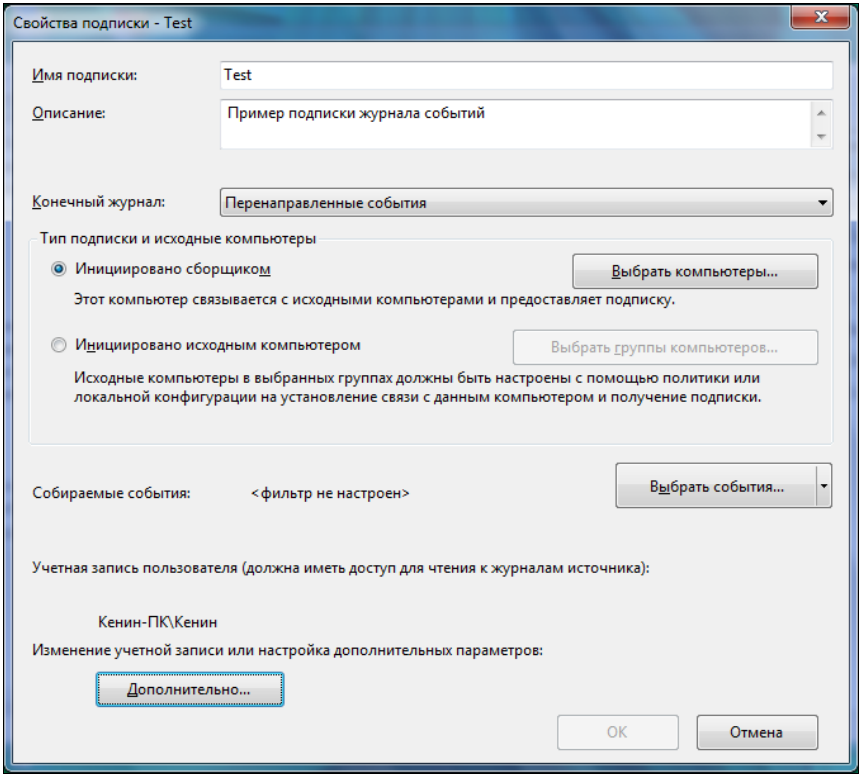


Рис. 7.5. Окно мастера настройки подписки

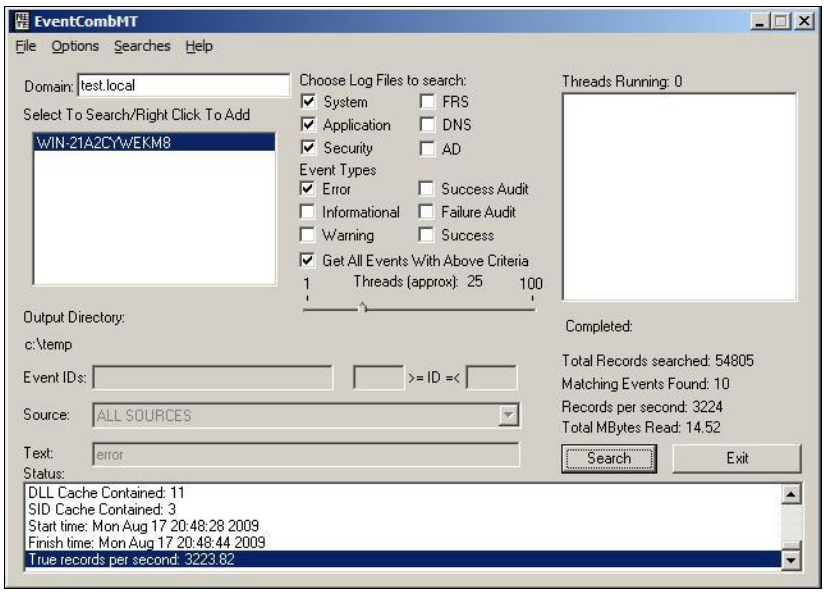


Рис. 7.6. Утилита *EventCombMT*. Администратор может достаточно просто настроить фильтры для поиска сообщений на любом числе компьютеров. Утилита специально спроектирована для многопоточного поиска, что позволяет быстро осуществлять поиск заданного события на многих компьютерах. Результаты работы утилиты сохраняются в текстовом файле

Создание собственных событий в журналах Windows

Поскольку мы умеем реагировать на события в журналах системы, то для настройки действий на любое другое событие в системе можно поступить очень просто: достаточно внести о нем запись в системный журнал, а далее уже использовать средства привязки задачи к такому событию.

Начиная с Windows 2003 в составе операционной системы присутствует команда `EVENTCREATE`. С ее помощью можно записать в любой журнал событие заданного типа (информация, ошибка и т. п.). Использование утилиты подробно описано в ее справке (`EVENTCREATE /?`), к которой мы и отошлем читателя.

Настройка журналирования в syslog

Системный журнал 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.

> ***Примечание***
>
> *Журналирование* — процесс записи информации о происходящих с каким-то объектом (или в рамках какого-то процесса) событиях в журнал (например, в файл).

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 – "|").

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
```

Утилиты мониторинга

Спектр программ мониторинга весьма широк.

Много программ осуществляет сбор сообщений из журналов системы и обработку их по заранее подготовленным критериям. Можно отметить решения EvenTrigger от компании IS Decisions (**www.eventrigger.com**), GFI LANGuard Security EventLog

Monitor (**www.gfi.com**), Advanced Host Monitor от компании KS-Soft (**http://www.ks-soft.net/hostmon.eng/index.htm**), MonitorMagic от Tools4ever (**http://www.tools4ever.com/products/monitormagic/**) и др. Много других программ доступно через поисковые системы, например в Желтых страницах Yahoo, в Google и т. п.

В сообществе присутствует большое число систем, разработанных для мониторинга информационных систем крупных предприятий с многочисленными филиалами. Комплексные системы управления, такие как HP Open View, Tivoli и аналогичные, практически не доступны, прежде всего, по экономическим соображениям, средним предприятиям нашей страны и даже многим крупным. Поэтому особое внимание привлекают продукты, либо приемлемые по цене для большинства заказчиков, либо полностью бесплатные (построенные на продуктах Open Source).

Среди Open Source-проектов можно упомянуть также такие решения, 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 этих проектов в Сети доступны многочисленные расширения, позволяющие достаточно просто обеспечить контроль работы информационной системы.

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/network-monitoring/download-free.html**), который может контролировать бесплатно до 10 систем (серверов Windows и Linux, активное сетевое оборудование).

Среди продуктов, предназначенных для мониторинга больших систем, признанными лидерами для Windows-систем является Microsoft System Control Center (коммерческий продукт) и Nagios (бесплатное решение для мониторинга Windows-, Linux-систем и активного оборудования, де-факто стандарт мониторинга).

Microsoft System Center Operation Management

System Center Operations Manager (SCOM) (ранее *Microsoft Operations Manager*, MOM) предназначен для централизованного отображения информации о функционировании различных компонентов инфраструктуры в единой консоли.

SCOM предназначен для крупных организаций (несколько сотен рабочих станций и несколько десятков серверов). Для небольших организаций существует продукт System Center Essentials, частично включающий в себя функционал System Center Operations Manager и System Center Configuration Manager.

Вариант построения мониторинга на SCOM

В состав SCOM 2007 входит много компонент, обеспечивающих мониторинг систем различной сложности: от самых простых до территориально распределенных с подключением офисов через Интернет, модули сбора и анализа отчетов, формирования графических представлений и т. п. Сразу скажем, что разобраться в на-

стройках SCOM и использовать данную систему для контроля собственных параметров достаточно сложно. Внедрение SCOM — трудоемкий и дорогостоящий процесс, требующий хорошей подготовки. На рис. 7.7 показан вариант реализации SCOM, причем в упрощенном виде, когда все службы сервера сгруппированы на одной системе.

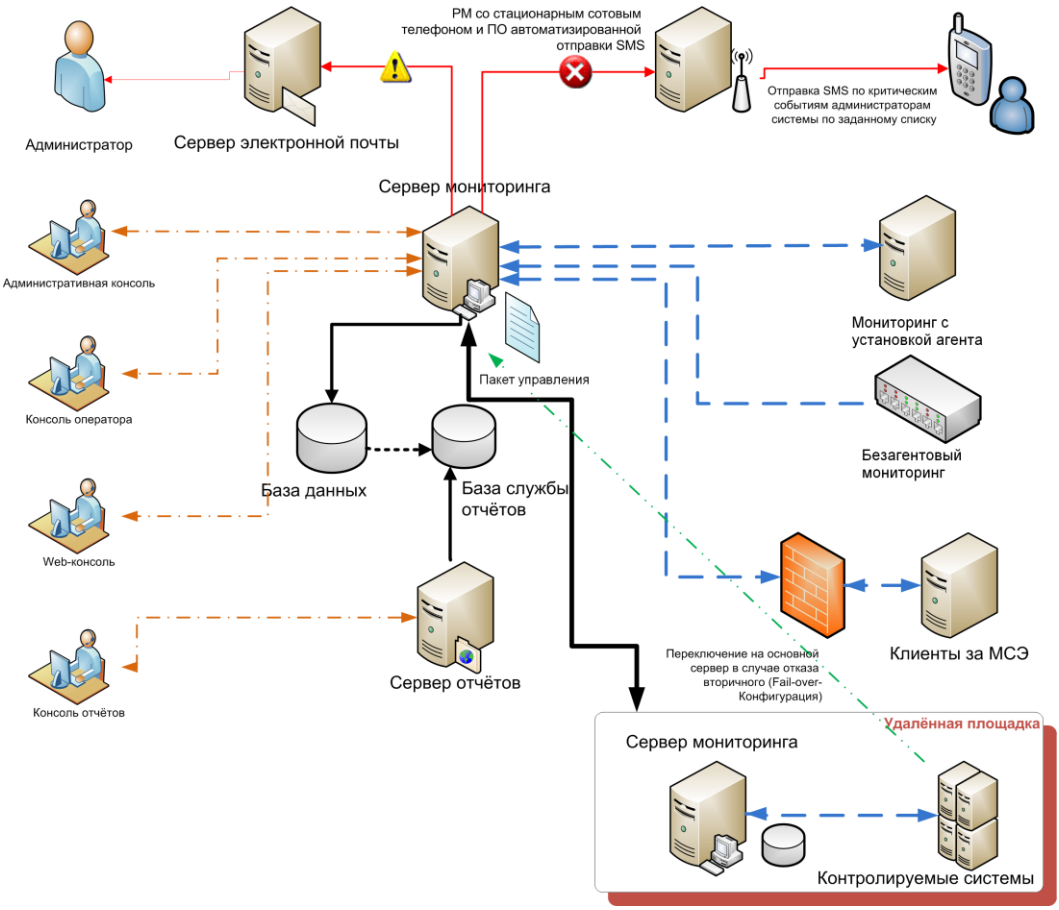


Рис. 7.7. Пример построения решения на SCOM

В качестве примера графического представления отчета, который может быть подготовлен SCOM, на рис. 7.8 показан график загрузки процессоров нескольких серверов в заданный промежуток времени.

Поэтому мы лишь коснемся основ установки и настройки сервера и посоветуем полнее использовать доступную[1] справочную документацию.

- Технический центр SCOM на сайте Microsoft TechNet: **http://technet.microsoft.com/ru-ru/systemcenter/om/default.aspx**.

[1] В Сети существует очень много информации, посвященной настройке и работе с SCOM, которая доступна через поисковые механизмы Интернета.

- Русскоязычный сайт, посвященный SCOM: **http://opsmgr.ru/**.
- Сайт System Center Forum, с которого можно загрузить различные справочные руководства (howto), примеры, сценарии и т. п.: **http://www.systemcenterforum.org/downloads/#OperationsManager2007**.

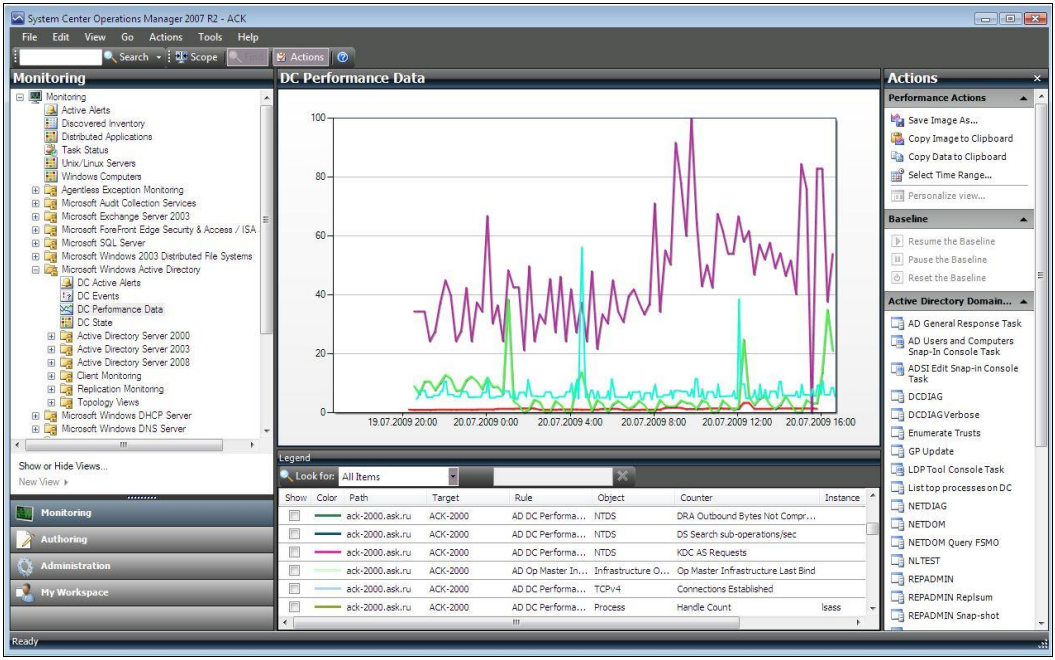


Рис. 7.8. Отчет, сформированный по результатам наблюдения за системой

Установка SCOM

Сервер мониторинга от Microsoft — весьма ресурсоемкий продукт: для комфортной с ним работы требуется производительный сервер. Только рекомендуемое значение оперативной памяти составляет 2 Гбайта. Кроме того, это программное обеспечение предполагает предварительную установку сервера баз данных (Microsoft SQL Server, коммерческого продукта).

Для работы SCOM требует установки на сервер ряда компонент. Их состав зависит от версии операционной системы. Проще всего запустить встроенную в SCOM проверку выполнения условий установки (рис. 7.9) и устранить отмеченные проблемы.

Сама установка предполагает указание администратором типовых параметров (путь установки, имя сервера баз данных и т. п.). Как правило, ответы на вопросы мастера установки легко дать любому администратору.

После завершения установки управление сервером будет осуществляться через его консоль. На рис. 7.10 показана консоль управления сервером SCOM 2007 R2. Это

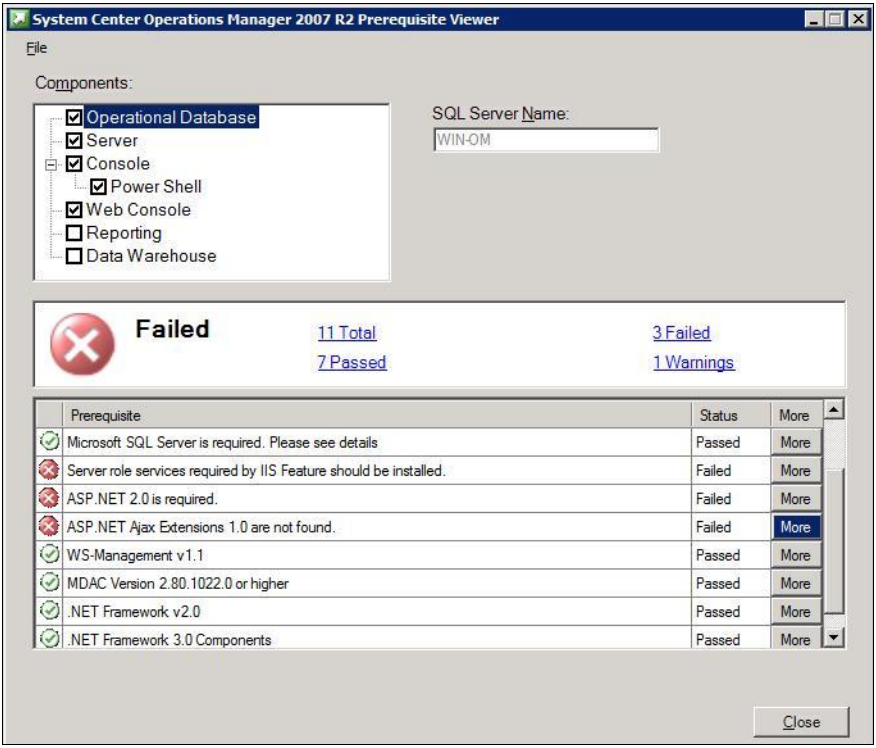


Рис. 7.9. Контроль требуемой для установки SCOM-конфигурации. Если нажать на клавишу More, то вы увидите описание необходимых шагов вплоть до ссылок на загрузку пакетов установки

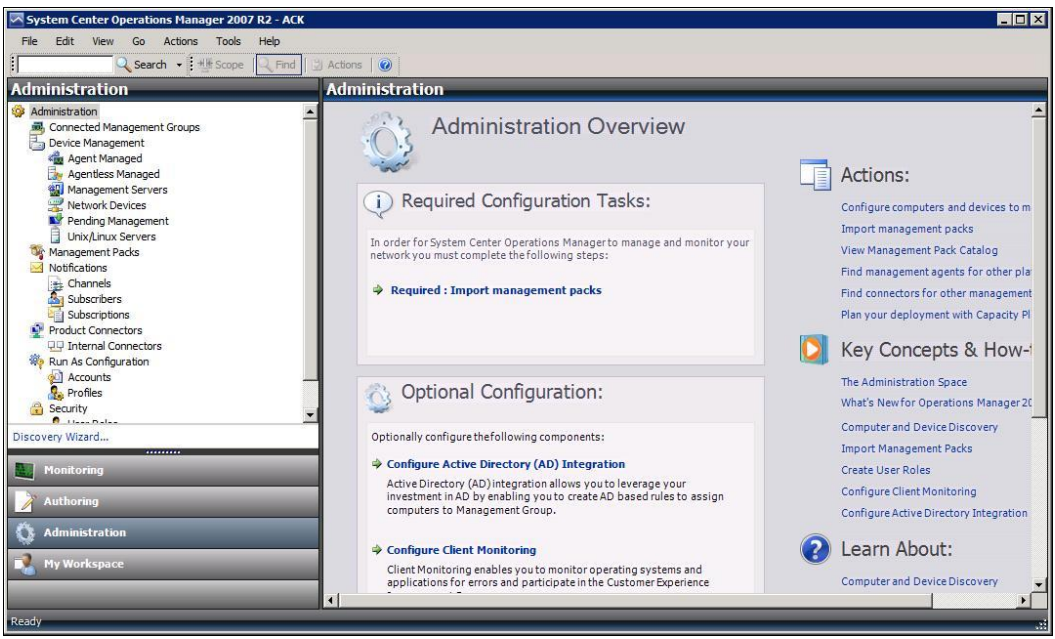


Рис. 7.10. Административная консоль SCOM 2007 R2

основной инструмент, используемый как для настройки, так и для текущей работы с сервером SCOM. Эту консоль можно установить на рабочие места операторов SCOM (в том числе, и на операционные системы рабочих станций).

Операции по настройке SCOM после установки

После завершения процесса инсталляции сервер SCOM практически не может использоваться по назначению. Чтобы начать контролировать системы, необходимо как минимум:

- установить пакеты управления;
- добавить системы, которые будут контролироваться;
- настроить оповещения по возникающим событиям для администраторов информационной системы.

Впоследствии вы можете настроить личное рабочее пространство в SCOM, разместив служебную информацию наиболее удобным способом, создавать собственные сценарии контроля и т. п. Также, как и во всякой большой системе, необходимо будет настроить права тех специалистов, которые будут эксплуатировать SCOM. Но это уже задачи периода опытной эксплуатации.

Импорт пакетов управления

Пакеты управления (*Management Packs*) представляют собой подготовленные комплекты сценариев проверки, правил обработки собираемой информации, программ для настройки соответствующих служб, базы знаний (описаний проблем) по контролируемым параметрам, форм отчетов и т. п. Существуют как бесплатные пакеты (в основном, это пакеты от Microsoft), так и коммерческие (доступны бесплатно только в триальном периоде).

Для поиска пакетов управления можно воспользоваться страницей System Center Marketplace (**http://systemcenter.pinpoint.microsoft.com/en-US/home**), а также поиском по сайтам соответствующих изготовителей оборудования и программ.

Для каждой контролируемой службы необходимо загрузить и импортировать в SCOM соответствующий пакет. Так, существуют пакеты для управления сервера баз данных, службы DHCP и DNS, состояния контроллеров домена, для проверки почтового сервера Exchange и работы SharePoint-сервера и т. д. Я рекомендую просмотреть весь список пакетов от Microsoft и загрузить те из них, которые соответствуют службам, эксплуатируемым в вашей информационной системе.

Пакеты необходимо загрузить на компьютер и запустить их на выполнение (установку). Выполнение пакета — это просто разархивирование содержащихся в нем файлов в отдельную папку. Обратите внимание, что вместе с файлами, которые потом будут импортированы в SCOM, в папке часто находится документация. Обязательно перед установкой пакета прочтите сопутствующие документы, поскольку для нормального функционирования выбранного средства контроля могут понадобиться дополнительные действия. Например, придется создать почтовый ящик, ис-

пользуемый для отправки/приема контрольных сообщений, или настроить значения порогов, в соответствии с которыми получаемые данные будут расцениваться как нормальные или критические, и т. п.

Импорт пакетов осуществляется командой в навигационной панели *Actions* консоли управления сервером или по операции в контекстном меню объекта **Management Pack**. Программа импорта предложит либо загрузить пакеты с сервера каталогов, либо импортировать их с локального диска.

Добавление контролируемых систем

SCOM надо сообщить, какие системы он должен контролировать. Существует вариант как ручного добавления систем, так и автоматического. В любом случае процесс начинается операцией Discovery. Процесс добавления систем аналогичен для различных платформ: необходимо указать критерии поиска (например, по части имени, по каким-либо атрибутам в службе каталогов и т. п.), ввести параметры учетной записи, используемой для подключения к системам и установки программного обеспечения клиента (или параметры *community* в случае использования SNMP), начать процесс установки клиента на удаленную систему.

При *ручном* варианте вы указываете критерии поиска, отмечаете системы, которые будете контролировать, и устанавливаете на них агента (или будете использовать безагентный вариант). После запуска установки можно закрыть окно установки и контролировать итоги в окне **Task Status** (рис. 7.11).

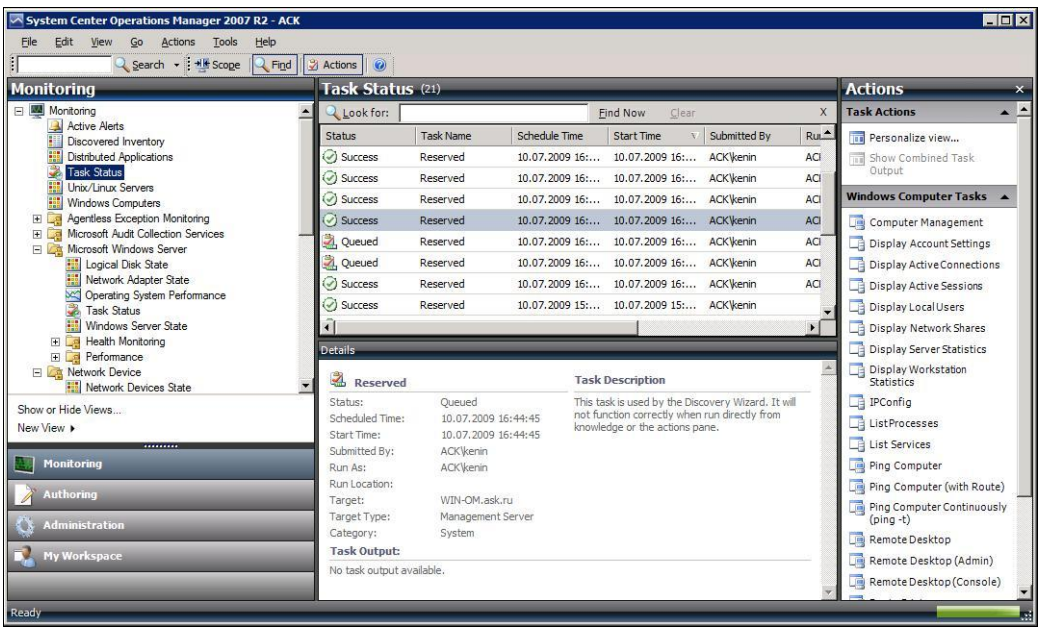


Рис. 7.11. Окно состояния выполнения заданий.
Многие задания в SCOM можно назначить к выполнению и затем просто контролировать ход их реализации в окне **Task Status**. В данном примере в окне задач вы видите состояние заданий по установке агентов мониторинга

В SCOM имеется возможность контролировать ряд параметров систем на основе Linux. К сожалению, перечень таких систем ограничивается только коммерческими выпусками (SuSe, RedHat, HPUX, AIX). Конечно, установочные пакеты для этих систем имеются в папках SCOM и вы можете преобразовать, например, пакеты RPM в пакеты DEB. Но такие действия вы будете выполнять на свой страх и риск и будете надеяться только на собственные силы при устранении сбоев, которые могут возникнуть при мониторинге. Без установки агента на Linux-системы вы можете только контролировать сообщения Syslog'a. Для этого необходимо настроить сбор таких сообщений и написать сценарии для их обработки (см. KB942863).

Настройка оповещений SCOM

Администраторы должны получить сообщения о неисправностях не только тогда, когда они работают в консоли SCOM, но и в любое другое время, предусмотренное регламентом обслуживания информационной системы. Для этого в SCOM необходимо настроить оповещения. Настройка оповещений состоит из:

- настройки каналов оповещений;
- настройки параметров операторов для оповещений;
- настройки критериев, в соответствии с которыми оповещения должны или не должны отсылаться данному оператору.

Канал оповещения (notification channel) — это способ передачи сообщения оператору. Например, отправка по электронной почте (SMTP-channel), отправка мгновенных сообщений (IM), посылка SMS и т. п. Естественно, что в системе должны существовать соответствующие службы. Например, для использования протокола SMTP (рис. 7.12) необходимо иметь работающий почтовый сервер, для отправки SMS следует установить программное обеспечение для работы с сотовым телефоном (и подключить сам телефон) и т. д.

Настройка операторов для получения оповещений, или, в терминах SCOM, — подписчиков (*subscriber*), сложности не представляет. Вы должны только указать параметры для всех доступных данному оператору каналов.

Более трудоемка настройка подписок (*subscriptions*). В некотором смысле операция напоминает создание правил автоматической обработки сообщений в почтовом клиенте: нужно выбрать и настроить все критерии, при соответствии которым сообщения будут отправлены данному оператору.

> ***Примечание***
>
> Начиная работу с SCOM, в качестве критерия выберите отправку всех сообщений о критических событиях (critical). Получив некоторый опыт работы, вы можете оптимизировать критерии подписок.

Немного о структуре объектов SCOM

Приступая к работе с SCOM, достаточно сложно понять назначение различных его элементов и принципы их использования. Поясним кратко основные моменты.

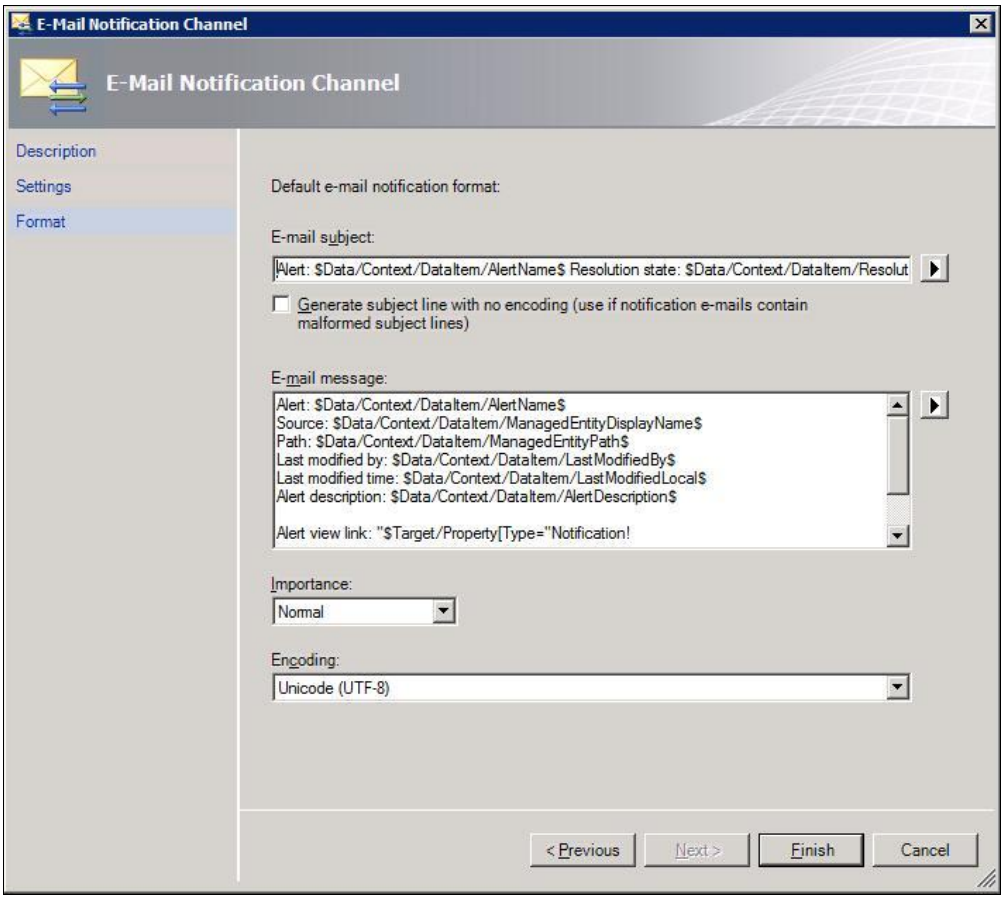


Рис. 7.12. Настройка каналов оповещения.
При выборе варианта оповещения по электронной почте мастер предложит указать параметры почтового сервера и определить текст сообщения, которое будет отсылаться в случае возникновения непредвиденных ситуаций

Как правило, SCOM работает с *группами* — логическими объединениями нескольких элементов. Обычно группы создаются при установке пакетов управления, но их можно создать и вручную. Например, по итогам анализа служб Windows делается оценка о наличии действующего сервера DHCP и система помещается в соответствующую группу (по версии операционной системы; в свою очередь, такая группа входит в общую группу DHCP-серверов).

Для групп пакеты управления создают *мониторы*, которые получают данные о работе необходимых служб. Полученные от них данные анализируются с помощью *правил* (*rules*).

Администраторы имеют возможность как создавать собственные объекты (группы, мониторы и т. п.), так и модифицировать существующие (например, изменить пороги классификации событий с критических на предупреждение и т. п.).

Реагирование на события системы

Консоль SCOM позволяет оптимизировать усилия администратора по контролю систем. Для контролируемых событий консоль на панели задач предлагает ссылки, которыми можно воспользоваться для проверки. Например, можно быстро проверить доступность системы (ping), подключиться к удаленному рабочем столу (причем в ссылке будет стоять нужное имя), запустить программу дефрагментации на той системе, для которой получено сообщение о необходимости данной операции и т. д.

Администратор может легко настроить автоматическое реагирование на возникающие события. Например, можно настроить систему так, чтобы учетная запись пользователя, который очистил журнал безопасности, автоматически блокировалась. Поскольку в этом случае есть основание предполагать, что эта операция призвана скрыть некие действия. В таком случае можно реализовать алгоритм, условно показанный на рис. 7.13.

Понятно, что разработка подобных сценариев реагирования будет оправдана только для решения постоянно возникающих проблем. И конечно, для создания собст-

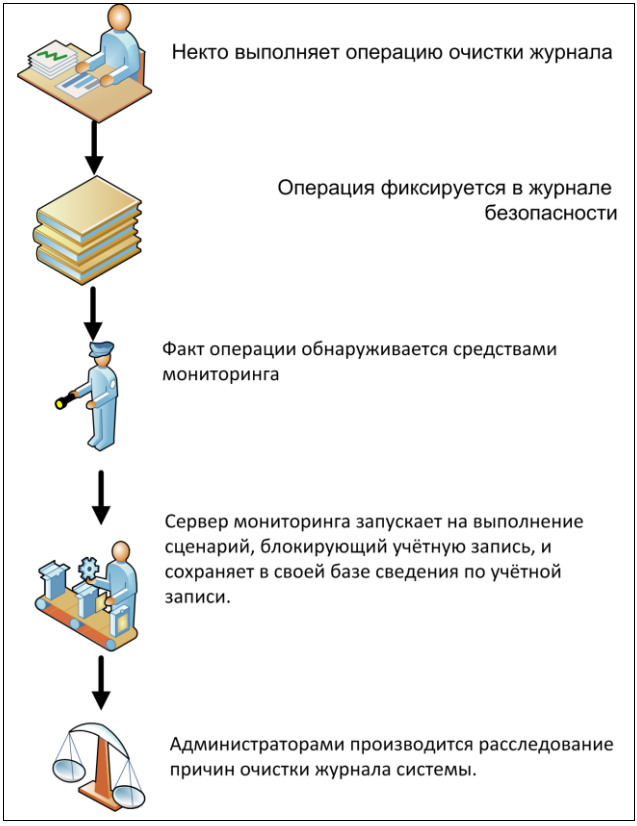


Рис. 7.13. Алгоритм реализации автоматического реагирования системы на событие

венных правил нужно постоянное участие как программиста, так и администратора, что сложно реализуемо в малых и средних организациях.

Nagios

Nagios является программой мониторинга информационных систем на основе открытого кода. Продукт является практически стандартом для систем мониторинга. Он позволяет (в том числе):

- контролировать хосты (загрузка процессора, использование диска, журналы и т. д.) с разнообразными операционными системами — Windows, Linux, AIX, Solaris и т. д.;
- контролировать сетевые службы (SMTP, POP3, HTTP, SSH и т. д.);
- подключать дополнительные модули расширения (плагины) на любом языке программирования (Shell, C++, Perl, Python, PHP, C# и др. — архитектура модулей должна быть открыта), использовать собственные способы проверки служб;
- 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.

Установка *Nagios*

Nagios является OpenSource-проектом, который доступен для установки как в исходных кодах, так и в подготовленных пакетах для различных клонов Linux. Понятно, что установка из исходных кодов имеет более свежую версию, чем подготовленные пакеты.

Установка из подготовленных пакетов осуществляется по правилам соответствующей версии операционной системы. Например, для Ubuntu команда будет выглядеть примерно так:

```
apt-get install nagios2
```

Это гарантирует установку всех необходимых для его работы библиотек и является самым простым способом, рекомендуемым для обычных пользователей.

Процедура быстрой установки программы на Ubuntu описана на сайте в разделе документации (**http://nagios.sourceforge.net/docs/3_0/quickstart-ubuntu.html**). Обратите только внимание на то, что за установкой из исходных кодов должна последовать и установка необходимых плагинов и дополнений.

После завершения установки работу программы можно проверить, открыв страницу **http://localhost/nagios/** (вместо *localhost* следует использовать имя сервера Nagios в случае открытия 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.

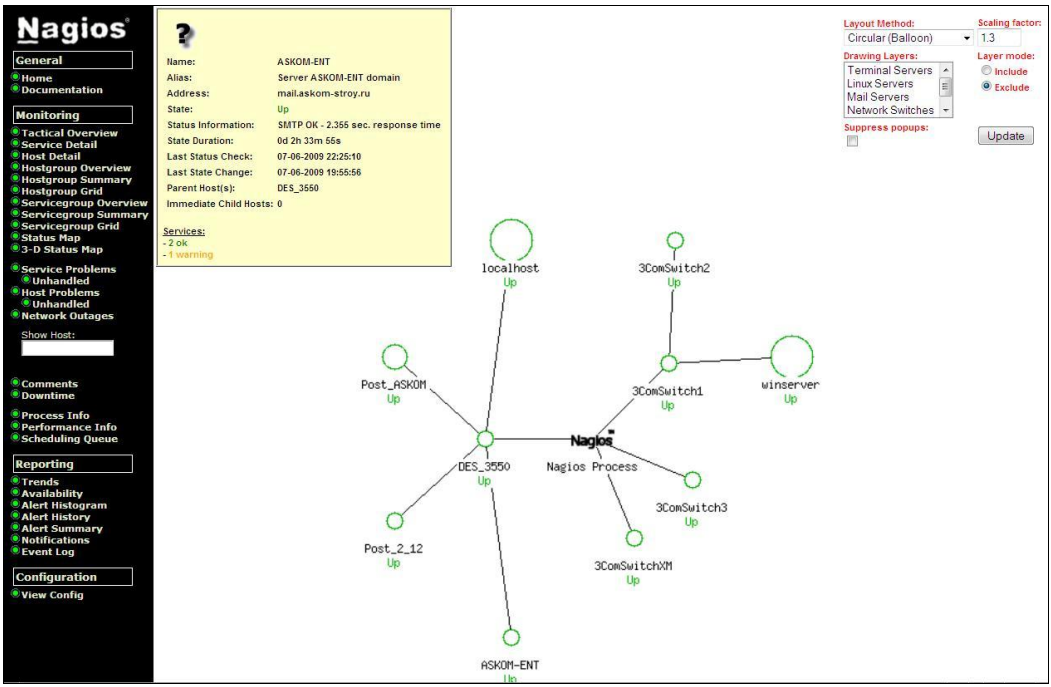


Рис. 7.14. Схема сети в *Nagios*

На рис. 7.14 показана одна из страниц программы — структура контролируемой Nagios небольшой системы (схема строится в Nagios автоматически).

Немного о логике работы *Nagios*

Nagios можно представить условно в виде двух частей: сервера (собственно о его установке и велась речь в предыдущем подразделе) и клиента, т. е. системы, которая контролируется при помощи агента или без его установки.

Существуют различные версии агентов, устанавливаемых на операционные системы. 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/**).

> ***Приложение***
>
> Исторически первым клиентом для Windows был вариант программы *NPRE*. В целях совместимости в *NSClient++* сохранен протокол, используемый в *NPRE*. Вы можете в настройках клиента указать использование как любого варианта работы, так и обоих (некоторые плагины, например, разработаны под конкретную версию клиента). Учтите, что в некоторых случаях *NPRE* предоставляет больше возможностей для контроля, например, с его помощью легко настроить выполнение сценариев на самой контролируемой системе.

Обратим внимание читателя на то, что для каждого клиента должна быть настроена конфигурация так, как описано в последующих разделах.

При помощи клиентов происходит *активный* мониторинг работы: сервер инициирует на клиенте заданную настройками команду и анализирует полученные данные. Кроме того, возможен *пассивный* режим работы в тех случаях, когда данные на сервер пересылаются по инициативе клиента. Например, так происходит обработка SNMP-трапов.

Как уже говорилось, для получения информации от клиента на сервере Nagios запускаются специальные команды (или программы). В терминах Nagios эти команды принято называть *плагинами* (*plugin*).

> ***Примечание***
>
> Плагины несложно найти в Сети: с сайта Nagios есть ссылка на проекты на SourceForge.net, можно использовать сайт обмена плагинами **http://www.monitoringexchange.org/** и другие источники.

Для того чтобы система мониторинга могла их использовать, такие команды должны быть *описаны* в специальном конфигурационном файле — commands.cfg. Именно эти описания в терминах Nagios и называются *командами* контроля.

Кроме описания самой команды, системе мониторинга надо знать, какие системы проверять, как часто запускать команду проверки, надо ли делать 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 отдельным блоком в файле, описывающим параметры контролируемой системы. Поскольку параметров в службе много (около полутора десятков) и многие из них обычно повторяются, то принято описывать повторяющиеся части в *шаблонах* (template), а непосредственно в описании службы просто указывать на такой шаблон (описания шаблонов хранятся в файле templates.cfg). Обратите внимание, что в шаблонах допускаются вложения: какую-то часть параметров можно выделить в отдельный шаблон и использовать его в других описаниях.

Каждая контролируемая система должна быть описана в конфигурации Nagios. Для удобства делается это в отдельных файлах (по типам устройств), которые при старте сервера включаются в общую конфигурацию. Первоначально ссылки на эти файлы "по направлениям" закомментированы, поэтому при необходимости начала контроля какого-либо класса устройств прежде всего следует удалить символ "#" в соответствующей строке файла nagios.cfg, а потом добавить блок описания системы в надлежащий файл.

В результате Nagios периодически выполняет на контролируемых системах заданные команды, собирает результаты и в случае возникновения критического события оповещает операторов. Результаты контроля можно сохранять (по умолчанию данные о производительности не хранятся) и представлять в графическом виде для анализа *(см. разд. "Построение графиков в Nagios")*. Также Nagios позволяет назначить команды, которые будут выполнены при возникновении событий. Таким способом можно автоматически устранять возникающие неисправности.

Если в системе будет контролироваться много компьютеров и устройств, то их удобно сгруппировать. В Nagios можно создать группы из компьютеров (уст-

ройств) и служб. Например, если нужно наблюдать за состоянием всех служб на серверах, то следует создать группу, в которую включить названия этих систем. А если вы хотите контролировать состояние, например, службы разрешения имен DNS, которая работает на нескольких физических системах, то в этом случае удобно создать группу для службы: достаточно будет видеть состояние всей группы как нормальное, чтобы быть уверенным в работе служб DNS на всех компьютерах. Так можно упростить администрирование и настройки мониторинга.

Из общих конфигурационных настроек отметим еще и параметры операторов — тех людей, кому программа будет отправлять сообщения в случае возникновения тех или иных событий. В Nagios индивидуальных операторов также можно объединять в группы и настраивать отправку сообщений определенного типа в конкретной группе специалистов. Также можно настраивать периоды времени. Их можно использовать для применения, например, различных типов контроля в рабочие и выходные дни, для разных способов оповещения администраторов (например, днем по электронной почте, а ночью — на пейджер) и т. д.

Оповещения могут эскалироваться: в случае появления повторяющихся событий оповещение может быть послано по иерархии следующему специалисту.

Структура конфигурационных файлов *Nagios*

Список стандартных файлов конфигурации Nagios приведен в табл. 7.1.

Таблица 7.1. *Список конфигурационных файлов Nagios*

Имя файла	**Назначение**
nagios.cfg	Файл основных настроек конфигурации. Содержит имя и адрес администратора *Nagios*, 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 Web-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*

Описание команд *Nagios*

Команды Nagios описываются в файле `commands.cfg` (путь по умолчанию /usr/local/nagios/etc/object/commands.cfg).

На практике в файле `commands.cfg` обычно необходимо указать расположение исполняемого файла, его название, которое будет использовано в Nagios, и параметры

строки запуска. По умолчанию в файле конфигурации установленной системы уже содержатся некоторые описания типовых команд проверки (проверки пингом — check_ping, проверки http-сервера — check_http и многие другие). По этим образцам легко можно создать собственные команды проверки, хотя обычно используют готовые разработки, которые, практически для любого варианта контроля, можно легко найти в Сети. Далее приведен пример описания простейшей команды — проверки достижимости хоста при помощи команды ping:

```
define command{
   command_name   check-host-alive
   command_line   $USER1$/check_ping -H $HOSTADDRESS$ -w $ARG1$ -c
$ARG2$ -p 5
   }
```

Это описание создает команду с именем check-host-alive, в качестве исполняемого файла используется команда check_ping из установленных утилит Nagios. Символы, заключенные в знаки доллара, указывают используемые переменные. В терминах Nagios это макросы (macros), которые заменяются значениями в момент выполнения. Поскольку обычно мы привыкли к другому определению макросов, в этой книге будем называть эти названия *переменными*. $HOSTADDRESS$ 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) или ошибки (c). Как правило, можно указывать абсолютные или относительные значения (или все вместе: в типовой конфигурации, например, параметр w указывается как 3000.0,80%). Последний ключ (-p) указывает, что команда ping должна послать пять проверочных пакетов.

Службы *Nagios*

Службы обычно описываются в файлах конфигурации отдельно для каждого типа контролируемых систем (в общую конфигурацию Nagios такие файлы импортируются директивами cgf_file=... в файле nagios.cfg). Построение файлов конфигураций начинается с описания шаблонов, за которыми следуют описания хостов и потом описания служб.

В описании службы уже можно не повторять общие значения из шаблонов, поэтому типовое определение службы может выглядеть примерно так:

```
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 качест-

ве 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 "`!`").

Обычно для контроля однотипных устройств можно использовать одинаковую команду. В этом случае в описании службы достаточно перечислить все такие устройства через запятую:

```
define service{
     use              generic-service
     host_name        3ComSwitch1,3ComSwitch2,3ComSwitchXM,DES_3550
     service_description   PING
     check_command    check_ping!200.0,20%!600.0,60%
     ...
        }
```

Для служб можно определять зависимости (*dependencies*). Делается это для того, чтобы скрыть "лишние" предупреждения. Например, если часть систем находится в локальной сети после маршрутизатора, то можно определить зависимость их от этого устройства. Понятно, что если этот маршрутизатор выйдет из строя, то и все устройства, находящиеся за ним, окажутся недоступными. Настройка зависимости позволит в случае его аварии скрыть предупреждения о недоступности зависимых устройств пока не восстановится работа коммутатора и не выполнять на них проверку состояния соответствующих служб.

Описание контролируемых систем в *Nagios*

Для удобства различные типы контролируемых систем принято описывать в различных конфигурационных файлах. Перечень типовых используемых файлов конфигураций приведен в usr/local/nagios/etc/nagios.cfg, причем часть файлов закомментирована. Так, если потребуется контролировать коммутаторы в сети, то раскомментируйте строку `#cfg_file=/usr/local/nagios/etc/objects/switch.cfg` и т. д.

Само описание хоста (оно будет содержаться в файле windows.cfg, или switch.cfg, или printer.cfg и т. д.) минимально может выглядеть в этом случае следующим образом:

```
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 включать два параметра, которые будут определять действия, выполняемые в случае возникновения сбоев в работе системы:

```
     event_handler          server-reboot
     check_command          check-host-alive
```

Nagios будет выполнять команду проверки `check-host-alive` и, как только будет обнаружена смена состояния хоста, начнется выполнение программы server-reboot. Таким способом можно, например, запускать остановившиеся службы на контролируемых серверах, перезагружать системы и т. п.

Для удобства анализа хосты можно объединять в группы. Для этого необходимо описать группу в файле конфигурации следующим образом:

```
define hostgroup{
        hostgroup_name имя_группы
        alias          полное имя группы ; допускаются пробелы и т. д.
        }
```

Так же, как и для служб, для хостов можно описывать зависимости одних систем от других.

Описание временных параметров

Временные параметры используются в различных конфигурациях: в описаниях хостов (период, когда нужно осуществлять мониторинг, и период, когда нужно отправлять сообщения), служб и контактов (периоды, когда можно отправлять сообщения по хостам и по службам). Синтаксис определения нового периода легко понятен по примерам, включенным в файл /usr/local/nagios/etc/objects/timeperiods.cfg.

Необходимо в описании дать название шаблону и перечислить построчно диапазоны времени, которые в него включаются. Причем можно использовать 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 использовать директиву `exclude` с последующим перечислением периодов времени (через запятую).

Использование встроенных в *Nagios* команд контроля

При стандартной установке Nagios и плагинов в нем присутствует ряд команд (плагинов), которые можно использовать для контроля систем. Список их приведен в табл. 7.2.

Таблица 7.2. *Список плагинов Nagios*

Утилита	Назначение
check_apt	Контроль обновлений систем Linux, осуществляемых 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

Таблица 7.2 *(продолжение)*

Утилита	Назначение
check_clamd	Проверка соединения *CLAMD* (антивирусная программа) с удаленным хостом
check_cluster	Проверка состояния хостов в кластере Linux
check_dhcp	Проверка доступности DHCP-серверов в сети
check_dig	Проверка работы DNS-службы на хосте (используется команда `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 использованием 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 с использованием протокола SNMP)
check_http	Проверка http-соединений с удаленной системой. Проверка может осуществляться как по протоколу HTTP, так и по протоколу 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 S.M.A.R.T.-технологии
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	То же 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

Таблица 7.2 *(продолжение)*

Утилита	Назначение
check_mailq	Проверка числа сообщений в очереди почтового сервера (работает с различными версиями sendmail, qmail)
check_mrtg	Проверяет заданную переменную в логе MRTG (Multi Router Traffic Grapher) на минимальное/максимальное значения (для контроля параметров производительности необходимо использовать *check_mrtgtraf*)
check_mrtgtraf	Проверяет значения исходящего и входящего трафика 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	Проверка NNTP-соединения 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 использовать *check_ntp_peer*
check_ntp_peer	Проверка NTP-сервера. Позволяет оценивать, в том числе, дрожание (jitter) сигнала времени
check_ntp_time	Этот плагин проверяет разницу времени между локальным сервером и указываемым удаленным серверов времени
check_nwstat	Используется 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	Проверка удаленных хостов 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), валидность сертификатов
check_smtp	Проверяет SMTP-подключение к серверу. Ответ почтового сервера может анализироваться на наличие заданных строк. Также контролируется время отклика

Таблица 7.2 *(окончание)*

Утилита	Назначение
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), валидность 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, наличие 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, наличие 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 *UPSD daemon* (**http://www.networkupstools.org**)
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`).

Для того чтобы задействовать плагин для мониторинга систем, в Nagios должна быть описана использующая его команда. В файле commands.cfg приведено несколько наиболее часто употребляемых примеров контроля систем. При практическом использовании Nagios этот файл должен быть расширен за счет ваших собственных команд контроля.

Мониторинг серверов Windows в *Nagios*

Для мониторинга систем на основе Windows разработано несколько различных агентов. Наиболее часто используемыми из них являются 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 использование агента NSClient++, являющегося, на взгляд автора, наиболее популярным из упомянутого списка.

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-битных платформ следует использовать различные версии

агента. Если вы загрузили архив, то его необходимо распаковать в желаемую папку и установить службу Windows командой

```
NSClient++ -install
```

Удобнее воспользоваться msi-файлом, поскольку в этом случае мастер установка сразу внесет в конфигурацию агента часть настроек по результатам ваших ответов (рис. 7.15).

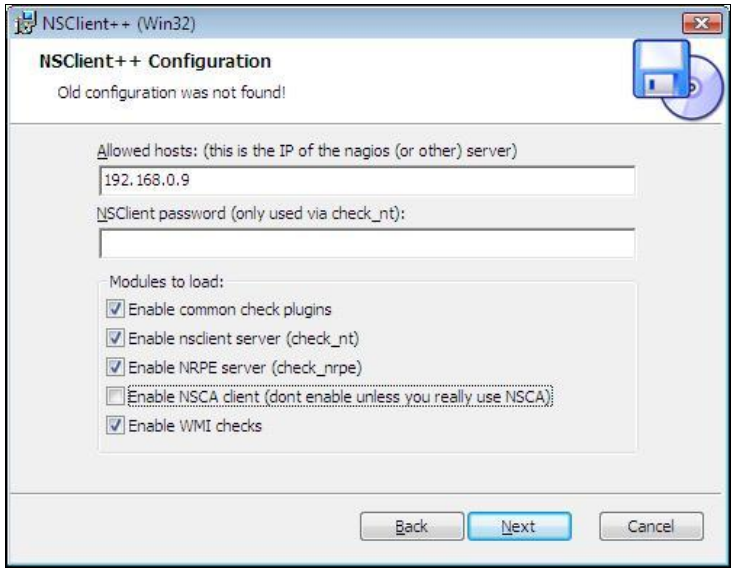


Рис. 7.15. Настройка параметров программы *NSClient++*. Настройки пользователя, введенные на этапе установки, будут сохранены программой в файле конфигурации

После установки необходимо разрешить взаимодействие службы с рабочим столом, для чего следует открыть свойства службы (**Панель управления** | **Администрирование** | **Службы** | найти службу **NSClientpp...** (полное название зависит от версии) и открыть ее свойства) и включить опцию **Разрешить взаимодействие с рабочим столом**.

Перед запуском службы следует ***обязательно*** проверить 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 следует 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.

Обратите внимание на возможность запуска агента в диагностическом режиме. При этом вы сможете как увидеть потенциальные ошибки в конфигурационном файле, так и отладить собственные запросы (рис. 7.16).

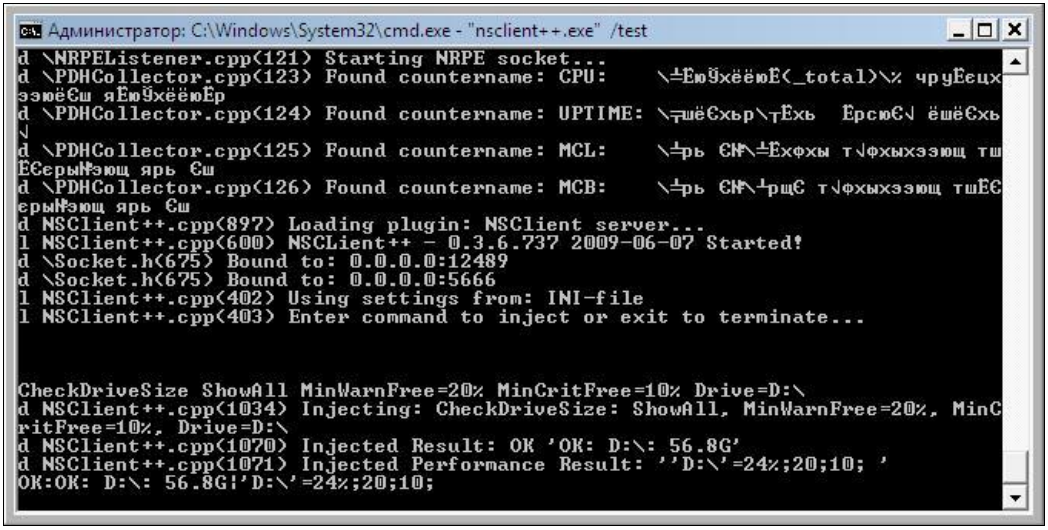


Рис. 7.16. Окно программы *NSClient++* в диагностическом режиме

Для запуска NSClient++ в диагностическом режиме достаточно в командной строке набрать

```
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. 7.16 показано окно отладки плагина, в котором введена команда `CheckDriveSize ShowAll MinWarnFree=20% MinCritFree=10% Drive=D:\` и виден ответ системы.

Плагин NSClient++ позволяет контролировать параметры, приведенные в табл. 7.3. Подробности использования подробно описаны в технической документации (**http://trac.nakednuns.org/nscp/wiki/CheckCommands**) и по имеющимся примерам легко составить собственные команды контроля состояния Windows.

Таблица 7.3. *Параметры Windows, 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)

Таблица 7.3 *(окончание)*

Параметр	Описание
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. Поскольку таких сообщения обычно много, использование данного контроля сильно загружает систему
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 надо 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 — в целях 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). Используются в процессах настройки и отладки системы

Перечисленным списком не ограничиваются возможности контроля Windows-систем. Вы можете добавить контролируемые параметры, например, за счет использования внешних сценариев.

Мониторинг систем Windows может осуществляться на основе различных протоколов. Наиболее часто используемыми являются протоколы NSClient и NRPE (для "пассивного" мониторинга можно использовать также протокол NSCA, о котором более подробно можно прочесть в онлайновой документации). На практике можно использовать любой из них, необходимо только включить/выключить соответствующие модули в файле настроек клиента (nsc.ini). В то же время, на взгляд автора,

протокол NRPE несколько более гибок в использовании и обеспечивает шифрование данных обмена.

При использовании протокола NRPE синтаксис команд строится следующим образом:

```
check_nrpe ... -c <команда> -a <аргументы>
```

Например, проверка доступной физической памяти может быть осуществлена так:

```
check_nrpe -H 192.168.0.9 -c CheckMem -a MaxWarn=70% MaxCrit=>80% type=physical
```

Мониторинг Windows-систем на основе WMI

В состав NSClient++ входит модуль CheckWMI.dll, позволяющий контролировать Windows-систему с использованием инструментария WMI.

Модуль CheckWMI фактически состоит из двух подмодулей: CheckWMIValue и CheckWMI. Модуль CheckWMIValue оптимизирован для контроля численных значений. Например, текущей загруженности процессора (это число процентов загрузки) или разрешения монитора (число 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 здесь команда составлена для использования 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 использования 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`, используемую 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**.

Модуль CheckWMI нужно использовать 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 использования фильтров. Синтаксис CheckWMI описан на странице **http://nsclient.org/nscp/wiki/CheckWMI/CheckWMI**. По своему построению запросы CheckWMI сходны с фильтрами, используемыми для анализа журналов работы системы.

Мониторинг серверов Linux в *Nagios*

Контроль работы серверов Linux осуществляется с использованием плагина NRPE, причем на сервере Nagios он должен быть установлен как плагин, а на контролируемой системе Linux — в качестве демона. Для установки может быть использована как подготовленная версия, так и исходные коды плагина.

Кроме стандартного комплекта администратор может использовать при мониторинге любой из доступных плагинов, которые широко представлены в Интернете.

Используя протокол NRPE, можно на контролируемом хосте вызвать команду `check_nrpe` для проверки другого хоста. Таким способом можно контролировать некоторую подсеть через один компьютер. При такой организации контроля на хосте, используемом в качестве прокси, обязательно должны быть установлены как демон протокола NRPE, так и плагин.

Мониторинг систем с использованием протокола SNMP

Для работы по протоколу SNMP в Nagios должен быть установлен соответствующий плагин. Он включен в состав плагинов Nagios, но воспользоваться им можно только в том случае, если предварительно был установлен пакет net-snmp. Поэтому, если предполагается использование SNMP-модуля, данный пакет необходимо загрузить с сервера **http://net-snmp.sourceforge.net/**, после чего заново перекомпилировать плагины и повторно установить их. Автор рекомендовал бы при новой установке сначала выполнить команду `make clean`, которая очистила бы настройки предыдущей инсталляции.

> ***Примечание***
>
> На сайте **http://net-snmp.sourceforge.net/** необходимый пакет представлен только в исходных кодах или в RPM-формате.

После настройки возможности контроля по протоколу SNMP необходимо протестировать[1] 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 |
```

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 состояния (ключи `-w` и `-c`) или диапазон значений (через двоеточие). Обратите внимание, что если вы

[1] В примерах использован протокол SNMP версии 1. В реальных условиях обычно используется протокол версии 3, поэтому примеры необходимо дополнить параметрами аутентификации.

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, то результат будет считаться нормальным состоянием, а если не попадает — то как предупреждение или критическое (в зависимости от использованного 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
```

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.

В Сети можно найти достаточное число примеров настройки Nagios для контроля устройств с использованием протокола SNMP, которые можно применить на практике. 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.).

Мониторинг коммутационного оборудования

Активное оборудование сети — коммутаторы, концентраторы, модемы и т. п. контролируются по протоколу SNMP (управляемые модели). Можно получать состояния портов оборудования, выдавать предупреждения в случае возникновения на портах некоторого числа ошибок передачи пакетов, наблюдать за температурой устройства и количеством VPN-сессий. Достаточно только выбрать соответствующие идентификаторы по описанию для мониторинга по протоколу SNMP. В большинстве случаев этого достаточно для контроля.

Однако, кроме указанных параметров, администраторы часто хотят знать реальную загрузку оборудования, процент использования пропускной способности. Эти значения нельзя получить, запрашивая тот или иной параметр состояния оборудования. Они вычисляются на основе анализа периодически получаемых данных. Специально для такого мониторинга создана одна из самых популярных программ — MRTG. Ее возможности обработки параметров коммутаторов используются в Nagios.

Программа MRTG по протоколу SNMP с активного оборудования собирает статистику, которая при помощи плагина check_mrtgtraf впоследствии передается в Nagios для отображения.

После установки программы MRTG необходимо создать файлы настроек, в которых указать устройства и значения параметров, которые программа будет собирать. Эти настройки должны быть приведены в файле /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 мы потом просто импортируем в файл настроек. В качестве имени такого файла удобно использовать имя (или адрес) опрашиваемого устройства:

```
cfgmaker community@адрес > /etc/mrtg/адрес.cfg
```

По итогам работы команды `cfgmaker` достаточно только оставить в файле конфигурации те блоки данных, которые предполагается анализировать для данного 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 установке пакета MRTG в системе настраивается автоматический сбор информации с коммутаторов один раз в течение пяти минут. При желании этот период можно увеличить, если соответствующим образом отредактировать файл /etc/cron.d/mrtg.

Графики производительности по отдельным портам устройств можно просмотреть, если открыть в обозревателе папку **http://nagiosserver/mrtg/** и выбрать соответствующий файл. При желании можно сформировать общий индексный файл для упрощения отображения. Делается это с помощью команды `indexmaker`. Необходимые ключи для формирования файла легко уточнить по справочной информации после вызова `indexmaker -h`.

Вслед за описанной настройкой можно использовать команды Nagios `check_mrtg` и `check_mrtgtraf` для сбора данных производительности. 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` указываются пары лимитов для исходящего и входящего трафика

по данному порту. По какому порту система будет контролировать данные, определяется выбранным файлом журнала.

На рис. 7.17 приведен пример графика, формируемого пакетом mrtg.

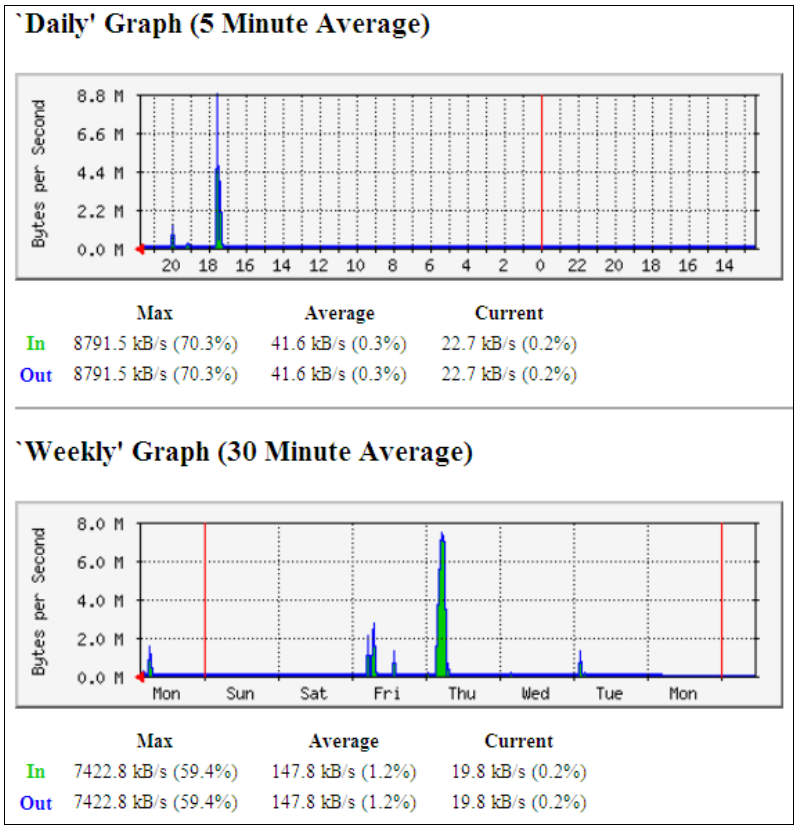


Рис. 7.17. График загрузки порта коммутатора

Использование собственных программ мониторинга

Nagios позволяет легко создать собственные плагины для мониторинга любой системы. В качестве таковых могут быть использованы любые исполняемые файлы. Необходимо только обеспечить, чтобы они сообщали код завершения работы в соответствии с табл. 7.4.

При создании сценариев необходимо учитывать, что запускаться они будут от имени службы агента мониторинга. По умолчанию эта служба имеет максимальные права для локальной системы, но не может взаимодействовать с компьютерами сети. Если вы предполагаете использовать сценарии для сбора данных с других компьютеров, то необходимо либо предусматривать в сценариях операции подключения с указанием параметров соответствующей учетной записи, либо настроить агент для запуска от другого имени.

Таблица 7.4. *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)

Построение графиков в *Nagios*

Команды Nagios, при помощи которых контролируются системы, возвращают не только состояние (хорошо или плохо), но и данные по конкретным параметрам (например, процент использования диска или число вошедших в систему пользователей). Эти данные по умолчанию не сохраняются, но могут быть использованы, например, для прорисовки графиков соответствующих служб.

Для реализации такой возможности необходимо установить дополнительный плагин. Одним из наиболее популярных плагинов для создания графиков в Nagios является пакет nagiosgraph, доступный к загрузке с сайта **http://sourceforge.net/projects/nagiosgraph/**.

На рис. 7.18 представлен пример страницы контроля состояния служб, на которой при подведении курсора мыши к соответствующему параметру динамически ото-

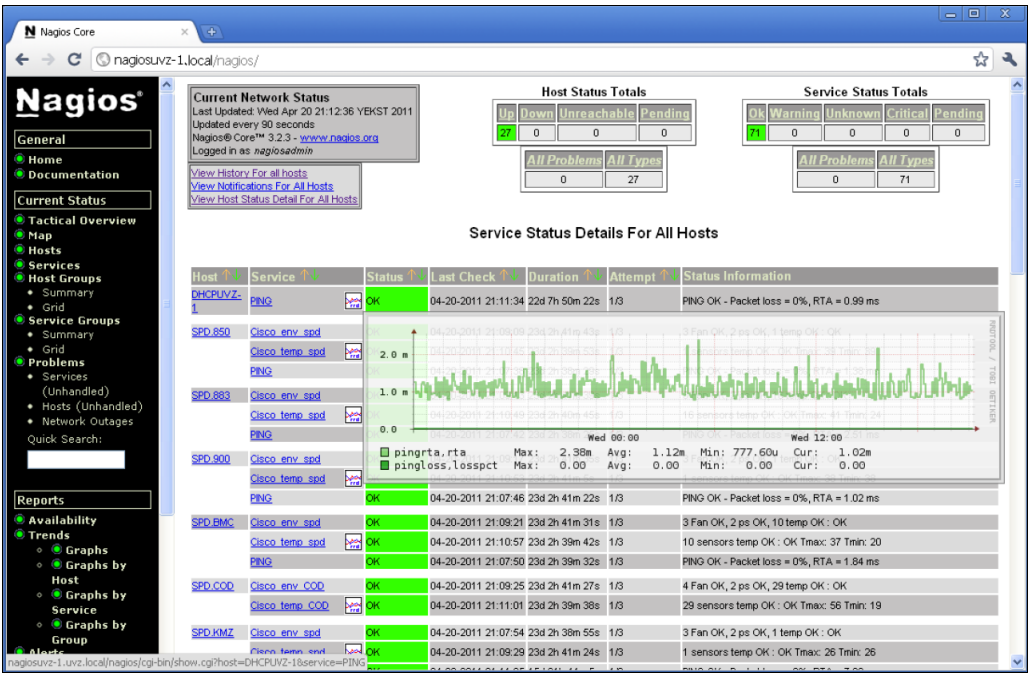


Рис. 7.18. Пример страницы с динамическим графиком

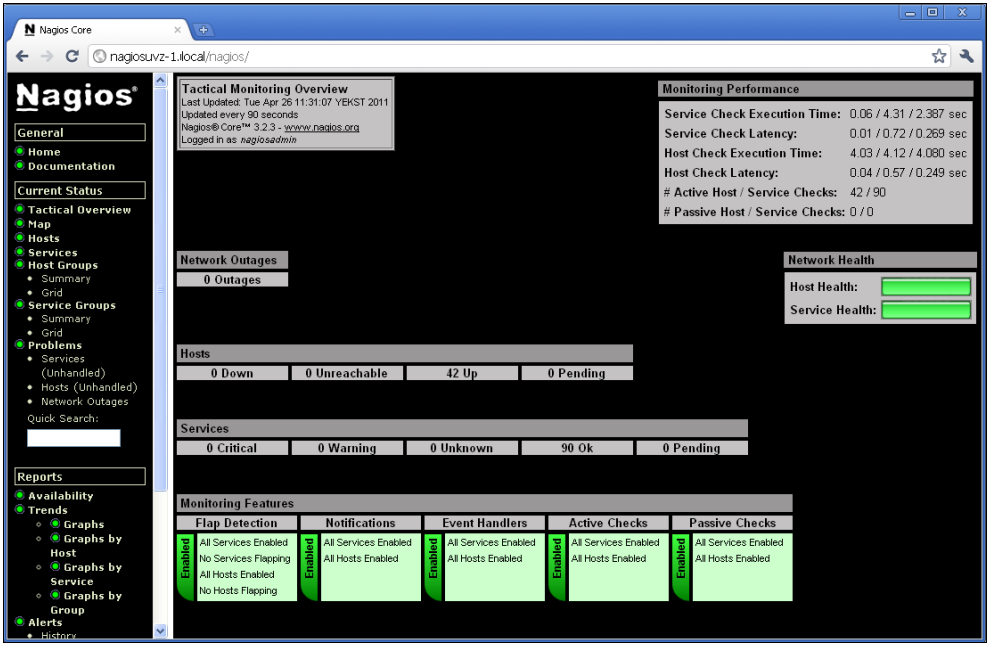


Рис. 7.19. Стандартный вариант отображения суммарного состояния системы в *Nagios*

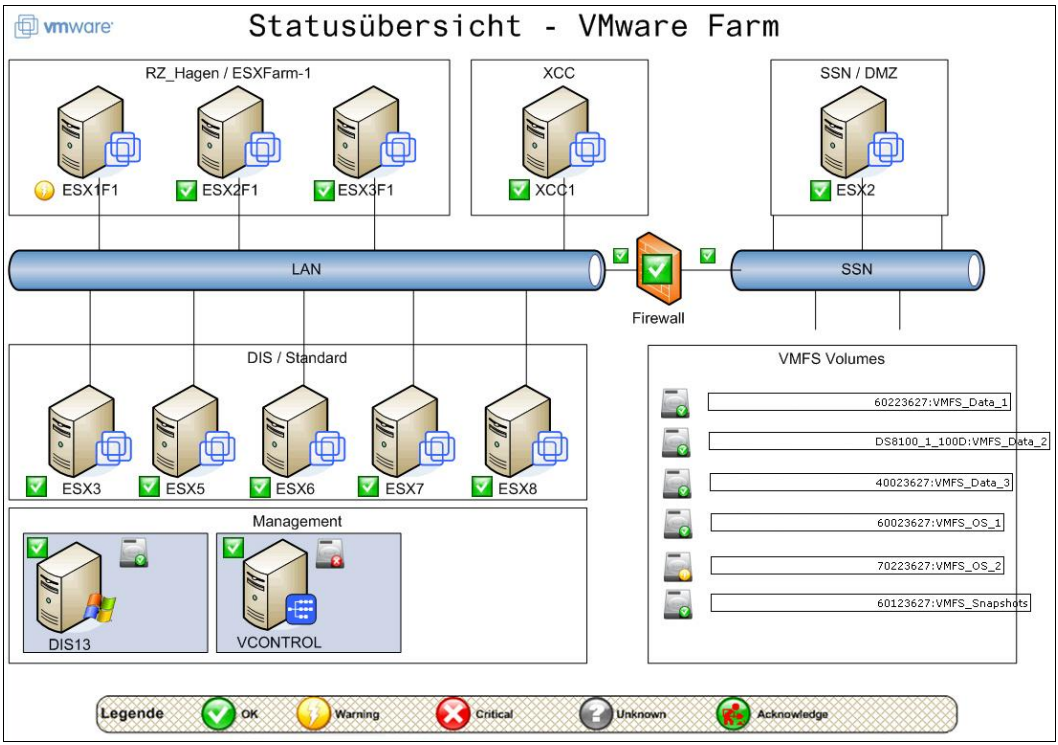


Рис. 7.20. Отображение состояния сети при использовании пакета *NagVis*

бражается график его изменения. При желании администратор может перейти к выбору графика по любой службе и за заданный период времени.

Настройка интерфейса *Nagios*

Для Nagios разработано много дополнений, которые позволяют настроить отображение данных мониторинга в соответствии с потребностями администратора. Так, вместо тактического обзора (рис. 7.19) можно использовать настраиваемые карты сети, на которых Nagios будет отображать состояние каждого устройства.

На рис. 7.20 (пример с сайта **http://www.nagvis.org**) приведен реальный вариант карты мониторинга, построенной при помощи пакета NagVis.

В этом случае Nagios в реальном режиме времени будет отображать индикаторы по устройствам и линиям связи. При этом на карте возможно отображать суммарные состояния по группам (хостов и служб), значения фактического трафика по линиям связи и т. п. Понятно, что такие представления очень удобны при практическом использовании.

ГЛАВА 8

Виртуализация

Термин *виртуализация* в последнее время стал очень популярным. Виртуальные решения в той или иной степени применяются в подавляющем большинстве информационных систем. Специалисты используют их в целях тестирования, для размещения дополнительных задач на существующем оборудовании, для обучения и т. п. Виртуализируют серверы, рабочие станции, системы хранения, сетевую инфраструктуру...

Экономические аспекты виртуализации

Прежде чем приступать к внедрению виртуальных систем, следует тщательно продумать, что мы хотим получить в результате и сколько это будет стоить. Несмотря на то, что практически в каждой презентации мы слышим об экономической эффективности технологии, на практике внедрение виртуализации сопровождается затратами, причем достаточно внушительными.

Во-первых, виртуализация требует наличия инфраструктуры, например, системы хранения данных, подключенной к нескольким серверам. Во-вторых, программное обеспечение, позволяющее использовать преимущества виртуальных сред: мигрировать виртуальные машины с одного физического сервера на другой в реальном режиме времени, балансировать нагрузку на физических серверах, выключая неиспользуемое оборудование и т. п., — является коммерческим и сравнительно недешевым продуктом. В результате экономический эффект перехода в виртуальные среды достигается, начиная с некоторого числа серверов. Если вам и не требуется сразу установить 10 новых серверов, то покупать новое оборудование придется сразу и в расчете на размещение всех будущих систем.

Эффективность управления комплексом виртуальных машин в наших условиях редко можно оценить в цифрах, поскольку штатных изменений среди ИТ-специалистов предприятия (например, сокращения числа системных администраторов) после внедрений решений по виртуализации не происходит, а расходы на электроснабжение серверных предприятия обычно не учитываются отдельной строкой.

В итоге внедрение виртуализации часто приводит только к дополнительным затратам на содержание ИТ-инфраструктуры.

Основные термины

Гипервизором (hypervisor) называют программное обеспечение, обеспечивающее виртуализацию ресурсов и позволяющее нескольким операционным системам работать одновременно на одном физическом устройстве, которое принято называть *хост-системой* или просто *хостом*. Название гипервизор сохранилось исторически, более понятным, на взгляд автора, был бы термин *"менеджер виртуальных машин"*.

Операционную систему, работающую под управлением гипервизора, принято называть *гостевой* операционной системой.

Жесткие диски гостевых операционных систем являются файлами на уровне гипервизора. Их принято называть *виртуальными жесткими дисками*. Соответственно сетевые адаптеры, память в гостевых системах называют *виртуальными адаптерами*, *виртуальной памятью* и т. д.

На уровне гипервизора можно создать различные *виртуальные сети*: с подключением к реальному сетевому адаптеру в режиме моста, в режиме трансляции сетевых адресов, сегмент сети без доступа к реальным адаптерам (внутренняя сеть) и т. п. Коммерческие решения виртуализации включают в себя виртуальные коммутаторы, которые вы можете настроить на необходимые правила пересылки и фильтрации пакетов из одной сети в другую.

Как правило, разработчики гипервизоров подготавливают специальные пакеты обновления, оптимизирующие работу гостевых операционных систем. Например, в гостевые ОС добавляются сетевые адаптеры, работающие на скорости внутренней шины гипервизора. При этом появляется возможность обмениваться данными между гостевыми ОС через буфер памяти, подключать папки хоста в качестве сетевых папок в гостевые ОС и т. д. Такое ПО принято называть *расширениями* виртуальных машин (virtual machine additions). Если нет специальных требований, то для повышения производительности систем расширения должны быть установлены в гостевой ОС (обычно команды установки расширений присутствуют в меню окна виртуальной машины).

> ***Примечание***
>
> Расширения для гипервизора Microsoft, предназначенные для установки в некоторых Linux-системах (они называются Linux Integration Services/Components for Hyper-V), следует дополнительно загрузить со страниц
> **http://www.microsoft.com/download/en/details.aspx?id=26837** и
> **http://www.microsoft.com/download/en/details.aspx?id=11674**.

Захватом курсора мыши (клавиатуры) называют передачу контроля над соответствующими устройствами виртуальной машине. В этом случае, например, курсор мыши будет работать только в пределах окна виртуальной машины. Чтобы "пере-

двинуть" курсор за пределы гостевой ОС, его необходимо освободить, нажав специальную клавишу. Обычно такой клавишей является правая клавиша <Crtl>.

VDI (Virtual Desktop Infrastructure, инфраструктура виртуальных рабочих столов) — так называют ПО, позволяющее управлять большим количеством виртуальных рабочих станций. Особенности данной технологии описаны *далее в разд. "Виртуальные рабочие станции"*.

Разработчики виртуальных решений

Существует несколько технологий виртуализации, разработанных различными вендорами. Мы приведем только краткий список наиболее активно, на взгляд автора, используемых на практике решений по виртуализации. Желающие получить дополнительную информацию могут обратиться к свободной онлайн-энциклопедии "Википедия"

(**http://en.wikipedia.org/wiki/Comparison_of_platform_virtual_machines**).

Лидером рынка виртуализации сегодня являются продукты компании VMware (**www.vmware.com**). Решения от VMware обеспечивают виртуализацию практически всей линейки операционных систем (Windows, Linux, Apple Macintosh и т. д.), ПО компании тесно интегрировано с аппаратными возможностями многих платформ, реализованы технологии отказоустойчивых решений и т. п. Линейка ПО представлена как свободно распространяемыми (гипервизор ESXi), так и коммерческими продуктами.

XEN (**www.xensource.com**, **www.virtualiron.com**, **http://www.xen.org/**) представляет собой гипервизор на основе открытого кода, ставший предшественником многих открытых решений.

На базе этого гипервизора компанией Citrix созданы серверы XenServer, которые также являются бесплатными решениями. Правда, ПО централизованного управления серверами XenServer является коммерческим продуктом.

Компанией Sun (ныне Oracle) выпущена виртуальная машина VirtualBox. Это решение бесплатно и может быть загружено с сайта Oracle (**http://www.oracle.com/us/technologies/virtualization/index.html**). У компании Oracle есть и решение по VDI — Oracle Virtual Desktop Infrastructure (VDI), причем в варианте до 10 виртуальных рабочих столов оно может бесплатно тестироваться в течение неограниченного времени.

В составе серверных операционных систем Windows 2008 присутствует гипервизор — HyperV, который может быть загружен с сайта Microsoft и в качестве отдельного продукта и может быть использован полностью бесплатно.

Продукты открытого кода в последнее время активно начинают использовать решение по виртуализации с названием KVM (например, этот гипервизор включен в состав Ubuntu, RedHat и т. д.). Гипервизор KVM реализует виртуализацию на Linux-системах и доступен как в составе соответствующих дистрибутивов, так и через пакеты установки.

Распределение ресурсов в *nix

В *nix-системах решения по распределению ресурсов между приложениями, по изоляции процессов давно используются в производственных системах. Сегодня одной из популярных операционных систем, предназначенных для применения в производственных условиях, является Oracle Solaris. Она может быть установлена на компьютеры *x*86 или RISC-архитектуры и включает в себя специальную технологию — создание *зон*, позволяющую тонко настраивать выделение ресурсов под различные задачи, обеспечивая полную изоляцию процессов.

На рис. 8.1 (из документации Oracle) показан пример структуры сервера, в котором ресурсы распределены между несколькими зонами. Причем в одной зоне выделены фиксированные ресурсы, а другие — динамически распределяют остальные ресурсы системы между собой.

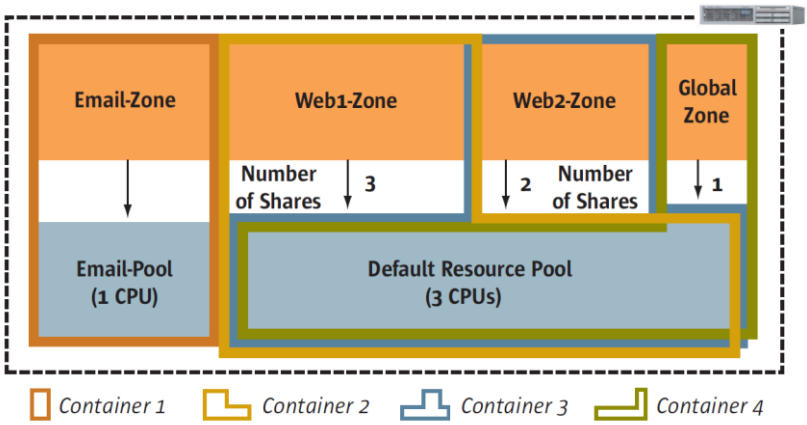


Рис. 8.1. Пример разбиения Solaris-сервера на зоны

Особенности выбора ПО гипервизора

Идеального решения по виртуализации на сегодня не существует. Выбор технологии будет зависеть от многих факторов. Во-первых, от поддержки оборудованием технологий виртуализации. Аппаратная виртуализация позволяет гостевой ОС работать с ресурсами "железа" напрямик, без эмуляции, причем объем данного функционала зависит от выбранного ПО гипервизора. Технологии аппаратной поддержки постоянно дорабатываются, поэтому необходимые требования следует уточнять по описаниям программ гипервизора. При этом некоторые гипервизоры требуют в качестве обязательного условия наличия аппаратной виртуализации (например, XenServer). Часть гипервизоров может быть установлена только на *x*64-платформы (XenServer, Hyper-V) и т. д.

Во-вторых, у многих гипервизоров существуют ограничения по типам гостевых ОС. Так, Hyper-V поддерживает весьма ограниченный список Linux-подобных ОС. И если вы хотите работать с виртуальными Linux, то лучше остановить свой выбор

на XenServer, KVM или Oracle VM. А для виртуализации MacOS — установить сервер VMware.

В третьих, гипервизоры имеют ограничения по максимальному числу поддерживаемых виртуальных процессоров, по объему памяти, по числу одновременно запускаемых гостевых систем, типам устройств хранения и т. п. Хотя, если смотреть с практической точки зрения, разница в максимально поддерживаемом числе нод кластера в 16 или 32 единицы для большинства случаев значения не имеет.

Сегодня наиболее популярными гипервизорами являются решения от компании VMware (VMware vSphere, это коммерческие решения, на рис. 8.2 показан пример логической организации сети с использованием решений vSphere), Microsoft (бесплатный Hyper-V R2, прежде всего для гостевых операционных систем Windows), KVM (open-source-решение, включается в поставку современных Linux-дистрибутивов).

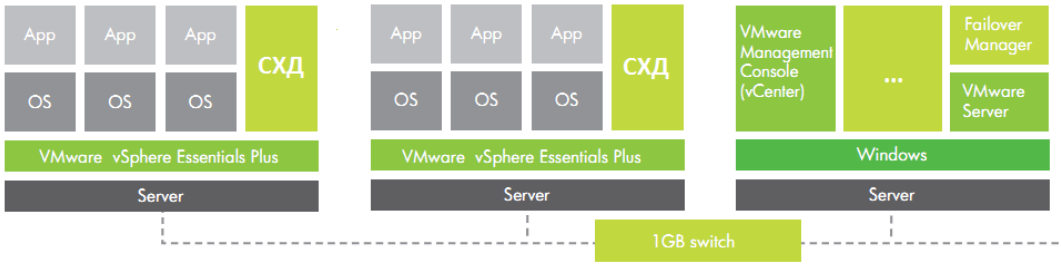


Рис. 8.2. Вариант логической структуры решения на продуктах компании VMware

Если рассматривать решения виртуализации для рабочих станций, то автор предпочитает решения Oracle VirtualBox: данное ПО позволяет тестировать все основные ОС, не предъявляет особых требований к хостовому компьютеру и не создает на нем излишней нагрузки.

Гипервизоры бывают двух типов: первый устанавливается непосредственно на компьютер и не требует наличия операционной системы (ESX, XenServer и др.), второй — интегрируется в существующую ОС (Oracle VirtualBox, KVM, Hyper-V). На практике оба типа демонстрируют примерно одинаковые параметры, так что выбор ПО более зависит от предпочтений администратора.

Какое ПО можно использовать в виртуальной среде

Виртуальная машина, естественно, отличается от реальной системы. Поэтому возможны случаи, когда использовать виртуальную машину для запуска определенных приложений невозможно.

При возникновении проблем с использованием программного обеспечения в виртуальной среде можно порекомендовать обратиться к онлайновой документации по соответствующим продуктам. Что касается решений от Microsoft, то в документе

KB897614 отмечается, что с Microsoft Virtual Server несовместимы следующие продукты самого изготовителя: Microsoft Speech Server, Microsoft ISA Server 2000/2004, Microsoft SharePoint Portal Server, Microsoft Identity Lifecycle Manager 2007, Microsoft Identity Integration Server 2003, Microsoft Identity Integration Feature Pack. Часть продуктов (см. документ KB897613) поддерживается только после установки определенного пакета обновлений: Microsoft Certificate Services, Microsoft Exchange Server, Microsoft Systems Management Server и т. д.

Особенности сетевых подключений виртуальных машин

Хостовая машина имеет один или несколько сетевых интерфейсов, подключенных к реальной сети передачи данных. Число же сетевых интерфейсов, которые могут быть созданы для виртуальной машины, может быть произвольно: и больше, и меньше реальных сетевых адаптеров. При этом программное обеспечение гипервизоров позволяет настроить для виртуальных машин несколько сетей.

Вариант *трансляции сетевых адресов* создает сервер NAT, внешним интерфейсом которого служит реальный сетевой адаптер, а интерфейсы виртуальных машин будут подключены к виртуальному интерфейсу, настройками которого (IP-адресом) можно управлять в ПО гипервизора. Обычно при этом включается сервер DHCP, так что сетевые интерфейсы виртуальных машин могут получить все параметры настройки автоматически. Виртуальным машинам будет доступна работа в реальной сети (через адрес хостовой системы), но "достучаться" извне до виртуальной машины будет весьма затруднительно: как известно, сервер NAT является и сетевых экраном, а настроить публикацию внутренних ресурсов в ПО гипервизора не является тривиальной задачей.

Если виртуальные машины должны работать с внешней сетью и наоборот, то для такого случая необходимо выбирать вариант *сетевого моста*. Сетевой мост предполагает, что пакеты, формируемые интерфейсом виртуальной машины, будут передаваться реальным физическим интерфейсом. Как будто все интерфейсы — физические и виртуальные — подключены в один коммутатор. Вы можете присвоить виртуальным интерфейсам любые сетевые настройки; взаимодействие систем будет происходить по стандартам IP-сетей.

Если сетевой трафик необходим только между виртуальными машинами, то гипервизоры позволят создавать *внутренние сети*. Внутренних сетей может быть несколько, отличаются они по тем именам, которые им присваиваются (новое имя — новая сеть). Передача данных возможна только внутри соответствующей внутренней сети. Таким способом можно существенно повысить безопасность сетевой инфраструктуры виртуальных машин (принципиально исключить видимость данных на внешнем, физическом интерфейсе).

Подключения можно комбинировать в зависимости от потребностей. Например, одним интерфейсом подключиться к реальной сети в режиме мост, а другой включить во внутреннюю сеть.

К одному физическому интерфейсу можно подключить любое количество виртуальных интерфейсов. Практическое ограничение связано только с параметрами сетевой активности виртуальных систем: суммарные потребности виртуальных интерфейсов не должны превышать возможностей реального сетевого адаптера.

Последние версии ПО виртуализации включают в себя и виртуальные коммутаторы, реализованные программным способом. Эти коммутаторы по своим возможностям идентичны "обычным" коммутаторам 2 и 3 уровней.

> ***Примечание***
>
> Сегодня эти решения доступны уже не только для коммерческих решений (VMware), но и для ПО открытого кода. Например, виртуальный коммутатор может быть добавлен в *Oracle VirtualBox*, хотя пока данный компонент реализован только в Linux-хостовой системе (подробности установки виртуального коммутатора и его настроек доступны в онлайновой справке продукта).

Лицензирование программного обеспечения виртуальных машин

При лицензировании программного обеспечения, используемого на виртуальных машинах, возникает много сложностей, особенно с лицензиями от Microsoft, применение которых не очевидно и в обычных условиях. Эта книга не посвящена вопросам практики лицензирования ПО, поэтому конкретные разъяснения необходимо уточнять на сайте разработчика (например, **http://www.microsoft.com/licensing/highlights/virtualization.mspx**).

Главное, что необходимо отметить — использование виртуальных сред не всегда требует приобретения дополнительных лицензий (см., например, документ Microsoft "Licensing Microsoft Server Products in Virtual Environments" (**http://download.microsoft.com/download/F/C/A/FCAB58A9-CCAD-4E0A-A673-88A5EE74E2CC/Licensing_Microsoft_Server_Products_Virtual_Environments.docx**). Так, лицензия на Windows Server Enterprise Edition позволяет в один момент времени иметь один работающий физический сервер и 4 виртуальных. А лицензия на SQL Server (в варианте Server/CAL) Workgroup Edition, Standard Edition and Enterprise Edition разрешает запускать любое количество инстанций на сервере. Таких примеров можно привести много, лучше всего особенности лицензирования уточнять по документам изготовителя ПО.

> ***Примечание***
>
> Обратите внимание, что формально миграция физического сервера в виртуальную среду (как описано ниже) не разрешена OEM-лицензией (если мигрируемый сервер или рабочая станция приобретены вместе с ПО — с OEM-лицензией).

Создание виртуальных машин

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 или дискет 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.

> ***Примечание***
>
> До установки расширений *Hyper-V* в виртуальной машине недоступно управление мышью. Чтобы облегчить управление с клавиатуры, целесообразно переключить виртуальную машину в полноэкранный режим.
>
> Если в качестве виртуальной ОС используется Linux с графической средой управления, то расширения необходимо переустановить, если после обновления ОС перестанет масштабироваться окно гостевой системы.

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. Для клонирования сначала создается виртуальная машина, на нее устанавливается необходимый набор программного обеспечения и результат используется в качестве шаблона при генерации новых гостевых систем.

Клонирование можно сделать вручную, если скопировать файл виртуального жесткого диска и при создании новой системы указать на использование уже существующего диска.

Главная сложность при этом — необходимость изменения *всех* уникальных параметров для клонированной операционной системы. Так, следует сменить в гостевой ОС сетевое имя на уникальное и настроить новые параметры сетевых интерфейсов. Кроме указанных очевидных настроек необходимо сменить и другие уникальные характеристики, присущие системам. Например, уникальный идентификатор безопасности для ОС Windows. Существует утилита NewSID (**http://technet.microsoft.com/ru-ru/sysinternals/bb897418**), позволяющая установить новый идентификатор безопасности 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.

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.

Если в ПО вендора присутствуют мастера операций, позволяющие подготовить ОС к клонированию (или переносу на другое оборудование), то рекомендуется не пренебрегать ими. В случае ОС Windows единственным поддерживаемым вариантом подготовки системы к клонированию является использование программы SysPrep. Данная утилита поставляется на установочном диске операционной системы. При ее запуске система переводится на последний этап установки — к моменту определения PnP-устройств. После копирования жесткого диска такой системы при первом запуске происходит завершение этапа установки, от пользователя запрашиваются новое имя компьютера и другие уникальные параметры. При этом сохраняются установленные программы, личные документы и т. п. Подробное описание использования SysPrep поставляется вместе с утилитой.

Снятие образа физического сервера

При внедрении виртуализации 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**).

После того как образ диска будет сформирован, останется только создать новую виртуальную машину и указать, что она использует существующий файл виртуального диска. Естественно, что необходимо будет выполнить и настройку подключения сетевого интерфейса в параметрах виртуальной машины.

> ***Примечание***
>
> Если в качестве хостовой ОС используется Windows 7, а для виртуализации применяется Microsoft Virtual PC, то клонированные виртуальные ОС запустятся только при наличии в оборудовании аппаратной виртуализации. Однако вендором выпущено обновление, которое позволяет запустить виртуальную машину и без аппаратной поддержки — см. **http://support.microsoft.com/kb/977206/**.

Миграция между решениями различных вендоров

На практике часто бывает необходимо подключить виртуальную машину, подготовленную в ПО одного вендора, к гипервизору другого разработчика. Например, протестировать 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.

Некоторые замечания к параметрам виртуальных машин

Жесткие диски

Во-первых, к виртуальной машине может быть подключено несколько жестких дисков. Во-вторых, сами жесткие диски могут быть различных типов.

Типы виртуальных дисков

Для рабочей среды должен использоваться преимущественно фиксированный жесткий диск, а динамические и разностные диски могут применяться в тестовых и тому подобных целях.

Толстый (*Thick*) или *фиксированный жесткий диск*. При создании файла такого виртуального диска под него выделяется сразу весь объем. Данный тип диска рекомендуется выбирать в случае повышенных требований к производительности операций ввода-вывода (ресурсы системы не затрачиваются на изменение размера файла).

Тонкий (*Thin*) или *динамический жесткий диск*. Файл виртуального диска создается минимального размера и затем автоматически увеличивается до заранее оговоренного максимального размера (при необходимости). Чтобы уменьшить размер файла тонкого диска (если часть дискового пространства в виртуальной машине освободилась по тем или иным причинам), нужно остановить виртуальную машину и выполнить операцию сжатия файла.

Разностные жесткие диски. Разностные диски могут использовать виртуальные машины Microsoft. На разностный диск пишутся только измененные данные по сравнению с некоторым образцом — *родительским* диском (родительский диск рекомендуется использовать в режиме *только для чтения*). Использование разностных дисков позволяет сэкономить дисковое пространство в случае создания нескольких подобных виртуальных машин (за счет исключения дублирования одинаковых данных).

> ***Примечание***
>
> Формат VHD стандартизован для файлов виртуальных дисков. Но на практике вендоры часто используют собственные форматы (например, VMware — vmdk).

Сквозное подключение физического диска (*pass-through*). Гипервизоры позволяют подключить физический жесткий диск к виртуальной машине. Теоретически это самый быстрый вариант диска для виртуальной машины, хотя на практике различия в скорости между фиксированным диском и диском, подключенным напрямую, достаточно незначительны.

> ***Примечание***
>
> Для того чтобы подключить жесткий диск напрямую к виртуальной машине, он должен быть предварительно отключен от хостовой системы. Сделать это можно, например, с помощью менеджера дисков (или утилитой *diskpart*).

RAW-диски. Описанные ранее тонкие, толстые и разностные диски представляют собой файлы, хранимые на хостовой системе. Некоторые гипервизоры могут использовать непосредственный доступ к жесткому диску. Например, в VMware присутствует механизм прямого доступа клиента vSphere Client к устройствам хранения FC или iSCSI. Соответствующие описания необходимо уточнить по документации продукта.

Необходимость блочного доступа к виртуальному диску

Файл виртуального жесткого диска может быть создан на устройстве, понимаемом системой как *локальный* жесткий диск. Это могут быть диски, как подключаемые локально, так и по технологии FC или iSCSI.

> ***Примечание***
>
> Существует еще технология передачи FC поверх сети Ethernet (FCoE), но она поддерживается сегодня только топовыми моделями коммутаторов и систем хранения и представляет в рамках этой книги более академический, чем практический интерес.

Некоторые коммерческие гипервизоры (например, ESX) позволяют работать и с устройствами, подключаемыми по сети (NAS/NFS), но это, скорее, исключение, чем правило.

Варианты подключения виртуального диска

В виртуальной машине жесткий диск можно подключить к IDE, так и SCSI-контроллеру. Часто рекомендуется для повышения производительности предпочтительнее выбирать SCSI-вариант, хотя практической разницы этих вариантов не наблюдается.

Обслуживание файлов виртуального диска

Файлы виртуальных дисков можно преобразовывать из одного типа в другой, дефрагментировать, сжимать (уменьшать в размере за счет исключения неиспользуемых участков). Для выполнения этих операций виртуальную машину необходимо предварительно выключить.

Учитывая существенные размеры файлов, данные операции следует заблаговременно планировать, поскольку выполняться они будут весьма длительное время.

Сохранение состояния виртуальной машины

Программы управления виртуальными машинами позволяют создавать *снимки* жестких дисков. Снимок является мгновенной копией текущего состояния системы и позволяет в случае необходимости восстановить виртуальную машину на этот момент времени.

Обычно снимки используются в целях тестирования: создается копия рабочей виртуальной машины, после чего на нее, например, устанавливаются обновления программного обеспечения и проверяется правильность функционирования. В случае отсутствия ошибок на копии можно провести обновление и основной производственной системы.

Распределение вычислительных ресурсов

Виртуальная машина запускается как еще один процесс основной операционной системы. Несколько запущенных виртуальных машин будут делить между собой процессор(ы) хостовой системы.

ПО гипервизора обычно позволяет при создании виртуальной машины выделить ей один или несколько виртуальных процессоров. Не рекомендуется выделять виртуальной машине больше виртуальных процессоров, чем их установлено в хостовой системе. Если нет каких-либо особых причин лучше предоставить виртуальной машине такое количество виртуальных процессоров, сколько физических процессоров (ядер) установлено в хостовой системе.

Администратор имеет возможность регулировать выделяемые каждой виртуальной машине вычислительные ресурсы, хотя и в ограниченных пределах: устанавливать относительные веса каждой виртуальной машины, гарантировать предоставление виртуальной машине некоторого минимального времени процессора и т. п. Эти настройки выполняются в ПО соответствующего гипервизора.

> ***Примечание***
>
> Процессоры с поддержкой технологии hyper-threading отображаются в операционной системе как два процессора. Данная технология позволяет несколько повысить общую производительность системы, но в случае создания виртуальных машин очень часто она *ухудшает* производительность, особенно при высокой загрузке процессора. Поэтому отключите поддержку технологии hyper-threading в BIOS компьютера, который предполагается использовать для размещения виртуальных машин.

Оперативная память

Обычно именно память является ограничителем количества одновременно запускаемых на одном компьютере виртуальных машин. Для каждой виртуальной машины необходимо выделить в ее настройках некий объем памяти. Если на момент запуска виртуальной машины требуемого объема памяти не окажется, то ее старт не состоится. В этом случае можно, во-первых, попытаться уменьшить объем выделенной памяти до допустимого предела, во-вторых, закрыть приложения основного компьютера, чтобы высвободить используемую ими оперативную память.

Совет

После неудачной — из-за отсутствия свободной памяти — попытки запуска виртуальной машины можно через некоторое время повторить процедуру. Достаточно часто операционная система в этом случае высвобождает занимаемую память, сохраняя данные в файле подкачки, и появляется возможность запуска виртуального компьютера.

Выделение излишней памяти виртуальным машинам, использование виртуальной памяти приводит к увеличению количества операций чтения/записи на жесткий диск, что сказывается на производительности как основной системы, так и виртуальных.

Сервисные операции

Резервное копирование и антивирусная защита

Виртуальные машины так же, как и "обычные" системы, нуждаются в резервном копировании, защите от вирусов и т. п. Эти действия могут проводиться так же, как и обычно: например, путем установки агента резервного копирования в операционную систему виртуальной машины с последующей настройкой операций.

Однако, учитывая возможность доступа к виртуальным машинам из среды гипервизора, в этих целях разработаны специальные программные решения. Для антивирусной защиты достаточно установить программное обеспечение только в гипервизор. Аналогично, резервное копирование можно выполнить без установки агентов в виртуальную машину. Подобные коммерческие решения предлагаются в настоящее время многими вендорами. Однако при их выборе следует предварительно проанализировать возможности такого ПО: для каких гостевых систем реализованы такие функции, с какими гипервизорами совместимы, дешевле ли такое решение или придется идти на дополнительные расходы и т. п.

Обмен данными

Примечание

Описываемые далее операции копирования доступны только после установки расширений виртуальной машины в гостевой операционной системе.

Копирование данных с хоста

Виртуальные машины поддерживают копирование данных методом "drag and drop". Однако копировать данные можно только из виртуальной машины на основную или наоборот. Если вам необходимо скопировать данные между несколькими виртуальными машинами, их следует сначала скопировать, например, на рабочий стол основного компьютера, и только потом — в другую виртуальную машину.

Общие папки

Часто необходимо обеспечить в виртуальной машине доступ к информации хостовой системы, например, для установки ПО, дистрибутив которого расположен на

диске сервера. Для этого на хостовой системе можно предоставить в общий доступ любые папки.

Папки, предоставленные в общий доступ средствами гипервизора, подключаются так же, как и сетевые папки. Отличия только в том, что общие папки могут быть созданы и без сетевого адаптера.

Настройка общих папок выполняется в консоли управления гипервизора. Достаточно указать предоставляемую в общий доступ папку и настроить режим доступа (полный или только для чтения). Подключение к общей папке в виртуальной среде происходит так же, как и подключение к общему ресурсу сети (рис. 8.3).

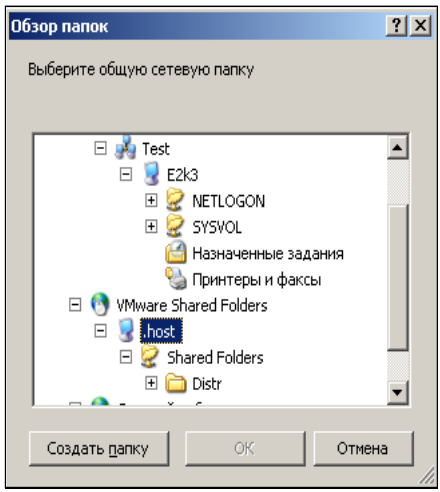


Рис. 8.3. Подключение папки хоста к гостевой машине для совместного использования

Миграция виртуальных машин

> ***Примечание***
>
> Для того чтобы перенести виртуальную машину с одного гипервизора на другой, файл ее виртуального жесткого диска должен быть доступен как одному, так и другому серверу. Иными словами необходимо использовать внешнюю систему хранения данных. Кроме того, с рабочего места, с которого осуществляется управление процессом миграции, должны быть доступны для администрирования оба гипервизора.

В этом разделе мы поговорим о переносе виртуальной машины с одного гипервизора (сервера) на другой. Сразу оговоримся, что такая миграция не является средством обеспечения непрерывной работы системы. Это, скорее всего, один из вариантов обслуживания, при котором необходимо планово перенести вычисления на другой сервер. Например, при обслуживании сервера (проведении планово-профилактических работ, связанных с его выключением) или переносом на более мощную вычислительную платформу.

Подобная миграция присутствует в большинстве гипервизоров. Реализуется она в консолях управления, причем наиболее просто — в коммерческих решениях (типа EMC vSphere или Microsoft System Center Virtual Machine Manager). Однако адми-

нистратор может осуществить перенос виртуальных машин и при помощи простейших сценариев. Например, в руководстве по миграции Hyper-V (**http://technet.microsoft.com/ru-ru/library/ee849855%28WS.10%29.aspx**) пошагово описан весь процесс подготовки и переноса виртуальных машин.

Правильно подготовленная миграция позволяет практически не прерывать обслуживание. Например, при миграции Hyper-V обычно происходит только потеря пары пакетов ping во время такого переноса. Однако подобный перенос может не привести к успеху в случае высокой вычислительной нагрузки (большого изменения данных в оперативной памяти сервера). Кроме того, следует учесть, что часть параметров после завершения миграции должна быть вновь настроена вручную (подключения iso-образов, параметры администрирования и т. п.).

Особо нужно отметить, что для успешности процесса лучше всего предусматривать *идентичные* конфигурации аппаратной и программной составляющих серверов: одинаковые модели процессоров, одинаковое их число, одинаковые версии операционной системы и т. д. и т. п. Постепенно число ограничений по идентичности параметров сервера-источника и сервера-назначения с выходом новых версий ПО гипервизиров уменьшается. Но в любом случае, планируя процессы миграции, необходимо свериться с описанием поддерживаемых конфигураций в документации применяемого гипервизора.

Подключения к виртуальным машинам

> ***Примечание***
>
> Рекомендуется использовать управление виртуальной машиной только по защищенным каналам связи (SSL, Secure Sockets Layer), как при работе на административной странице, так и через консоль управления (VMRC, Virtual Machine Remote Control). Этот совет особенно актуален при переключении на стандартный режим идентификации, поскольку в этом случае имена пользователей и их пароли доступа будут пересылаться по сети в *открытом* виде.

Средствами управления гипервизора можно подключиться к рабочему столу виртуальной машины. Обычно консоль гипервизора легко можно поставить на станции администратора и управлять с ее помощью виртуальными машинами. Администраторы сразу же включают на виртуальных машинах опцию доступа к рабочему столу; в таком варианте доступны все функции управления, кроме включения питания виртуальной машины.

Если виртуальная машина[1] размещена за межсетевым экраном, то следует открыть на нем порты 5900 (порт по умолчанию для управления), 1024 (порт по умолчанию для открытия страницы администрирования на веб-сервере), порты 137 и 138 для TCP и UDP (используются при аутентификации).

Существуют некоторые особенности посылки специальных сочетаний клавиш. Так, вместо сочетания <Ctrl>+<Alt>+<Del> в консоли управления обычно используется <Ctrl>+<Alt>+<Ins>. Хотя обычно данную команду вызывают из меню управления.

[1] Описываемые ниже примеры относятся к MS Virtual PC.

Переключение между режимами отображения виртуальной машины в окне и в полном экране осуществляется после нажатия сочетания клавиш: правой клавиши <Alt>+<Enter>.

До установки расширений при щелчке мышью внутри окна виртуальной машины курсор мыши начинает перемещаться *только* в пределах виртуальной машины. Чтобы "освободить" курсор от какого захвата, по умолчанию используется правая клавиша <Alt>.

Особенности выключения виртуальных машин

Существует несколько возможностей выключения виртуальной машины. Во-первых, можно завершить работу выключив виртуальную машину с сохранением данных при помощи ее внутренней команды **Завершить работу**. Во-вторых, можно сохранить состояние виртуальной машины из консоли управления гипервизора. В этом случае ее работа как бы заморозится; после восстановления вы сможете продолжить операции. Такой способ напоминает переход в режим "сна" (hybernate). В-третьих, можно просто "выключить" питание виртуальной машины, выполнив команду `turn off`. При последующем запуске возможна потеря несохраненной информации.

Если на вашем компьютере размещено несколько виртуальных машин, причем часть из них настроена на автоматический запуск при включении питания, то при выключении хостовой системы осуществляется сохранение состояния виртуальных машин. Этот процесс может существенно затянуться, если система будет сохранять много информации. В результате основная операционная система воспримет такую ситуацию как зависание прикладной программы с отсутствием ответа в течение заданного промежутка времени. Виртуальная машина будет аварийно завершена, что может вызвать проблемы при ее следующей загрузке. Чтобы зарезервировать время на сохранение параметров виртуальных машин в случае перезагрузки хостовой системы, измените значение параметра реестра `WaitToKillServiceTimeout` в ветви `HKLM\SYSTEM\CurrentControlSet\Control\`, установив необходимое время ожидания.

Виртуальные рабочие станции

Развитие технологий виртуализации позволило применить эти решения не только для серверов, но и для пользовательских рабочих станций (так называемые, desktop-решения). Технологии виртуализации рабочих станций получили названия VDI (*Virtual Desktop Interface*).

Сравниваем с терминальными клиентами

VDI-решения во-многом напоминают терминальные подключения пользователей. Поэтому следующие основные преимущества терминалов свойственны и виртуальным рабочим столам:

- VDI-решения существенно снижают затраты на администрирование, поскольку вместо нескольких десятков рабочих станций работать приходится с несколькими серверами;
- конфигурации систем унифицированы, любые обновления выполняются быстрее и проще и т. п.;
- сокращаются суммарные затраты на электроэнергию, оборудование используется более эффективно;
- все данные обрабатываются на сервере, и их легко защитить как для случая работы внутри локального сегмента, так и при доступе из публичной сети.

Так же, как и у терминальных клиентов, у пользователей виртуальных рабочих столов могут возникнуть следующие сложности:

- невозможность использования функций аппаратных ускорителей (обработки графики на современных видеокартах, модулей аппаратного шифрования и т. п.);
- проблемы с использованием USB-устройств (например, видеокамеры, сканеры, смарткарты и т. п.). Лучше использовать принтеры, имеющие сетевой (Ethernet) порт подключения.

При этом у пользователей виртуальных рабочих столов есть, на взгляд автора, только одно, но весьма существенное преимущество. Каждый пользователь получает собственный виртуальный компьютер, который может быть настроен только для него и при этом совершенно не будет мешать другим сотрудникам. На виртуальный компьютер можно поставить любое необходимое программное обеспечение, что практически было нереализуемо в условиях жестких настроек терминального сервера.

Немного об экономике VDI

Как и в любом ИТ-проекте, желательно сначала оценить, сколько будет стоить внедряемое решение и какую экономию (или убыток) оно принесет. Для сравнения приведем параметры, на которые ориентируются западные менеджеры и результаты расчета по которым приводятся на наших семинарах.

Таблица 8.1. *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$
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)

Таблица 8.1 *(окончание)*

Параметр	Эффект	Примечание
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.

Как видно из таблицы, экономия от внедрения решений VDI может быть только за счет разницы в стоимости рабочих станций и затрат на их обслуживание (электропитание, 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**).

Структура VDI-решений

VDI-решения объединяют различные элементы ИТ-структуры предприятия (рис. 8.4). Из службы каталогов берется информация о пользователях и группах. Например, некоторой группе пользователей можно поставить в соответствие определенный шаблон виртуального рабочего стола; в результате новому пользователю будет автоматически предоставляться конфигурация компьютера в соответствие с его функциональными обязанностями.

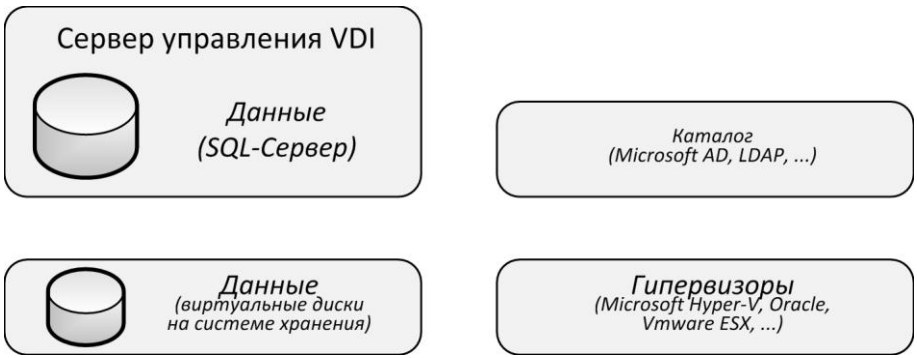


Рис. 8.4. Логическая структура VDI-решения

Программное обеспечение VDI может управлять (обеспечивать подключение) к виртуальным рабочим столам различных гипервизоров или к сессиям терминальных серверов.

Поскольку VDI-решения обслуживают большое количество рабочих столов, то они должны быть весьма надежными. Поэтому в производственной среде должны реа-

лизовываться отказоустойчивые решения: наряду с основным сервером управления следует предусматривать резервные (один или несколько), нужно установить несколько серверов, на которых будут запускаться виртуальные рабочие столы, выбрать надежную систему хранения, построить резервированную сеть передачи данных (рис. 8.5).

Рис. 8.5. Вариант аппаратной реализации VDI-решения

Некоторые особенности VDI-решений

VDI-решения обычно настраиваются на автоматическое создание виртуальных рабочих столов. Для этого администратором предварительно создаются шаблоны различной конфигурации, которые ставятся в соответствие группам пользователей из службы каталогов предприятия. При попытке подключения нового пользователя ПО предоставляет ему виртуальный рабочий стол, сформированный по соответствующему шаблону (для повышения производительности по шаблонам предварительно создается некоторое количество рабочих столов, которые находятся в неактивном состоянии). После отключения пользователя в зависимости от настроек виртуальная машина может сохраняться или уничтожаться для высвобождения ресурсов.

Поскольку однотипные конфигурации содержат значительное количество одинаковой информации на дисках и в памяти системы, то ПО VDI позволяет настроить совместное использование таких ресурсов.

Для подключения к VDI на рабочие места устанавливается клиентское ПО. При этом подключение к различным конфигурациям (различным виртуальным рабочим столам или терминальным сессиям) осуществляется через одну точку. Если пользователю разрешено подключение к нескольким рабочим столам/конфигурациям, то право соответствующего выбора предоставляется на экране подключения к VDI.

Производительность виртуальных систем

Анализ производительности виртуальных систем имеет некоторые особенности. Связано это с тем, что администратору необходимо учитывать две группы счетчиков: счетчики производительности гостевой системы и счетчики хостовой системы.

Счетчики производительности гостевой системы доступны в операционной системе виртуальной машины и позволяют найти узкие места самой виртуальной машины. Счетчики хостовой системы показывают, достаточно ли ресурсов оборудования для обеспечения работы всех установленных виртуальных машин. Чтобы исключить "бутылочные горлышки", необходимо чтобы показатели счетчиков производительности были в оптимальных границах как для гостевой, так и хостовой системы.

> ***Совет***
>
> Если какое-либо значение счетчика хостовой системы находится в критическом диапазоне, то необходимо проанализировать аналогичные счетчики в гостевых системах, найти виртуальные машины, имеющие максимальную загрузку по этому параметру, и попытаться оптимизировать для них загрузку.

В остальном рекомендации по оптимизации параметров систем не отличаются от описанных в *главе 11*.

Советы по оптимизации виртуальных систем

Следующие советы помогут улучшить показатели работы систем:

- если есть аппаратные требования к системе, которую предполагается реализовать в виртуальной среде, то для хостовой системы в этом случае нужно выбирать оборудование примерно на 20% более производительное, чем рекомендовано. Это относится, например, к числу процессоров, их частоте, объему оперативной памяти и т. п.;
- не забывайте, что оперативная память нужна и операционной системе гипервизора. Так, для Microsoft Hyper-V нужно 300 Майт памяти. На первый гигабайт оперативной памяти каждой виртуальной машины нужно 32 Мбайта и на последующие — по 8 Мбайт. Если на хостовой системе установлен Windows, то это еще 512 Мбайт. Эти значения описывают невыгружаемую память ядра. В результате на хостовой системе должно быть на 500—1000 Мбайт оперативной памяти больше, чем сумма значений оперативной памяти каждой виртуальной машины;
- оптимально, если одному виртуальному процессору будет соответствовать один физический (это снизит затраты на переключение ресурсов). При этом следует учитывать максимальные значения числа используемых процессоров в гостевых системах: 2 для ОС Windows XP/Vista/Windows 2003, 4 для Windows 2008);
- на гостевые машины устанавливайте преимущественно 64-разрядные операционные системы;

- используйте для размещения файлов виртуальных дисков быстрые RAID-массивы;
- вместо динамически расширяемых виртуальных дисков используйте диски фиксированного размера. Часто рекомендуют использовать SCSI-адаптеры гипервизора для монтирования виртуальных дисков. Связано это с тем, что данные адаптеры доступны *только* после установки гостевых расширений виртуальных машин. Тем самым гарантируется оптимальность конфигурации гипервизора. Если производительность диска является критическим параметром для виртуальной машины, то используйте прямое подключение жесткого диска;
- отключите поддержку технологии hyper-threading в BIOS хостового компьютера;
- отключите в хостовой системе все неиспользуемые роли (службы). Применяйте для гостевых систем "усеченные" версии операционных систем;
- обязательно устанавливайте расширения для виртуальных машин, в том числе и для хостовой операционной системы (если она установлена);
- периодически дефрагментируйте виртуальные диски средствами установленных на них операционных систем, после чего выполняйте дефрагментацию файла виртуального диска средствами программы управления;
- не включайте на виртуальных машинах различные визуальные эффекты, 3D-эффекты и т. п;
- используйте несколько сетевых адаптеров: один для доступа к хостовой системе, другие разделите между всеми виртуальными машинами. Используйте в виртуальных машинах сетевые адаптеры, устанавливаемые гостевыми расширениями вместо традиционных (отображаются в окне гипервизора с названием **Устаревший...**).

Некоторые дополнительные источники технической поддержки

Администраторы, использующие в своей работе решения на гипервизоре Microsoft, могут найти ответы на некоторые вопросы дополнительно в следующих источниках:

- сайте Hyper-V Server 2008 R2 — **http://www.microsoft.com/en-us/server-cloud/hyper-v-server/default.aspx**;
- сайте Datacenter Virtualization & Management — **http://www.microsoft.com/en-us/server-cloud/datacenter/virtualization.aspx**;
- Virtualization Support — **http://technet.microsoft.com/en-us/virtualization/cc150661.aspx**;
- в сетевом файле FAQ по гипервизору Hyper-V — **http://social.technet.microsoft.com/Forums/ru/virtualizationru/thread/df4caa03-5c31-40df-b407-75a1b645b583**.

Виртуализация в сетях передачи данных

Виртуализация давно используется в компьютерных технологиях. Одной из таких областей ее применения являются сети передачи данных.

Виртуальные частные сети

Технология виртуальных частных сетей — Virtual Local Area Network, VLAN — позволяет логически обособить участок физической сети. VLAN представляет собой логически (программно, иными словами, виртуально) обособленный сегмент основной сети. Пакеты данных пересылаются *только* в пределах одной VLAN. Одна VLAN может объединять порты нескольких коммутаторов (VLAN с одинаковым номером на разных коммутаторах считаются одной и той же VLAN). Устройства, подключенные к разным VLAN, не могут обмениваться пакетами напрямик, они *не видят* друг друга.

Целями создания VLAN является снижение количества широковещательного трафика и изоляция участков сети с информацией ограниченного пользования. Считается, что в "плоской" сети, т. е. в сети без VLAN, не должно работать примерно более 100 компьютеров.

VLAN можно создать *только* на управляемых устройствах; самые дешевые модели (часто их называют *офисными*) такую возможность не поддерживают.

Варианты создания VLAN

На практике существует несколько технологий создания VLAN. В простейшем случае VLAN создается путем ручного объединения нескольких портов коммутатора (port based VLAN или *группировка портов*). При этом одно физическое устройство логически разбивается на несколько: для каждой VLAN создается "отдельный" коммутатор. Очевидно, что число портов такого коммутатора можно легко изменить: достаточно добавить или исключить из VLAN соответствующий физический порт.

Второй часто используемый способ заключается в отнесении устройства к той или иной VLAN на основе MAC-адреса. Например, так можно обосабливать камеры видеонаблюдения, IP-телефоны и т. п. Этим способом вычленяется голосовой трафик (трафик VoIP — по маске MAC-адресов, выданных производителям оборудования для телефонии). При этом способе устройство не привязано к конкретному порту: его трафик будет помещаться в соответствующую виртуальную сеть при подключении к любому настроенному так порту.

Третий способ заключается в объединении устройств в сеть VLAN по сетевым протоколам. Например, можно "отделить" протокол IPX от IP, "поместить" их в разные VLAN и направить по различным путям.

Четвертый способ создания VLAN состоит в группировке многоадресных пакетов (так, например, можно создать VLAN для видеовещания и т. п.).

VLAN открывают практически безграничные возможности для конфигурирования сетевой инфраструктуры, соответствующей требованиям конкретной организации. Один и тот же порт коммутатора может принадлежать одновременно нескольким виртуальным сетям, порты различных коммутаторов — быть включенными в одну VLAN и т. п.

На рис. 8.6 показан пример построения VLAN из компьютеров, подключенных к различным коммутаторам. Обратите внимание, что при использовании агрегированных каналов (на рисунке для связи устройств Switch 2 и Switch 3) в состав VLAN на каждом коммутаторе должны включаться именно *агрегированные порты* (обычно получают названия AL1, AL2 и т. д.).

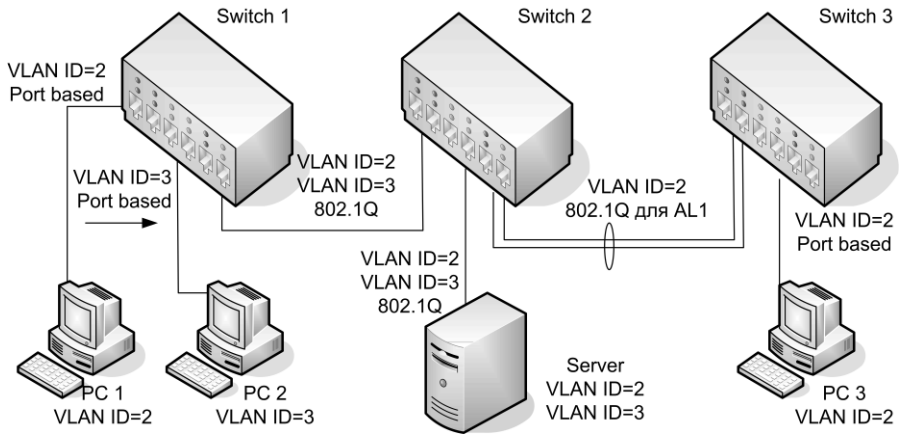


Рис. 8.6. Пример построения VLAN на нескольких коммутаторах. Поскольку предполагается, что сервер подключается к нескольким VLAN и серверный сетевой адаптер поддерживает создание tagged VLAN, то в этом случае используется настройка серверного порта коммутатора по стандарту 802.1q. Для реализации возможности передачи данных VLAN между коммутаторами соответствующие порты, подключенные к связующей линии, в режиме 802.1q настраиваются на членство в тех виртуальных сетях, данные которых должны передаваться через эту линию связи. Для простоты VLAN по умолчанию (ID = 1) не отображена

Теги 802.1q

В соответствии со стандартом 802.1q номер VLAN передается в специальном поле кадра Ethernet, которое носит название **TAG**. Поэтому пакеты, содержащие такое поле, стали называть *тегированными* (tagged), а пакеты без этого поля — *нетегированными* (untagged). Поле **TAG** включает в себя данные QoS (поэтому все пакеты, содержащие информацию о качестве обслуживания, являются тегированными) и номер VLAN, на который отведено 12 бит. Таким образом, максимально возможное число VLAN составляет 4096.

Сетевые адаптеры рабочих станций обычно не поддерживают теги, поэтому порты коммутаторов уровня доступа настраиваются в варианте untagged. Для того чтобы через один порт (обычно это магистральные порты или порты соединения двух коммутаторов) можно было передать пакеты *нескольких* VLAN, он включается в соответствующие VLAN в режиме tagged. Коммутатор будет анализировать поля

TAG принятых пакетов и пересылать данные только в ту VLAN, номер которой содержится в поле. Таким образом через один порт можно безопасно передавать информацию нескольких VLAN.

VLAN 1

При создании VLAN следует учитывать тот факт, что служебная сетевая информация пересылается нетегированными пакетами. Для правильной работы сети администратору необходимо обеспечить передачу таких пакетов по всем направлениям. Достаточно большое число моделей коммутаторов передают такие пакеты только по VLAN с номером 1 и не позволяют сменить эту настройку. В таком случае в целях безопасности все порты компьютеров, по которым передаются данные, необходимо перевести в VLAN с другими номерами, чтобы исключить несанкционированное подключение к коммутатору.

Маршрутизация в сетях предприятий

Информация внутри локальной сети, которая определяется IP-адресом и маской подсети, пересылается от одного компьютера к другому: отправитель посылает пакет непосредственно на физический адрес получателя. Если отправитель и получатель данных находятся в различных сетях, например, в VLAN с различными номерами, то они не могут переслать пакеты друг другу.

Передать данные между двумя сетями может специальное устройство — *маршрутизатор*. Маршрутизатор обычно подключен к нескольким сетям и на нем созданы правила, определяющие, куда пересылать данные.

В локальных сетях обычно существует только одна точка подключения к другим сетям: если это совсем небольшая организация, то такой точкой является устройство доступа в Интернет, для организаций с построенными VLAN таких точек может быть несколько (например, для отказоустойчивости).

В локальной сети правила пересылки данных поэтому крайне просты: информация для внешней сети должна пересылаться на одно устройство (его называют *шлюзом по умолчанию*), которое передает ее во внешнюю сеть.

Чтобы передать данные из одной VLAN в другую, нужно порту коммутатора, подключенного в эту VLAN, присвоить IP-адрес (говорят *присвоить IP-адрес интерфейсу VLAN*) и настроить правила коммутации. Эти действия называют *настройкой маршрутизации*.

Обычно маршрутизация выполняется средствами активного оборудования сети передачи данных. Коммутаторы, которые умеют передавать пакеты из одной сети в другую, называют *коммутаторами уровня 3 (см. разд. "Модель OSI" в главе 3)*. Коммутаторы уровня 2 могут только разбить сеть на несколько VLAN; передать же данные из одной VLAN в другую они не могут.

Функцию маршрутизации могут выполнить программным образом как серверы, так и рабочие станции Windows. Для включения маршрутизации в ОС Windows XP требуется ручная настройка параметров реестра. Это допустимо в небольших сетях,

но требует установки дополнительных сетевых адаптеров и соответствующей настройки программного обеспечения. Обычно функцию маршрутизации возлагают на активное сетевое оборудование, поскольку это более надежное и производительное решение.

Автоматизация настроек маршрутизации

В больших организациях VLAN распределены по всей сети и информация, предназначенная конкретному компьютеру, часто должна "пройти" через несколько промежуточных сетей. Соответствующие пути могут быть определены вручную *(статическая маршрутизация)*. Но при большом числе VLAN вручную отслеживать изменения, тем более автоматически перестраивать пути в случае повреждения каналов связи, становится практически нереальным. На помощь приходят протоколы автоматической маршрутизации.

В относительно небольших организациях применяются два протокола: RIP и OSPF.

RIP

RIP (Routing Information Protocol, протокол маршрутизации информации) — самый простой в использовании протокол автоматической маршрутизации. Он не требует никакой настройки от администратора. Достаточно только включить использование RIP для всего маршрутизатора и для каждого отдельного интерфейса VLAN.

RIP периодически рассылает широковещательным (RIP версии 1) или мультикастовым (RIP версии 2) образом информацию о собственной таблице маршрутизации. Приняв аналогичный пакет от другого маршрутизатора, RIP выполняет изменение локальной таблицы маршрутизации. В результате через некоторый промежуток времени коммутаторы будут "знать" маршруты, присутствующие на каждом устройстве.

Недостатками RIP являются излишняя "шумливость" (постоянная рассылка большого количества информации) и плохая масштабируемость для крупных сетей.

OSPF

Протокол *OSPF* (Open Shortest Path First, "первыми открываются кратчайшие маршруты") позволяет создавать таблицы маршрутизации больших сетей. Он требует предварительной настройки, хотя в случае не очень крупной сети эти операции не являются сколько-нибудь сложными.

В самой минимальной конфигурации достаточно включить использование протокола OSPF на коммутаторе, создать одну область (обычно ее называют *областью 0* — area 0) и активизировать протокол OSPF для каждого интерфейса VLAN.

Протокол OSPF позволяет настроить безопасную передачу данных о таблицах маршрутизации (данные будут приниматься, например, только после идентификации маршрутизатора безопасным способом).

Различным линиям связи можно назначить *весовые коэффициенты*, что позволит администратору более точно настроить выбираемые коммутатором пути передачи

данных. В случае сложной структуры сети можно создать несколько различных зон и настроить их параметры так, чтобы минимизировать служебный трафик и ускорить сходимость таблиц маршрутизации в случае изменения топологии.

DHCP-relay

Запросы на получение IP-адреса являются широковещательными и рассылаются только в пределах одной VLAN. Создание надежной службы DHCP для каждой VLAN обычно нерационально, поскольку один DHCP-сервер может обслуживать большое число сетей.

Для передачи запроса на получение IP-адреса из одной сети в другую необходимо использовать специальную программу, называемую агентом DHCP, которая будет проверять наличие в сети запросов на получение IP-адреса и переправлять их на сервер DHCP уже от своего IP-адреса. Такие пакеты маршрутизируются между сетями, поскольку являются одноадресными (приходит с адреса агента на адрес DHCP-сервера). Сервер DHCP, получив такой запрос, "знает", что нужно предоставить IP-адрес из диапазона адресов, соответствующего адресу агента, сообщает всю информацию агенту и процесс завершается обычным для аренды адреса образом.

DHCP-агента можно реализовать как программным образом на сервере Windows в настройке службы маршрутизации и удаленного доступа, так и на коммутаторах третьего уровня.

В случае настройки коммутатора достаточно включить данную функцию и для каждого интерфейса VLAN указать адреса DHCP-серверов, на которые следует пересылать запросы аренды адреса.

Программная маршрутизация

Рабочие станции Windows могут выступать в качестве маршрутизаторов только при установке специализированных программ третьих фирм, например, WinRoute. Существует большое количество аналогичных программ (многие из которых бесплатны), используемых даже в системах на Windows 9*x*. Серверы Windows уже включают в себя возможность маршрутизации — в их составе присутствует Служба маршрутизации и удаленного доступа (Routing and Remote Access Server, RRAS).

RRAS

Служба RRAS (Routing and Remote Access Server) осуществляет многопротокольную[1] маршрутизацию пакетов, позволяет создавать соединения по требованию и осуществлять для них маршрутизацию данных. Начиная с Windows 2000, служба RRAS устанавливается автоматически, но находится в *отключенном состоянии*. Для ее запуска следует открыть консоль управления RRAS и выполнить задачу **Настроить и включить маршрутизацию и удаленный доступ**.

Сервер RRAS может выполнять как *статическую*, так и *динамическую* маршрутизацию. Настройка статической маршрутизации через оснастку RRAS — это просто

[1] Служба маршрутизирует протоколы IP, IPX, AppleTalk.

использование графического интерфейса вместо утилиты route, запускаемой одноименной командой `route` . Больший интерес представляет возможность включения динамических протоколов маршрутизации — Routing Information Protocol (RIP) и Open Shortest Path First (OSPF).

Виртуальные маршрутизаторы

У классических маршрутизаторов правила, по которым пакеты пересылаются из одной сети в другую, — эти правила называют *таблицей маршрутизации* — едины для всего устройства. Это означает, что такое устройство не сможет правильно маршрутизировать данные между двумя VLAN, интерфейсам которых присвоены IP-адреса из одного диапазона. Хотя диапазонов адресов, предназначенных для внутреннего пользования, вполне достаточно для правильного назначения частным сетям, на практике возникают ситуации, когда менять диапазоны в VLAN не совсем удобно. Например, к сети большого предприятия подключается организация, у которой уже есть своя структура, удаленные офисы и т. д. И менять адреса в таком случае значит перенастраивать большое число устройств и программ.

Помочь в подобной ситуации может создание *виртуального маршрутизатора*. Протокол *VRF* (Virtual Routing and Forwarding) позволяет на одном устройстве создать несколько таблиц маршрутизации и пересылки данных (рис. 8.7).

В результате к маршрутизатору можно подключать локальные сети с совпадающими диапазонами IP-адресов.

Настройка протокола VRF достаточно проста. Необходимо дать команду на создание маршрутизатора, присвоить ему идентификатор и далее создавать таблицу маршрутизации. Подключение VLAN к конкретному виртуальному маршрутизатору осуществляется настройкой параметров VLAN на маршрутизаторе.

Недостаток решения — поддержка протокола VRF реализована не во всех моделях маршрутизаторов.

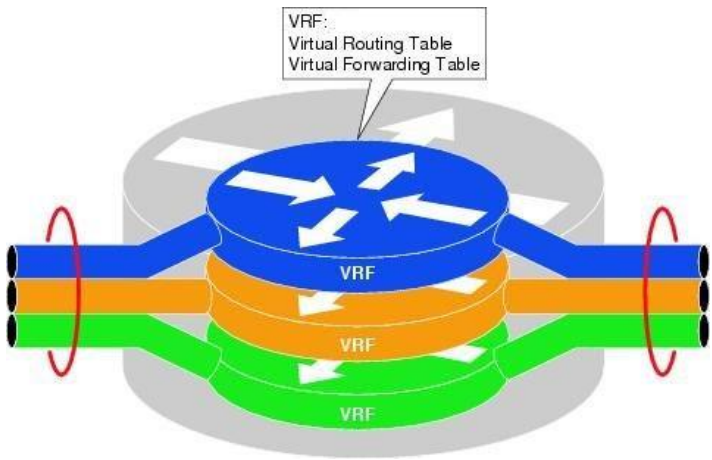


Рис. 8.7. VRF: один коммутатор разбивается на несколько виртуальных

ГЛАВА 9

Безопасность

Расходы на обеспечение защиты информации растут впечатляющими темпами. Но при этом часто не соизмеряют реальную ценность информации с мерами по ее защите и ставят перед собой невыполнимую задачу достижения абсолютной надежности.

В каждом конкретном случае затраты, выделяемые на обеспечение безопасности, должны коррелировать с потенциальной опасностью. Если злоумышленник задастся целью "сломать" систему, он обязательно это сделает и нам не поможет никакая защита. Важно снизить вероятность такого вторжения до экономически оправданных значений и минимизировать возможный ущерб.

Человеческий фактор

Как руководители, так и системные администраторы должны четко понимать, что удобство в работе пользователей и безопасность предъявляют к системе совершенно противоположные требования. Чем безопаснее система, тем больше ограничений накладывается на текущую работу и тем более неудобной она становится, и наоборот. Проще всего использовать систему, в которой отсутствуют какие-либо ограничения по безопасности данных. Любая реальная система содержит разумные компромиссы, определяемые в каждом конкретном случае индивидуально.

При реализации тех или иных организационных и технических мероприятий всегда следует учитывать человеческий фактор. Если вы потребуете от сотрудников частой смены пароля, то, чтобы не забыть, они начнут записывать пароли на различные памятки. Контроль сложности паролей не заставит пользователей формировать их при помощи генераторов случайных чисел. Скорее всего, большинство будет постоянно использовать один и тот же пароль, составленный на основе некоторой осмысленной последовательности символов, изменяя в нем (когда настанет срок очередной смены пароля) по одному символу.

Любая идеально спроектированная система защиты окажется неработоспособной, если она не будет учитывать практические аспекты эксплуатации информационной системы.

Интернет-ресурсы, посвященные безопасности

Системному администратору необходимо быть достаточно информированным о текущем состоянии компьютерной безопасности. Это предполагает периодическое ознакомление с данными специализированных сайтов, посвященных этой тематике, по возможности подписку на оповещения об обнаруженных критических уязвимостях.

Отмечу следующие источники.

- SecurityFocus (**http://www.securityfocus.com**).

  Сайт позволяет подписаться на многочисленные рассылки по проблемам безопасности. Честно говоря, автору больше нравится читать приходящие сообщения электронной почты, чем периодически посещать страницы Интернета, выясняя новости сайтов.

- Packet Storm (**http://www.packetstormsecurity.org**).

  Сайт включает в себя перечни эксплойтов, сценариев, кодов, которые применяются при атаках на компьютерные системы. Эти коды собираются с андеграунд-сайтов, правда, не всегда оперативно. Но информация сайта, а также приведенные на нем ссылки на ресурсы Интернета заслуживают внимания администратора.

- CERT vulnerability notes (**http://www.kb.cert.org/vuls/**).

  Сайт, на котором публикуется информация об уязвимостях от группы United States Computer Emergency Readiness Team. Эта группа существует с 2003 года и занимается анализом и предупреждением кибер-преступлений в США.

  На сайте также можно осуществить подписку на рассылку об обнаруженных уязвимостях.

- Common Vulnerabilities and Exposures (MITRE CVE, **http://cve.mitre.org**).

  Сайт посвящен вопросам стандартизации уязвимостей.

- IBM Internet Security Systems (**http://xforce.iss.net**).

  Сайт ISS (Internet Security Systems) — организации, являющейся одним из лидеров изучения безопасности и осуществляющей круглосуточный мониторинг Интернета. Администраторы могут загрузить различные патчи, устраняющие те или иные уязвимости.

- Еженедельная рассылка @RISK (**http://www.sans.org/newsletters/risk/**).

  Институт SANS (SysAdmin, Audit, Network, Security) занимается изучением уязвимостей и обучением специалистов безопасности. Данные об обнаруженных уязвимостях публикуются институтом в нескольких периодических рассылках, на одну из которых можно подписаться по указанному ранее адресу.

- Русскоязычный сайт с исследованиями уязвимостей (**http://securityvulns.ru/**).

- Группа реагирования на компьютерные инциденты (**http://www.ciac.org/ciac/index.html**).

Попытаемся разложить по полочкам

Защита информации представляет собой настолько всеобъемлющую задачу, что очень легко запутаться во всех мерах защиты. Прежде чем начать что-то делать, ответьте на несколько вопросов:

- ***что*** нужно защищать;
- ***где*** нужно защищать;
- ***от чего*** нужно защищать.

И только после этого можно решать ***как*** защищать.

Что защищаем

Информация может быть различных категорий. Часть данных публична, часть — является коммерческой тайной, часть подлежит защите как имеющая соответствующий гриф.

При этом системный администратор должен иметь четкое представление, каким категориям работников организации и в каком объеме разрешен доступ к информации определенного уровня. Соответствующее распоряжение должно быть сформулировано руководителями бизнеса совместно со специалистами.

Где защищаем

Необходимо четко представлять, где и как обрабатывается информация, как построена сеть организации, как данные из одной программы переносятся в другую, каким способом реализуется доступ в глобальную Сеть и т. п.

Объем информации зависит от уровня необходимой защиты. Например, если мы предполагаем реализовывать защиту от утечки данных через электромагнитное излучение, то должны получить схемы электропитания с указанием расположения кабелей (насколько они близко проложены к информационным линиям), схемы охранной и пожарной сигнализации, заземления, расположения оборудования относительно окон и т. п.

Чем точнее и полнее будет собрана информация, тем лучше можно будет организовать защиту.

От чего защищаем

После того, как в организации определено, что и где подлежит защите, необходимо подготовить список угроз, которым подвержена система. Говорят, что в этом случае нужно составить *модель угроз.*

Информация может быть утеряна, повреждена (временно недоступна) или же стать доступной третьим лицам. Все эти события нежелательны для системы. Причины, способные привести к указанным событиям, можно разделить на следующие группы:

- умышленные действия пользователей, имеющих доступ к информации и/или настройкам системы;
- не умышленные, ошибочные действия пользователей, имеющих доступ к информации и системе;
- умышленные действия лиц, не имеющих доступа к информации;
- отказ оборудования, порывы кабелей и т. д.

Для удобства подготовки мер противодействия удобно рассматривать эти угрозы по следующим уровням информационной системы:

- уровню сети (уязвимости протоколов TCP/IP, канального уровня);
- уровню операционных систем (особенности реализации и уязвимости различных ОС);
- уровню управления базами данных (выделен особо, поскольку практически все информационные системы используют те или иные базы данных);
- уровню прикладных приложений.

Таким образом, последовательность подготовки мер по защите информации будет выглядеть примерно так. Рассматриваем транспортный уровень сети. Что могут сделать допущенные к управлению сетью пользователи? Наверное, получить несанкционированный доступ к информации, модифицировать ее в своих интересах или нарушить связь. После этого пытаемся в общих чертах сформулировать возможности по каждому выявленному риску. Например, для получения доступа можно изменить настройки оборудования и направить копию данных на интерфейс своего компьютера. Можно подключиться к порту оборудования в другой частной сети, если для этого порта не настроен контроль доступа. И так далее.

После того как мы сформулируем риски, можно уже приступать к выработке мер противодействия.

Понятно, что для выявления возможных рисков и подготовки мероприятий необходимо наличие соответствующего опыта у системного администратора. Хотя для начала работ вполне достаточно тех материалов, которые есть в свободном доступе.

Наиболее трудоемки в определении риски, связанные с конкретной реализацией информационной системы и используемым в ней программным обеспечением. Чтобы правильно предусмотреть возможные опасности при использовании на одном компьютере программного продукта "A", на другом — "B" и при наличии, например, конкретного типа хранения данных на сервере, нужно обладать высокой квалификацией практически по всем используемым продуктам.

Хорошо, если такие специалисты в организации есть, и они могут выработать какие-либо *предупреждающие* мероприятия. В подавляющем же большинстве случа-

ев используется информация только о типовых уязвимостях, которые известны техническому персоналу.

Примечание

В силу особой важности этого положения, хочу еще раз акцентировать внимание на том, что ни одна программа, сканирующая сеть на наличие уязвимостей, ни одна аудиторская организация, приглашенная для анализа безопасности, не смогут предложить вам исчерпывающий перечень мероприятий. В большинстве случаев вы получите анализ типовых уязвимостей в типовой структуре. Так, сканеры безопасности проверяют, прежде всего, реализацию всех мер, предлагаемых изготовителем в инструкции по повышению безопасности *(см. разд. "Индивидуальная настройка серверов" далее в этой главе)*, и установку обновлений *(см. разд. "Исключение уязвимостей программного обеспечения" далее в этой главе)*. При сертификации системы особое внимание уделяется наличию комплекта организационно-распорядительной документации (приказов, инструкций, матриц доступа и т. п.). "Закрытие" всех этих уязвимостей не даст шанса "покоиться на лаврах".

Как защищаем

При выработке мер противодействия нужно учитывать стоимостные факторы. Как правило, существует несколько возможных путей решения, и вам необходимо, исходя из специфики организации, выбрать оптимальный. Например, риску кражи сервера с важной информацией можно противопоставить введение круглосуточной охраны, а можно предусмотреть какое-либо аппаратное шифрование данных на жестком диске. Если стоимость сервера меньше стоимости мер его защиты от пожара, то выгоднее пожертвовать конкретным компьютером, ограничившись резервным копированием данных.

В итоге описанной ранее процедуры анализа вы получите достаточно большой перечень возможных рисков. Понятно, что реализовать все мероприятия будет практически невозможно. Поэтому следует руководствоваться достаточно общим правилом "30/70": 70% всех уязвимостей могут быть закрыты реализацией лишь 30% мероприятий, надо только правильно ранжировать их по значимости.

К сожалению, практика оперативного появления в продаже практически любых баз данных, имеющих коммерческое значение, свидетельствует, что многие меры защиты существуют больше "для отчетности", чем реально обеспечивают конфиденциальность информации. Без *постоянного* внимания к вопросам информационной безопасности говорить о безопасности бессмысленно.

Три "кита" безопасности

Объем работ по обеспечению безопасности информационной системы составляет основную часть рабочего времени системного администратора, поэтому важно правильно организовать свою работу. На какие принципиальные моменты я бы советовал обратить внимание.

- Обеспечьте документальное оформление безопасности информационной системы организации.

Все действия, которые предпринимает системный администратор в части тех или иных технических настроек системы, являются только реализацией требований, которые должны быть заложены в концепции информационной безопасности предприятия и реализующих ее конкретных положениях и инструкциях.

- Реализовывайте эшелонированную систему обороны.

  При организации мер защиты информационной системы возьмите курс на создание нескольких рубежей защиты. Взломать два уровня защиты гораздо сложнее, чем один.

  Так, антивирусную защиту можно настроить на сервере (анализ сообщений на почтовом сервере, проверка трафика Интернета на прокси-сервере и т. п.) и на компьютере пользователя. Проверку пользователя можно выполнять как при физическом подключении (настройкой безопасности портов активного оборудования), при входе в сеть, при запуске прикладной программы (используя аутентификацию при входе в задачу) и т. д.

- Постоянно контролируйте систему.

  Ни одни правила не выполняются, пока нет реального контроля. Не доверяйте радужным отчетам. Проводите независимый контроль, организуя специальные проверки. Анализируйте данные статистики: отклонения от "нормального" поведения могут свидетельствовать о готовящейся атаке. Например, на одном из предприятий кража данных была обнаружена анализом статистики сетевого трафика: пользователь копировал информацию в ночное время, и эти действия проявились повышением сетевого трафика в часы, когда подобной активности не предполагалось.

И последний совет. Сколько бы усилий вы не прилагали, защищая систему, всегда может обнаружиться уязвимость, которая может позволить злоумышленнику провести успешную атаку. Поэтому целью защиты должна быть не гарантия 100%-й надежности — это недостижимая цель, а реализация таких мер, которые позволят ***уменьшить эффект*** от вторжения и с минимальными затратами для предприятия восстановить работу информационной системы.

Типовые меры защиты информационной системы

В каждой организации "лидеры" по эффективности мер обеспечения безопасности будут свои. Тем не менее существуют типовые мероприятия, реализовывать которые необходимо любому системному администратору. Условно эти меры можно сгруппировать по следующим характеристикам:

- выработка организационных мероприятий обеспечения безопасности;
- реализация мер защиты информационной системы от внешних угроз;
- реализация мер защиты серверов и станций от злонамеренного ПО;
- защиты информации периметром организации.

Организационное обеспечение информационной безопасности

Практика показывает, что организационные мероприятия по эффективности в несколько раз превосходят технические меры защиты.

Прежде всего, на уровне руководства предприятия необходимо сформировать четкое представление об основных положениях информационной безопасности. Предпочтительно создать концепцию информационной безопасности, в которой определены категории обрабатываемой информации, перечислены предполагаемые риски, установлены направления и объем защиты данных для каждой категории.

Каждая автоматизированная система предприятия должна иметь официально присвоенную ей категорию по конфиденциальности, любое рабочее место — паспорт, в котором должны быть перечислены конфигурация системы, установленное программное обеспечение, категории информации, с которой предполагается работать на данном компьютере. После того как такой укрупненный анализ будет выполнен, станет проще планировать и реализовывать защиту данных.

В организационно-распорядительных документах организации необходимо зафиксировать правила взаимодействия пользователя с информационной системой. Пользователь должен знать, с чем он работает, какие программы он может использовать, а какие утилиты запрещены в организации (например, сканирования сети) и т. п. В инструкциях необходимо оговорить правила работы с электронной почтой организации, поведение пользователя в случае возникновения предположения о наличии вируса, требования к взаимодействию с Интернетом и т. д.

Чем точнее определены права пользователя и ответственность за нарушение обязанностей, тем с большей вероятностью вы можете ожидать исполнения инструкций.

Естественно, что выполнение требований инструкций должно сопровождаться периодическими проверками, например, путем анализа журнала посещенных сайтов Интернета *(технический контроль)* или проверкой отсутствия записей паролей на стикерах *(организационные меры)*.

План обеспечения непрерывности функционирования информационной системы

Вам очень поможет в работе, особенно при построении взаимоотношений с руководителями, наличие плана 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, можно ли перенести функции сервера в случае его отказа на другое оборудование? Допустимо ли заменить его другим сервером, службы которого не критичны и от них можно отказаться на время ремонта основ-

ного компьютера? Где должны храниться дистрибутивы, чтобы операция могла быть проведена дежурным оператором? Какова должна быть процедура восстановления данных? Описав все аварийные ситуации и пути их устранения, вы сможете рассчитать ожидаемое время восстановления системы в каждом случае отказа.

Если такой план будет утвержден руководством, то, с одной стороны, вы получите защиту от неоправданных требований немедленного восстановления работы, поскольку для каждой ситуации период восстановления будет четко оговорен. С другой стороны, этот план станет инструкцией, что нужно делать в аварийной ситуации.

Безопасность паролей

Одним из самых "узких" мест безопасности являются пользовательские пароли. Если вы ни разу не использовали какую-либо утилиту для взлома паролей, то не поленитесь установить любую демо-версию и проверить стойкость реальных паролей. Вы будете приятно удивлены, узнав через несколько часов ее работы существенную часть паролей пользователей.

Для подкрепления рекомендаций по выбору паролей обычно используют простые расчеты: количество всех возможных паролей заданной длины делят на скорость работы программ перебора (обычно это несколько миллионов паролей в секунду). Полученную стойкость пароля считают достаточной, если расчетное время поиска пароля в несколько раз больше периода его плановой смены.

Однако все такие предположения не учитывают обычной пользовательской практики. Во-первых, пользователи крайне редко используют в паролях специальные символы, обычно составляя его из букв (русского или латинского алфавита, причем часто в пароле встречается только один набор), цифр и, иногда, знаков препинания (точка, тире и т. п.). Формальные требования сложности пароля, контролируемые автоматически, достаточно легко обходятся: пароль просто начинают с заглавной буквы, а в конце добавляют цифру или символ. В результате количество вариантов пароля, которые необходимо перебрать для его подбора, резко уменьшается.

Во-вторых, традиционные рекомендации усложнения паролей — замена одних символов на сходные по начертанию ("а" на "@", "о" на "0" и т. п.), "выбрасывание" гласных из слова, используемого в качестве пароля, прямой и обратный порядок букв, осмысленные слова и т. п. — давно учтены в программах перебора (рис. 9.1).

Существуют различные программы, предназначенные для "восстановления" паролей пользователей. Способов получения "первоначальных данных" по паролям много. Это и прослушивание сети (не надо надеяться на использование коммутаторов, поскольку существуют способы "обходить" их фильтрацию пакетов), использование базы безопасности локальной или удаленной машины (при наличии на это устройство административных прав), импорт соответствующих файлов (если есть доступ к данным из другой операционной системы). Программы способны перехватывать и дешифрировать все существующие в настоящий момент протоколы.

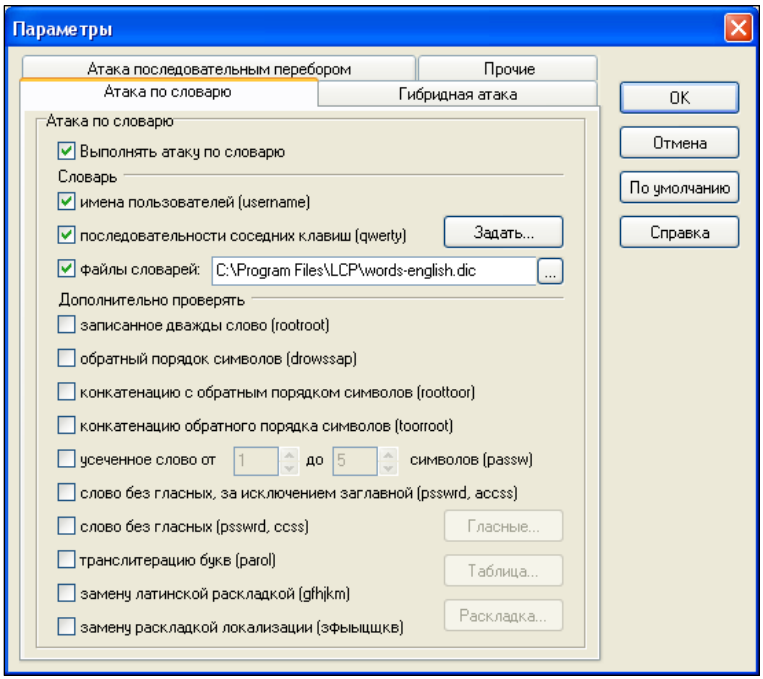


Рис. 9.1. Параметры подбора пароля "учитывают" типовые рекомендации "сложного" пароля

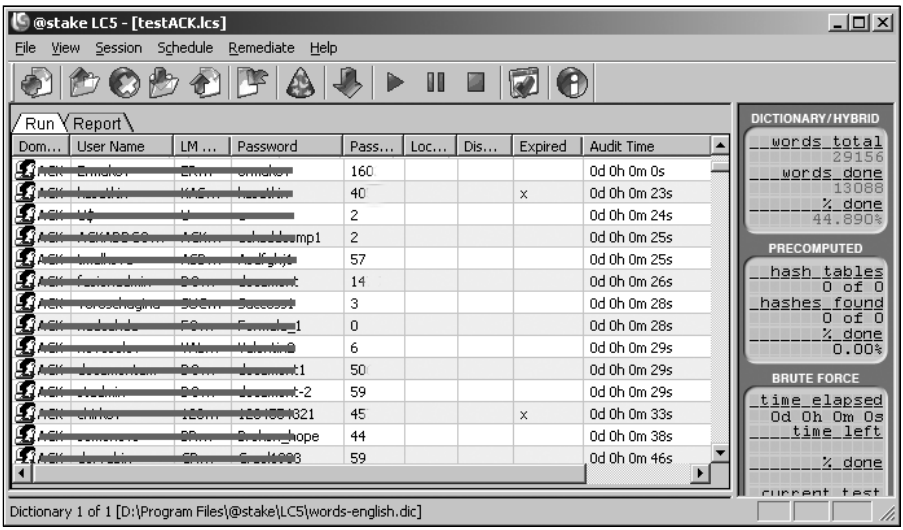


Рис. 9.2. Окно программы LC5 для восстановления паролей

На рис. 9.2 представлен результат работы программы LC5 от компании @stake (**www.atstake.com/lc**), которая позволяет узнавать пароли в Windows- и UNIX-сетях. Это данные по реальной сети (имена учетных записей закрыты), в которой политикой безопасности включено стандартное требование сложности пароля. Обратите внимание на колонку времени дешифрования каждого пароля — для всех

показанных на рисунке учетных записей оно составило менее 50 с. А если просмотреть те пароли, которые были дешифрованы быстрее всех, то основными причинами такого успеха явились действия пользователей, которые составляли пароли на основе своих данных с добавлением цифр (например, пароль `Valentin_1` дешифрирован за 29 с), из простых слов и цифр (например, `Cruel1234` "узнан" за 46 с) или последовательно расположенные клавиши (например, `ASDFGHj1`, 25 с).

Rainbow-таблицы

Операционные системы используют не пароли, а их *хэши*, созданные по известным правилам. Параметры вычислительной техники настолько выросли, что у хакеров появилась возможность не перебирать пароли, а составить базу данных хэшей паролей и затем просто выбирать из нее необходимые значения по полученным данным. В результате достаточно узнать (например, перехватить по сети) хэш пароля, выполнить запрос к подобной базе, которую называют Rainbow-таблицей, и получить значение пароля практически сразу.

Программы для использования Rainbow-таблиц доступны в Интернете, единственная проблема их использования заключается в объеме таблиц. В зависимости от набора символов и длины предполагаемого пароля вам придется закачать из Интернета до нескольких десятков гигабайт данных. Хотя стоит заметить, что с появлением безлимитных тарифов эти объемы стали доступны многим пользователям.

При желании можно создать подобную таблицу и самостоятельно. Так, генератор таблиц Rainbow из состава программы Cain & Abel от Massimiliano Montoro (**www.oxid.it**) позволяет построить таблицу хэшей для паролей, состоящих из всех букв латинского алфавита и цифр, длиной до 8 символов включительно менее чем за полтора дня (рис. 9.3).

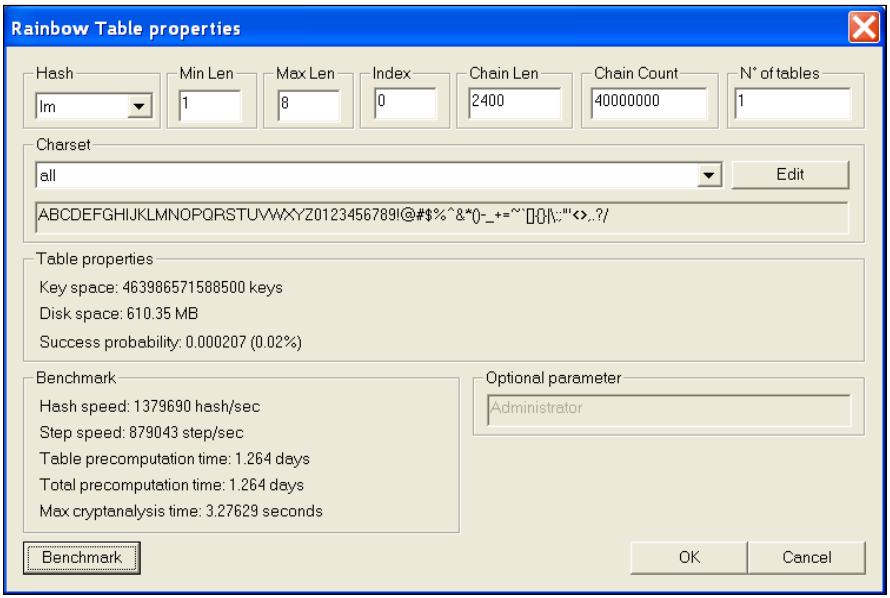


Рис. 9.3. Окно настройки параметров генератора Rainbow-таблицы

Рекомендации по составлению сложного пароля

Все рекомендации, предлагаемые пользователям, должны учитывать их психологию, а не только следовать техническим параметрам. Так, если установить небольшое время жизни пароля (около месяца), то (при одновременном требовании его сложности) это приведет к тому, что пароли начнут записывать, хранить их вблизи компьютера и т. п.

Из описанных ранее примеров атак на пароли следует главный вывод: пароль должен быть *очень* длинным, не менее 15—20 символов. Человеку сложно запомнить произвольную последовательность такой длины, гораздо проще запоминаются *фразы*. Составьте пароль из нескольких слов, разделенных пробелами или знаками препинания. Такой пароль крайне сложно подобрать.

При смене пароля следует перейти к новой фразе, а не модифицировать предыдущую путем добавления нескольких символов в начале или конце.

Ни в коем случае не следует использовать пароль учетной записи для доступа к сайтам Интернета, требующим идентификации. Для упрощения работы с паролями Сети используйте любую программу защищенного хранения паролей.

Технические пути решения проблемы

Организационные меры работы с паролями требуют, насколько это возможно, технического подкрепления. После выполнения рекомендаций по настройке безопасности выполнение ряда параметров будет контролироваться автоматически. Это обеспечит минимальный уровень безопасности.

Для особо ответственных учетных записей (администраторы предприятия и т. п.) необходимо внедрить аппаратные средства аутентификации: смарт-карты, биометрические средства контроля и т. п. Обратите внимание на отсутствие личных послаблений: не отключайте себе те ограничения на пароль (например, необходимость его периодической смены), которые введены для пользователей. Используйте длинный пароль (не менее 15 символов), по возможности один из его символов не должен вводиться с клавиатуры. Иными словами, символ должен набираться через его код: <Alt>+*код*. Перечень таких символов можно найти в справочной документации к операционной системе в разделе, посвященном строгости паролей.

> ***Совет***
>
> Ни в коем случае не используйте пароль администратора предприятия для входа на рабочие станции пользователей. Существует достаточное число утилит, которые, не обнаруживая себя в системе, протоколируют нажатия всех клавиш. При необходимости включите при помощи групповой политики какую-либо учетную запись в число администраторов рабочих станций и используйте эту учетную запись для их администрирования.

Блокировка учетной записи пользователя

Одним из способов борьбы с подбором пароля учетной записи пользователя является ее блокировка после некоторого числа неудачных попыток входа. Эта опция включается через групповую политику организации.

На практике данное правило не имеет особого значения, поскольку прямой перебор паролей пользователя обычно уже не используется. Однако включение ее все же позволит несколько повысить защищенность систем. При этом значение порога числа неудачных попыток набора пароля не должно быть слишком малым. Во-первых, пользователи достаточно часто допускают ошибки при вводе своего пароля. Во-вторых, если такая ошибка будет ими допущена при указании сохраняемого пароля (например, они укажут необходимость сохранения пароля в параметрах доступа к Интернету или к почтовому серверу), то это приведет к нескольким автоматическим повторам ввода неверного пароля и последующей блокировке учетной записи.

Автор рекомендовал бы установить порог блокировки учетной записи на уровне 10—20 неудачных попыток ввода. При этом период, в течение которого будут считаться данные попытки, а также время, через которое произойдет автоматическая разблокировка учетной записи пользователя, можно установить порядка одного часа.

> ***Примечание***
>
> Если к учетной записи предъявляются особые требования безопасности, то можно оставить только вариант ее ручного разблокирования, хотя это приведет к увеличению административной нагрузки, в том числе потребует и исследования каждого такого инцидента.

Блокировка учетных записей достаточно часто может возникать вследствие тех или иных неверных настроек, ошибок сохраненных паролей и т. п. Для исследования таких ситуаций можно загрузить комплект утилит — Account Lockout and Management Tools (ALTools.exe, **http://www.microsoft.com/downloads/details.aspx?familyid=7af2e69c-91f3-4e63-8629-b999adde0b9e&displaylang=en**.), позволяющий проанализировать причины блокировки учетных записей. В комплект входят программы, предназначенные для анализа систем, вызывающих блокировки, средства просмотра параметров учетных записей и поиска данных на контроллерах домена.

Смарт-карты

Существуют различные технические решения, которые позволяют аутентифицировать пользователя, не прибегая к вводу пароля, например, по каким-либо биометрическим показателям. Но наиболее используемым на практике методом является аутентификация на основе *смарт-карты*.

Смарт-карта представляет собой устройство, на которое можно с помощью специальных *считывателей* записывать (и считывать) информацию. Обычно на смарт-карте сохраняется сертификат пользователя, предназначенный для аутентификации его в системе. Чтобы сертификат не мог быть использован злоумышленником, он защищается специальным кодом — *PIN-кодом*. PIN-код — это не пароль пользователя в системе, это только защита на случай утери или кражи смарт-карты. Он не передается по сети (поэтому не может быть перехвачен анализаторами трафика) и используется только *локально* для доступа к сертификату. Поэтому он может быть достаточно коротким и удобным для запоминания.

В зависимости от объема памяти на карте, на нее принципиально можно записать несколько сертификатов, что позволит использовать смарт-карту для различных целей (например, вход пользователя в различные системы, хранение сертификатов для электронных подписей и т. п.).

Примечание

Поскольку в смарт-картах применяются сертификаты пользователей, то в организации должна быть развернута структура PKI (Public Key Infrastructure, инфраструктура открытых ключей) и опубликованы шаблоны сертификатов для аутентификации пользователей с помощью смарт-карт.

Существуют две возможности записи сертификата пользователя на смарт-карту. Первая — это выполнение операции самим пользователем. В этом случае пользователь должен предварительно войти в систему, используя свой сетевой пароль, после чего начать операцию получения сертификата для аутентификации с помощью смарт-карты. Недостаток этого варианта состоит в необходимости первоначального входа в систему с обычным паролем.

Второй способ предполагает выдачу сертификата администратором. Для этого на компьютер, на котором будет выполняться эта операция, необходимо установить специальный сертификат для выдачи сертификатов пользователям. Его принято называть *enroll agent*. Для этого необходимо опубликовать соответствующий шаблон на центре сертификатов и установить сертификат на компьютер. По умолчанию правом установки такого сертификата обладают только администраторы системы. Чтобы выдать сертификат пользователю смарт-карты в этом случае, необходимо начать операцию запроса сертификата, указав в опциях тип запрашиваемого сертификата — *enroll agent*. Далее на очередном шаге следует выбрать соответствующего пользователя из списка.

Смарт-карта может использоваться и для входа в удаленную систему в режиме терминального доступа. Такая возможность позволяет администратору не использовать свой сетевой пароль при операциях удаленного управления.

Смарт-карту можно использовать в любых операциях, требующих аутентификации пользователя. За некоторыми исключениями. Так, у автора не получалось использовать смарт-карту для аутентификации на других компьютерах при удаленной работе на терминальном сервере и т. д. Например, в операции **Запустить от имени...**. Для этого достаточно раскрыть список выбора пользователей в окне набора пароля, выбрать смарт-карту и набрать ее PIN-код (рис. 9.4).

В случае предъявления повышенных требований к безопасности администратор может наложить некоторые условия на использование смарт-карт. Так, можно разрешить локальный вход на конкретный компьютер только с использованием смарт-карты (устанавливается через локальную политику безопасности компьютера; кроме того, данное требование можно включить в групповую политику заданного подразделения). Аналогичное требование можно предъявить и к пользователю: разрешить ему работу в системе только с помощью смарт-карты. Это условие реализуется через параметры учетной записи.

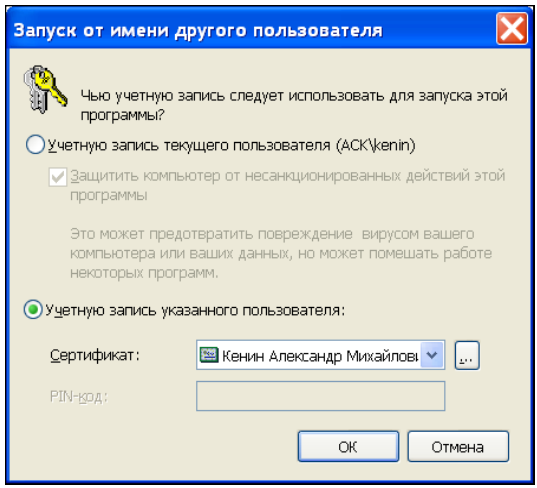


Рис. 9.4. Использование смарт-карты для аутентификации в операции **Запустить от имени..**

Кроме того, можно определить действия, выполняемые системой при вытаскивании смарт-карты (например, автоматически блокировать компьютер или производить отключение пользователя). Эти параметры также настраиваются через групповую политику.

eToken

Для использования смарт-карт необходимо наличие на компьютерах специального устройства — *считывателя смарт-карт*. В настоящее время такими устройствами в нашей стране оборудована лишь незначительная часть компьютеров. Существует техническое решение, которое позволяет использовать технологию смарт-карт для входа в систему стандартной комплектации. Это eToken (или российский аналог ruToken от компании "Актив", **http://www.rutoken.ru/**, **http://www.guardant.ru/**).

eToken представляет собой компактное USB-устройство. Подключение eToken в USB-порт воспринимается системой как вставка смарт-карты, однако перед использованием eToken нужно установить на систему дополнительный драйвер этого устройства.

Стоимость eToken соизмерима со стоимостью считывателя смарт-карт, но если в организации необходимо обеспечить повышенный уровень безопасности только для отдельных пользователей, то данное решение будет экономически оправданным.

Восстановление пароля администратора

Существует несколько утилит, позволяющих заменить пароль администратора (в том числе и администратора домена). Среди коммерческих вариантов едва ли не самая популярная — это программа ERD Commander (сегодня входит в состав Microsoft Desktop Optimization Pack). Программа создает загрузочный компакт-диск, который позволяет не только заменить пароль администратора, но и отредак-

тировать настройки реестра системы, использовать сетевой доступ для копирования файлов (после загрузки система "видит" сеть) и выполнить другие операции конфигурирования систем на основе Windows.

Среди бесплатно распространяемых программ можно отметить Offline NT Password Editor (**http://home.eunet.no/~pnordahl/ntpasswd/**), которая неоднократно успешно применялась автором для восстановления паролей на серверах и рабочих станциях. По информации с сайта программы ее можно использовать и для Windows 7. Эта программа предоставляется в виде образа загрузочного компакт-диска с операционной системой Linux. Стартовав с такого 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.

После того как пользователь заменит пароль администратора, он получит *полный* контроль над компьютером.

Методы социальной инженерии

В связи с постоянно совершенствующимися техническими мерами обеспечения безопасности злоумышленники все активнее начинают использовать для получения данных об информационной системе методы социальной инженерии. Представляясь новым работником или специалистом службы техподдержки, коммерческим агентом или интервьюером, можно попытаться получить сведения о структуре сети и расположении информационных сетевых служб, ознакомиться с действующими мерами обеспечения безопасности данных и т. п. В случае получения недостаточного объема информации от одного сотрудника, злоумышленник легко может обратиться ко второму, третьему и т. д. Широко распространены попытки использования различных анкет, запросов по электронной почте.

Исполнения каких правил поведения должны постоянно придерживаться сотрудники организации?

1. Не давать никакой информации в ответ на любые обращения по телефону, по электронной почте, при личных контактах лицам, если нет четкой уверенности в правомочности таких запросов.
2. Не сообщать никакой информации как личного, так и служебного характера в различных анкетах на страницах информационных серверов Интернета или пришедших по электронной почте.
3. Не отвечать на любые не ожидаемые рассылки по электронной почте, даже если в письме содержится указание на возможность прекращения подписки. Не пересылать писем, содержащих служебную информацию, по почте в незашифрованном виде.
4. При работе в Интернете внимательно следить за URL сайтов, чтобы быть уверенными в работе с конкретной организацией (а не с сайтом, созвучным по написанию с реальной организацией, например имеющим адрес ***организация*.org** вместо ***организация*.net**).

5. Не посещать сайты, предоставляющие сертификат (по протоколу HTTPS), к которому у операционной системы компьютера нет доверия (высвечивается желтый знак предупреждения).
6. При контактах с сотрудником, впервые представившимся вам по электронной почте, принять меры к проверке его данных. При этом не следует пользоваться контактными данными, опубликованными в Интернете; проверьте данные о фирме иными путями, например, через справочные службы.

Меры защиты от внешних угроз

Первое, с чего начинаются мероприятия по защите, — это ограничение доступа к информационной системе как чисто физическое (охраняемые помещения), так и по каналам связи (межсетевые экраны). Цель одна — доступ должен существовать только в пределах осуществляемых функций (опубликованных служб организации).

Физическая безопасность

Особая опасность наличия физического доступа к компьютеру состоит в том, что опытный злоумышленник не только получит разовый доступ к информации, но и сможет произвести такую замену служебных файлов системы, что в дальнейшем сможет получать доступ к любым данным в любое время (например, сможет обойти запреты файловой системы NTFS или отключить контроль записи на сменные устройства), причем эти действия будут скрыты от текущих пользователей и администратора.

Ограничения доступа к станциям

Если во время работы компьютера операционная система препятствует чтению защищенных данных, то при наличии физического доступа к компьютеру специальных мер для "взлома" применять не нужно. При загрузке с другой операционной системы (например, с дискеты или компакт-диска, при переносе жесткого диска в другой компьютер) никакие установленные в исходной системе ограничения NTFS не будут препятствовать копированию любой информации.

Понятно, что вы не сможете реально ограничить доступ пользователей к рабочим станциям. Даже если вы отключите дисководы гибких дисков, устройства чтения компакт-дисков и опломбируете компьютер, то будет ли у вас уверенность в том, что кто-то не принес внешний CD-ROM? Или не восстановил после своих действий все пломбы? А если вы установили программу, которая блокирует доступ к таким устройствам (например, DeviceLock от SmartLine), то будете ли вы уверены, что опытный пользователь не отключил этот контроль? На большинстве предприятий контроль над рабочими станциями практически не организован. Поэтому требование ограничения физического доступа относится, прежде всего, к серверам компьютерной сети. Во-первых, администраторы должны включить аудит событий включения/выключения серверов; правилами эксплуатации должен быть преду-

смотрен обязательный разбор причин нештатных выключений серверных станций. Во-вторых, серверы следует устанавливать в специальные помещения (или шкафы с датчиками), оборудованные средствами сигнализации о несанкционированном доступе.

Уровень физической защиты зависит от конкретных условий. Автор встречал ситуации, когда в небольшой организации сервер просто устанавливался в сейф. Более крупные организации размещают серверное оборудование в охраняемом помещении, устанавливая особые правила доступа в него. Существуют возможности оборудования кроссовых шкафов датчиками проникновения, "фирменные" серверы фиксируют каждый случай открытия крышек корпуса и т. п.

Не следует забывать, что данные резервного копирования могут быть использованы для восстановления конфиденциальной информации. Например, можно провести восстановление папок контроллера домена в новое место и получить доступ ко всем защищенным данным. Поэтому меры защиты серверов резервного копирования (устройств, на которые осуществляется копирование данных) должны быть не менее жесткими, чем применяемые к защите контроллеров домена.

Межсетевые экраны

Для ограничения доступа к системе по каналам связи традиционно применяются межсетевые экраны. Использование их мы подробно обсуждали *в главе 5*.

Обратим только еще раз внимание читателя, что, во-первых, нужно контролировать как входящий, так и исходящий трафик. Во-вторых, межсетевой экран не препятствует использованию злоумышленником разрешенных протоколов для доступа к системам (пример доступа извне через МСЭ также приведен *в главе 5*). И в-третьих, межсетевые экраны должны быть задействованы как на периметре информационной системы, так и на каждой рабочей станции и сервере.

Ограничения подключения нового оборудования

Пользователям сегодня доступно большое количество сменных устройств, использование которых может быть потенциально опасным с точки зрения защиты информации. Например, после подключения внешних 3G-модемов внутренняя сеть становится подключенной к сети Интернета. А на внешний диск можно записать порой в несколько раз больше данных, чем их хранится на сервере.

Существуют различные способы ограничения доступа пользователей к внешним устройствам. Во-первых, есть специальные программы, позволяющие точно настроить возможность работы пользователем с внешними дисководами, CD-RW и USB-портов. В качестве примера сошлюсь на GFI LANguard Portable Storage Control (**http://www.gfi.com/**). Данная программа устанавливает на рабочие станции специальные службы, которые контролируют доступ пользователя к подобным устройствам и разрешают операции только для тех учетных записей, которым подобные действия разрешены администратором. Аналогичными функциями обладает и продукт DeviceLock, сертифицированный в нашей стране. Опции контроля доступа к

съемным носителям оснащены и программные комплексы защиты хоста, наиболее известным примером которых является Symantec EndPoint Protection.

Второй вариант — это создание групповой политики Windows, позволяющей контролировать USB-устройства. Подробно данный способ описан в статье KB555324 на сайте Microsoft.

При выборе варианта защиты следует учитывать:

- позволяет ли продукт контролировать различные классы устройств (не только USB-устройства, но и, например, модемы, видеокамеры и т. п.);
- можно ли обойти защиту простыми средствами (например, отключив службу или загрузившись в безопасном режиме и т. п.);
- имеется ли возможность, запретив устройства по их классу, разрешить использование исключений по серийному номеру (реально всегда необходимо обеспечить такие исключения для администраторов, служебных устройств и т. п.).

Обеспечение сетевой безопасности информационной системы

Внешний доступ к информационной системе может быть получен и по каналам связи. Администратор должен обеспечить, чтобы к сети нельзя было подключить "чужое" устройство и чтобы по используемым каналам не было попытки взлома информационной системы.

Контроль проходящего трафика

По каналам связи могут осуществляться попытки взлома информационной системы с использованием как известных, так и неизвестных на настоящий момент уязвимостей. Обычно средствами предотвращений вторжений оснащаются системы защиты хоста. Но существуют способы и контроля всего трафика организации — специализированные средства обнаружения вторжений — *Intrusion Detection System* (IDS).

Решения по обнаружению попыток взлома могут быть как программными, так и аппаратными. Поскольку для такой обработки нужна очень высокая скорость вычислений, то обычно используются специализированные аппаратные устройства, позволяющие обновлять алгоритмы поиска зловредного кода.

Обычно IDS ведут анализ трафика, фиксируют предполагаемые отклонения и формируют соответствующие предупреждения администратору. Но на рынке есть и активные системы: они в реальном режиме времени могут блокировать трафик при обнаружении подозрительных кодов. Их называют *Intrusion Prevention System* (IPS).

Решения IDS/IPS представлены как открытыми продуктами (наиболее известный — Snort), так и коммерческими: Check Point IPS, McAfee IPS, IBM ISS Proventia IPS.

Контроль устройств по MAC-адресам

Самый простой способ контроля подключенного к сети устройства заключается в проверке его MAC-адреса. Этот контроль поддерживается практически всеми управляемыми коммутаторами. При включении этого режима коммутатор запоминает MAC-адрес из первого пришедшего пакета и в дальнейшем пропускает данные только с этого устройства.

Включение проверки MAC-адреса позволит защититься от такой уязвимости, как ARP-spoofing[1], при реализации которой злоумышленник может "расположиться" между двумя компьютерами, обменивающимися данными, и перехватывать весь трафик.

Но поскольку при обнаружении пакета с другим адресом коммутатор блокирует порт до явного вмешательства, администраторы не любят включать такую возможность по собственной инициативе.

Примечание

Этот способ следует применять только тогда, когда другие методы недоступны. Например, для портов, к которым подключены сетевые принтеры. Существует много способов заменить реальный MAC-адрес на произвольное значение. Это легко сделать даже средствами Windows (рис. 9.5), не говоря уже о различных специализированных утилитах, таких как SMAC (**http://www.klcconsulting.net/smac**) и др.

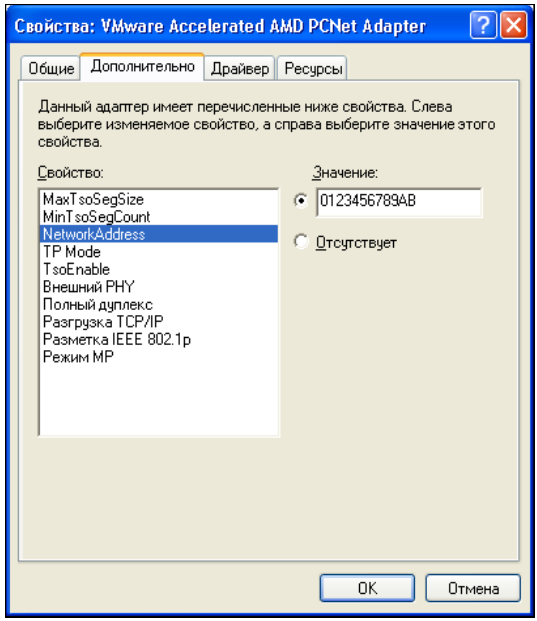


Рис. 9.5. Изменение MAC-адреса путем редактирования свойств адаптера. Если настройки сетевого адаптера не содержат возможности смены MAC-адреса, можно его изменить через реестр системы — параметр `NetworkAddress` ключа `HKLM\SYSTEM\CurrentControlSet\Control\Class\<GUID сетевого адаптера>`. После изменения MAC-адреса желательно перезапустить сетевой интерфейс (отключить и снова включить)

[1] Данная атака использует особенности реализации протокола разрешения имен (ARP) и не зависит от реализации программного обеспечения.

Протокол 802.1*x*

Наиболее безопасным средством контроля подключения к сети в настоящее время является использование протокола 802.1*x*. Протокол 802.1*x* предназначен для аутентификации устройства, подключаемого к локальной сети. Первоначально он был разработан для беспроводных сетей, но впоследствии стал применяться и для контроля устройств, подключаемых к проводным сегментам.

Принципы подключения, описываемые в стандарте, достаточно просты (рис. 9.6, далее в скобках приведена нумерация этапов, указанных на этом рисунке). Первоначально порт, к которому подключается устройство, находится в отключенном состоянии и может пропускать *только* пакеты процесса аутентификации (эти пакеты передаются между подключаемым устройством и службой аутентификации). Подключаемое устройство можно идентифицировать (1) как по его параметрам (например, по заранее известному MAC-адресу или сохраненному сертификату), так и по данным пользователя (в этом случае порт будет открыт после входа пользователя в операционную систему). В качестве службы аутентификации используется RADIUS (2). В сетях с централизованным каталогом сервер RADIUS проверяет параметры подключения на сервере каталогов (3), от которого получает данные аутентификации пользователя (4) и передает на коммутатор разрешение на открытие порта (5). После получения подтверждения от RADIUS порт коммуатора открывается для передачи информации в обоих направлениях (6). При этом RADIUS-сервер может сообщить коммутатору и номер VLAN, в которую должен быть помещен клиент.

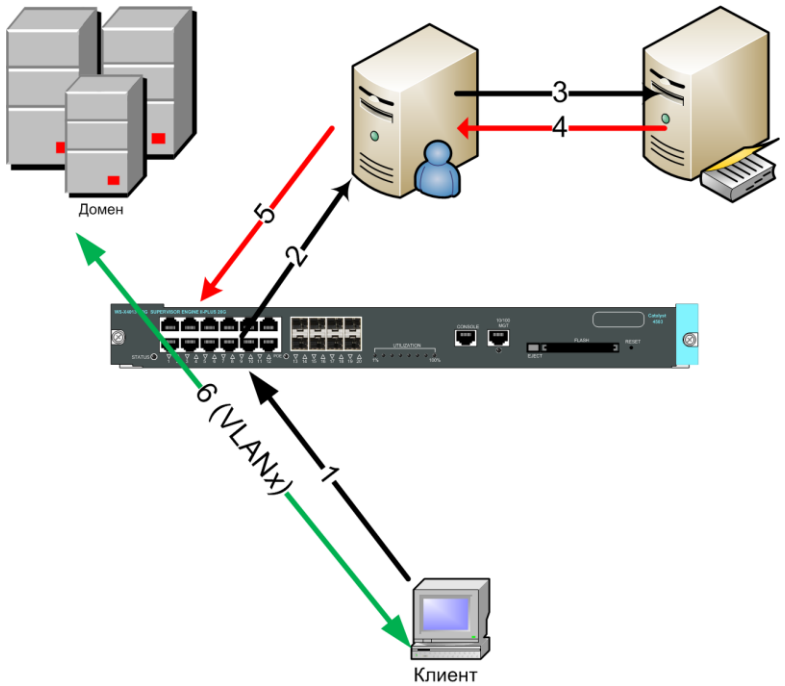


Рис. 9.6. Последовательность подключения клиента по протоколу 802.1x

В процессе аутентификации могут быть использованы различные технологии подтверждения устройства. Наиболее безопасным считаются идентификации на основе сертификатов. Именно настройки данного варианта мы и опишем в настоящем разделе.

Особенности применения протокола 802.1*x*

Протокол 802.1*x* следует использовать только на портах подключения *конечных* устройств. Применить его на уровне распределения и выше невозможно.

Стандарт предусматривает открытие порта после получения подтверждения идентификации устройства. В результате к порту коммутатора можно подключить небольшой сетевой концентратор с несколькими устройствами. После открытия порта аутентифицированным устройством другие компьютеры смогут беспрепятственно работать в локальной сети.

Для предупреждения такой опасности можно применить несколько решений. Во-первых, включить на портах контроль по MAC-адресам; такую возможность поддерживает большинство коммутаторов. Обнаружение на порту второго устройства с другим MAC-адресом заблокирует порт. Вторая возможность предусматривает контроль за подключенными устройствами; данный режим реализован не для всех моделей коммутаторов. Например, для коммутаторов Cisco режим, когда через порт может работать только одно устройство, называется *single-host*, а описанный в стандарте — *multiple-hosts*.

Если предприятие использует IP-телефонию, то подключение телефонных аппаратов и компьютера обычно осуществляется к *одному* порту коммутатора (используется коммутатор на два порта в телефоне). Как правило, настраивать аутентификацию для IP-телефонов не имеет смысла, поскольку, во-первых, при правильном администрировании подключение аппарата сопровождается вводом соответствующего пароля с консоли телефона, во-вторых, данные аудиопотока выделяются в отдельную VLAN. Поэтому многие модели коммутаторов имеют настройки, позволяющие включить необходимость аутентификации по протоколу 802.1*x* для всего трафика, *кроме* IP-телефонии.

Есть ряд устройств, которые не поддерживают данный протокол: во-первых, это компьютеры, на которых установлены старые версии операционных систем, во-вторых, — сетевые принтеры и аналогичные устройства.

В этом случае на соответствующих портах следует использовать иные методы контроля подключенных устройств (например, по MAC-адресам).

Настройка протокола 802.1*x*

Самый безопасный вариант настройки этого протокола — это использовать сертификаты при аутентификации компьютеров и пользователей.

В этом случае администратор должен обеспечить следующие настройки:

- ❒ настройку Центра сертификации;
- ❒ настройку службы каталогов;

- настройку службы RADIUS;
- настройку клиентского компьютера;
- настройку коммутатора.

Для аутентификации по протоколу 802.1*x* вам необходимо, чтобы, во-первых, клиенты имели соответствующие сертификаты, во-вторых, сертификат должен получить RADIUS-сервер.

Выдача сертификатов компьютерам

Часто для компьютеров, входящих в домен, удобно настроить автоматическую выдачу сертификатов. Это делается с помощью групповой политики путем настройки **Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Политики открытого ключа | Параметры автоматического запроса сертификатов | Создать необходимый автоматический запрос**.

RADIUS-серверу необходим специальный сертификат, который можно использовать при аутентификации по протоколу 802.1*x*. Этот сертификат могут выдать только центры сертификации, установленные на Enterprise-версии Windows-сервера. Их необходимо сначала опубликовать в центре сертификации, а затем сервере, на котором запущена служба IAS, открыть оснастку управления сертификатами *локального компьютера* с правами соответствующей учетной записи и запросить сертификат данного типа. После выполнения операции следует проверить наличие сертификата в соответствующем контейнере (рис. 9.7).

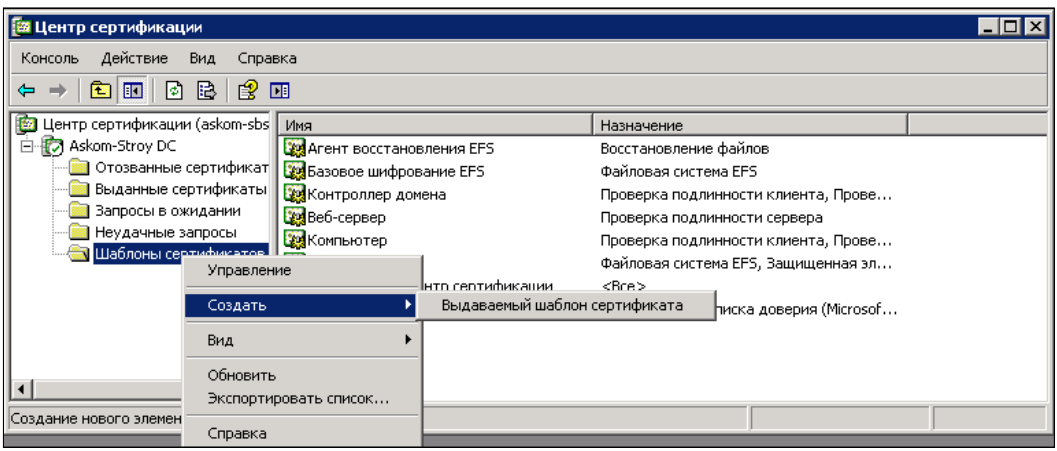


Рис. 9.7. Публикация шаблона сертификата RADIUS-сервера. Для использования в протоколе 802.1*x* аутентификации на основе сертификатов сервер IAS должен получить специальный сертификат, который по умолчанию не опубликован в Центре сертификации

Настройка службы каталогов

При подключении по протоколу 802.1*x* аутентифицироваться могут как компьютеры (их учетные записи в домене), так и сами пользователи. Политики подключения

RADIUS-сервера проверяют членство соответствующих учетных записей в группах безопасности. Поэтому для предоставления права доступа создайте в службе каталогов соответствующие группы безопасности и включите в них требуемые объекты.

Кроме того, не забудьте включить опцию разрешения входящих звонков для соответствующих учетных записей (в том числе и компьютеров).

Настройка службы RADIUS

Компьютер со службой IAS (реализация службы RADIUS в Windows) должен входить в специальную группу безопасности домена, чтобы иметь доступ к параметрам учетных записей. Эта операция выполняется путем авторизации службы в ее меню.

Настройка компьютера с IAS предполагает настройку *клиентов* и создание *политик удаленного доступа*.

Клиент — это коммутатор, который запрашивает у сервера RADIUS разрешения на включение порта. Каждый клиент должен быть зарегистрирован на RADIUS-сервере. Для этого необходимо ввести его IP-адрес и ключ. *Ключ* — это пароль, который должен быть одинаковым в настройках IAS и клиента. Рекомендуется для каждого клиента выбирать его уникальным и достаточно сложным — длиной более 20 символов; ключ вводится всего в двух конфигурациях и практически не меняется в процессе работы.

Возможность получения клиентом аутентификации от службы IAS всецело определяется *политиками удаленного доступа*. Обычно таких политик достаточно много (для различных вариантов подключения); они просматриваются по очереди, пока запрос клиента не совпадет с какой-либо из них.

Политику удаленного доступа следует создавать при помощи мастера создания политик, указывая вариант Ethernet и вводя на запрос о группах Windows названия групп, которым предоставлено право доступа.

В результате служба IAS будет проверять членство компьютера или пользователя в соответствующей группе. Если проверка выполнится успешно, то коммутатор получит соответствующее разрешение на открытие порта.

Настройка автоматического назначения VLAN для порта коммутатора

Многие коммутаторы имеют возможность назначить порт в тот или иной VLAN в соответствии с данными аутентификации. Для этого данные от службы IAS должны возвращать соответствующие параметры. Покажем, как это сделать.

После создания политики удаленного доступа откройте ее свойства и нажмите клавишу редактирования профиля. Выберите вкладку **Дополнительно** (рис. 9.8) и добавьте следующие три атрибута:

- 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 в случае удачной аутентификации (на рисунке выбрана VLAN с номером 20);
- Tunnel-Type со значением Virtual LANs.

При получении запроса служба последовательно проверит соответствие его данных имеющимся политикам удаленного доступа и возвратит первое удачное совпадение или отказ.

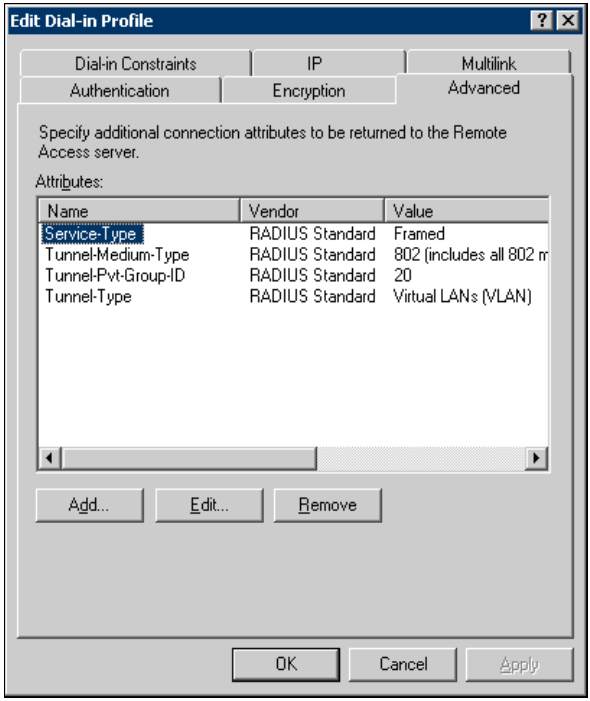


Рис. 9.8. Настройка атрибутов, используемых для автоматического назначения порта коммутатора в VLAN

Настройка клиентского компьютера

Для использования протокола 802.1*x* при подключении к локальной сети на компьютере должна быть запущена служба **Беспроводная настройка**. Только в этом случае в свойствах сетевого подключения появится третья вкладка, определяющая настройки протокола 802.1*x* (рис. 9.9). По умолчанию настройки предполагают использование для аутентификации именно сертификатов, так что никаких изменений данных параметров не требуется.

> ***Совет***
>
> Проще всего настроить данную службу на режим автоматического запуска с использованием групповой политики. Для этого следует открыть **Конфигурация компьютера** | **Конфигурация Windows** | **Параметры безопасности** | **Системные службы** и указать для службы **Беспроводная настройка** вариант автоматического запуска.

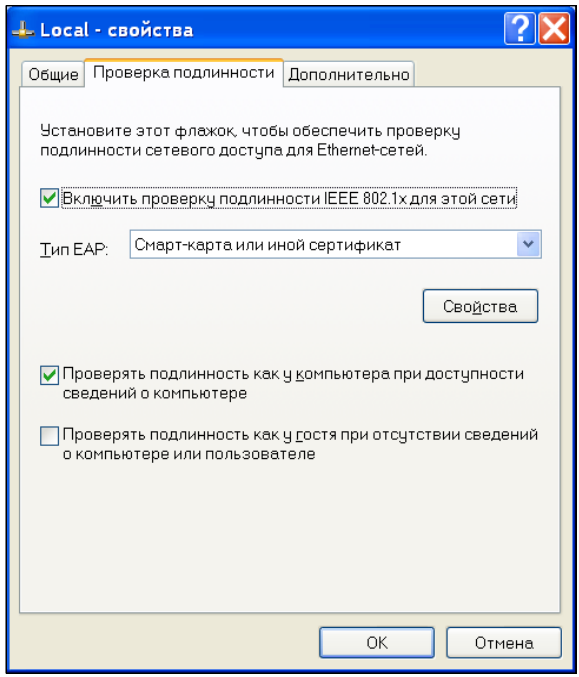


Рис. 9.9. Окно настройки протокола 802.1*x* на клиенте

Следующим шагом необходимо проверить наличие сертификата, на основании которого предполагается осуществить открытие порта коммутатора. Для этого нужно открыть консоль управления сертификатами, обратив внимание на выбор правильного контейнера для просмотра. Так, если предполагается аутентифицировать компьютер, следует просматривать контейнер **Локальный компьютер**.

Настройка коммутатора

Настройки коммутаторов отличаются для различных вендоров. Приведем в качестве примера вариант настройки коммутатора Cisco.

В данном примере использованы настройки по умолчанию для портов службы RADIUS, не включены параметры повторной аутентификации и некоторые другие. Кроме того, в качестве гостевой VLAN (в нее будет помещен порт, если устройство не поддерживает протокол 802.1*x*) определена VLAN с номером 200, а в случае неудачной аутентификации устройство будет работать в VLAN с номером 201.

Сначала в конфигурации коммутатора создается новая модель аутентификации, указывающая на использование службы RADIUS:

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

Далее включается режим использования протокола 802.1*x* и определяются параметры RADIUS-сервера:

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

После чего для каждого интерфейса настраивается использование протокола 802.1*x*. В качестве примера выбран порт номер 11:

```
interface GigabitEthernet0/11
 switchport mode access
dot1x port-control auto
dot1x guest-vlan 200
 dot1x auth-fail vlan 201
```

Этих настроек достаточно, чтобы использовать на коммутаторе аутентификацию по протоколу 802.1*x*.

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 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 802.1x;
- 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.

Как уже говорилось, технологии Cisco/Microsoft не являются единственными вариантами решений. На рис. 9.10 представлено сообщение, которое получает пользователь от системы безопасного доступа к сети, реализованной на оборудовании Nortel: программа предлагает посетить указанный сайт и установить отсутствующее программное обеспечение.

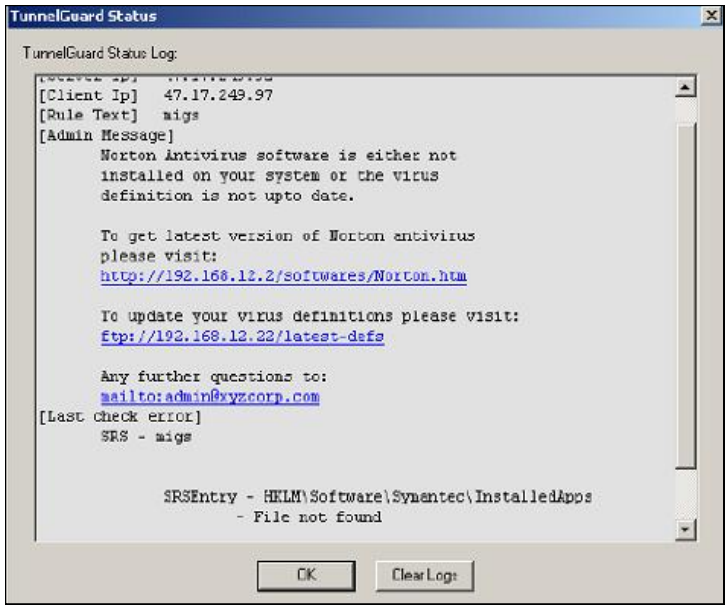


Рис. 9.10. Сообщение системы безопасного доступа о действиях, требуемых от пользователя для подключения к сети

Примечание

Сходная технология ограничения была предусмотрена в Windows 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.

За подробностями внедрения NAP мы отошлем читателя на сайт разработчика — страницу Networking and Access Technologies (**http://technet.microsoft.com/en-us/network/bb545879**).

Обнаружение нештатной сетевой активности

Вирусная эпидемия или атака на информационную систему не возникают "вдруг". Обычно существует некий период, который характеризуется повышенной нештатной сетевой активностью. Периодический анализ файлов протоколов систем и ис-

пользование тех или иных *обнаружителей сетевых атак* могут предупредить администратора и дать возможность предпринять встречные шаги.

Хотя профессиональные программы, предназначенные для обнаружения сетевых атак, достаточно дороги, требуют высокого уровня знаний от администратора и обычно не используются в малых и средних предприятиях, администраторы легко могут найти в Сети пакеты, которые позволяют прослушивать активность на TCP/IP-портах системы. Сам факт обнаружения активности на нестандартных портах уже может быть свидетельством нештатного поведения системы, а наличие сетевого трафика в неожидаемые периоды времени может косвенно свидетельствовать о "работе" троянов.

Отмечу несколько бесплатных программ, которые часто применяются для сканирования сети:

- nmap (**http://www.insecure.org/nmap/**, версии для Windows и Linux);
- Nessus (**http://www.nessus.org**, Linux-версии);
- NSAT (**http://sourceforge.net/projects/nsat/**, Linux-системы).

Следует отметить, что преобладание Linux-версий объясняется большими возможностями настройки данной операционной системы на низком уровне по сравнению с Windows-вариантами.

Контроль состояния программной среды серверов и станций

При эксплуатации системы администратор должен быть уверен в том, что на серверах и рабочих станциях отсутствуют известные уязвимости и что установленное программное обеспечение выполняет свои функции без наличия каких-либо закладок, недокументированных обменов данными и т. п. Понятно, что собственными силами проверить это невозможно, поэтому мы вынуждены доверять изготовителям программ и обеспечивать со своей стороны идентичность используемого комплекта ПО оригинальному дистрибутиву.

Индивидуальная настройка серверов

Типовая конфигурация операционной системы после стандартной установки "из коробки" позволяет сразу использовать систему в производственной деятельности. При этом в подавляющем большинстве случаев система содержит *излишние функции* и дополнительные компоненты в целях совместимости с эксплуатируемыми станциями, которые целесообразно отключить в целях повышения безопасности. Каждая избыточная функция — это дополнительный код, который может содержать потенциальные ошибки, может использоваться для проникновения в систему и т. п. Как правило, следует отключить запуск служб системы, не используемых в конкретной конфигурации, и настроить параметры безопасности (протоколы аутентификации, уровень предоставления информации анонимному пользователю и т. п.) по максимально возможному уровню с учетом специфики информационной

системы. Такие настройки индивидуальны для каждого случая применения 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 можно легко найти на сайтах разработчиков программного обеспечения по ключевым словам "hardening" или "security guide". В подобных руководствах 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 ревизовать предлагаемые к назначению настройки. Поэтому данный мастер следует рассматривать только как первый шаг настройки сервера.

Security Compliance Manager

Microsoft разработал 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/Windows 7/Windows 2008; продукт требует сервера базы данных (бесплатная версия может быть загружена и настроена в процессе установки утилиты).

> ***Совет***
>
> При установке продукта необходимо наличие подключения к Интернету: возможно, придется загрузить SQL Server Express. Кроме того, после установки продукт загружает с сайта Microsoft последние версии рекомендуемых параметров безопасности.

Microsoft подготовил рекомендуемые параметры настроек безопасности для систем, предназначенных для эксплуатации в типовых условиях, в условиях предприятия и для организаций с повышенным уровнем безопасности. Эти рекомендации представляют собой набор рекомендуемых параметров групповой политики для рабочих станций (Windows XP/Vista/Windows 7) и серверов (Windows Server 2003/2008). Обычно в конкретных условиях применить все рекомендации невозможно: например, какие-то компоненты, рекомендуемые для отключения, пред-

полагается 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.

Исключение уязвимостей программного обеспечения

Ошибки находят во всех операционных системах, они свойственны как самим операционным системам, так и прикладному программному обеспечению. Уязвимость в программном обеспечении потенциально позволяет злоумышленнику получить доступ к данным в обход защиты. Поэтому установка обновлений является одним из наиболее критических элементов системы безопасности, причем администратору необходимо следить не только за обнаружением уязвимостей в операционной системе, но и быть в курсе обновлений *всего установленного* программного обеспечения.

> ***Примечание***
>
> Исторически существуют различные названия обновлений: *заплатки* (Hot fix), которые обычно выпускаются после обнаружения новой уязвимости, *сервис-паки* (service pack), в которые включается не только большинство реализованных ко времени выпуска сервис-пака заплат, но и некоторые усовершенствования и дополнения основных программ и т. п. В данном контексте для нас не актуальны эти различия.

Использование эксплойтов

Уязвимости обнаруживаются постоянно, причем далеко не всегда — даже по критическим ошибкам — оперативно выпускаются нужные заплатки. При этом для того, чтобы воспользоваться уязвимостью, не надо быть "крутым" специалистом. Найти специальную программа (ее принято называть *exploit*), которая реализует эту уязвимость, в эпоху глобальных компьютерных сетей не представляет особого труда. В результате обычный пользователь получает инструмент, позволяющий ему, например, повысить свои права до уровня администратора или "свалить" сервер предприятия (рис. 9.11). Можно рассуждать о причинах такого поведения, но автору неоднократно приходилось сталкиваться с наличием подобного пользовательского интереса.

Информация о найденных уязвимостях тщательно скрывается до момента выпуска исправлений программного кода. Однако этот факт не гарантирует наличие прорех в защите систем, которые уже начали эксплуатироваться злоумышленниками.

Поэтому своевременная установка заплат является необходимым, но не достаточным средством мер обеспечения безопасности данных.

Как узнать об обновлениях

Информация об обнаруженных уязвимостях публикуется на специализированных сайтах, адреса которых перечислены в этой главе ранее в *разд. "Интернет-ресурсы, посвященные безопасности"*. Понятно, что просматривать оперативную информацию о событиях безопасности ежедневно практически нереально, поэтому целесообразно подписаться на существующие рассылки.

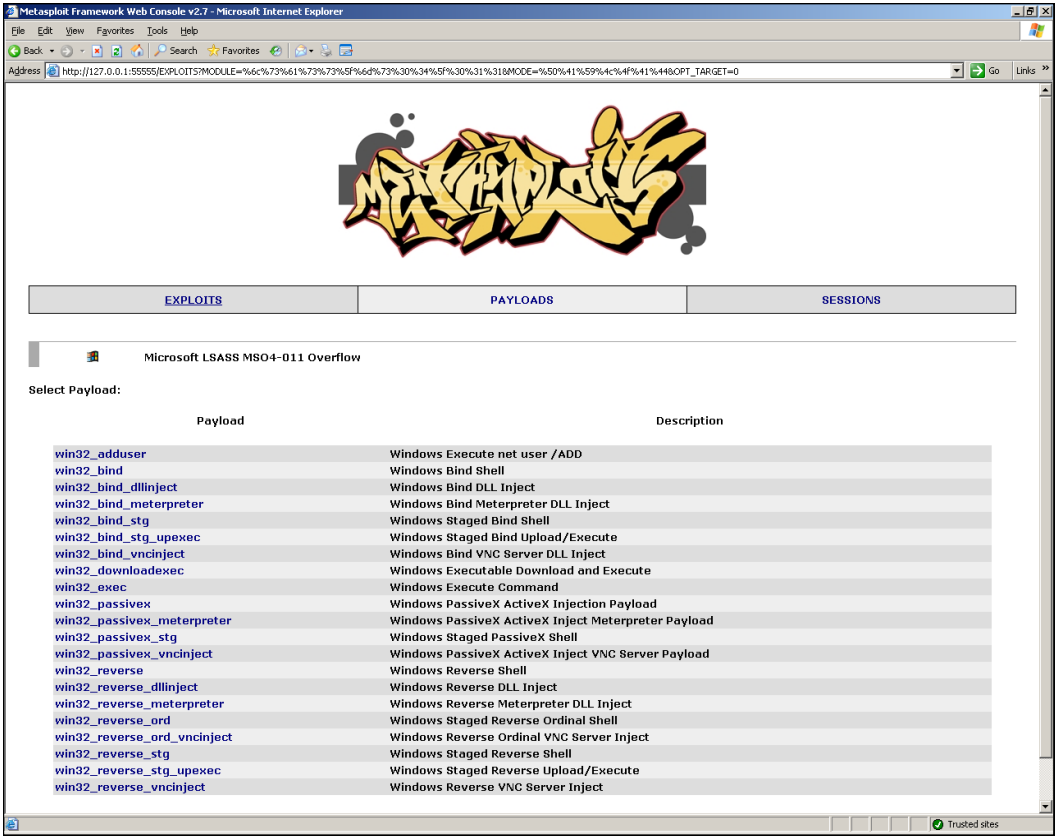


Рис. 9.11. Программа Metasploit предназначена для осуществления атак на компьютеры. Воспользоваться уязвимостью пользователь может, найдя в Интернете соответствующий эксплойт. Дальнейшие его действия будут заключаться только в выборе варианта вторжения на чужой компьютер

Ни в коем случае не следует доверять письмам электронной почты, советующим срочно установить то или иное обновление и часто содержащим "файл исправлений". Такие письма обычно являются фальсификацией.

Если у администратора появляется задача проанализировать какой-либо компьютер (или группу) на полноту установки обновлений безопасности, то самый простой способ — это загрузить с сайта Microsoft утилиту Microsoft Baseline Security Analyzer (MBSA, домашняя страница **http://technet.microsoft.com/en-us/security/cc184923**). Утилита MBSA позволяет выполнить анализ компьютеров в организации (локального, удаленной системы или целой подсети) на наличие установленных обновлений безопасности и сформировать некоторые советы по повышению уровня защищенности систем рис. 9.12. Для анализа используются актуальные данные, загружаемые с сайта изготовителя (список актуальных обновлений с сервера Microsoft; поэтому для сканирования необходимо подключение к Интернету, хотя загруженный каталог обновлений можно потом перенести вручную на другой, автономный компьютер).

Рис. 9.12. Результаты анализа системы с использованием MBSA

Существуют бесплатные средства проверки полноты установки обновлений и от других разработчиков. Если нужно проверить только один компьютер, то удобно воспользоваться Windows Vulnerability Scanner (**http://www.pspl.com/download/winvulscan.htm**) — утилитой объемом менее 1 Мбайт, которая проверит состав установленных обновлений Microsoft. По результатам тестирования будет сформирован список отсутствующих обновлений, причем щелчок по номеру бюллетеня

безопасности откроет в обозревателе Интернета страницу, с которой можно загрузить соответствующий патч (рис. 9.13).

Эта программа удобна для анализа автономных компьютеров, поскольку содержит в себе список выпущенных патчей; очевидно, что она нуждается в периодическом обновлении с сайта изготовителя. Из неудобств работы я бы отметил то, что программа отображает больший список требуемых обновлений, чем детектируются средствами Microsoft (утилита не учитывает в некоторых случаях поглощение одних патчей другими).

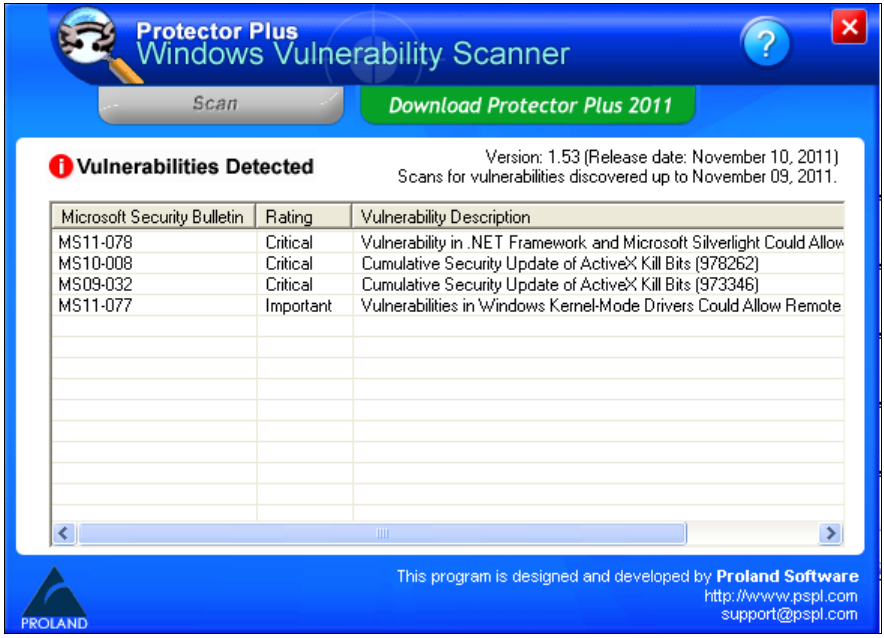


Рис. 9.13. Программа *Windows Vulnerability Scanner* отображает список обновлений, которые необходимо установить на компьютер

Администратор может воспользоваться и любой программой, предназначенной для анализа безопасности компьютерных систем. Сегодня выбор на рынке подобных продуктов довольно разнообразен. Как правило, программы сканирования уязвимостей выполняют типовые операции: проверяют наличие уязвимостей по имеющейся у них базе, сканируют IP-порты, проверяют ответы на типовые HTTP-запросы и т. д. По итогам таких операций формируется отчет, предоставляемый администраторам, и приводятся рекомендации по устранению уязвимостей. На рис. 9.14 представлено окно одной из подобных программ — XSpider (**http://www.xspider.ru/**).

Примечание

При тестировании информационной системы с помощью подобных программ следует проявлять особую осторожность. Во-первых, при тестировании резко повышается нагрузка на сеть. Во-вторых, отдельные тесты могут привести к аварийному завершению работы компьютеров.

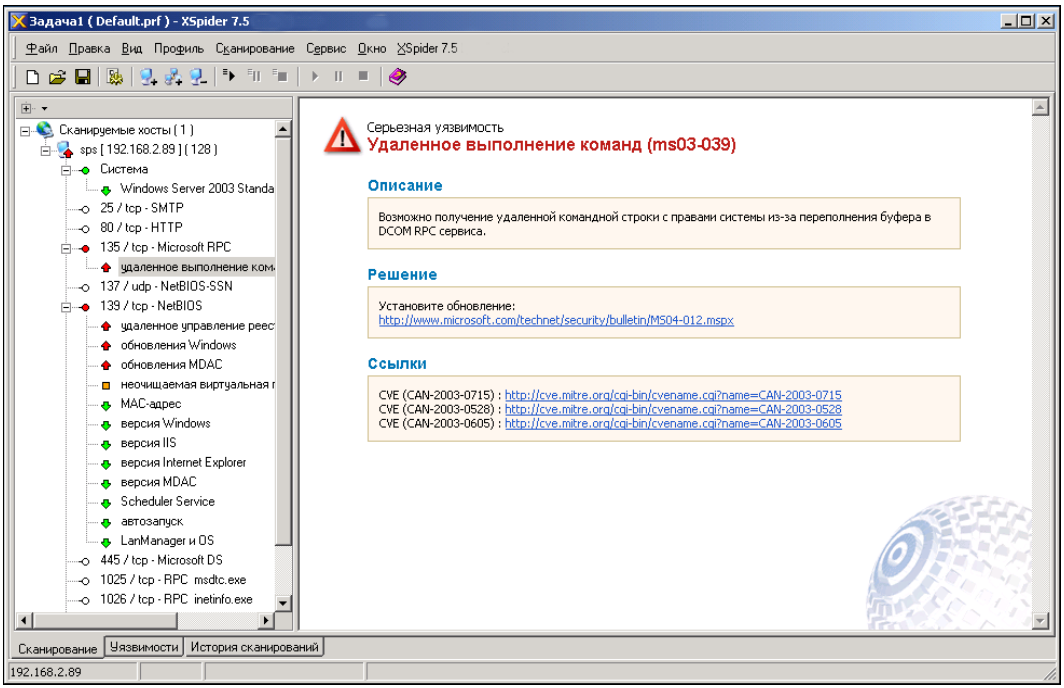


Рис. 9.14. Программа *XSpider* провела тестирование системы и обнаружила уязвимости

Тестирование

К сожалению, сами обновления нередко становятся причиной ошибок в работе компьютерной системы. Те, кто более или менее периодически знакомится с конференциями по программным продуктам, наверняка помнят пики эмоций, когда после установки очередного сервис-пака система просто переставала работать. Автору неоднократно приходилось сталкиваться с ситуациями, когда установка обновлений приводила к сбоям системы, причем часто проблемы возникали не сразу, а уже в процессе эксплуатации, когда сбой в работе системы становился критичным для обеспечения бизнес-процессов организации.

Поэтому администратор поставлен перед дилеммой: применять обновление и рисковать стабильностью работы системы или не ставить и ждать, что атака злоумышленника минует компьютеры небольшой и незаметной организации.

Разработчики программного обеспечения советуют в обязательном порядке тестировать все устанавливаемые на рабочие компьютеры обновления. Тестирование должно проводиться в типовой для данной организации конфигурации для каждой версии операционной системы. Администратору следует самостоятельно определить, выполнение каких функций необходимо проверить после обновления. Понятно, что полностью протестировать систему после установки обновлений в условиях малой или средней организации практически нереально, но проверить хотя бы возможность загрузки компьютера и правильность выполнения основных бизнес-процессов — вполне возможно.

Совет

Ставьте полученные обновления сначала на неосновные компьютеры, в частности, попробуйте провести эту операцию на своей машине. И, конечно, заранее продумайте, как вы будете восстанавливать систему в случае ее краха. Например, есть ли у вас актуальные файлы резервной копии и насколько будет нарушено функционирование организации, если такое восстановление придется проводить сразу после применения обновления?

Обновления операционных систем Linux

Современные операционные системы Linux поддерживаются выпуском заплат на обнаруженные уязвимости. Этот процесс можно автоматизировать (запускать обновления по графику с использованием демона cron) или же устанавливать обновления вручную.

Операции выполняются по правилам соответствующей версии операционной системы. Например, для операционной системы Ubuntu ручное обновление выполняется двумя командами:

```
# apt-get update
# apt-get upgrade
```

Первая команда обновляет локальный список информации о пакетах, вторая — устанавливает новые версии пакетов.

В отличие от Windows-систем при установке обновлений на серверы Linux (без графической подсистемы) крайне редко требуется перезагрузка.

Для обновления рабочих станций Linux используются мастера операций (в графическом режиме), автоматически запускаемые в случае обнаружения исправлений.

Индивидуальные обновления Windows-систем

Примечание

Службы WSUS не поддерживают следующие продукты: Visual Studio 2002 или Visual Studio 2003, Report Viewer 2005 или Report Viewer 2008, Platform SDK: GDI+, Компоненты Office 2003, Office 2007 и Office 2010, все продукты Macintosh, MSN Messenger, Windows Live Messenger.

Обновления для Windows-систем публикуются службой Microsoft Update на серверах Microsoft (**http://www.update.microsoft.com/microsoftupdate**). На этой странице можно выполнить ручное сканирование систем Windows XP/2003 на наличие уязвимостей и установить необходимые пакеты. Для Windows 7/2008 нужно воспользоваться Центром обновления системы, который проверит наличие обновлений, поможет выбрать и установить нужные.

При установке систем одной из рекомендаций является настройка режима работы службы обновлений. Для индивидуальных рабочих мест можно выбрать вариант автоматической загрузки и установки обновлений (рис. 9.15).

Для серверов режим автоматической установки не является оптимальным. Поскольку сервер обычно достаточно плотно используется: в рабочее время обслужи-

вает пользователей, ночью выполняются сервисные операции. Поэтому незапланированная операция перезагрузки может быть нежелательна. Вследствие этого лично я советую выполнять установку обновлений только в ручном режиме, под контролем оператора сервера

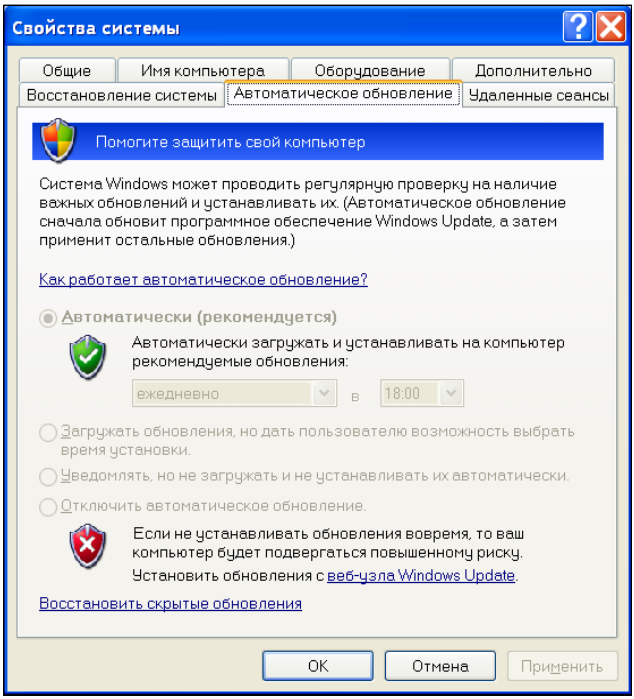


Рис. 9.15. Включение режима автоматических обновлений

Организация обновлений Windows-систем на предприятии

Обновление систем на предприятии имеет несколько особенностей.

Во-первых, обновления от Microsoft часто весьма объемны по размеру и их одновременная загрузка на несколько систем может негативно сказаться на доступе в Интернет даже на безлимитных тарифах, не говоря уже про экономию для тарифов с оплатой за трафик.

Во-вторых, установка обновлений в организации должна быть контролируемой: обновления должны авторизоваться (получать разрешение от администратора на установку, лучше всего — после тестирования), операции нужно проводить по графику, с учетом типа компьютеров (отбор по группам, площадкам и т. п.), весь процесс должен протоколироваться с возможностью легкого составления отчетов по результатам.

В этих целях целесообразно использовать *службу автоматического обновления* — Windows Software Update Services (WSUS). Она распространяется бесплатно и предназначена для установки как обновлений операционной системы Windows, так и ряда продуктов Microsoft.

Страница с описаниями службы находится по адресу **http://technet.microsoft.com/en-us/windowsserver/bb332157**. С этой страницы можно перейти на ссылку, по которой установочный пакет может быть загружен для серверов Windows 2003. Для Windows 2008 Server служба WSUS является дополнительной ролью, устанавливаемой в диспетчере сервера. Однако для того, чтобы эта роль появилась в списке доступных ролей, необходимо установить на сервер дополнение, описанное в документе **http://support.microsoft.com/kb/940518**.

Сама служба представляет собой приложение, работающее на веб-сервере IIS. Поэтому для ее установки необходимо выполнить ряд условий (установить компоненты). Установка компонент выполняется мастером в Windows 2008 Server (рис. 9.16), но в случае Windows 2003 Server подготовительные операции следует выполнить в соответствии с инструкцией по установке (доступна на домашней странице продукта).

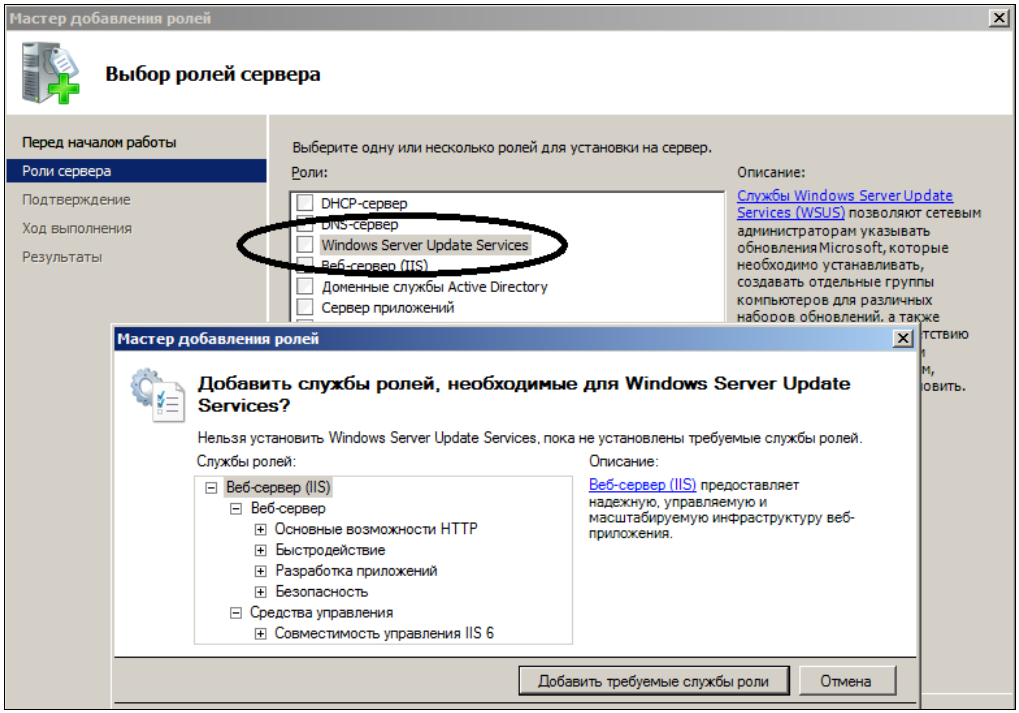


Рис. 9.16. Установка роли WSUS на сервере Windows 2008

Архитектуру обновления можно построить по нуждам организации: служба допускает виртуализацию, каскадирование (загрузка обновления с другого сервера WSUS), балансировку нагрузки (обслуживание инфраструктуры несколькими серверами) и т. п.

Основные настройки службы (параметры прокси-сервера, выбор продуктов, для которых закачиваются обновления, настройка языков, графика синхронизации и т. д.) выполняются во время установки продукта, но их можно уточнить и в консоли службы (рис. 9.17).

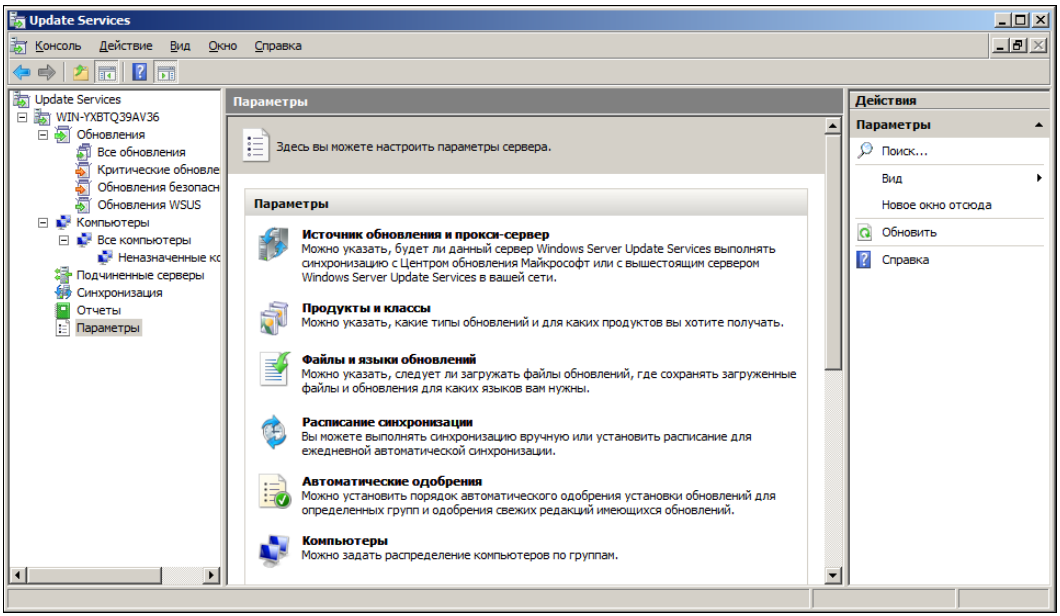


Рис. 9.17. Консоль управления WSUS (настройка параметров)

После установки компьютеры необходимо разбить по группам (в зависимости от требований к установке обновлений) и настроить режимы (например, автоматическое согласие на установку определенной категории обновлений и т. п.).

Чтобы клиенты выполняли установку обновлений с сервера WSUS, надо в групповой политике явно указать имя сервера, с которого будет осуществляться обновление.

> ***Примечание***
>
> Для индивидуальной настройки системы на локальный сервер WSUS (если компьютер не использует групповые политики) следует добавить в ветвь `HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate` реестра клиентской системы два ключа: `WUServer` (тип `Reg_SZ`) и `WUStatusServer` (тип `Reg_SZ`). Оба они должны указывать на внутренний WSUS-сервер (например, **http://wsus**).

Обновление ПО с использованием специализированных средств

Существуют специализированные продукты для управления программными продуктами. Microsoft для управления ИТ-системами разработала System Center (SC), который может быть использован и для разворачивания обновлений. Преимуществом SC является то, что его можно использовать для установки обновлений *любого ПО*, а не только обновлений системы, критичных для ее безопасности, или MS Office.

Поскольку SC ведет инвентаризацию аппаратной составляющей и программного обеспечения компьютеров, то администратор получает возможность практически

индивидуальной настройки обновлений (например, учитывая версии установленного ПО, наличие свободного места на диске и т. п.) с последующим анализом операций в удобной форме отчетов.

Установка обновлений через групповые политики

Обновления можно устанавливать с помощью групповых политик. К такому способу можно прибегнуть, например, при необходимости срочного разворачивания заплатки.

Специально для автоматизации установки обновления выпускаются в MSI-формате. Загрузив файл обновления, его следует распаковать в папку на локальном диске, запустив с ключом `-x`. Затем, используя программу редактирования групповой политики, можно создать пакет установки, импортировав msi-файл из этой папки. Единственное неудобство данного решения — необходимость создания различных политик, учитывающих установленную версию операционной системы и программ MS Office. Поскольку в малых и средних организациях обычно придерживаются однотипности устанавливаемого ПО, то подобные действия не должны вызвать затруднений администратора.

Защита от вредоносных программ

Попытки доступа к информации (с целью кражи, уничтожения и т. п.) обычно совершаются с помощью установки на компьютер какой-либо программы. Способов установки настолько много и они зачастую так замаскированы, что для исключения подобных ситуаций создан специальный класс программ — программ защиты хоста.

Эти программы позволяют предупредить запуск вредоносного кода (антивирусный компонент), исключить невидимую установку в систему кодов, которые могут красть данные или выполнять иные задачи (трояны, руткиты — объединяют термином *malware*-программы от английских терминов *malicious software*). Обычно в такие продукты также включены средства контроля оборудования и программ, предупреждения вторжений (контроль сетевого трафика) и другие функции.

На рис. 9.18 представлена программа Symantec Endpoint Protection, которая помимо функций антивирусной защиты включает современный межсетевой экран и средства обнаружения атак и вторжений. Программа способна обнаруживать клавиатурные шпионы; блокировать хосты, осуществляющие атаки; маскировать операционную систему (подменять типовые ответы на контрольные пакеты IP). В ней содержатся опции, включавшиеся ранее только в специализированные программы, например, защита от подмены MAC-адреса, интеллектуальный контроль протоколов DHCP, DNS, обнаружение руткитов и т. д.

Особенности эксплуатации антивирусных программ

Индивидуальные версии антивирусных программ целесообразно использовать только в очень малых сетях. Корпоративные решения позволяют администратору

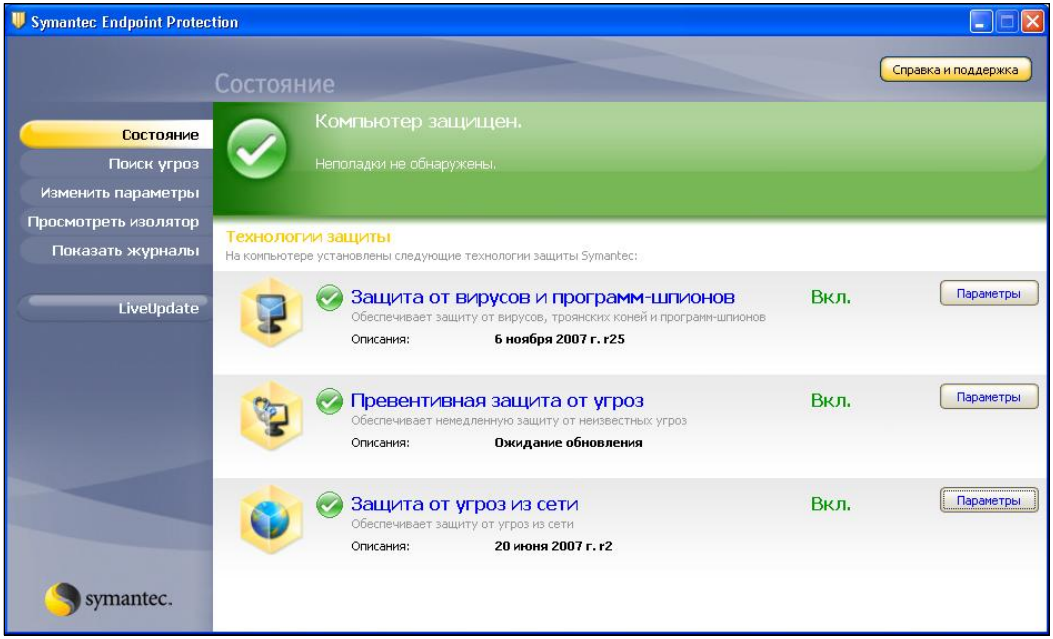


Рис. 9.18. Интерфейс программы *Symantec Endpoint Protection*

настроить единые правила защиты (например, профили для работы в локальной сети и в публичной с автоматическим переключением при смене места нахождения и т. п.), снизить объем загружаемых обновлений (обновления будут получены из Интернета только один раз, а потом просто распространены по локальной сети), централизованно настроить опции антивирусной защиты (например, установить частоту загрузки обновлений, исключить из проверки некоторые типы файлов и т. п.), получать статистические данные по пользовательским системам и т. п.

Следует особо тщательно подходить к выбору программ, предназначенных для антивирусной защиты контроллеров домена, почтовых и других серверов — часть файлов в таких системах должна быть исключена из проверки. При этом некорректная настройка антивирусной защиты может не только снизить производительность системы, но даже и нарушить ее функционирование. Общие рекомендации по исключаемым из проверки папкам и типам файлов можно почерпнуть из KB822158 (**http://support.microsoft.com/kb/822158**). Но следует иметь в виду, что, например, для большинства серверных продуктов Microsoft есть рекомендации по настройке антивирусных программ (например, для Team Foundation Server 2010 и Team Foundation Server Proxy 2010 — **http://support.microsoft.com/kb/2636507**, для кластеров — **http://support.microsoft.com/kb/250355**, для Microsoft Forefront Client Security — **http://support.microsoft.com/kb/943556** и т. д.).

График обновлений баз

Опыт последних вирусных пандемий свидетельствует о том, что они достигают своего пика уже на второй, максимум третий день после начала распространения вирусов. Обновления антивирусных баз обычно появляются уже через несколько

часов после обнаружения вируса, поэтому в условиях сети организации имеет смысл настроить график обновлений несколько раз в сутки, например, каждые 4 часа. Если сеть организации изолирована и обновления баз приходится выполнять вручную (через перенос на носителе), то все равно, не следует делать эту операцию *реже одного раза в сутки*.

Внимательность пользователя

Уровень безопасности системы может быть существенно повышен, если пользователь в своих действиях будет учитывать потенциальную возможность заражения вирусом.

В условиях корпоративной среды от пользователя не должно требоваться специальных действий: администратор должен контролировать наличие антивирусной программы и актуальность установленных на компьютере пользователя баз описаний вирусов. Если нет полной уверенности в наличии такого контроля, то пользователь должен выполнять такую операцию самостоятельно. Обычно в этих целях достаточно просто следить за индикатором программы.

Поскольку основной путь распространения вирусов сегодня связан с электронной почтой, то желательно объяснить пользователю необходимость выполнения простейших правил:

- по умолчанию использовать оформление письма в виде "только текст" — неформатированное послание принципиально не может содержать никакого опасного кода;
- не открывать любые вложенные в письмо файлы. Если возникает необходимость отправки вложения, то следует предварительно письмом в формате "только текст" предупредить адресата о предстоящей отправке.

На чисто человеческих слабостях основывается еще один тип вирусов — *вирусы-мистификации*. Обычно это письма электронной почты, не содержащие никакого вируса, но составленные так, что мы сами отправляем их копии в несколько новых адресов. А способность к размножению — это основной признак вируса. Такое письмо может содержать, например, сведения о новом вредоносном вирусе, о котором следует срочно предупредить своих знакомых. Другой классический пример — приглашение поучаствовать в рекламной акции за какое-либо вознаграждение и т. п.

Лечение вирусов

Если компьютер поразил вирус, то следует сначала обновить базу данных антивирусной программы, если она установлена. В большинстве случаев после этого она сама сможет обезвредить вирус.

Некоторые вирусы блокируют запуск антивирусных программ (если вирус уже внедрился в систему с устаревшей базой данных о вирусах). В этом случае нужно постараться выяснить название вируса, загрузить утилиту, которая позволит устранить внесенные им в систему изменения, после чего можно будет загрузить обнов-

ления и выполнить полную проверку системы. Для установления имени вируса следует воспользоваться сканированием системы, например, с дискеты или посредством онлайнового антивирусного сервиса. Практически все крупные производители антивирусных продуктов создали подобные службы. Например, Symantec Security Check (**http://security.symantec.com/sscv6/default.asp?langid=ie&venid=sym**), Trend Micro (**http://housecall.trendmicro.com/housecall/start_corp.asp**), Panda (**http://www.pandasecurity.com/activescan/index/**) и т. д. При работе в составе локальной компьютерной сети можно воспользоваться также возможностью антивирусных программ осуществлять проверку сетевых ресурсов.

Если антивирусная программа не установлена, то следует первоначально провести проверку на вирусы, используя заведомо "чистое" программное обеспечение. Как правило, все антивирусные пакеты имеют версии программ для сканирования и лечения системы, которые можно запустить в режиме командной строки. Эти версии можно бесплатно загрузить с соответствующего сайта изготовителя. При проверке необходимо быть уверенным, что в памяти компьютера отсутствуют вирусы. Для этого система должна быть загружена, например, с заведомо чистой дискеты или с компакт-диска.

После ликвидации вирусов нужно установить антивирусную программу и обновить ее данные о вирусах.

Защита от вторжений

Антивирусные программы проверяют файлы, сохраняемые на носителях, контролируют почтовые отправления и т. п. Но они не могут предотвратить атак, базирующихся на уязвимостях служб компьютера. В таких случаях опасный код содержится в передаваемых по сети данных, он не хранится в файловой системе компьютера.

Программы защиты хоста включают и модули, контролирующие передаваемые по сети данные. Если такой модуль обнаруживает сигнатуру, которая применяется для атак с использованием ошибок операционной системы или прикладных программ, то он блокирует соответствующую передачу данных.

Так же как и антивирусные базы данных, состав этих сигнатур нуждается в постоянном обновлении с центрального сервера. Обычно обновление осуществляется единой операцией.

Программы-шпионы. "Троянские кони"

В Интернете широко распространена практика установки на компьютер пользователя определенных программ без его ведома. Иногда их действия просто надоедливы (например, перенаправление стартовой страницы обозревателя на определенные ресурсы Сети в целях рекламы последних), иногда такие программы собирают информацию с локального компьютера и отсылают ее в Сеть (например, о предпочтениях пользователя при посещениях сайтов или передача злоумышленнику данных, вводимых пользователем при работе с сайтами интернет-банков и т. п.).

Часть таких программ обнаруживается системами защиты, и их работа блокируется. Но многие программы не детектируются как вирусы, поскольку их действия часто идентичны типовым операциям пользователя. Обнаружить программы-трояны весьма сложно. Поэтому важно периодически осуществлять контроль запущенного на компьютере программного обеспечения.

Существует специальный класс программ, специализированных на поиске троянов. В качестве примера можно привести Ad-aware от компании LavaSoft, которую можно найти на сайте **http://www.lavasoftusa.com/**. Такие программы ориентированы на поиск следов троянов (ключей в реестре, записей на жестком диске и т. п.) и особенно полезны при выезде администратора в другую организацию для осуществления технической поддержки. Объем файлов установки позволяет быстро загрузить их из Сети и оперативно очистить компьютеры клиентов от вредоносных кодов в случае обнаружения непредвиденных действий и т. п.

В качестве превентивных мер можно рекомендовать чаще осуществлять проверку электронных подписей защищенных файлов системы, с помощью групповой политики повысить до максимума уровень безопасности офисных программ и обозревателя, разрешить выполнение только подписанных электронной подписью сценариев и т. п.

Поскольку администраторам достаточно часто приходится самостоятельно заниматься поиском троянских программ, опишем основные способы их автоматического запуска.

Вредоносный код может быть запущен, используя:

- файлы autoexec.bat, config.sys: вариант используется нечасто, поскольку новые операционные системы обычно не учитывают параметры этих файлов;
- файл win.ini: хотя этот файл сохраняется в целях обратной совместимости, но включение программ в строки `run` и `load` позволяет обеспечить их запуск системой;
- папку Автозагрузка для всех пользователей и профиля данного пользователя: достаточно просто проверить содержимое данной папки, чтобы обнаружить такую программу;
- ключи реестра, описывающие автоматически загружаемые программы[1]:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices
```

[1] Параметры `RunServices` и `RunServicesOnce` не используются в новых версиях ОС.

```
HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
```

Порядок загрузки программ из этих ключей следующий:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
<Logon Prompt>
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
StartUp Folder
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

Администратор домена через групповую политику при старте системы может отключить автоматический запуск программ, определенный в параметрах `Run` и `RunOnce`. Для этого используется ветвь **Конфигурация компьютера | Административные шаблоны | System | Logon |** с параметрами **Do not process...** и аналогичная ветвь для пользовательской части политики. Одновременно необходимые программы могут быть назначены для автозагрузки через параметр групповой политики. Эти значения записываются на компьютере в ветвях

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
```

- Browser Helper Object (BHO): в Windows имеется возможность встраивать в Internet Explorer специально разработанные программы, призванные расширить функциональность обозревателя. Поскольку данные программы имеют практически неограниченные права доступа к локальной системе, хакеры часто используют эту технологию для отслеживания действий пользователя, для показа рекламы или перенаправления на порносайты и т. п.

  Эти программы подключаются через ветвь реестра по их GUID

  ```
  HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
  Objects
  ```

  Поскольку среди таких программ присутствуют и "полезные" расширения, то при анализе системы необходимо найти в реестре программу, зарегистрировавшую данный GUID. Помочь в быстром поиске BHO могут такие утилиты, как HijackThis (**http://www.spywareinfo.com/~merijn/files/hijackthis.zip**);

- некоторые другие ключи, которые обычно не приводятся при описании возможных вариантов автозапуска программ, однако возможность использования которых также нельзя исключать:

  ```
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
  HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell
  ```

```
HKCU\Software\Policies\Microsoft\Windows\System\Scripts
HKLM\Software\Policies\Microsoft\Windows\System\Scripts
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
```

Примечание

Автору не раз приходилось сталкиваться с ситуациями, когда запуск вредоносного кода тщательно маскировался: зараженная программа создавала ничем не выделяющийся процесс, который и пытался активизировать собственно вирус. В подобных случаях помогут утилиты, отображающие иерархию процессов системы (рис. 9.19).

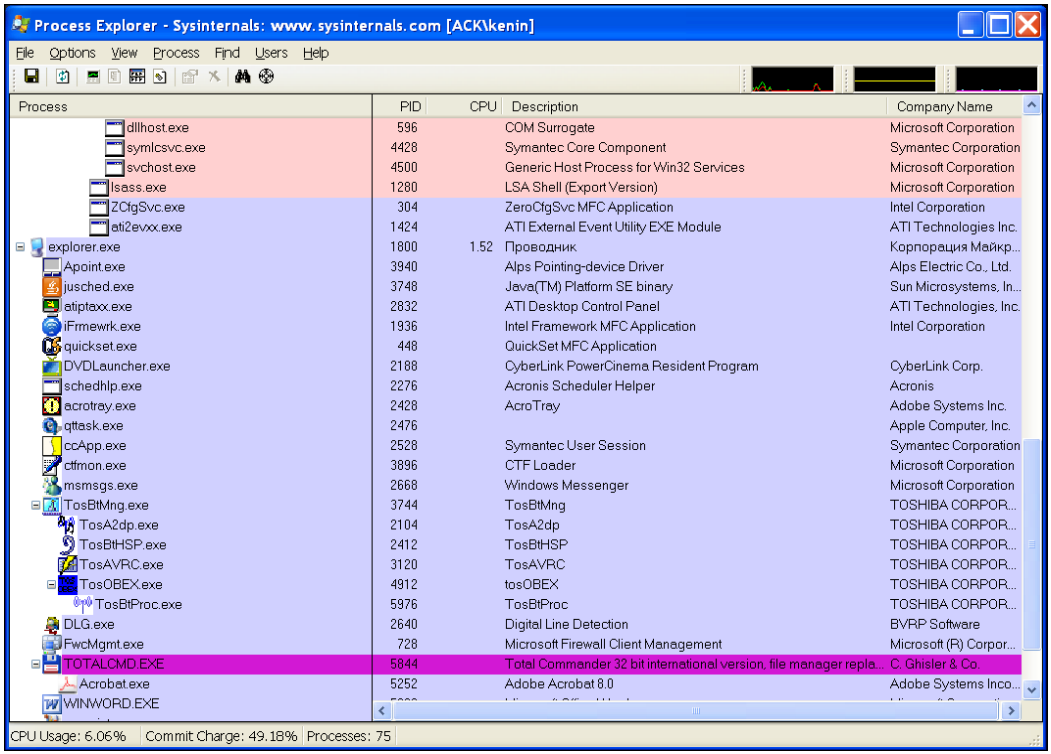


Рис. 9.19. Программа Process Explorer позволяет увидеть иерархию запущенных в системе процессов

- запуск программ через назначения в расписании: вариант запуска, легко обнаруживаемый простым просмотром назначенных заданий;
- ActiveX — вариант используется не так часто, поскольку в современных ОС для установки ActiveX требуется явное согласие пользователя при наличии у модуля электронной подписи. Кроме того, в любой момент можно просмотреть установленные модули (**Свойства обозревателя** | вкладка **Общие** | **Параметры** | кнопка **Просмотр объектов**) и удалить ненужные;
- службы и драйверы — установленный в виде нового драйвера или службы сторонний код обычно трудно обнаружить, поскольку пользователю системы необходимо точно знать собственную настройку и список драйверов устройств. На-

пример, таким способом устанавливалась одна из версий защиты компакт-диска от копирования. Кроме того, злоумышленники могут скрыть исполняемый код из отображаемых процессов системы, тем самым не давая повода сомневаться в надежности системы. Обнаружить такой код крайне сложно. Нужно использовать специализированные средства (если программа защиты хоста не блокирует код) по обнаружению руткитов, например, RootkitRevealer — **http://technet.microsoft.com/ru-ru/sysinternals/bb897445**.

Примечание

Руткит (rootkit) — это программа, использующая технологии маскировки своих файлов и процессов. Эта технология широко используется и не только злоумышленниками. Например, антивирусная программа (Kaspersky Antivirus) использует эту технологию для сокрытия своего присутствия при чтении NTFS-данных.

Генерация списка автозагружаемых программ

Список автоматически загружаемых программ можно редактировать при помощи утилиты msconfig (рис. 9.20). Программа показывает как элемент автозагрузки, так и путь его запуска и позволяет отключать загрузку элемента.

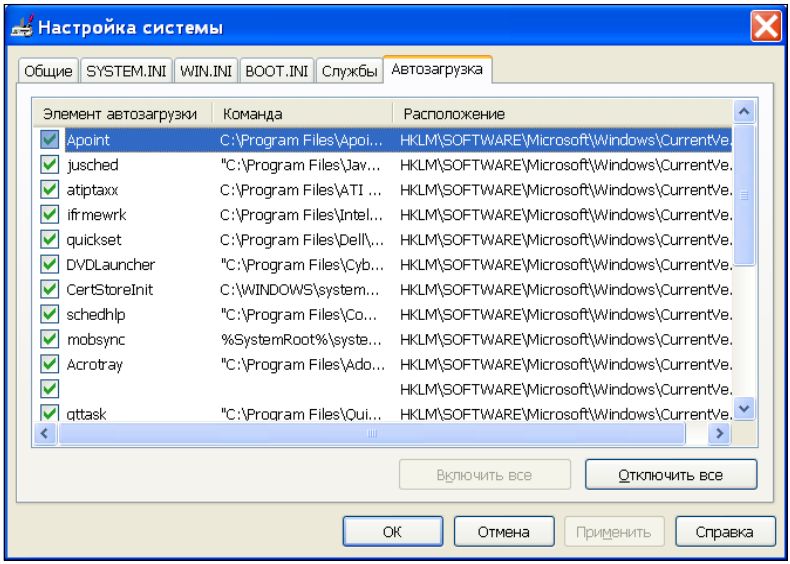


Рис. 9.20. Окно программы *msconfig*

Безопасность приложений

Сколь бы хорошо ни защищалась операционная система, сколь бы правильно ни были написаны фильтры и политики брандмауэров, но если прикладное программное обеспечение, или его уязвимости, позволят получить доступ к защищенным данным, то все предпринятые усилия окажутся напрасными. Примеры такого поведения программ легко можно найти в Интернете: в смартфоны встроены програм-

мы, мониторящие активность пользователя, клиент Skype позволяет принять вызов от человека, не входящего в список контактов (это означает, что из внешней сети есть доступ к локальному компьютеру с возможностью выполнения действий, не разрешенных пользователями) и т. п.

Прикладное ПО может явиться причиной утечки конфиденциальных данных не только из-за ошибок его разработки, но и просто благодаря недостаточному вниманию к документированным функциям. Так, файлы документов, подготовленные в программе Microsoft Word, кроме самого текста могут содержать и конфиденциальные данные, не предназначаемые для посторонних глаз: имена компьютера и пользователя, путь к сетевому принтеру, список редактировавших документ лиц, возможно, адреса их электронной почты и т. п. А если документ будет сохранен со включенными версиями или режимом исправлений, то партнер сможет проследить, например, позиции различных сотрудников по ценам, предлагаемым в документе, что отнюдь не будет способствовать принятию варианта, наиболее благоприятного для вашей организации.

Проконтролировать действия установленных программ практически невозможно. Наиболее рациональный выход — это использование ПО с открытым кодом, поскольку залогом его безопасности является независимая экспертиза. Но в силу объективных обстоятельств это возможно далеко не всегда. Поэтому следует придерживаться нескольких принципов:

- ограничьте минимумом количество программ, установленных на серверах и станциях;
- используйте средства контроля запуска программного обеспечения;
- исключите возможность передачи данных с серверов в сеть Интернета (заблокируйте, например, по их IP-адресам);
- по возможности, используйте программы анализа поведения.

Средства контроля запуска программного обеспечения

Во-первых, необходимо добиться, чтобы на предприятии существовал единый фонд дистрибутивов, чтобы все установки программ на рабочие станции и серверы выполнялись только из проверенного источника.

Во-вторых, необходимо включать средства контроля запуска программ. Максимально безопасный вариант — запретить запуск любых программ по умолчанию и создать исключения: те программы, которые необходимы для работы. Контроль запуска программ можно реализовывать через групповые политики (вариант описан в *главе 6*), но более тонкие настройки можно выполнить, применяя программы защиты хоста. На рис. 9.21 показан пример выбора параметров, которые можно использовать при формировании правил запуска в программе Symantec Endpoint Protection. При помощи использования подобных настроек — контроля доступа к параметрам реестра, к файлам и папкам, попыткам запуска или прекращения процесса, загрузки библиотек — можно очень точно настроить правила разрешения и блокирования.

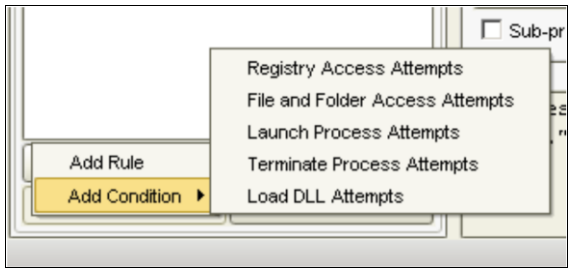


Рис. 9.21. Выбор критериев правил контроля запуска ПО

Неизменность системы

Одним из способов защиты системы от вредоносного кода является запрет на внесение изменений на локальный диск. Традиционный совет для тех, кто не хочет "подхватить" что-то в Интернете, заключается в загрузке с какого-либо LiveCD при путешествиях по Сети. Кстати, Microsoft подготовила специальную модификацию для Windows, 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 выбирать режимы сохранения изменений на локальный диск).

Защита от утечки данных

Во время работы компьютера доступ к информации контролируется средствами операционной системы и программного обеспечения. Порядок настройки прав доступа не представляет особой сложности и успешно реализуется администраторами. Но как только данные выходят из-под контроля операционной системы (например, компьютер выключается или данные переносятся на сменный носитель), то исключить их попадание в чужие руки крайне сложно.

Шифрование данных

Шифрование данных на сегодня является самым надежным способом обеспечения конфиденциальности информации.

Применение шифрования ограничено действующим законодательством (например, требуется лицензия, необходимо применять только сертифицированные алгоритмы шифрования и т. п.), но на практике существует и применяется много вариантов кодирования данных.

Шифрование данных на устройствах хранения

Примечание

При работе с зашифрованной информацией важно исключить утечку по другим каналам: например, через временные файлы, которые система создает при обработке данных, через электромагнитное излучение монитора, на котором воспроизведен текст и т. п.

Шифрование архивов

Самый простой способ, но далеко не самый надежный. Для многих архиваторов разработаны программы подбора паролей, и, учитывая склонность пользователей к простым вариантам, информация из архивов может быть получена за конечное время.

Нужно также учитывать, что коммерческие варианты архиваторов могут иметь инженерные пароли, с помощью которых соответствующие службы при необходимости прочтут данные.

Бесплатные программы шифрования данных

Существует несколько программ, которые позволяют шифровать данные с высокой степенью надежности. Можно отметить такие продукты, как SCARABAY (**http://www.alnichas.info/**, предназначена для шифрования личных данных и паролей), Crypt4Free (**http://www.secureaction.com/**, шифрует файлы на любых носителях, использует алгоритмы 128-битный DESX и 448-битный Blowfish) и др.

Я же хочу порекомендовать утилиту TrueCrypt (**http://www.truecrypt.org/**). Это бесплатное кроссплатформенное решение, версии которого есть для Windows 7/Windows XP, Mac OS, Linux). Косвенно качество программы подтверждает факт ее применения в вооруженных силах Израиля.

Утилита TrueCrypt создает виртуальный зашифрованный диск и монтирует его как реальный диск. Шифрование данных осуществляется в реальном режиме времени и не требует никаких дополнительных операций. При этом виртуальный зашифрованный диск может являться просто файлом на диске или сменном носителе компьютера или быть полностью преобразованным логическим диском (в том числе, и системным). Программа использует строгие алгоритмы (AES-256, Twofish и др.), для нее легко найти русификатор.

Среди особенностей программы отметим возможность создания скрытого тома (рис. 9.22).

Цель создания скрытого тома следующая. Вы можете попасть в такую ситуацию, что вынуждены будете раскрыть пароль зашифрованного диска (специалисты смогут найти обнаружить контейнер, используемый для хранения зашифрованной информации). Для такого случая TrueCrypt позволяет создать для одного контейнера *два* зашифрованных диска, доступ к которым осуществляется по различным паролям. Вы можете сообщить первый пароль и расшифровать диск, на котором будет ничего не значащая информация. Обнаружить на свободной части этого диска на-

личие зашифрованных данных *невозможно* — там будут просто случайные данные, шум.

Примечание

Скрытый том создается вторым этапом на свободном месте первого зашифрованного диска. Программа никак не может контролировать запись данных на это место при работе с первым диском. Поэтому сначала нужно создать "открытый" вариант зашифрованного диска, заполнить его некими данными, а потом на оставшемся свободном месте создать скрытый том. И больше не записывать данные на первый диск.

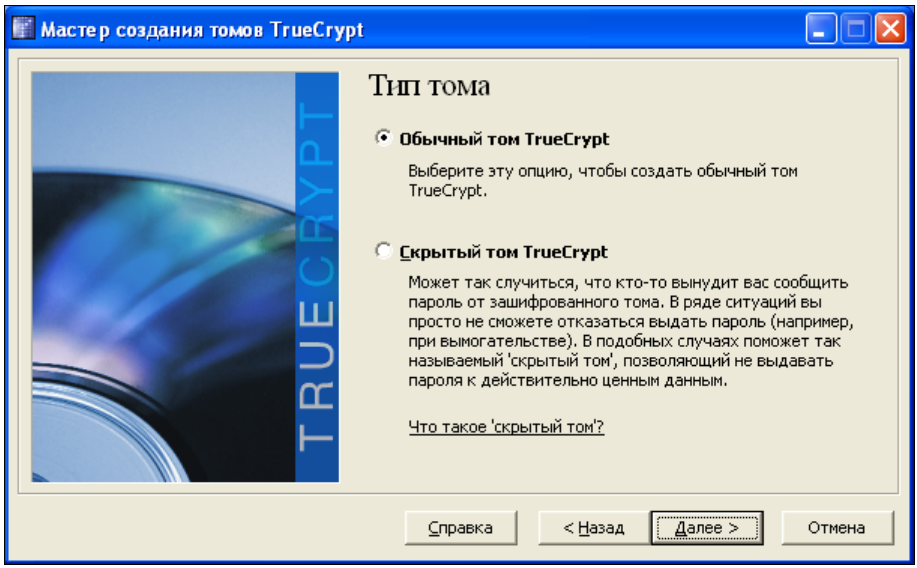


Рис. 9.22. Мастер создания скрытого тома

Максимум, чем вы рискуете в такой ситуации, так это потерей данных на скрытом томе, поскольку знающий о такой возможности специалист может дописать данные на первый диск и исключить возможность дешифрования скрытого тома.

Утилиту TrueCrypt можно использовать и без установки (переносной, portable, вариант). Для этого нужно только на этапе установки программы выбрать **Extract** на втором шаге и распаковать в нужную папку переносную версию.

Шифрование дисков: коммерческие программы

Существует достаточное количество программ сторонних фирм, позволяющих реализовать возможность шифрования *всего* диска. Например, PGP, которая позволяет не только шифровать диски, но и осуществлять безопасную переписку по электронной почте (рис. 9.23).

Можно упомянуть также программы: Private Disk компании Dekart, SafeGuard компании Utimaco (в том числе версии для мобильных компьютеров, смартфонов), DriveCrypt компании SecurStar и др.

Коммерческие программы отличаются обычно большим количеством возможностей. Среди основных можно упомянуть поддержку специализированных сменных устройств для хранения ключей шифрования, что повышает стойкость защиты. Например, можно использовать устройства eToken, в которых реализована защита ключей шифрования — ключ не может быть считан, устройство сообщает только результаты его проверки.

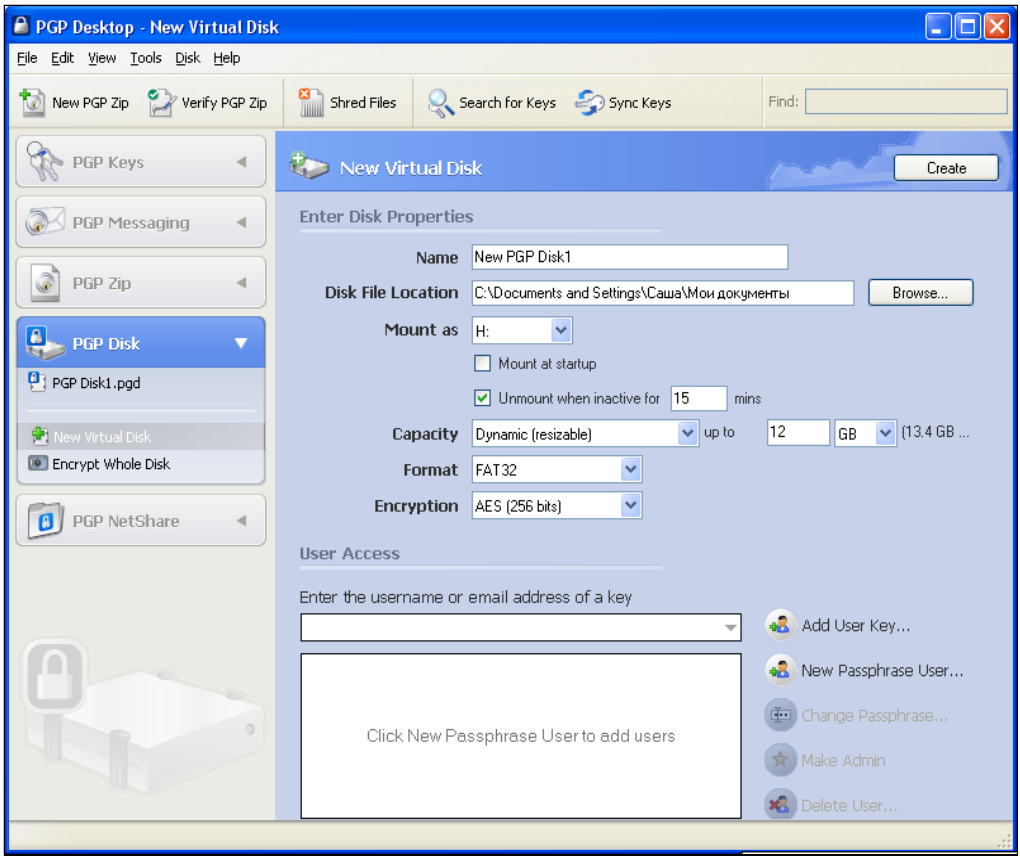


Рис. 9.23. Для создания зашифрованного диска в программе *PGP* достаточно определить только несколько параметров

Шифрование в Linux

Функции шифрования в Linux поддерживаются на уровне ядра операционной системы. В последних версиях, например, Ubuntu шифрование домашнего каталога предлагается в качестве выбора при установке операционной системы.

В случае необходимости шифрования всего диска и т. п. Соответствующие рекомендации легко найти в Сети (поиск по ключу *dm-crypt*).

Шифрование файловой системы Windows

Шифрование файлов присутствует в Windows, начиная с версии Windows 2000. Для этого диск компьютера должен быть отформатирован в файловой системе NTFS, а сам способ носит название *EFS* (Encrypted File System).

> ***Примечание***
>
> Ограничение, которое существует при шифровании файлов, — это невозможность одновременного сжатия файлов и их шифрования. Вы можете либо сжимать данные для экономии места на диске, либо шифровать их в целях обеспечения безопасности данных.

Зашифровать файл (или папку с файлами) можно следующим образом: выделить его в задаче Проводник (или в любом окне просмотра папок диска) и открыть меню **Свойства**. Далее на вкладке **Общие** нажать кнопку **Дополнительно** и в окне **Дополнительные атрибуты** установить флажок **Шифровать содержимое для защиты данных**. После подтверждения операции данные будут зашифрованы. Если вы сохранили настройку параметров интерфейса в значениях по умолчанию, то шифрованные файлы и папки будут отображены светло-зеленым цветом.

После того как файл зашифрован, открыть его может только тот пользователь, который осуществил шифрование. Тот, кто зашифровал файл, может расширить число пользователей, имеющих возможность чтения данных. Для этого нужно опять раскрыть меню свойств файла и дойти до вкладки **Дополнительные атрибуты**. Если файл уже зашифрован, то будет доступна кнопка **Подробно**. При ее нажатии вы увидите окно, в котором перечислены пользователи (рис. 9.24), которые могут расшифровать файл.

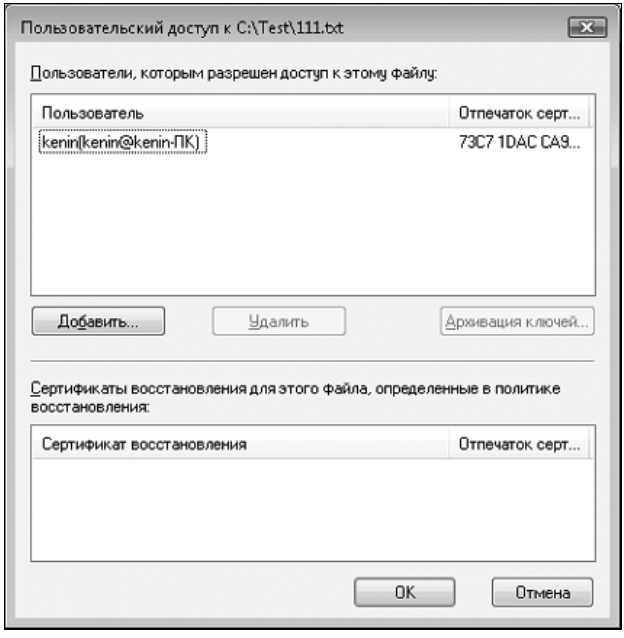


Рис. 9.24. Список пользователей, которым разрешено расшифровать данные файла

Чтобы добавить нового пользователя, достаточно нажать кнопку **Добавить** и выбрать пользователей, которые *имеют на данном компьютере сертификат*.

> ***Совет***
>
> Самый простой способ получения сертификата — попытаться зашифровать файл. Во время операции будет создан сертификат, если он отсутствовал.

Если вы работаете в составе домена, то учитывайте, что в корпоративных политиках предусматривается наличие специального пользователя, которому разрешается расшифровывать все данные. Делается это в целях сохранности производственной информации в непредвиденных ситуациях (несчастный случай с работником и т. п.).

Технически такая политика реализуется либо включением дополнительного сертификата восстановления (пользователя) в свойства файла. Кроме того, администратор может настроить опции так, что при создании пары ключей пользователя его закрытый ключ будет храниться в виде копии в службе каталогов. В результате специально назначенный администратор сможет при необходимости восстановить этот ключ и получить доступ к файлу (фактически от имени пользователя).

При шифровании файлов следует учитывать также то, что параметры операции привязаны к параметрам безопасности учетной записи. Если получить доступ к паролю, то можно и расшифровать этот файл. Так, в Интернете сегодня можно найти несколько утилит, с помощью которых восстанавливается информация из зашифрованных таким способом файлов.

EFS можно использовать и для сменных носителей, но для этого их нужно сначала отформатировать в файловой системе NTFS.

Шифрование диска при помощи BitLocker

В старшие версии Windows (Windows Vista/Windows 7 Максимальная/Корпоративная, Windows 2008 R2) включена возможность шифрования данных на диске по технологии BitLocker. Помимо требований к версии ОС, для установки необходим компьютер с совместимой версией BIOS, наличием модуля TPM версии 1.2 (Trusted Platform Module — специальной микросхемы на материнской плате компьютера для хранения конфиденциальной информации). При наличии модуля TPM один из ключей, используемых при шифровании данных, хранится в этом модуле, что обеспечивает самый высокий уровень его защиты.

С использованием BitLocker могут быть зашифрованы системные логические диски и диски с данными (отформатированные в NTFS, FAT16/32, ExFAT), сменные носители, использующие флэш-память (флэшки), логические диски на RAID-массивах — все независимо от варианта подключения (IDE, ATA, SATA, SCSI, USB, Fireware).

Если предполагается зашифровать системный диск, то перед включением BitLocker необходимо, чтобы на диске было создано как минимум два раздела: на одном из них, размером не менее 100—300 Мбайт (размер зависит от выпуска ОС), размещаются загрузочные файлы и среда для восстановления (Windows PE). Этот раздел

невидим, ему не присваивается буква логического диска и создается он автоматически при новой установке Windows 7. Но если, например, компьютер обновлен с Windows XP, то такого раздела в системе не будет.

Если сменный диск отформатирован в FAT, а потом зашифрован с помощью BitLocker To Go, то этот носитель может быть прочитан и при подключении к Windows XP. Но именно прочитан, т. к. запись на него в Windows XP будет невозможна.

BitLocker может быть распространен централизованно. Так же централизованно могут храниться и данные для восстановления (доступа к зашифрованным дискам).

> ***Совет***
>
> При использовании BitLocker могут проверяться параметры BIOS. Поэтому в случае необходимости обновления BIOS внимательно изучите соответствующие разделы описания технологии. В противном случае вам придется использовать вариант доступа к диску в режиме восстановления.

Процесс шифрования диска занимает достаточно длительное время и зависит от объема диска. В этот период можно продолжать работать на компьютере, хотя его производительность несколько снижается.

Сам BitLocker тоже влияет на производительность системы. Но обычно снижение производительности происходит в диапазоне нескольких процентов.

> ***Совет***
>
> Технология BitLocker позволяет создавать ключ *восстановления* при любом варианте шифрования. Не пренебрегайте этой возможностью. Иначе, например, в случае аппаратных проблем вы потеряете все свои данные.

Использование BitLocker на компьютерах без TPM

Технология BitLocker может быть использована и на компьютерах, *не имеющих TPM-модуля*.

Можно зашифровать диск, используя сменный USB-носитель для хранения ключа. Такая возможность включается *только* через настройки групповой политики. Для открытия редактора групповой политики наберите в командной строке `mmc` и добавьте в оснастку консоли Редактор групповой политики. При запросе объекта редактирования выберите **Локальный компьютер.**

Параметры, которые необходимо изменить для включения дополнительных возможностей шифрования, находятся по следующему пути: **Политика "Локальный компьютер" | Конфигурация компьютера | Административные шаблоны | Компоненты Windows | Шифрование диска BitLocker | Диски операционной системы |** *параметр* **Обязательная дополнительная проверка подлинности при запуске** (рис. 9.25). В свойствах параметра необходимо разрешить использование BitLocker без совместимого TPM.

Обратите внимание, что в этом случае BIOS должна поддерживать чтение с USB в режиме старта.

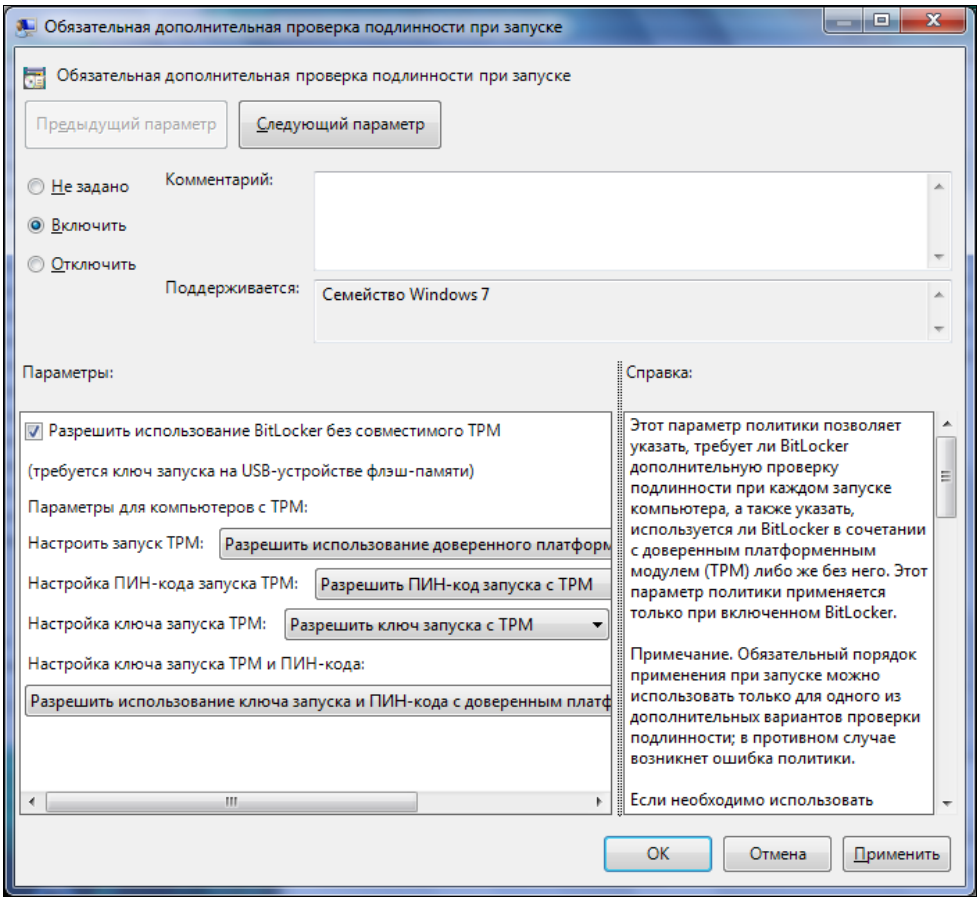


Рис. 9.25. Настройка параметров для включения BitLocker на компьютерах без TPM

Включение шифрования

Включение шифрования BitLocker осуществляется с помощью **Панель управления | Шифрование диска BitLocker**. Если все необходимые для шифрования условия выполнены, то в окне появляется опция **Включить шифрование**. После ее выбора запускается мастер операций.

Вам нужно просто следовать указаниям программы.

Режим восстановления

В случае выхода из строя оборудования (модуля TPM или всей материнской платы), изменения загрузочных файлов (например, перепрошивке BIOS и т. п.) нормальная загрузка компьютера становится невозможной. Вы увидите черный экран с предложением ввести пароль восстановления.

Пароль восстановления создается на одном из этапов подготовки диска к шифрованию с помощью мастера операций. Потом его можно продублировать, воспользовавшись соответствующими опциями задачи шифрования. Пароль представляет

собой последовательность цифр. Для того чтобы можно было отличить один пароль от другого (если вы работаете с несколькими системами), вам сообщается также его название, состоящее из ряда цифр и букв. И название пароля, и его значение сохраняются в один файл, так что легко можно выяснить, подойдет ли данный пароль для восстановления.

Как уже было сказано, пароль состоит только из цифр и вводится при помощи не цифровых, а функциональных клавиш, при этом клавиши <F1>, <F2>, ..., <F10> соответствуют цифрам 1, 2, ..., 0.

После ввода пароля система продолжит загрузку, а затем вы можете отключить режим шифрования.

Обратите внимание, что есть две возможности отключения шифрования. Первая предполагает полное дешифрование диска; это довольно длительная операция. Вторая только временно отключает режим шифрования, если вы собираетесь, например, заменить на компьютере BIOS.

Шифрование почты

Электронная почта передается по открытым каналам связи, поэтому не исключен риск ее перехвата или модификации. Электронная подпись письма гарантирует, что текст сообщения никем не изменен, а шифрование делает просмотр письма недоступным для посторонних.

Можно использовать различные варианты шифрования сообщений (например, вкладывать в письмо заранее зашифрованный какой-либо программой текст), но одним из самых удобных является стандарт *S/MIME* (Secure/Multipurpose Internet Mail Extensions). Почтовая программа автоматически шифрует текст письма и пересылает полученный код в виде файла, вложенного в обычное почтовое сообщение, поэтому шифрованные письма могут без каких-либо дополнительных настроек пересылаться обычными почтовыми системами.

Работа с подписанными или шифрованными сообщениями не представляет сложности. Система автоматически обрабатывает сообщение, пользователю достаточно только включить соответствующую опцию в свойствах письма. О том, что письмо зашифровано, сообщают только пиктограммы в панели инструментов сообщения (рис. 9.26, выделено стрелкой). Сам текст автоматически расшифровывается в момент открытия сообщения. Если щелкнуть по пиктограммам, то можно увидеть информацию по сертификату, использованному при составлении письма.

Получение открытого ключа для защищенной переписки

Шифрование сообщения по стандарту S/MIME производится с помощью открытого ключа получателя письма личным ключом отправителя. Поэтому расшифровано оно может быть только тем пользователем, у которого имеется соответствующий использованному открытому ключу закрытый ключ.

Поскольку для шифрования требуется знать открытый ключ получателя, то его необходимо иметь *до отправки письма*. В рамках организации (домена Windows)

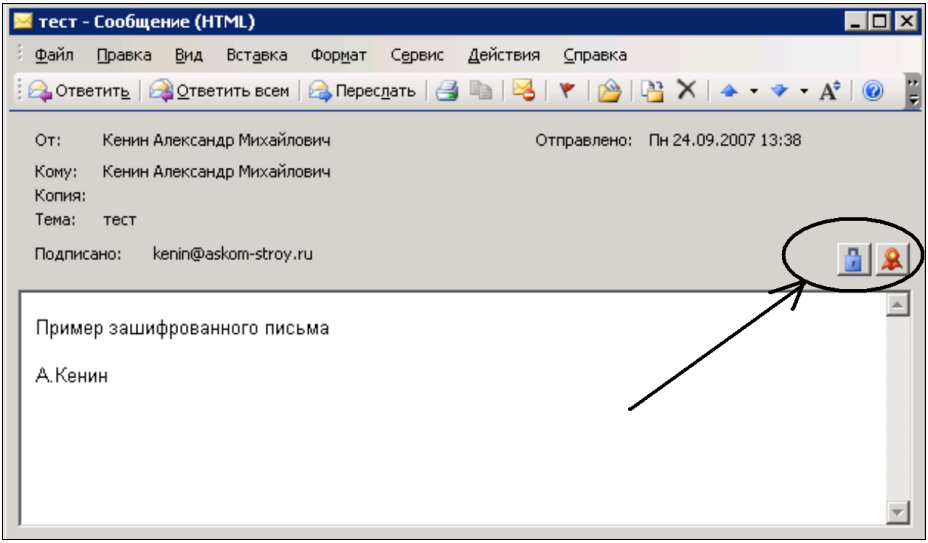


Рис. 9.26. Образец почтового сообщения с электронной подписью и шифрованием текста

открытые ключи пользователей доступны через службу каталогов. Если же вы хотите написать письмо внешнему адресату, то предварительно следует получить его открытый ключ, например, запросив письмо с электронной подписью.

Получение цифрового сертификата для защищенной переписки

Для того чтобы использовать для защищенной переписки пару ключей, они должны быть заверены удостоверяющим центром, которому доверяют как отправитель, так и получатель сообщения. Если использовать цифровые удостоверения, выданные серверами организации, то к ним не будет доверия у внешних пользователей, и у получателя сообщения появится предупреждение о нарушении электронной защиты. Хотя сам текст сообщения может быть и не поврежден, большинство адресатов просто не будут открывать такие письма.

Если необходимо использовать защищенную переписку между двумя организациями, то существует два варианта решения. Первый — это обменяться сертификатами удостоверяющих центров своих организаций и установить к ним доверие в каждой организации. Недостаток подобного решения — такие "обмены" придется осуществлять с *каждой* организацией, с сотрудниками которой необходимо осуществлять защищенную переписку.

Второй способ заключается в использовании сертификатов от публичных удостоверяющих центров, к которым по умолчанию существуют доверительные отношения в операционной системе. В большинстве случаев получение подобного сертификата является платной услугой, хотя некоторые центры предоставляют возможность получения временных бесплатных сертификатов. Обычно такие сертификаты не предполагают возможности строгого шифрования сообщения и фактически удостоверяют только сам адрес электронной почты.

После получения сертификата он должен быть добавлен в настройки программы почтового клиента.

Электронная подпись

Электронная подпись формируется следующим образом. Для текста сообщения (и вложений) вычисляется *хэш*, который шифруется с помощью *закрытого ключа пользователя*. Полученный код добавляется к электронному сообщению.

В точке приема почтовая программа, во-первых, вычисляет хэш полученного сообщения. Во-вторых, пытается дешифровать хэш, вложенный в письмо при его отправке. Если программе удается дешифровать хэш (его расшифровка производится с помощью открытого, т. е. публично доступного ключа пользователя), то это означает, что письмо действительно получено от этого автора. Если расшифрованный хэш совпадает с тем, который вычислен для принятого письма, то это подтверждает отсутствие изменений в сообщении.

Защита электронной почты с использованием PGP

Программа PGP (*Pretty Good Privacy*) приобрела популярность в связи с открытостью кода и, как следствие, отсутствием инженерных ключей и т. п. После того как эта технология стала коммерческим продуктом, ее популярность резко снизилась, хотя на практике можно столкнуться с сообщениями, которые подписаны электронной подписью PGP.

Эта технология также использует для защиты сообщений пару ключей, причем для хранения открытых ключей используются серверы PGP.

Почтовые клиенты с PGP также прозрачно обрабатывают сообщения, клиенты без PGP показывают в случае электронной подписи только наличие вложенного файла.

Шифрование в базах данных

Значительная часть информации организации хранится на серверах баз данных. Современные версии производственных серверов имеет возможность выборочного (по столбцам таблиц) или полного (всей базы) шифрования данных.

> ***Примечание***
>
> Возможность шифрования в базах данных была и раньше. Но эта функциональность должна была использоваться программой, работающей с данными.

Эти функции реализуются средствами сервера баз данных, и поэтому шифрование "прозрачно" для прикладных программ. Администратору необходимо определить критичную информацию (излишнее шифрование не имеет смысла, а производительность системы будет снижаться) и включить шифрование средствами управления SQL-сервера.

Если рассматривать Microsoft SQL Server 2008, то архитектура решения представлена на рис. 9.27.

Каждая база данных шифруется собственным ключом. Для этого используется сертификат, зашифрованный мастер-ключом базы Master, который, в свою очередь,

шифруется ключом службы сервера базы данных, создаваемый при установке сервера.

Обратите внимание, что прозрачное шифрование данных предотвращает доступ к информации в резервных копиях, на остановленных серверах (выключенных системах). Но если злоумышленник попытается получить доступ через работающий SQL-сервер (например, получив параметры доступа пользовательской учетной записи), то такая попытка завершится успехом. В этом случае должны срабатывать средства контроля доступа SQL-сервера.

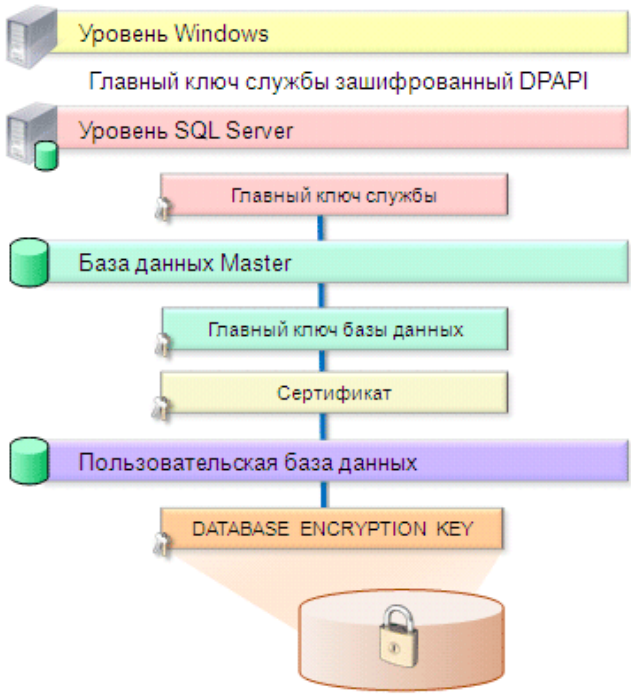


Рис. 9.27. Архитектура шифрования данных в SQL 2008

Цифровые права документов

Существует вариант использования шифрования для ограничения распространения документов. Идея цифровых прав в общих чертах достаточно проста.

Документ шифруется уникальным ключом, причем для доступа к данным необходима связь с сервером организации. Программное обеспечение, которое осуществляет прозрачное шифрование и дешифрование документа, следит за параметрами ключа: так, можно разрешить автономное (без связи с сервером) использование документа, ограничить срок работы (документ невозможно будет открыть после заданной даты) и т. д. А на самом сервере процессы работы с ключами легко поддаются управлению групповыми политиками, можно управлять разрешениями для групп пользователей и т. д.

При этом клиентское ПО службы управления цифровыми правами документов блокирует операции копирования (в том числе, возможности пересылки по электронной почте), редактирования, печати документов.

Можно упомянуть два продукта, реализующие цифровую защиту документов. Это Oracle RMS и Microsoft RMS. Они имеют некоторые отличия с точки зрения используемых технологий, например, Microsoft RMS хранит ключи в контейнере вместе с документом, Oracle RMS — на сервере и т. п., что приводит и к отличиям при использовании (если ключи хранятся на сервере, то их можно одномоментно заблокировать и т. п.). Главное, что оба продукта имеют конечный список форматов документов, которые можно защищать этой технологией (хотя Oracle RMS и предлагает интерфейс для разработчиков, оценивая подготовку нового типа документа в 10—15 трудодней программиста). Обычно цифровыми правами защищаются документы офиса (Microsoft Office). Второе ограничение технологии — сложности предоставления прав для внешних пользователей (не аутентифицирующихся на сервере каталогов организации).

> ***Примечание***
>
> Технология RMS встроена в Windows Server, начиная с выпуска 2003. Для ее использования должна приобретаться *дополнительная лицензия*.

Обратите внимание, что хотя RMS и позволяет ограничить пользователя в копировании полученного документа, данная технология не защищает информацию от распространения. Например, используя права отладчика операционной системы, можно получить копию данных. Никто не исключает и просто возможность снять картинку с монитора обычным фотоаппаратом, а потом просто распознать текст, тем более что современные средства делают эту операцию просто, безошибочно, даже сохраняя оформление исходного документа.

Конечно, можно зафиксировать перечень запускаемых на компьютере программ, но в итоге окажется проще использовать стандартный комплекс защиты конфиденциальной информации, чем настраивать подобную систему.

Иными словами, RMS имеет, прежде всего, психологическое воздействие на пользователя, показывая ему, что данный документ по правилам организации не может быть скопирован и передан другому лицу.

Стеганография

Лучший способ защиты информации — не показать злоумышленнику, что эта информация есть. Технология стеганографии предполагает маскировку данных среди ничего не значащей информации.

Самый простой способ — это добавить (склеить с изображением) в конец файла изображения еще один архив. Изображение будет нормально просматриваться в графических программах, но при открытии его в архиваторе вы сможете извлечь исходные данные.

Анализ поведения пользователей

По результатам некоторых западных исследований примерно 2/3 высокотехнологичных корпораций постоянно сталкиваются с внутренними угрозами безопасности информации.

Традиционные способы защиты — ограничение доступа к информации, контроль периметра (почты, различных мессенджеров, сменных носителей и т. д.) по ключевым словам (сигнатурам) и т. д. — становятся малоэффективными.

Во-первых, информация часто похищается теми, кто имеет доступ к соответствующему классу данных. Кроме того, используя методы социальной инженерии для злоумышленника не представляет труда получить доступ к желаемой информации. Во-вторых, пользователи становятся более опытными и подготовленными. Они могут легко узнать, какие продукты используются для защиты данных, какие сигнатуры анализируются даже поставить себе для изучения триальную версию продукта. В результате злоумышленник сможет вынести из организации достаточное число информации, имеющей коммерческую ценность.

Для исключения подобных ситуаций стали появляться продукты, анализирующие модель поведения пользователя. Простейший пример, если в текущей работе сотрудник на данном рабочем месте столько-то раз открывает документы из такой-то папки, производит поиск по таким-то ключевым словам и т. д., то его поведение может быть описано соответствующей моделью. Если сотрудник начинает готовиться к уходу из организации и собирает кажущуюся ему полезной информацию, то такие дополнительные операции будут восприняты программой как отклонения от профиля и специалисты службы безопасности получат предупреждение.

Подобные продукты являются коммерческими решениями. Здесь мы не станем описывать конкретные решения, поскольку они специфичны для различных типов информации.

DLP-технологии

Защищаемая информация может покинуть организацию различными путями через каналы связи и сменные носители, электронную почту, ICQ, Skype, флэшки и т. п. Причем это может быть сделано как умышленно, так и случайно (например, перепутав адрес получателя при создании письма).

На рынке сегодня имеется несколько продуктов, позволяющих контролировать периметр организации и блокировать возможную утечку данных. Такие решения называют *DLP* (Data Loss Prevention). Основная задача DLP — обнаружить и заблокировать запрещенную передачу конфиденциальных данных по любым каналам связи и устройствам.

Большинство таких продуктов работают уже "по факту", т. е. сообщают о наличии подозрительного трафика и утечке данных. Кроме того, методы анализа данных не позволяют говорить о надежности распознавания конфиденциальной информации, тем более что каждой категории данных требуется своя адаптированная технология анализа.

Для анализа документов применяется теория отпечатков. Каждому документу ставится в соответствие цифровой отпечаток, который сравнивается с хранимыми цифровыми отпечатками документов, которые эксперты отнесли к конфиденциальной информации. На основе такого анализа определяется вероятность присутствия в документе конфиденциальных данных. Кроме того, проводится морфологический и грамматический разбор текста для обнаружения искомых данных.

DLP-решения являются недешевыми продуктами. О целесообразности их внедрения с экономической точки зрения имеет смысл говорить при числе контролируемых рабочих мест порядка нескольких сотен и более. Кроме того, решение, выносимое такой системой, является вероятностным (хотя и с достаточно высокой степенью правильной идентификации).

Поэтому подобные технологии сегодня пока применяются в крупных организациях, где очень высока стоимость утечки данных (финансовый сектор и т. п.).

Анонимность работы в глобальной Сети

В отличие от зарубежных наши пользователи практически не уделяют внимания анонимности работы в Интернете. Хотя анализ активности человека дает чрезвычайно много информации. Следует учитывать также, что соответствующие службы имеют техническую возможность перехвата любого трафика — обеспечение данной технической возможности является условием получения провайдерской лицензии.

Мы приведем некоторые советы по обеспечению анонимности работы в Интернете. Понятно, что они не гарантируют защиту персональных данных, что технологии слежки развиваются и что для обеспечения анонимности серфинга Интернета пользователю необходимо постоянно уделять этой проблеме часть своего времени.

Скрытие своего IP-адреса

При доступе к любому ресурсу в Интернете (страница веб-сервера, почта, торрент-ресурс и т. д.) на соответствующем сервере может быть записан IP-адрес хоста, с которого был выполнен запрос. Эта же информация доступна и просто при перехвате пакетов в сети.

Знание IP-адреса позволяет легко установить личность пользователя: регион доступен в открытой информации (по принадлежности зарегистрированного диапазона IP-адресов), а фамилия может быть получена запросом к провайдеру.

Самый простой способ скрыть свои координаты — использовать анонимный прокси-сервер. Прокси-сервер принимает запросы от пользователя, пересылает их на требуемый ресурс от своего имени и возвращает ответ пользователю. Анонимные прокси-серверы скрывают все пользовательские данные, запрос идет только с параметрами прокси-сервера.

Список бесплатных прокси-серверов легко найти в Интернете, например на **http://www.proxy-list.org/ru/index.php**. Конечно, есть вероятность, что какие-то

данные прокси-сервер все же отсылает, но этот факт можно проверить. В Интернете легко можно найти сайты, проверяющие анонимность прокси.

Понятно, что журналы самих прокси-серверов позволяют легко найти реальный адрес. Поэтому некоторые пользователи выстраивают несколько прокси-серверов в цепочку; правда, не все серверы позволяют выполнить подобную настройку. Другой способ — автоматически переключать прокси-серверы. Для этого даже создано много программ, многие из которых бесплатны для применения (см., например, **http://www.poststar.ru/proxy_programs.htm**).

> ***Примечание***
>
> В корпоративных сетях пользователю недоступны параметры смены настроек прокси-сервера. В подобных случаях можно использовать такие ресурсы, как **http://www.proxy-anonymous.info/**, позволяющие анонимно подключаться к ресурсу через страничку, открываемую в любом обозревателе Интернета.

Использование анонимного прокси-сервера не гарантирует абсолютное скрытие своего реального IP-адреса. Например, простейший сценарий, встроенный в просматриваемую страничку (на Java, VB, ActiveX и т. п.), легко вычислит адрес компьютера и передаст его на сервер. Защититься от этого, как правило, невозможно, поскольку при отключении сценариев существенная часть ресурсов практически неработоспособна.

> ***Примечание***
>
> Если компьютер имеет серый адрес, то это может помочь защититься от такой проверки. Другой вариант — настройка межсетевых экранов и контроль за передачей в Интернет сведений с локального компьютера. Последний вариант обычно требует наличия у пользователя некоторого опыта работы.

Владельцы ресурсов тоже могут догадаться, что их посетитель использует анонимные прокси-серверы. Либо просто по списку таких серверов, либо анализируя cookies пользователя: смена IP-адреса в этом файле может быть признаком использования нескольких прокси.

Другим недостатком прокси-серверов является возможность их использования только для посещения веб-страниц. Протоколы кроме HTTP/HTTPS обычно не поддерживаются прокси-серверами.

Защита от файлов слежения на компьютере

При работе в Интернете многие ресурсы пытаются сохранить на компьютере ту или иную информацию. На слуху большинства пользователей — файлы cookies. Но это только малая часть "айсберга". Например, обращали ли вы внимание, что модуль чтения Adobe Flash Player хранит данные на локальном диске (рис. 9.28; многие ли пользователи просто открывали эти настройки)? А ведь без данных компонентов редко когда обходятся популярные сайты.

Этот пример относится только к одному модулю. А как можно регулировать возможности хранения данных для других программ? Поэтому последние версии обозревателей Интернета дополнены специальным режимом — *приватным* (InPrivate) просмотром.

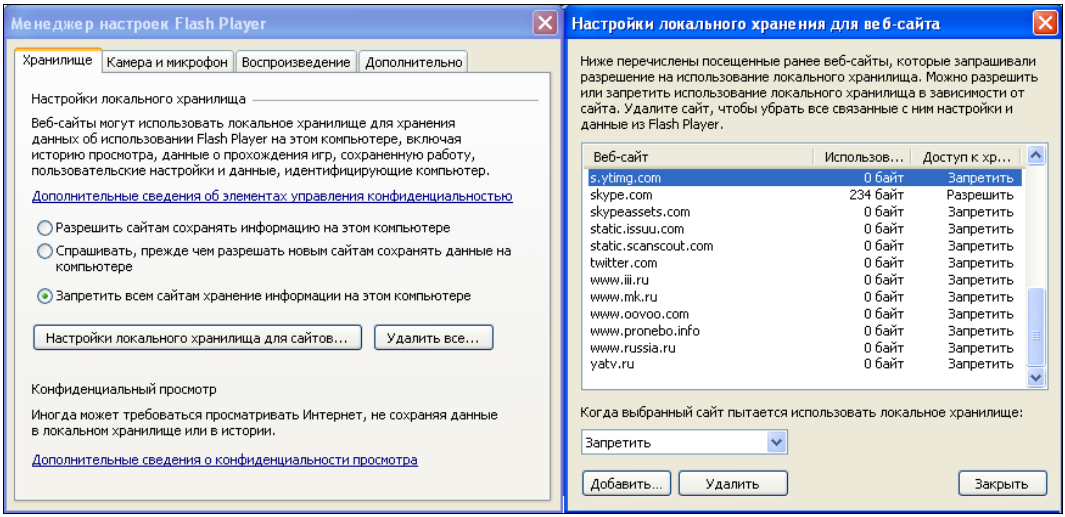


Рис. 9.28. Параметры хранения информации Adobe Flash Player

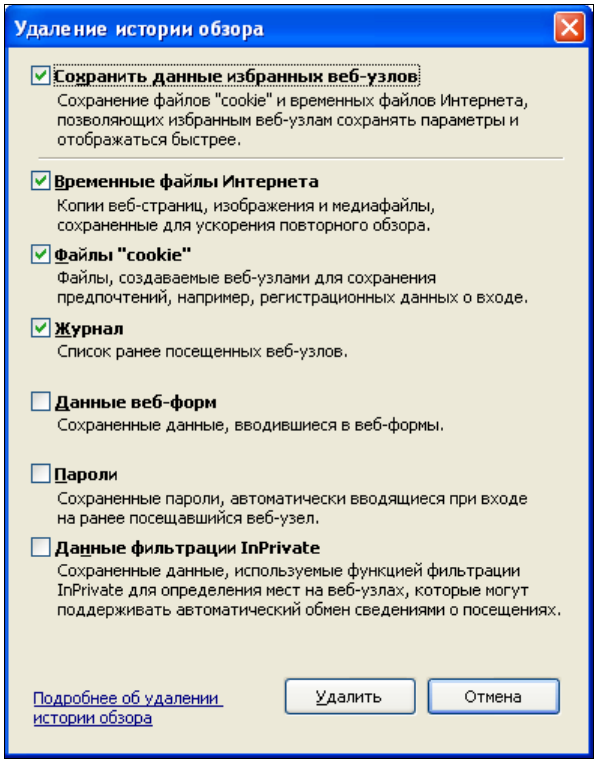


Рис. 9.29. Параметры команды удаления истории обозревателя Internet Explorer

В режиме приватного просмотра на компьютере не должны сохраняться никакие данные: отключена запись истории посещенных сайтов, запрещено формирование файлов cookies, блокируются попытки программных модулей сохранить информацию на жестком диске.

Как показывают данные статистики, данный режим используется в основном при посещении сайтов для взрослых и интернет-магазинов подарков.

К сожалению, приватный режим не гарантирует полную приватность. Во-первых, исследования показывают, что некоторым модулям удается сохранить данные. Правда, с совершенствованием обозревателей таких возможностей остается все меньше.

Во-вторых, есть простой способ узнать[1] перечень посещенных сайтов: введите команду `ipconfig /displaydns` и вы увидите желаемый список. И, в-третьих, не стоит забывать, что вся история посещений сохраняется у провайдера.

Если режим приватного просмотра не используется, то для удаления основной части сохраненных данных можно использовать соответствующую команду из меню обозревателя (рис. 9.29).

Использование наложенных сетей

Другой способ обеспечения анонимности заключается в построении поверх Интернета собственных сетей. Эти сети могут как хранить некоторую информацию зашифрованной и распределенной по многим хостам (на каждой системе будет только часть зашифрованных данных), так и просто скрывать запросы пользователей. Одним из наиболее известных проектов в этой области является TOR-проект (от The Onion Router) (**https://www.torproject.org/**).

Пользователи подключаются к этой сети, пользовательский трафик шифруется (провайдер не может увидеть, какие запросы делает пользователь), а запросы к внешним ресурсам поступают только от нескольких серверов проекта. Хотя имеются данные об успешных попытках взлома технологии и получения реальных адресов (см. **http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29**), но в целом данное решение остается достаточно популярным.

Можно упомянуть также проекты iNet, I2P, Bunzilla, но любознательный читатель легко найдет и другие решения.

[1] Конечно, эта информация доступна до перезагрузки или очистки кэша командой `ipconfig /flushdns`.

ГЛАВА 10

Построение отказоустойчивой информационной системы

Мы все больше начинаем зависеть от различных информационных систем. 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.

Надежная система — это система, в которой отсутствует единая точка отказа. Искусство проектировщика состоит не только в подборе технологий, резервирующих ту или иную точку отказа, но и в способности выявить все такие точки.

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.

Иными словами, при проектировании информационной системы следует учитывать особенности размещения ее элементов и предусматривать меры, позволяющие восстановить данные при любых ситуациях.

Центры обработки данных

Для размещения вычислительных мощностей информационной системы принято использовать специально подготовленные помещения, в которых обеспечивается

оптимальный режим работы оборудования. Такие объекты принято называть центрами обработки данных (ЦОД).

Существует несколько уровней оснащенности ЦОД. Если говорить о третьем уровне надежности, то для него предусматривается полное дублирование всех систем жизнеобеспечения. Иными словами, ЦОД должен продолжать нормальное функционирование при выходе из строя или при выключении на обслуживание *любого* узла. Это очень серьезное требование, реализуемое путем тщательного проектирования. В результате стоимость такого ЦОД (строительные работы, системы кондиционирования, электропитания, контроля доступа, аварийного освещения и т. д.) усредненно составляет 25 000$ за 1 м^2.

В Сети можно легко найти подробные рекомендации по оснащению ЦОД. Поэтому мы кратко рассмотрим только основные положения. Естественно, что требования к ЦОД в каждом конкретном случае должны быть разумно откорректированы.

Требования к помещениям ЦОД

Требования к помещениям ЦОД определены санитарными нормами и правилами. Если кратко, то ЦОД должен размещаться — желательно — 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 с ЦОД и т. п.).

Поскольку в ЦОД будет эксплуатироваться дорогостоящее оборудование, то помещение должно быть стойким к взлому (по действующим требованиям) и оснащено системами контроля доступа.

Материалы, используемые для внутренней отделки, должны исключать выделение пыли, наличие статического электричества. Часто для обеспечения чистоты в ЦОД реализуется наддув очищенного воздуха, в этом случае помещение герметизируется и оборудуется входным тамбуром.

Размеры помещения определяются из предполагаемого количества оборудования (с учетом резерва, часто в 30—60%) и наличия зон обслуживания (для установки серверов и т. п).

Климат-контроль помещений ЦОД

Основным требованием является поддержание заданной температуры (обычно около 18 °С). Параметры влажности не являются значимыми, если в ЦОД не эксплуатируются ленточные библиотеки. Обычно только требуется, чтобы была исключена возможность выпадения росы. Поскольку в помещении ЦОД не предполагается работа персонала, то требований по воздухообмену обычно не предъявляют.

Так же, как и все системы ЦОД, оборудование климат-контроля выполняется в резервированном варианте.

На кондиционирование расходуется большая часть потребляемой ЦОД электроэнергии. Поэтому сегодня много внимания уделяется решениям, позволяющим

снизить соответствующие затраты. Например, использование зимой внешнего холодного воздуха для поддержания необходимой температуры внутри помещения.

Резервирование электроснабжения ЦОД

ЦОД обязательно оборудуется системой резервного электроснабжения. Главным параметром является максимальное время автономной работы. Поскольку потребляемая мощность ЦОД часто составляет десятки киловатт, то даже незначительное увеличение времени автономной работы приводит к серьезному удорожанию решения. При необходимости автономной работы свыше 30 минут обычно единственным решением становится установка дизель-генератора с автоматическим запуском.

В результате разработчики применяют различные ухищрения, позволяющие снизить расходы. Например, использование больших буферных резервуаров теплоносителя позволяет отключать сами кондиционеры на время пропадания электричества, в результате снижается существенно мощность системы резервного электропитания (в автономном режиме в этом случае необходимо будет запитывать только вентиляторы и насосы теплоносителя).

Кроме того, можно ввести различные категории оборудования ЦОД и не поддерживать функционирование наименее важных подсистем в автономном режиме и т. п.

Системы пожаротушения ЦОД

При площади ЦОД 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.

Обычно трудно обосновать максимальное время автономной работы, на основании которого выбираются аварийные источники питания. Часто эта цифра берется "с потолка" или "как у других". При этом даже небольшое увеличение этого времени приводит к существенному удорожанию оборудования. В качестве критерия оценки можно использовать время выключения информационной системы с сохранением всех данных. Это значение нужно умножить на 2 или 3, а выбор оборудования проводить с запасом примерно 30—50%. Так вы получите минимальное значение, которое можно использовать при расчете источников аварийного питания.

> ***Совет***
>
> При настройке решений, автоматически выключающих информационные системы в случае аварий систем электроснабжения, следует выбирать не задержку от времени пропадания электричества, а запуск по уровню зарядки аккумуляторов.

Надежность сетевой инфраструктуры

Необходимым условием надежной работы информационной системы является безотказное функционирование каналов связи. Данная задача решается путем *дублирования* как собственно каналов связи, так и активного оборудования (коммутаторов). 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.

Отказоустойчивая топология сети передачи данных

Принцип создания отказоустойчивой сети достаточно прост: линии связи должны быть дублированы (причем трассы не должны проходить по одним и тем же участкам), а активное оборудование — резервировано. Понятно, что это вдвое удорожает инфраструктуру, поэтому данный принцип реализуют на уровнях распределения, ядра и подключения серверной фермы, а оконечные устройства — пользовательские станции — подключают к коммутатору нерезервированной линией связи.

> ***Примечание***
>
> Отказоустойчивые схемы, несмотря на кажущуюся простоту, требуют предварительного проектирования, выбора оборудования и его тщательной настройки. При этом в зависимости от выбранного варианта конфигурации может потребоваться использование протоколов, которые не поддерживаются относительно дешевыми моделями оборудования.

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 проектирования и первоначальной настройки активного оборудования. У коммутаторов, предназначенных для использования на уровне доступа, обычно по умолчанию включены протоколы, которые "разорвут" такое

кольцо. Коммутаторы уровня ядра не имеют подобных настроек, поэтому возникновение кольца быстро приведет к падению сегмента сети.

Существует два варианта построения отказоустойчивой сети с дублированными каналами. Первый вариант использует протоколы, работающие на втором уровне модели OSI. Второй основан на протоколах маршрутизации третьего уровня модели OSI.

Построение отказоустойчивой сети на основе протоколов второго уровня

Отказоустойчивая конфигурация, построенная с использованием протоколов второго уровня, обеспечивает более быстрое восстановление в случае аварии, чем протоколы 3 уровня. Сеть может восстановиться за 1—3 сек или даже еще быстрее в случае использования проприетарных протоколов.

> ***Примечание***
>
> *Проприетарным* называют протокол, не описываемый открытым стандартом, а являющийся уникальной технологией определенного вендора. Хотя использование проприетарных решений позволяет получить лучшие показатели по сравнению с открытыми стандартами, но такой выбор связан с ориентацией на использование оборудования только одного вендора и с вытекающими из этого рисками.

Использование протоколов остовного дерева

Протоколы остовного дерева — *Spanning Tree Protocol* (STP, стандарт 802.1d) и *Rapid Spanning Tree Protocol* (RSTP, стандарт 802.1w) — используются для автоматического построения связей сетевой структуры. Коммутаторы пытаются вычислить оптимальные маршруты между всеми устройствами по определенным алгоритмам. Для определения маршрутов и контроля соединений по специальным алгоритмам постоянно рассылаются служебные пакеты (*Bridge Protocol Data Units, BPDU*), коммутатор анализирует их и "понимает", где подключены конечные станции, где — активное оборудование и т. п. При обнаружении петель происходит блокировка (отключение) порта, подключенного к параллельной линии связи. Если топология сети меняется (появляются новые коммутаторы и, как следствие, от них начинают рассылаться пакеты BPDU — или наоборот), то осуществляется переконфигурирование структуры. Этот процесс занимает от 30 сек до нескольких минут в зависимости от размера сети для протокола STP. При использовании протокола RSTP (усовершенствованной версии STP) время перестройки уменьшается до нескольких секунд.

Протоколы STP/RSTSP могут обеспечить связность сети без каких-либо ручных настроек. При построении структуры алгоритмы учитывают скорость соединения и количество коммутаторов на дублированных линиях связи между точками подключения. Администратору нужно только включить данные протоколы на портах (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.

Алгоритм построения конфигурации сети в этих протоколах в "центр" ставит коммутатор с самым малым весом[1] (Bridge ID или Bridge Priority), поэтому для оптимизации процесса целесообразно *вручную* назначить приоритеты. Коммутатор в центре сети должно иметь самый малый "вес"; чем дальше от логического центра, тем большее значение Bridge ID нужно назначить коммутатору. Кроме того, в случае использования 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.

Протоколы STP/RSTP поддерживаются всеми современными коммутаторами. Однако серьезным недостатком их применения является *отключение* резервных связей. Резервные связи не используются для передачи данных и включаются только в случае повреждения основного канала.

> ***Примечание***
>
> Поддержку протоколов STP/RSTP следует включать 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. Обычно протоколы STP/RSTP на коммутаторах уровня доступа включены по умолчанию.

Использование стандарта MSTP

Протокол *MSTP* (Multi Spanning Tree Protocol описан в стандарте 802.1s) и является расширением протокола RSTP на сеть с VLAN, точнее протокол RSTP стал частью протокола MSTP.

В отличие от RSTP, протокол MSTP строит дерево связей с учетом созданных на коммутаторах VLAN. Поэтому предупреждение петель происходит не путем отключения порта коммутатора, а через отключение передачи данных *только* для определенной VLAN. Иными словами, можно настроить MSTP таким образом, 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 первый канал будет основным, а второй — резервным; в другом — наоборот. Таким образом все соединения будут передавать данные. В случае повреждения канала связи протокол MSTP обнаружит это событие и автоматически перестроит структуру.

Главный недостаток решения на протоколе MSTP заключается в сложности настройки такой структуры. Администратор должен четко представлять разбиение

---

[1] Алгоритм выбора приоритета коммутатора основан на MAC-адресе устройства, поэтому ранее установленное и, соответственно, 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 целесообразно поместить самое новое и, следовательно, самое производительное устройство.

системы на VLAN, оценить потоки данных в каждом сегменте и путем ручной настройки добиться относительно равномерного использования всех каналов связи.

Также следует учитывать, что во многих моделях коммутаторов (особенно бюджетного ряда) поддержка протокола MSTP не реализована.

Использование "агрегированных" каналов

Стандарт 802.3ad описывает агрегированные каналы. Агрегированный канал позволяет объединять несколько линий связи между коммутаторами в один общий канал передачи данных. Соответственно, агрегированный канал имеет пропускную способность, равную сумме пропускных способностей объединяемых каналов. При передаче данных задействованы оба канала, причем в случае отказа одного из соединений все данные начинают передаваться через оставшийся канал. Распределение данных по отдельным каналам выполняется на основе подсчета хэш-функции от MAC-адресов источника и назначения. В результате каналы загружаются относительно равномерно, но передача данных между компьютером "А" и компьютером "Б" всегда происходит только по одному каналу, поэтому максимальная скорость передачи данных между двумя устройствами всегда определяется только одним каналом передачи данных. При этом в целом происходит общее увеличение пропускной способности.

Агрегированный канал может настраиваться как вручную явным указанием объединяемых портов, так и автоматически на основе специального протокола LACP — Link Aggregation Control Protocol. Соответствующие настройки выполняются в программе конфигурирования коммутаторов.

К сожалению, стандарт не описывает многоточечное подключение, т. е. соединение должно быть осуществлено *только* между двумя устройствами.

На практике многие вендоры создали решения, позволяющие "обойти" данное ограничение. Были разработаны технологии, в которых агрегированный канал создается из двух и более линий, соединяющих объединенные в один стек коммутаторы. При этом настройка такого решения выполняется аналогично созданию агрегированного канала в пределах одного коммутатора.

Подобные решения требуют специальной организации стека коммутаторов; они разработаны различными вендорами (HP, Nortel, Cisco и т. п.), но могут в каждом случае иметь уникальные названия. При этом конкретные реализации могут быть совместимы между оборудованием различных вендоров (например, MLT от Nortel идентичен технологии EtherChannel от Cisco и т. д.). Самым главным для администраторов сетей является тот факт, что два канала подключения любого его устройства к различным коммутаторам могут быть объединены в один агрегированный канал на основе открытого стандарта — 802.3ad таким образом, как будто подключение осуществляется к одному коммутатору. Например, так можно осуществить отказоустойчивое подключение сервера к ферме коммутаторов: достаточно, чтобы программное обеспечение было настроено на поддержку протокола LACP.

Добиться полной отказоустойчивости такого решения можно, объединив коммутаторы в *отказоустойчивый* стек. При его создании все коммутаторы объединяются

в кольцо, последний коммутатор объединяется возвратным стековым кабелем с первым коммутатором. В результате отказ любого устройства стека сохранит возможность передачи данных на верхний уровень сети. Такая конфигурация стека возможна не во всех моделях оборудования, поэтому выбор моделей коммутаторов должен учитывать требования к системе передачи данных и позволять создать необходимые конфигурации.

Построение отказоустойчивой сети на основе протоколов третьего уровня

Основным используемым на практике вариантом создания отказоустойчивой конфигурации сети на сегодня являются 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 сек), 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". Причем переключение на другие пути передачи данных в случае повреждения каналов связи будет происходить за счет изменения таблиц маршрутизации.

Недостаток такого решения — использование половины каналов: данные передаются только по одной линии связи, резервная не задействована в нормальных условиях.

VRRP

К коммутаторам уровней распределения и ядра подходят несколько каналов связи, в случае отказа одного из них с помощью того или иного используемого протокола работа продолжается на исправном. Но для рабочих станций (компьютеров виртуальной частной сети подразделения) обычно существует только одна точка доступа к другим сетям: *шлюз по умолчанию*. Это является узким местом такого решения, поскольку в случае выхода из строя шлюза компьютеры потеряют связь с другими сетями.

Для предупреждения подобных ситуаций можно использовать протокол *VRRP* (Virtual Routing Reduntance Protocol), конечно, если оборудование не поддерживает другие технологии, например, агрегированные каналы на разные коммутаторы стека или подключение к кластеру коммутаторов.

> ***Примечание***
>
> Протокол VRRP реализован далеко не на всех моделях коммутаторов. Как правило, модели, приобретаемые малыми организациями, не имеют поддержки данного протокола.

Идея создания отказоустойчивого шлюза с использованием протокола VRRP состоит в следующем. В сети устанавливаются два коммутатора с поддержкой данного протокола. На каждом из них настраиваются сетевые интерфейсы и включается протокол VRRP. После этого проводится настройка интерфейса 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 они оба 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, не зависящая 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 обеспечения отказоустойчивости имеют оба устройства. Поэтому, например, в коммутаторах Nortel реализовано расширение функциональности протокола VRRP. Оба коммутатора будут работать в качестве шлюза и передавать данные в другие сети. Мы не будет останавливаться подробно на реализации такой технологии. При ее использовании к одному IP-адресу шлюза привязываются два MAC-адреса: один для клиентов первого коммутатора, другой — для клиентов второго. В результате пакеты, переданные на один шлюз (один IP-адрес), достигают различных устройств. Однако если один из них выйдет из строя, его 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 сети очень сложно. На основе использования открытых стандартов реально достичь восстановления обслуживания за период не более 3—5 сек.

Использование проприетарных технологий может сократить данный период менее чем до 1 сек. Однако к подобным прогнозам следует относиться крайне осторожно: часто даже крупные вендоры в маркетинговых целях презентуют крайне низкие значения периода восстановления (например, 20 мсек), не делая акцента на тех специальных условиях, при которых получен такой показатель. Если отказ внутри шассийного коммутатора может быть парирован за данную величину, но на восстановление после другой неисправности требуется несколько секунд, то 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 используемым технологиям, читать технические описания оборудования, обращая внимания на любые оговариваемые особенности. Во-вторых, стараться быть в кур-

се тестов, проводимых независимыми лабораториями, такими как Tolly Group (**http://www.tolly.com/**), обращая при этом внимание на условия проведения теста.

В-третьих, просчитывать необходимые параметры для конфигурации именно вашей сети. Каждая конфигурация индивидуальна, и не факт, что лучшее решение для идеальной лаборатории окажется таковым в реальной ситуации.

Серверные фермы

Серверная ферма представляет собой несколько совместно работающих серверов. Это решение, в первую очередь, направлено на балансировку нагрузки, но может рассматриваться и с точки зрения повышения отказоустойчивости.

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 — использовать балансировку сетевой нагрузки, решение, реализуемое стандартными средствами Windows-серверов.

Серверные фермы используют в тех случаях, когда нагрузку легко разделить между серверами. Например, для веб-серверов (между серверами можно распределить как запросы от разных пользователей, так и запросы внутри одной страницы) или для терминальных серверов (разделение по пользователям или приложениям).

Настройка серверной фермы осуществляется по соответствующей документации. Например, установщик веб-платформы Windows доступен к загрузке с адреса **http://go.microsoft.com/?linkid=9739157**. Как правило, обеспечение серверной фермы требует наличия соответствующей архитектуры системы (на рис. 10.1 показан пример архитектуры серверов Citrix).

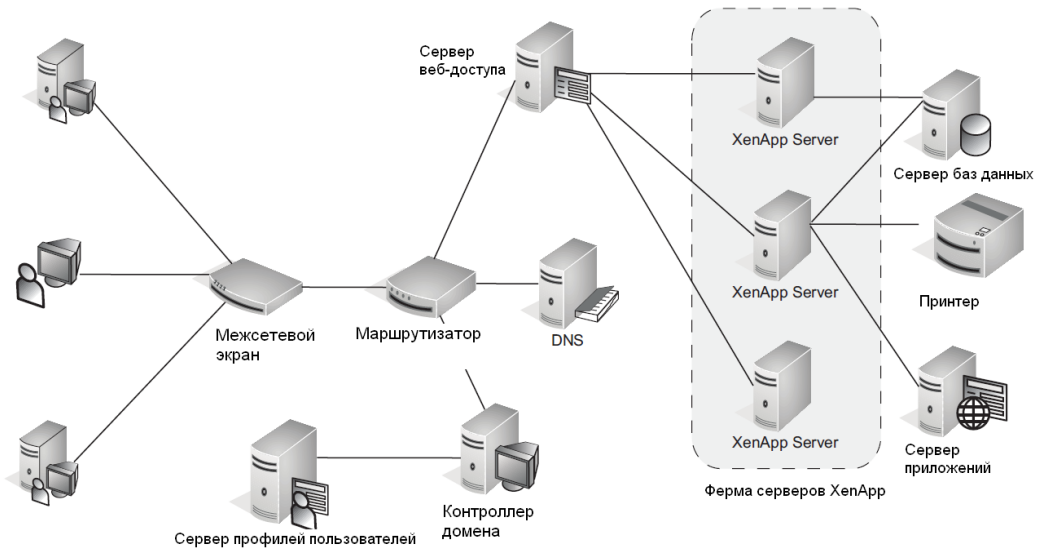


Рис. 10.1. Пример архитектуры фермы серверов Citrix

Отказоустойчивые решения приложений

Для многих приложений разработчики предусмотрели собственные механизмы обеспечения высокой доступности. Обычно такие варианты решений наиболее эффективны на практике.

DHCP-сервер

При построении отказоустойчивых информационных систем важно обеспечить стабильную работу сетевых служб, в том числе сохранить функционирование службы автоматического присвоения параметров IP-адреса в случае выхода сервера DHCP из строя.

Реализация DHCP на основе сервера Microsoft имеет серьезный недостаток, связанный с невозможностью создания горячего резерва данной службы для одного диапазона IP-адресов. Документы Microsoft предлагают для повышения отказоустойчивости два способа. Первый заключается в размещении службы DHCP на серверном кластере. В этом случае база адресов будет храниться на общем диске, а при выходе из строя одного сервера его работу "подхватит" второй сервер кластера. К сожалению, такое решение часто не доступно малым и средним организациям из-за высокой стоимости реализации отказоустойчивого кластера.

Второй вариант решения проблемы отказоустойчивости службы DHCP от Microsoft заключается в настройке для организации *двух* серверов DHCP с *различными* (неперекрывающимися) частями используемого диапазона адресов организации. В этом случае клиент будет получать параметры адреса от любого сервера (вернее, от того, который ответит раньше), а при выходе из строя одного из серверов второй продолжит обслуживание организации.

Иначе решается вопрос в Linux. Существует простой способ объединения двух или более серверов DHCP в отказоустойчивый пул. Для этого достаточно внести в конфигурацию DHCP-демона следующий блок настроек:

```
pool {

    failover peer "foo";

    pool specific parameters
};
```

(Параметры пула следует уточнить по онлайновой документации).

Пул использует один диапазон выделяемых адресов для всех серверов, серверы постоянно обмениваются информацией между собой и учитывают адреса, выданные каждым участником пула.

DNS-серверы

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.

Oracle Real Application Cluster (RAC)

Кластер Oracle RAC предназначен для обеспечения высокой доступности и распределения нагрузки приложений, работающих с сервером баз данных Oracle.

Oracle RAC — это кластерное решение для сервера баз данных с архитектурой общего кэша. В состав кластера может входить большое число серверов, при этом средства управления Oracle обеспечивают равномерное распределение нагрузки и перемещение вычислений в случае отказа одного из узлов.

Обратите внимание, что в отличие от описываемых в этой книге других кластерных решений, Oracle RAC загружает *все* серверы. Чем больше серверов, тем большая вычислительная мощность будет у распределенной базы данных.

Распределенная база 1С

Данное решение позволяет использовать программу 1С одновременно как в центральном офисе, так и в филиалах (складах, участках и т. п.). Решение основано на периодической синхронизации данных: изменения данных, внесенные на сервере, записываются в файл и передаются (например, по электронной почте) на другое рабочее место. Принятый файл автоматически обрабатывается, и данные вносятся в локальную копию.

Исходя из описанного принципа работы, понятны и ограничения: работа будет проходить без конфликтов, если организационными мерами разделить зоны ответственности операторов.

Дублирование данных

Одним из способов обеспечения надежной работы информационных систем являются различные технологии дублирования данных. Принцип хранения данных на двух или более серверах во многих случаях оказывается достаточным для требуе-

мого уровня безопасности системы, а реализуются такие решения многими способами, причем часто не требующими дополнительных затрат.

Зеркалирование серверов баз данных

Большинство приложений, работающих с систематизированными данными, хранит их на серверах баз данных или SQL-серверах. В связи с распространенностью для SQL-серверов разработаны решения, обеспечивающие дублирование данных одного сервера на другом.

Репликация данных SQL-серверов

Репликацию данных часто называют *зеркалированием* баз данных.

> ***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 от, например, построения кластерной системы:

- отсутствие необходимости использования дополнительного оборудования (систем хранения данных), дублирование производится по обычной сети передачи данных;
- зеркалирование можно настроить раздельно для каждой базы (в кластере резервируется все базы сервера);
- нет ограничений по оборудованию, которое может применяться для других вариантов (например, по числу процессоров);
- 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. п., 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. Простейший случай, когда данные могут меняться только на одном сервере. Обычно проблем при таком варианте настроек не возникает.

Проблемы будут, 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, выбор алгоритма 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 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. Данная 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.

Распределенная файловая система

Подключение к общим сетевым ресурсам традиционно осуществляется с использованием следующего пути: `\\сетевое_имя_сервера\имя_ресурса`. Понятно, что при выходе из строя сервера-источника, сетевой ресурс становится недоступным.

Распределенная файловая система призвана исключить такую точку отказа, позволяя клиентам использовать не привязанные к конкретным системам пути. 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.

Создание DFS

Структура DFS напоминает дерево каталогов: на самом "верху" расположена одна точка входа, называемая *корнем DFS*, к которой подключены вложенные папки. Корень DFS представляет собой коллекцию ссылок на совместно используемые ресурсы, находящиеся на различных компьютерах сети. Следует заметить, что структура DFS-домена хранится в службе каталогов (AD).

Корень DFS может быть создан на любом сервере Windows 200*x*, причем на рядовых серверах возможно создание только одного корня DFS, тогда как в домене может поддерживаться *несколько корней DFS* (разными контроллерами).

В качестве корня DFS указывается любая совместно используемая папка (мастер создания DFS позволяет создать такую папку в процессе настройки). Рекомендуется не хранить в этой папке никаких файлов, а использовать ее только для создания ссылок на сетевые ресурсы.

После создания корня DFS необходимо начать "собирать" структуру папок распределенной файловой системы. Для этого с помощью оснастки управления DFS следует добавить ссылки на уже существующие *совместно используемые ресурсы сети*. Причем возможно указать несколько ссылок на аналогичные ресурсы на разных компьютерах. Операция обычно не представляет никакой сложности.

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 для клиентов все используемые ими сетевые пути (если, конечно, они указывали на структуру DFS) останутся неизменными.

> ***Примечание***
>
> Конечно, можно воспользоваться и средствами автоматической репликации для такого переноса данных (создать пустую папку и добавить ее в репликацию). Но при большом объеме файлов ресурсов системы может не хватить для нормального завершения операции. Например, на практике автора система потребовала изменения настроек в реестре при попытке создания автоматической копии структуры папок документов объемом порядка 5 Гбайт.

Репликация DFS

Как уже говорилось, структуру DFS можно сделать *отказоустойчивой*. Каждую ссылку можно продублировать, создав вторую ссылку на аналогичный сетевой ресурс на другом компьютере. В результате при недостижимости одного ресурса клиенты будут автоматически 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 должны быть расположены в папках с NTFS 5.0, поскольку система использует систему протоколирования этой файловой структуры для отслеживания изменений.

> ***Примечание***
>
> Если необходимо использовать ограничения прав доступа к документам в папках DFS, то эти настройки следует применить *только* к папкам сервера (\\<*имя_сервера*>\<*имя_папки*>). Иначе при создании ссылки DFS по новому месту репликации папка унаследует права родительской структуры.

По умолчанию репликация не включена. Чтобы организовать синхронизацию данных нескольких серверов, необходимо выделить соответствующие ссылки на ресурсы и выбрать команду **Синхронизовать**. При создании репликации требуется указать, какой ресурс будет являться основным *(мастером)*. Когда первоначальная репликация завершится, все ссылки станут равнозначными: изменение в одном месте повлечет изменение по другой ссылке.

> ***Примечание***
>
> Существует несколько технологий репликации. В общем случае необходимо учитывать структуру организации, практику работы с документами и т. п. В большинстве случаев достаточно согласиться с предложением мастера создания репликации.

Автоматически синхронизируются не все файлы. Из репликации исключаются временные файлы (список расширений можно просмотреть в настройках). Сами файлы реплицируются только после того, как с ними завершена работа пользователя. 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.

Репликацию можно использовать для поддержания копий документов на нескольких территориально разделенных площадках. Тем более, что в последних версиях серверов используется механизм пересылки только измененных блоков, а не всего документа, что снижает трафик между узлами. Тем не менее, часто имеет смысл ограничить время репликации периодами минимальной загрузки канала. Для этого в меню расписания следует определить разрешенные периоды, в течение которых будет проводиться синхронизация данных.

Настраивается график репликации 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 (рис. 10.2).

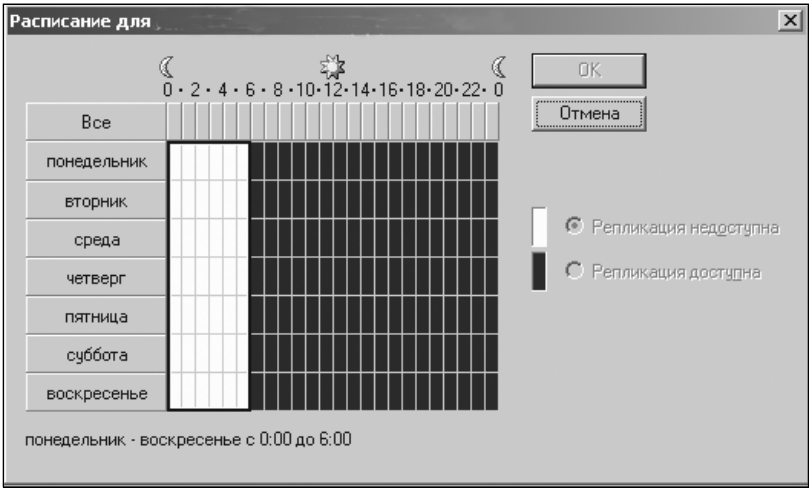


Рис. 10.2. Настройка графика репликаций DFS

Поддержка DFS в Linux-системах

На Linux-системах могут быть размещены корни DFS. Обеспечивает эту функциональность пакет Samba. Для того чтобы разместить корень DFS, достаточно в глобальной секции конфигурации Samba указать `host msdfs = yes`, а в определение совместно используемого ресурса добавить `msdfs root = yes`.

Поскольку корни DSF включают линки на другие совместно используемые ресурсы, то для их создания используется команда `ln` с указанием типа ресурса (`msdfs`):

```
# ln -s msdfs:storageA\\shareA linka
# ln -s msdfs:serverB\\share,serverC\\share linkb
```

Указание двух линков на один ресурс соответствует включению балансировки ресурсов.

В результате настройка корня DFS в конфигурации демона Samba будет выглядеть примерно так:

```
...
    [global]
        host msdfs = yes
...
    [dfs]
        path = /usr/local/samba/dfs
        msdfs root = yes
...
```

Корни DFS на Samba-сервере функционируют со всеми DFS-клиентами Windows (начиная от Windows 95).

Администратор должен назначить необходимые права доступа на папки с ресурсами и проконтролировать, чтобы на момент создания состав предполагаемых к балансировке папок был идентичным.

> ***Примечание***
>
> Имена DFS-корням в Samba должны назначаться только в нижнем регистре. Если администратор преобразует в корень DFS существующий совместно используемый ресурс, то клиенты Windows в таком случае нуждаются в перезагрузке.

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[1] Edition или Datacenter. Для создания кластера необходимо 2 физических

[1] Advanced Server, если говорить о версии Windows 2000 Server.

сервера (желательно идентичных) и система хранения, позволяющая осуществить одновременное подключение диска к двум серверам. Для подключения системы хранения обычно используется технология FC (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 2003 Server 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. 10.3.

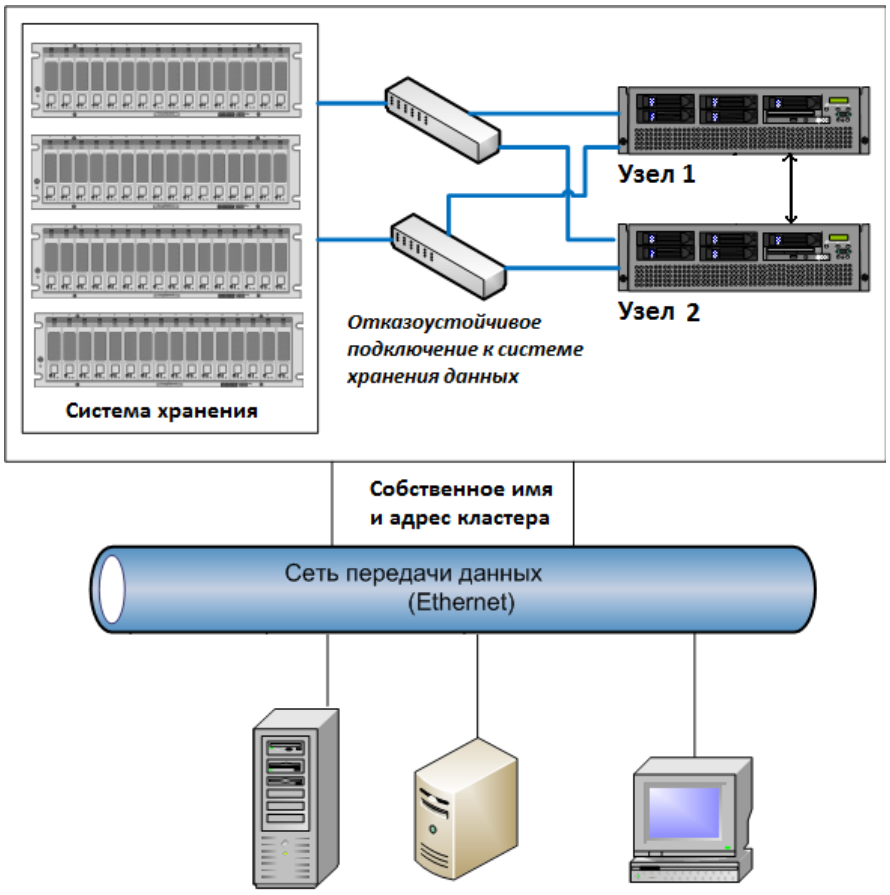


Рис. 10.3. Вариант построения кластера от Microsoft

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, 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 сервер баз данных и почтовый сервер.

При установке приложения в кластер используется специальный вариант запуска программы установки, который создает новый экземпляр сервера (новое имя, новый адрес) и прописывает в настройках службы кластеров параметры резервированных компонент.

На рис. 10.4 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.

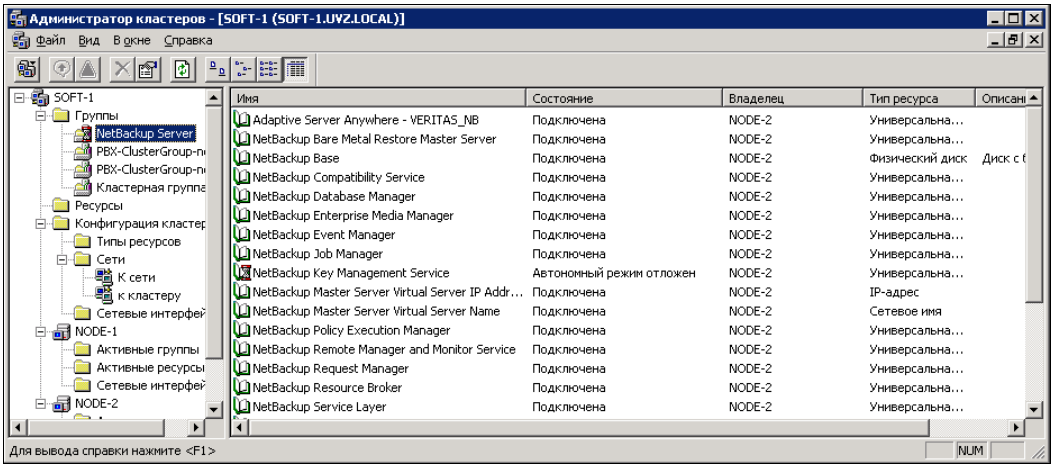


Рис. 10.4. Администратор кластеров для ресурсов NetBackup

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 что 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 распространено 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 сети Интернета). Существуют варианты конфигурации кластера, которые используют разнесенные системы хранения, данные на которых реплицируются средствами самой системы хранения и т. п. (рис. 10.5).

Основное преимущество данного решения — большая распространенность, универсальность и наличие более широкого круга приложений.

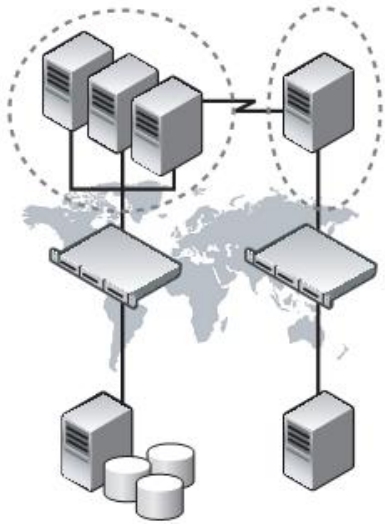


Рис. 10.5. Территориально разнесенный кластер

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. 10.6 из документации продукта).

Рис. 10.6. Логическая структура виртуального сервера everRun

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 мсек. 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.

Главная особенность технологии состоит в том, как создаются виртуальные компоненты. Они создаются из реальных компонентов на уровне операций. Например,

[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.

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. 10.7 из документации производителя).

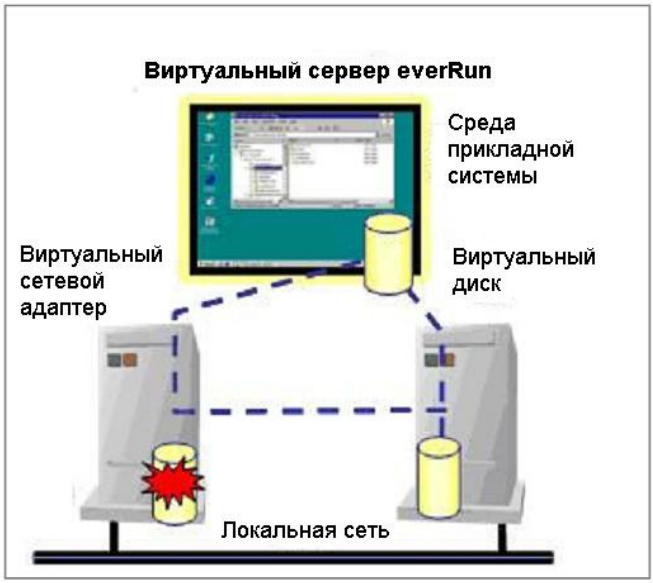


Рис. 10.7. Построение виртуального диска при отказе одного физического диска

Аналогично система будет вести себя при выходе из строя сетевого адаптера и других компонент. 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 только специально разработанные приложения, то технология everRun защищает *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.

Распределенные каталоги

Для обеспечения централизованного управления сетевыми ресурсами (пользователи, серверы, общие папки, принтеры и т. п.) были созданы как специализированные средства — *каталоги*, так и стандартизованы протоколы работы с ними (X500, LDAP и т. д.). Понятно, что реализация каталогов изначально строилась с учетом обеспечения распределения нагрузки и исключения единой точки отказа.

Существует много реализаций каталогов, но среди коммерческих продуктов можно отметить Microsoft Active Directory (для серверов Windows NT 4 служба называлась NT Directory Service (NTDS)), среди бесплатных — проект OpenLDAP.

Репликация данных каталогов

В целях отказоустойчивости в системе обычно устанавливается несколько серверов каталогов. Между ними настраивается репликация данных.

В службе каталогов Microsoft в целях отображения физической структуры системы на логическую введено понятие *сайта*. Сайт объединяет серверы (и пользовательские системы) в пределах локальной сети (быстрые каналы связи). Сайты объединяются друг с другом более медленными линиями, например, ATM, ISDN, T1, T3 и т. п. Основываясь на оценке скорости канала связи между серверами каталогов, система создает правила репликации. Для сложных структур информационных систем, особенно в случае наличия разнотипных каналов связи, эту операцию лучше выполнить вручную, явно указав, как должны передаваться данные. Это может стать сложной задачей, интересующегося читателя мы отошлем к первоисточнику по управлению межсайтной репликацией — **http://technet.microsoft.com/en-us/library/cc961783.aspx**.

Хозяева операций

Для функционирования распределенной системы службы каталогов необходима постоянная синхронизация данных всех серверов. Поскольку в реальной жизни невозможно исключить сбои, то были разработаны специальные механизмы обеспечения работы распределенной структуры. Так появились *хозяева операций.*

Хозяин операции — это сервер каталога, являющийся головным (мастер-сервером) по какой-либо функции. 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 контролировал, что все эти пять операций не потеряли хозяина.

Смена хозяев операций

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.

При корректном исключении сервера каталога (путем снижения его роли командой `dcpromo`) мастер операций отслеживает состояние ролей. В случае аварий система может остаться без хозяина какой-либо роли. В этом состоянии служба каталогов не может находиться долго, необходимо назначить нового хозяина операции.

Все операции по переносу ролей можно выполнить в командной строке. Для этого используется утилита ntdsutil. Главное, что эту утилиту можно использовать не только для переноса ролей при *работающих* контроллерах, но и для *назначения* нового владельца роли в случае аварийного выхода из строя прежнего хозяина.

> ***Примечание***
>
> Назначение ролей следует использовать с осторожностью, при наличии 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 чего 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.

> ***Примечание***
>
> Если в структуре предприятия присутствует *несколько* доменов, то совмещение ролей Infrastructure Master с сервером глобального каталога *недопустимо*.

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 системе создаются специальные контроллеры, которые хранят (в режиме *только для чтения*) *все объекты леса*, но только 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 выполняется через оснастку AD Сайты и Службы. Раскрыв узел, соответствующий нужному контроллеру, в свойствах **NTDS Settings** необходимо включить параметр использования контроллера в качестве GC.

Примечание

В локальных сетях рекомендуется назначать серверами глобального каталога не менее двух контроллеров домена.

Серверы GC хранят наиболее часто используемые атрибуты объектов. Условно можно считать, что объем хранимых на GC данных снижается примерно в 2 раза по сравнению с "полным" вариантом описания объекта. Но если конкретным приложениям необходим частый доступ к нереплицируемым атрибутам, то администратор может внести изменения в параметры GC, откорректировав *схему организации*. Для этого достаточно в консоли управления оснасткой AD Schema включить репликацию в свойствах соответствующих атрибутов; по умолчанию этой оснастки нет в списке меню, ее следует добавить в консоль управления.

Примечание

Некоторые приложения активно используют обращения к GC. Например, MS Exchange Server. В этих случаях сервер GC обязательно должен быть включен в соответствующий сайт ("рядом" с таким приложением).

В реальной сети необходимо обеспечить некую разумную избыточность GC, имея в виду, что каждый дополнительный GC — это и дополнительный объем копирования данных, передача которых может привести к повышенной нагрузке на системы и каналы связи.

Отказоустойчивые решения на виртуальных системах

В корпоративных версиях VMware реализуются технологии обеспечения высокой доступности. Компоненты vSphere для обеспечения высокой доступности должны быть специально приобретены предприятием (входят только в максимальные комплектации).

Высокая доступность реализуется за счет параллельной работы нескольких виртуальных машин. Специальные компоненты обеспечивают синхронизацию оперативной памяти двух машин и переключение расчетов в случае отказа основной виртуальной системы. Соответственно, по этой технологии защищаются любые приложения и данные на виртуальной машине.

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 (vCenter) и создания решения высокой доступности на существующем кластере высокой доступности VMware, 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.

Среди особенностей данного решения от VMware следует отметить, что высокодоступное решение может быть реализовано для любых операционных систем, которые поддерживаются vSphere.

ГЛАВА 11

Порядок настройки и определения неисправностей

Отказы информационной системы все в большей степени влияют на эффективность бизнес-процессов предприятия, поэтому одна из главных задач администратора работающей системы состоит в *предупреждении* отказов и максимальном сокращении времени простоя обслуживания.

Прежде чем начать...

Если отказ все же случился, не спешите сразу же начинать что-то *делать*. Попробуйте успокоиться, может быть, выпить кофе и только после этого приступать к активной деятельности.

Прежде всего, попытайтесь получить о неисправности максимум информации как от пользователей, так и по данным объективного контроля.

Попытайтесь конкретизировать проблему. После этого следует составить предварительный перечень возможных причин отказа с оценкой времени устранения по каждой позиции. Старайтесь не начинать ремонт с наиболее затратных позиций, если только вы абсолютно не уверены, что именно они явились причиной неисправности.

Выполните операции, которые вы запланировали для ликвидации отказа. Проверьте результат. Если успех не достигнут, то придется повторить шаги: высказать новые предположения о причинах, составить новый план действий и т. д.

Не пытайтесь вносить сразу много изменений в настройки. Протоколируйте все свои шаги. Часто, если систему не удается восстановить за короткое время, без таких записей очень сложно не запутаться и вернуться к исходной точке.

Если вы долго не можете справиться с отказом, попробуйте рассказать о неисправности кому-либо еще. Во-первых, пытаясь объяснить проблему, вы разложите ее для себя "по полочкам". Во-вторых, советы неспециалистов часто могут направить вас на неожиданный путь решения.

Обязательно составьте какой-нибудь документ по результатам инцидента, чтобы специалисту, который придет на ваше место, было легче ориентироваться в состоянии системы.

Пять девяток?

Цель, которую ставят изготовители оборудования и разработчики программного обеспечения, — достичь доступности информационной системы на "пять девяток" — 99,999%. При круглосуточной работе этот показатель соответствует примерно пяти минутам простоя *за год*.

Конечно, достижение такого показателя требует весьма существенных затрат как на соответствующее оборудование, так и на обслуживание, нереальных для малых и средних организаций. В то же время в силах системного администратора как наладить работу по предупреждению отказов, так и создать условия для оперативного восстановления информации. Администратор должен быть готов к возникновению любой нештатной ситуации и иметь некий план действий — 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 оговорены. С другой стороны, этот план станет инструкцией, что нужно делать в аварийной ситуации.

Будьте готовы к худшему

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, что независимо от принимаемых мер защиты ваша система либо может быть взломана, либо возникнет другая ситуация с полной потерей данных. И практически единственное, что может помочь, — это подготовленность к восста-

новлению данных "с нуля", наличие и регулярное создание резервных копий информации.

Получить копию данных, достаточную для полного восстановления сервера, можно различными способами. Начиная от обычных операций копирования на отчуждаемый носитель и заканчивая коммерческими системами поддержания актуальной копии данных в реальном режиме времени. Все зависит от требований, предъявляемых к информационной системе. Сколько данных может быть потеряно, за какой период времени система должна быть восстановлена "с нуля" и т. п.

Главное, что нужно запомнить, — резервная копия, резервная копия и еще раз резервная копия!

Запасные детали

Любая информационная система нуждается в ЗИП — запасных инструментах и принадлежностях. 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% — цифра 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...

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".

- **Windows Help.**

  Первое, к чему необходимо обратиться при возникновении любой проблемы в работе компьютера, — это встроенная справочная система. С каждой новой версией Windows эти системы становятся все более содержательными и полезными (если только вы знаете, что хотите найти, и правильно формулируете условия поиска).

- **Онлайновая база данных Microsoft.**

  Громадный объем документации содержится на сайте корпорации Microsoft по адресу **http://msdn.microsoft.com/**. В различных разделах этого ресурса вы можете найти как описания работы отдельных компонентов операционной систе-

мы, так и технические статьи, содержащие сведения об обнаруженных ошибках и методах их устранения.

Онлайновая справочная база Microsoft локализована практически в полном объеме. Страницы с русской версией сайта корпорации можно найти по адресу **http://www.microsoft.com/rus/**, однако следует учитывать, что англоязычные материалы публикуются оперативнее переводов.

- **Материалы Интернета.**

Способы разрешения многих проблем, особенно если таковые случились не только у одного пользователя, можно найти на многочисленных сайтах сети Интернет. 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. Не стоит надеяться, что вы гарантированно получите ответ, но обращение в конференцию является одним из наиболее эффективных способов получения необходимой помощи. Обычно ту или иную подсказку по проблеме удается найти поиском по сообщениям в тематической конференции.

> ***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 сократить 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. Для оценки можно принять, что стоимость сопровождения за год составляет примерно пятую часть стоимости оборудования и программного обеспечения. 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 о приобретении пакета данной поддержки должно приниматься индивидуально с учетом анализа опыта других предприятий.

Сбор информации об отказе

Для успеха восстановления большое значение имеет качество собранной информации об отказе. Вначале проверьте кажущиеся очевидными факты: включено ли оборудование, горят ли индикаторы состояния, не появились ли дополнительные шумы и т. п.

Затем систематизируйте информацию о системе:

- доступные журналы (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.

Анализ журналов системы

Неисправность практически невозможно определить без обращения к протоколам, в которых фиксируются события, возникающие в системе. 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.

На практике часто для анализа проблемы приходится собирать информацию с нескольких систем. Можно выполнить это штатными средствами, например, просто подключаясь к журналу удаленного компьютера в консоли Просмотр событий. Но администратор обычно не ограничивается штатными средствами. Для сбора данных и последующего анализа используются любые доступные утилиты сторонних разработчиков, контролирующие систему в реальном режиме времени. На рис. 11.1 приведен пример подобной программы, которая отображает результаты доступа

к службе каталогов домена Windows. При этом вы можете видеть, какая программа и какой запрос адресовала к AD, оценить ответ службы, скорость его формирования и т. п.

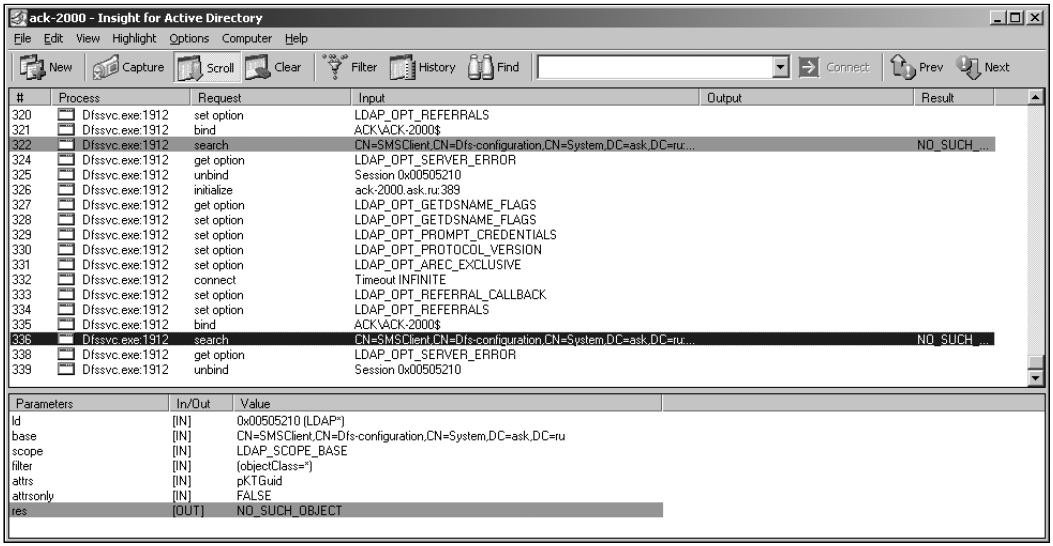


Рис. 11.1. Insight for Active Directory протоколирует все попытки доступа к службе каталогов на контроллере домена

Средства просмотра журналов системы

В Windows для просмотра журналов событий применяется специальная программа Просмотр событий (рис. 11.2), вызов которой выполняется через **Панель управления | Административные задачи | Просмотр событий.**

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. Читать их удобно при помощи команды `tail`, позволяющей отображать события в реальном режиме вре-

мени. 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 (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.

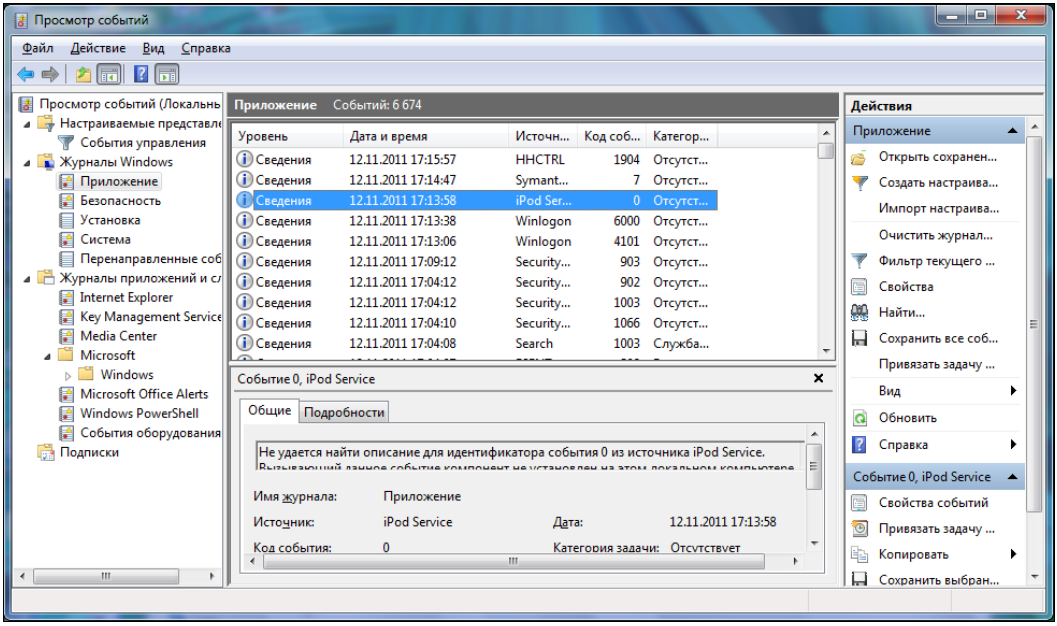


Рис. 11.2. Средство просмотра журнала событий в Windows 7

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, от-

фильтровать 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>
```

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/2008R2 присутствует возможность настройки сбора событий с различных компьютеров. Для этого используется опция **Подписка.**

При создании подписки (рис. 11.3) 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 2003 Server, режим подписки с которыми не работает. В этом случае можно использовать скрипт EVENTQUERY.vbs из состава Windows 2003 Server, который позволяет вывести события как с локального, так и с удаленных компьютеров, используя необходимые фильтры (по дате, по номеру события, типу и т. п.).

[1] Программа samba обеспечивает реализацию общего доступа к файловым ресурсам и принтерам, совместимого с аналогичным в системах Windows.

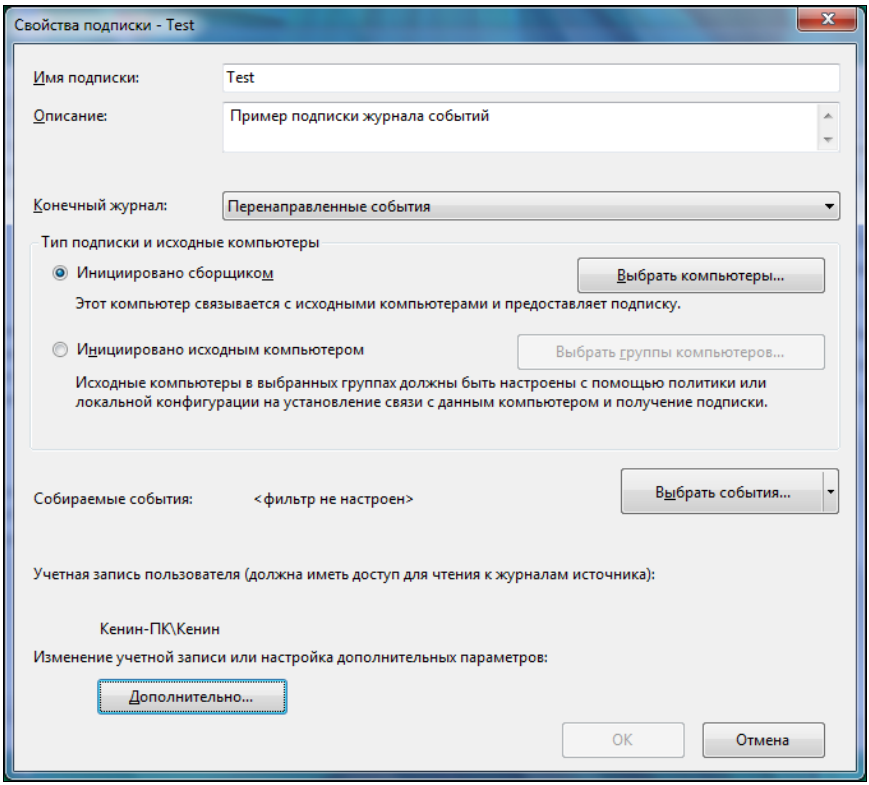


Рис. 11.3. Настройка подписки в Windows 7

Правда, в отличие от режима "Подписка" данный сценарий каждый раз проводит анализ событий на удаленных системах и возвращает отобранные события.

При желании использовать графический интерфейс при анализе журналов можно обратиться к специальной утилите — EventCombMT, бесплатно загружаемой с сервера Microsoft (рис. 11.4).

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.

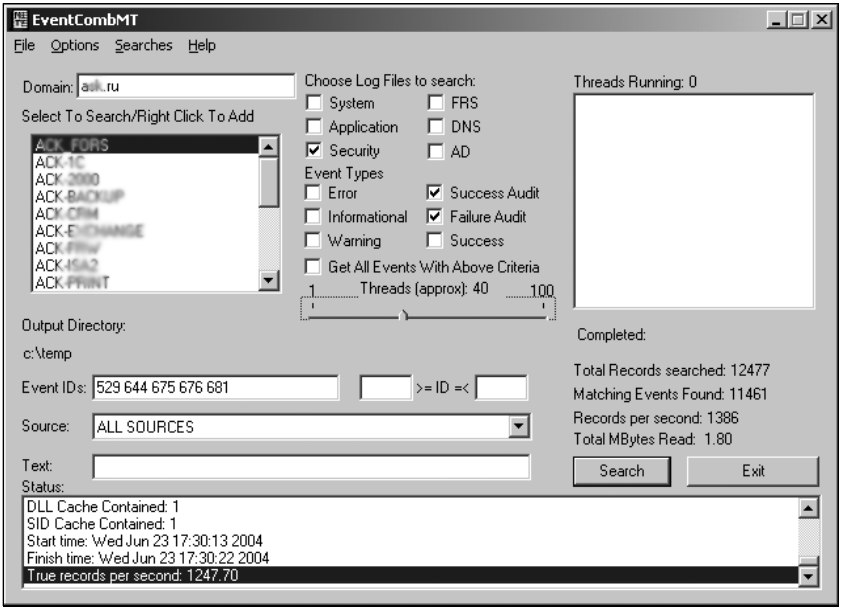


Рис. 11.4. Окно утилиты *EventCombMT*

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. 11.5 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.).

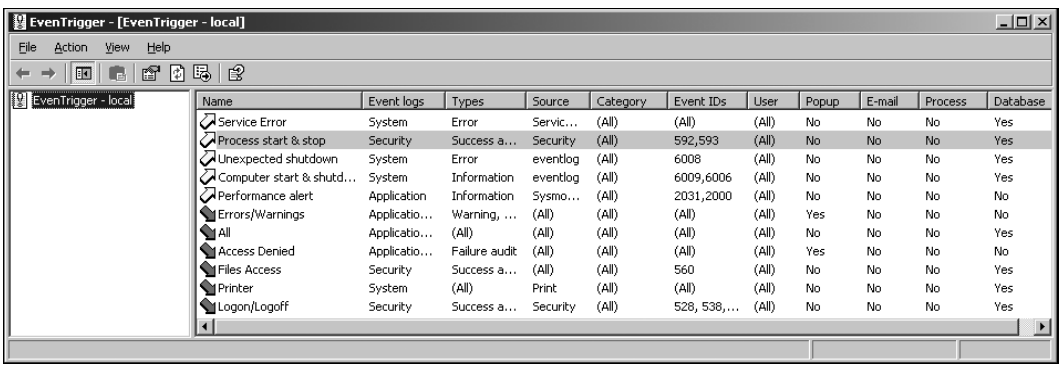


Рис. 11.5. Окно программы *EvenTrigger*

Подобные функции реализованы и во многих других программах, доступных системным администраторам (GFI LANGuard Security EventLog Monitor, Microsoft Operation Management Server и т. д.).

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/Vista/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. 11.6).

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 2003 Server в журналы можно записать и пользовательские события. Это команда `EVENTCREATE`. Использование утилиты подробно описано в ее справке (`EVENTCREATE /?`), поэтому мы не будем специально приводить ее описание.

Для систем более ранних, чем Windows 2003 Server, 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.

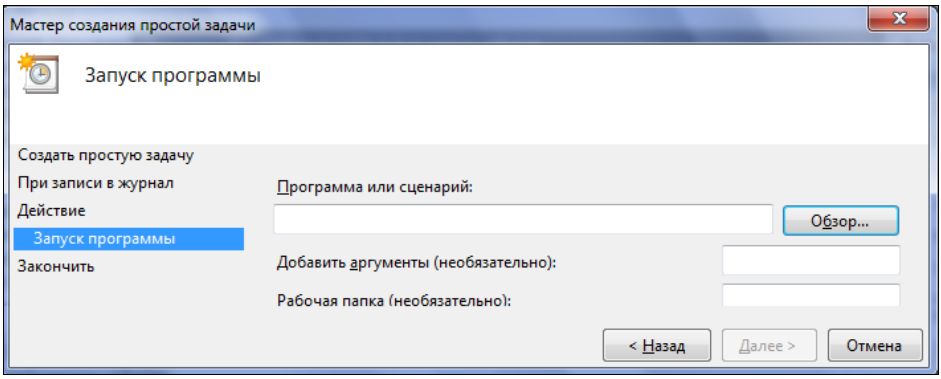


Рис. 11.6. Мастер создания простой задачи на возникновение события в журнале

Настройка аудита событий безопасности

Объем событий, которые фиксируются в журнале безопасности, целиком определяется настройками системы, и их журналирование по умолчанию на рабочих станциях не ведется. Наиболее полный объем аудита событий безопасности можно установить при наличии на диске файловой системы NTFS.

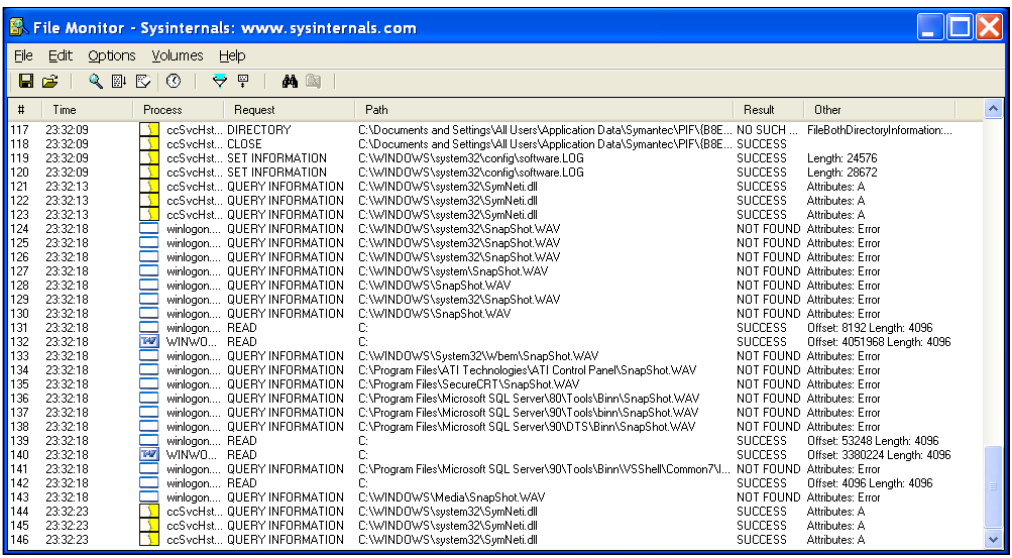
Чтобы начать протоколирование событий безопасности, необходимо сначала *разрешить аудит* событий безопасности в политике безопасности. Это может быть сделано как локально — в локальной политике безопасности, так и централизованно — путем задания соответствующих параметров в групповой политике. Если администратор хочет отслеживать доступ к файлам и принтерам, то следует *задать объекты*, для которых должен осуществляться аудит событий.

> ***Примечание***
>
> Политика безопасности включает возможность аудита как успешных, так и неудачных событий для различных объектов. Не следует без необходимости вести аудит всех событий, поскольку это может привести к нерациональной загрузке компьютера и потери производительности.

Если необходимо вести протокол работы с файлами, то следует включить аудит доступа к объектам, после чего в свойствах объекта на вкладке **Безопасность** следует нажать кнопку **Дополнительно** и выбрать вкладку **Аудит**. Затем нужно добавить сведения о том, какие действия и от каких пользователей следует фиксировать в журнале.

Утилиты от Sysinternals

Для поиска проблем администратору часто необходимо отслеживать процессы доступа программ к файлам, к реестру системы и т. д. Наблюдение за такими процес-



#	Time	Process	Request	Path	Result	Other
117	23:32:09	ccSvcHst...	DIRECTORY	C:\Documents and Settings\All Users\Application Data\Symantec\PIF\{B8E...	NO SUCH ...	FileBothDirectoryInformation:...
118	23:32:09	ccSvcHst...	CLOSE	C:\Documents and Settings\All Users\Application Data\Symantec\PIF\{B8E...	SUCCESS	
119	23:32:09	ccSvcHst...	SET INFORMATION	C:\WINDOWS\system32\config\software.LOG	SUCCESS	Length: 24576
120	23:32:09	ccSvcHst...	SET INFORMATION	C:\WINDOWS\system32\config\software.LOG	SUCCESS	Length: 28672
121	23:32:13	ccSvcHst...	QUERY INFORMATION	C:\WINDOWS\system32\SymNeti.dll	SUCCESS	Attributes: A
122	23:32:13	ccSvcHst...	QUERY INFORMATION	C:\WINDOWS\system32\SymNeti.dll	SUCCESS	Attributes: A
123	23:32:13	ccSvcHst...	QUERY INFORMATION	C:\WINDOWS\system32\SymNeti.dll	SUCCESS	Attributes: A
124	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\system32\SnapShot.WAV	NOT FOUND	Attributes: Error
125	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\system32\SnapShot.WAV	NOT FOUND	Attributes: Error
126	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\system32\SnapShot.WAV	NOT FOUND	Attributes: Error
127	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\system\SnapShot.WAV	NOT FOUND	Attributes: Error
128	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\SnapShot.WAV	NOT FOUND	Attributes: Error
129	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\system32\SnapShot.WAV	NOT FOUND	Attributes: Error
130	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\SnapShot.WAV	NOT FOUND	Attributes: Error
131	23:32:18	winlogon....	READ	C:	SUCCESS	Offset: 8192 Length: 4096
132	23:32:18	WINWO...	READ	C:	SUCCESS	Offset: 4051968 Length: 4096
133	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\System32\Wbem\SnapShot.WAV	NOT FOUND	Attributes: Error
134	23:32:18	winlogon....	QUERY INFORMATION	C:\Program Files\ATI Technologies\ATI Control Panel\SnapShot.WAV	NOT FOUND	Attributes: Error
135	23:32:18	winlogon....	QUERY INFORMATION	C:\Program Files\SecureCRT\SnapShot.WAV	NOT FOUND	Attributes: Error
136	23:32:18	winlogon....	QUERY INFORMATION	C:\Program Files\Microsoft SQL Server\80\Tools\Binn\SnapShot.WAV	NOT FOUND	Attributes: Error
137	23:32:18	winlogon....	QUERY INFORMATION	C:\Program Files\Microsoft SQL Server\90\Tools\binn\SnapShot.WAV	NOT FOUND	Attributes: Error
138	23:32:18	winlogon....	QUERY INFORMATION	C:\Program Files\Microsoft SQL Server\90\DTS\Binn\SnapShot.WAV	NOT FOUND	Attributes: Error
139	23:32:18	winlogon....	READ	C:	SUCCESS	Offset: 53248 Length: 4096
140	23:32:18	WINWO...	READ	C:	SUCCESS	Offset: 3380224 Length: 4096
141	23:32:18	winlogon....	QUERY INFORMATION	C:\Program Files\Microsoft SQL Server\90\Tools\Binn\VSShell\Common7\I...	NOT FOUND	Attributes: Error
142	23:32:18	winlogon....	READ	C:	SUCCESS	Offset: 4096 Length: 4096
143	23:32:18	winlogon....	QUERY INFORMATION	C:\WINDOWS\Media\SnapShot.WAV	NOT FOUND	Attributes: Error
144	23:32:23	ccSvcHst...	QUERY INFORMATION	C:\WINDOWS\system32\SymNeti.dll	SUCCESS	Attributes: A
145	23:32:23	ccSvcHst...	QUERY INFORMATION	C:\WINDOWS\system32\SymNeti.dll	SUCCESS	Attributes: A
146	23:32:23	ccSvcHst...	QUERY INFORMATION	C:\WINDOWS\system32\SymNeti.dll	SUCCESS	Attributes: A

Рис. 11.7. Программа протоколирует операции доступа к файлам компьютера

сами может существенно помочь в выяснении причин сбоев. В этом случае можно воспользоваться бесплатными утилитами, доступными для загрузки с сайта **www.sysinternals.com** (**http://technet.microsoft.com/ru-ru/sysinternals**). Окно одной из таких утилит представлено на рис. 11.7.

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.

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. Некоторые возможные решения по мониторингу изложены в *главе* 7.

Неисправности подсистемы передачи данных

С одной стороны, неисправность подсистемы передачи данных легко обнаружить. Достаточно попытаться скопировать по сети большой файл, например, в 100 Мбайт. По сети с пропускной способностью 100 Мбит/сек файл должен передаться менее чем за 20 сек, для гигабитной сети — менее чем за 5 сек. Если время копирования больше, то следует искать проблемы.

С другой стороны, такие отказы часто бывает сложно локализовать. Например, автор встречался с ситуациями, когда пересохший кабель приводил к исчезающим проблемам при незначительном его перемещении, когда неисправность была связана с плохим контактом в разъеме сетевого адаптера, который приводил к нестабильной работе после того, как патчкорд просто задевали, когда ошибки возникали в работе коммутатора, продолжавшего безмятежно мигать своими индикаторами и т. п.

Обнаружение неисправностей сетевой инфраструктуры

Неисправность пассивной инфраструктуры можно определить специальными тестерами. Они с помощью особых тестов проверяют линии связи на соответствие всем требованиям стандарта (см., например, рис. 3.7). 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.

Случаи выхода из строя сетевых портов нередки. 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).

Если порты исправны, то между ними должны передаваться пакеты данных. Сегодня в большинстве систем применяется протокол TCP/IP, поэтому опишем последовательность проверки соединения для такого случая.

Диагностика IP-протокола

Для диагностики соединения с использованием протокола TCP/IP рекомендуется использовать следующую 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/200x/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 после запуска утилиты ifconfig, с помощью одноименной 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 симво-

лов 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 следующую 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. Вы должны увидеть приблизительно следующие строки:

   ```
   kenin@test:~$ ping -c 1 127.0.0.1
   PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
   64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.100 ms

   --- 127.0.0.1 ping statistics ---
   1 packets transmitted, 1 received, 0% packet loss, time 0ms
   rtt min/avg/max/mdev = 0.100/0.100/0.100/0.000 ms
   ```

   > ***Примечание***
   >
   > В листинге приведена информация, выводимая данной командой в среде Ubuntu. Поскольку в ОС Linux команда `ping`, применяемая без ключей, передает пакеты непрерывно, то явно указана необходимость посылки только одного пакета (можно ввести команду без ключа с последующим прерыванием посылки пакетов сочетанием клавиш <Ctrl>+<C>).

   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>
   ```

   Результат, который должен быть выведен на экран в случае нормальной работы, практически аналогичен полученному в предыдущем примере.

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 мсек. Наличие такого отклика свидетель-

ствует, 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.

Проверка доступности приложений на удаленном компьютере

Часто администраторы запрещают в межсетевых экранах прохождение ping-пакетов, открывая только порты, используемые установленными приложениями. В этом случае убедиться в доступности удаленного компьютера можно, если вы знаете порт, на котором работает соответствующая программа. Например, в практике автора был случай, когда администраторами провайдера были закрыты порты, необходимые для создания безопасного подключения.

Существуют различные возможности проверить удаленные системы. Во-первых, в Support Tools 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
```

Результатом будет, например, такой вывод:

```
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`).

Сходные утилиты, позволяющие получить ответ на запрос, отправленный на конкретный порт, легко найти в Интернете. Но проще использовать программу telnet, которая входит в состав всех операционных систем. Для систем Windows

NT 6.0 и старше ее надо добавить в число установленных компонентов (она называется *клиентом telnet*). В предыдущих версиях утилита доступна по умолчанию. Запуская эту утилиту с параметрами в виде имени удаленной системы и номером порта, вы осуществляете попытку подключения к соответствующему порту. Если попытка подключения будет происходить, то либо на экране появится ответ, либо экран на некоторое время "зависнет", после чего соединение разорвется по тайм-ауту. Если порт не отвечает, то вы увидите на экране сообщение о невозможности подключения. Далее приведен листинг команды `telnet` при проверке доступности порта 25 (порт почтового сервера, попытка неудачна) и 80 (порт сервера WWW, видно, что порт ответил на запрос).

```
>telnet 192.168.29.1 25
Подключение к 192.168.29.1...Не удалось открыть подключение к этому узлу, на
порт 25: Сбой подключения

>telnet 192.168.29.1 80
HTTP/1.0 400 Bad Request
Date: Fri, 11 Nov 2011 10:58:58 GMT
Server: Boa/0.94.11
Connection: close
Content-Type: text/html; charset=ISO-8859-1
<HTML><HEAD><TITLE>400 Bad Request</TITLE></HEAD>
<BODY><H1>400 Bad Request</H1>
Your client has issued a malformed or illegal request.
</BODY></HTML>
```

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 команды `tracert` таков:

```
E:\ 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.
```

Утилита показывает узлы, через которые пересылается пакет, и задержку в его передаче на каждом этапе. 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`).

После того как выяснена вся цепочка пути пакета, можно последовательно проверить доступность портов на каждом устройстве.

Проверка качества канала связи

Если связь существует, то это не означает, что она высокого качества. Бывают различные ситуации, когда связь есть, но данные либо передаются крайне медленно, либо приложения периодически завершают работу с ошибками.

Обычно такие ситуации связаны с перегрузкой канала: пропускная способность магистральных линий всегда меньше суммы пропускных способностей подключенных к ней каналов связи. В правильно спроектированной локальной сети предприятия такие ситуации встречаются редко. Обычно проблемы возникают только в случае внедрения видеонаблюдения (5—6 камер при передаче кадров высокого разрешения успешно исчерпывают полосу 100 Мбит сети) или в точке выхода в Интернет. В глобальной сети ситуация более типовая, но вы не сможете повлиять на нее. В критических ситуациях можно приобрести канал передачи между двумя точками с заданным качеством обслуживания, но подобные решения доступны не всегда и стоимость часто не позволяет применить их на практике.

Кроме того, проблемы качества передачи данных могут возникнуть из-за повреждения кабелей или сетевых портов.

Объективные показатели качества канала связи

На практике объективные показатели снимаются с активного сетевого оборудования с помощью протокола SNMP. Поскольку многие характеристики меняются в течение дня, желательно собирать эти показания локально для последующего анализа.

> ***Примечание***
>
> Качество линии связи должно проверяться между каждыми активными портами сети. Иными словами, указанные показатели должны анализироваться на каждом порту

коммутаторов и маршрутизаторов локальной сети. Счетчики производительности, значения которых можно оценить в операционных системах компьютеров, характеризуют только качество линии компьютер-коммутатор.

Для объективного анализа состояния линии связи можно использовать следующие основные показатели:

- коэффициент использования пропускной способности сети;
- число ошибочных пакетов;
- величина коллизий;
- загрузка процессора активного оборудования.

Коэффициент использования пропускной способности сети

Для сети Ethernet значение этого показателя выше примерно 70% свидетельствует уже о критической ситуации.

Число ошибочных пакетов

При нормальной работе число ошибочных пакетов 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). Late collision — это коллизия, обнаруживаемая после передачи первых 64 байтов. Причиной late collision часто бывает большое количество повторителей в локальной сети.

Загрузка процессора активного оборудования

Активное сетевое оборудование не только коммутирует пакеты, но может осуществлять различную их обработку, например, шифровать информацию между двумя точками или фильтровать данные по каким-либо правилам. Большое количество таких настроек приводит к исчерпыванию мощностей процессора и замедлению обработки информации. Ситуация пока достаточно редкая, поскольку на практике администраторы предприятий нечасто используют подобные возможности оборудования на "полную мощность".

На рис. 11.8 представлен фрагмент окна программы Observer, которое отображает данные по пропускной способности портов маршрутизатора. Для их получения используются стандартные параметры SNMP для маршрутизатора; информация запрашивается и отображается на графике каждые 2 секунды. Четко видно, что загрузка одного из портов составляет в среднем 70—80%. Фактически это означает исчерпание ресурсов пропускной способности канала (на рисунке показаны данные

маршрутизатора, установленного на канале доступа в Интернет с ограниченной пропускной способностью).

Примечание

На рис. 11.8 показано окно коммерческой программы, однако аналогичные данные могут быть получены и при помощи бесплатных утилит. Например, на сайте **www.mrtg.org** можно найти программу *Multi Router Traffic Grapher* (и ее исходные коды) для отображения данных статистики маршрутизатора. Изначально программа предназначалась для Linux, но имеется также ее бесплатная версия для Windows, работающая на Perl.

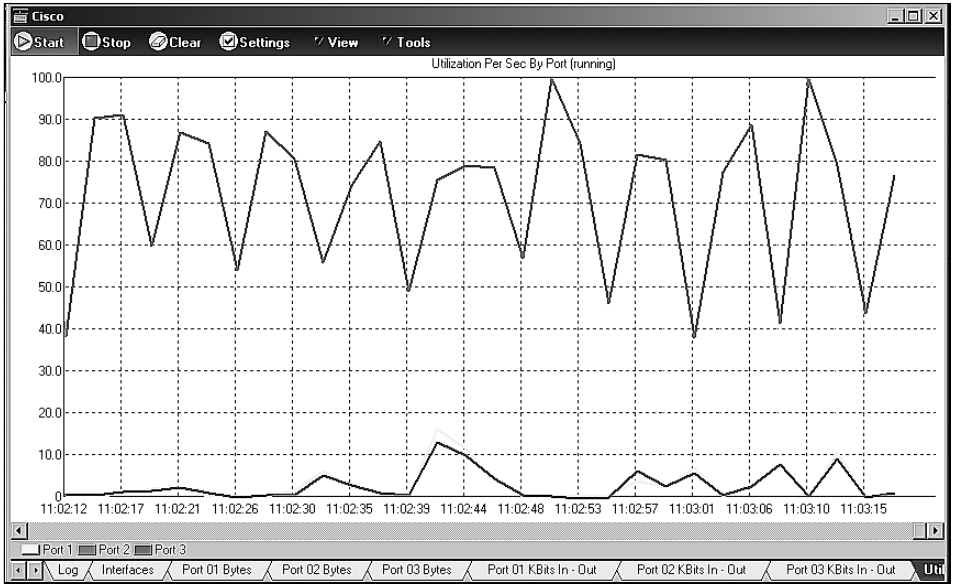


Рис. 11.8. Мониторинг состояния сети по протоколу SNMP

Утилита pathping

В Windows есть одна малоиспользуемая утилита, которая позволяет быстро оценить качество связи до любого хоста. Это утилита pathping. Она определяет цепочку, по которой передается информация между двумя хостами, и посылает на каждую систему серию проверочных пакетов (по 100 штук). В итоге на экран выводится информация о количестве откликов и среднем времени ответа:

```
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.
```

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 сек). Первым параметром выводится время доступа к данному хосту, затем показано количество отправленных на него пакетов и число неполученных ответов (с процентом успеха). После этого отображаются аналогичные значения для достижимости конечного хоста при расчете прохождения пакетов от данной промежуточной точки. Так, цифры в 14-й строке говорят о том, что время доступа к хосту составляет 1059 мсек и при отправке 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 ответ

был бы получен на все. В завершение после имени данного промежуточного хоста утилита сообщила, что количество успешных пакетов составило 96%.

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 потоки — 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.

Задержка при передаче данных ip-телефонии

Считается, что задержка меньшая 200 мсек комфортна для ведения телефонного разговора. Величина большая 700 мсек 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 буферы. Понятно, что такая компенсация имеет пределы, после которых искажения уже будут слышны.

Допустимые потери пакетов в телефонном 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.

Способы получения объективных показателей передачи мультимедийных данных

Из описанных ранее основных показателей качества видно, что для формирования оценки 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 наиболее популярных и функциональных программ этого класса — это Observer производства Network Instruments, LLC (**www.networkinstruments.com**).

> ***Примечание***
>
> Программа для мониторинга сети из состава Windows (Network Monitor) позволяет перехватывать пакеты, передаваемые по сети, но не содержит серьезных средств анализа полученных данных. *Observer* — коммерческий продукт, но для проведения анализа состояния сети можно воспользоваться бесплатно предоставляемой версией ограниченного срока пользования (trial-версией). Кроме того, серьезными возможностями обладает бесплатный сниффер *Wireshark* (бывший Ethereal — **http://www.wireshark.org/**). В том числе, возможностью перехвата и анализа голосового трафика. На рис. 11.9 (из документации продукта) показан пример окна анализа RTP-трафика.

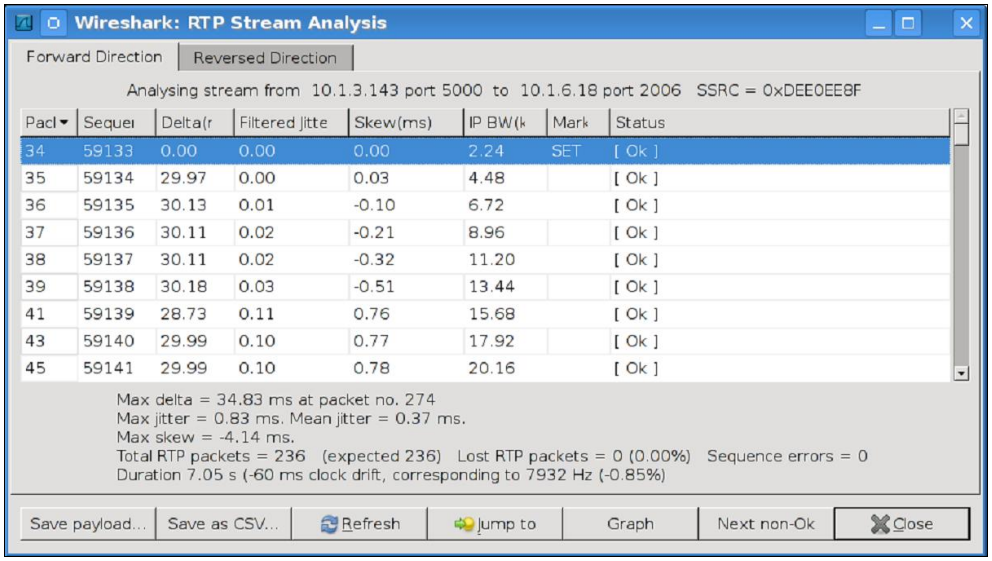


Рис. 11.9. Окно анализа голосового потока

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.

Неисправности аппаратной части компьютера

Легко обнаружить неисправность аппаратной части компьютера, если она приводит к его полной неработоспособности, тогда как выявить "исчезающую" неисправность, обусловленную проблемами "железа", крайне сложно. Как правило, компьютер в таких случаях прекрасно проходит специальное тестирование, но все же более-менее постоянно "подвисает" на определенных задачах.

В случае подозрения на аппаратную неисправность необходимо вначале выполнить следующие операции:

1. Проверить оперативную память компьютера (последовательность операций описана далее).
2. Обновить BIOS материнской платы компьютера до последней версии изготовителя.
3. Выполнить чистую установку операционной системы (без каких-либо "лишних" прикладных программ), после чего установить все обновления от ее изготовителя.
4. Установить последние версии драйверов для материнской платы, видеоадаптера и т. п.

> ***Примечание***
>
> Драйверы оборудования прилагаются к системному блоку. Вам следует обязательно проверить наличие на сайте производителя новых версий, и если они обнаружены, то скачать и установить именно их. Обратите внимание, что при наличии сертифицированных версий и новых разработок (бета-версии) следует устанавливать только последние сертифицированные варианты.

5. 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 продолжает периодически возникать, то такой блок следует передать на техническое обслуживание.

> ***Примечание***
>
> На практике часто встречаются случаи, когда простая замена одних узлов на аналогичные даже той же модели ликвидирует такие исчезающие неисправности. Причем оба переставленных узла будут функционировать нормально.

По опыту работы, наиболее ненадежными узлами компьютерных систем являются жесткие диски. Следующей часто встречающейся причиной нестабильной работы является некачественная память. Отказывают и материнские платы, и процессоры, и периферийные устройства.

Контроль жестких дисков

В операционные системы встроены утилиты проверки файловых структур, которые автоматически запускаются во время перезагрузки компьютера в случае обнаруже-

ния 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 перезагрузка 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).

Восстановление данных с жестких дисков

В Windows не предусмотрено штатных средств для восстановления удаленных данных, кроме программы Корзина. Наиболее часто применяемыми средствами для восстановления информации с жестких дисков являются 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. Имеются возможности восстановления диска после форматирования, "сборки" файлов на основе их типа и т. п.

Использование указанных программ достаточно очевидно. Сначала проводится анализ структуры жесткого диска, предлагается определить восстанавливаемый раздел и тип файловой системы, после чего начинается поиск информации. Найденный список можно при необходимости отфильтровать по тем или иным критериям (например, восстанавливать только файлы документов), а затем выполнить восстановление.

> ***Примечание***
>
> Восстановление всегда осуществляется на другой диск, чтобы не повредить исходные данные. Поэтому при отсутствии сетевых подключений необходимо позаботиться о дополнительном устройстве хранения.

Восстановление файлов данных

Если возникли дефекты устройства хранения данных, то обычно повреждается лишь небольшой участок файла. Программа лечения заменяет поврежденный блок

на новый, файл доступен (например, для копирования), но 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, функции восстановления офисных файлов (Microsoft Word, Excel, Access, PowerPoint) встроены в саму программу офиса, для файлов личных папок электронной почты (pst), архива (zip), баз данных (dbf) и т. п. Соответствующие утилиты легко найти в Сети. Версии их меняются с модификацией основных программ, поэтому я отошлю читателя к самостоятельному их поиску в Интернете.

Принцип работы таких утилит достаточно прост. Они анализируют файл, находят поврежденный блок данных и восстанавливают структуру файла так, чтобы он мог быть открыт в основной программе с минимальными потерями.

Проверка оперативной памяти

В Windows 7/Vista/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

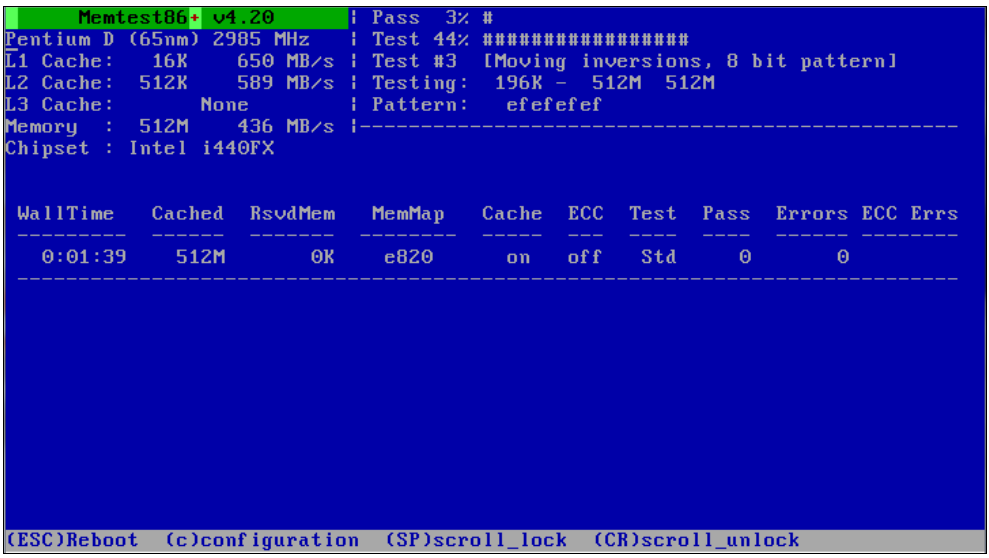


Рис. 11.10. Окно программы проверки памяти в Ubuntu

компьютера с установочного компакт-диска в главном меню (на первом экране) — рис. 11.10.

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.

Контроль теплового режима работы системы

Часто причиной нестабильной работы компьютера бывает неудовлетворительный тепловой режим в системном блоке.

Одним из самых ненадежных узлов компьютера являются вентиляторы охлаждения. Они устанавливаются на процессоре, видеоадаптере, на корпусе, в блоке питания и т. п. Количество 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 (при каждом вскрытии системного блока) визуально контролировать скорость вращения лопастей вентилятора и своевременно заменять неисправные. Допустимо смазывать оси вентиляторов специальной смазкой. Но после такой операции следует проверять данные вентиляторы не реже одного раза в три-четыре месяца.

Температура внутри корпуса компьютера может повыситься не только из-за ухудшения качества вентиляторов. Например, 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, количество которых постоянно увеличивается в последние годы.

Все эти причины могут привести к перегреву компьютера и, как следствие, возникновению сбоев в его работе или даже выходу из строя.

В оценочных целях можно использовать следующие цифры. Температура внутри корпуса компьютера обычно на 15—20 градусов превышает температуру окружающей среды, поэтому администратор должен начать предпринимать срочные меры, если температура внутри серверного шкафа превысит (ориентировочно) 30 °C.

Ошибки программного обеспечения

Из-за разнообразия возможных ситуаций крайне тяжело дать какие-либо конкретные рекомендации по устранению отказов, связанных с программным обеспечением. Можно лишь еще раз порекомендовать придерживаться последовательности шагов, изложенной в начале этой главы.

Весомой частью успеха станет установление последовательности операций, в результате которых появляется ошибка. Случайным образом возникающие отказы устранить крайне сложно.

Нужно максимально изолировать проблему, убедиться, что она возникает только в данном продукте и не повторяется в других пакетах. Например, если ошибка связана с печатью на конкретный принтер, то убедитесь, что задачи печати также не выполняются и из программ Блокнот и т. п. Очень сложно бывает разобраться в проблемах, возникающих на стыке двух продуктов. В подобной ситуации не стоит ожидать реальной помощи и от служб техподдержки.

Скорее всего ваша проблема уже проявлялась и на других системах. Выполните поиск по симптомам ошибки в Интернете и на сайте изготовителя продукта. Используйте несколько поисковых систем. Если об ошибке есть запись в журнале системы, включите в строку поиска это сообщение (исключив индивидуальные параметры — название компьютера и т. п.). Если ответ не найден, попробуйте сформулировать запрос на английском языке. Часто рекомендации оперативнее появляются на языке оригинала. Конечно, в этой ситуации большое значение имеет опыт администратора и его способность составить запрос в тех терминах, которые приняты разработчиком.

Если удается воспроизводить неисправность и она не возникает при взаимодействии с продуктом другого вендора, то можно обратиться в службу технической поддержки изготовителя. Конечно, оперативно решать проблему они будут только при наличии сервисного контракта, но есть вероятность, что помогут и по вашей неисправности.

Восстановление "упавших" систем

Если сервер перестал загружаться, то администратор имеет несколько следующих возможностей восстановления работоспособности информационной системы:

- ❒ восстановление из резервной копии;
- ❒ восстановление загрузчика системы;
- ❒ загрузка в специальных режимах с последующими операциями устранения неисправностей;
- ❒ откат к предыдущим состояниям (для Windows: загрузки последней удачной конфигурации, возвращение к сохраненному состоянию — точке восстановления);
- ❒ переустановка.

Восстановление из резервной копии

Восстановление из резервной копии — самый простой и быстрый способ решения проблемы. Быстрый, потому что вы уже знаете все необходимые шаги. Простой, потому что никаких проблем решать не нужно, достаточно действовать по заранее подготовленному сценарию. Главное, чтобы вы имели актуальную копию данных.

Восстановление из резервной копии хорошо еще тем, что оно позволяет возобновить работу системы на новом оборудовании (в случае физического выхода сервера из строя). Подготовка к такому восстановлению является достаточно простой операцией и подробно описана в соответствующих руководствах. К сожалению, такой функциональностью обладают коммерческие программы резервного копирования, но это один из тез случаев, когда экономия может обойтись дороже.

На рис. 11.11 показан процесс восстановление системы на новое оборудование в программе NetBackup Bare Metal Restore компании Symantec. Система была загружена по сети, программа провела разметку жесткого диска и выполняет копирование с сервера сохраненных данных. При этом сама программа формирует актуальную копию данных, собирая ее из файлов полного и промежуточного резервного копирования. После завершения восстановления необходимо будет только добавить драйверы новых устройств, если таковые появились в системе (драйверы систем хранения и сетевых адаптеров для нового оборудования в случае необходимости готовятся на этапе формирования задания восстановления).

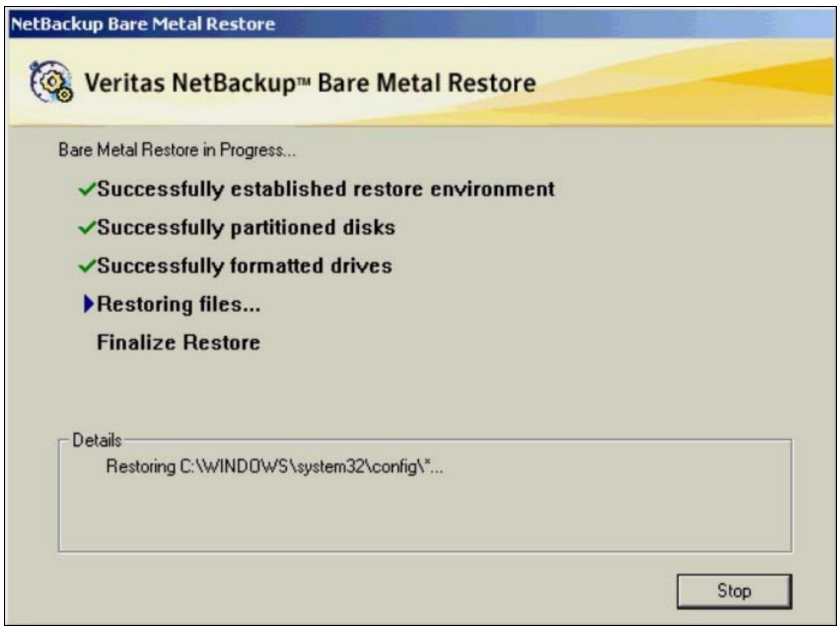


Рис. 11.11. Процесс восстановления системы на новое оборудование из резервной копии

Все описываемые далее способы восстановления не гарантируют достижения успеха и требуют подготовленности администратора. К ним прибегают, если по тем или

иным причинам необходимо сохранить данные сервера, отсутствующие в резервной копии.

Восстановление загрузчика системы

В современных системах ситуация с невозможностью начала загрузки является достаточно редкой. На производственных системах она возникает в случае катастрофического выхода из строя загрузочного диска. Ситуация чаще встречается для полигонов и возникает вследствие ошибок администратора (например, при установке нескольких операционных систем).

Восстановление загрузчика — только первый шаг; обычно за ним следуют операции по восстановлению загрузки в полном объеме (успешного старта всех служб сервера).

Восстановление загрузки Windows 7/2008/Vista

В перечисленные операционные системы встроен мастер, который автоматически запускается при обнаружении проблем со стартом системы (рис. 11.12).

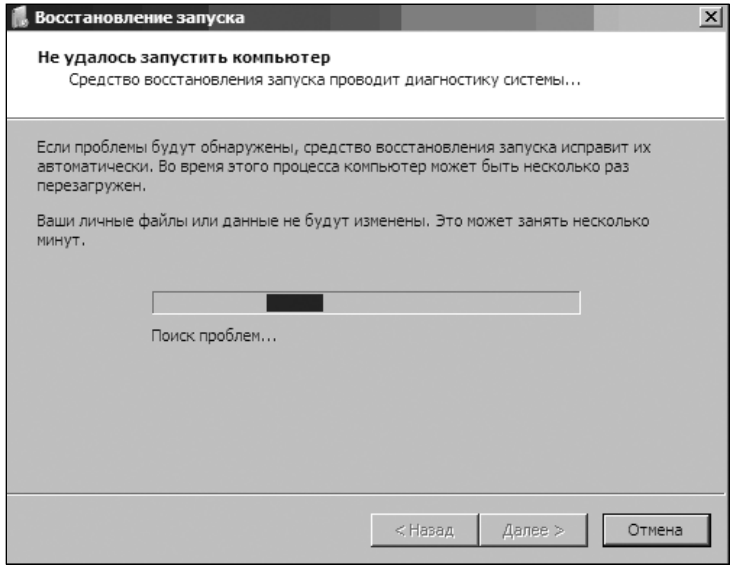


Рис. 11.12. Попытка автоматического восстановления системы

Если работа мастера не привела к успеху (редкая ситуация), то можно в варианте восстановления открыть командную строку и попытаться выполнить операции вручную (часть описана далее для консоли Windows XP).

Восстановление загрузки Windows XP/2003/2000

Восстановить загрузку перечисленных систем можно с помощью консоли восстановления. *Консоль восстановления* — это фактически режим командной строки,

доступный при загрузке с установочного диска. В консоли восстановления присутствует ограниченный набор команд, с помощью которых можно выполнить операции настройки системы и восстановления структуры жесткого диска. Полный перечень команд доступен при вызове справки в режиме командной строки (`help /?`).

Консоль восстановления можно добавить заблаговременно как дополнительный вариант загрузки операционной системы, если вызвать команду установки операционной системы с ключом `/cmdcons` (`i386\winnt32.exe /cmdcons`). Обычно же необходимость использования консоли восстановления возникает внезапно, когда на вашем компьютере отсутствует соответствующий вариант загрузки. В этом случае в режим консоли восстановления можно перейти следующим способом:

1. Укажите в BIOS компьютера вариант загрузки с компакт-диска.
2. Вставьте в устройство чтения компакт-дисков дистрибутив операционной системы и начните с него установку Windows.
3. Когда программа установки запросит, что вы хотите выполнить, выберите операцию восстановления операционной системы.
4. На следующем шаге выберите вариант загрузки консоли восстановления.

Программа проанализирует установленные на жестком диске операционные системы, а затем предложит вам выбрать каталог, в котором находится восстанавливаемая версия, и ввести пароль, соответствующий учетной записи администратора.

Если компьютер загружается с устройства хранения данных, драйвер которого не входит в стандартную поставку Windows, то для входа в режим консоли восстановления применяется традиционный способ: необходимо нажать клавишу <F6> и вставить дискету с драйверами изготовителя устройства.

> ***Примечание***
>
> Если папка, предназначенная для установки системы (файлы реестра), повреждена, то вы попадете в командную строку программы без запроса пароля. В этом случае следует обязательно проверить и восстановить структуру диска. Если на компьютере повреждена загрузочная область жесткого диска, то для входа в консоль восстановления (если под рукой нет компакт-диска с дистрибутивом) приготовьте загрузочные дискеты для соответствующей версии Windows и включите в файл *boot.ini* следующую строчку:
>
> ```
> C:\CMDCONS\BOOTSECT.DAT="Windows Recovery Console" /cmdcons
> ```

Перечислим основные операции, которые приходится выполнять в режиме консоли восстановления.

- **Восстановление загрузочных областей диска.**

  Для этой цели следует использовать команды `fixboot` и `fixmbr`.

> ***Примечание***
>
> Если у вас на диске установлена только одна операционная система, то можно проигнорировать предупреждения, которые будут выводиться командами.

- **Восстановление отсутствующих загрузочных или системных файлов.**

  Поскольку в режиме консоли восстановления доступен привод CD-ROM, то вы можете просто скопировать нужные файлы с дистрибутива в соответствующие папки. Обратите внимание, что буквы логических дисков в режиме консоли восстановления могут не совпадать с названием логических дисков в работающей системе. Вам следует ориентироваться, например, по размерам дисков, находящимся в них папкам и т. п.

- **Решение проблем со службой (драйвером нового устройства).**

  Воспользуйтесь командой `listsvc` для отображения списка служб и устройств и командой `enable` для отключения подозрительных служб (драйверов).

- **Восстановление структуры жесткого диска.**

  Выполняется стандартно с использованием команды `chkdsk`. Единственное, что программа может запросить у вас, — вручную указать путь к файлу библиотек, используемому при запуске этой утилиты (если повреждена системная папка; следует указать папку на компакт-диске).

- **Устранение нарушений в реестре.**

  Часто система не может загрузиться из-за нарушений структуры реестра, причем не помогает даже выбор последней удачной конфигурации. Попробуйте вручную восстановить последнюю копию той ветви реестра, о которой сообщает программа загрузки. Для этого перейдите в каталог SYSTEM32\CONFIG, найдите файл реестра и переименуйте его (по умолчанию текущие файлы не имеют расширения), после чего скопируйте (переименуйте) одноименный файл с расширением sav в файл без расширения. Другое место, откуда можно взять файлы копий реестра системы, — это точки восстановления *(см. разд. "Загрузка конфигурации из точек восстановления Windows" далее в этой главе)*.

  После выполнения операции перезагрузите систему в нормальном режиме.

Восстановление загрузки Linux-систем

Для восстановления следует воспользоваться установочным диском. Например, в Ubuntu опция загрузки в режиме восстановления находится последней строчкой на первом экране. Называется она **Восстановление системы** (или **Rescue broken system**, если вы не выбрали русский язык отображения).

После выбора этой опции начнется выбор настроек системы, определение параметров оборудования, выбор пакетов — словом, внешне все будет примерно так, как при новой установке. Отличие — в наличии строки **Режим восстановления** в левом верхнем углу экрана. В итоге программа предложит выбрать раздел, к которому следует подключиться (если установлена только одна операционная система, то обычно следует выбрать первую позицию списка), после чего на экране появится главное меню программы установки (рис. 11.13).

Для того чтобы восстановить загрузку, нужно выбрать вариант **Установка системного загрузчика GRUB на жёсткий диск** и следовать рекомендациям мастера операций.

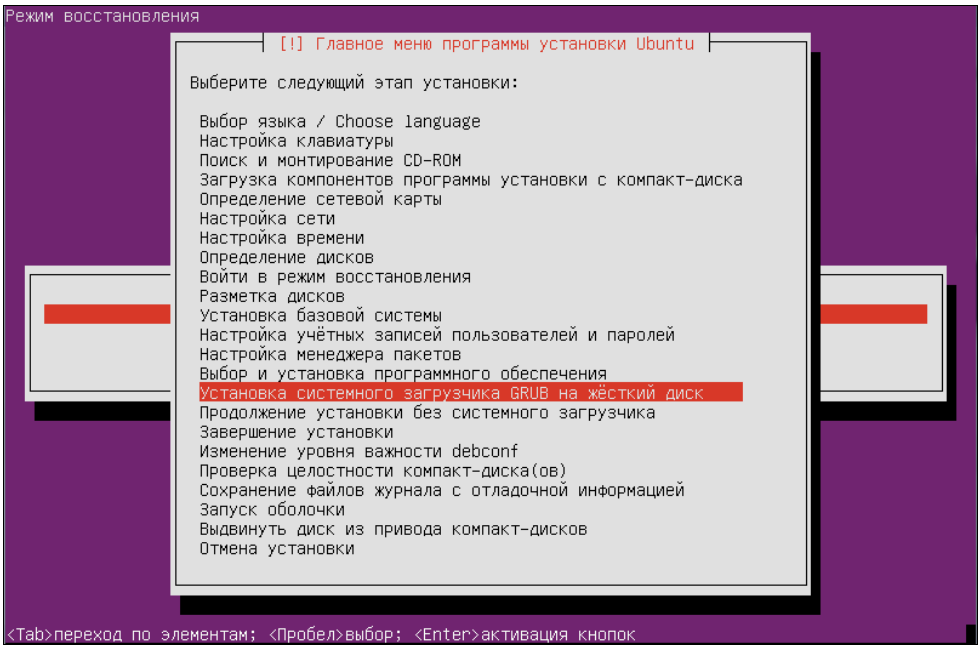


Рис. 11.13. Окно режима восстановления Ubuntu

Примечание

Если программа не сможет проанализировать жесткий диск компьютера (например, на нем повреждена таблица разбиения), то будет предложено перейти в режим командной строки. В этом случае администратору будет доступен ряд команд, с помощью которых можно попытаться определить и ликвидировать неисправность.

Если опции восстановления недоступны

Описанные ранее способы восстановления загрузки "работают", если не нарушена структура жесткого диска. Если, например, повреждена таблица разбиения диска или он был по ошибке отформатирован, то сначала нужно вылечить сам диск.

В Сети можно найти много различных программ, собранных на загрузочные компакт-диски. Загрузившись с такого компакт-диска, можно вызвать соответствующую программу и попытаться восстановить структуру диска. Мы не приводим конкретных ссылок, поскольку ссылки подвержены изменениям, но найти их не представляет труда. Желательно заблаговременно подготовить такую сборку.

Понятно, что это все требует существенных затрат времени и должно использоваться только, если нет другого варианта.

Загрузка в специальных режимах

Выбор специального варианта загрузки осуществляется при старте системы. Меню выбора показывается на небольшое время, в течение которого администратору необходимо выбрать желаемый вариант.

Загрузка Windows в безопасном режиме

В варианте загрузки в безопасном режиме можно решить следующие проблемы:

- ошибки конфигурации системного программного обеспечения;
- сбои из-за установки новых устройств или программ, в том числе и ошибки, возникшие вследствие установки сервис-паков и обновлений.

Если вам удается загрузиться в безопасном режиме, то далее уже можно приступить к лечению: заблокировать устройства, перевести сбойные службы в отключенный режим и т. п.

> ***Примечание***
>
> Если настройками отключен вывод меню загрузки, то перейти в безопасный режим можно, удерживая нажатой клавишу <Shift> при включении компьютера (или нажимая клавишу <F8>).

Загрузка *nix-систем в однопользовательском режиме

Для *nix-систем основным вариантом лечения "тяжелобольных" является загрузка в однопользовательском режиме.

Опция перехода в однопользовательский режим обычно отображается последним пунктом в меню загрузки. Но даже если такой позиции нет, то вызвать режим достаточно просто: нужно выбрать пункт меню загрузки, перейти в опции его редактирования и добавить параметр **S** (или слово *Single*, эта рекомендация относится к загрузчикам Grub, для других вариантов необходимо уточнить по документации) в конец строки и начать загрузку.

В этом режиме вход пользователя осуществляется с правами суперпользователя (пароль не запрашивается), скрипты инициализации не выполняются и администратору доступны любые настройки системы. Главное неудобство для администраторов, воспитанных на Windows, — необходимость работы в режиме командной строки (в том числе, и в текстовом редакторе типа **vi**) и наличия некоторого опыта: где что искать и как править.

Откат к предыдущим состояниям системы

Загрузка последней удачной конфигурации Windows

Загрузка последней удачной конфигурации поможет в случаях:

- ошибок конфигурации во время последней сессии;
- установки неверного драйвера устройства.

Данный вариант загрузки поможет в тех случаях, когда пользователь *не заходил* в систему: после входа конфигурация сохраняется, поэтому в следующий раз вы будете загружаться уже в нее. Но если после каких-либо изменений система даже не доходит до окна входа в нее, то загрузка последней удачной конфигурации поможет решить проблему.

Загрузка конфигурации из точек восстановления Windows

Начиная с Windows Vista в системе предусматривается создание *точек восстановления*. Их можно создавать вручную, но делать это регулярно забывает большинство администраторов. Хотя было бы хорошей практикой сохранять состояние системы перед выполнением тех или иных модификаций.

В последнее время создание точек восстановления встраивают в установочные пакеты программ и оборудования. В результате точка восстановления создается автоматически и может быть использована для отказа к нормальному функционированию.

Возврат к предыдущему состоянию может быть проведен в работающей системе выбором соответствующей команды. Таким способом можно компенсировать неудачные попытки установки оборудования или программ. Но откат можно выполнить и не только из самой системы. Это можно сделать как из режима восстановления самой операционной системы, так и из программ типа ERD Commander в режиме загрузки с компакт-диска (рис. 11.14).

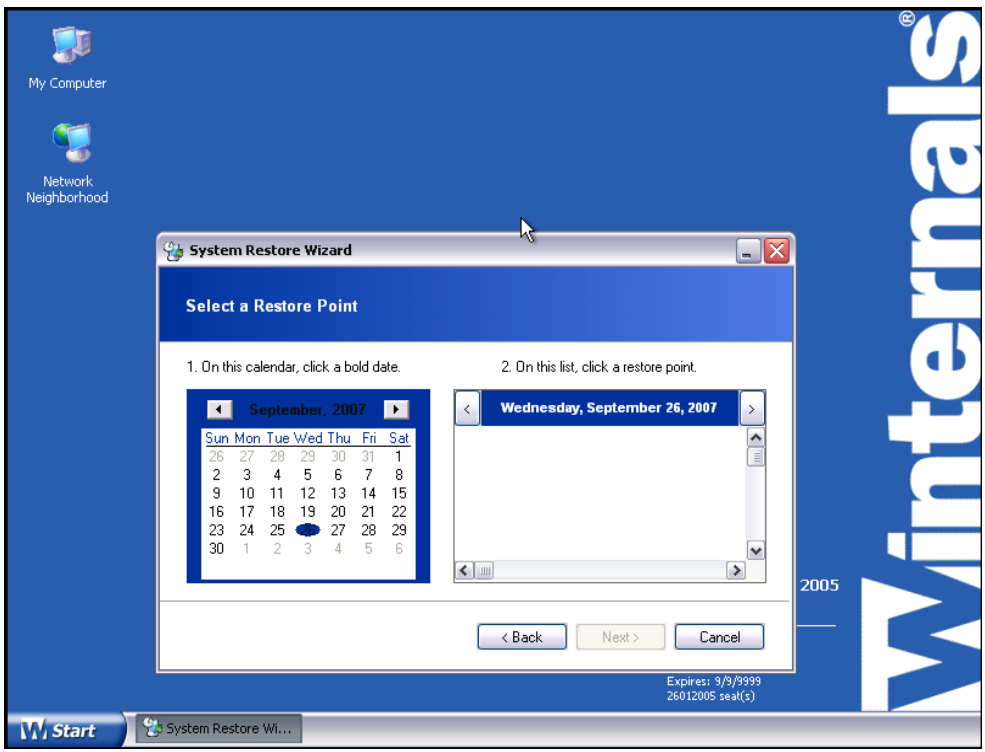


Рис. 11.14. Мастер отката к предыдущим точкам восстановления системы при загрузке с внешнего компакт-диска (пакет ERD Commander 2005)

Значения реестра системы сохраняются в папках точек контрольного восстановления системы — System Volume Information. При работе операционной системы эта папка доступна только системной учетной записи. Администратор может настроить

для себя права доступа к ней. В режиме консоли восстановления контроль прав доступа не действует, данные из папки будут доступны без дополнительных операций. Эти параметры обычно более точно соответствуют последним настройкам системы, чем копии реестра, например, в папке \Windows\Repair (здесь и далее в примерах этого раздела считается, что система установлена в папку C:\Windows; иначе следует заменить название каталога).

Данные хранятся в каталогах с именами, аналогичными _restore{CFA91D90-58C3-4176-A156-29790E9DAF6B} (после "restore" идет значение GUID). Следует зайти в папку, которая соответствует самой поздней дате восстановления, открыть в ней каталог RP*номер* и зайти в папку snapshot.

В папке snapshot сохранены файлы реестра, правда, под именами, отличающимися от тех, которые используются в папке конфигурации. Поэтому для замены файлов реестра администратору необходимо скопировать файлы, перечисленные в табл. 11.1, в папку \Windows\System32\Config и переименовать их так, как указано в правом столбце.

Таблица 11.1. *Соответствие имен файлов*

Имя файла в папке восстановления	Имя файла после переименования
_REGISTRY_USER_.DEFAULT	DEFAULT
_REGISTRY_MACHINE_SECURITY	SECURITY
_REGISTRY_MACHINE_SOFTWARE	SOFTWARE
_REGISTRY_MACHINE_SYSTEM	SYSTEM
_REGISTRY_MACHINE_SAM	SAM

Примечание

К сожалению, программа копирования режима консоли восстановления не поддерживает использование масок, поэтому для копирования нескольких файлов придется выполнить соответствующее число операций. Также в этом режиме не работает функция завершения набора имени файла по первым символам, что потребует точного ручного ввода всех используемых в операциях имен файлов и папок.

Восстановление Windows путем переустановки

В Windows существует возможность восстановления работоспособности системы путем восстановления к настройкам установки (при этом данные пользователя и установленные программы сохраняются). Часто этот способ является самым простым для неподготовленного пользователя.

Если система перестала запускаться, загрузите ее с установочного компакт-диска и начните установку. После того как вы укажете для установки диск, на котором операционная система была установлена ранее, программа обнаружит это и предложит провести *восстановление*. При подтверждении выбора данного режима установка продолжится, внешне не отличаясь от обычной, однако после ее завершения вы об-

наружите, что все ранее установленные программы сохранили свою работоспособность.

Режим восстановления не доступен, если:

- для восстановления используется не тот вариант дистрибутива, с которого была установлена система (например, делается попытка восстановления с дистрибутива на другом языке);
- в системе возникли серьезные повреждения (например, разрушения файловой структуры, в результате чего программа не может обнаружить папки установленной системы).

Учтите, что система восстанавливается к состоянию обновлений, соответствующим установочному пакету. Поэтому после такого восстановления необходимо сразу же установить все обновления, имевшиеся на исходной системе, поскольку в противном случае возможно возникновение ошибок в работе. Чтобы минимизировать операции после такого восстановления, желательно интегрировать в установочный пакет последний сервис-пак и необходимые обновления.

Восстановление удаленных данных

Администратору часто приходится восстанавливать один или несколько файлов, случайно удаленных пользователем. Оптимально, если на предприятии будет настроена система резервного копирования и пользователь сможет сам восстанавливать удаленные данные.

Однако большой объем информации доступен к восстановлению штатными средствами.

Корзины

"Штатная" Корзина ОС Windows малоэффективна прежде всего из-за наличия лимита по объему: если удалено файлов больше, чем настроен лимит в свойствах Корзины, то данные уже не будут доступны к восстановлению. Кроме того, Корзина не защищает файлы, удаляемые по сети, в режиме DOS и т. п.

Для такой защиты доступны коммерческие решения в виде специализированных корзин (например, Norton Protected Recycle Bin) или специализированных серверных решений, таких как Executive Undelete от Executive Software International, Inc. или аналогичных. Подобные программы могут быть централизованно развернуты администратором на рабочие станции и позволяют выполнять операции восстановления как непосредственно пользователем, так и администратором при подключении по сети.

Восстановление из теневых копий

В Windows 7/2008 реализована технология *теневого копирования* для локальных дисков (в Windows 2003 эта возможность присутствует только для сетевых ресурсов и носит название *восстановление предыдущей версии документа*; по умолчанию эта опция не настроена).

Технология теневого копирования (shadow copy) состоит в создании по определяемому администратором графику копий информации. По умолчанию она включена, администратор может изменить график создания копий или отключить данную функциональность.

Предел количества хранимых копий за различные моменты времени определяется только размером дискового пространства, отведенного для данной операции (рис. 11.15). При этом сама технология очень экономно использует дисковое пространство: десяти процентов объема диска может хватить на хранение промежуточных копий за несколько месяцев интенсивной работы.

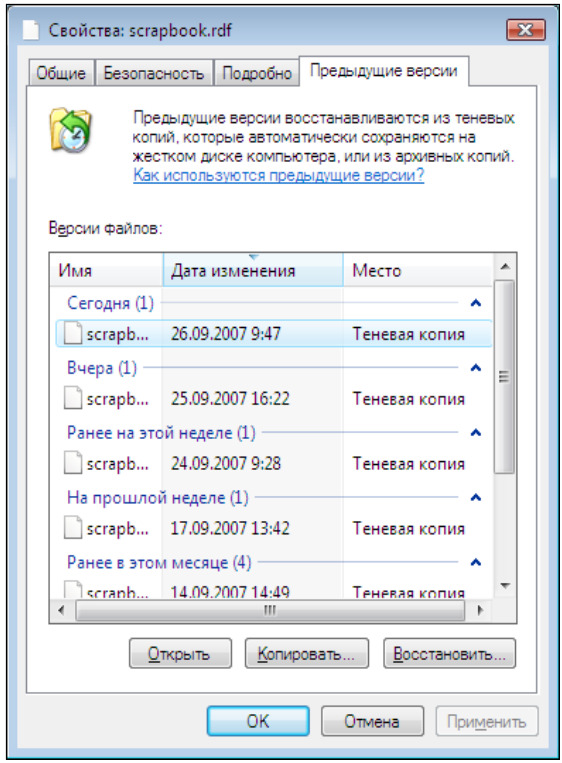


Рис. 11.15. Просмотр предыдущих версий файла

Технология теневого копирования позволяет, во-первых, осуществлять резервное копирование *всех* данных, в том числе и открытых на момент операции. Во-вторых, у пользователей появилась прекрасная возможность без всяких дополнительных затрат иметь *несколько версий* документа. Например, после внесения очередных правок вы поняли, что более правильным решением был предыдущий вариант договора. Если он не был сохранен в качестве отдельного документа, то вернуться к прежним формулировкам ранее было затруднительно. При использовании технологии теневого копирования достаточно посмотреть перечень предыдущих версий документа и восстановить необходимую (в другую папку, чтобы не затереть текущую версию).

Примечание

Для доступа к предыдущим версиям из Windows XP необходимо установить специального клиента. Его установочные файлы находятся в папке установки сервера Windows 2003 по пути *Windows\system32\clients\twclient* и далее — в зависимости от типа платформы клиента. После установки этой программы при открытии свойств файла в сетевой папке появляется дополнительная вкладка **Предыдущие версии**. На этой вкладке можно выполнить необходимые операции восстановления информации.

Оптимизация настроек компьютера

Зачастую на администратора компьютерной сети небольшого предприятия ложится выбор приобретаемых моделей компьютеров. В большинстве случаев покупается типовая на данный момент конфигурация у того поставщика, с которым организацию (администратора) связывают длительные отношения. Часто многие организации не могут позволить себе приобретение компьютерных брендов, поэтому большинство эксплуатируемых у них моделей собрано специалистами региональных предприятий из отдельных блоков. На сбалансированность таких конструкций часто обращается немного внимания, поскольку производительность современных моделей обычно существенно превосходит требования, предъявляемые на индивидуальных рабочих местах, и если производительность компьютера перестает удовлетворять потребности пользователя, то взамен его приобретают более совершенную модель.

Однако во многих случаях причиной неудовлетворительной работы является какое-либо узкое место в конфигурации системы ("бутылочное горлышко", Bottleneck). И "расшивка" его может оказаться экономически существенно более оправданной, чем покупка нового сервера. Кроме того, правильная конфигурация сможет сэкономить существенные средства.

Что такое "медленно"

Удовлетворенность производительностью системы — субъективная оценка. Если для пользовательского интерфейса время реакции не должно составлять более 0,6 сек (например, после щелчка мышью по команде диалоговое окно с параметрами должно появиться за указанный промежуток), то длительность обработки данных зависит от многих параметров: объема данных, сложности вычислений и т. п. Так, в зависимости от условий вычисление может считаться быстрым, если оно завершится за 5 минут, а другое — если быстрее чем за 8 часов. Например, для квартального закрытия склада можно выделить всю ночь, но для открытия типовых форм кадрового учета не должно затрачиваться более нескольких секунд.

Поэтому медленной можно назвать такое функционирование информационной системы, которое не обеспечивает разумную комфортность работы пользователей.

Основные узкие места 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 становится один из следующих компонентов:

- процессор;
- оперативная память;
- дисковая подсистема;
- сетевой адаптер (сетевая инфраструктура).

В идеальном случае каждый компонент не должен "простаивать", но и не сдерживать работу других частей. Для того чтобы проанализировать показатели использования того или иного компонента системы, используются *счетчики производительности*.

В счетчиках постоянно обновляются показатели. Это обновление можно отключить, но особого смысла такая операция не имеет: на производительность системы счетчики практически не оказывают влияния. В операционных системах на базе ядра Windows NT для отображения состояния счетчиков служит программа Производительность (*Performance Monitor*). Для *nix-операционных систем можно найти большое количество утилит, но наиболее популярными являются: top (отображает загрузку процессора, использование памяти и данные по наиболее загруженным процессам), iostat (показывает загрузку процессора и параметры использования дисков), nmon (отображает основные параметры нагрузки и позволяет записывать их с заданной периодичностью в файл с последующей обработкой и формированием отчетов) и др.

Число счетчиков непостоянно и может меняться в зависимости от установленного программного обеспечения и подключенного оборудования. Хотя суммарное число доступных для наблюдения и анализа показателей весьма велико (для Windows-системы составляет несколько сотен параметров), но для качественной оценки информационной системы достаточно перечисленных далее. Полный спектр параметров доступен для анализа только квалифицированным специалистам в целях тонкой настройки приложений.

Администраторы сейчас могут найти не одну программу, которая соберет данные производительности системы и сформирует общие рекомендации. Например, Server Performance Advisor от Microsoft (бесплатное ПО) позволяет в течение нескольких минут составить отчет по параметрам системы и представить его руководителю. Но, на взгляд автора, системный администратор должен владеть основами оценки параметров системы.

В табл. 11.2 приведены значения параметров производительности, по которым можно судить о состоянии системы.

Таблица 11.2. *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 процессором	< 4%	> 10%
Обмен страниц памяти в секунду	< 500	> 1000
Среднее время операции записи-чтения на логический диск	< 15 мсек	> 25 мсек
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 процессора

Примечание

Поскольку современные компьютеры имеют возможность снижать скорость своей работы (например, в случае перегрева процессора), предварительно убедитесь, что высокая загрузка процессора не связана со снижением его тактовой частоты. Для этой цели можно использовать показания программ, контролирующих состояние датчиков системы.

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. На рис. 11.16 приведен листинг 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.

```
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
```

Рис. 11.16. Листинг утилиты *iostat*

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.

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.

- **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.

  Когда процессор не успевает выполнять задания от различных процессов, то эти задания становятся в очередь, процент полезного использования процессора снижается (основное время тратится на переключения между заданиями), а система крайне медленно реагирует на команды.

  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, 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 дополнительный 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.

- **% Disk Time.**

  Счетчик показывает процент времени, в течение которого система "занята" операциями ввода/вывода. Значения счетчика, достигающие 50%, свидетельствуют о необходимости использования 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 операции 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, поможет программа Монитор ресурсов. Администратор может отсортировать процессы по желаемому типу активности, отфильтровать информацию и т. д. (рис. 11.17).

Для Linux-систем аналогичной функциональностью обладает, например, утилита iotop, позволяющая вывести на экран названия процессов с наибольшей дисковой активностью и отобразить соответствующие файлы

> ***Примечание***
>
> Программа *Монитор ресурсов* доступна только для ОС Windows Vista/Windows 7/2008. Определить причины дисковой активности в предыдущих версиях (например, в Windows XP/2003) значительно труднее. Можно порекомендовать воспользоваться в этом случае утилитами от Sysinternals (*FileMonitor*, *ProcessMonitor*) или другими аналогичными средствами.

- **Показатели производительности дисков.**

  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 мсек. Оно должно быть соответственно меньше с учетом объединения дисков в RAID-массив.

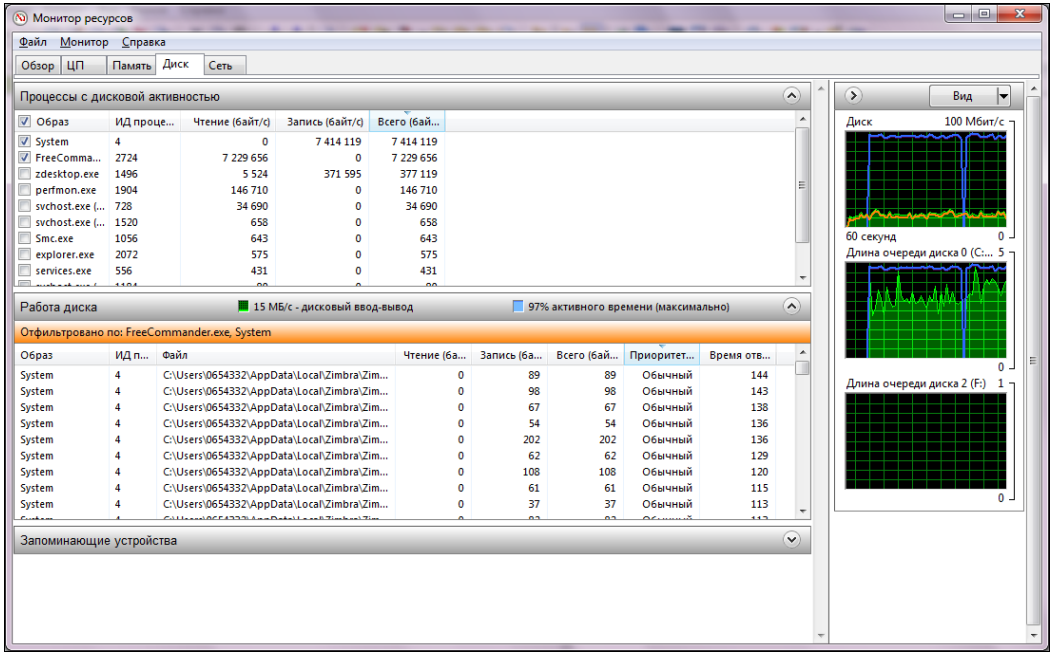


Рис. 11.17. Окно программы *Монитор ресурсов* с отфильтрованными данными дисковой активности

Существует несколько утилит, предназначенных для проверки параметров скорости работы устройств хранения, но наиболее известным и практически профессиональным 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 тестиро-

вания в корне диска (заменить значение Maximum Disk Size на допустимое число секторов[1] в файле теста, иначе файл будет создан на всем свободном пространстве 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. 11.18). 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.

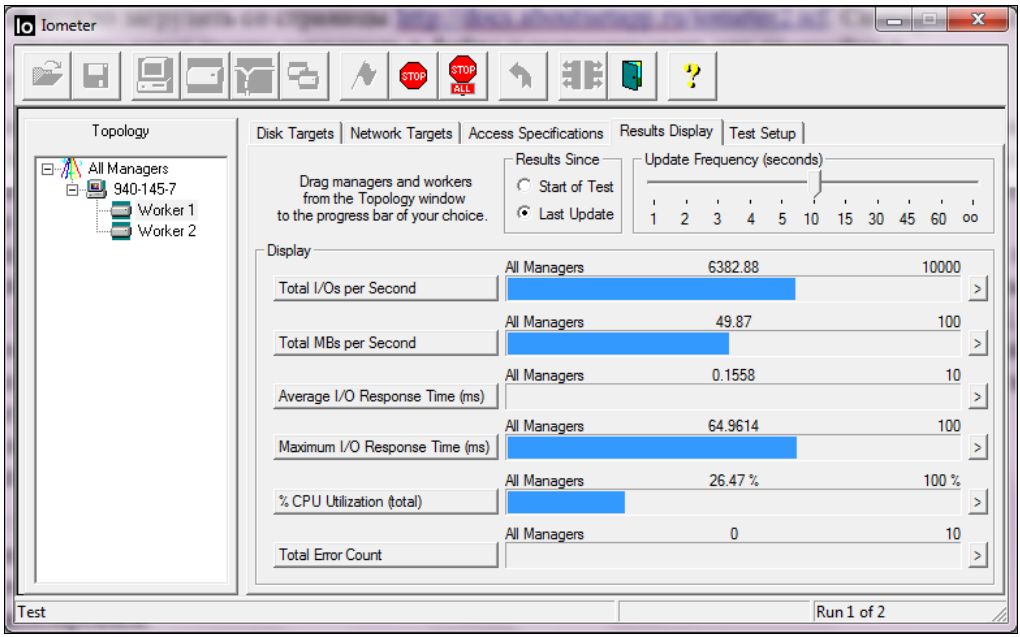


Рис. 11.18. Параметры диска, отображаемые утилитой *iometer*

Пути оптимизации дисковой подсистемы

Какие могут быть варианты решения проблемы при обнаружении узкого места в дисковой подсистеме?

[1] Не забывайте, что один сектор равен 512 байтам. Соответственно и рассчитывайте размер файла.

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.

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 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%. Администраторы обычно используют для оценки состояния сети различные SNMP- и RMON-мониторы, которые имеют возможность автоматически высылать предупреждения при достижении установленных пороговых значений.

Примечание

Счетчики отображают объемы передаваемой и принимаемой информации в *байтах*, тогда как скорость сети указывается в *битах* (100 Мбит/сек, 1 Гбит/сек и т. д.). Поэтому показания счетчика надо умножить на 8, чтобы сравнивать с максимально возможной скоростью передачи данных.

С помощью счетчиков так же можно выяснить, какое приложение генерирует максимальный трафик. Хотя на практике это имеет несущественное значение: обычно администраторам это приложение известно.

Пути оптимизации системы передачи данных

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 подтверждение 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*).

Некоторые советы по анализу показаний производительности

Чтобы снятие показаний счетчиков меньше сказывалось на загрузке проверяемой системы, лучше всего эту операцию делать удаленно, например, подключая задачу Производительность к удаленному серверу. Если вы хотите, чтобы работа самой программы при отображении данных вносила минимальные искажения в параметры производительности, то запускайте ее с низким приоритетом (`start /low` для `Windows-систем`).

Для объективной оценки производительности системы необходимо использовать усредненные за некоторый период показания счетчиков. Чем за больший период времени будут сняты показания, тем более объективные выводы оценки производительности системы можно будет выполнить. Например, кратковременная загрузка процессора, близкая к 100%, при выполнении расчета вполне допустима. Но если процессор загружен более 70% в течение длительного периода времени, то этот факт свидетельствует о необходимости расшивки данного узкого места.

Как правило, программы мониторинга производительности имеют возможность записи показаний счетчиков в файл в реальном режиме времени. Администратору необходимо только задать периодичность снятия показаний и указать длительность записи. В качестве примера на рис. 11.19 приведен один из графиков отчетов, сформированных программой nmon (бесплатное ПО для мониторинга производительности *inux-систем) реального компьютера. Часто такие отчеты снабжаются указаниями на параметры, значения которых зафиксированы в неоптимальных коридорах.

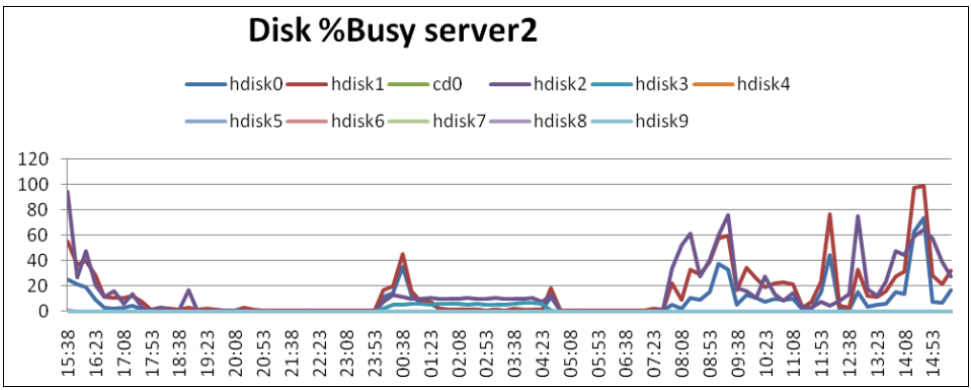


Рис. 11.19. Один из графиков отчета по данным мониторинга AIX-системы программой *nmon*

Кроме того, в период замеров следует выполнять обычные для данного компьютера операции. Например, для рабочей станции это открытие файлов, их печать, чтение электронной почты, работа в программах офиса или выполнение текущих операций

в базе данных и т. п. Чем больше такие операции будут соответствовать типовым вариантам использования компьютера, тем точнее получатся рекомендации на основе анализа показаний счетчиков.

Оптимизация приложений

Пользователь может сказать, что компьютер работает медленно, что ему хотелось бы, чтобы расчеты выполнялись не более чем за некоторый, заранее определенный, промежуток времени. Задача администратора — определить причины недостаточной производительности, понять, какой параметр вносит наибольшее замедление в работу информационной системы, и попытаться устранить проблему.

Еще раз отметим, что невозможно добиться ускорения вычислений сразу по всем параметрам. Следует выделить операции, наиболее существенно замедляющие работу, попытаться оптимизировать их и затем повторять эти шаги снова и снова, пока не будет достигнут требуемый эффект. Обязательно следует выбрать типовые операции, зафиксировать время их выполнения до начала оптимизации и контролировать эффект каждого шага.

Современные коммерческие приложения обычно имеют много *тонких* внутренних настроек, позволяющих оптимизировать вычисления под конкретную конфигурацию заказчика. Поэтому, наряду с устранением узких мест аппаратной составляющей (так, как это описано ранее) следует ознакомиться с подобными руководствами по оптимизации и реализовать изложенные в них настройки.

Однако все эти меры не всегда могут уменьшить время обработки данных до приемлемых величин. Поэтому администратору обычно необходимо и разбираться в том, как осуществляются расчеты в приложении. Часто наибольший эффект может дать изменение алгоритма расчетов. Например, расчет заработной платы для всего предприятия можно провести за меньшее время, если одновременно запустить несколько процессов — параллельно по нескольким подразделениям. А формирование отчета за длительный период можно ускорить, если предварительно сформировать отчеты за промежуточные периоды и т. д.

Задача администратора в подобной ситуации — выяснить причины проблемы и подсказать возможные пути их разрешения.

Диагностика службы каталогов

Следствием неисправностей функционирования службы каталогов (Active Directory, AD) неизбежно являются отказы информационной системы.

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. 11.3.

Таблица 11.3. *Перечень файлов, 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

К сожалению, появление записей об ошибках в протоколах событий, как правило, уже свидетельствует о наличии проблем. Конечно, можно включить расширенные возможности 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, необходимо использовать любую систему мониторинга реального времени.

Следует внимательно относиться ко всей информации пользователей. Например, информация 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 можно использовать любые утилиты, которые взаимодействуют с AD.

В первую очередь это три стандартные консоли управления AD: пользователи и компьютеры, доверительные отношения и домены, сайты. В состав Resource Kit входит ряд утилит, которыми можно воспользоваться для диагностирования проблемы. Это dcdiag, специально предназначенная для тестирования AD. Кроме того, для тестирования инфраструктуры можно воспользоваться утилитами, перечисленными в табл. 11.4.

Можно также воспользоваться утилитами, позволяющими отображать необходимую структуру AD и менять параметры объектов (табл. 11.5).

Таблица 11.4. *Утилиты для тестирования инфраструктуры*

Утилита	Для чего используется
netdiag.exe	Проверка сетевой инфраструктуры
netdom.exe	Проверка и управление доверительными отношениями
nltest.exe	Проверка состояния secure channel
ntfrsutl.exe	Управление службой репликации файлов
dsastat.exe	Анализ состояний AD на различных контроллерах
repadmin.exe	Проверка репликации данных AD, возможности инициировать частичную или полную репликацию заданного контекста
replmon.exe	Контроль репликации данных и запуск ручной репликации (графическая утилита)

Таблица 11.5. *Утилиты для отображения структуры AD и изменения параметров объектов*

Утилита	Для чего используется
ADSI Edit	Просмотр и редактирование объектов AD, установка списков доступа (access control lists, ACLs)
ldp.exe	Взаимодействие с AD по протоколу LDAP

Для проверки сетевых соединений и их качества можно использовать любые утилиты из состава операционной системы *(см. разд. "Диагностика IP-протокола" ранее в этой главе)*. Кроме того, при анализе и настройке AD придется использовать оснастки управления DNS, монитора производительности, утилиту редактирования реестра, утилиту управления AD с возможностью модификации ее метаданных — ntdsutil.exe и т. д.

Проверка разрешения имен

Как уже было сказано, комплексную проверку доступности служб AD можно осуществить с помощью утилиты dcdiag. Но поскольку она устанавливается дополнительно, то в оперативных случаях следует быть готовым выполнить простейшие проверки стандартными средствами операционной системы. Обычно достаточно проконтролировать возможность разрешения имен с помощью типовых утилит. Необходимо проверить достижимость контроллера домена по его краткому (без доменного суффикса) и полному имени, а также 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 команды `nslookup`, выполнить попытку разрешения имен, перечисленных в табл. 11.6. Для разрешения имен служб (записи типа SRV) в `nslookup` предварительно следует 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.

Таблица 11.6. *Перечень имен, проверяемых в процессе теста*

Имя	Тип записи	Чему соответствует
_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

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.

ГЛАВА 12

Плановые операции обслуживания

Обязанность контроля функционирования информационной системы влечет за собой выполнение ряда рутинных операций. Их состав специфичен для каждого предприятия. Однако я попытаюсь привести примерный шаблон, на основе которого может быть составлен конкретный план периодических мероприятий. Удобно, если этот план будет выполнен в виде соответствующего перечня, выполнение каждого пункта которого будет отмечаться в этом же документе.

> ***Примечание***
>
> В данном плане приводятся только позиции, которые следует проверить администратору. Естественно, что обнаружение каких-либо ошибок предполагает соответствующие действия администратора по ликвидации проблемы.

Конечно, объем операций должен быть скорректирован с учетом размера организации, наличия и объема мониторинга и т. п.

Ежедневные операции

Ежедневные операции направлены, в первую очередь, на контроль текущего состояния информационной системы. Каждая позиция данного шаблона должна быть дополнена конкретными операциями проверки. Можно назвать следующие далее операции проверки.

- **Оценка внешнего состояния серверов и окружающей среды.**

  Администратору необходимо оценить температуру вокруг серверов, проверить отсутствие внешних признаков вскрытия корпусов, состояние кабельной системы и т. д.

- **Проверка функционирования основных служб информационной системы.**

  Администратор обязан проверить состояние всех основных служб системы: работоспособность канала Интернета, возможность приема и отправки сообщений электронной почты, отклики от информационного сервера Интернета предпри-

ятия и т. д. Объем подобных операций зависит от состава информационной системы.

- **Оценка показаний датчиков аппаратного контроля.**

  Серверные платформы оснащены датчиками, позволяющими контролировать температурный режим внутри корпуса, параметры электропитания, частоту вращения вентиляторов, состояние RAID-контроллеров. Администратору необходимо убедиться, что соответствующие показания находятся в допустимых диапазонах.

- **Проверка результатов выполнения операций резервного копирования.**

  Следует убедиться, что *все* операции резервного копирования завершились успешно и без каких-либо сообщений об ошибках. Особо хочется обратить внимание, что контролю подлежат все операции резервного копирования: выполняемые как системными средствами, так и внутренними операциями прикладного программного обеспечения.

- **Проверка результатов обновления антивирусных баз.**

  Необходимо убедиться, что все работающие компьютеры (серверы и рабочие станции) имеют последнюю версию вирусных баз локального сервера, а этот сервер, в свою очередь, успешно обновлен из Сети.

- **Проверка результатов иных плановых операций в системе.**

  В информационной системе могут существовать иные операции, выполняемые по специальным графикам. Например, мероприятия по оптимизации баз данных SQL-сервера, формирование отчетов статистики использования Интернета и т. п. Администратору следует проверить итоги выполнения таких операций.

- **Проверка содержимого протоколов работы серверов.**

  Администратор должен просмотреть и проанализировать протоколы работы всех серверов информационной системы, в первую очередь обращая внимание на протоколы системы безопасности и на сообщения об ошибках или предупреждения. Следует отметить, что и чисто информационные сообщения могут существенно помочь опытному администратору в предупреждении аварии.

- **Проверка доступного объема жестких дисков.**

  Необходимо проверить наличие на основных производственных серверах достаточного свободного объема дискового пространства, которое позволит продолжить нормальное выполнение бизнес-операций. Это требование относится к тем серверам, объем информации на которых может меняться. Например, почтовый сервер (прием большого числа сообщений), файловый сервер (пользователи перенесли на него существенный объем данных), сервер баз данных (разработчики изменили структуру информации, вследствие чего размер баз существенно вырос) и т. п. Естественно, что для серверов, выполняющих такие функции, как маршрутизация сетей и т. п., данный контроль не актуален.

- **Проверка работы служб систем.**

  Администратор должен проверить, что все автоматически запускаемые службы *всех* серверов информационной системы находятся в состоянии *"работает"*.

Конечно, существуют службы, которые автоматически запускаются и впоследствии останавливаются. Но я на этом не буду заострять ваше внимание.

Еженедельные операции

В следующей далее группе еженедельных операций представлены задачи, которые администратор должен выполнять несколько раз в месяц. Конкретная периодичность — раз в неделю или раз в две недели — должна быть определена в зависимости от специфики информационной системы.

- **Формирование отчета.**

  Хотя это чисто организационное предложение, наличие периодического отчета системного администратора, с одной стороны, стимулирует самого администратора, с другой — позволяет держать руководителя в курсе состояния информационной системы.

- **Очистка фильтров вентиляторов охлаждения.**

  Практика показывает, что в условиях обычного учреждения воздушные фильтры "забиваются" уже через одну-две недели. В связи с этим следует еженедельно очищать фильтрующие элементы как всего помещения, так и на корпусах оборудования (конечно, если соответствующие фильтры предусмотрены).

- **Проверка производительности серверов.**

  Администратору необходимо проверить параметры производительности серверов системы и проанализировать их изменения по сравнению с прошлыми периодами. В случае снижения параметров — принять меры по поддержанию необходимого уровня обслуживания пользователей.

Плановые операции другой периодичности

Администратору не следует забывать и о тех работах, выполнять которые ему приходится достаточно редко. Следующие далее работы можно запланировать, например, в квартальном или полугодовом планах.

- **Установка обновлений.**

  Администратор должен периодически проверить наличие обновлений для всего программного обеспечения, используемого в организации. Даже если в организации реализована система текущего обновления безопасности, необходимо убедиться в отсутствии обновлений, которые не охватываются ею.

- **Удаление устаревших объектов службы каталогов.**

  Часто создание и удаление учетных записей пользователей отстает от фактического кадрового состава предприятия, состав компьютеров, перечисленных в

службе каталогов, не соответствует реальности. Имеет смысл периодически удалять устаревшие объекты из службы каталогов, хотя бы на основе времени, прошедшего с момента последнего входа соответствующей учетной записи в домен.

- **Очистка оборудования от пыли.**

  Обычно данную операцию совмещают с проведением на оборудовании тех или иных работ, поскольку при этом обычно предполагается отключение электропитания. Периодичность работ определяется качеством окружающей среды, и при отсутствии специальных мер по фильтрации воздуха данная операция должна выполняться не реже одного раза в три—пять месяцев.

- **Тренировки полного восстановления системы.**

  Крайне важно, чтобы специалист мог оперативно выполнить комплекс работ по полному восстановлению информационной системы после аварийной ситуации. Поэтому в организации должны быть запланированы работы по восстановлению тестовой системы на основе тех резервных копий, которые создаются в плановом порядке.

- **Корректировка руководящей документации.**

  Целесообразно раз в год приводить в порядок документацию: актуализировать схемы сетей, отражать выполненные ремонты и т. п. Следует пересмотреть руководящие документы организации, касающиеся ИТ-технологии, внести в них необходимые изменения, учитывающие состояние дел, утвердить и опубликовать на внутренних ресурсах для ознакомления пользователей.

- **Планирование развития.**

  По итогам загруженности информационной системы за некоторый период администратор может предположить о дополнительных ресурсах, которые могут потребоваться для дальнейшего нормального функционирования системы (например, приобретение дополнительного жесткого диска). Соответствующие предложения должны быть направлены руководителю.

План-отчет операций

На основе приведенного в предыдущих разделах плана мероприятий следует составить список конкретных, текущих операций администратора. При этом каждая позиция должна быть пооперационно развернута в соответствии со спецификой информационной системы примерно в следующем виде, позволяющем непосредственно в бланке отмечать результаты проверки каждого пункта (табл. 12.1).

Заполненный администратором отчет будет являться документом, по которому можно оценить как работу специалиста, так и объективно проанализировать состояние системы.

Таблица 12.1. *Список конкретных текущих операций администратора*

Отчет о проверке					
Администратор:	*Иванов*		Дата:	*23.01.12*	
... Операция: проверка параметров производительности сервера					
Сервер	**Счетчик**		**Измеренное значение**		**Время измерения**
server1	% Processor Time		16%		09.30
	...		...		...
... Операция: проверка наличия обновлений программного обеспечения					
• Проверить наличие обновлений для Windows 2008					
• Проверить наличие обновления для Office 2010					
...					
...					

Предметный указатель

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

А

Б

В

Г

Д

Ж

З

И

К

Л

М

Н

О

П

P

C

Т

У

Ф

Х

Ц

Ш

Э