Так видит журнал читатель, который забыл оформить подписку:

НОВОГОДНИЕ КАНИКУЛЫ ЗАТЯНУЛИСЬ

БЫСТРО РАСКУПИЛИ ТИРАЖ

УЕХАЛ В ОТПУСК

ПОСЛЕ ОТПУСКА АВРАЛ НА РАБОТЕ

НЕОЖИДАННО ЗАКОНЧИЛИСЬ ДЕНЬГИ

Так видит журнал читатель, оформивший подписку:

ПОДПИШИТЕСЬ И ЧИТАЙТЕ!

Роспечать – 20780, 81655

Пресса России – 88099, 87836

Интер-почта – тел. (495) 500-00-60

№1(74) январь 2009 системный администратор

системный администратор

№1(74) январь 2009
подписной индекс 20780
www.samag.ru

ISSN 1813-5579
09001
9 771813 557005

Автоматическая установка драйверов

Вы еще не используете Windows Vista?

Оптимизируем PPD-файлы

Анализируем трафик с Nulog2

Hyperic HQ – система мониторинга корпоративного уровня

Контролируем изменения в конфигурационных файлах

nUbuntu – дистрибутив для тестирования защищенности

Используем универсальные отчеты и обработки в «1С:Предприятии 8»

JQuery: магия JavaScript

Winbinder PHP: создаём GUI-интерфейс за 2 клика

12 лет

НАША КОМПАНИЯ ПРЕДОСТАВЛЯЕТ ЛИНИИ СВЯЗИ В САМЫХ НЕПРОХОДИМЫХ МЕСТАХ МОСКВЫ

10 МБИТ - $500, ВКЛЮЧЕНО МНОГО ТРАФИКА. ANYTHING ELSE?

ЗВОНИТЕ, ДОГОВОРИМСЯ!

г. Москва, Хлебный переулок 2/3, тел. 291-61-32, 202-61-43 (круглосуточно)
e-mail: support@redline.ru

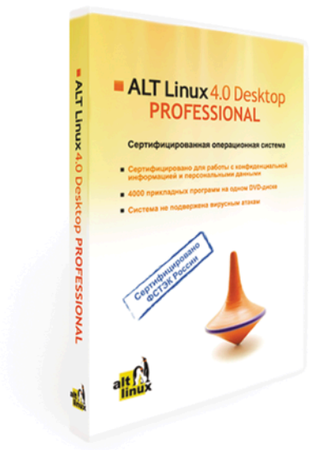
Реклама

Сертифицированные продукты ALT Linux

Для кого предназначены сертифицированные продукты?

- Для **организаций**, которым необходимо иметь **сертифицированное ПО**. Это многие государственные учреждения, оборонные предприятия и т.д.;
- Для **организаций**, работающих **с конфиденциальной информацией и персональными данными**. Под эту категорию попадают практически все фирмы, имеющие базу данных паспортов, номеров сотовых телефонов и т.п. (туристические фирмы, страховые компании, банки и т.д.), фирмы, проводящие анкетирование.

ALT Linux 4.0 Desktop Professional
сертифицированный продукт для рабочих станций



ALT Linux 4.0 Desktop Professional сертифицирован Федеральной службой по техническому и экспортному контролю (ФСТЭК России).
Сертификат соответствия **№1649 от 23 июля 2008**:

- Классификация по уровню контроля отсутствия недекларированных возможностей (НДВ) — **4 уровень**.
- Показатели защищённости от несанкционированного доступа к информации (СВТ) — по **5 классу защищённости**.

ALT Linux 4.0 Desktop Professional — это:

- Удобная в работе операционная система, дающая пользователю возможность решать обычные задачи, не опасаясь вирусов и не затрачивая время на поиск нужных прикладных программ в сети Интернет и на полках магазинов;
- Дружественная программа установки, работа с которой будет особенно приятна начинающим пользователям;
- ALTerator — интуитивно понятный инструмент настройки и управления системой.

Рекомендуемая розничная цена: 3800 руб.

ALT Linux 4.0 Server Edition
сертифицированный продукт для серверов

Всё, что можно сделать по настройке сервера без вмешательства пользователя, уже реализовано в дистрибутиве **ALT Linux 4.0 Server Edition**.
ALT Linux 4.0 Server Edition сертифицирован Федеральной службой по техническому и экспортному контролю (ФСТЭК России).
Сертификат соответствия **№1501 от 8 ноября 2007**:

- Классификация по уровню контроля отсутствия недекларированных возможностей — **4 уровень**.
- Показатели защищённости от несанкционированного доступа к информации — по **5 классу защищённости**.

ALT Linux 4.0 Server Edition — серверный дистрибутив с широким спектром возможностей, включающий комплект готовых решений для актуальных задач организации: построения корпоративной сети и среды обмена информацией. Простые веб-интерфейсы управления, включённые в дистрибутив, позволяют существенно ускорить развёртывание корпоративного сервера.

Рекомендуемая розничная цена: 22000 руб.

реклама

www.altlinux.ru
По вопросам приобретения: zakaz@altlinux.ru

Позвольте поздравить всех вас, уважаемые читатели, с окончанием самых длинных в году праздников. Честно сказать, я не слишком люблю затяжные каникулы, потому как последствия для работы они создают самые ужасные. Необходимое время для адаптации к работе и общее нежелание заставлять себя что-то делать после почти двухнедельного отдыха практически парализуют работу компаний едва ли не до конца января.

Однако праздники закончились, и мы с горем пополам приступили к выполнению своих прямых обязанностей или... к поиску нового места работы. В этом году сотрудники многих компаний были отправлены на принудительный отдых до 15, а то и до 19 января. Выходя на работу 16-го или 20-го числа, некоторые сотрудники имели неприятную возможность неожиданно оказаться безработными. Хочется верить, что читателей нашего журнала миновала эта незавидная участь.

Новый, 2009 год обещает быть интересным хотя бы потому, что никто толком не может понять, чего от него следует ожидать. Кто-то запасается рисом, кто-то подумывает, а не уехать ли куда-нибудь и желательно подальше, а кто-то... совершенно неожиданно для себя получает крайне интересные предложения по работе. Причем зачастую эти счастливчики (в момент получения предложений) не являются безработными. Вообще, насколько я могу судить, уверенные в себе специалисты и сейчас запросто срываются с насиженных мест и ищут новую работу. И находят ее, что самое интересное.

В этом году нам всем придется приложить немало усилий для того, чтобы сохранить и приумножить то, к чему мы так привыкли. Однако я предлагаю не унывать, пока не смотреть новостные каналы (дабы те своими истериками не мешали создавать правильный позитивный настрой) и, веря в успех, смело двигаться вперед.

Алексей Коршунов

Google развивает Chrome по всем направлениям

В начале декабря Аарон Будман (Aaron Boodman), представляющий коллектив разработчиков веб-браузера с открытым кодом Google Chrome, опубликовал в своем блоге ссылку на информацию о готовящейся системе расширений. Тогда о расширениях впервые заговорили в новом для Chrome ключе: они все же нужны и вовсе не обязательно будут мешать «легковесности» браузера. Главное выдвинутое требование к расширениям – высокий уровень их качества («как будто эти расширения создавали разработчики самого браузера»). Кроме того, расширения будут обновляться незаметно для пользователя. Сроки реализации проекта расширений для Chrome неизвестны.

Вскоре в СМИ появилось новое сообщение о Chrome: Google сняла с браузера статус «бета» – всего через три месяца после первого публичного релиза. Это событие ознаменовалось исчезновением в 15-м релизе Chrome соответствующей подписи («бета») при запуске программы.

В январе стали известны подробности о сроках выпуска долгожданных версий Chrome для GNU/Linux и Mac OS X. Эти релизы запланированы на июнь наступившего года. Пока готовы лишь базовые версии Chrome для Linux и Mac, которые позволяют только «хорошо отображать большую часть веб-страниц».

И в завершение череды событий про Chrome стоит отметить интересные изменения в тестовой сборке Chrome (2.0.156.1). В ней реализована поддержка скриптов Greasemonkey (Greasemonkey – расширение к Mozilla Firefox, позволяющее пользователям устанавливать скрипты, преобразующие HTML-страницы на лету), появились профили, автоматическое дополнение в веб-формах, полное масштабирование страниц, импорт закладок из Google Bookmarks, автоматический скроллинг.

Sun и WINE сделали важные шаги навстречу 64-битным системам

За ноябрьским анонсом выпуска альфа-версии Adobe Flash Player 10 для 64-битных Linux-систем последовали не менее значимые декабрьские релизы.

Так, компания Sun Microsystems, выпустив предварительную версию грядущего обновления к Java (Java 6 Update 12), представила плагин для веб-браузеров на машинах с 64-битной архитектурой. Java-плагин для веб-браузеров пользователей систем с 64-битной архитектурой – это столь давняя проблема, что достаточно указать дату соответствующей записи в системе баг-трекинга Sun: 14 января 2003 года (баг #4802695). Из-за этого обладателям 64-битных систем приходилось пользоваться 32-битными сборками браузеров или идти на другие ухищрения. По-видимому, уже в ближайшее время пользователи смогут забыть о былых неудобствах. Пока 64-битный Java-плагин доступен (на https://jdk6.dev.java.net/6uNea.html) только для Firefox на платформах GNU/Linux и Windows. Когда появится его сборка для Solaris, не сообщается.

Почти одновременно с этим Маартен Ланкхорст (Maarten Lankhorst) из проекта WINE объявил об успешном запуске первого приложения, созданного для 64-битной версии ОС Windows. Для этого потребовалось переработать GCC, чем занимался Кэй Тайтц (Kai Tietz). «Впрочем, для того чтобы эти наработки попали в основную ветку, потребуется сделать еще много вещей», – подчеркнул Ланкхорст. Наработки по проекту wine64 доступны в Git-дереве wine64.git (http://repo.or.cz/w/wine/wine64.git).

Sun выпустила веб-сервер с открытым кодом

Sun Microsystems представила результаты проекта открытия исходного кода своего веб-сервера Sun Java System Web Server (SJSWS). В середине января было объявлено об официальном запуске нового продукта компании – Open Web Server.

Open Web Server – это ядро Sun Java System Web Server, исходный код которого доступен всем желающим под лицензией BSD. Он лишен некоторых возможностей SJSWS (например, WebDAV, поиска, административного графического и консольного интерфейсов), но несмотря на это, в Sun его называют «тем же самым высокомасштабируемым HTTP-сервером, обеспечивающим функционирование многих нагруженных веб-сайтов, требующих высокого уровня надежности».

Среди возможностей, поддерживаемых в Open Web Server, можно выделить HTTP 1.0/1.1, SSL, CGI/FastCGI, SHTML, ACL, LDAP/LDAPS, NSAPI, кэширование файлов (NSFC), локализации, мониторинг.

Open Web Server стал частью так называемого веб-стека (Web Stack) проекта операционной системы OpenSolaris.

Linux Foundation объявила конкурс на рекламный ролик

В середине января организация Linux Foundation (LF), занимающаяся продвижением операционной системы GNU/Linux, объявила о начале приема рекламных видеороликов на участие в конкурсе «I'm Linux».

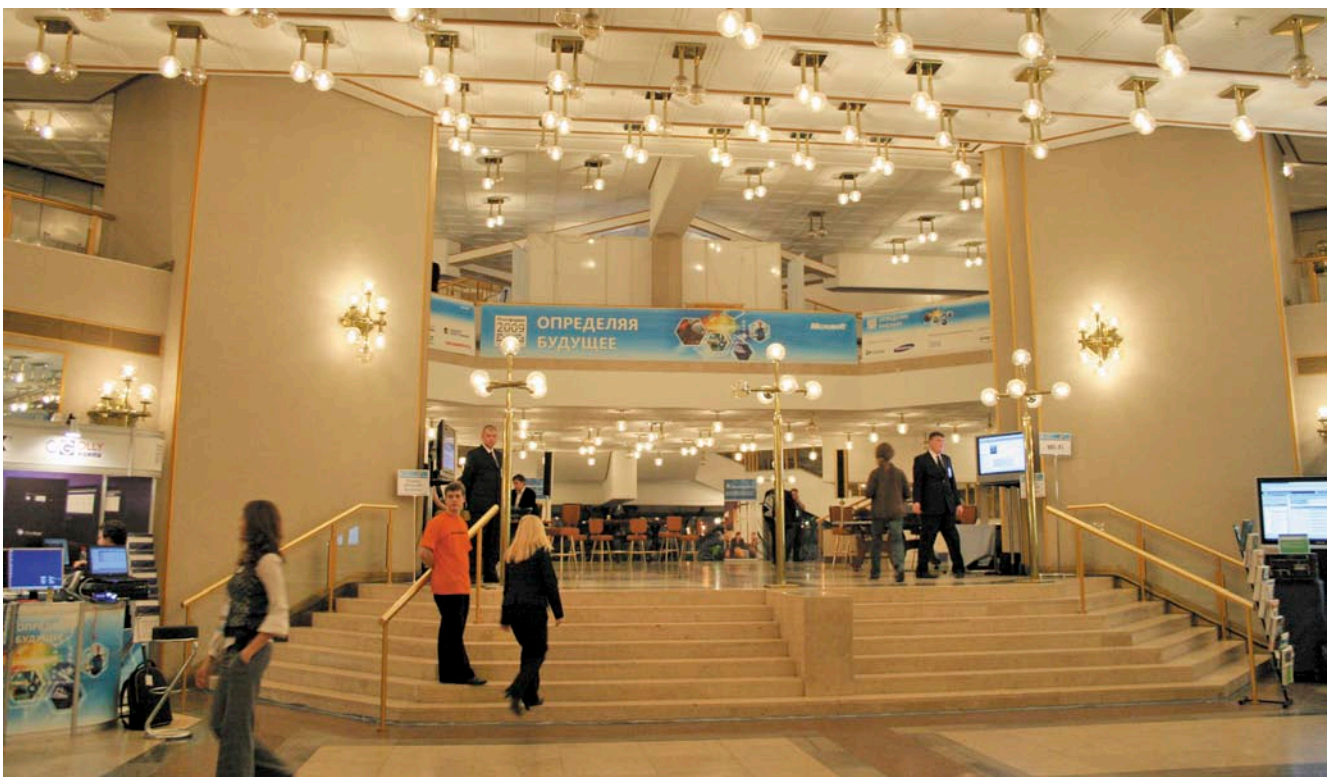
Конкурс на лучший 60-секундный рекламный видеоролик был анонсирован Linux Foundation во второй половине декабря. Название конкурса, которое должно содержаться в каждом видео, было выбрано не случайно: оно является прямой пародией на недавние рекламные кампании Apple («I'm a Mac») и Microsoft («I'm a PC»). Победитель конкурса получит возможность бесплатного участия в Japan Linux Symposium, что пройдет в Токио (Япония) в октябре 2009 года.

Участник конкурса должен быть старше 18 лет, уложиться в 60 секунд и показать в ролике, почему он любит Linux. Юмор в роликах рекомендуется, но не является обязательным. Комиссия LF будет оценивать в роликах оригинальность, ясность посылки и то, «насколько он вдохновляет других на использование Linux».

Присланные на конкурс «I'm Linux» работы доступны на video.linuxfoundation.org.

Подготовил Дмитрий Шурупов
по материалам www.nixp.ru

Платформа 2009. Определяя будущее



4-5 декабря 2008 года в Москве в здании Академии Наук РФ прошла десятая ежегодная конференция Microsoft – «Платформа 2009. Определяя будущее». На ней было представлено большое количество тематических докладов, но обо всем по порядку.

Начну с того, что за несколько месяцев до начала конференции на сайте и блогах, посвященных предстоящей «Платформе», многими пользователями высказывалось сомнение в целесообразности проведения мероприятия, в условиях глобального экономического кризиса. Объяснялась такая точка зрения тем, что в нынешних условиях заказчики не будут покупать новое программное обеспечение, и соответственно, нет смысла проводить конференцию. И хотя конференцию не отменили, но все же, мировые экономические проблемы внесли определенные коррективы в планы организаторов. Изначально местом проведения предполагалось выбрать Крокус Сити, но потом было выбрано более привычное место – здание РАН. Также, изначально хотели пригласить до 5000 человек, однако реально на конференцию были приглашены только 1500.

Темы докладов

На конференции было представлено 60 технических докладов в нескольких тематических секциях. Также проводились круглые столы, посвященные различным техническим проблемам, партнерская выставка, лабораторные работы, как с инструктором, так и для самостоятельного выполнения, действовала зона «Спроси эксперта». Еще до начала конференции было объявлено, что основным докладчиком будет Марк Руссинович, известный специалист по операционной системе Windows.

Для тех, кто не смог лично присутствовать на конференции, была развернута веб-трансляция, которая, правда, не всегда работала.

Но вернемся к темам докладов. Вот основные из них.

- Инструменты и технологии разработки программного обеспечения.
- Базы данных.
- Бизнес-аналитика и отчеты.
- Управление IT-инфраструктурой.
- Портальные решения и групповая работа.
- Операционные системы.
- Архитектура систем и приложений.
- Безопасность.
- Объединенные голосовые и почтовые коммуникации.
- Доклады партнеров.

Операционные системы

Уместить в одной статье даже краткое описание всех докладов довольно сложно, попробуем рассмотреть более подробно, что входило каждую из этих тем. Открывал конференцию, как и было заявлено, Марк Руссинович.

Начнем с «Операционных систем». Здесь было семь выступлений. В докладе «Windows – как создается операционная система» было рассказано, как создается Microsoft Windows, как устроен процесс разработки и тестиро-

вания, что происходит с Windows после выпуска и как решаются проблемы сопровождения и поддержки. При этом, в качестве примера была представлена разработка новых возможностей Windows 7 и реальных ошибок, исправленных в разных версиях Windows.

В другом докладе «Windows Server 7 – новые технологии в Windows Server 2008 R2» рассказывалось о новых возможностях готовящейся к выходу операционной системы.

Еще один интересный доклад был посвящен платформе Microsoft Windows Embedded. Данная платформа предназначена для встраивания в различные устройства, от промышленных контроллеров до сложных мультимедийных решений.

Доклад «Построение инфраструктуры систем высокой доступности» был посвящен созданию отказоустойчивых решений на основе механизмов Failover Clustering и системы виртуализации Microsoft Hyper-V.

Следующий доклад был посвящен достаточно актуальной теме – причинам несовместимости приложений с Windows Vista и их устранению. Основной упор автором доклада делался на понимании причин несовместимости и устранения и обхода этих проблем.

Windows Embedded был также посвящен еще один доклад «Разработка устройств на базе Windows Embedded Standard». В этом докладе рассматривался процесс разработки образов операционной системы Windows Embedded Standard для различных устройств, основные этапы разработки и обзор инструментария разработки ОС. В конце доклада была продемонстрирована сборка образа Windows Embedded Standard и загрузка в виртуальной среде.

И наконец, был доклад Марка Руссиновича «Технологии безопасности Windows». В этом докладе автор рассмотрел такие новые функции Windows Server 2008 как User Account Control, Cod Integrity и PatchGuard, а также то, что изменилось в уже имевшихся функциях в Windows Server 2003, таких как, подсистема обеспечения сессий пользователей.

Безопасность

По теме «Безопасность» было восемь докладов. Доклад «Claim-based identity: обзор технологий «Geneva» был посвящен набирающим популярность в последнее время Identity, то есть средствам управления учетными записями в различных приложениях. В докладе рассматривались продукты семейства Geneva для обеспечения управления учетными записями.

Другой доклад был посвящен Network Access Protection, средствам обеспечения контроля доступа устройств в корпоративную сеть.

Доклад «System Center Data Protection Manager 2007 – защити данные как Герой» рассказывал об одном из ключевых продуктов семейства Microsoft System Center, обеспечивающего непрерывную защиту данных посредством резервного копирования, серверных и клиентских систем семейства Windows, файловых серверов, приложений и данных Exchange, SQL и SharePoint.

«Безопасный обмен данными между организациями с использованием Active Directory Rights Management Services и Active Directory Federation Services» – этот доклад рассказывал о новых средствах безопасности, представленных в Windows Server 2008 и Vista: контролем прав и новых функций в Active Directory.

Доклад «Стратегия Microsoft в области информационной безопасности в России» был посвящен стратегии Microsoft в этой области и ее особенностям для российского рынка. Описываются общие тенденции развития данных средств и использование новых технологий в продуктах Microsoft.

Средствам борьбы с вирусами и спамом был посвящен доклад «Теория и практика борьбы со спамом и вредоносным кодом с помощью технологий Microsoft». Как и следовало ожидать, в докладе прежде всего рассматривались продукты семейства Forefront, а также новые средства защиты от спама в Microsoft Exchange 2007.

Доклад с интригующим названием «Что в филиале мне твоём?» был посвящен новым средствам создания распределенной доменной инфраструктуры Active Directory и нововведениям в области безопасности, появившимся в Windows Server 2008.

Восьмым же докладом по тематике «Безопасность» был уже упоминавшийся мной доклад Марка Руссиновича. Вообще, следует отметить, что тематическое деление было весьма условным, и многие доклады попадали сразу в несколько тематик.

Управление IT-инфраструктурой

Еще одной популярной темой конференции было «Управление IT-инфраструктурой». В этой тематике был представлен доклад «Microsoft Services Business Architecture – методология формирования IT-стратегии», посвященный методологии Microsoft Services Business Architecture (MSBA), используемой службой консалтинга Microsoft в проектах, связанных с формированием IT-стратегии.

Еще один доклад, рассказывающий о методах работы службы консалтинга Microsoft – «Как Microsoft Consulting Services делает крупные инфраструктурные проекты». Этот доклад раскрывал тему развертывания Enterprise-класса инфраструктурных решений силами Microsoft Consulting Services и партнеров.

Следующий доклад был посвящен продуктам Small Business Server 2008 и Essential Business Server 2008, и рассказывал о преимуществах их использования. В частности, их внедрение позволит существенно снизить затраты на развертывание и обслуживание IT-инфраструктуры, и тем самым сэкономить немало средств вашей компании.

«Как продать свой IT-отдел?» – этим вопросом озадачился автор следующего доклада. В докладе рассматривался вопрос вывода IT-отдела в отдельную дочернюю компанию, оказывающую услуги аутсорсинга. Экономический эффект от операции, повышение качества поддержки, привлечение новых заказчиков.

Еще один доклад по схожей теме – «Как спланировать и построить инфраструктуру объединенных коммуникаций». В докладе сообщалось о методиках планирования решения, выборе партнерского ПО, дополняющего наше решение для объединенных коммуникаций и этапах внедрения полученного комплекса. Аналогичный доклад «Построение концепции развития IT-системы предприятия: подход Microsoft – оценка, планирование, вы-

годы» рассматривал вопросы обоснования необходимости инвестирования в проблемные области перед руководством компании, а также давались рекомендации для IT-специалистов по реализации этих планов.

Довольно интересное выступление было посвящено мониторингу приложений с помощью System Center Operations Manager и AVIcode Intercept Studio. Здесь был рассмотрен вопрос использования средств System Center для мониторинга нестандартных .NET-приложений.

Еще один доклад Марка Руссиновича был посвящен поиску и устранению неисправностей в Windows-системах. В докладе на реальных примерах сбоев системы и приложений были продемонстрированы приемы работы с Microsoft Debugging Tools и утилитами Sysinternals, такими как Process Explorer, Process Monitor, и Accesschk.

Средства разработки

Продолжая свой рассказ о докладах конференции, мне хотелось бы рассказать о выступлениях, посвященных инструментам и технологиям разработки программного обеспечения. Здесь были доклады, посвященные перспективам языка C#, новым возможностям платформы для создания графических интерфейсов для веб-приложений Silverlight 2, новой версии системы разработки приложений Visual Studio 2010.

Доклад «Windows Presentation Foundation 3.5 SP1 – новые возможности разработки интерактивных клиентских приложений» был посвящен средствам создания интерактивных приложений с учетом существенных улучшений в .NET Framework 3.5 SP1.

Еще в одном докладе рассказывалось о будущей технологии ASP.NET 4.0. Вообще, стоит отметить, что многие технические доклады, посвященные средствам разработки были связаны с использованием веб-технологий, как альтернативы клиентским приложениям.

Один из докладов так и назывался «Актуальна ли еще разработка клиентских приложений или настало время писать только под Web?». Его авторы проводили анализ текущих технологических возможностей и ориентиров для Windows и веб-приложений.

В выступлении «Доступ к данным через Web с использованием ADO.NET Data Services» сообщалось о технологии ADO.NET Data Services, которая позволяет построить REST-сервис для доступа к данным.

Еще один достаточно актуальный доклад был посвящен написанию полноценных бизнес-приложений на Windows Mobile. В нем рассказывалось обо всех аспектах решения данной задачи с учетом технологических особенностей мобильных устройств.

Базы данных и порталы

Тематика «Базы данных» как и предполагалось, целиком состояла из сообщений, посвященных SQL Server 2008. Были темы, посвященные как общему устройству данного программного продукта, так и отдельным службам, например SQL Server Analysis Services 2008.

Доклады из темы «Портальные решения и групповая работа» были посвящены различным аспектам разработки и внедрения бизнес-порталов для увеличения эффективности работы предприятия в целом.

Объединенные голосовые и почтовые коммуникации

Продолжая рассказ о темах конференции, хотелось бы рассмотреть направление «Объединенные голосовые и почтовые коммуникации». Здесь был доклад «Новый виток эволюции в объединенных коммуникациях. Office Communication Server 2007 R2», посвященный новым возможностям Office Communication Server 2007 и средствам построения систем объединенных коммуникаций в корпоративной сети.

Также в этой теме были уже упоминавшиеся ранее доклады по средствам защиты от спама в Microsoft Exchange и построению инфраструктуры объединенных коммуникаций.

Доклады партнеров

В завершение своего отчета о конференции, я расскажу о докладах партнеров. Прежде всего следует отметить доклады от Citrix. Этот производитель представил ряд сообщений, в которых рассматривалось использование различных средств виртуализации, от датацентра до десктопа.

Еще один интересный доклад был посвящен Citrix NetScaler – контроллеру доставки веб-приложений, позволяющему осуществлять балансировку нагрузки при доставке контента.

Citrix Provisioning Server 5 – это новое средство потоковой доставки операционной системы. При этом доставка ОС может осуществляться как на физические, так и на виртуальные машины. В презентации рассматривались технологии, лежащие в основе этого продукта, возможные области применения: например, для обновления клиентских операционных систем на всём предприятии или построения отказоустойчивых датацентров.

Citrix также представил доклад, посвященный увеличению защищенности корпоративных ресурсов, посредствам таких продуктов Citrix, как Citrix XenApp, Password Manager и Access Gateway, позволяющим организовать безопасную защищенную доставку любого приложения или сервиса, оптимизировать парольную защиту приложений и создать систему глобального видео-аудита работы пользователей с приложениями.

Помимо Citrix в этой тематике были также представлены доклады о средствах виртуализации от HP, решения Sun на базе четырехядерных процессоров AMD Opteron и решения по созданию систем документооборота на основе Microsoft Sharepoint.

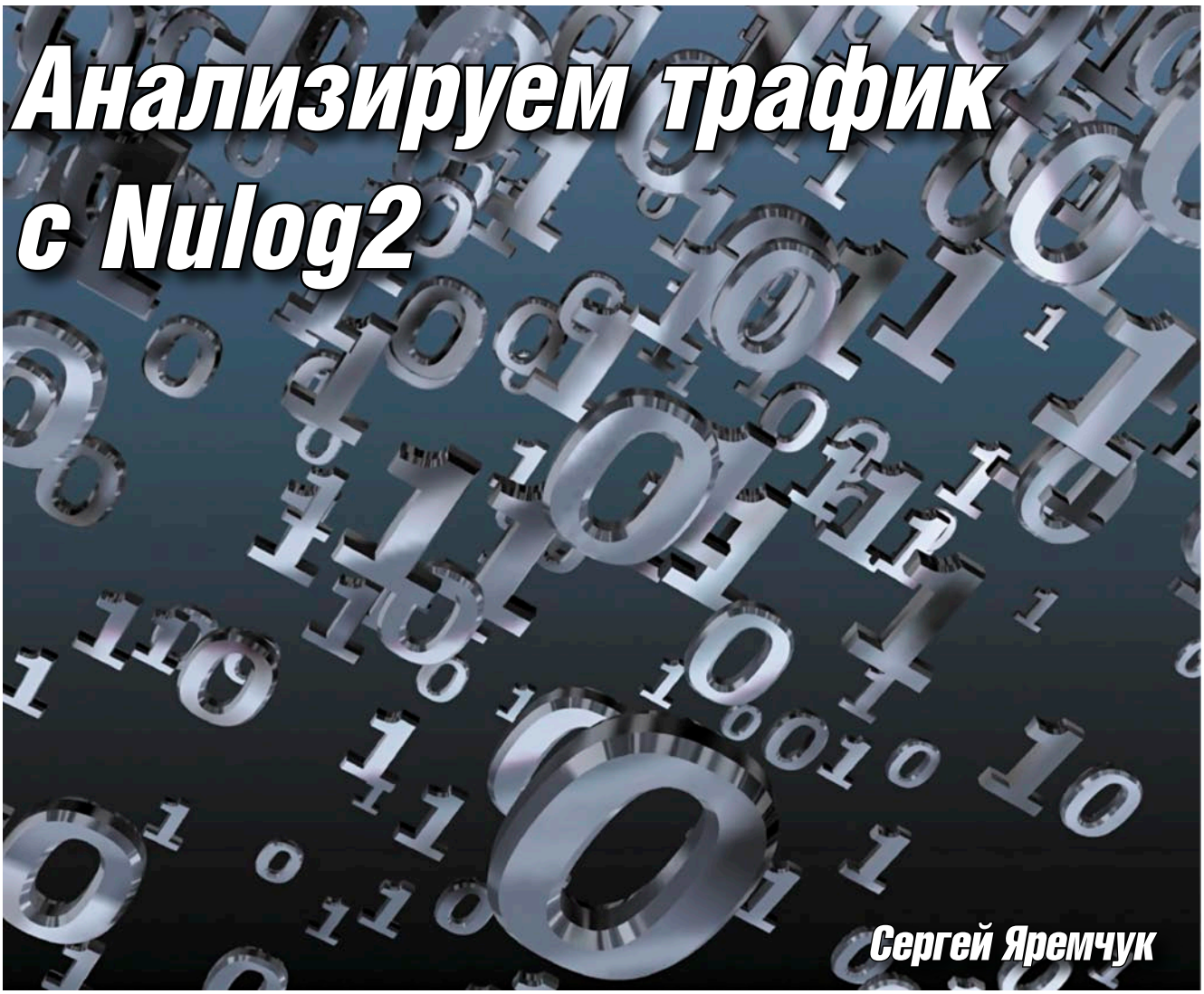
В завершении конференции было сделано важное объявление, Стен Биргер, возглавлявший российское представительство Microsoft, покидает свой пост, и на его место приходит Николай Пряничников, до этого руководивший «Вымпелкомом». Таким образом, со следующего года во главе компании человек, хорошо знакомый со спецификой российского бизнеса и его современными реалиями.

В целом конференция произвела положительное впечатление. Было много интересных докладов, посвященных новым технологиям. Так что, полагаю, «Платформа 2009» задала вектор развития современных IT-технологий на ближайшее время.

Сайт, посвященный конференции, – http://platforma2009.ru.

Текст: Андрей Бирюков
Фото: Евгения Тарабрина

Анализируем трафик с Nulog2



Сергей Яремчук

Рассмотрим настройку веб-интерфейса NuLog2, позволяющего администратору в удобном виде просматривать информацию о соединениях, проходящих через Netfilter и uFW.

Проект NuLog2

В GNU/Linux все сетевые пакеты проходят через Netfilter, в силу чего он и обладает самой достоверной информацией о количестве переданных и принятых данных. В 2000 году Гаральдом Велте (Harald Welte) был написан патч к ядру – ULOG (Userspace Logging), позволяющий получать эту информацию в пространстве пользовательских процессов (user space) в удобном виде. Несмотря на то что «добраться» до нужных данных теперь стало на порядок проще, администраторам приходилось самостоятельно решать проблему их съема, обработки и выдачи в нужном виде. Как результат появилось несколько проектов, решающих эти проблемы. Некоторые обеспечивали понятный интерфейс к получению данных с ULOG, например, демон ulogd [1], написанный самим Гаральдом Велте, specter [2], построенный на базе ulogd 1.02, и ulog-acctd [3]. Стоит заметить, что основные разработки представленных проектов датированы 2005 годом, правда, это не мешает их полноценно использовать и до сих пор. И только ulogd, о возможностях которого будем говорить по ходу статьи, недавно начал опять активно развиваться. Другие проекты нацелены на выдачу информации, полученной при помощи программ первой группы в удобной форме – scanulog, ulog-monitor, Webfwlog и Nulog2. Возможностям последнего и посвящена статья.

Проект NuLog2 [4] является дальнейшим развитием PHP-интерфейса к ulogd и NuFW [5]– NuLog (в Интернете встречаются и другие его названия – NuLog1 или ulogd-php). Разработка последнего приостановлена в июле 2007 года, но уже через месяц начата работа над его второй версией – NuLog2, которая позиционируется уже как анализатор журналов Netfilter и NuFW.

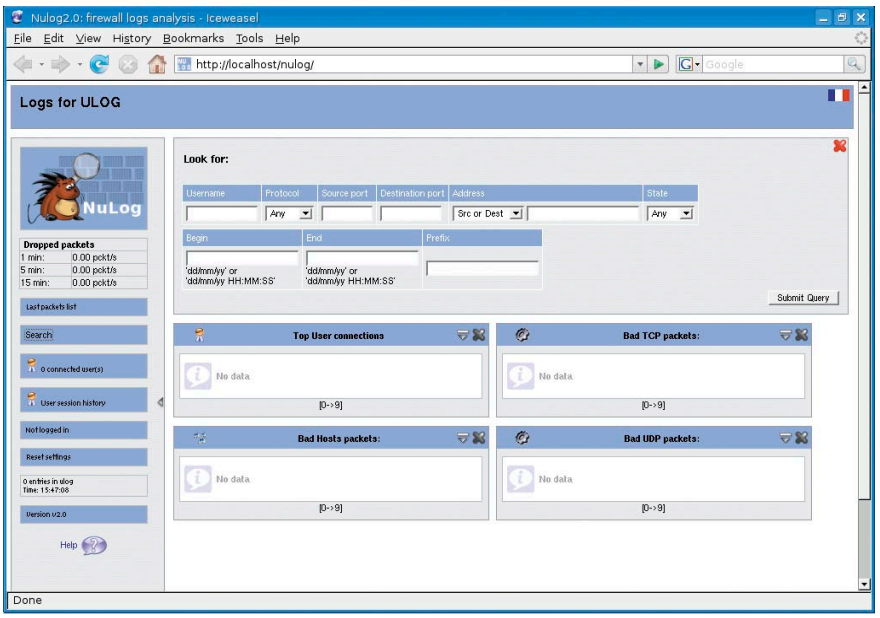
В отличие от предшественника, написанного на PHP, код NuLog2 полностью переписан на Python с использованием среды разработки Twisted. Но, несмотря на все отличия, NuLog2 использует ту же модель данных, поэтому очень просто можно перейти с NuLog на NuLog2 без потери информации. Кроме среды разработки, изменена и лицензия с GPL v2 на GPL v3.

В настоящее время интерфейс обеспечивает просмотр информации

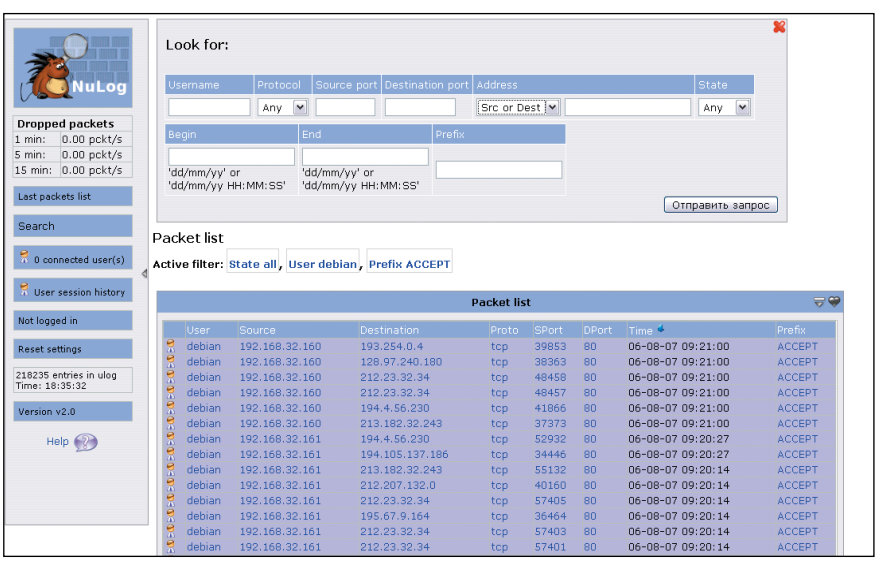
о разрешенных, заблокированных пакетах по IP-адресам и пользователям (только NuFW), TCP- и UDP-портам, а также приложениям, задействованным в процессе соединения (только NuFW).

Поддерживаются обе версии протокола IPv4 и IPv6, возможен детальный просмотр каждого пакета, вывод истории запросов. Все данные сведены в таблицы и графики, предлагающие просмотр в удобном виде. Возможен экспорт данных в CVS-файл.

Реализованы функции поиска, интерфейс, написанный с использованием технологии AJAX, полностью настраиваемый. В настоящее время NuLog2 не локализован, но все параметры понятны и без перевода, так как соответсвуют устоявшимся терминам. Предвидя вопросы, скажу, что, к большому сожалению, такой востребованной функции как учет трафика, в NuLog2 нет.



Интерфейс NuLog2 сразу после установки



В NuLog2 реализованы функции поиска по нескольким параметрам

Установка и настройка ulogd

Ознакомиться с возможностями Nulog2 (а также NuFW и интерфейса для его настройки Nuface) можно в дистрибутиве NuFW.live [6], который выполнен в формате LiveCD, основанном на KNOPPIX. Мы же рассмотрим установку его на рабочую систему на примере Ubuntu 8.04 LTS, хотя много из сказанного применимо и для других дистрибутивов.

Для регистрации событий необходим модуль ядра ipt_ULOG.o, который появился в ядре начиная с версии 2.4.18-pre8. Тому, кто использует более ранний релиз ядра, следует его обновить или установить патч ulog-patch с netfilter patch-o-matic. Ядро, используемое в Ubuntu 8.04 по умолчанию:

```
$ uname -r
2.6.24-16-generic
```

В параметрах сборки ULOG активирован:

```
$ grep -i ulog /usr/src/linux/.config
CONFIG_BRIDGE_EBT_ULOG=m
CONFIG_IP_NF_TARGET_ULOG=m
```

Забегая чуть вперед, скажу, что после загрузки демона ulogd в списке lsmod должен появиться нужный модуль:

```
$ lsmod | grep -i ulog
ipt_ULOG               10116  2
```

В репозитарии Ubuntu имеются нужные пакеты для установки ulogd. Но следует знать, что сегодня существует две ветки: стабильная 1.2x и находящаяся пока в стадии разработки ulogd-2.x. Последняя имеет несколько больше встроенных модулей, кроме этого, в ней реализована система фильтров (подробнее во врезке «Сборка ulogd2 в Ubuntu»). Для работы NuLog2 достаточно и релиза 1.23 (апрель 2005 года), который и доступен в репозитарии Ubuntu.

```
$ sudo apt-cache showpkg  ulogd | grep -i versions
Versions: 1.23
```

Устанавливается стандартно:

```
$ sudo aptitude install ulogd ulogd-mysql
```

По умолчанию ulogd сохраняет данные в файл текстового формата, подключив плагины, можно добавить поддержку записи в базы данных MySQL, PostgreSQL, SQLLite3,

Аутентификация пользователя в NuLog2

В настоящий момент NuLog2 не имеет никаких средств аутентификации пользователей. Доступ к статистике можно ограничить несколькими способами: параметром address в файле wrapper.conf, который будет указывать на внутренний интерфейс, правилами iptables/NuFW, разрешающими доступ к нужному порту только с определенных адресов или пользователей. Разработчики предлагают для этих целей использовать веб-сервер, который будет отсылать HTTP-заголовок Nulog_User, включающий имя пользователя.

Для веб-сервера Apache записываем в конфигурационный файл /etc/apache2/apache2.conf следующие директивы (см. **листинг**).

```
<VirtualHost *>
            ServerName nulog

            ProxyPreserveHost Off
            ProxyPassReverse /nulog http://localhost:8080/nulog

<Location /nulog>
                Allow from all
                AuthType Basic
                AuthName nulog
                AuthUserFile /etc/apache2/users
                AuthBasicProvider file
                Require valid-user

                RewriteEngine on
                RewriteCond %{LA-U:REMOTE_USER} (.+)
                RewriteRule /nulog(.*) http://localhost:8080/nulog$1 [P,E=RU:%1]
                RewriteRule /nulog(.*) http://localhost:8080/nulog$1 [P]
                RequestHeader set Nulog_User %{RU}e
                RequestHeader unset Authorization
    </Location>
  </VirtualHost>
```

Далее создаем учетные записи при помощи htpasswd.

файл формата PCAP/Tcpdump или syslog. Для работы NuLog2 в выбранном варианте необходима поддержка MySQL, модули для работы с которой как раз и находятся во втором пакете.

Конфигурационный файл по умолчанию находится в /etc/ulogd.conf, если он раположен в другом месте, на него можно указать при помощи параметра -c. В отличие от ulogd2, в котором на порядок больше настроек, файл ulogd.conf гораздо проще, значения основной части понятны:

```
[global]
# Файл журнала и уровень журналирования
logfile="/var/log/ulog/ulogd.log"
# debug(1), info(3), notice(5), error(7) or fatal(8)
# Вначале лучше поставить 1, а затем после полного
# прогона переключить на 5
loglevel=1
# Плагины вывода
# Текстовый формат
plugin="/usr/lib/ulogd/ulogd_LOGEMU.so"
# Для вывода в MySQL, пока отключаем
#plugin="/usr/lib/ulogd/ulogd_MYSQL.so"
# Параметры вывода для разных плагинов
# Текстовый
 [LOGEMU]
file="/var/log/ulog/syslogemu.log"
# Подключение к MySQL
[MYSQL]
table="ulog"
pass="pass"
user="user"
db="ulogd"
host="localhost"
```

Далее нужно в правилах iptables указать, чтобы он использовал ULOG вместо LOG. В общем случае идея очень проста, нужно в правилах заменить строки вида:

```
iptables -A FORWARD $FILTER -j LOG
```

на

```
iptables -A FORWARD $FILTER -j ULOG
```

Но в Ubuntu начиная с версии 8.04 для управления правилами Netfilter используется – UFW (Uncomplicated firewall). Поэтому весь процесс здесь выглядит несколько иначе, чем в других дистрибутивах.

Все настройки UFW находятся в каталоге /etc/ufw, синтаксис команд несколько напоминает iptables, но чуть проще и понятнее. По умолчанию UFW отключен, и перед запуском демона необходимо в файле /etc/ufw/ufw.conf разрешить его запуск, заменив строку:

```
# set to yes to start on boot
ENABLED=no
```

на

```
ENABLED=yes
```

Правила регистрации находятся в файле /etc/ufw/after.rules и по умолчанию выглядят так:

```
$ cat /etc/ufw/after.rules
...
# catchall for logging
-A ufw-after-input -m limit --limit 3/min ↵
      --limit-burst 10 -j LOG ↵
      --log-prefix "[UFW BLOCK INPUT]: "
-A ufw-after-forward -m limit --limit 3/min ↵
      --limit-burst 10 -j LOG ↵
      --log-prefix "[UFW BLOCK FORWARD]: "
```

Чтобы переключить их на ULOG, достаточно заменить LOG на ULOG (параметры с limit можно убрать):

```
-A ufw-after-input -m limit --limit 3/min ↵
      --limit-burst 10 -j ULOG ↵
      --ulog-prefix "[UFW BLOCK INPUT]: "
-A ufw-after-forward -m limit --limit 3/min ↵
      --limit-burst 10 -j ULOG ↵
      --ulog-prefix "[UFW BLOCK FORWARD]: "
```

Теперь включаем регистрацию:

```
$ sudo ufw logging on
Logging enabled
```

И проверяем:

```
$ sudo iptables -L -n | grep ULOG
Logging enabled
ULOG       all  --  0.0.0.0/0           0.0.0.0/0
```

```
limit: avg 3/min burst 10 ULOG copy_range 0 nlgroup 1 prefix
`[UFW BLOCK FORWARD]: ' queue_threshold 1
ULOG       all  --  0.0.0.0/0            0.0.0.0/0
limit: avg 3/min burst 10 ULOG copy_range 0 nlgroup 1 prefix
`[UFW BLOCK INPUT]: ' queue_threshold 1
```

Перезапускаем демон ulogd:

```
$ sudo /etc/init.d/ulogd restart
```

Параллельно проверяем записи в файле журнала:

```
$ tail -f /var/log/ulog/syslogemu.log
```

```
Dec 23 21:56:06 router FORWARD IN=eth0 OUT=eth1
MAC=00:e0:4d:07:c2:03:00:1d:60:9a:b8:8e:08:00  SRC=192.168.1.195
DST=192.168.0.1 LEN=48 TOS=00 PREC=0x00 TTL=127 ID=26261 DF
PROTO=TCP SPT=1135 DPT=8080 SEQ=508149838 ACK=0 WINDOW=65535
SYN URGP=0
```

Если все нормально, можно снимать комментарии со строк, отвечающих за работу с MySQL. В пакете ulogd-mysql имеется файл /usr/share/doc/ulogd-mysql/mysql.table, предназначенный для создания таблиц в MySQL. Но разработчики NuLog предлагают свой файл, который и необходимо использовать. Работа с NuFW ранних версий описана в [5], поэтому останавливаться на этом вопросе не буду. Тем более что NuFW для NuLog2 идет как опциональный компонент. Теперь все готово к установке NuLog2.

Установка NuLog2

Для установки и работы NuLog2 потребуется ряд пакетов.

В Ubuntu установить их можно командой:

```
$ sudo apt-get install python2.4 python-twisted ↵
      python-nevow python-matplotlib gettext ↵
      python-soappy python-mysqldb python-cairo ↵
      python-ipy python-numpy python-docutils
```

Разработчики в документации приводят вместо apt-get программу aptitude, но в первом случае будет скачано всего 45 Мб архивов вместо 154 Мб при использовании aptitude. Актуальной версией на момент написания этих строк являлась 2.1.3, датированная декабрем 2008 года, которую и будем устанавливать. Архивы с исходными текстами доступны по адресу http://software.inl.fr/releases/Nulog2.

Скачиваем и распаковываем обычным образом. Создаем базу данных и учетную запись.

```
$ mysql -uroot -prootpassword
> CREATE DATABASE ulogd;
> GRANT ALL PRIVILEGES ON ulogd.* TO 'user'@'localhost' ↵
      IDENTIFIED BY 'pass';
```

В подкаталоге scripts архива находятся файлы для создания таблиц. Для IPv4-сети выбираем файл ipv4.sql:

```
$ mysql -uuser -ppass ulogd < ./scripts/ipv4.sql
```

Для улучшения производительности можно использовать триггеры, которые будут задействованы при вставке данных в некоторые таблицы (usersstats, offenders, tcp_ports, udp_ports):

```
$ mysql -uroot -ppass ulogd < ./scripts/triggers.py
```

В ранних версиях MySQL (младше 5.0.32) перед запуском скрипта следует удалить строку:

```
DROP TRIGGER IF EXISTS update_cache;
```

иначе получим ошибку. Перезапускаем ulogd, чтобы он начал собирать данные в базу:

```
$ sudo /etc/init.d/ulogd restart
```

Чтобы установить Nulog2, достаточно выполнить скрипт setup.py, находящийся в дистрибутиве:

```
$ sudo ./setup.py install
```

И затем для сборки документации:

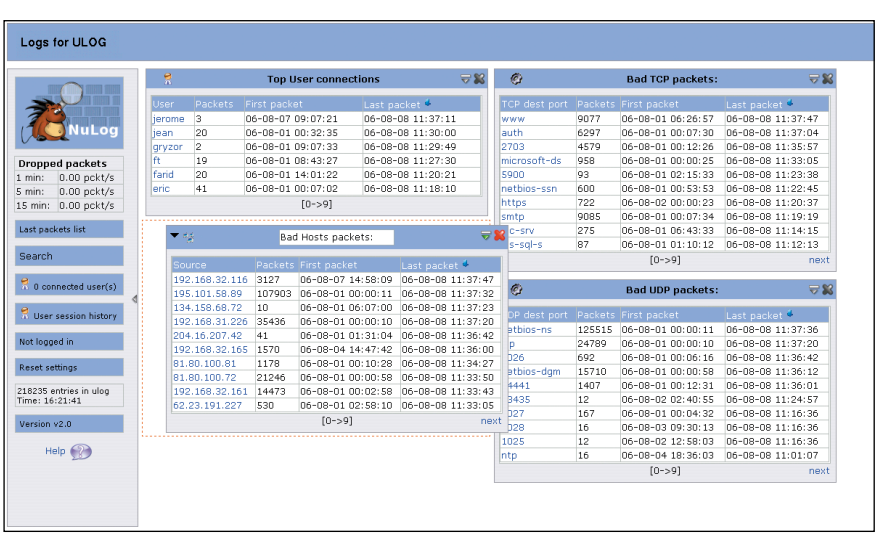
```
$ make
```

Теперь можно приступать к настройкам. Конфигурационные файлы Nulog2 находятся в каталоге /etc/nulog, внутри имеется несколько файлов, три из которых основные: default.wrapper.conf, default.core.conf' и default.nulog.conf. Чтобы их активировать, нужно убрать префикс default из имени – wrapper.conf, core.conf' и nulog.conf.

NuLog2 для визуализации и вывода данных использует собственный веб-сервер, настройки которого указываются в wrapper.conf.

```
[server]
port=8080
vardir = /var/lib/nucentral/
address = 0.0.0.0

# список модулей
[modules]
nulog-core=yes
nulog-web=yes
auth=yes
```



Интерфейс NuLog2 легко видоизменить

Сборка ulogd2 в Ubuntu

Тем же, кто решил установить самую последнюю версию ulogd, приведу краткую инструкцию по компиляции. Возможности во второй версии несколько шире. Так, уже реализовано три типа плагинов: источник, фильтр и вывод. Плагины комбинируются в стек (stack), который, собственно, и указывает, что нужно делать демону. То есть теперь, чтобы захватить и вывести данные в файл, необходимо явно задавать:

```
stack=log1:NFLOG,op1: LOGEMU
```

Иначе получим ошибку вроде:

```
Mon Dec 29 21:53:14 2008 <8> ulogd.c:1102
not even a single working plugin stack
```

Означающую, что ulogd попросту не знает, что ему делать.

В стек может входить только по одному плагину источника и вывода. Количество фильтров неограничено. Конфигурация может содержать несколько стеков, поэтому отбор нужной информации можно настроить действительно тонко.

Кроме этого, в ulogd2 используется несколько измененная схема SQL, в которой данные разделены на несколько таблиц (вместо одной в ulogd), что дает возможность легко добавить дополнительную информацию, создав новую таблицу. В отличие от ulogd1 вторая версия построена таким образом, что изменение схемы SQL никак не повлияет на его работу. Кроме ULOG, поддерживается и NFLOG.

Для сборки, кроме самого архива с исходными кодами, потребуются самые последние версии библиотек – libnfnetlink, libnetfilter_log (захват пакетов) и libnetfilter_conntrack (захват потока conntrack), которые можно скачать по ссылкам на странице http://www.netfilter.org/projects. Некоторые из этих библиотек есть в репозитарии, но их версия существенно отстает от требуемой. В случае возникновения проблем конфигурационный скрипт самостоятельно укажет, чего ему не хватает.

```
checking for LIBNETFILTER_CONNTRACK... no
configure: error: Cannot find libnetfilter_
conntrack >= 0.0.95
```

Компиляция библиотек стандартна:

```
$ ./configure
$ make
$ sudo make install
```

Для удобства можно собрать deb-пакет, воспользовавшись инструкцией The Ubuntu Packaging Guide (https://help.ubuntu.com/6.10/ubuntu/packagingguide/C).

Если в процессе конфигурирования ulogd будут получены сообщения вроде:

```
configure: WARNING: mysql.h not found
checking for mysql_close in -lmysqlclient... no
configure: WARNING: libmysqlclient.so not found
```

Это означает, что нет заголовочных файлов для активации поддержки MySQL. Так как для работы NuLog2 такой модуль необходим, доустанавливаем пакет, в котором находятся нужные файлы.

```
$ sudo aptitude install ↵
      libmysqlclient15-dev
```

На момент написания этих строк была актуальной версия ulogd-2.0.0beta2, при использовании которой могут появляться разного рода ошибки. Поэтому лучше использовать более «свежую» svn/git-версию. В этом случае для сборки, кроме, собственно, build-essential и subversion в Ubuntu, потребуется установить еще ряд пакетов:

```
$ sudo apt-get install autoconf ↵
      automake1.9 libtool
```

Далее как обычно.

```
$ svn co https://svn.netfilter.org/ ↵
      netfilter/branches/ulog/ulogd2
$ cd ulogd2
~/ulogd2$ ./autogen.sh; ./configure; ↵
      make; sudo make install
```

Так как по умолчанию установка производится в /usr/local, следует указать путь к /usr/local/lib/ulogd в файле /etc/ld.so.conf, чтобы динамические библиотеки были видны.

Кроме этого, необходимо вручную перенести конфигурационные файлы и создать ссылки для запуска:

```
$ sudo cp -v ulogd.conf ↵
      /usr/local/etc/ulogd.conf
$ sudo cp -v ulogd.logrotate ↵
      /etc/logrotate.d/ulogd
$ sudo cp -v ulogd.init ↵
      /etc/init.d/ulogd
$ sudo ln -s /etc/init.d/ulogd ↵
      /etc/rcS.d/S99ulogd
```

После настроек советую в первый раз запустить демон в консоли, чтобы просмотреть возможные ошибки.

```
$ sudo /usr/local/sbin/ulogd
```

Далее для создания рабочего окружения запускаем скрипт install_defconf.sh.

```
$ ./script/install_defconf.sh
```

Скрипт задаст несколько вопросов по размещению рабочего каталога и конфигурационных файлов NuLog и NuFW. В большинстве случаев можно использовать настройки, предлагаемые по умолчанию.

Параметры подключения к MySQL описываются в файле core.conf:

```
# Database configuration
[DB]
host=localhost
db=ulog
user=user
password=pass

# Тип БД mysql/pgsql
dbtype=mysql

# Тип sql scheme ulog/triggers
type=triggers
ip=4
table=ulog
```

Файл nulog.conf содержит настройки, актуальные для веб-интерфейса (их скорее всего трогать не придется).

```
# URL для доступа к основной странице
url=/nulog/

# Заголовок веб-страницы
maintitle=Log ULOG
# Использование Nuface2 ACLs
# nuface_acl=https://localhost/nuface/%%s.php?acl=%%s

[Sessions]
# разрешение на анонимное подключение
anonymous=yes
[Misc]
# формат даты
datetime=%%y-%%m-%%d %%H:%%M:%%S
# Интеграция с панелью дистрибутива Edenwall
# (http://www.edenwall.com), можно просмотреть в NuFW.Live
edenwall_integration=0
```

Разработчики приготовили стартовый скрипт для более удобного запуска NuLog2. Копируем его в нужное место и создаем необходимые ссылки для автоматической загрузки.

```
$ sudo  cp -v ./debian/init.d /etc/init.d/nulog
$ sudo  ln -s /etc/init.d/nulog /etc/rcS.d/nulog
```

И запускаем:

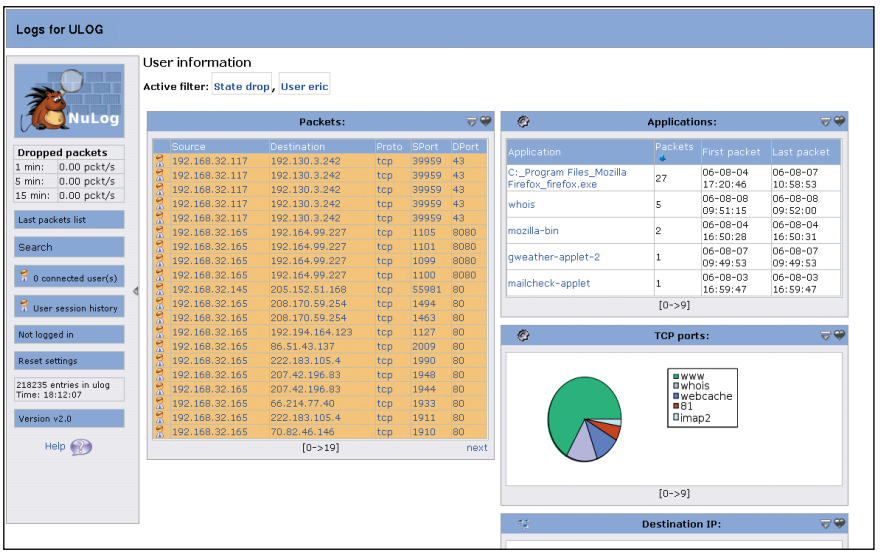
```
$ sudo /etc/init.d/nulog restart
```

Или чтобы получить больше отладочной информации:

```
$ sudo twistd -noy /usr/sbin/nulog.tac
```

Набираем в веб-браузере http://localhost:8080/nulog/ и попадаем на главную страницу.

Чтобы разобраться с возможностями Nulog2, потребуется от силы 5 минут. Все достаточно просто и понятно.



Использование NuFW расширяет возможности NuLog2

Итог

Мы получили систему, которая позволяет отслеживать сетевые события. Конечно, чтобы полностью оценить возможности NuLog2, потребуется установить и настроить NuFW, что позволит не только разрешать выход в Интернет по учетным записям, а не IP-адресам, но и привязать события к конкретному пользователю или приложению.

1. Сайты проекта ulogd – http://www.gnumonks.org/projects, http://www.netfilter.org/projects/ulogd.
2. Сайт проекта specter – http://joker.linuxstuff.pl/specter.
3. Сайт проекта ulog-acctd – http://alioth.debian.org/projects/pkg-ulog-acctd.
4. Сайт проекта NuLog2 – http://software.inl.fr/trac/wiki/EdenWall/NuLog.
5. Яремчук С. Шлюз аутентификации пользователей NuFW. //Системный администратор, №3, 2006 г. – С. 46-50.
6. LiveCD, демонстрирующий возможности NuFW – http://live.nufw.org.

Hyperic HQ – система мониторинга корпоративного уровня

Дмитрий Петухов

Компьютерная инфраструктура – критически важная среда для ведения бизнеса, требующая постоянного контроля и обеспечения ее бесперебойной работы. Всегда быть в курсе происходящего и предотвратить какие-либо проблемы поможет внедрение системы мониторинга ресурсов сети.

Внедрение на предприятии системы мониторинга ресурсов сети является верным шагом на пути управления развивающейся инфраструктурой. За счет постоянного контроля всех важных узлов и элементов повышается надежность и отказоустойчивость всей системы в целом. При возникновении критических ситуаций, система оповестит ключевой персонал о возникших неполадках, либо и вовсе поможет предотвратить проблему. Одной из основных проблем при внедрении такой системы, становится выбор из всего многообразия предлагаемых продуктов. В этом обзоре мы подробно остановимся на одном из таких вариантов – системе мониторинга корпоративного уровня Hyperic HQ.

О системе Hyperic HQ

Hyperic HQ – это всеобъемлющий набор инструментов, который позволяет:

- отслеживать производительность системы;
- собирать и хранить данные об аппаратных средствах сети, средствах виртуализации и приложениях;
- создавать оповещения об интересующих нас событиях – используя единый центр управления, доступный через веб-интерфейс.

Комплекс достаточно прост в установке и может быть развернут на Linux, Solaris 10 или старше, Mac OS X (Intel x86), Windows 2003 Server, посредством инсталлируемых на серверы агентов.

Hyperic HQ доступна в двух вариантах для загрузки: Enterprise и Open Source. На настоящий момент последней стабильной версией является 3.2. Отличие версии Enterprise от Open Source заключается в отсутствии у последней некоторой функциональности, в частности технической поддержки, возможности создания своих шаблонов оповещения, авторизации LDAP и Kerberos, но, несмотря на это, она вполне пригодна для использования на малых предприятиях со средней сложности инфраструктурой.

Также стоит упомянуть о существовании совместного открытого проекта компаний Red Hat и Hyperic, под названием RHQ, нацеленного на управление корпоративной информационно-технической инфраструктурой. RHQ разрабатывается как единый набор инструментов, которые будут включены в будущие издания продуктов Red Hat, таких как JBoss Operations Network и Red Hat Network, а также в сам Hyperic HQ.

Архитектура системы базируется на следующих четырех основных абстракциях:

- **Platform (платформа)** – машина, операционная система или любая комбинация сетей и устройств хранения данных. Платформы являются самым нижним уровнем в архитектуре управления и могут включать в себя такие элементы, как процессоры, сетевые интерфейсы, жесткие диски, а также файловые системы.
- **Server (сервер)** – это любое серверное программное обеспечение, которое установлено на платформу. Hyperic HQ способно управлять различными типами серверов, такими как веб-серверы с базами данных, серверы обмена и многое другое.
- **Service (служба)** – это один из компонентов серверов, который выполняет конкретную задачу. Примером такой службы может являться виртуальный хост в настройках Apache.
- **Application** – это понятие представляет собой идею того, что одна общая задача выполняется на различных платформах и обеспечивается разными серверами. Пользовательский интерфейс предлагает способ управления инфраструктурой с прикладной точки зрения в противовес аппаратной. Смысл в том, чтобы объединить службы, выполняющие одну глобальную задачу в единые группы. Для большей наглядности и понимания этой абстракции предлагаю взглянуть на **рис. 1**.

Системные требования

Необходимое аппаратное обеспечение для нормальной работы серверной части:

- Процессор Pentium 4 или эквивалент, 1 ГГц или выше (рекомендуется два процессора Pentium Xeon 2.4 ГГц или эквивалент);
- 1 Гб или выше (рекомендуется 4 Гб или более);
- 1-5 Гб свободного дискового пространства;
- Поддерживаемые операционные системы Linux, Windows XP или 2003 Server, Solaris 8 или выше, HP-UX.

Hyperic HQ Server по умолчанию настроен на работу со своей собственной базой данных, однако есть возможность хранения информации и в других базах данных. Поддерживаются следующие БД:

- PostgreSQL 8 или выше;
- Oracle 9i или 10g;
- MySQL 5.0.45 или выше.

Необходимое аппаратное обеспечение для нормальной работы агента:

- Celeron 500 МГц или выше, или эквивалент;
- 256 Мб ОЗУ;

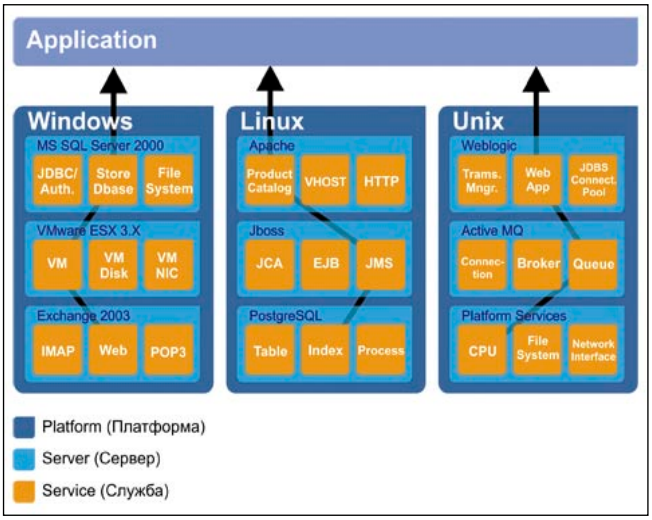


Рисунок 1. Модель Application

- 500 Мб свободного дискового пространства;
- поддерживаемые операционные системы Linux, Windows XP или 2003 Server, Solaris 8 или выше, HP-UX, AIX, FreeBSD.

Общими требованиями для сервера и агента является наличие JRE или JDK 1.4 или 1.5. И сервер, и агент уже содержат в комплекте JRE, которое рекомендовано для использования. Однако иногда бывает предпочтительнее использовать JRE (или JDK), которые могут быть уже установлены в системе.

Установка Hyperic HQ

Установка и тестирование системы производилось мной на Windows Vista Ultimate SP1 и CentOS 5.1. Хотя Windows Vista и не заявлена в документации как поддерживаемая платформа, Hyperic HQ была проинсталлирована, и без каких- либо проблем выполняла свои функции.

Процесс установки системы на Windows достаточно прост. После скачивания архива распаковываем его в корень системного диска и запускаем файл setup.bat из корня установочной директории. Откроется консоль со следующим содержимым:

```
C:\<Installation Directory>\setup.bat
Initializing Hyperic HQ Installation...
Choose which software to install:
1: Hyperic HQ Server
2: Hyperic HQ Shell
3: Hyperic HQ Agent
You may enter multiple choices, separated by commas.
```

Здесь предлагается выбрать компоненты для установки, причем можно выбрать сразу несколько компонентов через запятую. Выбираем установку сервера и агента, то есть вводим «1, 3».

Далее предлагается выбрать путь для установки сервера, по умолчанию это C:\Program Files, мы не будем мудрить и просто нажмем клавишу <Enter>. Если на вашей системе не обнаружен SMTP-сервер, который будет использоваться системой для отправки уведомлений, то будет запрошен его адрес или доменное имя. Следующим шагом установщик запросит путь для установки аген-

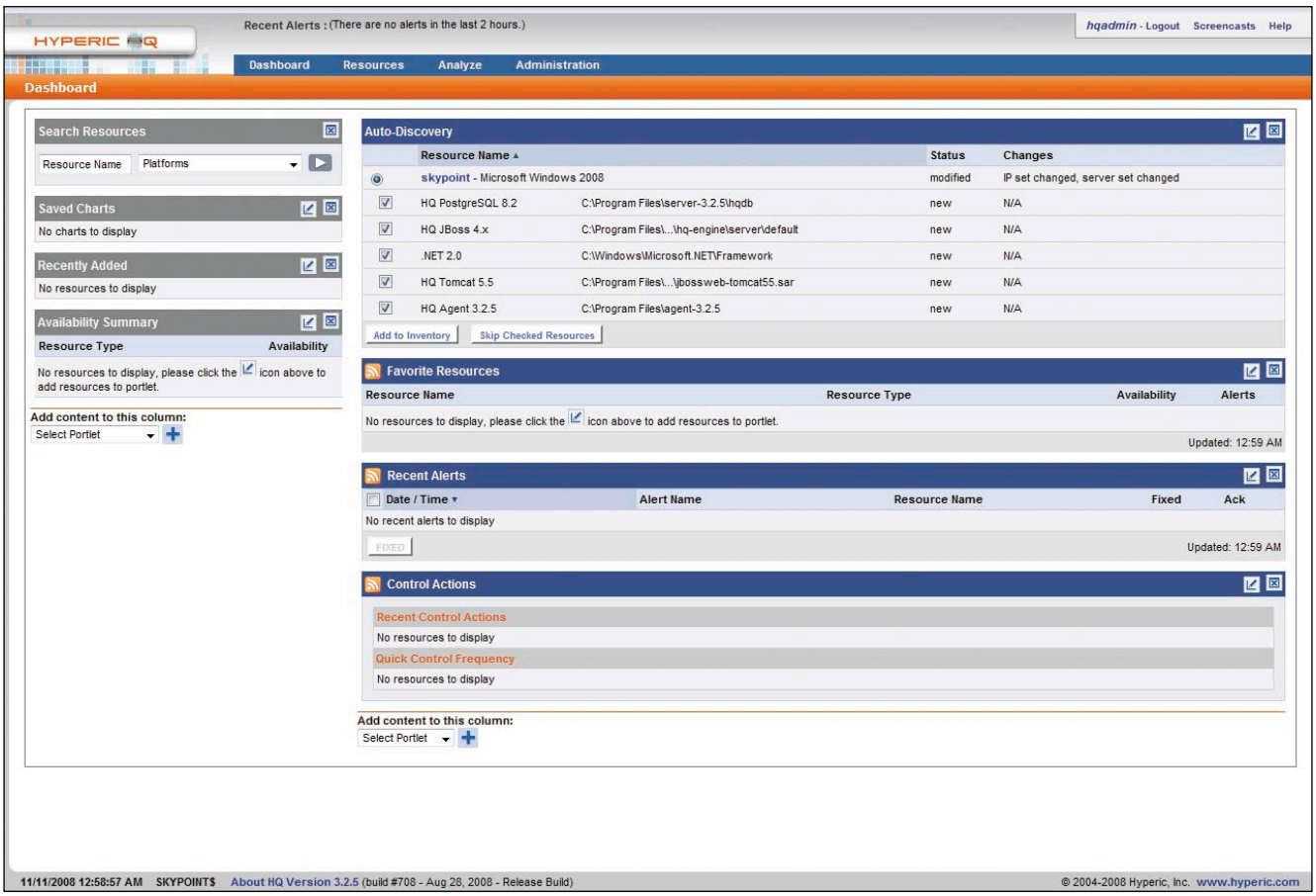


Рисунок 2. Обобщенная информация о ресурсах

та, по умолчанию это опять все тот же C:\Program Files. На этом вопросы заканчиваются, и начинается установка сервера, агента и встроенной базы данных. Если установка остановится на Starting built-in database... то нажмите <Enter> для продолжения. По завершении установки инсталляционный скрип сообщит вам об удачной установке.

Следующим шагом инсталляции будет установка сервера, в качестве службы Windows. Для этого проследуйте в директорию C:\Program Files\server-x.x.x\bin, где x.x.x номер версии, и запустите оттуда файл hq-server.exe с ключом -i. После чего стартует сервис из оснастки «Управление компьютером → Службы». Заметьте, что вместе со службой сервера была также установлена служба Hyperic HQ Database, которая стартует автоматом сразу после запуска сервера.

Далее переходим к агенту. Запуск производится из директории C:\Program Files\agent-x.x.x\bin, где x.x.x номер версии. После старта hq-agent.exe в консоль выводится:

```
Starting agent
- Unable to load agent token file.  Generating a new one ... Done
- Invoking agent
Agent successfully started

[ Running agent setup ]
What is the HQ server IP address:
```

Здесь предлагается ввести IP-адрес сервера, так как серверная часть находится на той же машине, что и агент, то мы пишем 127.0.0.1.

Затем спрашивается, хотим ли мы, чтобы соединение между сервером и агентом было безопасное, – по умолчанию это нет. Включить эту опцию имеет смысл в том случае, если сервер и агент для соединения используют Интернет. В нашем же случае оставляем все как есть и жмем <Enter>.

```
Should Agent communications to HQ always be secure [default=no]:
```

Далее, предлагается ввести номер порта для связи с сервером – по умолчанию это порт 7080. Жмем <Enter> и переходим к следующему пункту.

```
What is the HQ server port     [default=7080]:
```

Следующими двумя пунктами будут запрошены логин и пароль для доступа к серверу – по умолчанию это hqadmin/hqadmin, если вы не изменяли ни то, ни другое, то жмем <Enter> и идем далее.

```
- Testing insecure connection ... Success
What is your HQ login [default=hqadmin]:
What is your HQ password:
```

Теперь определяем IP-адрес и порт, которые сервер будет использовать для связи с агентом, здесь также все оставляем по умолчанию.

```
What IP should HQ use to contact the agent [default=127.0.0.1]:
What port should HQ use to contact the agent [default=2144]:
```

Если инсталляция прошла успешно, вы должны увидеть следующее:

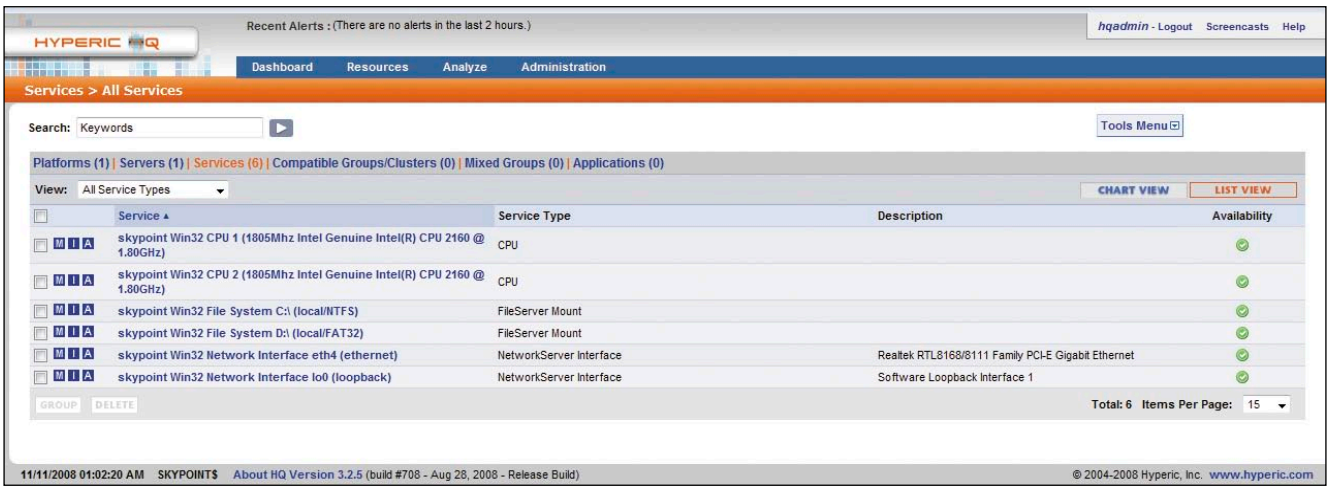


Рисунок 3. Наши сервисы

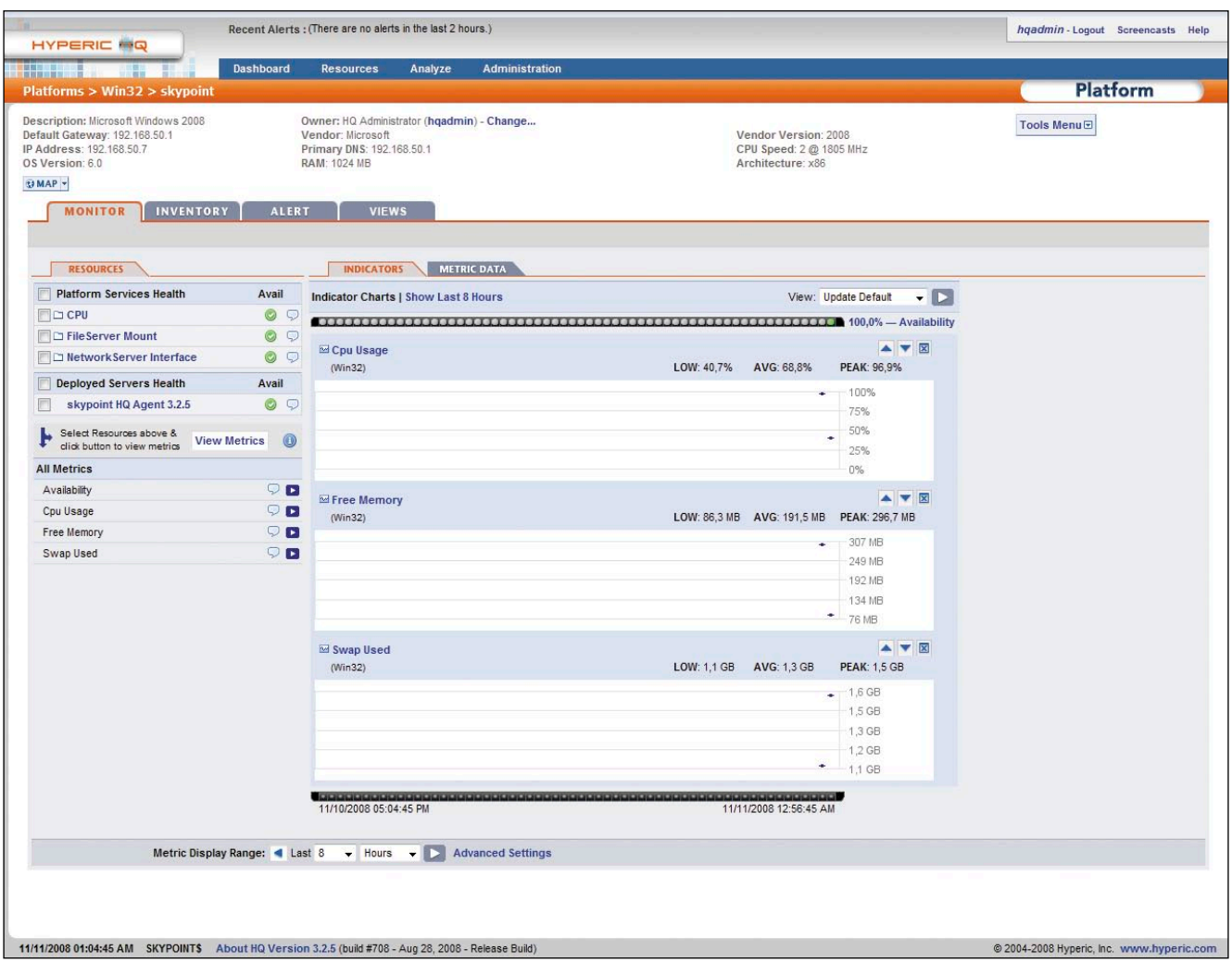


Рисунок 4. Индикаторы метрик

```
- Received temporary auth token from agent
- Registering agent with HQ
- HQ gave us the following agent token
    1104817706987-8534327776788402831-4021000845020676153
- Informing agent of new HQ server
- Validating
- Successfully setup agent
```

Вся установка агента завершена успешно. Для того чтобы агент выполнялся в качестве службы, запускаем его, так же как и сервер с ключом -i, и стартуем сервис. Установка агента и сервера под Linux производится путем запуска установочного скрипта setup.sh и никаких затруднений вызывать не должна. После установки запускаем сервер /home/hyperic/bin/hq-server.sh start и агент /home/hyperic/bin/hq-agent.sh start. Все вопросы, выводимые в консоль, полностью идентичны тем, что выводятся при запуске сервера и агента в Windows.

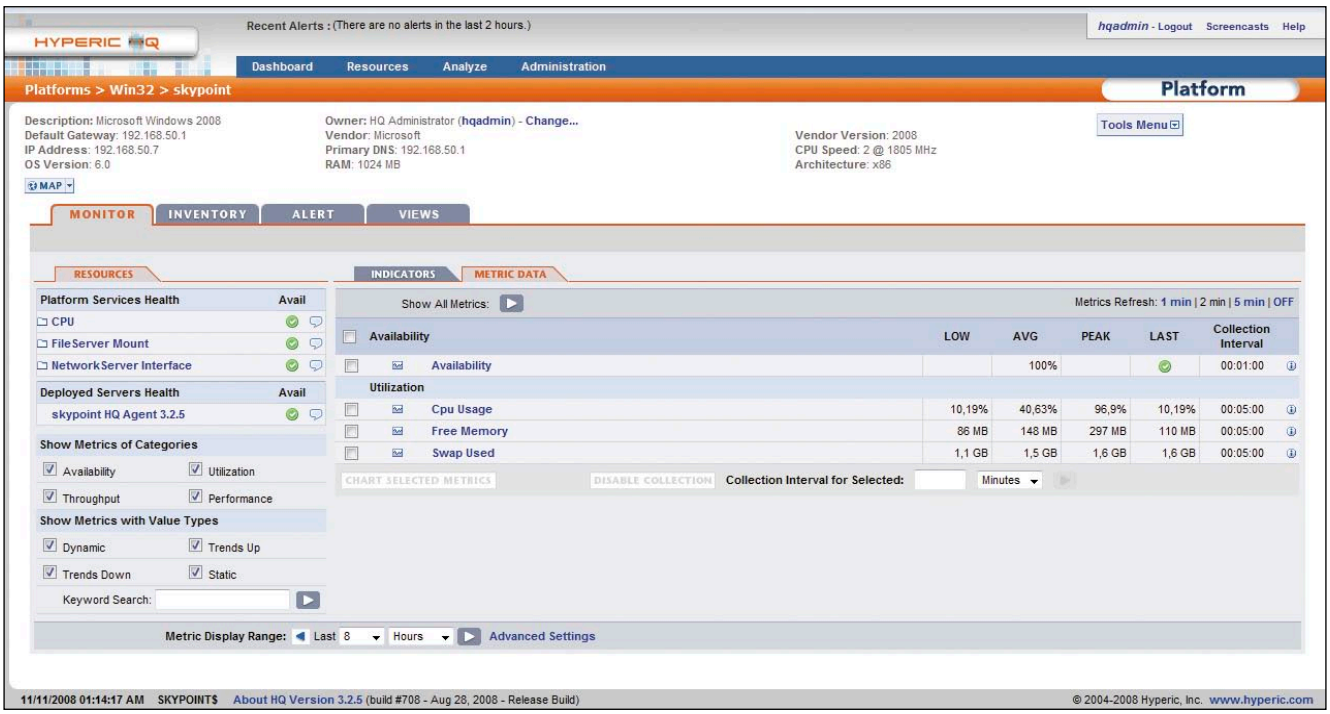


Рисунок 5. Данные метрик

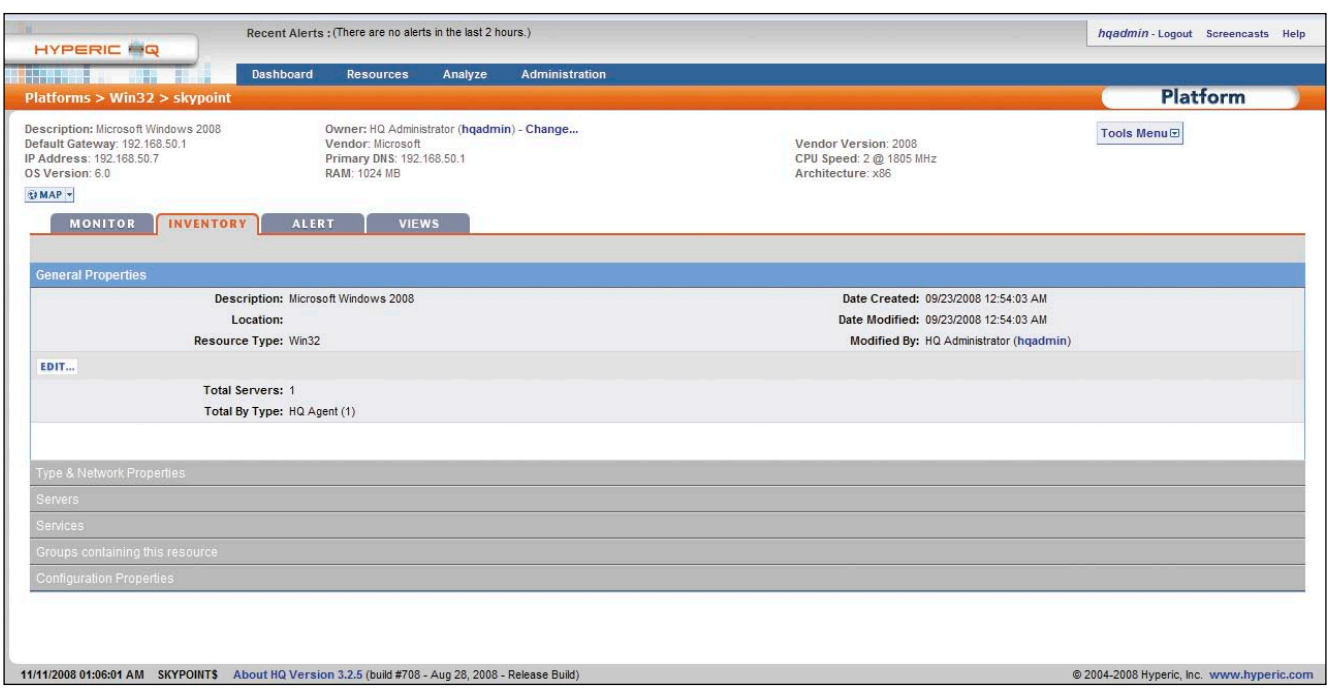


Рисунок 6. Опись данных о ресурсе. Вкладка Inventory

Работа с программой

После того как сервер и клиент установлены и сконфигурированы, можно переходить к проверке работоспособности и настройке программы. Для контроля и анализа полученных сервером данных, а также оповещения об интересующих нас событиях, программа имеет весьма удобный веб-интерфейс. Если вы не меняли номер порта при установке, то он доступен на порту 7080, поэтому набираем в адресной строке вашего любимого браузера your _ip:7080 и попадаем на страницу авторизации, по умолчанию логин/пароль для доступа к серверу hqadmin/ hqadmin, после регистрации на сервере в целях безопасности рекомендуется сразу же сменить пароль – это можно сделать в разделе Administration веб-интерфейса.

При успешной регистрации вы попадете на стартовую страницу Dashboard (см. **рис. 2**), здесь собрана вся основная информация о работе системы, избранные ресурсы, недавние оповещения и тому подобные вещи, позволяющие видеть картину происходящего в целом. На данный момент нас интересует раздел Auto-Discovery – это автообнаружение сервисов. Если при инсталляции вы выбрали установку агента, и он у вас запущен и нормально функционирует, то вы увидите, что компьютер, на котором установлен агент, в нашем слу-

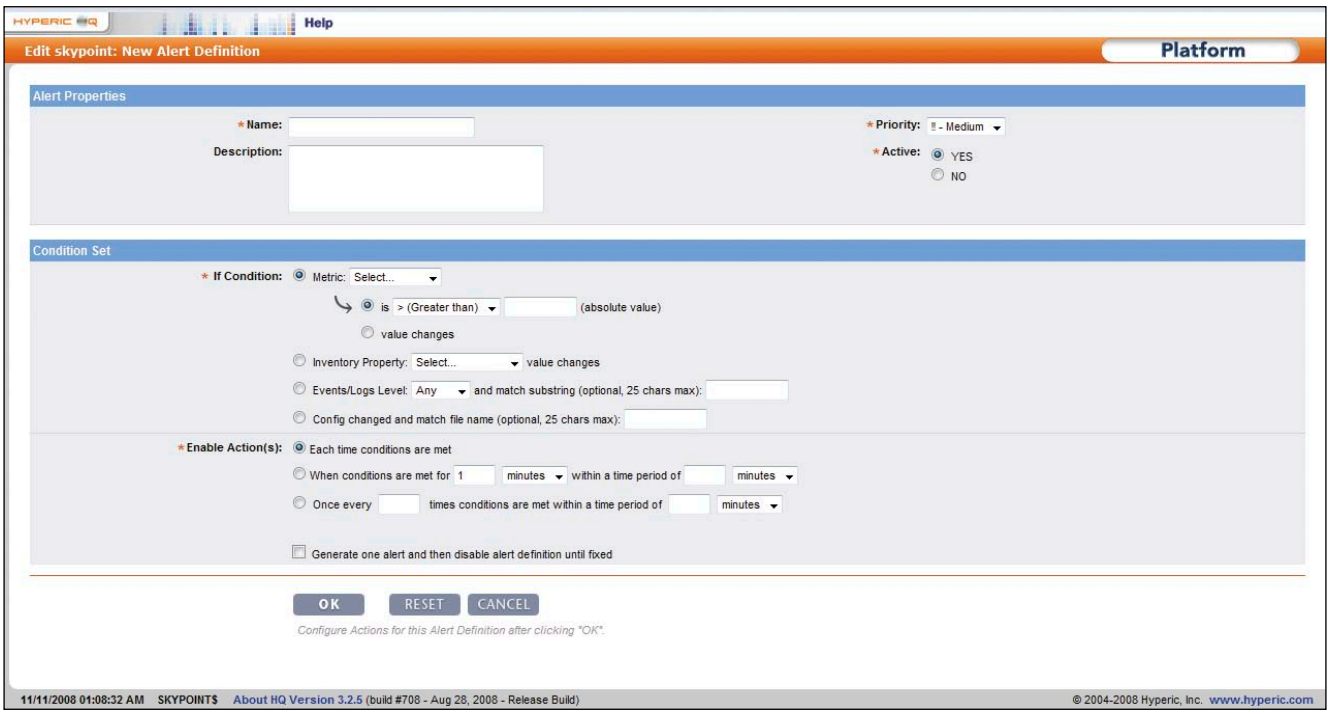


Рисунок 7. Страница создания оповещений

чае, это тот же компьютер, на котором установлен сервер, то он появился в списке вместе с перечнем ресурсов для мониторинга. Ставим галочки напротив тех сервисов, которые желаем контролировать, и жмем Add to Inventory – все наши ресурсы добавлены в опись сервисов.

Теперь посмотрим, что у нас получилось. Переходим через главное меню на вкладку «Resource → Browser» (см. **рис. 3**). Здесь мы видим уже знакомые нам из описанной выше архитектуры системы разделы. В разделе Platforms отображается наша платформа, пока она у нас одна. В разделе Servers – наши серверы, среди которых виден и наш агент, согласно архитектуре системы агент, также является сервером. В разделе Services находятся наши сервисы, которые в данный момент мониторятся системой. Также имеются разделы Compatible Groups/Clusters, Mixed Groups и Applications, которые мы можем создать при необходимости через Tools Menu, расположенные в верхнем левом углу. Просмотр списков ресурсов может осуществляться двумя способами: по умолчанию – это List View, т.е. простой список, либо Chart View – каждый пункт отображается с миниатюрами графиков и цветовым представлением доступности сервиса. Переключение между режимами просмотра осуществляется одноименными кнопками, расположенными в верхнем правом углу списка.

Теперь, если мы в разделе Platforms нажмем на нашу, пока что единственную платформу, то попадем в раздел текущего состояния ресурсов. Так можно сделать, нажав на любой из имеющихся ресурсов, будь то платформа, сервер или сервис. Но мы начнем с платформы, так как она является самым нижним уровнем абстракции в архитектуре системы. Итак, здесь сверху мы видим краткую информацию о конфигурации нашей платформы: операционная система, параметры сети, количество оперативной памяти, тип процессора. Ниже несколько вкладок, в нашем случае их четыре, в зависимости от того, что открыто, их может быть разное количество. Первая вкладка Monitor (см. **рис. 4**), в левой колонке Resources – список сервисов и серверов, находящихся на данной платформе. Середина страницы разделена на две вкладки, первая Indicators, здесь расположены индикатор доступности, ниже отображаются графики метрик, обычно это загрузка процессора, использование оперативной памяти, это опять же зависит от того, что открыто, и еще ниже индикатор отслеживания событий. Во вкладке Metric Data (см. **рис. 5**) мы видим все то же самое, только в виде таблицы с отображением минимального, среднего, пикового значений, также показатели доступности и интервал обновления данных.

Теперь, чтобы описание системы не сводилось к сухому описанию вкладок, давайте здесь мы перейдем к практике, и для наибольшей понятности и наглядности создадим сервис. Итак, перейдем на вкладку Inventory (см. **рис. 6**), здесь в разделе Services отображаются сервисы, относящиеся непосредственно к нашей платформе. Жмем кнопу NEW и попадаем на страницу создания нового сервиса. Тут пишем имя создаваемого сервиса, при желании его описание, и ниже выбираем тип. Для примера давайте создадим сервис, контролирующий состояние службы Windows «Диспетчер печати», выберем Windows Service и нажмем OK. Далее, в разделе Configuration Properties жмем кнопку Edit и в поле service_name вписываем реальное имя службы, в нашем случае это Spooler, жмем OK. Все, сервис создан, теперь, перейдя на вкладку Monitor, мы можем отслеживать состояние нашей службы.

Имея данные о доступности службы и используемых ей ресурсов, мы можем на основании этого строить систему оповещения. Например, мы хотим получить оповещение, если наша служба Spooler стала недоступ-

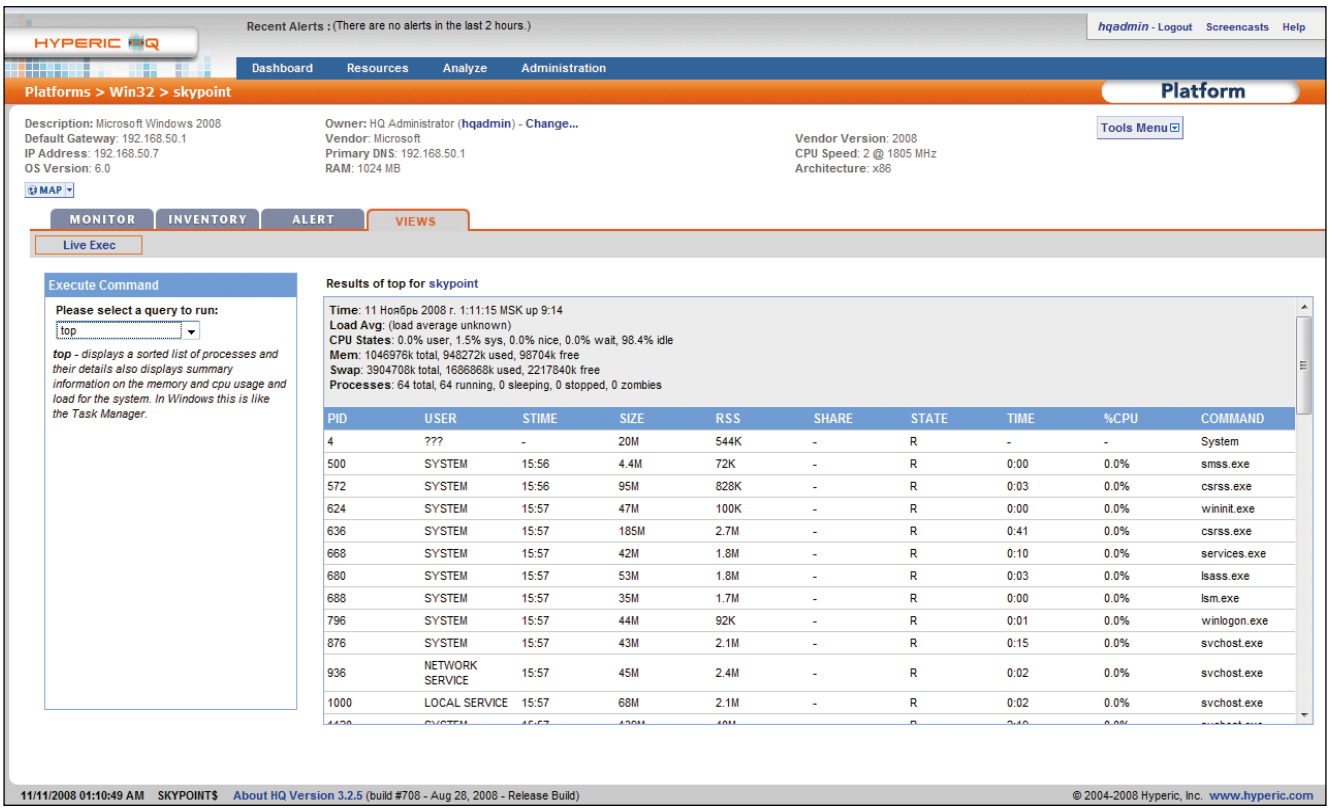


Рисунок 8. Просмотр информации о системе

на. Для создания оповещения переходим во вкладку Alert и жмем NEW (см. **рис. 7**), задаем имя и описание в соответствующих полях. Ниже в Condition Set задаем наше условие. Выбираем метрику Availability и условие «is !=(Not Equal to) 100%», то есть доступность службы не равна 100%, и жмем OK. После нажатия кнопки OK мы попадаем на страницу нашего оповещения, здесь внизу мы можем задать схему эскалации оповещения, что бывает удобно для некоторых событий, схемы эскалации можно создавать в разделе Administration главного меню, а также кому будут отправлять оповещения. Оповещения можно отправлять пользователям, которые имеются в системе, – вкладка Notify HQ Users, а также на произвольно заданные почтовые ящики – вкладка Notify Other Recipients. Ну вот теперь, если остановить службу «Диспетчер печати» , вы получите оповещение об этом на свой почтовый ящик.

Понятие о том, как создавать оповещения, мы получили, теперь переходим к следующей вкладке. Вкладка Control имеется не везде, но в нашем случае она есть, здесь можно производить какие-либо действия над контролируемым объектом, в нашем случае это служба Windows, и мы можем произвести над ней действия Start, Stop и Restart прямо через веб-интерфейс. Также можем посмотреть историю выполняемых действий в подвкладке History.

Следующая вкладка Views, но, перейдя на нее, вам сообщат, что для данного ресурса элементы просмотра отсутствуют. В этой вкладке доступны для просмотра данные в реальном режиме времени, поступающие с платформы, поэтому при помощи меню Map, расположенного в верхнем левом углу экрана, переходим к нашей Win32 platform. Там появилась кнопка Live Exec (см. **рис. 8**), нажав на нее, мы переходим к экрану просмотра. Слева есть выпадающее меню, в котором доступна для выбора информация о центральном процессоре и его использовании, информация о файловой системе, информация о статистике и конфигурации сети, а также процессы, запущенные в системе, и информация о залогинившихся пользователях.

Следующий раздел интерфейса Analyze содержит в себе два инструмента, предназначенные для просмотра и анализа оповещений Alert Center и событий Event Center. Они могут быть полезны, если вам необходимо просмотреть какие-либо события или оповещения, отфильтровав их в разрезе каких-либо критериев.

В последнем разделе Administration предоставляется возможность управления пользователями системы, схемами эскалации, а также настройками самой системы и платинами.

Заключение

Данная система, конечно, в первую очередь предназначена для крупных компаний, таких как дата-центры и хост провайдеры, система может применяться в гетерогенных сетях, осуществляет сбор данных по SNMP, поддерживает мониторинг виртуальных машин, таких как VMware или Xen, имеется возможность кластеризации. Для небольших компаний она менее пригодна, ввиду того, что для своей работы требует достаточно больших вычислительных мощностей, и как следствие выделение под себя отдельного сервера, что не всем по карману, в любом случае выбор за вами.

Удачи!

1. Сайт проекта Hyperic HQ – http://www.hyperic.com.
2. Сайт проекта RHQ-Project – http://www.rhq-project.org.

Mandriva

LINBOX RESCUE SERVER

LINBOX RESCUE SERVER: полный контроль за ИТ-инфраструктурой

Linbox Rescue Server (LRS) это пакет программ, предоставляющий все функции надлежащего локального или удаленного управления ИТ системой. Он может быть использован как в одном подразделении, так и в десятках, размещая, контролируя и исправляя все (в основном Windows и GNU/Linux) компьютеры в сетях LAN и WAN. LRS может установлен на машину с GNU/Linux с любой поддерживаемой локальной сетью. Администратор может управлять через Веб-браузер с любого локального или удаленного компьютера. Он использует систему загрузки PXE и не требует установки специализированного клиентского ПО на машины.

• Легкость администрирования за счет использования единой мультифункциональной Веб-консоли. Использование зашифрованного туннеля и системы авторизации гарантирует контроль и конфиденциальность передачи через локальную или глобальную сеть.

• Резервирование и восстановление систем с Windows или GNU/Linux за несколько минут (примерно 10-15 минут для Windows+Office XP). Резервирование системы ведется в виде полного образа на жестком диске, который содержит операционную систему, программное обеспечение и параметры. Единственный образ (master) может быть использован для множества ПК, благодаря пост-инсталяционным особенностям (например введение компьютеров с Windows в домен). Вы можете выбрать какие разделы вы хотите резервировать или восстановить. Копия может быть сохранена на жестком диске, CD или DVD.

• Резервирование и восстановление файлов пользователей как под Windows и GNU/Linux, так и под Unix. Инкрементные или полные резервные копии автоматически сохраняются на жестких дисках и/или лентах для любых созданных или модифицированных файлов с заданной частотой. Как правило вы можете сохранить непрерывные копии за 30 дней на дисках сервера LRS. Система сжатия и различные функциональные особенности снижают объем требуемого места для сохранения данных до 1/3 от исходного. Восстановление очень легко и требует всего лишь нескольких кликов в Веб-интерфейсе.

• Полный учет программного обеспечения и оборудования. Сервер осуществляет полную опись машин и их окружения для всех подключенных компьютеров 24 часа в сутки: Опись оборудования (процессор, карт, памяти жесткого диска, числа дисков...), переферии (принтеры, сканеры и т.п.) а также программного обеспечения (тип, версия, редакция и т.п.) и сетевой информации (IP адреса, выходы и т.п.). Администратор может получить предупреждение по электронной почте при изменениях между двумя сессиями учета.

• Удаленные контроль за клиентскими ПК. Администратор может воспользоваться безопасным доступом к клиентской машине (через ssh туннель в случае необходимости), после его приглашения пользователем.

Автоматическая установка драйверов

Иван Коробко

Решить задачу пакетной установки драйверов можно разными способами. Среди них наиболее распространенный – интеграция в дистрибутив операционной системы, однако он не единственный. Поговорим о малоизвестных способах пакетной установки драйверов.

В крупных организациях парк компьютеров, как правило, унифицирован. Однако он постоянно обновляется. Самый распространенный из них – интеграция пакета драйверов в дистрибутив операционной системы. Существует еще несколько альтернативных способов, которым стоит уделить внимание: установка пакета драйверов с помощью командного файла и с помощью Driver Package Installer.

Довольно часто возникает ситуация, когда необходимо предустановить пакет драйверов. В целях безопасности большинство сотрудников в сети не обладают административными правами и не могут устанавливать устройства. По этой причине они не могут подключить без помощи администратора различные внешние устройства с интерфейсом USB, Fire Ware и т. д.

Для решения этой проблемы необходимо инсталлировать часто используемые драйверы на всех компьютерах на этапе разворачивания программного обеспечения.

Для обеспечения автоматической пакетной установки драйверов можно использовать либо командный файл, либо Driver Package Installer (DPInst). Рассмотрим подробнее два способа.

Командный файл

Алгоритм установки драйверов устройств описан в INF-файле. В нем находится информация о том, какие библиотеки и куда необходимо скопировать, какие изменения сделать в реестре и т. д.

В Windows используется два интерпретатора INF-файлов: SETUPAPI и ADVANCEDINF, которые представляют собой два DLL-файла, располагающихся в каталоге %SystemRoot%/System32.

Интерпретатор SETUPAPI находится в библиотечном файле setupapi.dll, интерпретатор ADVANCEDINF – в библиотечном файле advpack.dll. Основным интерпретатором является SETUPAPI. Для получения доступа к интерпретаторам используется запускаемый файл RUNDLL32.EXE. Формат запуска любой библиотеки следующий:

```
rundll32.exe DLL,Function Parameters
```

где:

- **DLL** – имя файла библиотеки. В данном случае setupapi.dll или advpack.dll.
- **Function** – функция, вызываемая из библиотеки, или, как ее еще называют, точка входа. Обратите вни-

мание: название файла и вызываемой функции разделены запятой без пробелов.
- **Parameters** – параметры, передаваемые функции.

Интерпретатор SETUPAPI

Интерпретатор SETUPAPI позволяет:
- управлять реестром: создание и удаление ключей, параметров и их значений;
- распаковывать CAB-файлы;
- управлять файлами и папками, их атрибутами;
- устанавливать и удалять драйверы устройств.

Для запуска процесса установки драйверов используется функция InstallHinfSection, для удаления – соответственно unInstallHinfSection. В **листинге 1** приведен пример установки драйверов, описанных в файле HP_1200.INF.

Листинг 1. Установка драйверов с помощью интерпретатора SETUPAPI

```
rundll32.exe setupapi,InstallHinfSection HP_1200_PPD 132 ↵
     C:\HP_1200.INF
```

Функция InstallHinfSection имеет три параметра. Первый из них – имя выполняемой секции INF-файла, второй – флаг обработки файла. В **таблице** приведены возможные значения флага. Третий параметр – непосредственно имя INF-файла.

Интерпретатор ADVANCEDINF

По своей сути интерпретатор ADVANCEDINF является надстройкой над SETUPAPI, позволяющей выполнять дополнительно следующие функции:
- однократное выполнение доустановки после входа в систему при инсталляции и деинсталляции (Active Setup);
- предварительная запись изменяемых ключей реестра в бинарный файл (функция отката);
- запуск исполняемых файлов с параметрами в скрытом и нормальном режимах;
- вывод диалоговых окон.

Стандартные функции ADVANCEDINF передает на исполнение интерпретатору SETUPAPI.

В **листинге 2** приведен аналогичный пример установки PostScript драйвера принтера HP 1200. Несмотря на то что в функции использованы те же три параметра, их порядок изменился. Первый параметр – имя INF-файла, второй – название секции, третий – флаг обработки файла (см. **таблицу**).

Листинг 2. Установка драйверов с помощью интерпретатора SETUPAPI

```
rundll32.exe advpack,LaunchINFSection ↵
     C:\HP_1200.INF HP_1200_PPD 132
```

Вывод

Бесспорным преимуществом является интегрированность обоих интерпретаторов, используемых в командных файлах, в операционную систему, однако при этом необходимо точно указывать местонахождение драйвера и секцию INF-файла, служащую его точкой входа. Для этого администратор должен разбираться в синтаксисе.

Driver Package Installer

Driver Package Installer (DPInst) – компонент, разработанный компанией Microsoft, входящий в состав пакета Microsoft Windows Driver Install Frameworks (DIF). В настоящее время используется DIF v 2.1. DPInst обладает возможностями:
- Установка Plug and Play (PnP) драйверов. По умолчанию устанавливаются все подписанные PnP-драйверы, находящиеся в каталоге с файлом dpinst.exe. Для отключения проверки используется ключ /LM.
- Пакетная установка драйверов с помощью файла dpinst.xml. Описание структуры XML-файла см. далее.
- Поддержка «тихого» режима установки. Для включения режима используется ключ /S или /Q.
- Поддержка многоязычного интерфейса установщика драйверов.
- Ведение журнала установки.
- Деинсталляция драйверов.

Из перечисленных возможностей видно, что с помощью DPInst можно реализовать автоматическую установку группы драйверов в «тихом» режиме. По умолчанию DPInst устанавливает в системе все драйверы, INF-файлы которых находятся в одном каталоге с этой утилитой, однако устраивать помойку из драйверов по меньшей мере некорректно. Для решения этой проблемы используется DPInst.XML, находящийся в одном каталоге с DPInst.EXE. Он представляет собой обычный текстовый файл в формате XML. Единственное его отличие от других файлов – наличие стандартизированных тегов.

Установка пакета драйверов

Существует два способа пакетной установки: с помощью тега <group> и <search>. Принципиальная разница между этими способами заключается в том, что с помощью тега <group> реализована установка драйверов, местоположение которых точно указано. Используя тег <search>, можно установить все драйверы в указанной и ее дочерних папках. Рассмотрим подробнее оба способа.

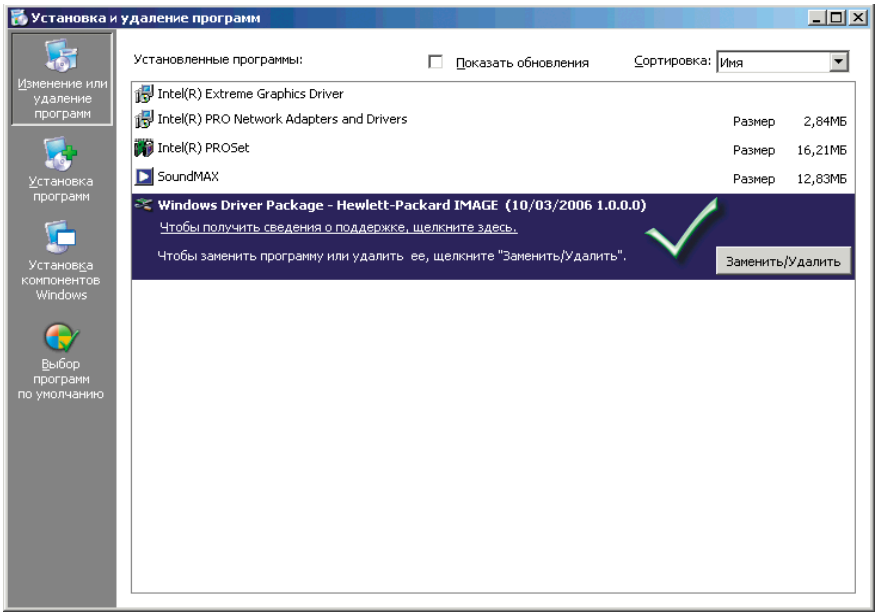
Пакетная установка драйверов с помощью тега <group>

Для обеспечения установки пакета драйверов в файле DPInst.XML используется тег <group>, в котором может быть три типа дочерних тегов:
- **<package path = «…»/>** – таких тегов может быть неограниченное количество. Значение параметра path – относительный или абсолютный путь к INF-файлу драйвера.

Возможные флаговые значения обработки файлов

Значение	Описание
0 или 128	Не перезагружать компьютер
1 или 129	Перезагрузка компьютера без запроса
2 или 130	Спросить у пользователя: перезагрузить компьютер или нет
3 или 131	В случае необходимости перезагружать компьютер без запроса
4 или 132	В случае необходимости спросить у пользователя: перезагружать компьютер или нет

- **<installAllOrNone/>** – в случае ошибки установки одного из драйверов осуществляется деинсталляция всех драйверов данного пакета. Этот тег по действию аналогичен ключу /A утилиты DPInst.exe.
- **<suppressAddRemovePrograms/>** – при наличии этого параметра мастером установки не будет создаваться соответствующая запись для каждого драйвера в папке «Установка и удаление программ», находящейся в «Панели управления» (см. **рисунок**). Этот тэг по действию аналогичен ключу /SA утилиты DPInst.exe.



Регистрация драйвера в «Установка и удаление программ»

Для автоматической установки пакета драйверов, состоящего из трех драйверов, находящихся в папках C:\hp1200\1200.inf, C:\hp3380\3380.inf, C:\hp4100\4100.inf, рекомендуется использовать XML-файл, приведенный в **листинге 3**.

Листинг 3. XML-файл, для автоматической установки

```
<?xml version="1.0" ?>
<dpinst>
   <group>
      <package path="c:\hp1200\1200.inf " />
      <package path="c:\hp3380\3380.inf " />
      <package path="c:\hp4100\4100.inf " />
   <group/>
</dpinst>
```

Для обеспечения автоматической установки рекомендуется для запуска утилиты DPInst.exe использовать два ключа, включающих тихий режим установки (/S) и позволяющих устанавливать неподписанные драйверы (/LM):

```
DPInst .exe / S /LM
```

Пакетная установка драйверов с помощью тега <search>

Для пакетной установки драйверов на практике используется более быстрый способ, реализованный с помощью тега <search>. Его преимущество, которое в определенной ситуации является серьезным недостатком, – инсталляция всех найденных драйверов в указанном месте (**листинг 4**).

Листинг 4. Установка найденных драйверов в подпапках

```
<search>
    <subDirectory>*</subDirectory>
 </search>
```

Установка пакета драйверов с использованием интерфейса

Утилиты DPInst.exe поддерживает многоязычный интерфейс. Текст всех диалоговых окон, лицензионное соглашение и другая информация могут быть переведены разработчиком драйверов или администратором. Рассмотрим этот вопрос подробнее на примере создания русскоязычного интерфейса. Для описания интерфейса служит тэг <language>. С помощью параметра code задается кодовая страница, например, 0x0409 соответствует английскому языку, а 0x0419 – русскому (**листинг 5**).

Листинг 5. Шаблон файла DPInst.XML

```
<dpinst>
       <language code="0x0419">
                    ...
        </language>
       <group>
                ...
       <group/>
</dpinst>
```

В тэге <language> могут быть приведены различные элементы, которые логически можно разделить на две группы. К первой группе отнесем те из них, которые управляют интерфейсом основного диалогового окна инсталлятора, ко второй – управляющие интерфейсом лицензионного соглашения. Поскольку перед системным администратором обычно стоит задача реализовать «тихую» установку, то ограничимся упоминанием о поддержке многоязычного интерфейса. Полное описание всех тегов находится в MSDN.

Вывод

Driver Package Installer имеет неоспоримые преимущества перед установкой драйверов с помощью командного файла благодаря реализованной возможности автоматического поиска драйверов в указанном месте. При этом за один заход можно установить в систему неограниченное количество драйверов.

Заключение

В заключение, хочется сказать несколько слов в защиту командных файлов. Достаточно часто встречаются ситуации, когда все способы перепробованы, но по тем или иным причинам достичь желаемого результата не удалось, тогда приходят на выручку такие способы, как установка драйверов с помощью командного файла.

Спуфинг атака в ISC BIND

Программа: BIND 9.0 все версии; BIND 9.1 все версии; BIND 9.2 все версии; BIND 9.3.0, 9.3.1, 9.3.2, 9.3.3, 9.3.4, 9.3.5, 9.3.6; BIND 9.4.0, 9.4.1, 9.4.2, 9.4.3; BIND 9.5.0, 9.5.1; BIND 9.6.0.

Опасность: Низкая.

Описание: Уязвимость существует из-за того, что некоторые функции ISC BIND некорректно проверяют данные, возвращаемые OpenSSL-функциями EVP_VerifyFinal() и DSA_do_verify(), при проверке подлинности DSA- и NSEC3DSA-ключей. Удаленный пользователь может подменить ответы от зон, использующих DSA- или NSEC3DSA-ключи. Для успешной эксплуатации уязвимости зона должна использовать DSA- или NSEC3DSA-алгоритмы.

URL производителя: www.isc.org/software/bind.

Решение: Установите последнюю версию 9.3.6-P1, 9.4.3-P1, 9.5.1-P1 или 9.6.0-P1 с сайта производителя. В качестве временного решения производитель рекомендует запретить использование DSA- и NSEC3DSA-алгоритмов.

Множественные уязвимости в Trillian

Программа: Trillian версии до 3.1.12.0.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за ошибки при генерации XML-тегов для изображений. Удаленный пользователь может с помощью специально сформированного имени графического изображения вызвать переполнение стека и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки при обработке XML-кода. Удаленный пользователь может вызвать повреждение памяти и выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за ошибки проверки границ данных при обработке XML-тегов. Удаленный пользователь может вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

URL производителя: www.ceruleanstudios.com.

Решение: Установите последнюю версию 3.1.12.0 с сайта производителя.

Уязвимость при обработке ответов в Symantec Mail Security for SMTP

Программа: Symantec Mail Security for SMTP 5.0.1 с исправлением 189, возможно, другие версии.

Опасность: Низкая.

Описание: Уязвимость существует из-за ошибки при обработке неудачной доставки писем. Удаленный пользователь может вызвать доставку email-сообщения на специально сформированный сервер, вернуть приложению специально сформированный ответ. Удачная эксплуатация уязвимости позволит злоумышленнику постоянно завершать работу службы Filter Hub, что не позволит дальнейшую обработку писем.

URL производителя: www.symantec.com/enterprise/products/overview.jsp?pcid=1008&pvid=845_1.

Решение: Установите исправление 200 для версии 5.0.1 с сайта производителя.

Переполнение буфера в SAP GUI TabOne ActiveX-компоненте

Программа: SAP GUI 6.40 Patch 29, возможно, другие версии; SAP GUI 7.10, возможно, другие версии.

Опасность: Высокая.

Описание: Уязвимость существует из-за ошибки проверки границ данных в TabOne ActiveX-компоненте (sizerone.ocx) при копировании заголовков вкладок. Удаленный пользователь может с помощью метода AddTab() добавить большое количество вкладок, вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

URL производителя: www.sap.com.

Решение: Установите последнюю версию 7.10 PL с сайта производителя, которая отключает уязвимый ActiveX-компонент.

Целочисленное переполнение в BitDefender Antivirus Scanner for Unices

Программа: BitDefender Antivirus Scanner for Unices 7.60825 и более ранние версии.

Опасность: Высокая.

Описание: Целочисленное переполнение существует при обработке некоторых PE-файлов, собранных с помощью NeoLite или ASProtect. Удаленный пользователь может с помощью специально сформированного PE-файла выполнить произвольный код на целевой системе.

URL производителя: www.bitdefender.com/PRODUCT-80-en-BitDefender-Antivirus-Scanner-for-Unices.html.

Решение: Установите исправление с сайта производителя.

Отказ в обслуживании в Sun Solaris

Программа: Sun Solaris 10.

Опасность: Средняя.

Описание: Уязвимость существует из-за неизвестной ошибки в IPv4-перенаправлении. Удаленный пользователь может вызвать панику ядра системы. Для успешной эксплуатации уязвимости на системе должен использоваться IPv4, должен присутствовать маршрут через адрес 127.0.0.1 без флага blackhole и должно быть установлено исправление 120011-14 (SPARC) или 120012-14 (x86).

URL производителя: www.sun.com.

Решение: Установите исправление с сайта производителя.

Отказ в обслуживании в ClamAV

Программа: ClamAV версии до 0.94.2.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки бесконечной рекурсии в функции cli_check_jpeg_exploit() в файле libclamav/special.c. Удаленный пользователь может с помощью специально сформированного JPEG-изображения вызвать переполнение стека и аварийно завершить работу приложения.

URL производителя: www.clamav.net.

Решение: Установите последнюю версию 0.94.2 с сайта производителя.

Составил Александр Антипов

Вы еще не используете Windows Vista?

Андрей Бирюков

Основные возможности и нововведения операционной системы.

Прошло уже почти два года со времени выхода операционной системы Windows Vista. За это время продукт от Microsoft уже успел наделать много шума на интернет-форумах и в различных печатных изданиях. Одни пользователи отчаянно ругают эту операционную систему, другие восхищаются. Попробуем разобраться в том, что же такое Windows Vista.

Вашему вниманию предлагается цикл статей, посвященных различным возможностям Vista. В этой статье я расскажу об основных новшествах данной операционной системы и опишу ее установку и базовую настройку.

Прежде всего поговорим о существующих редакциях Windows Vista. Их довольно много, поэтому новичку может оказаться непросто в них разобраться (см. **таблицу**). Пусть вас не пугает присутствие новых названий в таблице, о том, что они означают, мы поговорим позднее.

Кроме приведенных в **таблице**, по требованиям ЕС в Европе вы можете встретить редакции Home Basic и Business, которые содержат другой набор компонентов, прежде всего мультимедийных.

Как видно из **таблицы**, каждая из редакций имеет свою целевую аудиторию, позволяя не тратить деньги на тот функционал, который вам не требуется. Говоря о возможностях, следует отметить появление новых средств, которые также упоминались в таблице.

Прежде всего это Aero – новый интерфейс, который содержит различные средства визуализации. Например, прозрачные заголовки и границы, плавное сворачивание и разворачивание окон, Flip3D – все это новые графические компоненты, появившиеся в Vista.

Архитектура Aero содержит несколько уровней. Возможность использования каждого из них зависит от характеристик оборудования. Чем мощнее конфигурация компьютера, тем более высокий уровень Aero поддерживается системой. Основных уровня всего два – Windows Basic и Aero (ранее так же известные, как Aero Express и Aero Glass).

Первый уровень содержит эффекты уровня Glass, кроме прозрачности заголовков, Flip3D, и анимированных эффектов при сворачивании/разворачивании окон.

Второй уровень – Aero Glass – обладает всеми ранее перечисленными эффектами. Aero Glass – применение прозрачных (с размывкой заднего плана) заголовков и панелей в окнах в стиле оформления «Windows Aero». Windows Flip – новый вид меню <alt> + <tab>, в котором показываются эскизы открытых окон и их значки. Windows Flip 3D – замена <win> + <tab>, теперь все окна выстраиваются в ряд в 3D. При помощи стрелок клавиатуры или колесика мышки можно прокручивать окна. Клавиша <Enter> или клик мышкой активируют окно стоящее по середине ряда.

Вообще, говоря про Aero, следует заметить, что далеко не все оборудование поддерживает данный интерфейс, о том, как проверить это и попробовать включить, мы поговорим далее в этой статье. На момент написания статьи поддерживалось 203 устройства.

Наилучших результатов можно достигнуть с графическими процессорами следующих конфигураций:

- 64 Мб графической памяти для поддержки монитора с разрешением менее 1 310 720 пикселов (1280x1024);
- 128 Мб графической памяти для поддержки монитора с разрешением от 1 310 720 до 2 304 000 пикселов (1600x1200);
- 256 Мб графической памяти для поддержки монитора с разрешением более 2 304 000 пикселов (2560x1600).

Еще одна новая функция – это Media Center. Фактически это средство для полноценного просмотра не только видео, но и телевидения (при наличии ТВ-тюнера). Здесь сразу возникает вопрос, с какими устройствами работает Vista Media Center. На сайте компании Microsoft есть раздел сертифицированных под Media Center устройств – видеорекордеров и ТВ-тюнеров [1].

Также в таблице упоминалась 64-битная архитектура. Скажу несколько слов о совместимости. 32-битную редакцию можно использовать на 64-битной архитектуре, однако обратное невозможно. Использовать 64-битную редакцию на 32-битной архитектуре вам не удастся. Вообще при планировании установки вы можете воспользоваться статьями и инструментами на странице [2].

Для проверки компьютера на совместимость с Vista вы можете воспользоваться специальным инструментом – Windows Vista Upgrade Advisor, позволяющим проверить машину на совместимость. Данная утилита предназначена для работы с 32-битными архитектурами. Получить ее можно по адресу [3].

Редакции Windows Vista

Редакция	Аппаратные ограничения	Предназначение
Vista Starter	Поддерживается только один 32-битный процессор, нет поддержки Aero, нет шифрования, не поддерживаются входящие соединения, нельзя включать в домен, возможны не более трех одновременных исходящих подключений, нельзя использовать Media Center	Данная редакция позиционируется разработчиками как рабочая платформа для различных веб-киосков и платежных терминалов. Не думаю, что в России получит широкое распространение
Vista Home Basic	Поддерживаются как входящие, так и исходящие соединения, 32-битная архитектура, нельзя включать в домен	Предназначена для домашних компьютеров, на которых не требуются мощные функции по воспроизведению мультимедиа
Vista Home Premium	Аналогично редакции Home Basic, но поддерживает 64-битную архитектуру и Media Center	Эта редакция, по мнению разработчиков, должна стать оптимальной рабочей средой для домашних компьютеров
Vista Business	Схожа с редакцией Home Premium, но нет Media Center, шифрования и есть возможность включения в домен	Операционная система для рабочих станций, не требующих мощных вычислительных нагрузок
Vista Enterprise	Нет только Media Center. Поддерживается 64-битная архитектура	Для продвинутых рабочих станций
Vista Ultimate	Поддерживаются все возможные функции Windows Vista	Для высокопроизводительных рабочих станций, требующих постоянной работы с большими потоками медиаданных

Обратите внимание на то, что для работы Vista Upgrade Advisor вам необходимо установить Microsoft Core XML Services 6.0 и .NET Framework 2.0. Данные компоненты также можно найти на сайте Microsoft.

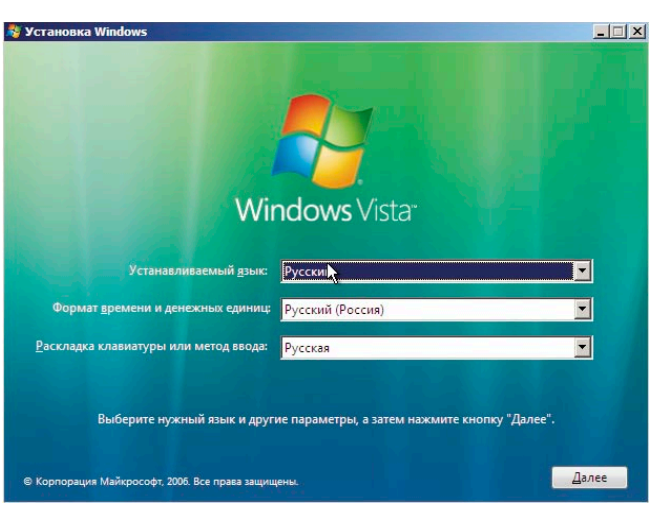
Непосредственно установка

Итак, определившись с редакцией и убедившись в аппаратной совместимости, приступим к установке новой операционной системы. Рассмотрим установку системы на «чистый» раздел. Надо отдать должное разработчикам, они упростили и автоматизировали процесс развертывания. Инсталлятор сначала задает все необходимые вопросы, а затем самостоятельно копирует системные файлы и настройки и перезагружает рабочую станцию. Согласитесь, это новшество весьма полезно в тех случаях, когда приходится выполнять сразу несколько инсталляций.

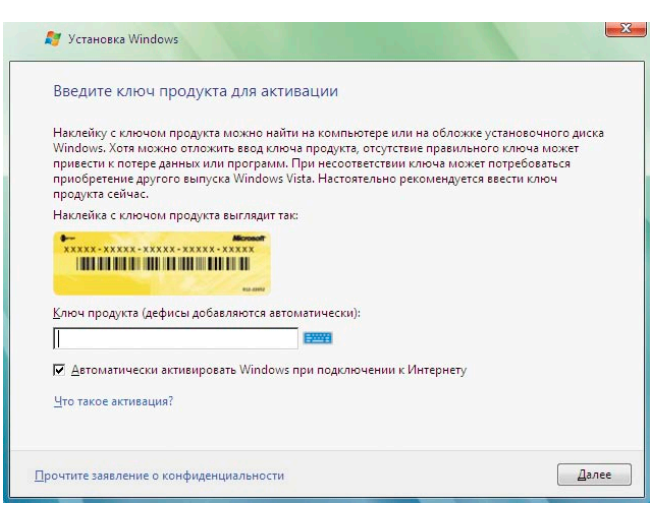
Перед началом установки хочу обратить внимание еще на один небольшой момент, а именно, дистрибутив Vista распространяется на DVD-дисках, поэтому не забудьте убедиться, что во всех рабочих станциях, на которые вы собираетесь устанавливать новую ОС, есть DVD-приводы.

После загрузки с установочного диска на первом шаге у вас спросят язык, формат даты и язык ввода с клавиатуры. Затем вам необходимо указать Product Key, состоящий из 25 символов.

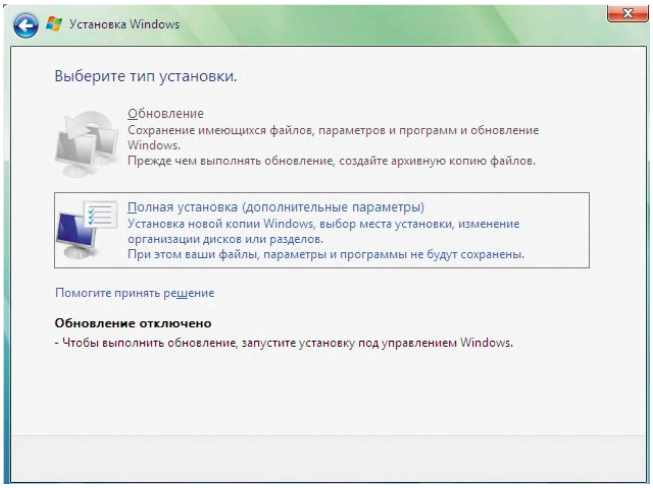
После этого вам будет предложено активировать систему. Я бы рекомендовал отказаться от активации в процессе установки по нескольким причинам. Прежде всего система активации



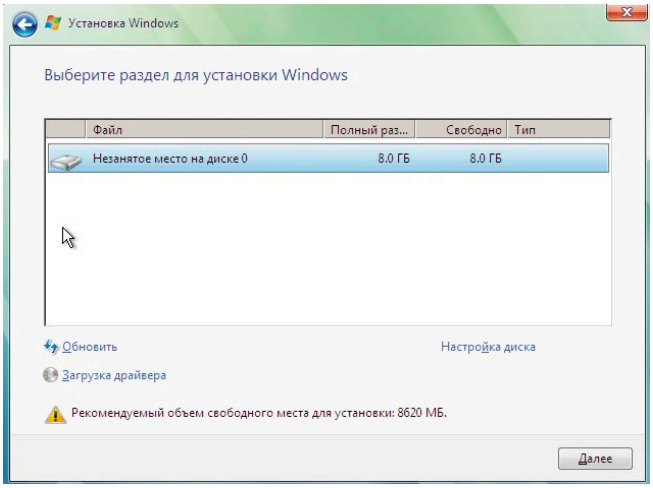
Начало установки Vista



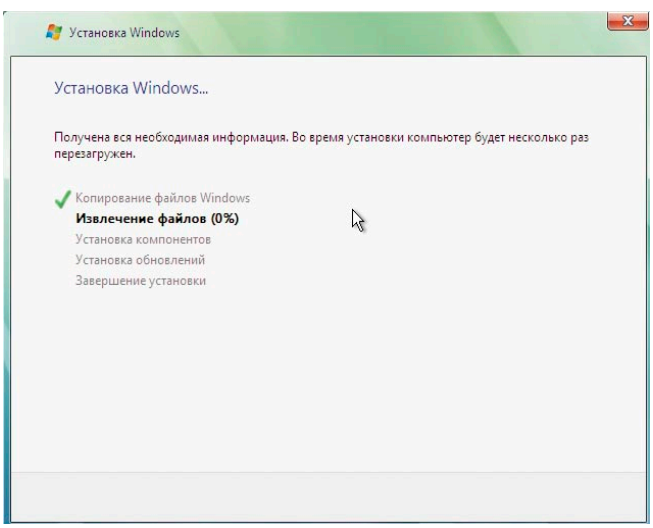
Ключ продукта



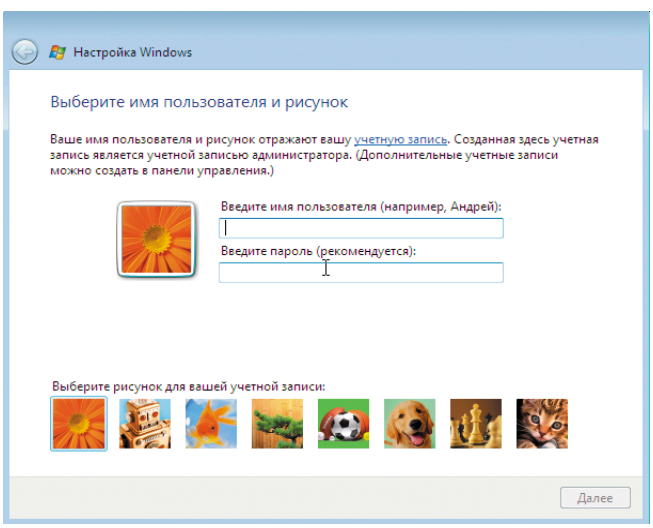
Выбор режима установки



Выбор раздела для установки



Процесс установки



Выбор имени пользователя

позволит вам переустановить систему только один раз, если вам придется переустанавливать ОС более одного раза, то нужно будет связываться со службой поддержки Microsoft, что может занять немало времени. К тому же в случае если после установки какое-либо устройство будет работать некорректно, вполне возможно, что вам придется менять аппаратную конфигурацию (например, материнскую плату), а такие изменения также требуют повторной активации системы. Так что в течение месяца вы можете работать без активации, проверяя работоспособность операционной системы.

На следующем шаге вам необходимо выбрать редакцию. Здесь вы можете выбрать любую редакцию, однако в случае если ваш ключ активации не предназначен для данной редакции, продолжить установку вам не удастся. При необходимости вы можете вернуться назад, чтобы ввести другой ключ.

Далее нужно указать раздел, на который производится установка. Если вы используете RAID-контроллеры или жесткие диски со специфическими драйверами, то на этом шаге вы можете загрузить данные драйвера.

После этого программа установки начнет копирование системных файлов. После этого вам нужно будет указать имя пользователя и пароль, а затем имя компьютера. На следующем шаге вам будет предложено установить обновления. Стоит ли это делать в процессе установки или нет, думаю, каждый системный администратор должен решить самостоятельно, основываясь на собственном опыте установки Vista. К тому же если вы выберете Ask Me Later, то вы сможете позднее использовать в качестве источника обновлений локальный сервер WSUS (Windows Server Update Services), если он у вас развернут, что позволит сэкономить на интернет-трафике.

На следующем шаге вам нужно указать дату и время, а также часовой пояс. И выбрать текущее расположение (Location). Microsoft рекомендует использовать Public Location.

На этом установка системы завершена. Теперь посмотрим на нововведения, появившиеся в Windows Vista. Сразу отмечу, что в этой статье речь пойдет только о новшествах в GUI. Для начала попробуйте включить интерфейс Aero. Прежде всего ваша видеокарта должна соответствовать тем требованиям, которые я приводил ранее в этой статье.

Для запуска выполните следующие несложные действия: «Пуск → Панель управления → Персонализация → Цвет и внешний вид окон (включить прозрачность) → Открыть свойства классического внешнего вида для выбора других возможностей → Параметры оформления → Цветовая схема → Windows Aero → Применить». Однако,

как выясняется, даже если ваша видеокарта соответствует требованиям, то интерфейс Aero не всегда работает. Приведу несколько рекомендаций, которые могут пригодиться при решении проблем с Aero.

Решение проблем с запуском Aero

Для начала убедитесь, что для цвета установлена разрядность 32 бита, частота обновления экрана монитора выше 10 герц, тема установлена в Windows Vista, для цветовой схемы выбрана Windows Aero и включена прозрачность рамки окна. Для того чтобы установить 32-битную цветопередачу откройте окно настройки параметров экрана. В списке «Цвета» выберите «Высшее (32 бита)» и нажмите OK. (Если не удается выбрать 32 бит, убедитесь, что установлено максимально возможное разрешение, а затем попытайтесь снова.) Установить частоту обновления экрана можно в окне настройки параметров экрана.

Во вкладке «Дополнительные параметры» перейдите на вкладку «Наблюдать», а затем выберите частоту обновления выше 10 герц. Для смены частоты обновления необходимо некоторое время. Если требуется сохранить изменения, нажмите «Применить». Если изменения не будут сохранены в течение пятнадцати секунд, частота обновления вернется к своему прежнему значению.

Для того чтобы сменить тему рабочего стола, необходимо щелкнуть по ссылке и открыть «Параметры темы» и в списке «Тема» выбрать Windows Vista.

Для установки цветовой схемы в Windows Aero в списке «Цветовая схема» выберите Windows Aero и нажмите OK.

Чтобы включить прозрачность рамки окна, сначала необходимо установить цветовую схему в Windows Aero. Для этого в «Панели управления» щелкните «Оформление и личная настройка», «Персонализация», а затем выберите «Цвет и внешний вид окна». Установите флажок «Включить прозрачность». Эти стандартные действия должны помочь при работе с Aero.

В случае если они не помогают, есть еще не совсем стандартные средства. Для запуска Aero можно также внести некоторые правки в параметры реестра. В редакторе реестра необходимо изменить значение следующих параметров:

- HKCU\Software\Microsoft\Windows\DWM\Composition изменяем на 1 (32-bit DWORD),
- HKCU\Software\Microsoft\Windows\DWM\CompositionPolicy изменяем на 2 (32-bit DWORD).

После этого нужно перезагрузить машину и в командной строке выполнить:

```
net stop uxsms
net start uxsms
```

И снова перезагрузить рабочую станцию. Данный способ также может быть полезен и в случае если вам необходимо включить Aero с помощью сценария на нескольких компьютерах.

Заключение

Что же еще нового мы можем увидеть в Windows Vista? Целый ряд новшеств связан с обеспечением безопасности и целостности данных. Появились такие функции, как Parent Control (родительский контроль), User Account Control (UAC, управление учетными данными пользователей), улучшенный Windows Firewall, поддержка NAP (Network Access Protection, защита сетевого доступа) и другие функции. Обо всем этом в других статьях, а следующая будет посвящена средствам обеспечения безопасности в Windows Vista.

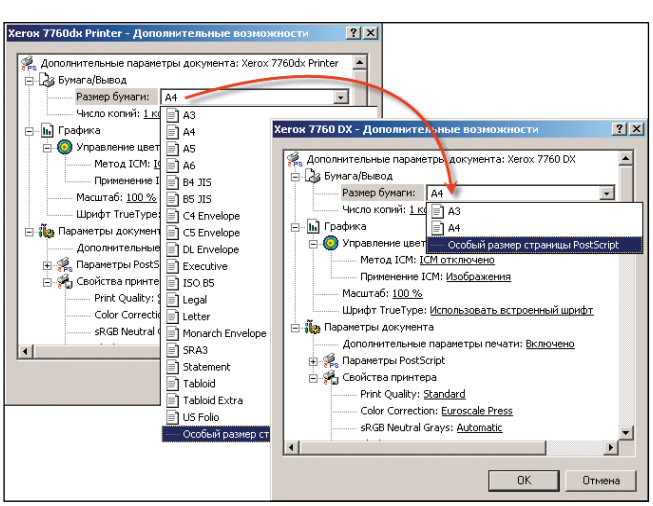
1. http://www.microsoft.com/windows/compatibility/Browse.aspx?type=Hardware&category=TV%20Devices&subcategory=TV%20Tuners – список совместимых с Vista ТВ-тюнеров.
2. http://technet.microsoft.com/ru-ru/windows/aa904820.aspx – статьи по планированию и развертыванию Windows Vista.
3. http://www.microsoft.com/windows/windows-vista/get/upgradeadvisor.aspx – инструмент Windows Vista Upgrade Advisor.

Оптимизируем PPD-файлы

Иван Коробко

Все основные настройки Post Script-драйверов хранятся в отдельных файлах. Рассмотрим их подробнее.

Перед запуском документа на печать необходимо выбрать принтер и определить ряд обязательных параметров. По умолчанию им уже присвоены значения. Однако не все они отвечают требованиям конечного пользователя. Например, на принтере формата A4 в большинстве случаев по умолчанию установлен формат бумаги letter, хотя необходим A4. В одном случае из ста может возникнуть необходимость распечатать на конверте. Возникает закономерный вопрос: как изменить значение по умолчанию и сократить предлагаемый список форматов бумаги до разумного (см. **рисунок**). Аналогичная ситуация возникает с качеством печати: зачем на обычном принтере печатать с качеством 1200 точек на дюйм, когда вполне достаточно 300 dpi или 600 dpi.



Список размеров бумаги в настройках драйвера принтера

Все вышеуказанные параметры хранятся в текстовом файле с расширением PPD, который поставляется производителем принтера в комплекте драйверов.

Структура PostScript-драйвера

Любой PostScript или PS-драйвер состоит из нескольких библиотек, входящих в комплект операционной системы. Несмотря на это они включаются в дистрибутив драйвера принтера для удобства его установки. В **таблице 1** приведен список библиотек стандартного PS-драйвера Windows 2K. После установки все файлы драйвера копируются в папку C:\Windows\System32\spool\drivers\w32x86.

В **листинге 1** приведен стандартный INF-файл, обеспечивающий установку PS-драйвера для принтера. На практике производитель создает для драйвера графическую оболочку, которая видоизменяет его до неузнаваемости. Основной недостаток GUI-оболочки заключается в снижении работоспособности драйвера. Иногда ошибки программистов, создавшие графическую оболочку, могут привести к невозможности распечатать документ. Любую GUI-оболочку драйвера можно убрать (см. [1]).

Листинг 1. Шаблон INF-файла стандартного PS-драйвера

```
[Version]
Signature="$Windows CHICAGO$"
ClassGUID={4D36E979-E325-11CE-BFC1-08002BE10318}
Class=Printer
Provider="temp"

[Manufacturer]
%Company%=firm

[firm]
"Product Name" = **********, unique_identifier

[**********]
CopyFiles=@*****.PPD,PSCRIPT_NT   ; PPD-файл.
DataSection=PSCRIPT_DATA
DataFile=*****.PPD
Include=NTPRINT.INF      ; инсталляция NTPRINT.INF.
Needs=PSCRIPT.OEM        ; инсталляция PSCRIPT.

[DestinationDirs]
DefaultDestDir=66000
[SourceDisksNames]
1 = "HP",,,""
[SourceDisksFiles]
HP1200.ppd = 1,,,,,,,11,3
[Strings]
Company = "Firm Name"
```

Что такое PPD-файл?

PostScript Printer Description или PPD-файл представляет собой текстовый файл в кодировке ASCII. С его помощью обеспечивается программная поддержка принтером различных размеров бумаги, двухсторонняя печать, разбор по копиям в случае необходимости, цветность, значения по умолчанию и другие характеристики.

Все настройки описаны в этом файле с помощью языка PostScript, разработанного компанией ADOBE. Полное описание этого языка можно загрузить из источника [2], а описание PPD-файлов находится в [3].

Структура PPD-файла

Прежде чем приступить к чтению PPD-файла, необходимо сказать несколько слов о синтаксисе: любой файл состоит из строк, каждая из которых начинается с символа звездочки «*». Строка может состоять из нескольких подстрок. В этом случае строка не начинается с символа «*», комментарий начинается с «*%».

В общем виде строка строится по следующему шаблону:

```
*command:value
```

где command – зарезервированная команда (см. [2]), value – его значение.

Заголовок PPD-файла

В любом файле присутствует несколько обязательных команд, список и описание которых приведены в **таблице 2**. В **листинге 2** приведен текст стандартного заголовка PPD-файла:

Листинг 2. Типичный заголовок PPD-файла

```
*PPD-Adobe: "4.3"

*% ================================================
*% Printer Description File
*% Copyright 1992-2001 Hewlett-Packard Company
*%================================================
*% PPD for HP LaserJet 1200 Series
*%================================================

*% === PPD File Version Information ====
*FileVersion:   "1.004"
*FormatVersion:  "4.3"
*LanguageEncoding: ISOLatin1
*LanguageVersion: English
*PCFileName:    "HP1200_7.PPD"

*% === Product Version Information ====
*ModelName:   "HP LaserJet 1200 Series"
*ShortNickName: "HP LaserJet 1200 Series PS"
*NickName: "HP LaserJet 1200 Series PS"
*Product:    "(HP LaserJet 1200 Series)"
*Manufacturer: "HP"
*PSVersion:   "(2014.108) 1"
```

Необходимо отметить, что все вышеперечисленные параметры обязательны. Более того, порядок их взаимного расположения также имеет значение.

Таблица 1. Библиотеки стандартного PS-драйвера

Файл	Название библиотеки	Описание
PS5UI.DLL	PostScript User Interface	Интерфейс драйвера
PSCRIPT5.DLL	PostScript Printer Driver	PS-драйвер принтера
PSCRIPT.NTF	Fonts	Бинарный файл, содержащий в себе стандартные шрифты, поддерживаемые устройством
PSCRIPT.HLP	Help	Файл справки PS-драйвера
*.INF	Information	Файл-инсталлятор драйвера
*.PPD	PostScript Printer Description	Описание возможностей принтера: лотки, форматы бумаги, цветность и т. д.

Таблица 2. Обязательные команды PPD-файла

Название команды	Значение	Комментарий
*PPD-Adobe	4.3	Версия PPD. Сейчас используется версия 4.3, вышедшая 09 февраля 1996 года
*FileVersion	1.004	Версия файла
*FormatVersion	4.3	Версия PPD. Значение совпадает со значением параметра *PPD-Adobe
*LanguageEncoding	ISOLatin1, Cyrillic	Кодировка, используемая в драйвере. Для английского языка ISOLatin1, для русского – Cyrillic
*LanguageVersion	English, Russian	Язык, используемый в настройках драйвера
*Manufacturer	HP	Производитель оборудования
*ModelName	HP LaserJet 1200 Series	Модель принтера. Назначается производителем
*NickName	HP LaserJet 1200 Series PS	Локальное имя принтера, задаваемое при установке устройства мастером. В нем также обычно указывается версия драйвера. Длина не ограничена
*ShortNickName	HP LaserJet 1200 Series PS	Локальное имя принтера, задаваемое при установке устройства мастером. В отличие от *NickName длина ограничена 31-м символом
*Product	(HP LaserJet 1200 Series)	Уникальное Название продукта. По этом полю система определяет установлен ли драйвер в системе и предлагает один из вариантов действия: заменить, пропустить
*PSVersion	(2014.108) 1	Версия драйвера
*PCFileName	HP1200_7.PPD	Название PPD-файла (этого файла). Значение *PCFileName состоит из 8 символов имени и 3- расширения (PPD). Первые 2 символа имени – производитель, а оставшиеся 6 – уникальный идентификатор модели

Решение типовых задач

Для удобства восприятия рассмотрим примеры решения задач, которые могут встретиться вам на практике. Приведу некоторые из них:

- Управление форматами бумаги.
- Назначение размера бумаги по умолчанию.

Управление форматом бумаги

За формат бумаги отвечает параметр PageSize. Список, задаваемый в блоке его описания, отображается конечному пользователю (см. **рисунок**). Рассмотрим подробнее фрагмент файла (см. **листинг 3**). Описание блока начинается со строки *?PageSize:, а заканчивается – *End. Сам блок при этом заключен в кавычки. Перед описанием списка необходимо зарезервировать пункты с помощью команды dict. В **листинге 2** присутствует команда «17 dict». Это обозначает, что пользователь сможет выбрать один из 17 предложенных форматов бумаги. Допустим, необходимо обеспечить выбор одного из 2 форматов бумаги: A4 и Postcard (стандартный конверт). В этом случае требуется указать количество пунктов в выпадающем меню, равное двум: «2 dict». Каждый из пунктов меню описывается командой Dup и Put. Описание одного пункта списка выглядит следующим образом:

```
Dup [x y] string Put
```

где x и y – размеры в pt (point, пункт), string – текст, отображаемый в меню.

Например, размер для бумаги формата A4 – 210x297 мм. В файле указывается величина бумаги в миллиметрах, умноженная на коэффициент, равный 2,83 (1 mm = 2,8346 pt). После округления получим 595x842 pt (см. **листинг 3**). Таким образом, для описания 2 вышеупомянутых форматов бумаги после удаления описаний лишних форматов **листинг 3** будет видоизменен (см. **листинг 4**).

Листинг 3. Описание поддерживаемых форматов бумаги

```
*?PageSize: "
   save
   currentpagedevice /PageSize get aload pop
   2 copy gt {exch} if
   (Unknown)
   17 dict
   dup [612 792]  (Letter) put
   dup [522 756]  (Executive) put
   dup [612 1008] (Legal) put
   dup [595 842]  (A4) put
   dup [420 595]  (A5) put
   dup [297 420]  (A6) put
   dup [499 709]  (ISOB5) put
   dup [516 729]  (B5) put
   dup [612 936]  (w612h936) put
   dup [284 419]  (Postcard) put
   dup [419.5 567](DoublePostcard) put
   dup [297 684]  (Env10) put
   dup [279 540]  (EnvMonarch) put
   dup [312 624]  (EnvDL) put
   dup [459 649]  (EnvC5) put
   dup [499 709]  (EnvISOB5) put
   dup [558 774]  (w558h774) put
   { exch aload pop 4 index sub abs 5 le exch
      5 index sub abs 5 le and
      {exch pop exit} {pop} ifelse
   } bind forall
   = flush pop pop
   restore
"
*End
```

Листинг 4. Описание поддерживаемых форматов бумаги

```
*?PageSize: "
   save
   currentpagedevice /PageSize get aload pop
   2 copy gt {exch} if
   (Unknown)
   2 dict
   dup [595 842]  (A4) put
   dup [284 419]  (Postcard) put
   { exch aload pop 4 index sub abs 5 le exch
      5 index sub abs 5 le and
      {exch pop exit} {pop} ifelse
   } bind forall
   = flush pop pop
   restore
"
*End
```

Рекомендуется удалить лишние описатели форматов бумаги в секциях PageSize и PageRegion, каждый из которых имеет формат, описанный в **листинге 5**.

Листинг 5. Описатели формата бумаги

```
*PageRegion string1/string2: "
  <</PageSize [x y] /ImagingBBox null>> setpagedevice"
*End
```

где string1 – сокращенное название формата бумаги, а string2 – полная форма. В большинстве случаев значения обеих строк равны. x и y – размер бумаги в дюймах.

Назначение размера бумаги по умолчанию

Размер бумаги по умолчанию назначается с помощью параметров *DefaultPageSize, *DefaultPageRegion, значения которых должны совпадать. Значение по умолчанию задается в одноименных блоках.

Рассмотрим изменение размера по умолчанию на примере параметра *DefaultPageSize. Отмечу, что назначение размера бумаги по умолчанию идет перед описанием форматов бумаги. Как и в описании формата бумаги, в ее размере задается только сокращенное название (см. **листинг 6**).

Листинг 6. Назначение формата бумаги по умолчанию

```
*OpenUI *PageSize: PickOne
*OrderDependency: 30 AnySetup *PageSize
*DefaultPageSize: Letter
*PageSize Letter/Letter: "
  <</PageSize [612 792] /ImagingBBox null>> setpagedevice"
*End
.....
```

Заключение

Достаточно подробно изучив вопрос коррекции списков и значений по умолчанию на примере форматов бумаги, читатель сможет с помощью этой статьи и документации (в случае необходимости) оптимизировать драйвер для своих целей.

1. Коробко И. Сетевое сканирования с помощью МФУ от HP. //Системный администратор, №12, декабрь 2008 г. – С. 44-48.
2. PostScript® language reference, third edition – http://www.adobe.com/products/postscript/pdfs/PLRM.pdf.
3. PostScript Printer Description File Format Specification – http://www.adobe.com/devnet/postscript/pdfs/5003.PPD_Spec_v4.3.pdf.

Уязвимость в Trend Micro HouseCall ActiveX-компоненте

Программа: Trend Micro HouseCall ActiveX Control версии до 6.6.0.1285; Trend Micro HouseCall Server версии до 6.6.0.1285.

Опасность: Высокая.

Описание: Уязвимость существует из-за использования освобожденной памяти в HouseCall ActiveX-компоненте (Housecall_ActiveX.dll). Удаленный пользователь может с помощью веб-сайта, содержащего специально сформированную функцию notifyOnLoadNative(), вызвать разыменование ранее освобожденной памяти и выполнить произвольный код на целевой системе.

URL производителя: www.trendmicro.com.

Решение: Установите последнюю версию с сайта производителя.

Спуфинг атака в OpenSSL

Программа: OpenSSL версии до 0.9.8j.

Опасность: Средняя.

Описание: Уязвимость существует из-за того, что некоторые OpenSSL-функции некорректно проверяют данные, возвращаемые функцией EVP_VerifyFinal(), при проверке подписей для DSA- и ECDSA-ключей. Злоумышленник может обойти проверку подписи, например, при отправке специально сформированной подписи сертификата клиенту. Для успешной эксплуатации уязвимости сервер должен использовать сертификат, содержащий DSA- или ECDSA-ключ.

URL производителя: www.openssl.org.

Решение: Установите последнюю версию 0.9.8j с сайта производителя.

Повышение привилегий в ESET Smart Security

Программа: ESET Smart Security версии до 3.0.684.

Опасность: Низкая.

Описание: Уязвимость существует из-за недостаточной обработки параметров пользовательского пространства в IOCTL-обработчике драйвера epfw.sys. Локальный пользователь может с помощью специально сформированного IOCTL-запроса выполнить произвольный код на целевой системе в пространстве ядра.

URL производителя: www.eset.com/smartsecurity/index.php.

Решение: Установите последнюю версию 3.0.684 с сайта производителя.

Повышение привилегий в FreeBSD

Программа: FreeBSD 6.3, 6.4, 7.0.

Опасность: Низкая.

Описание: Уязвимость существует из-за некорректной инициализации некоторых указателей функций netgraph- и bluetooth-сокетов в реализации ядра. Локальный пользователь может выполнить произвольный код на целевой системе в пространстве ядра.

URL производителя: www.freebsd.org.

Решение: Установите исправление с сайта производителя.

Переполнение буфера в Microsoft SQL Server

Программа: Microsoft SQL Server 2000 8.00.2050; Microsoft SQL Server 2000 Desktop Engine (MSDE 2000); Microsoft SQL Server 2005; Microsoft SQL Server 2005 Express Edition 9.2.3042.00.

Опасность: Низкая.

Описание: Уязвимость существует из-за ошибки проверки границ данных в реализации процедуры sp_replwritetovarbin(). Удаленный пользователь может передать уязвимой процедуре специально сформированные аргументы, вызвать переполнение динамической памяти и повысить свои привилегии на системе.

URL производителя: www.microsoft.com.

Решение: В настоящее время способов устранения уязвимости не существует.

Раскрытие данных в Samba

Программа: Samba версии 3.0.29 по 3.2.4.

Опасность: Низкая.

Описание: Уязвимость существует из-за ошибки проверки границ данных при обработке запросов trans, trans2 и nttrans. Удаленный пользователь может с помощью специально сформированных запросов получить доступ к памяти smbd.

URL производителя: www.samba.org.

Решение: Установите последнюю версию 3.2.5 или 3.0.33 с сайта производителя.

Множественные уязвимости в IBM AIX

Программа: IBM AIX версии 6.1.0, 6.1.1, 6.1.2.

Опасность: Низкая.

Описание: 1. Уязвимость существует из-за ошибки проверки границ данных в /usr/sbin/ndp в setuid-приложении. Локальный пользователь может вызвать переполнение буфера и выполнить произвольный код на целевой системе. Для успешной эксплуатации уязвимости демон netcd должен быть запущен.

2. Уязвимость существует из-за ошибки проверки границ данных в привилегированной команде /usr/sbin/autoconf6. Локальный пользователь может вызвать переполнение буфера и выполнить произвольный код на системе. Для успешной эксплуатации уязвимости должен использоваться RBAC, и атакующий должен авторизоваться в aix.network.config.tcpip.

3. Уязвимость существует из-за ошибки в привилегированной команде /usr/bin/enq. Локальный пользователь может удалить произвольные файлы, если /etc/qconfig определяет очередь печати.

4. Уязвимость существует из-за ошибки в привилегированной команде /usr/bin/crontab. Атакующий, авторизовавшийся в aix.system.config.cron, может повысить свои привилегии на системе.

URL производителя: www-03.ibm.com/systems/p/os/aix/v61/index.html.

Решение: Установите исправление с сайта производителя.

Составил Александр Антипов

Перенос профиля пользователя в Windows XP Professional Edition и Windows 2000 Professional

Рамиль Айзятуллен

Хотите организовать или перевести старый домен на новое программное обеспечение, при этом чтобы пользователи ничего не заметили? Я поделюсь с вами опытом по самой трудоемкой части этого процесса – переносу профилей пользователей.

Возникла задача перевести учетные данные всех пользователей из домена Samba в домен Windows. Самое сложное и утомительное во всем этом – перенос профилей пользователей.

Итак приступим. У нас есть два домена, старый OLD (домен Samba 3) и новый new.local (домен Windows 2003). На рабочих станциях установлены операционные системы Windows 2000 Professional и Windows XP Professional Edition.

Внимание! Рекомендую прежде всего проверить на всех рабочих станциях наличие учетной записи локального администратора и убедиться в том, что вы знаете к ней пароль, иначе, когда вы выведете компьютер из домена, придется этот пароль сбрасывать [1].

Коротко опишу состояние локальной сети. Мы имеем два настроенных домена, один на платформе FreeBSD с установленным пакетом Samba 3 (почитать об установке и настройке можно на в моем блоге [2]), и другой домен AD на MS Windows 2003. На сервере Samba включена служба WINS для сопоставления netbios-имён компьютеров с IP-адресами узлов.

На отдельном сервере на платформе FreeBSD запущены службы DNS и DHCP. В DHCP первым DNS-сервером прописан DNS Windows 2003, вторым остался DNS сервера на FreeBSD. Также в DHCP прописан сервер WINS, установленный на Samba 3.

На сервере DNS Windows 2003 включена пересылка запросов DNS, которые не могут быть обработаны самим сервером (например, адресованные в Интернет).

В качестве сервера, куда пересылаются запросы, указан IP-адрес сервера DNS на платформе FreeBSD.

Согласно принятой политике безопасности пользователи сами назначали себе пароли, и потому в новом Windows 2003 домене были созданы такие же учетные записи поль-

зователей, но с одинаковым паролем. В свойствах учетной записи всех пользователей на вкладке «Учетная запись» установлена галка «Требовать смену пароля при следующем входе в систему».

В обоих доменах имеется сценарий входа, подключающий сетевые диски с Samba-сервера.

У нас есть два домена, и они прекрасно существуют в одной сети. Думаю, что если подобным образом переходить из одного Windows-домена в другой, проблем также не возникнет.

А теперь к делу: перенос профилей пользователей из одного домена в другой.

Регистрируемся в старом домене с учетной записью администратора домена и выводим компьютер из домена (у обычных пользователей недостаточно для этого прав). В ходе этой операции будут запрошены имя пользователя и пароль, можно ничего не вводить.

После успешного вывода в рабочую группу (например, OLD) потребуется перегрузить компьютер пользователя.

После перезагрузки компьютера регистрируемся с учетной записью локального администратора и находим профиль пользователя данного компьютера (который требуется перенести), в нашей локальной сети использовались локальные профили пользователей. К примеру, это может быть папка C:\Documents and Settings\ivanov. Переименовываем эту папку, к примеру в ivanov123.

Далее вводим машину в новый домен new.local, здесь понадобится пароль администратора этого домена, и перезагружаем компьютер. Регистрируемся на рабочей станции с доменной учетной записью ivanov.

После этого опять перезагружаем компьютер, это необходимо, чтобы выгрузилась ветка реестра пользователя ivanov. Если этого не сделать, не получится полностью удалить папку C:\Documents and Settings\ivanov.

Регистрируемся в новый домен с учетной записью пользователя администратор нового домена. Удаляем папку C:\Documents and Settings\ivanov, а папку ivanov123 переименовываем в ivanov.

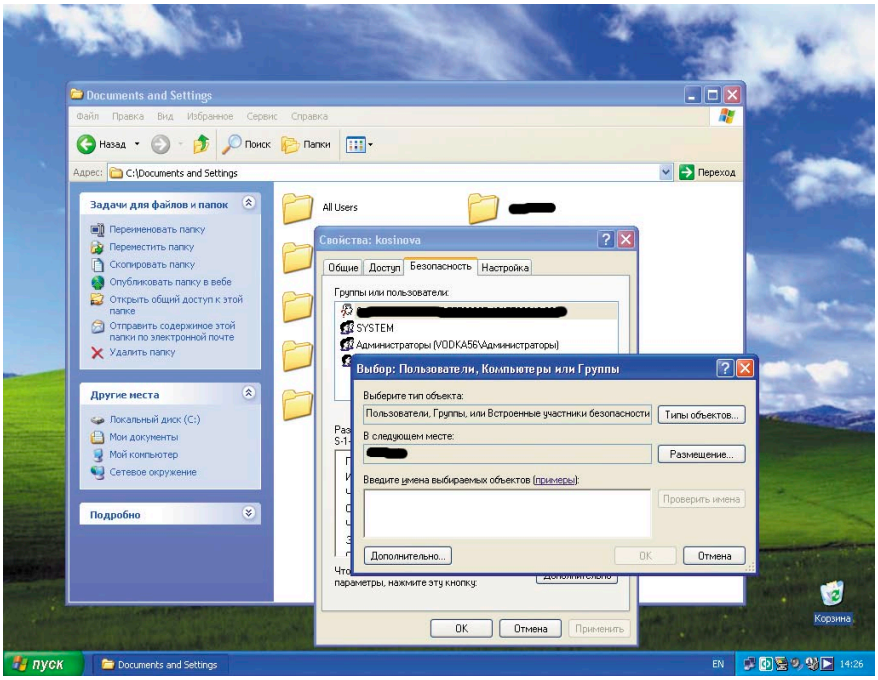


Рисунок 1. Установка прав пользователя к папке профиля в Windows XP

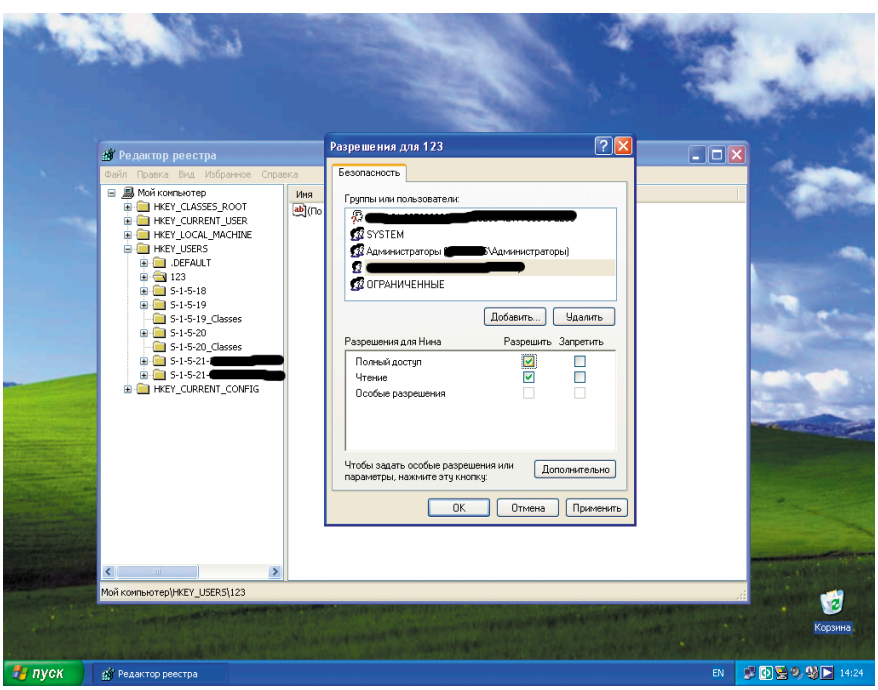


Рисунок 2. Установка прав пользователя на ветку реестра в Windows XP

Открываем свойства папки ivanov, переходим на вкладку безопасность и даем полный доступ к этой папке пользователю ivanov из нового домена (см. **рис. 1**).

Далее запускаем программу regedit для операционной системы Windows XP (нажимаем «Пуск → Выполнить», в поле «Открыть» набираем команду «regedit», нажимаем Ok) и программу regedt32 для Windows 2000. Запустится редактор реестра, затем выбираем раздел HKEY_USERS. Нажимаем в меню «Файл → Загрузить куст», выбираем файл C:\Documents and Settings\ivanov\NTUSER.DAT. Так как этот файл скрытый, то нужно предварительно в проводнике Windows выбрать папку C:\Documents and Settings\ivanov и в меню «Сервис → Свойства папки → Вид» включить «Показывать скрытые файлы и папки».

На предложение указать имя раздела пишем, например, 123. После этого выбираем данный раздел и даем полный доступ к нему пользователю

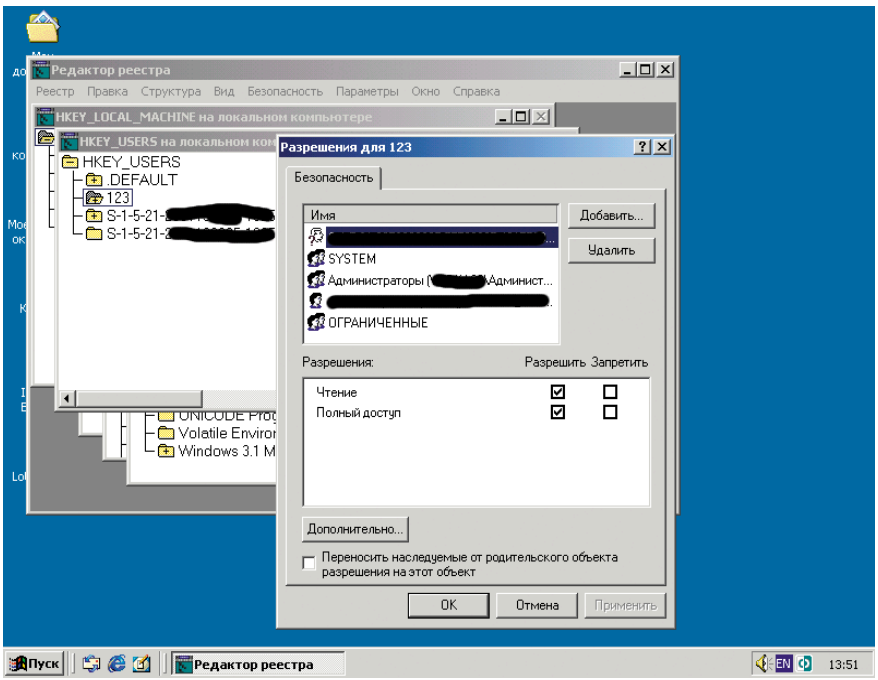


Рисунок 3. Установка прав пользователя на ветку реестра в Windows 2000

ivanov из нового домена. Далее выбираем в меню «Файл → Выгрузить куст» (см. **рис. 2**). Для Windows 2000 в меню есть специальный пункт «Разрешения», вот и все отличие (см. **рис. 3**).

Завершаем сеанс администратора и регистрируемся в домен с учетной записью пользователя ivanov. Видим старый рабочий стол пользователя со всеми его ярлыками, файлами, программами.

Внимание! Что было утеряно:

- головная боль всех администраторов – пароль Skype (в Windows XP, в Windows 2000 он сохранился);
- адрес прокси-сервера в Internet Explorer (Mozilla Firefox лишена этой проблемы), сохраненные логин и пароль для доступа к прокси-серверу;
- пароль на почтовый ящик в Outlook Express;
- Lotus Notes 6.5 работает (установлен в конфигурации для всех пользователей), если у пользователя нет прав локального администратора, необходимо дать ему полный доступ на папку C:\Documents and Settings\All Users\Application Data\Lotus (но это уже отдельная история).

Кстати, давать пользователям права локального администратора без острой необходимости не нужно.

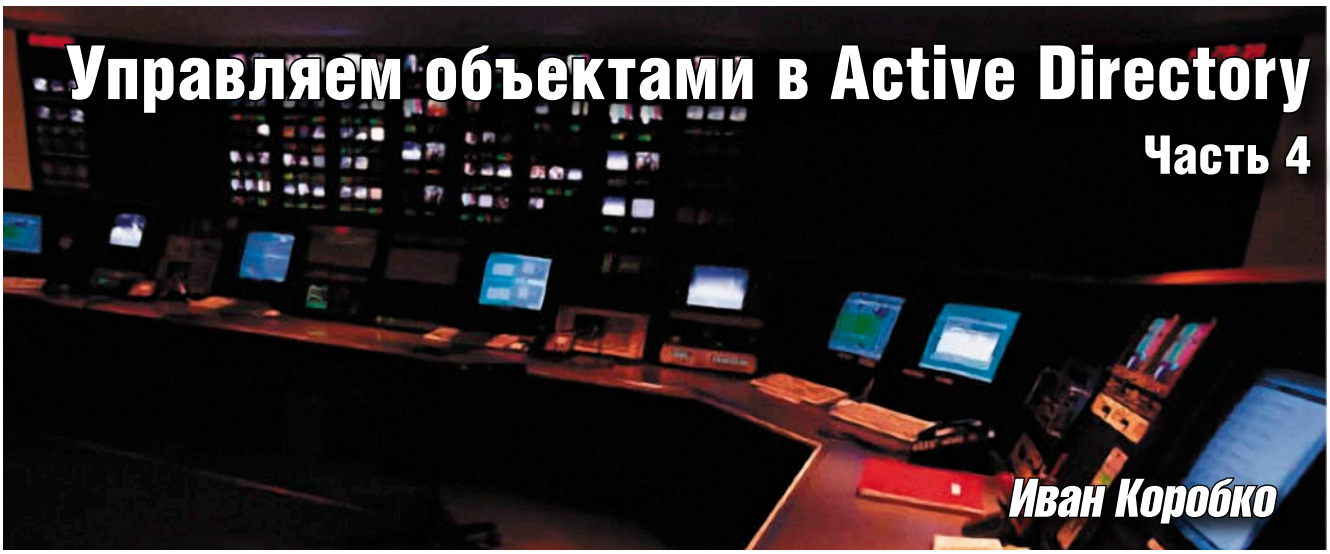
Резюме

При достаточной сноровке, современном компьютере и не очень большой папке C:\Documents and Settings\ivanov перенос профиля занимает в среднем 15-20 минут, а значит, за один рабочий день силами только одного системного администратора офис небольшой компании в 20 рабочих мест может быть переведен из домена в домен. Обсудить статью можно на форуме – http://www.samag.ru/forum.

1. Сброс локальных паролей Windows – http://home.eunet.no/~pnordahl/ntpasswd.
2. Настройка Samba – http://argo-uln.blogspot.com/2006/08/samba-3-pdc-ldap-freebsd-61.html.
3 PDC LDAP FreeBSD 6.1.

Управляем объектами в Active Directory

Часть 4



Иван Коробко

Группа безопасности – один из основных объектов Active Directory, определяющего правила доступа к ресурсам домена. Умение управлять этим объектом дает большие возможности в автоматизации управления Active Directory.

Группа безопасности, так же как и учетная запись пользователя, – очень важный объект, значение которого нельзя недооценивать, несмотря на его простоту по сравнению с последним. С помощью групп безопасности определяют уровень доступа к сетевым или локальным ресурсам; используя членство пользователей в группах, создают интеллектуальные сценарии регистрации пользователей в сети.

В этой статье, являющейся четвертой частью цикла статей о внутреннем устройстве Active Directory, рассмотрим анатомию группы Active Directory и принципы программного управления этим объектом.

Основные понятия

Прежде чем перейти к описанию объектной модели группы безопасности, рассматривать вопрос членства учетных записей пользователей в группе, необходимо определить понятие «группа безопасности».

Группа безопасности (security group) – объект, в котором могут содержаться дочерние объекты: учетные записи групп и пользователей. Она используется для определения разрешений доступа к файлам и другим ресурсам. Любая группа безопасности характеризуется двумя параметрами: ее типом и областью действия (см. **таблицу 1**).

Тип группы (group type) определяет, является ли группа – группой рассылки или же группой безопасности.

Существует два типа групп: Security (безопасности) и Distribution (распространения).

Вторая важная характеристика – область действия группы (Group scope). Областью действия определяют, каким образом может быть использована группа: как локальная, как глобальная или как универсальная. При наличии в лесу двух и более доменов область действия группы играет значение, однако при наличии в нем одного домена – область действия не имеет значения.

Создание группы

Существует минимум два способа создания группы безопасности: с помощью мастера и сценария. Рассмотрим сначала работу мастера, уделив особое внимание изменениям, которые происходят в это время в каталоге Active Directory. Основные параметры, задаваемые при создании группы администратором – ее имя и тип. Изменение остальных параметров возможно только после создания объекта с помощью соответствующего мастера.

Создание группы с помощью мастера

Запуск мастера создания группы осуществляется из MMC-консоли Active Directory Users and Computers выбором пункта «New → Group» из контекстного меню папки, в которой необходимо создать учетную запись. Таким образом, определяется местоположение объекта, которому в Active Directory соответствует значение атрибута объекта distinguishedName.

Работа мастера состоит из одного шага (см. **рис. 1**). Во время создания группы безопасности необходимо назначить имя и тип группы, определить область действия и имя группы для совместимости (Pre-Windows 2000) с доменом Windows NT (см. **таблицу 1**).

Рассмотрим параметры, задаваемые мастером во время создания учетной записи. Первым из них является название группы (атрибут Group). В каталоге Active Directory ему соответствует атрибут cn. Значение атрибута name – отображаемое имя, назначается автоматически, идентично значению cn. Однако впоследствии оно может быть изменено в свойствах группы безопасности.

Одновременно с этим значением назначается имя группы, используемое для совместимости с доменами Windows NT – значение параметра Group name (Pre-Windows 2000). В каталоге Active Directory ему соответствует атрибут sAMAccountName.

Значения атрибута cn и sAMAccountName можно изменить, только пере-

именовав объект. Изменяя имя объекта с помощью мастера, администратор изменяет только его отображаемое имя.

С помощью двух оставшихся блоков определяют тип и область действия группы. По умолчанию мастер предлагает создать глобальную группу безопасности (groupType = -2147483646). Каждому из выбранных значений соответствует цифровой эквивалент (см. **таблицу 2**). В каталог Active Directory записывается суммарное значение в числовое поле groupType.

Таблица 1. Параметры группы

Параметр мастера	Атрибут объекта в Active Directory	Тип данных	Описание
Group name	cn, name	String	Название группы в домене
Group name (Pre-Windows 2000)	sAMAccountname	String	Название группы, используемое для совместимости с доменом Windows NT
Group scope	groupType	Radio Button	Суммарным значением параметра описывается область действия и тип создаваемой группы безопасности

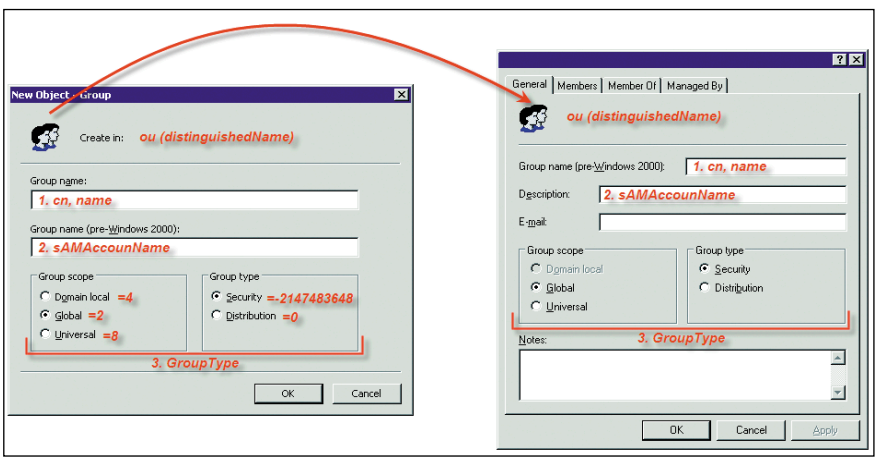


Рисунок 1. Создание группы с помощью мастера

Создание группы с помощью сценария

Для создания учетной записи группы программным способом (VBScript), как и при работе мастера, необходимо жестко задать несколько параметров. В **листинге 1** приведен сценарий, позволяющий создать учетную запись группы. Исходные данные для его создания приведены в **таблице 3**.

Листинг 1. Создание учетной записи группы

```
      set RootDSE = GetObject("LDAP://RootDSE")
      Domain = rootDSE.Get("defaultNamingContext")
Set objUsers = GetObject("LDAP://OU=WorkGroup," & Domain)
Set objNewUser = objUsers.Create("group", "cn=Test")
objNewUser.Put "sAMAccountName", "Test"
objNewUser.Put "groupType", "-2147483646"
      objNewUser.SetInfo
```

Обратите внимание! Если в листинге не указать тип и область действия группы с помощью параметра groupType, то система автоматически создаст этот параметр, присвоив этому параметру значение -2147483646, что эквивалентно глобальной группе безопасности.

Рассмотрим работу листинга. В первых двух строках сценария осуществляется определение RDN-имени (relative distinguished name, относительное составное имя) текущего домена с помощью виртуального объекта RootDSE. Затем в контейнере WorkSpace, находящемся в корне схемы Active Directory, создается группа безопасности с помощью функции Create(), имеющей два параметра. Первый параметр – тип объекта (последний элемент массива objectType), второй – имя объекта в формате «cn = …».

Замечание. RDN является одним из обязательных атрибутов объекта, значение которого характеризует его положение в иерархической структуре домена. Максимальная длина RDN-имени составляет 255 символов, однако схема Active Directory накладывает свои ограничения на его составные части. Например длина атрибута cn ограничивается 64 символами. Подробно о RDN см. [1].

Удаление группы

Аналогично описанию процесса создания группы рассмотрим удаление группы с двух ракурсов: работы мастера и сценария, их взаимосвязи.

Удаление группы с помощью мастера

Для запуска мастера удаления учетной записи какого-либо объекта, в том числе и группы, необходимо установить курсор на удаляемый объект (в данном случае – группа). Таким образом, определяют один из важнейших параметров – путь к объекту (поле distinguishedName). Вызвав контекстное меню объекта с помощью правой кнопки мыши, удаляют объект, выбрав пункт меню delete (см. **рис. 2**).

Таблица 2. Расшифровка значений параметра groupType

Тип группы	Значение	Тип группы	Значение
Global Security Group	-2147483648	Global Distribution Group	2
Local Security Group	-2147483644	Local Distribution Group	4
BuiltIn Group	-2147483643	Universal Distribution Group	8
Universal Security Group	-2147483640	–	–

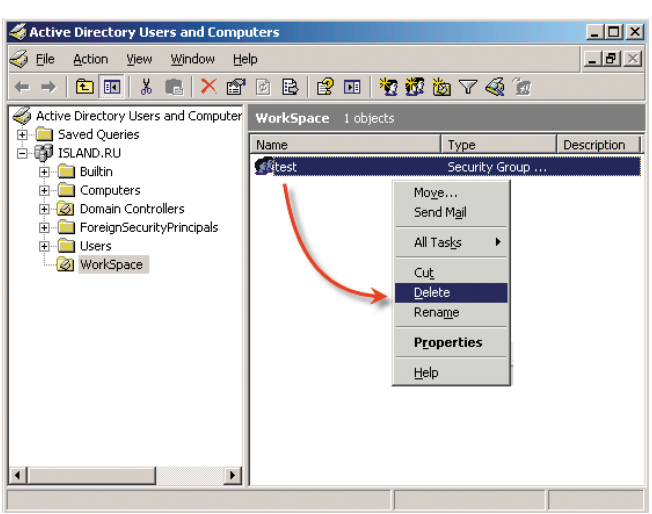


Рисунок 2. Удаление учетной записи группы с помощью мастера

Удаление объекта с помощью сценария

В сценарии удаления объекта необходимо указать тип удаляемого объекта и путь к этому объекту в каталоге Active Directory. Оба параметра в сумме составляют значение distinguishedName. Например, если требуется удалить группу Test, то необходимо определить значение параметра distinguishedName. Затем – имя объекта (значение cn) и папку, в которой он находится.

Таблица 3. Параметры сценария для создания учетной записи пользователя

Параметр	Описание	Способ назначения
cn = Test	Отображаемое имя	Явный
sAMAccountName = Test	Имя в сети для совместимости с доменами Windows NT	Явный
groupType = -2147483646	Область действия и тип группы	Явный
distinguishedName = CN=Test, OU=WorkSpace,DC=Island,DC=ru	Путь к создаваемой учетной записи группы	Неявный

Листинг 2. Удаление учетной записи группы

```
      set RootDSE = GetObject("LDAP://RootDSE")
      Domain = rootDSE.Get("defaultNamingContext")
Set objUsers = GetObject("LDAP://OU=WorkGroup," & Domain)
objUsers.delete "group", "cn=Test"
Set objUsers = nothing
```

Членство в группах

В группах безопасности можно производить операции:

- получать список объектов;
- добавлять объекты;
- удалять объекты.

Каждый из этих способов можно реализовать как программно, так и с помощью мастера MMC-консоли, открыв вкладку Members учетной записи в свойствах группы (см. **рис. 3**).

Получение списка членов группы

Членами группы безопасности могут быть группы или пользователи. Список членов группы хранится в массиве Member, который хранится в виде составного LDAP-пути (см. **листинг 3а**).

В графической оболочке отображается преобразованное каноническое имя, которому соответствует значение поля cn. Такое преобразование приведено в **листинге 3б**.

Листинг 3а. Получение списка членов группы (стандартный вариант)

```
path = …
Set objGroup = GetObject("LDAP:// " & path)
temp = ""
For Each obj In objGroup.member
temp = temp +  obj + vbNewLine
Next
MsgBox temp
```

Листинг 3б. Получение списка членов группы (улучшенный вариант)

```
path = …
Set objGroup = GetObject("LDAP:// " & path)
For Each obj In objGroup.member
               temp = temp +  GetObject("LDAP:// " & ↵
                        obj.cn) + vbNewLine
Next
MsgBox temp
```

Добавление и удаление объекта в группе

Поскольку механизм добавления и удаления членов в группу одинаков, то рассмотрим их вместе.

Алгоритм работы сценария в обоих случаях следующий. На первом этапе с помощью функции GetObject() получают доступ к группе. Затем, вызывая функцию, аргумент которой составное имя группы или учетной записи, осуществляют требуемое действие, причем вызывать setInfo() для записи данных в каталог Active Directory не нужно.

Для добавления учетной записи используется функция Add (см. **листинг 4а**), а для удаления – Remove (см. **листинг 4б**).

Листинг 4а. Добавление объектов в группу

```
path = …
objPath=…
Set objGroup = GetObject("LDAP:// " & path)
objGroup.Add("LDAP:// " & objPath)
```

Листинг 4б. Удаление объектов из группы

```
path = …
objPath=…
Set objGroup = GetObject("LDAP:// " & path)
objGroup.Remove("LDAP:// " & objPath)
```

Заключение

Практическая ценность использования групп безопасности заключается в том, что на основе членства в группе пользователю можно предоставлять определенный администратором набор сервисов, причем независимо от рабочей станции, на которой работает пользователь. Широкое применение эта идея нашла в сценариях регистрации пользователей в сети.

Надеюсь, эта статья поможет автоматизировать некоторые процессы в вашей сети.

1. Object Naming – http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/distrib/dsbb_act_kjpw.mspx?mfr=true.

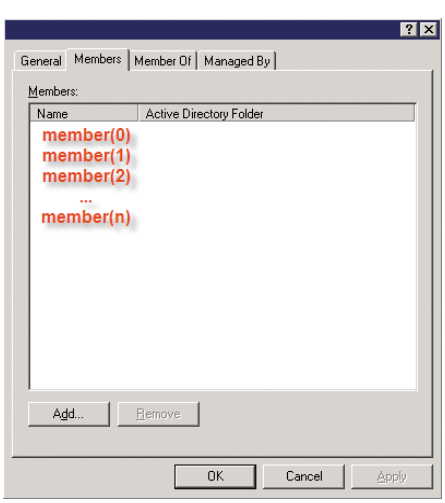
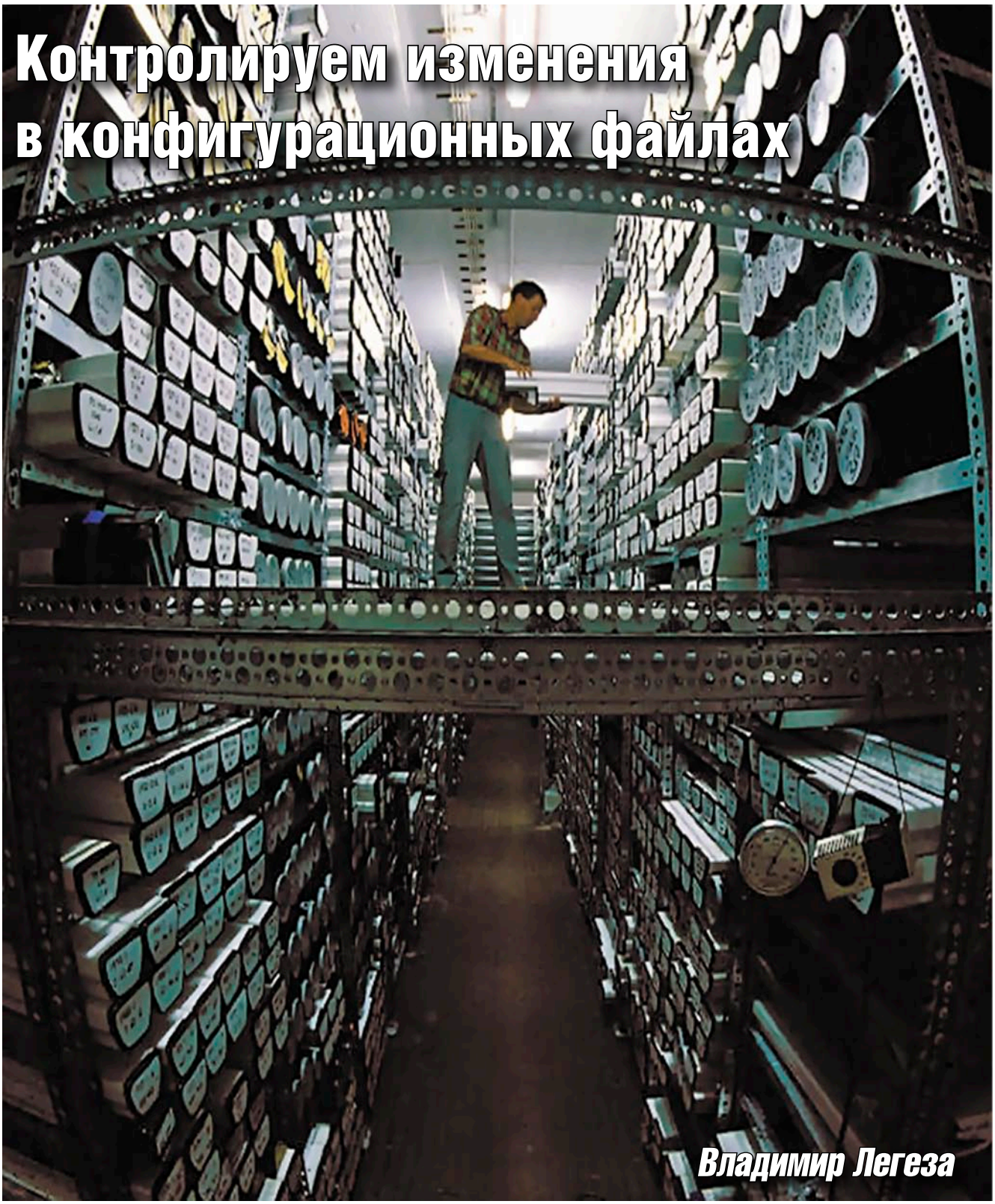


Рисунок 3. Вкладка Members свойств группы безопасности

Контролируем изменения в конфигурационных файлах



Владимир Легеза

Многие системные администраторы хорошо знакомы с трудоемким процессом «ручного исправления» конфигурационных файлов. Да, вполне можно себе представить ситуацию, когда несколько администраторов ежедневно исправляют сотни конфигурационных файлов на десятках серверов. Расскажу о наиболее сложных проблемах, с которыми приходится сталкиваться, и о том, как с ними бороться.

Одна из классических проблем, с которой я часто встречался на практике, является самой распространенной и звучит так:

- **«Только что работало, а сейчас не хочет»** – возникает, как правило, когда во время редактирования случайно было задето что-то лишнее. Например, удалены несколько строк. Если эта оплошность не внесла нарушения в синтаксис файла, то устранить ее можно будет только после того, как станет известно «что» и «где» перестало работать. В другом примере, приложение не обладает встроенным контролем синтаксиса файла конфигурации, и отыскать несколько символов, по той или иной причине оказавшихся в неположенном месте, – задача не из легких. Особенно если в файле несколько тысяч строк.
- **«Я его случайно удалил!»** – другая проблема, чуть менее распространенная, но не менее неприятная. Вам повезло, и у вас есть бэкап! Но радоваться рано – еще предстоит вспомнить и воссоздать модификации, которые в бэкап не попали.
- **«Мои изменения куда-то делись! Но я ведь проверял, что они сохранились!»** – достаточно редкое, но весьма грустное явление. Такое зачастую происходит, когда один и тот же файл одновременно редактируется несколькими людьми с разных терминалов.
- **«А правил ли кто-нибудь...»** – когда никто ничего не трогал, но все упало. Файлы правятся не только администраторами, как мы знаем, но и менеджерами пакетов, различными утилитами и так далее. К счастью, проблемы такого класса встречаются не так уж часто.
- **«Откатите, пожалуйста, назад изменения, которые вы делали на прошлой неделе»** – кто-то действительно помнит, как было до этого? И снова бэкап, ленты, сравнение файлов, и т. д.

Все эти трудности связаны с тем, что мы хотим знать: кем, когда, что и как изменилось или изменяется в настоящий момент, а также помнить историю изменений.

Теория

На все вопросы «кем, когда, что и как» нам дает ответ любая система контроля версий. С ее помощью можно видеть все вносимые изменения, а также историю о том, кем и когда они были сделаны. И многое другое.

Система контроля конфигурационных файлов состоит из двух частей.

- **Репозитарий.** Внутри репозитария хранится вся история изменений со всей сопутствующей информацией.
- **Файлы.** Назовем их «последней версией, извлеченной из репозитария». Это те самые файлы, которые непосредственно используются приложениями (такими как Apache, Bind и т. д.). Содержимое каждого из них идентично последней версии, находящейся в репозитарии.

Основной принцип сводится к тому, что после каждого изменения конфигурационного файла его новый вариант сохраняется в репозитарии.

На сегодняшний день системы контроля версий сменили третье поколение:

- **Локальные** – системы способны контролировать отдельные файлы, каждый из которых обладает собственным файлом репозитария. Представителем этого класса является RCS (Revision Control System). Это первая в истории система контроля версий с открытым кодом, созданная еще в середине 80-х годов. Несмотря на свой возраст, она по-прежнему «широко используется в узких кругах».
- **Централизованные** – отличительной особенностью является способность хранить несколько файлов и каталогов в одном репозитарии, который может находиться удаленно. Это завоевавшие сердца миллионов CVS (Concurrent Versions System) и позднее пришедшая ей на смену SVN (Subversion).
- **Децентрализованные системы** – принципиально новый подход в решении задач версионности. В последнее время они все чаще начинают использоваться в проектах с очень внушительным количеством файлов и большими, зачастую территориально разделенными группами разработчиков. Наиболее заметными реализациями с открытым кодом стали GIT (создававшаяся в первую очередь для ведения процесса разработки ядра OS Linux) и Mercurial, появившиеся практически в одно время.

С точки зрения инструмента для работы с конфигурационными файлами основное отличие между всеми этими системами в большей степени заключается в удобстве и простоте использования. К примеру, установка контроля над файлом в системе RCS может быть достигнута всего одной командой. В Mercurial – минимум двумя. А в SVN это может превратиться в настоящую эпопею – если нужный файл имеет десяток вышестоящих в иерархии каталогов, каждый из которых придется последовательно инициализировать в системе.

Функции, позволяющие осуществлять хранение конфигурационных файлов в отдаленных (remote) репозитариях, практически неприменимы. Создание локального репозитария более целесообразно, поскольку в этом случае его функционирование не зависит от работоспособности сторонних систем и обеспечивает доступность данных в случае потери связи с «внешним миром».

Единственный случай, при котором перемещение репозитариев находит свое применение, – это синхронизация конфигурационных файлов нескольких серверов в системах с распределением нагрузки. Несмотря на то что этот способ синхронизации гарантирует идентичность изменений на каждом из серверов, применяется он крайне редко. Связано это с тем, что чаще всего конфигурация синхронизируется теми же средствами, что и основной контент.

Репозитарии

Каждый из репозитариев, созданных в соответствующей системе контроля версий, имеет особенности в механизме инициализации и внутреннем устройстве.

Репозитарий RCS создается отдельно для каждого нового файла и представляет собой файл с одноименным названием и дополнительным суффиксом (*,v), находящийся

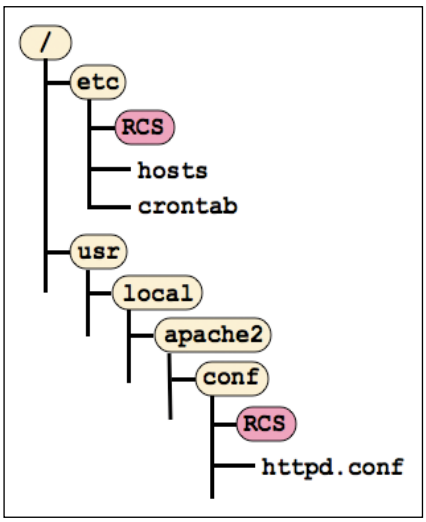


Рисунок 1. Репозитарий RCS

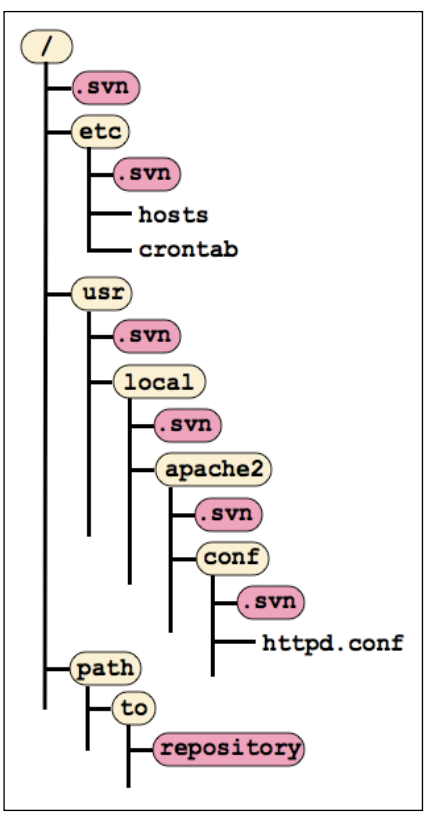


Рисунок 2. Репозитарий Subversion

в том же месте, где и оригинальный файл конфигурации. Ситуацию можно немного улучшить, создав каталог RCS. В этом случае все репозитарии будут создаваться внутри этого каталога. Однако такой каталог должен располагаться непосредственно рядом с оригинальным файлом. Вследствие этого, на каждом из серверов со временем образуется достаточно большое количество таких каталогов, рассредоточенных по всей файловой системе. Пример получившейся структуры каталогов показан на **рис. 1**.

Рассматривая SVN, первое неудобство, с которым сталкиваешься, – необходимость хранить репозитарий отдельно от извлеченной текущей версии файлов. Далее. Каждый извлеченный из репозитария каталог (отдельный файл не может быть добавлен без каталога, в котором находится!) содержит папку с метаданными репозитария (.snv). И этими метаданными ваша система наводняется гораздо сильнее, чем каталогами RCS (см. **рис. 2**).

Самыми элегантными репозитариями, как оказалось, обладают децентрализованные системы. Всего один-единственный каталог в корне репозитария, который содержит в себе «все» (.hg – у Mercurial). Достаточно инициализировать корневой каталог сервера («/») и добавлять столько файлов, сколько потребуется. Никакого дополнительного мусора в системе нет – все в одном месте, в репозитарии (см. **рис. 3**).

Нюансы

Как вы думаете, нужно ли проверять состояние файла до того, как вы начинаете с ним работать? Ответ утвердительный.

Система RCS требует, чтобы перед работой файл был извлечен из репозитария, а после окончания помещен обратно. Если попытаться достать файл из репозитария дважды, будет выведено предупреждение. Но никаких предупреждений мы не увидим, если начнем извлекать файл, измененный до извлечения! Так происходит, например, в ситуациях, когда изменения нужно сделать очень срочно и терять драгоценное время на лишние команды нельзя.

Нюанс заключается в том, что если сразу не довести начатое до конца (сохранить в репозитарий или, как минимум, не заблокировать), то с вероятностью 90% эти изменения будут уничтожены руками ваших коллег. Оставшиеся 10% приходятся на бдительных администраторов, которые первым делом проверяют статус (так как RCS не выводит информацию о наличии изменений, это можно сделать, сравнив текущий файл с последней его версией в репозитарии). Все более поздние системы лишены таких сложностей.

Второй нюанс. Децентрализованные системы ориентированы на работу со всем репозитарием, а не отдельным файлом. Так что одно изменение может затрагивать несколько файлов. Это очень удобно. Нюанс заключается в том, что в ревизию попадают не только измененные файлы, а весь «конфигурационный состав». Абсолютно все контролируемые системой файлы! Это значит, что при извлечении определенной ревизии целиком (checkout) – абсолютно все файлы вернутся к состоянию, соответствующему выбранной ревизии. Такой нюанс требует хорошего понимания механизмов работы репозитария, но не является препятствием к использованию децентрализованных систем. Далее я на примере покажу, как извлечь отдельный файл.

Третий немаловажный нюанс – отсутствие возможности контролировать права доступа к файлам. Это касается как традиционных прав доступа, так и Access Control Lists (ACL – расширение для файловой системы, позволяющее более гибко управлять правами доступа). Подвержены этому все упомянутые ранее системы.

Если описать кратко, единственное, что сохраняется в метаданных о правах доступа, – это является ли файл запускаемым или нет. В остальном все извлекаемые файлы создаются точно так же, как если бы они создавались текстовым редактором. Кроме того, RCS изменяет право на запись в зависимости от состояния блокировки. Запись разрешается, только если файл заблокирован.

Нюанс с правами очень важен, если затрагиваются такие файлы, как /etc/shadow. Эту ситуацию администраторы вынуждены решать собственными силами. Кто-то прибегает к созданию файлов, в которые записывают все права, и добавляют в репозитарий.

Некоторые идут дальше и пишут скрипты для автоматизации процесса. Так на свет появилась утилита etckeeper (http://joey.kitenet.net/code/etckeeper) – созданная любителями дистрибутива Debian для реализации контроля над правами и автоматического перемещения изменений в репозитарий (операция commit) после обновления пакетов в операционной сис-

теме. К радости некоторых администраторов, etckeeper способен работать с Git, Mercurial и Bazar.

В моей практике проблеме с правами уделяется не много внимания, поскольку я стараюсь контролировать версионность исключительно тех файлов, которые действительно в этом нуждаются (файлы типа shadow или group к ним не относятся). Вы можете возразить, но мой аргумент – хорошая система бэкапа, а информация о том, как файл shadow выглядел пару лет назад, не представляет никакого интереса.

Последним нюансом будет отсутствие функционала блокировок у децентрализованных систем. Механизм не вписывается в концепцию децентрализации. К сожалению, даже etckeeper эту проблему не решает.

Кому отдать предпочтение

Вместе со мной в компании работают порядка пяти сотен программистов. Разработка ведется на множестве языков (от PHP и JAVA до C) и для самых разнообразных платформ (от Windows до Solaris и Z/OS). При выборе системы контроля версий в качестве корпоративного стандарта нам хотелось найти систему с открытым кодом, которая могла бы стать единой для всех.

Учитывая то количество проблем и нюансов, которые в моей практике удалось разрешать только при помощи децентрализации (например, с ее помощью удалось избежать остановки процесса разработки в региональных представительствах при длительном отсутствии связи с центральным офисом), вопрос о выборе типа репозитариев даже не рассматривался.

В свете «единой для всех» система должна быть кроссплатформенной. И в этом плане в лидеры вышел Mercurial благодаря наличию клиентов под множество ОС.

Далее Mercurial выделился привычным для пользователей Subversion интерфейсом и хорошей документацией. Это серьезно облегчает переход на новые «рельсы» тем, кто ранее работал с CVS или SVN.

Финальным аккордом стал проект TortoiseHG (http://tortoisehg.sourceforge.net) – клиент для MS Windows, интегрирующийся с Internet Explorer (многие почему-то к нему быстро привыкают).

Единственной преградой на пути интеграции Mercurial для нужд администраторов оставался механизм блокировок, а точнее его отсутствие. Ее удалось обойти «малой кровью» – написав небольшой скрипт, который я назвал hglock (сообразно названиям оригинальным командам системы). Актуальную версию можно скачать по ссылке http://primtech.ru/files/hglock. Возможно, стоит организовать такой функционал в виде дополнительного модуля. Но пока это не было сделано. Позже был добавлен механизм автоматической разблокировки при сохранении изменений в репозитарии. И после этих изменений нам больше ничто не препятствовало.

Нельзя однозначно сказать, какую из систем использовать лучше. Главное, чтобы решалась основная задача – «контроль за изменениями» и «ничего не терялось». А в остальном – это дело привычки или конкретной ситуации. Могу лишь добавить, что чем проще с системой работать, тем меньше шансов наделать ошибок.

Для администраторов, которые раньше не сталкивались с системами контроля версий, а также для небольших организаций, я рекомендую сначала попробовать RCS. Он самый простой как в плане понимания, так и в плане применения.

Интеграция

Для того чтобы описываемый метод работы стал не обузой, а эффективным инструментом, достаточно придерживаться нескольких правил:

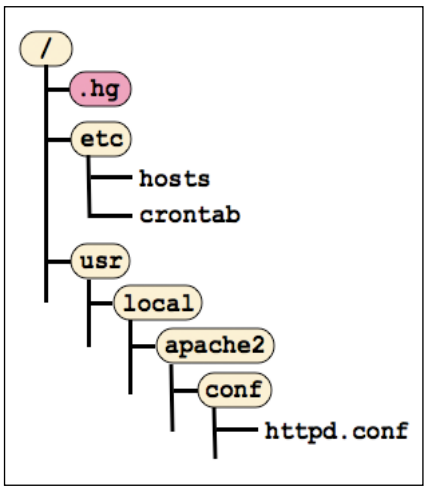


Рисунок 3. Репозитарий Mercurial

Во-первых, система контроля версий должна применяться только к файлам, которые являются уникальными для данной системы и имеют версионную ценность.

Как я уже упоминал ранее, нет необходимости хранить файлы с паролями, группами или сетевыми настройками. Также нет смысла сохранять файлы, которые для большинства серверов идентичны. Например, настройки почтовой маршрутизации или правила авторизации пользователей (PAM, LDAP, SSH...). Сюда же я отношу все файлы, которые всегда прибывают в том состоянии, в каком были установлены вместе с системой. В итоге остается только очень небольшое число файлов, с которыми действительно постоянно приходится работать. Среди них named.conf, nginx.conf, crontab (в компании, где я работаю, рядовым пользователям запрещено самостоятельно создавать записи в cron, это делается администраторами по заявке строго определенной формы), на почтовых серверах – конфигурация почтовых систем, на брандмауэрах (firewall) – непосредственно настройки фильтрации и т. д.

Во-вторых, необходимо, чтобы все администраторы в вашей команде также следовали выбранной методологии.

Другими словами, необходим регламент, описывающий правила работы с конфигурационными файлами.

Для примера успешной интеграции на основе описанных правил могу сказать, что в одной очень крупной компании с помощью RCS команда из шести администраторов управляет конфигурацией приблизительно трехсот UNIX-серверов.

Практика

Практика показывает, что нагляднее всего – несколько простых примеров.

Предполагается, что все задействованные в примере конфигурационные файлы разрешено корректировать только пользователям, обладающим соответствующими привилегиями. Все приведенные ниже команды выполняются с привилегиями суперпользователя (root).

Обращаю ваше внимание на то, откуда берутся имена пользователей, сохраняемые в репозитории. При повышении привилегий пользователя изменяется только «эффективный» (effective id) идентификатор, а «реальный» (real id) остается неизменным. Скрипт hglock использует именно «реальный» идентификатор, то есть имя пользователя (login), использовавшееся при входе в систему. Mercurial же извлекает имя пользователя из переменных окружения, а также позволяет определять его самостоятельно в файле ~/.hgrc. Это означает, что не следует использовать методы повышения привилегий, изменяющие оригинальное окружение (например «su – »). В ином случае авторство будет приписано пользователю root.

Итак, демонстрация работы администратора будет показана на сервере под управлением ОС Solaris.

Прежде всего убедимся в том, что Mercurial установлен и функционирует.

```
$ hg --version
Mercurial Distributed SCM (version 0.9.5)
. . .
```

Несколько предварительных персональных настроек пользователя:

```
$ id
uid=100(john) gid=1(other)

$ echo >~/.hgrc<<EOF
> [ui]
> editor = vim
> fallbackencoding = UTF-8
> username = John Doe <john@example.com>
EOF
```

Повышаем уровень привилегий:

```
$ su
Password:

# id
uid=0(root) gid=0(root)
```

Убедимся, что реальный идентификатор при этом остался неизменным:

```
# who am i
john       pts/2        Nov 20 18:00    (172.30.0.215)
```

Теперь можно создать репозитарий. Так как в нашем примере конфигурационные файлы выходят далеко за рамки /etc, логично будет инициализировать корневой каталог:

```
# hg init /
```

По умолчанию созданный репозитарий доступен для чтения абсолютно всем. В тех случаях, когда планируется поместить в репозитарий файлы, содержащие закрытую информацию (например, ключи ssh), рекомендую применить самый старый и проверенный способ: установить ограничения доступа на уровне файловой системы.

Закроем весь репозитарий от посторонних глаз:

```
# chmod 700 /.gh
# ls -ld /.hg
john       pts/2        Nov 20 18:00    (172.30.0.215)
```

Если возникает необходимость скрыть только определенный файл, права нужно изменять не у репозитария, а у соответствующего файла в каталоге /.hg/store/data . Например, файлу /etc/inet/hosts будет соответствовать файл /.hg/store/data/etc/inet/hosts.i.

Установим скрипт работы с блокировками и внесем соответствующие настройки в репозитарий:

```
# cp hglock /usr/bin/
# cat >>/.hg/hgrc<<EOF

> [hooks]
> port-commit = hglock -C
> post-add = hglock -A
> EOF
```

Если мы попробуем вывести статус репозитария, то вопреки нашим ожиданиям процесс займет несколько минут, а в результате нашему вниманию будет продемонстрирован список абсолютно всех файлов сервера.

Следующая команда решает эту проблему. Она заставляет игнорировать все файлы, о которых нет записей в репозитарии.

```
# echo `^` >/.hgignore
```

Теперь пришло время добавить несколько файлов. Обращаю внимание на то, что в Solaris файл /etc/hosts является символической ссылкой на /etc/inet/hosts.

```
# hg add /etc/inet/hosts
# hg add /usr/local/apache2/conf/httpd.conf
# hg add /var/spool/cron/crontabs/root
```

Посмотрим, как теперь выглядит вывод статуса:

```
# hg status
A etc/inet/hosts
A usr/local/apache2/conf/httpd.conf
A var/spool/cron/crontabs/root
```

Сейчас – в момент добавления файлов – мы можем убедиться, что автоматически установилась блокировка:

```
# cat /.hg/locksfile
```

```
etc/inet/hosts:john:15:47 2008.11.20
usr/local/apache2/conf/httpd.conf:john:15:47 2008.11.20
var/spool/cron/crontabs/root:john:15:47 2008.11.20
```

Хорошо. Помещаем файлы в репозитарий:

```
# hg commit -m "Init"
```

Посмотрим на блокировку теперь:

```
# cat /.hg/locksfile
```

Отлично.

При помощи следующей нехитрой команды в любой момент можно узнать о том, какие из файлов уже находятся в репозитарии:

```
# hg locate
```

```
etc/inet/hosts
usr/local/apache2/conf/httpd.conf
var/spool/cron/crontabs/root
```

Все пути к файлам указываются от корня репозитария. Если сомневаетесь, в каком из репозитариев находитесь, поможет команда:

```
# hg root
```

Все самое сложное позади. Репозитарий настроен, файлы добавлены. Теперь покажу пару несложных команд (по сути, их действительно только две), которые впишутся в вашу повседневную администраторскую жизнь.

Первая команда. Перед тем как изменять /etc/hosts, заблокируем его:

```
# hglock /etc/inet/hosts
```

Если же вас кто-то опередил, вы получите сообщение:

```
# hglock /etc/inet/hosts
```

```
File already locked by "other_user" at 19:00 2008.11.20.
```

Изменим hosts:

```
# cd /etc/inet
# sed -e "s/oldalias/newalias/" hosts > /tmp/1
# mv /tmp/1 hosts
```

Наличие изменений теперь отразится в hg status:

```
# hg status
```

```
M etc/inet/hosts
```

Вторая команда – это нечто иное, как commit.

```
# hg commit -m "first change" /etc/inet/hosts
```

В принципе имя файла можно опустить. Но так как hglock не проверяет, кем заблокирован файл, то есть опасность убрать еще и чужую блокировку.

Давайте рассмотрим еще несколько часто используемых команд.

Кем вносились последние изменения:

```
# cd /etc/inet
# hg log hosts
```

```
changeset:   1:3d8a608232b9
tag:         tip
user:        John Doe <john@example.com>
date:        Thu Nov 20 00:46:46 2008 +0300
summary:     first change

changeset:   0:9fe2667c2ab3
user:        John Doe <john@example.com>
date:        Thu Nov 20 00:44:37 2008 +0300
summary:     Init.
```

Мы видим первую строчку комментария «first change» и номер последней ревизии (changeset) 1.

Давайте посмотрим, что в этой ревизии было нами изменено.

```
# hg diff -r 0 -r 1
```

```
diff -r 9fe2667c2ab3 -r 3d8a608232b9 hosts
--- a/hosts       Thu Nov 20 00:44:37 2008 +0300
+++ b/hosts       Thu Nov 20 00:46:46 2008 +0300
@@ -2,4 +2,4 @@
 # that require network functionality will fail.
 127.0.0.1        localhost.localdomain         localhost
 ::1    localhost6.localdomain6       localhost6
-10.32.0.69 oldalias
+10.32.0.69 newalias
```

Как вы видите, была изменена запись с «10.32.0.69 oldalias» на «10.32.0.69 newalias».

И еще. Скажу о том, как восстановить файл, если его случайно удалили. Потому как путь к его восстановлению не совсем очевиден. Этой же командой можно извлечь только один из файлов указанной ревизии.

```
# rm hosts
# hg log hosts
```

```
changeset:   1:3d8a608232b9
tag:         tip
user:        John Doe <john@example.com>
date:        Thu Nov 20 00:46:46 2008 +0300
summary:     first change

changeset:   0:9fe2667c2ab3
user:        John Doe <john@example.com>
date:        Thu Nov 20 00:44:37 2008 +0300
summary:     Init.
```

```
# hg cat -r 1 hosts > hosts
# cat hosts
```

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1         localhost.localdomain         localhost
::1     localhost6.localdomain6       localhost6
10.32.0.69 newalias
```

Теперь наш файл снова на месте. У нас снова все прекрасно работает. Надеюсь, что теперь и у вас тоже.

nUbuntu

дистрибутив для тестирования защищенности

Сергей Яремчук

Популярный дистрибутив Ubuntu Linux традиционно ассоциируется с простотой в использовании и поэтому в первую очередь рекомендуется начинающим. Но среди его многочисленных клонов имеется специальное решение nUbuntu [1], ориентированное на специалистов.

Выбор решения

Пик популярности специальных дистрибутивов, ориентированных на специалистов в области безопасности, пришелся приблизительно на 2003 год. Как раз в этот период появились первые LiveCD-дистрибутивы, самым ярким представителем которых стал KNOPPIX. Простота сборки своего решения, работа прямо с привода компакт-дисков без предварительной установки на жесткий диск и автоматическая настройка под любое оборудование были оценены как обычными пользователями, так и группами и организациями, в задачу которых входила оценка защищенности сетей и компьютеров.

Как результат, за относительно короткий срок появился целый ряд решений – Whoppix (чуть позже WHAX), KNOPPIX-NSM, PHLAK, Auditor Security Linux, Hakin9 Live и другие. Положительной стороной таких сборок было то, что специалист получал в свои руки готовый инструмент, содержащий весь необходимый софт, который быстро приводился в «боевое» положение.

Минусы, конечно, тоже были. Учитывая количество программ в дистрибутиве, уже через некоторое время сама сборка практически полностью требовала обновления. Это было неудобно как разработчикам, так и пользователям.

Это ли было причиной, но через некоторое время интерес к специальным дистрибутивам стал постепенно угасать.

В результате некоторые проекты практически перестали выпускать обновления (Hakin9 Live) или совсем исчезли, другие проекты объединились. Например, команды Auditor Security Linux и WHAX на основе своих разработок создали довольно неплохой дистрибутив BackTrack [2]. Появились и новые решения вроде Samurai [3], раз-

работка которого сегодня идет весьма активно.

Но как только Linux «научился» нормально загружаться и работать с USB-флеш-устройств и появился целый подкласс небольших сетевых компьютеров – нетбуков, интерес у специалистов к дистрибутивам, предназначенным для проверки безопасности, снова начал расти.

Поиск «своего» решения нужно начинать с сайта securitydistro.com. Назначение большинства представленных там дистрибутивов совпадает, но основа, начинка и, главное, их возможности существенно отличаются. В итоге без подбора нужного решения здесь не обойтись.

Например, задачей BackTrack является обеспечение пользователя инструментами, позволяющими провести тестирование на проникновение (penetration test), и он, кроме многочисленных сетевых сканеров, анализаторов протоколов, сниферов и другого сопутствующего софта, под завязку набит эксплойтами от SecurityFocus, PacketStorm, Metaspl0it Framework 2/3 и другими. Его основой является SLAX.

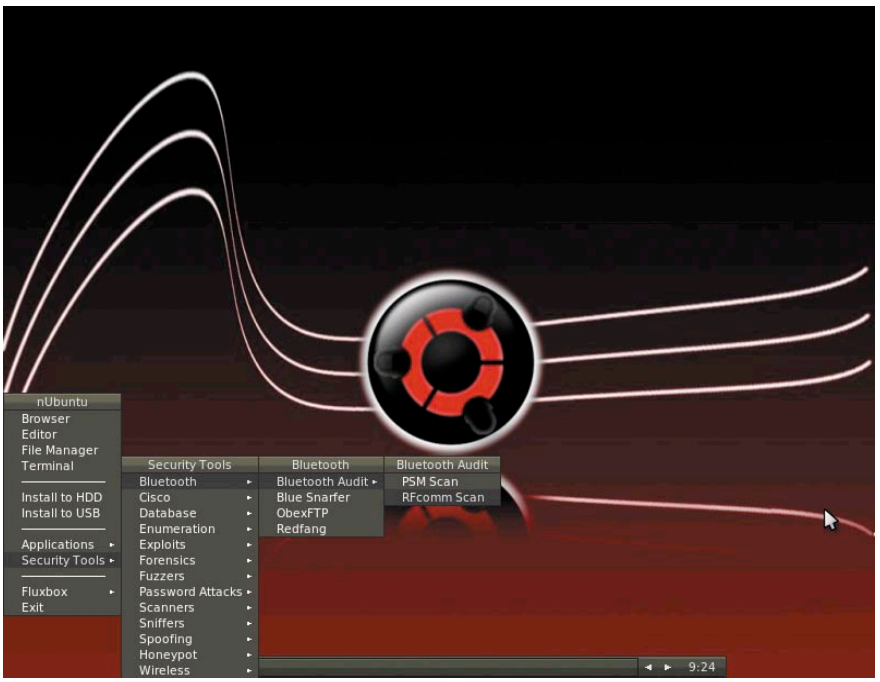
Практически аналогичное назначение – у Samurai, построенного на Debian. Только ориентирован он на web pen-testing environment, то есть тестирование веб-приложений.

Дистрибутив grml [5], также построенный на Debian, предназначен для решения более широкого круга задач – от восстановления системы и редактирования системных файлов до анализа структуры сети.

Не остались в стороне достижения Ubuntu на десктопах. В итоге предложено, как минимум, два решения на его основе – Protech ONE и nUbuntu (Network Ubuntu). Проект Protech ONE после нескольких тестовых релизов представил (в сентябре 2007 года) лишь единственную версию, и о его дальнейшем развитии информации в настоящее время нет.

Дистрибутив nUbuntu

Проект nUbuntu появился в конце декабря 2005 года. Основной его задачей было создание LiveCD-версии набиравшего тогда популярность дистрибутива Ubuntu (в то время он не имел LiveCD-варианта), оснащенного утилитами для тестирования сетей и систем. На распространенный вопрос «Зачем еще один дистрибутив?» разработчики отвечают, что им интересен в первую очередь сам процесс его создания, а использовать результат их работы или нет – это выбор каждого.



Рабочий стол nUbuntu

Первая стабильная версия была анонсирована сразу же после выхода Ubuntu 6.06, с тех пор дистрибутив по мере появления новых версий Ubuntu несколько раз обновлялся. В настоящее время актуальной является Alpha-версия 8.10.

В качестве графической среды в nUbuntu вместо KDE или GNOME использован легкий Fluxbox, плюс убраны все «лишние» приложения вроде OpenOffice.org, почтовые клиенты, игры и так далее. Это позволило уменьшить размер дистрибутива до 430 Мб.

Также стоит отметить, что в отличие от остальных подобных решений интерфейс nUbuntu локализован, хотя и частично. Выбор языка системы производится стандартно для LiveCD Ubuntu – в загрузочном меню. Конечно, отсутствие интерфейса на родном языке не должно останавливать пользователя, на которого рассчитаны специальные дистрибутивы, но такая функциональность лишней не будет.

Тестирование показало, что nUbuntu хорошо себя чувствует на самом разном оборудовании и на виртуальных машинах. Например, сконфигурированный вручную сетевой интерфейс в дистрибутиве BackTrack 3 может запросто «исчезнуть» вне зависимости от виртуальной машины: VirtualBox или VMware.

Запуск LiveCD происходит быстро из-за того, что графическая подсистема по умолчанию не загружается. В процессе обнаруживаются и автоматически настраиваются все устройства, включая проводные и беспроводные сетевые карты.

По окончании в консоли выдается краткий список рекомендаций по дальнейшим действиям. В отличие от большинства решений, все действия в nUbuntu производятся от имени непривилегированного пользователя nubuntu.

Для выполнения задач, требующих прав администратора, используется sudo, что является стандартом в Ubuntu. Хотя при выборе некоторых меню для запуска утилит (Nmap, например) сразу открывается рутовская консоль.

Чтобы загрузить Fluxbox, достаточно набрать «startx».

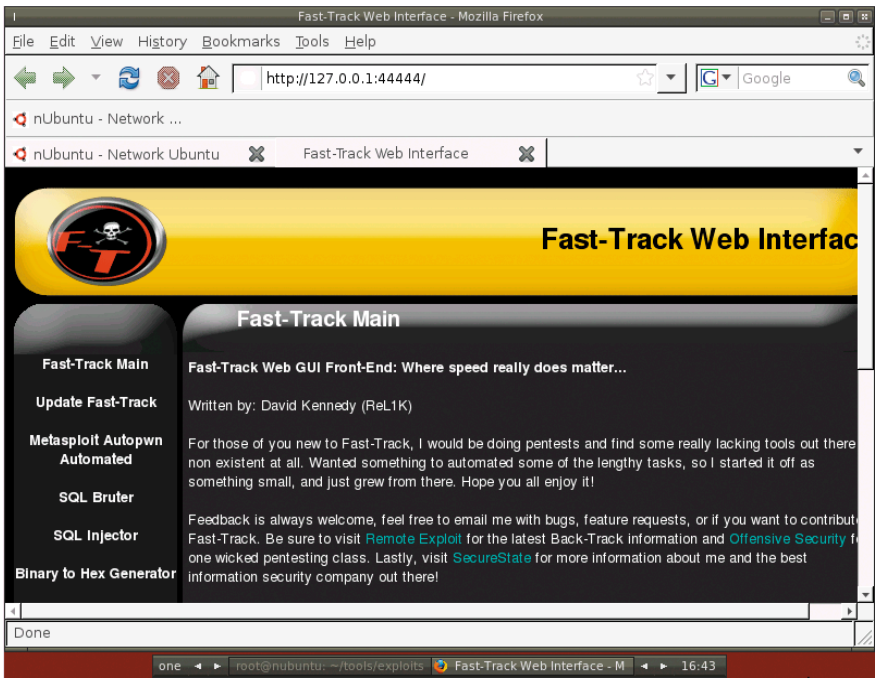
Кроме инструментов безопасности, дистрибутив содержит некоторые стандартные приложения:

- **текстовые редакторы** – VIM, Gvim и GNU/Nano;
- **сетевые приложения** – XChat, irssi, gFTP;
- **клиенты удаленного рабочего стола** – RDesktop и VNC Viewer;

- **файловый менеджер** – Thunar.

Веб-браузер Mozilla Firefox 3.0.3 содержит несколько специфических расширений, позволяющих проверить открытую страницу на наличие уязвимостей или отредактировать заголовки HTTP или Cookies: Access Me, SQL Inject Me, XSS Me, HackBar, Tamper Data, User Agent Switcher и другие. Почему-то не включены в состав популярный файловый менеджер Midnight Commander и консольные веб-браузеры links/lynx.

nUbuntu – дистрибутив для подготовленного пользователя. Каких-либо дополнительных утилит для настройки сервисов или оборудования не предусмотрено, большая часть настроек, если таковые понадобятся, осуществляется правкой конфигурационных файлов.



Веб-интерфейс к FastTrack в nUbuntu

До версии 8.10 программа установки дистрибутива на жесткий диск ubiquity не входила в комплект поставки, теперь ее дополнительно устанавливать не нужно. Ее работа не отличается от аналогичной в Ubuntu. Для установки необходимых приложений можно использовать apt-get. При вызове меню Install то USB появляется ошибка:

```
Could not open /cdrom/.disk/info
Please run this application on a Ubuntu live system|
or mount a Ubuntu live ISO to /cdrom
```

После чего программа прекращает дальнейшую работу. Судя по сообщениям на форуме проекта, эта ошибка уже известна разработчикам и будет исправлена в дальнейших релизах. Поэтому будем надеяться, что установка на флешку не будет вызывать проблем, это только добавит плюсов nUbuntu.

Основной арсенал средств проверки безопасности собран в отдельном меню – Security Tools, в котором насчитывается 13 подпунктов. Большая часть находящихся здесь утилит находится в подкаталоге ~/Tools (его размер 150 Мб), только утилиты, доступные в официальном репозитарии Ubuntu (Nmap, Amap, Wireshark), вызываются из /usr/bin.

Список основных утилит приведен в документе «List of Tools included in nUbuntu 8.10», доступном на WiKi проекта. Здесь есть все что необходимо для проверки сетей и систем:

- **сканеры** – Nmap, Amap, Nessus, Nikto, w3af, wapiti;
- **снифферы** – Ettercap, Wireshark, DSniff, SSHow, MailSnarf, URLSnarf;
- **спуфферы** – ARPSpoof, DNSSpoof;
- **анализ Bluetooth и Wi-Fi** – Bluetooth Audit, Blue Snarfer, ObexFTP, Kismet, Wicrawl, coWPAtty;
- **проверки сервисов на предмет переполнения буфера (fuzzers)** – BED (Bruteforce Exploit Detector), CIRT Fuzzer, ZZUF;
- **Cisco** – Asleap, Cisco Explorer, Cisco Auditing Tools.

А еще инструментарий для взлома и подбора паролей, Honeypot-система Nepenthes, утилиты для поиска уязвимостей в базах данных и так далее.

Работа с эксплойтами в nUbuntu, как мне кажется, организована удобнее по сравнению с BackTrack. В подменю Exploits находим ссылку на Metasploit Framework 3.1, которые можно запускать из командной строки, при помощи веб-интерфейса или обновлять одним нажатием клавиши. Хотя в BackTrack, к слову, есть и GUI к Metasploit, а количество самих эксплойтов больше.

Поиск и обновление эксплойтов лучше производить через пункт Exploit Tree. Запустить скрипт FastTrack, который позволяет произвести автоматическое тестирование системы на наличие уязвимостей (написан хакером ReL1K из SecureState), из меню Fluxbox не удается. Скрипту необходимо задать режим работы, а настройки меню этого не предусматривают. Поэтому необходимо самостоятельно перейти в консоли в каталог ~/tools/exploits/fasttrack и затем вызвать скрипт fast-track.py, указав один из режимов. По мере необходимости будет запрошена загрузка из Интернета дополнительных модулей.

Заключение

Естественно, nUbuntu – дистрибутив, не рассчитанный на широкий круг пользователей, и в отличие от своего прародителя требует некоторого уровня подготовки для его настройки и использования большинства утилит. Специалисты, занимающиеся безопасностью, по достоинству оценят его возможности.

1. Сайт проекта nUbuntu – http://www.nubuntu.org.
2. Сайт проекта BackTrack – http://www.remote-exploit.org/backtrack.html.
3. Сайт проекта Samurai – http://samurai.inguardians.com.
4. Сайт Secur[IT]y Distro – http://securitydistro.com.
5. Сайт проекта grml – http://grml.org.

Lustre FS. Настраиваем и используем кластерную систему в промышленных масштабах

Часть II

Виталий Банковский

Продолжая цикл статей про кластерные системы, представляю следующую тему – повышение отказоустойчивости кластерной файловой системы Lustre.

В первой части статьи (см. №11 за 2008 г.) я описал процедуру установки и настройки кластерной файловой системы Lustre. На данный момент текущая версия ФС Lustre не поддерживает технологий избыточности информации (RAID, replication), поэтому при отключении какого-либо сервера с данными они будут недоступны клиентам.

В этой статье я расскажу, как можно повысить отказоустойчивость системы путем дублирования информации на серверах с данными. Для этого мы воспользуемся двумя известными проектами High-Availability Linux Project (Linux HA) и Distributed Replicated Block Device (DRBD).

Топология системы

Предполагается, что данные каждого сервера будут реплицированы на запасной сервер средствами DRBD. Для прозрачного переключения между серверами будет использоваться пакет Linux HA.

Установка и настройка DRBD

В этом разделе я опишу процесс создания программно-аппаратного комплекса из двух серверов с использованием программы DRBD. Как результат, первый сервер будет находится в режиме Master, второй же будет содержать реплицированные данные с первого сервера.

Установка программы DRBD

В своей работе я использую CentOS, поэтому описание процедуры установки и настройки будет ориентировано на этот дистрибутив. Получаем последнюю версию программы DRBD (на момент написания была доступна версия 8.2.7 с сайта производителя http://www.drbd.org, раскрываем архив и устанавливаем программу:

```
tar -xzvf drbd-8.2.7.tgz
make KDIR=/usr/src/linux
make tools
make install
make install-tools
```

где переменная KDIR указывает на каталог с исходными текстами используемого ядра Linux.

Вышеуказанные шаги нужно произвести на каждом из серверов из пары Master/Slave. Обычно я устанавливаю критические программы из исходных кодов вместо уже собранных пакетов, потому что производители последних часто очень опаздывают с выпуском обновленных версий.

Настройка DRBD

На этом этапе необходимо настроить репликацию данных между серверами oss1-a и oss1-b. Для этого в файл /etc/drbd.conf вносим следующие конфигурационные строки:

```
# Название нашего ресурса (диска)
resource r0 {
# Синхронный протокол репликации
protocol      C;
# Временные настройки
 startup { wfc-timeout 0; degr-wfc-timeout     120; }
# Отключать ресурс в случае сбоя диска
disk { on-io-error detach; }
# Ограничение скорости передачи данных между серверами
# Slave и Master
syncer { rate 10M; }
# Описание подсистемы на oss1-a
on oss1-a1.domain.com {
      # Путь к устройству хранилища DRBD
      device      /dev/drbd1;
      # Путь к физическому диску, где будут храниться
      # метаданные и сами данные сервиса DRBD
      disk        /dev/hda7;
      # IP-адрес первого сервера
      address     10.40.10.10:7791;
      # Указание, где будут храниться метаданные сервиса DRBD.
      # В данном случае я использовал внутренний объем
      # раздела, где хранятся данные.
      meta-disk   internal;
}
}
```

По аналогии создаем описание устройства DRBD в этом же файле для второго сервера oss1-b:

```
on oss1-b.domain.com
{
      device      /dev/drbd1;
      disk        /dev/sda7;
      address     10.40.10.11:7791;
      meta-disk   /internal;
}
```

Копируем этот файл на сервер oss1-b.domain.com в каталог /etc.

Описание ресурсов

Компонент	Описание
oss1-a.domain.com	Имя master-сервера
10.40.10.12/25/eth0	Отказоустойчивый IP-адрес, маска для него и на каком интерфейсе он должен включаться
drbddisk::r0	Drbddisk – скрипт, который расположен в /usr/local/etc/ha.d/resource.d/ r0 – имя ресурса (из настроек DRBD)
Filesystem::/dev/drbd1::/mnt/ost1::lustre	Описание файловой системы. Соответственно: /dev/drbd1 – наше drbd-хранилище /mnt/ost1 – точка монтирования lustre – тип файловой системы

Запуск сервиса DRBD и инициализация хранилищ

Перед инициализацией хранилищ DRBD необходимо запустить сервис drbd на обоих серверах:

```
/etc/init.d/drbd start
```

На каждом сервере необходимо выполнить следующие шаги. Создание блока метаданных:

```
drbdadm create-md r0
```

Подключение раздела для данных к ресурсу:

```
drbdadm attach r0
```

Подключение сервисной части DRBD к ресурсу:

```
drbdadm connect r0
```

Затем запускаем синхронизацию с сервера oss1-a:

```
drbdadm -- --overwrite-data-of-peer primary r0
```

По умолчанию синхронизация может занять несколько дней, если данные не поступают в хранилище. У меня это заняло несколько дней, поэтому для ускорения я применил следующую команду на сервере oss1-a:

```
drbdadm adjust r0
```

Далее проверяем содержимое /proc/drbd, в котором должен быть виден прогресс синхронизации. По завершении репликация сервера oss1-a на oss1-b должна быть в состоянии Primary/Secondary:

```
cat /proc/drbd
version: 8.2.7 (api:88/proto:86-88)
GIT-hash: xxxx build by root@oss1-a1
1: cs:Connected st:Primary/Secondary ds:UpToDate/UpToDate C r---
ns:140 nr:0 dw:668 dr:1186 al:5 bm:15 lo:0 pe:0 ua:0 ap:0 oos:0
```

Форматируем раздел /dev/drbd1 под файловую систему Lustre:

```
mkfs.lustre --reformat --ost --fsname=webstorage ↵
      --mgsnode= mds.domain.com@tcp0 /dev/drbd1
```

В случае возникновения проблем необходимо проверить системные журналы сообщений на предмет ошибок.

Установка и настройка Linux HA

Перед установкой Linux HA необходимо проверить наличие пакетов разработчика: библиотека Perl LibNet, libgcrypt, gnutls, libgpg-error. Описание процесса установки этих пакетов выходит за рамки данной статьи, и я рекомендую обратиться к сопроводительной документации этих пакетов за подробными инструкциями. Также необходимо убедиться, что в ядре включены следующие опции: CONFIG_CONNECTOR (раздел Device Drivers) и CONFIG_CRYPTO_HMAC (раздел Cryptographic options).

Установка Linux HA

Домашняя страница проекта находится по адресу http://linux-ha.org. Загружаем архив последней версии программы Linux HA, раскрываем, проводим конфигурацию, компилируем и устанавливаем:

```
tar -xvf STABLE-2.1.4.tar
cd Heartbeat-STABLE-2-1-STABLE-2.1.4
./ConfigureMe configure
make
make install
```

При этом все настройки будут установлены в каталог /usr/local/etc/ha.d. Добавляем учетную запись пользователя hacluster и группу haclient согласно документации:

```
adduser hacluster
groupadd haclient
```

Небольшое отступление. Когда master-сервер переходит в состояние сбоя, то Linux HA должен смонтировать реплицированный раздел /dev/drbd1 на Slave-сервере в режим Master. Для этого существует скрипт drbd, который входит в поставку программы Linux HA. Его нужно скопировать из каталога scripts в каталог ресурсов Linux HA:

```
cp /usr/src/drbd-8.2.7/scripts/drbddisk ↵
      /usr/local/etc/ha.d/resource.d/
```

Настройка Linux HA

Система настроек Linux HA состоит из трех файлов:

- **ha.cf** – общие настройки;
- **haresources** – настройка ресурсов;
- **authkeys** – файл аутентификации.

Общие настройки

Находятся в файле /usr/local/etc/ha.d/ha.cf. Минимальный набор состоит из следующих строк:

```
# Порт, на котором будут приниматься сообщения от других
# серверов
udpport 694
# Способ оповещения других серверов. В данном случае –
# broadcast через интерфейс etho
bcast eth0
# Не использовать формат XML для настройки ресурсов.
# Использовать текстовый формат настроек
crm no
# Список серверов
node oss1-a.domain.com
node oss1-b.domain.com
# Временные настройки
keepalive 1
deadtime 3
hopfudge 1
# Включение режима failover
auto_failback on
```

```
# Включить использование системного syslog для лог-файлов
use_logd on
```

Настройка ресурсов

Файл /usr/local/etc/ha.d/haresources содержит список ресурсов, которые должны активизироваться на slave-сервере в случае отключения master-сервера. Описание каждого ресурса для типичного случая содержит компоненты:

- имя master-сервера;
- отказоустойчивый адрес-IP;
- описание общей файловой системы;
- список сервисов, которые должны быть запущены на активном сервере (не используются на серверах OSS, так как сервисы обычно запускаются на клиентах ФС Lustre).

В нашем случае строка ресурсов выглядит так:

```
oss1-a.domain.com 10.40.10.12/25/eth0 drbddisk::r0 ↵
      Filesystem::/dev/drbd1::/mnt/ost1::lustre
```

Настройка файла аутентификации authkeys

Этот файл authkeys расположен в /usr/local/etc/had.d/ и содержит описание методов, которые используются для аутентификации сервера Slave на сервере Master и наоборот.

Формат записей следующий:

```
auth 1
1 sha1 your_password_here
```

где:

- 1 – номер ключа, ассоциированный с этой строкой;
- sha1 – метод шифрования;
- your_password_here – сам пароль в открытом виде.

Поддерживаются следующие алгоритмы шифрования:

- **sha1** – SHA1-шифрование (используется ключ);
- **md5** – проверка данных по MD5 (используется ключ);
- **crc** – простая проверка целостности через подсчет контрольной суммы.

Пример такого файла:

```
auth 1
1 md5 my_god_password_nobody_will_know
```

Также нужно сделать, чтобы файл с паролями был доступен для чтения только системному пользователю root:

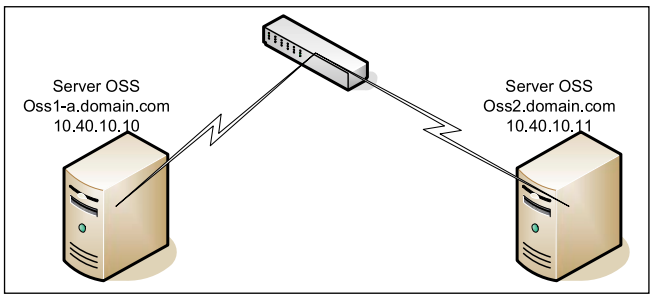
```
chmod 600 /etc/ha.d/authkeys
```

Запуск и тестирование подсистемы Linux HA

После того как все настроено, можно перейти к запуску и тестированию всей системы. Последовательно запускаем Linux HA на сервере oss1-a и oss1-b:

```
/etc/init.d/heartbeat start
```

По истечении нескольких секунд на сервере можно будет увидеть, что сервис Linux HA смонтировал раздел /dev/drbd1 на точку монтирования /mnt/ost1:



Топология системы

```
mount | grep drbd
/dev/drbd1 on /mnt/ost1 type lustre (rw)
```

Соответственно на сервере MDS в лог-файлах можно увидеть следующую строку:

```
Connection restored to service webstor-webstorage using nid xx.xx.xx.xx@tcp.
```

где 10.40.10.12 – наш отказоустойчивый адрес IP (смотрите **таблицу**).

Тестирование Failover

Выключаем сервер oss1-a, ждем несколько минут и проверяем сервер oss1-b. Если все правильно настроено, то можем обнаружить, что наш «плавающий» IP появился на этом сервере. Также сервис DRBD находится в состоянии Master, и что файловая система Lustre смонтирована:

```
mount | grep drbd
/dev/drbd1 on /mnt/ost1 type lustre (rw)
```

Проверяем лог-файл на сервере MDS и обнаруживаем следующую строку:

```
Lustre: : Connection restored to service
webstorage-OST0001 using nid 10.40.10.12@tcp.
```

Что означает, что сервер MDS удачно смог восстановить соединения с сервером OSS.

Примечание. В Linux HA есть механизм под названием STONITH, который может быть использован для принудительного выключения сбойного сервера. Этот механизм обычно используется в системах с совместным доступом к общему ресурсу, например Serial Attached Network (SAN). Но в данном случае каждый сервер имеет собственное хранилище, поэтому механизм не используется.

Финальные шаги

Если все нормально было настроено и все работает как ожидалось, необходимо включить загрузку программ DRBD и Linux HA в процедуру запуска сервера. Для этого на обоих серверах выполняем следующие команды:

```
chkconfig drbd on
chkconfig heartbeat on
```

Теперь все.

1. http://wiki.lustre.org.
2. http://gazette.linux.ru.net/rus/articles/clusters.html.
3. http://xgu.ru/wiki/DRBD.

Квартет: «САМО», «1С», wine и Etersoft

Сергей Барановский

Если проблемы миграции «САМО-Тур» под Linux постепенно исчезают, то с запуском «1С:Предприятие 7.7» пришлось изрядно повозиться. Запуск программы – это половина проблемы, гораздо важнее организация гибко настраиваемого экспорта данных. В этом вопросе разработчики не шли и не идут навстречу пользователям, желающим применять Open Source ПО в связке с программами «1С». Нюансов настолько много, что даже специализированные решения от Etersoft не могут закрыть все пробелы.

На рынке туроператоров наша фирма уже больше года держит «флаг первенства» в переходе на ОС Linux. Несмотря на то что приятно быть первыми, другие компании не решаются на столь отважный шаг. Информация о переходе в других компаниях нашей отрасли мне не известна. Если частичный переход на Open Office осуществили десятки туристических фирм, в том числе и наши партнёры, то малая популярность использования ОС Linux состоит в том, что не все компании могут организовать её грамотную поддержку. Однако когда число компьютеров исчисляется сотнями, даже первичная оценка стоимости покупки различных лицензий и обновления железа отрезвляет.

В процессе перевода «рабочих мест» сотрудников под ОС Linux выяснилось, что для сотрудников нужны не только офис, браузер и почта, но и другие нестандартные приложения, такие как бухгалтерские программы, банк-клиенты, on-line-системы бронирования, системы учёта кадров и пр. Если вначале нам казалось, что камнем преткновения являлась программа «САМО-Тур» и компания «САМО-Софт» недружелюбно к нам относилась, то сейчас, в сравнении с «1С», можно сказать, что мы ошибались. Запустить «САМО-Тур» под Linux удалось [1, 2], а имеющиеся ошибки неспешно исправляются разработчиками, когда мы о них сообщаем. С «1С» возникло больше вопросов, чем ответов. Несколько лет мы не можем добиться помощи, а ответы их технической поддержки похожи на шутку: «Извините, у нас нет туалетной бумаги, зато есть наждачная».

В своей работе для бухгалтерского учёта мы используем версию «1С:Предприятие 7.7» (далее по тексту «1С»). К переходу на версию 8 мы не готовы, так как за десятилетие в версию 7.7 было внесено столько исправлений различными программистами, что «голая» восьмёрка нам никак не подойдёт, а дорабатывать её накладно. Предполагаю, что на рынке ситуация аналогична: фирмы, работающие с программой более 8-10 лет, полностью адаптировали её под свои нужны и не видят смысла в лишних затратах на обновление. Поэтому наш опыт запуска «1С:Предприятие 7.7» может пригодиться читателям.

«1С:Предприятие 7.7» под Linux

На форумах много информации о запуске «1С» под Linux, но мало информации о работе сетевой версии. Поэтому что-то будет неизбежным повторением ранее придуманных решений, а что-то окажется новым. Установка будет производиться в ОС Linux Fedora 8. Попутно будут небольшие замечания о работе «САМО-Тур», так как изначальной целью установки была работа двух этих приложений под ОС Linux.

Первым делом ставим wine, на сегодня последняя версия доступная через yum 1.1.9.

```
# yum install wine
```

В результате ставится 11 пакетов:

```
================================================================================
 Package            Арх.       Версия            Repository            Size
================================================================================
Installing:
 wine               i386       1.1.9-2.fc8       updates-newkey        23 k
Installing for dependencies:
 wine-capi          i386       1.1.9-2.fc8       updates-newkey        27 k
```

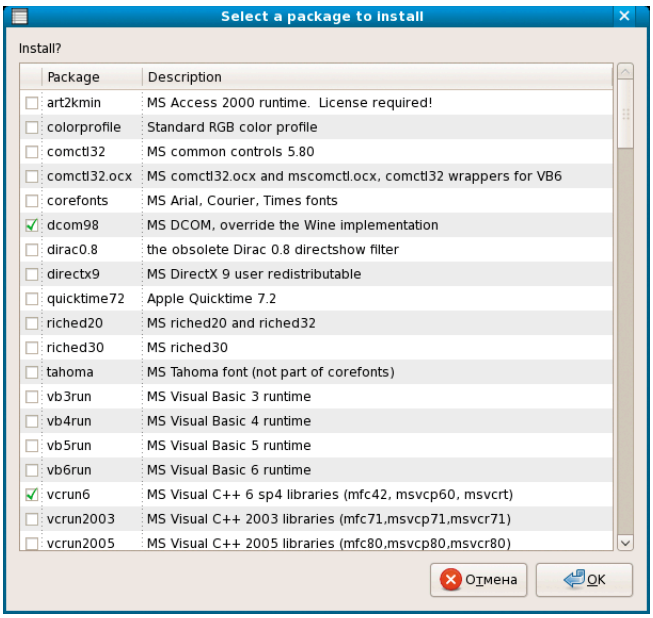


Рисунок 1. Выбор пакетов для установки с помощью winetricks

```
 wine-cms           i386       1.1.9-2.fc8       updates-newkey        42 k
 wine-core          i386       1.1.9-2.fc8       updates-newkey        11 M
 wine-desktop       i386       1.1.9-2.fc8       updates-newkey        26 k
 wine-esd           i386       1.1.9-2.fc8       updates-newkey        37 k
 wine-jack          i386       1.1.9-2.fc8       updates-newkey        39 k
 wine-ldap          i386       1.1.9-2.fc8       updates-newkey        91 k
 wine-nas           i386       1.1.9-2.fc8       updates-newkey        25 k
 wine-tools         i386       1.1.9-2.fc8       updates-newkey       626 k
 wine-twain         i386       1.1.9-2.fc8       updates-newkey        48 k

Transaction Summary
================================================================================
Install      11 Package(s)
```

Программа «1С:Предприятие» успешно ставится без каких-либо проблем, но запускаться и работать не хочет. При запуске в консоли получаем следующие сообщения:

```
$ pwd
/home/labirint/.wine/drive_c/Program Files/1Cv77/BIN
$ wine ./1cv7s.exe
err:module:import_dll Library MFC42.DLL (which is needed by
L"C:\\Program Files\\1Cv77\\BIN\\Type32.dll") not found
err:module:import_dll Library Type32.dll (which is needed by
L"C:\\Program Files\\1Cv77\\BIN\\Frame.dll") not found
err:module:import_dll Library MFC42.DLL (which is needed by
L"C:\\Program Files\\1Cv77\\BIN\\Frame.dll") not found
err:module:import_dll Library Frame.dll (which is needed by
L"C:\\Program Files\\1Cv77\\BIN\\1cv7s.exe") not found
...
err:module:import_dll Library MFC42.DLL (which is needed by
L"C:\\Program Files\\1Cv77\\BIN\\1cv7s.exe") not found
err:module:LdrInitializeThunk Main exe initialization for
L"C:\\Program Files\\1Cv77\\BIN\\1cv7s.exe" failed, status c0000135
```

Из сообщений видно, что программе явно не хватает MFC42. Удобнее всего установить библиотеки и другие пакеты, воспользовавшись утилитой winetricks [3]. Для этого скачиваем программу и запускаем:

```
$ wget http://kegel.com/wine/winetricks
$ sh ./winetricks
```

Замечание: вполне возможно, вам понадобится установить cabextract, например, через команду:

```
yum install cabextrac t
```

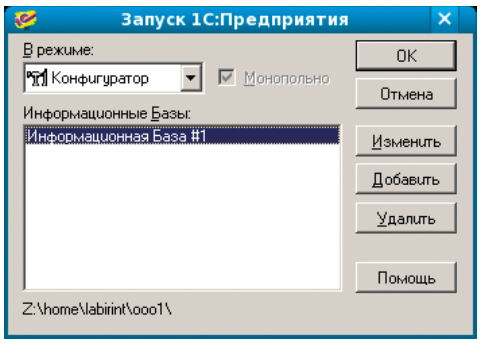


Рисунок 2. Окно запуска «1С» в режиме конфигуратора

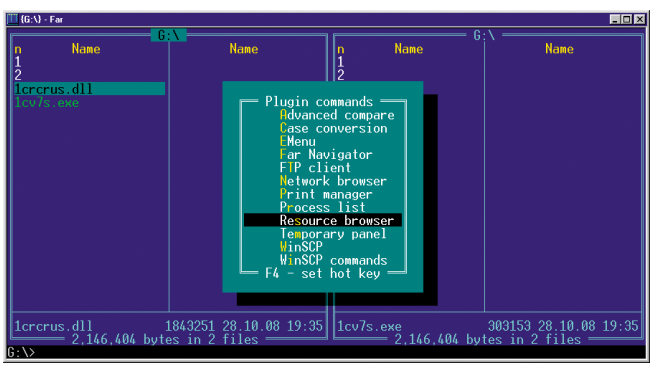


Рисунок 3. Выбираем расширение Resource Browser

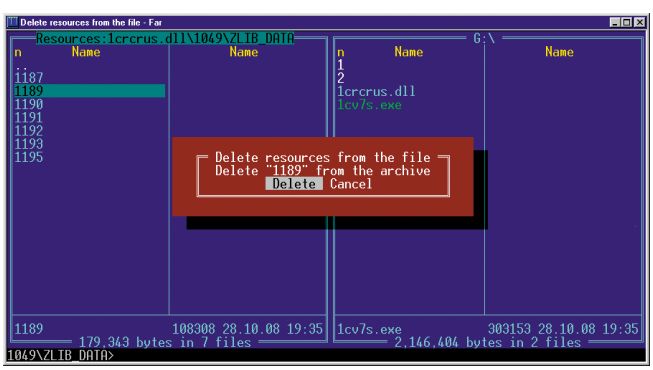


Рисунок 4. Удаляем ресурс 1049\ZLIB_DATA\1189 с помощью Resource Browser

Если не указать параметры, то в консоли появляются различные сообщения, а далее выскакивает графическое окошко, где следует выбрать пакеты для установки (см. **рис. 1**).

Выбираем dcom98 и vcrun6 и нажимаем кнопку «OK». Далее выскочит окно с запросом на установку библиотек DCOM98, отвечаем «Да».

Замечание: несмотря на то что для установки DCOM98 не требуется подтверждение прочтения лицензии, ознакомиться с ней можно тут: http://www.microsoft.com/com/dcom/dcom98/eula.asp, откуда следует, что у вас должна быть лицензия на Windows98. При желании можно обойтись и без использования DCOM98, например с помощью Wine@Etersoft, подробнее читайте далее.

В процессе установки в консоли проскакивают различные сообщения:

```
$ sh ./winetricks
Gtk-Message: (for origin information, set GTK_DEBUG): failed to
retrieve property `GtkTreeView::odd-row-color' of type `GdkColor'
from rc file value "((GString*) 0x9c594a0)" of type `GString'
Setting Windows version to win98
Executing wine regedit /home/labirint/.wine/drive_c/winetrickstmp/
set-winver.reg
Executing wine /home/labirint/.winetrickscache/DCOM98.EXE
fixme:setupapi:SETUPX_CreateStandardLDDs LDID_SRCPATH: what exactly
do we have to do here ?
fixme:setupapi:GenInstall16 unsupported flag: GENINSTALL_DO_REGSRCPATH
fixme:setupapi:vcpUICallbackProc16 (0x5a60, 0705, 0000, 00000000,
003452ac) - semi-stub
...
fixme:setupapi:GenInstall16 unsupported flag: GENINSTALL_DO_CFGAUTO
fixme:rpc:DllRegisterServer (): stub
Using native,builtin override for following DLLs: ole32 oleaut32
rpcrt4
Executing wine regedit /home/labirint/.wine/drive_c/winetrickstmp/
override-dll.reg
Using builtin override for following DLLs when running services.exe:
ole32 oleaut32 rpcrt4
...
Clearing Windows version back to default
Executing wine regedit /home/labirint/.wine/drive_c/winetrickstmp/
unset-winver.reg
Install of dcom98 done
fixme:setupapi:SetupDefaultQueueCallbackW notification 262144 params
32f9ac,0
err:setupapi:SetupDefaultQueueCallbackW copy error 0 L"C:\\windows\\
temp\\IXP001.TMP\\comcat.dll" -> L"C:\\windows\\system32\\comcat.dll"
Executing cabextract /home/labirint/.winetrickscache/vcredist.exe
Extracting cabinet: /home/labirint/.winetrickscache/vcredist.exe
  extracting VCRedist.inf
  extracting PreSetup.exe
  extracting 50comupd.exe
  extracting asycfilt.dll
  extracting atla.dll
  extracting comcat.dll
  extracting mfc42.dll
  extracting mfc42u.dll
  extracting msvcirt.dll
  extracting msvcp60.dll
  extracting msvcrt.dll
  extracting oleaut32.dll
  extracting olepro32.dll
  extracting stdole2.tlb
  extracting atlu.dll
  extracting ADVPACK.DLL
  extracting W95INF32.DLL
  extracting W95INF16.DLL

All done, no errors.
Install of vcrun6 done
winetricks done.
```

Из директории ~/.wine/drive_c/Program Files/1Cv77/BIN запускаем ещё раз «1С».

```
$ wine ./1cv7s.exe
```

Программа запускается, мы нажимаем кнопку «Добавить», выбираем директорию, где находится база, и запускаем её в режиме конфигуратора (см. **рис. 2**).

Начинается запуск, и система зависает на заставке. Опытным путём удалось установить, что зависание происходит потому, что окно входа в систему (для ввода логина и пароля) находится под заставкой, поэтому наша следующая задача либо поменять их местами, либо отключить заставку.

Поиск по форумам привёл к различным решениям [4, 5] – от указания ключа no_splash_show, до внесения правки в exe-файл. Предложенные патчи и подходы не подошли, зато было найдено другое работающее решение, а именно, с помощью внесения исправления в одну из библиотек. Для этих целей можно использовать, например, утилиту Resource Hacker [15] или файловый менеджер Far [6] с расширением Resource Browser [7].

Для этого создаём директорию, например resource_browser в директории %System Drive%\Program Files\Far\Plugins и помещаем туда файлы из архива frb100b5.zip [7].

Перезапускаем Far, ставим курсор на файл 1crcrus.dll и жмём <F11>, выбираем расширение Resource Browser (см. **рис. 3**) и заходим внутрь файла.

Далее можно удалить ресурс 1049\ZLIB_DATA\1189 (см. **рис. 4**). Это и есть стартовая заставка «1С», сжатая архиватором ZIP.

Замечание: приобретённый и используемый нами дистрибутив «1С:Предприятие 7.7. Бухгалтерский учёт. Типовая конфигурация» лицензионным соглашением, где бы запрещалось или разрешалось модифицировать библиотеки для собственных целей, на момент приобретения не комплектовался. На сайте www.1c.ru найти информацию не удалось. По телефону в ответ на вопрос о лицензионном соглашении подтвердили отсутствие лицензионного соглашения для данного продукта. Выгоды из предлагаемого решения мы не получаем, авторские права фирмы «1С» мы не нарушаем. Так как журнал может быть прочитан за пределами РФ, ответственность за соблюдение местных законов лежит на читателях. Вариантом другого решения может быть использование Wine@Etersoft.

После удаления заставки повторяем запуск в режиме конфигуратора. Заставка не появляется, а через некоторое время мы видим окно входа в систему.

После ввода правильных аутентификационных данных мы попадаем в программу «1С» в режиме конфигуратора, где необходимо убрать галочку «Окна → Панель окон → Показать» (см. **рис. 5**), так как нижняя панель некорректно работает под wine и приводит к закрытию всего приложения при обычном запуске.

Если у вас не используется SQL-сервер или сетевое хранение данных, то на этом настройка системы закончена. Можно перегрузиться в пользовательском режиме и работать.

Продолжение настройки для работы с SQL-сервером

Если у вас более сложная конфигурация и используется SQL-сервер, то его необходимо прописать в «1С». Для этого заходим в «Администрирование → Параметры базы данных SQL...» (см. **рис. 6**), появляется окно, где вводим адрес SQL-сервера, имя базы данных, имя пользователя и пароль (см. **рис. 7**).

После этого выходим из конфигуратора и настраиваем сетевую папку для базы. В нашем случае это CIFS-ресурс на компьютере 192.168.0.1.

Прописываем в файле /etc/fstab:

```
//192.168.0.1/base_1c   /base_1c   cifs   ↵
   auto,rw,username=1c,password=xxx,uid=500,gid=500   0 0
```

500 – это UID пользователя, от которого будет осуществляться запуск «1С». Узнать его можно либо с помощью команды id, или посмотрев файл /etc/passwd.

Запустив команду mount, убеждаемся, что ресурс примонтирован:

```
#mount | grep 1c
```

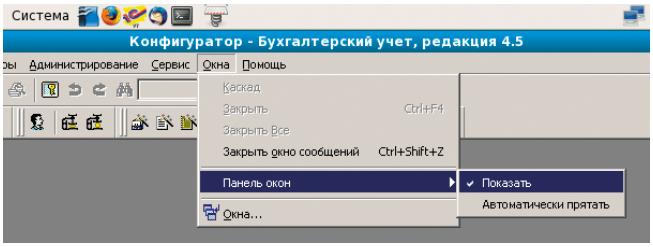


Рисунок 5. Убираем галочку «Окна → Панель окон → Показать»

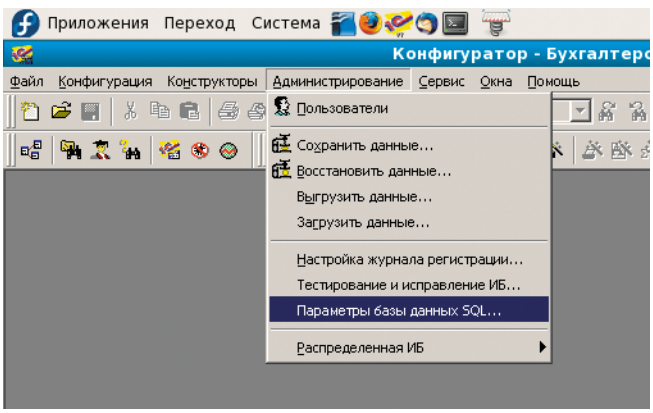


Рисунок 6. «Администрирование → Параметры базы данных SQL...»

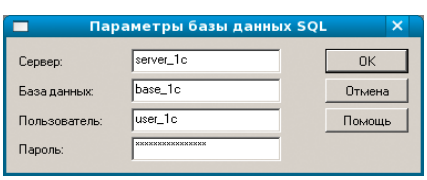


Рисунок 7. Вводим адрес SQL-сервер, имя базы данных, имя пользователя и пароль

```
...
//192.168.0.1/base_1c on /base_1c type cifs (rw,mand)
```

Читателям придётся поверить на слово, но на практике было установлено, что штатный CIFS-модуль ядра не работает корректно с блокировками, поэтому для успешного запуска «1С» в многопользовательском режиме модуль следует заменить на аналогичный бесплатный – etercifs от фирмы Etersoft [9].

Скачиваем и устанавливаем исходные коды последней версии:

```
$ wget http://updates.etersoft.ru/pub/Etersoft/ ↵
      WINE@Etersoft/1.0.9/CIFS/Fedora/8/ ↵
      etercifs-4.0.0-eter2fedora.noarch.rpm

# rpm -ihv etercifs-4.0.0-eter2fedora.noarch.rpm
Подготовка...      ########################################### [100%]
   1:etercifs      ########################################### [100%]
Etersoft CIFS module...                                       [PASSED]
```

После установки необходимо скомпилировать модуль (подразумевается, что компилятор gcc, необходимые библиотеки и исходные коды с заголовками ядра у вас установлены):

```
# /etc/rc.d/init.d/etercifs build
Building for 2.6.26.6-49.fc8 Linux kernel
(headers in /lib/modules/2.6.26.6-49.fc8/build)
```

```
/usr/bin/gcc
make: Entering directory `/usr/src/kernels/2.6.26.6-49.fc8-i686'
...
make: Leaving directory `/usr/src/kernels/2.6.26.6-49.fc8-i686'
make: Entering directory `/usr/src/kernels/2.6.26.6-49.fc8-i686'
  CC [M]  /tmp/Etercifs.VTDm4513/kernel-source-etercifs-2.6.26-1.53/
cifsfs.o

Building for 2.6.26.6-49.fc8 Linux kernel
(headers in /lib/modules/2.6.26.6-49.fc8/build)
/usr/bin/gcc
make: Entering directory `/usr/src/kernels/2.6.26.6-49.fc8-i686'
make: Leaving directory `/usr/src/kernels/2.6.26.6-49.fc8-i686'
make: Entering directory `/usr/src/kernels/2.6.26.6-49.fc8-i686'
  CC [M]  /tmp/Etercifs.VTDm4513/kernel-source-etercifs-2.6.26-1.53/
cifsfs.o
  CC [M]  /tmp/Etercifs.VTDm4513/kernel-source-etercifs-2.6.26-1.53/
cifssmb.o
...
  CC [M]  /tmp/Etercifs.VTDm4513/kernel-source-etercifs-2.6.26-1.53/
cifs_spnego.o
  CC [M]  /tmp/Etercifs.VTDm4513/kernel-source-etercifs-2.6.26-1.53/
dns_resolve.o
  CC [M]  /tmp/Etercifs.VTDm4513/kernel-source-etercifs-2.6.26-1.53/
cifs_dfs_ref.o
  LD [M]  /tmp/Etercifs.VTDm4513/kernel-source-etercifs-2.6.26-1.53/
etercifs.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /tmp/Etercifs.VTDm4513/kernel-source-etercifs-2.6.26-1.53/
etercifs.mod.o
  LD [M]  /tmp/Etercifs.VTDm4513/kernel-source-etercifs-2.6.26-1.53/
etercifs.ko
make: Leaving directory `/usr/src/kernels/2.6.26.6-49.fc8-i686'
Copying built module to /lib/modules/2.6.26.6-49.fc8/kernel/fs/cifs
```

Замечание: VTDm4513 – случайные символы. Могут быть другими, например AMCk6167 или что-то ещё.

Далее надо отмонтировать сетевую файловую систему для «1С», выгрузить старый модуль cifs, чтобы он не мешал работе etercifs. Если не отмонтировать – будет сообщение об ошибке. Смотрим, какой модуль загружен, и выполняем действия.

```
# lsmod |grep cifs
cifs                  211381  1

# rmmod cifs
ERROR: Module cifs is in use

# umount /base_1c
# rmmod cifs
# /etc/rc.d/init.d/etercifs start
Loading CIFS kernel module...                              [ DONE ]

# lsmod |grep cifs
etercifs              227060  0
```

Как видим, нужный модуль загрузился, поэтому можем примонтировать нашу файловую систему либо все CIFS-файловые системы, указанные в /etc/fstab:

```
# mount -t cifs -a
```

Чтобы нужный модуль использовался после перезагрузки системы, его надо прописать с помощью создания мягких ссылок утилитой chkconfig в директориях соответствующих уровней запуска:

```
# chkconfig etercifs on
```

Для удобства в директории ~/.wine/dosdevices создаём мягкую ссылку, чтобы, например, диск d: под wine был нашей сетевой директорией:

```
$ ln -s /base_1c d:
```

После настраиваем подключения к SQL-серверу, для этого ставим freetds (подробнее см. [1, 2]). В файле /etc/freetds.conf прописываем базу:

```
[Server1c]
        host = 192.168.0.1
        port = 1433
        tds version = 8.0
        client charset = WINDOWS-1251
```

Далее настраиваем unixODBC.

Файл tds.driver.template:

```
[FreeTDS]
Description=FreeTDS for MSSQL
Driver=/usr/lib/libtdsodbc.so.0
```

Файл tds.datasource.template:

```
[serv]
Driver          = FreeTDS
Description             = 1C_base
Trace           = No
Servername              = Server1c
Database                = base_1c
```

После чего мы выполняем с правами администратора установку драйвера:

```
# odbcinst -i -d -f tds.driver.template
```

В результате получим:

```
odbcinst: Driver installed. Usage count increased to 1.
    Target directory is /etc
```

Далее с правами пользователя(!) устанавливаем базу, которая будет работать через драйвер, установленный администратором (root) для всех:

```
$ odbcinst -i -s -f tds.datasource.template
```

Эта команда выполняется «молча».

Замечание: настройка для «САМО-Тур» проходила аналогично, если вы уже ставили драйвер, то повторно устанавливать его не надо. Подключения к базе можно проверить с помощью isql, до запуска «1С». Подробнее смотрите в [1, 2].

В результате в ~/.odbc.ini должна оказаться информация о подключении к SQL-серверу для работы с «1С». Имя сервера мы прописали заведомо как «serv».

Для того чтобы не было ошибок при разрешении имени в IP-адрес во время выполнения программы, на сайте Etersoft и других местах рекомендуют не использовать имена для адреса сервера, а прописывать IP-адрес. Мы же поступим иначе, пропишем соответствие имени и IP в файле /etc/hosts, дописав туда строчку:

```
192.168.0.1          serv
```

Проверить правильность можно командой:

```
$ ping -c3 serv
```

В случае успеха команда ping правильно переведёт имя в IP-адрес и будет посылать ICMP-пакеты по соответствующему IP-адресу.

После всех этих действий можем запустить «1С» из директории ~/.wine/drive_c/Program Files/1Cv77/BIN, выполнив команду:

```
$ wine ./1cv7s.exe
```

Далее прописываем базу на диске d: и нажимаем «OK». Программа начинает грузиться, но после «слетает» с ошибкой:

```
 Call from 0x603f2a90 to unimplemented function odbc32.dll.SQLDriverConnectA,
aborting
wine: Unimplemented function odbc32.dll.SQLDriverConnectA called at address
0x603f2a90 (thread 002d), starting debugger...
Unhandled exception: unimplemented function odbc32.dll.SQLDriverConnectA
called in 32-bit code (0x603f2b12).
Register dump:
 CS:0073 SS:007b DS:007b ES:007b FS:0033 GS:003b
 EIP:603f2b12 ESP:0032f3f0 EBP:0032f454 EFLAGS:00200202(   - 00      - - I1)
 EAX:603dc8e5 EBX:60470820 ECX:00000000 EDX:023fd920
 ESI:023fd920 EDI:7caec710
```

Посмотрев внимательно сообщение, делаем предположение, что надо установить odbc32. Для чего ещё раз запускаем winetricks и ставим MDAC 2.8:

```
$ sh ./winetricks
```

```
Gtk-Message: (for origin information, set GTK_DEBUG): failed to
retrieve property `GtkTreeView::odd-row-color' of type `GdkColor'
from rc file value "((GString*) 0x98eb4a0)" of type `GString'
Using native,builtin override for following DLLs: odbc32 odbccp32
Executing wine regedit /home/labirint/.wine/drive_c/winetrickstmp/
override-dll.reg
Setting Windows version to win98
Executing wine regedit /home/labirint/.wine/drive_c/winetrickstmp/
set-winver.reg
Executing wine /home/labirint/.winetrickscache/mdac28/MDAC_TYP.EXE
err:richedit:ReadStyleSheet ReadStyleSheet: skipping optional
destination
...
```

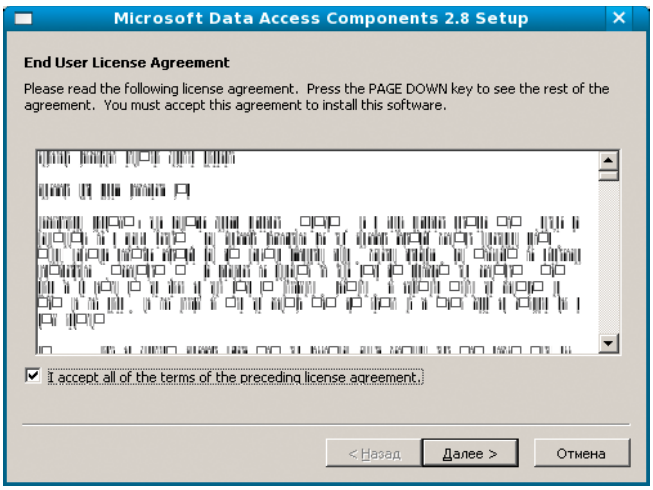


Рисунок 8. Непонятные символы во время установки MDAC 2.8

```
fixme:setupapi:SetupAddInstallSectionToDiskSpaceListA Stub
...
fixme:advpack:set_ldids Need to support changing paths - default
will be used
fixme:setupapi:extract_cabinet_file awful hack: extracting cabinet
"C:\\windows\\temp\\IXP001.TMP\\msvcrt.CAB"
fixme:advpack:set_ldids Need to support changing paths - default
will be used
fixme:setupapi:extract_cabinet_file awful hack: extracting cabinet
"C:\\windows\\temp\\IXP001.TMP\\mtxfiles.CAB"
...
"C:\\windows\\temp\\IXP001.TMP\\SQLOLDB.CAB"
fixme:advpack:set_ldids Need to support changing paths - default
will be used
fixme:setupapi:extract_cabinet_file awful hack: extracting cabinet
"C:\\windows\\temp\\IXP001.TMP\\JETFILES.CAB"
Clearing Windows version back to default
Executing wine regedit /home/labirint/.wine/drive_c/winetrickstmp/
unset-winver.reg
Install of mdac28 done
winetricks done.
```

Во время установки вместо русских и английских букв в окне с лицензионным соглашением будут непонятные символы (см. **рис. 8**). Если согласны, то ставим галочку (I accept...) и продолжаем установку.

Замечание: внутри скачанного файла MDAC_TYP.EXE имеется файл mdaceula.rtf с полным текстом лицензии, внутри которого указано, что «Разрешается установка и использование неограниченного количества копий продукта исключительно для внутреннего пользования в помещениях вашего предприятия». Чтобы знать, с чем вы соглашаетесь, прочитайте файл!

После установки MDAC 2.8 запускаем «1С» ещё раз...и... Ура, «1С» запустилось! (См. **рис. 9**.)

Проверяем, работает ли «САМОТур». К сожалению, после установки MDAC 2.8 – нет, так как нельзя выбрать базу. Поле «Источник ODBC» пустое (см. **рис. 10**).

Проверяем и прописываем заново настройки. В настройках BDE нужно выставить значение параметра SHAREDMEMLOCATION, равное 9000 [14] (см. **рис. 11**).

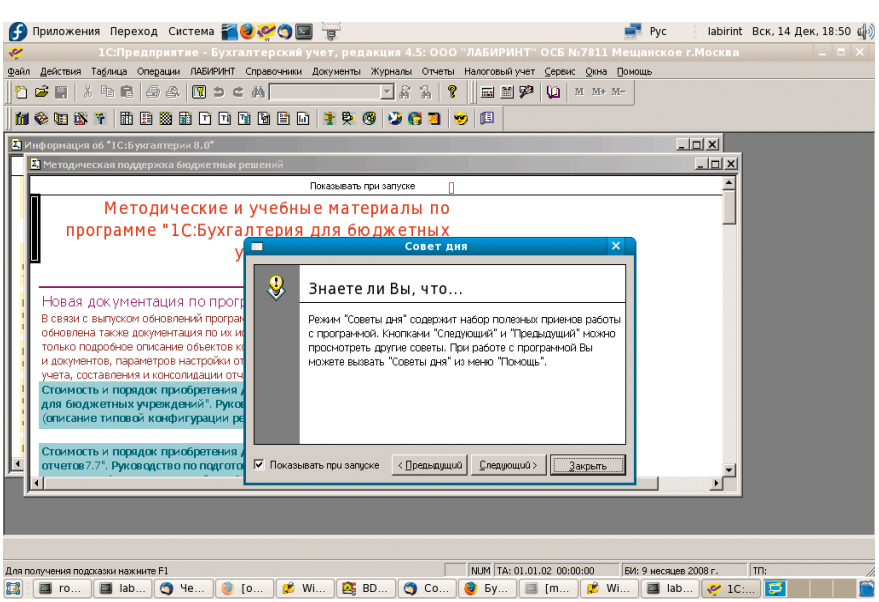


Рисунок 9. «1С:Предприятие» работает под Linux Fedora 8

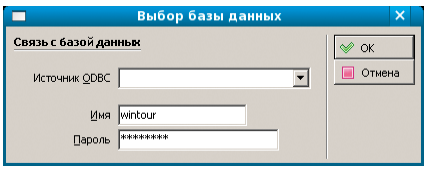


Рисунок 10. После установки MDAC 2.8 невозможно запустить «САМО-Тур» – поле «Источник ODBC» пустое

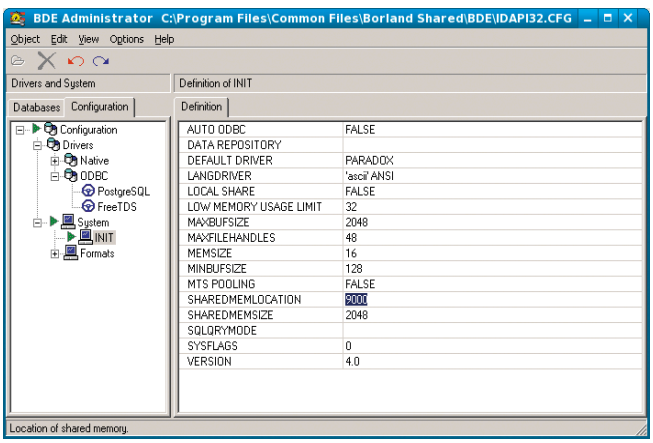


Рисунок 11. Устанавливаем в настройках BDE Administrator значение параметра SHAREDMEMLOCATION, равное 9000

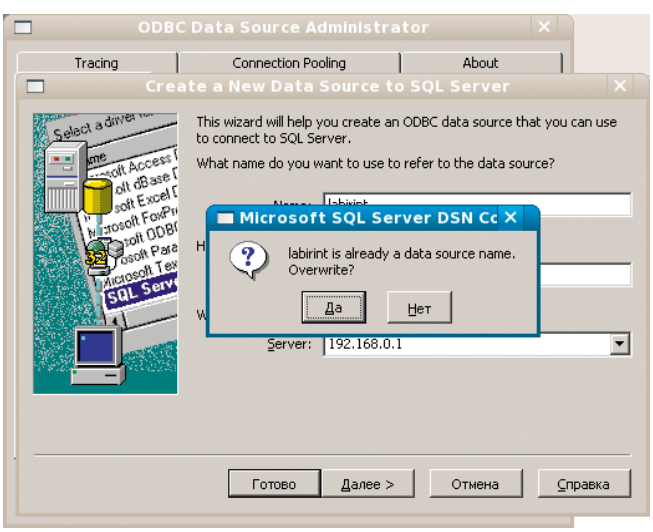


Рисунок 12. Сообщение о том, что база уже существует

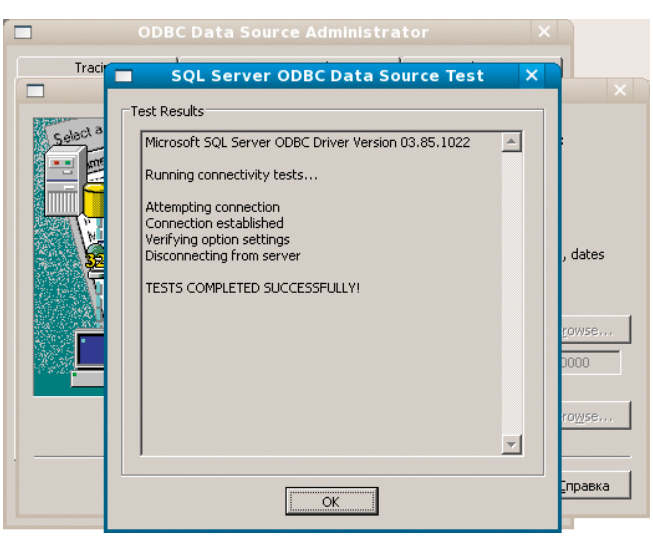


Рисунок 13. Тест базы данных успешно пройден

Далее с помощью C:\Windows\System32\odbcad32.exe прописываем заново базу для «САМО-Тур». Будет сообщение, что такая база уже есть, игнорируем сообщение и вносим все настройки поверх (см. **рис. 12**).

В конце настройки тест источника баз данных должен быть успешно пройден (см. **рис. 13**).

Теперь, когда «САМО-Тур» работает, пробуем запустить «1С» в многопользовательском режиме. Оказывается, что порядок подключения к базе имеет значение.

Если первым к базе подключился пользователь из-под ОС Linux, то его подключение (и возможное последующее отключение) никак не влияют на работу пользователей под ОС Windows.

Если же первым было подключение пользователя, запустившего программу из-под ОС Windows, то зайти в базу «1С» вторым и более пользователем на компьютере с ОС Linux нельзя. Система выдаёт сообщение об ошибке (см. **рис. 14**).

В процессе запуска «1С» под ОС Linux были испробованы разные способы и настройки системы, о своих попытках хотелось бы поведать читателям. Например, были попытки работать через модуль cifs, тогда выдавались другие ошибки, но они были решены переходом на модуль etercifs. Читатель проскочил эту тупиковую ветвь выше.

Как решить проблему запуска «1С» вторым пользователем в многопользовательском режиме под wine 1.1.9 мне пока не ясно, но, видна положительная тенденция в улучшении работы wine.

Например, сейчас не выдается ошибка, и в систему успешно входит и работает хотя бы один пользователь из-под ОС Linux (а после могут работать и другие пользователи из-под Windows), в то время как с предыдущими версиями wine вообще не удавалось запустить «1С», даже в режиме конфигуратора. Выдавалась ошибка (см. **рис. 15**).

Что интересно, эта ошибка привела нас на форум «Этерсофта» [10], где присутствовали интересные ответы, от чего она может возникнуть.

Там советовали проверить, установлена ли коммерческая часть WINE@Etersoft. Это можно было выполнить командой winediag (если такой команды нет, значит, коммерческая часть отсутствует).

WINE@Etersoft SQL

Таким образом, через месяц мучений стало ясно, что перейти на WINE@Etersoft SQL судьба. Мы удалили бесплатный wine и установили новый:

```
# yum remove wine wine-core
...
Removed: wine.i386 0:1.1.9-2.fc8 wine-core.i386 0:1.1.9-2.fc8
Dependency Removed: wine-capi.i386 0:1.1.9-2.fc8 wine-cms.i386
0:1.1.9-2.fc8 wine-desktop.i386 0:1.1.9-2.fc8 wine-esd.i386
0:1.1.9-2.fc8 wine-jack.i386 0:1.1.9-2.fc8 wine-ldap.i386
0:1.1.9-2.fc8 wine-nas.i386 0:1.1.9-2.fc8 wine-tools.i386
0:1.1.9-2.fc8 wine-twain.i386 0:1.1.9-2.fc8
Complete!

# rpm -ihv wine-1.0.9-eter37fedora.i586.rpm ↵
      wine-etersoft-sql-1.0.9-eter15fedora.i586.rpm
libwine-1.0.9-eter37fedora.i586.rpm
Подготовка...      ########################################## [100%]
   1:libwine               ########################### [ 33%]
```

```
groupadd: группа wine существует
groupadd: группа wineadmin существует
   2:wine                  ########################### [ 67%]
WINE: Registering binary handler for Windows program: [ DONE ]
   3:wine-etersoft-sql     ############ ############### [100%]
Running etersafed...                                  [ DONE ]
```

Замечание: в промежутке между удалением старой версии wine и установкой новой директория ~/.wine была вручную удалена.

Как ни странно, но если в ранних версиях WINE@Etersoft SQL были проблемы, то после нашего регулярного общения по почте с «Этерсофтом» версия 1.0.9 научилась запускать и «САМО-Тур».

Программы «1С» и «САМО-Тур» были установлены заново. Настройка «1С» не отличается от указанных выше. Настройка «САМО-Тура» производилась как если бы эта программа ставилась под ОС Windows, то есть ни freetds, ни unixODBC, ни BDE ставить не пришлось. Была прописана база через настройки odbcad32.exe и параметр SHAREDMEMLOCATION (см. **рис. 11**) как в шаге после установки MDAC 2.8.

После обе программы успешно заработали. «1С» в том числе стала заходить на сервер, даже если там уже работают другие пользователи.

Удивительно, но «1С» и «САМО-Тур» работают, в первом случае даже не надо возиться с отключением заставки, окно ввода имени пользователя и пароля отображается правильно. Поставил и работай. Не зря «Этерсофт» специализируется на запуске Windows-приложений под Linux, наверняка «не одну собаку съели».

Несмотря на то, что WINE@Etersoft SQL – коммерческий продукт, от процесса его тестирования и общения с сотрудниками фирмы только положительные впечатления. Может, когда-нибудь они откроют секрет, что надо сделать с обычным wine, чтобы работала SQL-версия «1С». Не очень они любят говорить про бесплатный wine, видимо, есть чем гордиться в их закрытой версии, хотя как вариант можно и не ждать, ведь есть и некоммерческая сборка wine [11]. Работа «1С» под ней нами ещё не тестировалась из-за отсутствия времени, но в случае успеха можно будет сравнить исходные коды и получить ответ уже сейчас, если «1С» заработает.

Вообще это приятно, когда коммерческая фирма берётся развивать некоммерческие проекты, подобно тому как существуют Red Hat и Fedora, а то, что это российская фирма и есть форум на русском языке, вдвойне приятно.

Ошибка экспорта в Word

Но несмотря на оптимизм последнего удачного запуска программы «1С» под ОС Linux, есть и недостатки в её работе. Они не связаны вообще с операционной системой, а скрываются в программе, «1С:Предприятие. Версия 7.7» писалась во времена господства на рынке пиратских версий ОС Windows и MS Office, поэтому она с ними только и работает. Фирма «1С» никак не нацелена на адаптирование своего продукта к OpenOffice или альтернативным почтовым клиентам.

Из хорошего – половина экспортов происходит независимо от наличия пакета MS Office сразу в файлы, которые после можно либо копировать по сети, либо открывать в любой подходящей программе. Подобным образом, через внешний файл работает экспорт и импорт в банк-клиент.

Что же касательно «САМО-Тура», то тут «САМО-Софт» потрудились, написали и продают модуль, работающий напрямую с их БД, правда, работает он только в одну сторону, в другую обмен информацией происходит также через внешний xml-файл.

Некоторые экспорты из «1С» всё же не работают на компьютерах без офиса, так как используется COM-метод обращения к приложениям. Например, если зайти в меню «Журналы → Путёвки» и щёлкнуть на любую путёвку, далее, в окошке шаблон выбрать .dot- или .doc-файл шаблона, а после в печати выбрать пункт «Печать Word» (см. **рис. 16**), то возникает ошибка (см. **рис. 17**).

Радует одно – этим экспортом в нашей фирме пользуется только одна сотрудница. Переводу всех остальных под Linux ничего не мешает.

Но даже и эту ошибку можно попробовать исправить в будущем. Для этого надо воспользоваться проектом unioffice [12]. Эта программа позволяет транслировать запросы (точнее, COM-объекты), направленные к MS Office в запросы к OpenOffice.

Маленькая проблема в том, что сейчас (версия 0.4) транслируются только запросы, направленные к электронным таблицам Excel. Поддержка некоторых, наиболее часто используемых COM-интерфейсов приложения Word планируется в ближайшем будущем. Может, к выходу статьи уже будет реализована. По крайней мере мы уже успели направить свои пожелания в Etersoft, который этим и занимается в свободное от других проектов время.

Чтобы понять, что вызвало ошибку (вам это может тоже понадобиться) и знать, какие методы используются, чтобы послать их разработчикам, в первую очередь надо запустить «1С» в режиме конфигуратора, а далее, находясь в нём, нажать клавишу <F11>, после чего запустится ещё одна копия программы «1С», уже рабочая, где следует повторить все действия, приводящие к ошибке. Далее надо щёлкнуть на красные буковки «err» слева от ошибки, в конфигураторе откроется новое окно, где вы попадёте на участок кода, вызвавший ошибку:

```
Процедура ПоКнопкеВорд()
   Знак = "0";
   Если СокрЛП(ИмяФайла)<>"" Тогда
        Состояние("Выполняется подключение к шаблону ↵
                MS Word...");
        Word=СоздатьОбъект("Word.Application");
        Word.Documents.Add(ИмяФайла);
              Word.Selection.GoTo(-1,,, "ДатаСозданияПутёвки");
        Word.Selection.Delete(2,1);
.....
        Word.Selection.GoTo(-1,,, "Сумма2");
        Word.Selection.Delete(2,1);
```

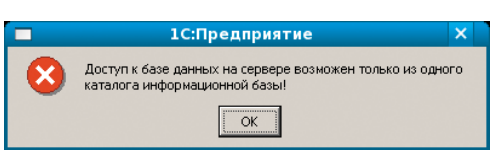


Рисунок 14. Ошибка «1С:Предприятие»

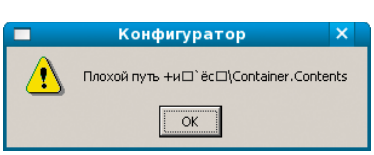


Рисунок 15. Ошибка конфигуратора

```
        Word.Selection.TypeText(Строка(Формат ↵
          (ТурОбслуживание1_ВвалютеКОплате,"Ч15.2,")) + ↵
          "  ");          //Word.Selection.TypeText ↵
          (Строка(ТурОбслуживание1_ВвалютеКОплате) + "  ");
              Word.Visible=1;
    Иначе
        Предупреждение("Укажите имя файла Word !");
    КонецЕсли;
КонецПроцедуры
```

Просмотрев код, можно легко понять, какие COM-интерфейсы были использованы, они идут после последовательности «Word».

Пример решения с почтой

Существует и другая задача, а именно отправка бухгалтерских подтверждений или счетов по почте. Счета удобнее всего выставлять из «1С» нажатием пары кнопок. В этом вопросе фирма «1С» также не удосужилась пойти навстречу клиентам. Для отправки почты существует внешний компонент V7Mail (v7plus.dll), но работать с нужными программами он не хочет. Как не пошли в фирме «1С» нам навстречу два и три года назад, так и не хотят делать это сейчас. Гораздо проще ответить, что: «Работоспособность V7Mail с почтовым клиентом Mozilla Thunderbird не проверялась, поэтому подобных рекомендаций дать не можем.

Компонент V7Mail разработан для работы с почтовыми клиентами Outlook и Outlook Express. Кроме этих клиентов, он может работать с любым MAPI-совместимым почтовым клиентом, который корректно поддерживает спецификацию Simple MAPI».

Хотя все другие программы успешно используют, зарегистрированный по умолчанию клиент Mozilla Thunderbird и используемый MAPI их устраивает.

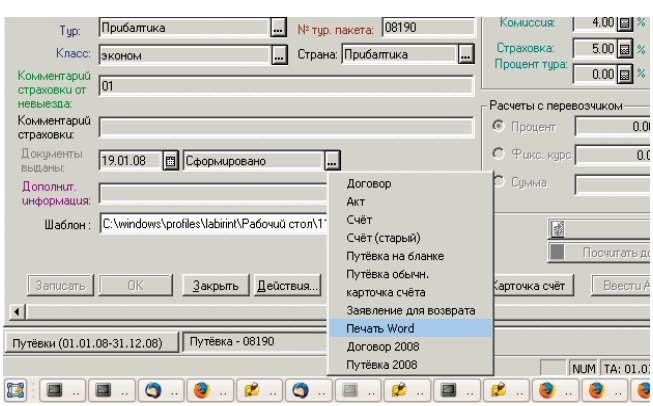


Рисунок 16. Выбираем «Печать Word»

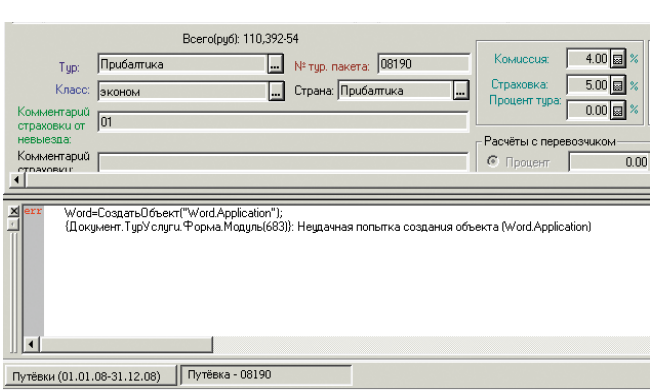


Рисунок 17. Ошибка при экспорте в Word

Эту проблему можно также попытаться обойти, сделав решение для клиентов кроссплатформенным, а именно: вместо V7Mail и MAPI использовать компонент ROM-mail, работающий с протоколом SMTP напрямую.

Для этого придётся немного переписать код в базе «1С», а далее, если надо отслеживать отправленные счета, следует поднять SMTP-прокси, на котором помещать копию отправленных писем в папку Sent, доступ к которой можно организовать на том же сервере по протоколу IMAP, например, с помощью IMAP-сервера Dovecot, при этом пользователи смогут использовать привычный им клиент Mozilla Thunderbird, который не удалось заставить работать первым способом через MAPI.

Сообщения есть, а как «оно» работает многие даже не задумываются. Решение может быть как на базе любого MTA вроде Sendmail, так и в виде небольшой программы на C, использующей файл для сохранения писем и два сокета – один на прослушивание подключений от «1С», а другой для подключения к провайдерскому SMTP-сервису. Скорее, это тема следующей статьи.

Заключение

Несмотря на то, что удалось успешно решить часть проблем по запуску «1С» под Linux, постоянно появляются новые и новые проблемы, не позволяющие нам полностью расслабиться.

1. Барановский С. Как запустить «САМО-Тур» для Windows под Linux. //Системный администратор, №5, май 2008 г. – С. 42-49.
2. Барановский С. Лебедь, рак да щука: «САМО-Софт», wine, Etersoft. //Системный администратор, №9, сентябрь 2008 г. – С. 44-49.
3. Утилита winetricks – http://wiki.winehq.org/winetricks.
4. Как отключить заставку в «1С» – http://www.itland.ru/forum/index.php?showtopic=5223.
5. Как отключить заставку в «1С» – http://forum.windowsfaq.ru/archive/index.php/t-67859.html.
6. Файловый менеджер Far – http://farmanager.com.
7. Resource Browser (позволяет смотреть и редактировать ресурсы EXE- и DLL-файлов) – http://plugring.farmanager.com/downld/files/frb100b5.zip.
8. Убрать галочку «Окна → Панель окон → Показать» – http://forum.ubuntu.ru/index.php?topic=34421.15.
9. Компания «Этерсофт» – http://www.etersoft.ru.
10. Наиболее часто встречающиеся вопросы при использовании WINE@Etersoft – http://www.etersoft.ru/content/view/102/83.
11. Проект по развитию альтернативного свободного репозитория eterwine – http://freesource.info/wiki/WINE, http://winehq.org.ru.
12. UniOffice@Etersoft, транслятор COM-объектов MS Office – http://wiki.etersoft.ru/UniOffice.
13. Способы отправки почты из «1С» – http://love1c.kiev.ua/prog/mail.htm.
14. Тестирование «САМО-Тур» – http://bugs.etersoft.ru/show_bug.cgi?id=1946.
15. Resource Hacker, утилита для просмотра, изменения, добавления, удаления и извлечения ресурсов из 32-разрядных исполняемых файлов – http://www.angusj.com/resourcehacker.

Сдаём бухгалтерскую отчётность в электронном виде

Максим Лобов

В конце прошлого года директору нашей фирмы пришло официальное письмо с исходящим номером и за подписью заместителя начальника инспекции Федеральной налоговой службы, где мы состоим на учёте. В тексте предлагалось прийти на встречу в назначенное время «по вопросу сдачи отчётности через Интернет».

Судя по тексту письма, в ИФНС России №17 по г. Москве решили сделать благое дело и перевести фирмы на сдачу отчётности в электронном виде. По задумке, это должно сулить меньше очередей, оптимизацию процесса сдачи и проверки, в целом подход прогрессивный, учитывая, что столица наиболее компьютеризирована и практически везде есть доступ в Интернет. Однако глобальные планы по строительству светлого будущего были испорчены конечным решением.

Гладко было на бумаге....

Если бы фирмам предложили зайти на сайт (например mosnalog.ru) и заполнить там регистрационную анкету, получить аккаунт, а после через веб-форму сдавать отчётность, то это было бы воспринято всеми на ура и переход был бы гладким и быстрым.

Но так сделано не было – то ли нет хороших специалистов по веб-технологиям в ФНС, то ли думают по другому. Что же было предложено?

Понимая, что передавать государственные секреты между отчитывающейся фирмой и налоговой инспекцией надо в зашифрованном виде, а стандартный протокол https не поддерживает алгоритм шифрования ГОСТ-28147-89, то есть отечественную стойкую криптографию, сертифицировать такое решение никто не будет, а значит, быстрый и удобный механизм сдачи отчётности через веб-интерфейс потерпит фиаско. Никто не хочет оказаться крайним в ситуации, когда на столичных рынках в подполье появятся DVD-диски с налоговой отчётностью различных фирм.

Поэтому были выбраны фирмы, которые получили разрешения и были сертифицированы для передачи конфиденциальных данных по сети как с использованием VPN-решений, так и без. То есть, фактически, образовалось несколько фирм, работникам которых надо также выплачивать зарплату, которые законно занимаются сбором налоговых сведений от фирм по защищённым каналам, подписыванием сданных отчётов или удостоверением легитимности цифровой подписи фирмы и передачей их в ФНС. Бесплат-

Веб-решения и сертифицированная криптография под ОС Linux успешно работают

Что интересно, решения через кроссплатформенные веб-технологии уже имеются и широко используются в банковской сфере. Например, бывший Инвестсбербанк несколько лет предлагал своим клиентам (юридическим лицам) услугу доступа к собственному счёту через веб-интерфейс. Они использовали клиентские Java-апплеты совместно с сертифицированными ФСБ РФ многоплатформенными криптобиблиотеками Агава-С [14]. Там, где кроссплатформенность не предусмотрена разработчиками, фирма Этерсофт на сегодня предлагает поддержку по запуску в ОС Linux более шести различных банк-клиентов: Балтийского банка, Восточно-европейской финансовой корпорации (ВЕФК), Петро-Аэро-Банка, ИнкасБанка, Таврического банка, Межбанковского процессингового центра Faktura.ru, ВТБ24 (шифрование через Inter-Pro v4), ИБанка (Юниаструм Банк), РосЕвроБанка (шифрование через Inter-Pro v4) [15]. Фирма Амикон, работающая со Сбербанк-клиентом, с ноября 2008 года ведёт работы по портированию своего продукта ФПСУ-IP/Клиент под ОС Linux, о чём у нас имеется официальный ответ.

но никто работать не будет, поэтому фирмы за свои услуги требуют деньги. В столице, по традиции, побольше, в регионах поменьше.

Подробности задуманного

Так как по закону нас обязать кому-то что-то платить никто не может, мы решили выяснить более подробно, что же нам предлагают и есть ли в этом для нас выгода.

Для упрощения сдачи отчётности и получения помощи в переходе на новые технологии нам предлагали выбрать одну из четырёх фирм, которая будет нас обслуживать:

- «Контур-Экстерн» [1];
- «Тензор» [2];
- «Гарант-Телеком» [3];
- «Такском» [4].

В целом, вроде и выбор есть, как может показаться, но увы...

Оценка затрат

Подходящий нам тариф обслуживания стоит порядка 9000 рублей в год. За это мы сможем отказаться от услуг нашего курьера, которому надо 14 раз в году перейти дорогу (налоговая практически соседнее здание с нами), постоять в очереди (обычно около часа) и сдать отчётность. Давайте оценим трудозатраты нашего сотрудника. Если предположить, что мы среднему сотруднику платим зарплату 20000 рублей в месяц (курьеры обычно получают меньше, тысяч 10), то это будет в пересчёте на 20 рабочих дней 1000 рублей в день для квалифицированного сотрудника и 500 рублей для курьера. Учитывая, что отчётность сдаётся пару часов – округлим вверх до половины дня, выйдет 7 рабочих дней. То есть получится 7000 рублей, если отчётность будет ходить сдавать бухгалтер или 3500 рублей, если послать курьера. В обоих случаях мы получаем экономию!

В ситуации мирового финансового кризиса руководство требует экономить каждую копейку, поэтому наш выбор очевиден, обойтись своими силами. Экономия небольшая, предположим, что фирмы снизят цены, но тут мы столкнулись с другой проблемой.

Наша бухгалтерия успешно работает под операционной системой Linux, это хорошо сказывается на стабильности работы, позволяет экономить на лицензировании. На вопрос, заданный исполнителю присланного нам документа: «А какое решение, вы, господа налоговики, предлагаете для операционной системы Linux?» мы не услышали ответ и были перенаправлены всё в те же четыре фирмы, со словами, что в технических деталях они не разбираются. Увы, в перечисленных выше фирмах ответить про то, как это будет работать под операционной системой Linux, не смогли. Где-то сразу ответили: «работать не будет», где-то посоветовали использовать эмуляторы или всё же найти средства и купить «Windows-машину». Это означает, что в денежной оценке вопроса прибавится ещё стоимость лицензирования рабочего места, а также мы не учли затраты по трафику.

Наиболее интересный разговор был в СКБ «Контур». С одной стороны, они обещали найти человека, который перепишет программу под Linux за деньги, с другой стороны, когда мы решили узнать точно, сколько это будет стоить, «обещанный» человек не был найден. Желая узнать больше о новой технологии сдачи налоговой отчётности, мы выяснили, что фирма «Тензор» предлагает решение на базе комплекса «Крипто-Про 3.0». На форуме «Крипто-Про» мы нашли тему, где обсуждалась возможность работы этого комплекса под ОС Linux [6]. Что интересно, в этой ветке форума, одна из сотрудниц отдела технического сопровождения компании «Крипто-Про» (судя по подписи под сообщением) предложила потестировать продукт под Linux. То есть задел для того, чтобы обеспечить транспорт данных на канальном уровне из операционной системы Linux в защищённом виде, есть.

А вот дальше, увы, потестировать работу GUI и транспортной программы под ОС Linux с сертифицирующими центрами рекомендованных фирм вряд ли получится. Нет заинтересованности с их стороны.

Вовсю в стране идёт переход на ОС Linux, пилотные проекты успешно отработали в школах [7, 8], появляются новые российские дистрибутивы ОС Linux и успешно сертифицируются ФСТЭК [11], но увы, эти проекты оказываются оторванными от обслуживающей общество инфраструктуры. На 10 февраля 2009 года запланирован семинар «Свободное программное обеспечение в государственном и некоммерческом секторе» при поддержке Российского агентства развития информационного общества [8, 9], но там нет предполагаемых тем докладов о сдаче налоговой отчётности.

Возможно, лет через пять новое поколение школьников и студентов исправит положение, но как быть сейчас, в эпоху кризиса?

Сайт mosnalog.ru

Желая получить больше информации, мы обратились к сайту налоговой инспекции. На присланном нам бланке в шапке документа были указаны адреса: mosnalog.ru и www.mosnalog.ru. Что интересно, первый не отвечает, так как их администраторы просто не прописали это имя на DNS-сервере. Может, поленились, а может, за-

Что мешает использованию криптографических средств под ОС Linux?

Если смотреть глобально на возможные проблемы при работе с криптографическими средствами в ОС Linux, то всё упирается в хранение ключевой информации. Обычно это какое-то внешнее устройство. Если используются однопроводные решения в виде «таблеток» Touch Memory (iButton), то под ОС Linux в ядре реализована поддержка протокола 1-Wire. Если это ключи на USB, то имеется PC/SC. Про дискеты вообще излишне говорить. То есть реально проблем нет, было бы желание разработчиков.

были. Второй, в независимости от географической, принадлежности обращающегося переадресовывает нас на www.r77.nalog.ru. Возможно, была задумка обращающихся перенаправлять к доменам своих регионов, но эксперименты с использованием разных анонимизирующих прокси-серверов дали один и тот же результат.

Попав на сайт, первым делом мы ввели слово Linux в поиске, а в ответ получили ошибку (см. **рисунок**).

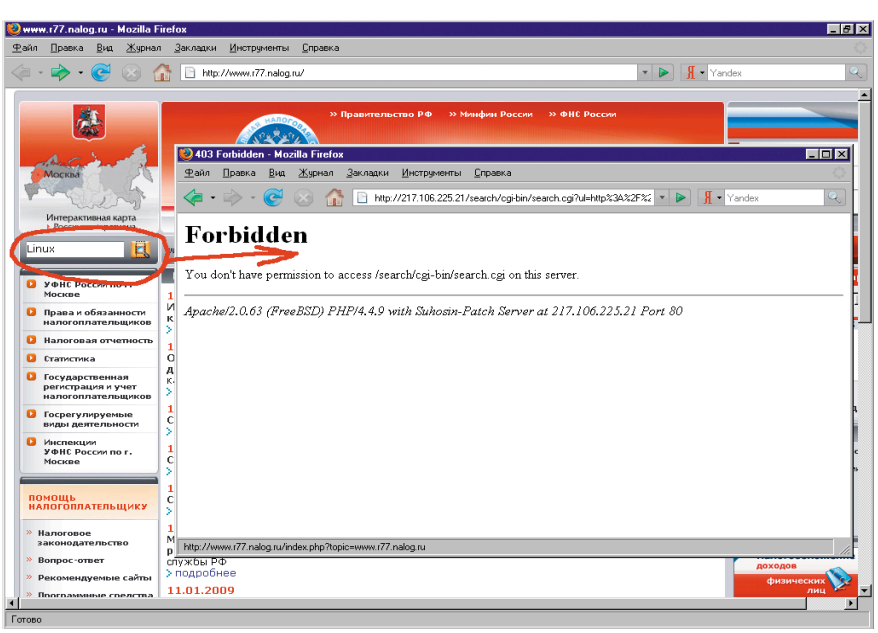
Это ошибка никак не связана с операционной системой Linux, просто забыли мелочь – права доступа на скрипте поиска исправить, что накладывает общий отпечаток на всю ФНС, «за державу обидно», хотя и бальзам на душу, что сервер работает под управлением FreeBSD. Что интересно, за те два месяца, что я писал статью, ошибка так и не исчезла. Поискав на сайте «вручную», мы нашли страницу «Система представления налоговой и бухгалтерской отчетности в электронном виде по телекоммуникационным каналам связи» [12] и узнали, что существует «Формат представления налоговой и бухгалтерской отчетности в электронном виде. Версия 4.00»[13].

Вывод

Прочитав эти документы вместе с коллегами, мы поняли, что работа по стандартизации сдачи налоговой отчётности ведётся, но принимаемые документы и решения по ним далеки от конечных потребителей. Требования к формату передачи данных должны быть открыты и доступны, но, к сожалению, в нашей фирме нет «Кулибиных» способных перевести их в работающую программу под Linux, как и лишних средств для покупки готовых программ под ОС Windows.

По закону нас не могут обязать покупать что-то у сторонней фирмы. Все предлагаемые решения должны быть бесплатны и удобны в использовании. Поэтому дальше мы так и будем сдавать отчётность по старинке, пока не появятся новые эффективные и удобные решения данной проблемы.

Буду очень рад, если на форуме журнала http://samag.ru/forum возникнет обсуждение данного вопроса.



Ошибка поиска на сайте ФНС

1. Сдача налоговой отчётности через фирму «Контур-Экстерн» – http://kontur-agent.ru, http://real-soft.ru/cgi-bin/h.pl?kontur.
2. Сдача налоговой отчётности через фирму «Тензор» – http://ereport.sbis.ru/podkl/podkluchenie.
3. Сдача налоговой отчётности через фирму «Гарант-Телеком» – http://telecom.garant-corp.ru.
4. Сдача налоговой отчётности через фирму «Такском» – http://www.taxcom.ru.
5. В помощь налогоплательщику – http://www.robotech.ru/articles/detail.php?id=48.
6. http://www.cryptopro.ru/cryptopro/forum2/default.aspx?g=posts&t=87.
7. Пакет свободного программного обеспечения для образовательных учреждений России – http://freecode.pspo.perm.ru/glossary/index.html, http://linux.armd.ru/ru/news/project_news/index.php?id110=101459.
8. В сентябре 2008 году «Армада» объявила о завершении пилотного проекта по созданию и поставке свободного программного обеспечения на базе Linux в школы... – http://www.cnews.ru/news/line/index.shtml?2008/11/06/326563.
9. Семинар «Свободное программное обеспечение в государственном и некоммерческом секторе» – http://linux.armd.ru/ru/news/gosspo/index.php?id110=101480.
10. Российское Агентство развития информационного общества – http://www.rario.ru.
11. Дистрибутив ALT Linux Desktop Professional получил сертификат ФСТЭК – http://cnews.ru/news/top/index.shtml?2008/08/01/310364.
12. Система представления налоговой и бухгалтерской отчетности в электронном виде по телекоммуникационным каналам связи – http://www.r77.nalog.ru/index.php?topic=sb77.
13. Формат представления налоговой и бухгалтерской отчетности в электронном виде. Версия 4.00 – http://www.nalog.ru/document.php?id=25597&topic=nal_otch_400.
14. Сертифицированные ФСБ РФ многоплатформенные криптобиблиотеки – http://www.bifit.com/ru/technologies/cryptography/index.html.
15. Список банк-клиентов, работающих под Linux – http://www.etersoft.ru/news/82.

Используем универсальные отчеты и обработки в «1С:Предприятие 8»

Альберт Балаков

Фирмой «1С» разработан ряд универсальных отчетов и обработок, которые представляют собой мощный инструмент для манипулирования данными в среде «1С:Предприятие 8». Они названы универсальными, потому что работают с любой конфигурацией и позволяют решать широкий круг задач.

Эти универсальные инструменты можно найти на дисках информационно-технологического сопровождения, поставляемых фирмой «1С» в разделе «Работаем с программами → Методическая поддержка 1С:Предприятия 8 → Универсальные отчеты и обработки». Часть из них встроена в типовые конфигурации.

Рассмотрим некоторые из существующих в настоящее время универсальных отчетов и обработок, обсудим их функциональное назначение, рассмотрим примеры использования.

Универсальные подбор и обработка объектов

Обработка предназначена для массовой обработки справочников и документов. Встроенные возможности позволяют выполнить:

- Установку реквизитов справочников и документов;
- Перенумерацию справочников и документов;
- Пометку на удаление элементов справочников и документов;
- Непосредственное удаление документов и элементов справочников из базы данных (минуя пометку удаления);
- Провести или отменить проведение документов.

Рассмотрим функционирование обработки на примере справочника «Контрагенты». Выберем в шапке объект поис-

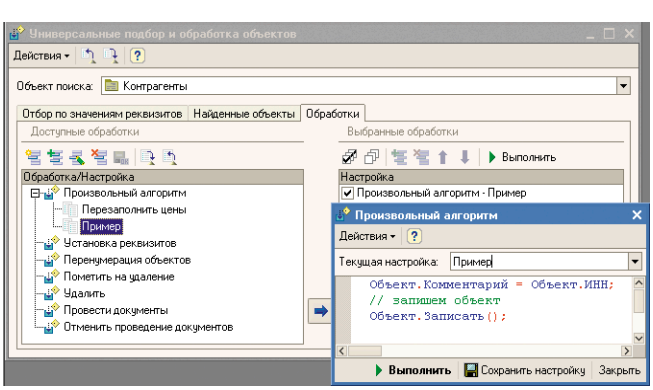


Рисунок 1. Обработка «Универсальные подбор и обработка объектов»

ка – «Контрагенты» (см. **рис. 1**). На закладке «Отбор по значениям реквизитов» зададим условия отбора, используя в качестве фильтра как любые реквизиты самого справочника, так и поля реквизитов и нажимаем кнопку «Найти объекты».

На закладке «Найденные объекты» будут представлены отобранные объекты, для которых можно как выбрать перечисленные выше предопределенные действия, так и выполнить произвольный алгоритм на встроенном языке. Текст программы вносится непосредственно в обработке и может быть сохранен для дальнейшего использования.

На **рис. 1** представлена наша обработка «Пример», осуществляющая копирование ИНН контрагента в поле «Комментарий». После нажатия кнопки «Выполнить» она будет последовательно выполнена для каждого отобранного элемента справочника. Обратите внимание, что в тексте программы обращение к текущему обрабатываемому элементу осуществляется через переменную «Объект».

Загрузка данных из табличного документа

Обработка позволяет загрузить данные в справочники, регистры сведений, табличные части документов и справочников из dbf-, csv- и xls-файлов.

Рассмотрим функционирование обработки на следующем примере: из старой учетной системы данные о контрагентах выгрузили в таблицу MS Excel. Требуется загрузить эти данные в «1С:Управление торговлей 8».

Запустим обработку, выберем режим «Загрузка в справочник», вид справочника – «Контрагенты». С помощью кнопки «Открыть файл...» импортируем данные из таблицы MS Excel на закладку «Табличный документ» (см. **рис. 2**). Далее по тексту данные этой закладки будем называть исходной таблицей.

На закладке «Настройка» сделаем поле «№ колонки» доступным – включим режим ручной нумерации колонок («Нумерация колонок → Ручная нумерация колонок»).

Для каждого реквизита справочника укажем, из какой колонки исходной таблицы следует загружать данные. Для этого введем порядковый номер колонки с данными в поле «№ колонки».

На **рис. 3** у реквизита «ИНН» установлен флажок в колонке «Поле поиска». Тем самым мы указываем обработке предварительно выполнить поиск контрагента с таким ИНН и, если нашли, перезаполнить существующий элемент новыми данными.

В колонке «Режим загрузки» мы можем выбрать один из трех режимов: «Устанавливать», «Искать», «Вычислять».

Режим «Устанавливать». В этом режиме в реквизит заносится фиксированное значение из колонки «Значение по умолчанию». В нашем примере, представленном на **рис. 3**, в поле «Комментарий» всех контрагентов будет записана строка «Загрузка из файла».

Режим «Вычислять». Этот режим обеспечивает широкие возможности по настройке обработки под конкретные нужды: в поле «Выражение» можно записать произвольный алгоритм на встроенном языке, «вернув» результат расчетов через переменную «Результат». Простой пример использования режима представлен на **рис. 3**: в поле «Полное наименование» заносится наименование из исходной таблицы, перед которым добавляется строка «Контрагент:».

Режим «Искать». Если режим установлен для реквизита примитивного типа (строка, число и т. п.), то в соответствующее поле объекта переносятся данные из исходной таблицы (с приведением типов). Для реквизита ссылочного типа запускается поиск элемента, используя данные исходной таблицы в качестве ключа. В нашем примере (см. **рис. 3**) основной менеджер контрагента должен выбираться из справочника «Пользователи». При этом мы видим, что данные для поиска извлекаются из четвертой колонки исходной таблицы и в обработке указано, что искать в справочнике «Пользователи» следует по полю «Наименование».

Рисунок 2. Обработка «Загрузка данных из табличного документа», закладка «Табличный документ»

Важно заметить, что в типовых решениях фирмы «1С» на платформе «1С:Предприятие 8» выделены специальные документы для ввода начальных остатков. Обработка «Загрузка данных из табличного документа» может использоваться не только для загрузки справочников, но и для заполнения таких документов на основе внешних источников. Это делает ее высокоэффективным инструментом при переносе данных, способным сэкономить IT-специалистам массу усилий и времени.

Универсальный обмен данными в формате XML

Обработка предназначена для загрузки из файла и выгрузки в файл данных из любой конфигурации, реализованной на платформе «1С:Предприятие 8».

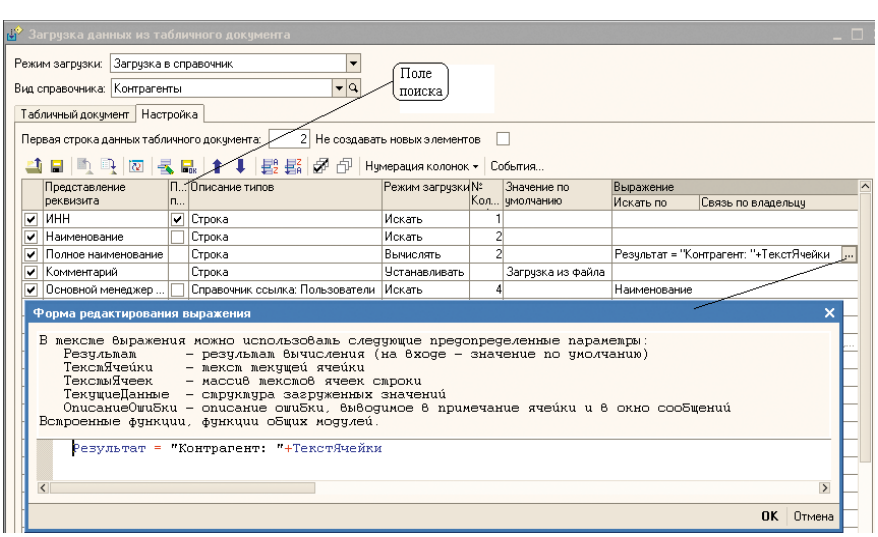


Рисунок 3. Обработка «Загрузка данных из табличного документа», закладка «Настройка»

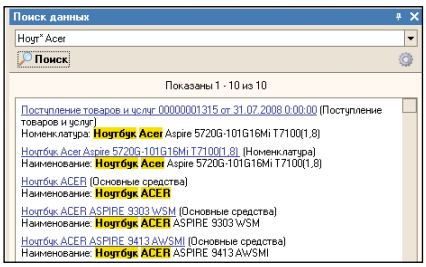


Рисунок 4. Обработка «Поиск данных»

Выгрузка данных осуществляется на основе правил обмена. Предположим, мы хотим выгрузить данные из конфигурации, назовем ее Источник, в конфигурацию – Приемник. Структура информационных баз может не совпадать, поэтому следует иметь правила обмена, описывающие то, как данные конфигурации – Источника преобразовываются в формат данных конфигурации – Приемника. Правила обмена представляют собой XML-файл и могут быть настроены в специальной конфигурации «Конвертация данных, редакция 2».

Поиск и замена значений

Обработка предназначена для поиска и замены ссылочных значений в информационной базе «1С:Предприятия 8». Часто возникает ситуация, когда в каком-либо справочнике ошибочно введено две записи вместо одной. Например, в справочник «Контрагенты» введено два элемента: «ООО Мир» и «Мир, ООО», причем оба уже используются в документах.

Воспользовавшись обработкой «Поиск и замена значений», мы можем найти все вхождения элемента «ООО Мир» в документах и иных объектах конфигурации и заменить их на другой элемент – «Мир, ООО». После этого первый элемент может быть удален.

Здесь следует сделать важное замечание. В типовых конфигурациях фирмы «1С», например, в документах, влияющих на взаиморасчеты, указывается не только контрагент, но и договор контрагента. Если мы выполним приведенный пример в типовой конфигурации, то контрагент в документах будет один, а договор – принадлежать другому контрагенту, что неприемлемо.

Поэтому важно понимать, что обработка работает универсально, не учитывая логическую взаимосвязь объектов. При необходимости следует изменить и те данные, которые зависят от замененных значений. Перед заменой значений рекомендуется сделать архивную копию информационной базы.

Удаление помеченных объектов

Встроенные средства платформы «1С:Предприятие 8» позволяют непосредственно удалить из базы данных помеченные на удаление объекты только в монопольном режиме. Данная обработка позволяет это сделать в раздельном режиме работы, но при этом есть риск нарушения логической целостности данных. Чтобы избежать этого, всем активным пользователям следует воздержаться от записи объектов, имеющих помеченные на удаление ссылочные реквизиты.

Выгрузка данных в реляционные структуры

Обработка предназначена для выгрузки данных информационной базы «1С:Предприятия 8» во внешние реляционные структуры данных. Имеет два режима работы: «Выгружать все» и «Только изменения». Второй вариант функционирования использует механизм планов обмена и позволяет периодически синхронизировать информационную базу с внешним источником, передавая только новые и измененные объекты.

Для выгрузки данных необходимо настроить вариант выгрузки, содержащий перечень выгружаемых объектов метаданных. При настройке имеется возможность указать выгружаемые реквизиты объектов.

Поддерживаемые типы СУБД – приемников:

- Microsoft SQL Server;
- Oracle;
- IBM DB2;
- PostgreSQL;
- MySQL.

Консоль анализа журнала регистрации

В «1С:Предприятии 8» имеется возможность ведения журнала регистрации событий. Это позволяет выяснить, какие действия и когда предпринимал тот или иной пользователь, какие события происходили в системе. Подробнее см. в журнале № 9 за 2007 г.

Консоль отчетов

Обработка предназначена для настройки и вывода произвольных отчетов без использования конфигуратора «1С».

Для настройки отчета следует отредактировать схему компоновки данных, после этого отчет может быть выведен как в табличный документ, так и в диаграмму.

Для анализа полученных данных становится доступно все разнообразие средств системы компоновки данных: настройка произвольных группировок строк и колонок, состава выводимых данных, условий отбора и т. п.

Консоль запросов

Обработка предназначена для составления и исполнения запросов «1С:Предприятия» без использования конфигуратора.

Результат выполнения запроса можно проанализировать в виде простого списка, дерева или сводной таблицы.

Консоль кластера серверов

Позволяет выполнять функции администрирования кластеров серверов «1С:Предприятия 8.1». В обработку встроены средства анализа динамики нагрузки в виде графиков.

Свертка информационной базы

Обработка предназначена для формирования начальных остатков и данных регистров сведений на дату свертки, а также удаления неиспользуемых документов и движений по регистрам сведений, накоплений и бухгалтерии до даты свертки.

Обработка формирует начальные данные с помощью документов «Корректировка записей регистров» и «Операция (бухгалтерский и налоговый учет)», поэтому является ограниченно универсальной и на текущий момент предназначена исключительно для использования со следующими типовыми конфигурациями:

- Бухгалтерия предприятия, редакция 1.6;
- Управление торговлей, редакция 10.3;
- Управление производственным предприятием, редакция 1.2.

Настройка технологического журнала

Обработка предназначена для редактирования конфигурационного файла технологического журнала. Она позволяет настроить перечень событий и свойств, которые должны отражаться в технологическом журнале, и условия их записи в него.

Консоль заданий

Обработка предназначена для визуального контроля состояния и управления работой регламентных и фоновых заданий.

Поиск данных

В технологическую платформу «1С:Предприятия 8» встроен механизм полнотекстового поиска, позволяющий осуществлять поиск в базе данных с указанием поисковых операторов (и, или, не, рядом и другие).

Обработка иллюстрирует применение этой полезной возможности (см. **рис. 4**). Перед использованием обработки следует разрешить полнотекстовый поиск и создать или обновить индекс. Для этого выберите пункт «Операции → Управление полнотекстовым поиском».

Универсальный журнал документов

Данная обработка позволяет работать с перечнем документов различных видов в едином журнале. Причем пользователь самостоятельно настраивает набор видов документов, состав граф журнала, отборы и порядок сортировки.

Из формы универсального журнала можно выполнить большинство сервисных функций, доступных из стандартных динамических списков и журналов, задаваемых на этапе конфигурирования: создание, изменение, копирование, проведение документов, просмотр движений документа по регистрам и др.

Изменение конфиденциальной информации

Обработка предназначена для выборочного изменения или очистки информации в информационной базе. Может быть полезна при необходимости передачи информационной базы на сторону, когда часть информации является конфиденциальной и должна быть скрыта.

Рассмотрим функционирование обработки на простом примере. Предположим, в информационной базе «1С:Управление торговлей 8» требуется скрыть информацию о поставщиках и покупателях – изменить поля «Наименование», «Полное наименование» и «ИНН» справочника «Контрагенты» (см. **рис. 5**).

Для этого запустим обработку и выполним настройку изменения реквизитов так, как показано на **рис. 6**. После нажатия кнопки «Выполнить» отмеченные реквизиты будут изменены для каждого элемента справочника «Контрагенты».

Если в колонке «Тип настроек» для реквизита выбрано «Индивидуальные», то метод изменения реквизита берется из колонки «Значение настроек». Если же в колонке «Тип настроек» указано «Общие», то метод изменения реквизита определяется настройками закладки «Общие настройки изменения данных».

	Код	Наименование	ИНН	Полное наименование
	000000001	Дочерние структуры		
	000000120	Агидель, ООО	0256034177	ООО "Агидель"
	000000121	Петров С. А., ИП	032560385561	ИП Петров Сергей Андреевич

Рисунок 5. Справочник «Контрагенты» до запуска обработки «Изменение конфиденциальной информации»

Рисунок 6. Обработки «Изменение конфиденциальной информации», закладка «Список объектов»

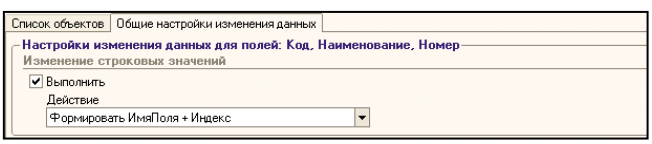


Рисунок 7. Обработки «Изменение конфиденциальной информации», закладка «Общие настройки изменения данных»

	Код	Наименование	ИНН	Полное наименование
	000000001	Наименование042		
	000000120	Наименование043	4843f06185	Контрагенты043
	000000121	Наименование044	4a6201b9e75f	Контрагенты044

Рисунок 8. Справочник «Контрагенты» после запуска обработки «Изменение конфиденциальной информации»

В нашем примере (см. **рис. 6**) поле «ИНН» всех элементов справочника «Контрагенты» будет замещаться случайным набором символов, а порядок изменения поля «Наименование» определяется настройками, представленными на **рис. 7**.

На **рис. 8** приведена форма списка справочника «Контрагенты» после запуска обработки.

Конвертация внешних обработок

Технологическая платформа «1С:Предприятие 8» активно развивается. Данная обработка предназначена для решения задачи массовой конвертации файлов внешних обработок (обновления формата) при переходе на более старшие релизы платформы.

Обработка позволяет:

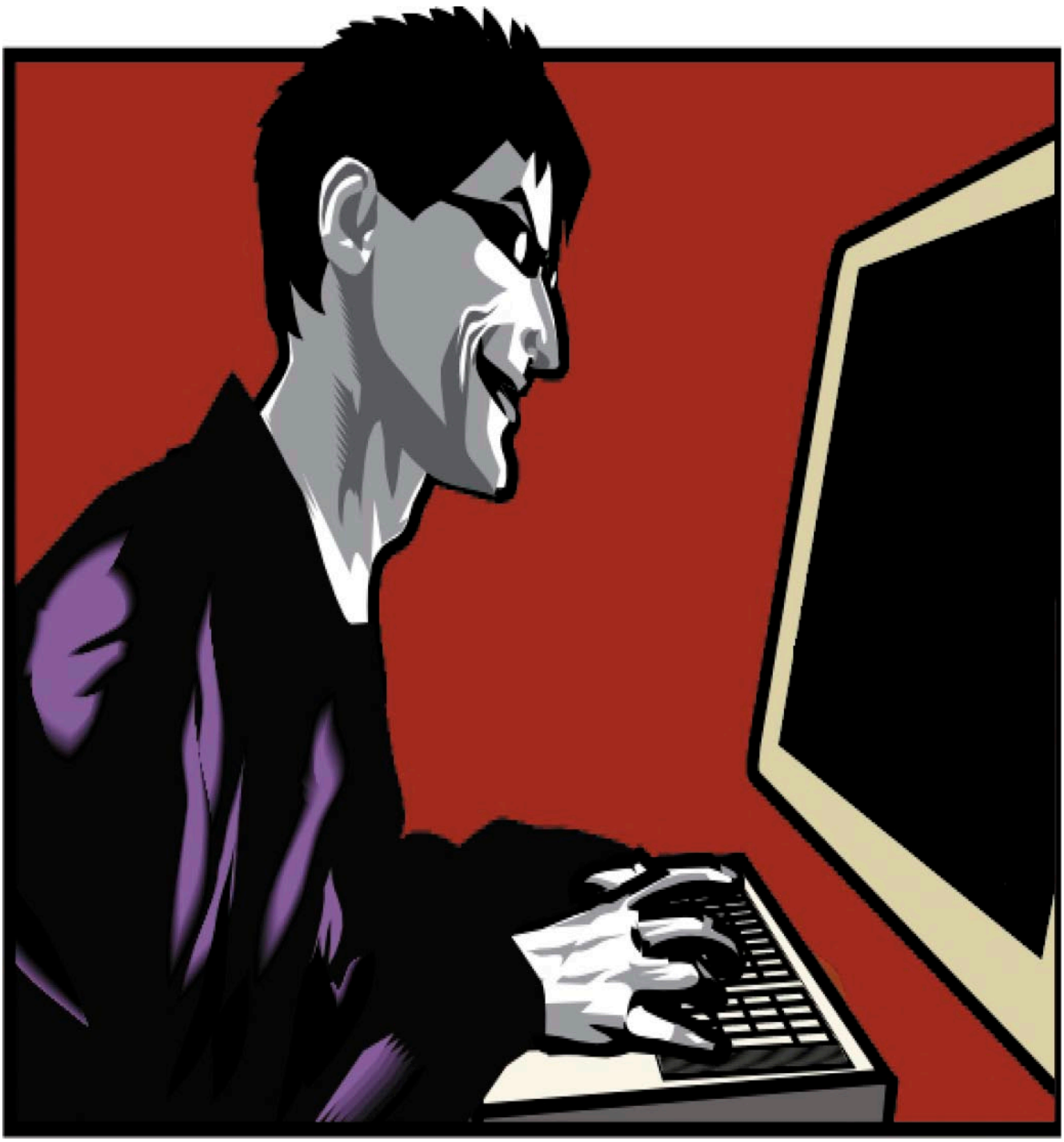
- Выгрузить обработки из справочника «Внешние обработки» типовых конфигураций, выполнить их массовую автоматическую конвертацию и загрузку.
- Выполнить автоматическую конвертацию файла или каталога с обработками.

Заключение

В заключение отмечу, что функциональная мощь новой технологической платформы фирмы «1С» позволила создать множество инструментов, облегчающих задачи администрирования и использования систем на ее основе.

При подготовке статьи использовались материалы, публикуемые фирмой «1С» для пользователей программ на платформе «1С:Предприятие 8».

Исследование уязвимостей с помощью Metasploit Framework



Павел Троицкий

Учиться никогда не поздно, а учить других – приятное занятие... Из этой статьи вы сможете узнать о том, как просто и наглядно можно продемонстрировать работу большинства уязвимостей с помощью Metasploit Framework.

Всё что ни случается в жизни – к лучшему... В одно субботнее утро мне пришлось отважно поработать. Согласитесь, не самое приятное занятие, особенно в свой выходной день. Но на ситуацию можно посмотреть и с другой стороны.

Через несколько часов утренней работы, когда я освободился и пребывал в состоянии сна на ходу, меня уже не тянуло домой. Я плыл по коридору, где стояла убаюкивающая тишина по сравнению с шумными буднями. Не помню как, наверное, сработало любопытство, услышав издалека характерные непрекращающиеся звуки быстрого нажатия клавиш на клавиатуре, я на автопилоте изменил курс и пришвартовался в соседнем отделе.

Люблю наблюдать за увлечённо работающими людьми. Оказалось, мой тёзка и коллега сидит за двумя своими мониторами и что-то решает. Я мягко приземлился в одно из пустующих кресел, включил чайник и стал ждать.

Пашок вернулся к жизни и заметил меня лишь только когда чайник закипел и громко щёлкнул своим термовыключателем на всю комнату. Видимо, сработало то, что чайник он не ставил.

Увидев меня, он быстро заварил себе кофе, сел обратно на своё место и явно обрадовался тому, что сможет излить мне свою душу во время чаепития и найти понимание. Так и оказалось. Он решал одну интересную задачу, которую ему поставил шеф, с микроконтроллерами, при этом думая и о другом задании, на которое времени не хватало.

Второе задание было более интересным, чем первое, я постараюсь описать его вам, а далее предложить придуманное нами решение.

Закрытый код – враг народа?

Не секрет, что технический отдел с его руководством косо посматривают на тех, кто использует программы с закрытым кодом, к тому же содержащие много уязвимостей. Когда руководство компании понимает проблему, это хорошо. Техническому отделу дается зелёный свет, и вся организация переходит на более правильные и безопасные для фирмы решения.

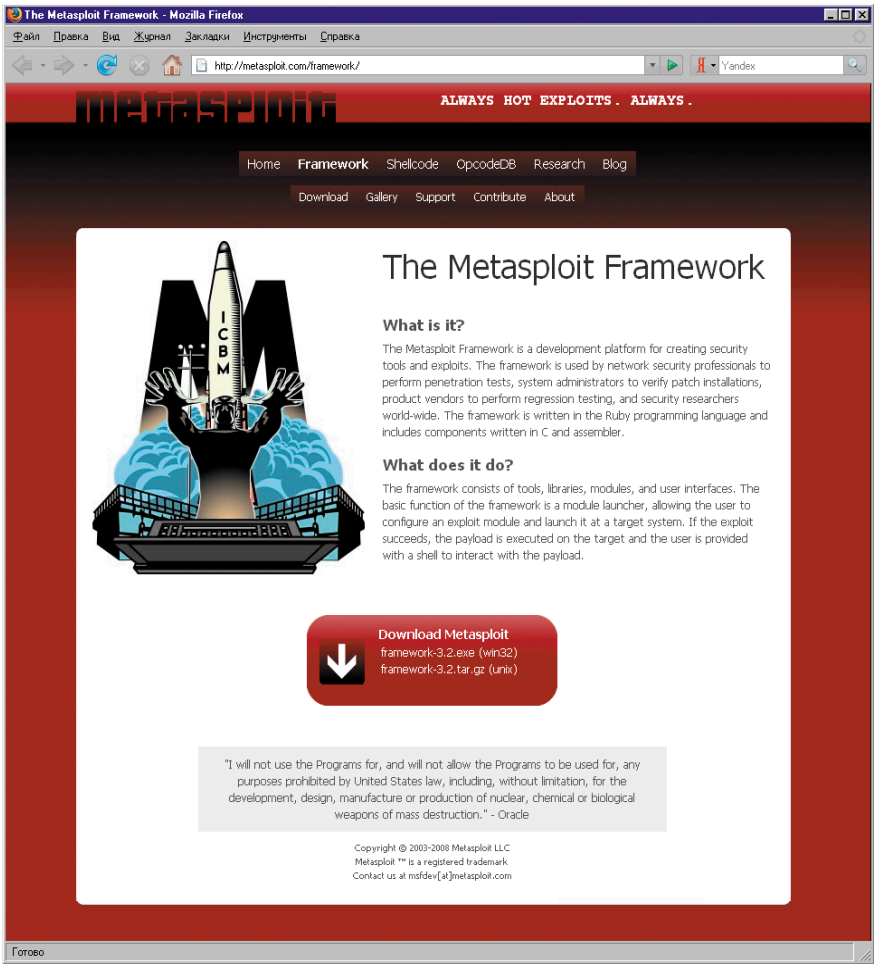


Рисунок 1. Раздел Framework и ссылка для скачивания

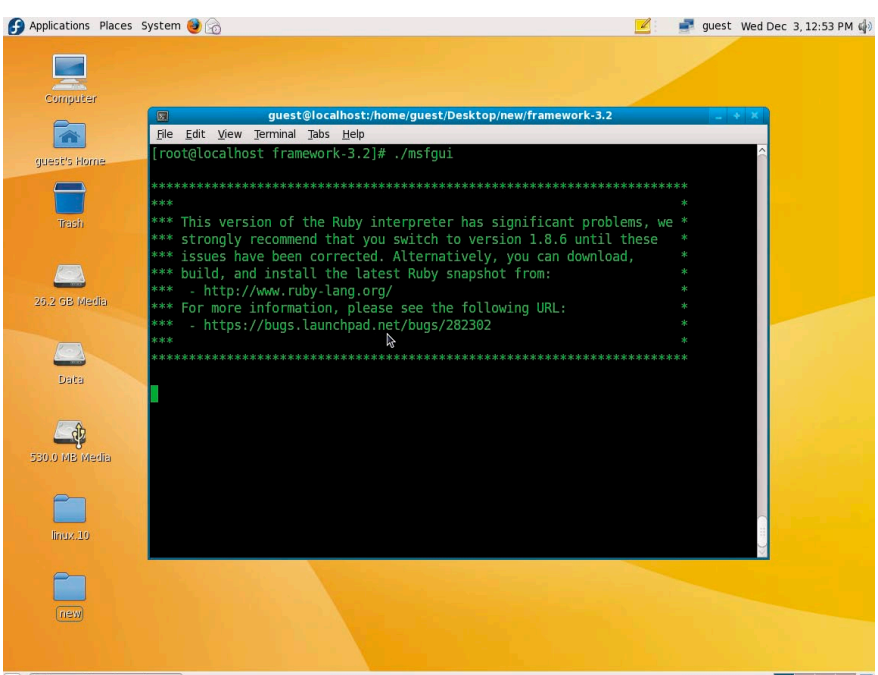


Рисунок 2. Запуск программы Metasploit Framework

Но бывают и другие случаи, когда руководство, опираясь на мнение друзей и знакомых, делает вид, что разбирается, а на самом деле это не так.

Например, не все оценивают преимущества новых версий Linux, OpenOffice или браузера Mozilla Firefox (по сравнению с их закрытыми

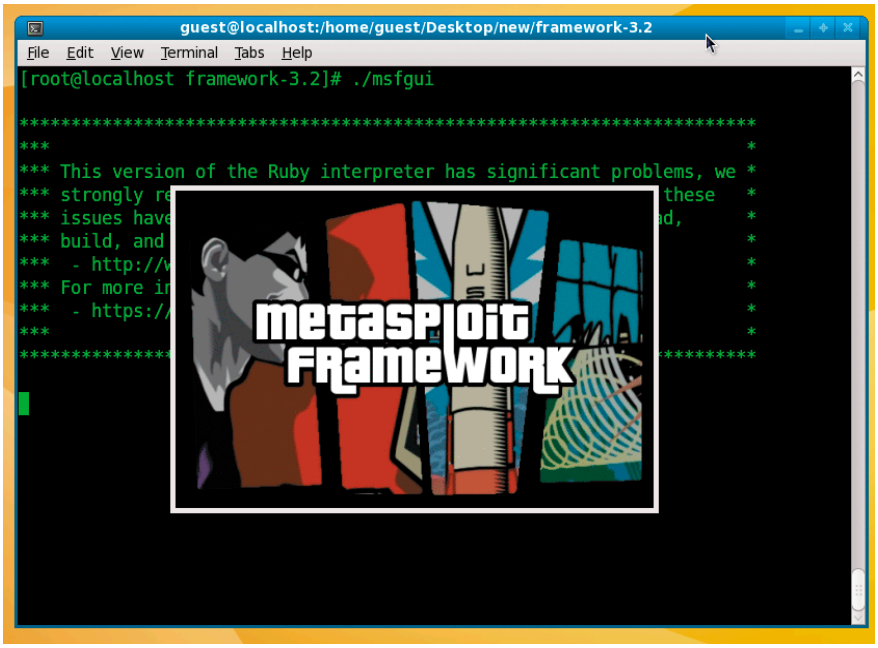


Рисунок 3. Логотип программы Metasploit Framework, показываемый во время запуска

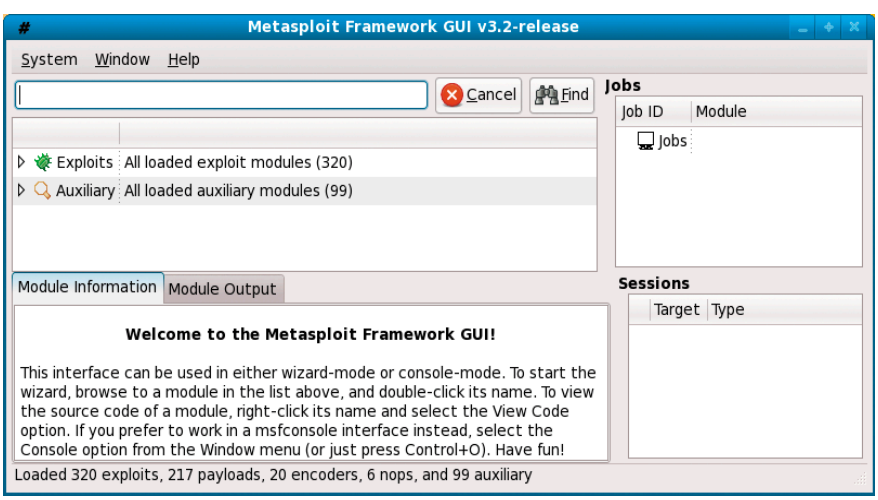


Рисунок 4. GUI программы Metasploit Framework

и не всегда стабильно работающими аналогами: Windows, MSOffice или IE).

Люди инертны, привыкли к чему-то и менять ничего не хотят. Рыба гниёт с головы – бывают случаи, когда руководство не допускает технический отдел к своим компьютерам (особенно ноутбукам), являясь не только источником нарушений безопасности, но и первой целью для происков конкурентов.

Цель задания состояла в том, чтобы вернуть авторитет техническому отделу, прочитать ознакомительную лекцию для персонала и провести в жизнь решения по установке и переходу на более безопасные Open Source аналоги, мотивируя это не своим желанием, а приказом руководства, стоящего над техническим отделом.

Задача, кажется, ясна, если у вас есть многолетний опыт, наверняка вы смогли в ней увидеть что-то пересекающееся из своей жизни или похожее. Давайте рассмотрим случай решения, когда хитрость идёт на пользу общему делу. Если у вас есть более интересные решения – пишите на форум журнала, обсудим!

Решение

Как действовать? Так как Глобальной сетью пользуются практически все, а она представляет немалую угрозу любому подразделению, то поставим цель – отучить пользователей использовать IE.

Если обратиться к классике, то существует не так много различных подходов к решению проблем [1, стр. 88]:

- если сделать проверку на используемый браузер и отключить обращения IE в сеть на прокси-сервере, то это будет не самое лучшее решение, а администратора можно будет классифицировать как «маньяка»;
- если удалить всем пользователям IE, то это будет администратор-«идиот», и проблема также не решится;
- если пытаться пакостить пользователям, запускающим IE, это будет администратор-«фашист» – успеха он тоже не добьётся, так как будет все силы тратить на борьбу со следствием.

Наиболее правильно – это пойти на хитрость и бороться с причиной. Представьте, если все пользователи осознанно откажутся от какого-то решения, то какой будет смысл в мире бизнеса производителю продвигать это решение?

Наиболее удачно для нашей задумки подходит тип администратора «технический бандит».

Мы изучим различные нюансы работы браузеров и существующие в них уязвимости, поставим специальные программы, демонстрирующие скрытые возможности, возникающие из-за ошибок, и тем самым заставим руководство принять правильное решение.

Проверь систему на уязвимость

Очевиден факт, что в любой большой программе есть ошибки. Это практически все понимают, и начальство в том числе. Поэтому для проверки сетей и отдельных хостов давно придумали различные сканеры. Но не все понимают специфику их работы.

Если Nessus, Shadow Security Scanner, nmap, XSpider и другие в какой-то мере удобны и успели себя хорошо зарекомендовать, то опираться на их результаты следует с пониманием происходящего.

Например, как быть со случаем, когда исполнение какого-либо кода (содержащего уязвимость) происходит со стороны пользователя, а не инициируется внешним сканером? Не секрет, что многие, просканировав свой компьютер (или сервер) и не обнару-

жив открытых портов и уязвимых сервисов, ошибочно думают, что их системы в полном порядке.

Мы попытаемся доказать эту ошибку на примере браузера IE с помощью программы Metasploit Framework.

План действий. Немного теории

Получая различные рассылки по вопросам безопасности или посещая сайты по подобной тематике, периодически встречаешь информацию о различных уязвимостях. Такая-то уязвимость позволяет передать клиенту и выполнить на его стороне какой-либо код, такая-то просто завершает приложение.

В теории получается следующее: вы заходите на сайт XXX, а у вас вместо этого открывается окно терминала, где запускается команда «format c:».

Пример утрирован, но, если вам в это сложно поверить, к концу статьи вы сможете провести аналогичный эксперимент у себя.

The Metasploit Project

Это проект [2], созданный фирмой Metasploit LLC, содержащий полезную информацию для людей, занимающихся пополнением баз данных для СОА (систем обнаружения атак), а также исследованием уязвимостей и того, как они работают.

Цель ресурса – собрать различную информацию об известных эксплоитах и уязвимостях вместе с реализующими их кодами, чтобы эта информация была доступна администраторам безопасности и разработчикам.

На сайте содержится несколько разделов, содержащих полезную информацию.

Нам понадобится раздел Framework (см. **рис. 1**), посвящённый платформе, на которой можно реализовать наш план.

Ищем Download внизу и скачиваем framework-3.2.tar.gz.

Установка Metasploit Framework

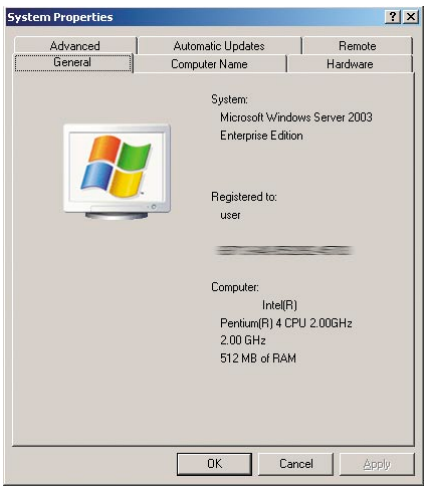
Ранее программа была доступна только через CLI (интерфейс командной строки), в связи с чем была известна только в узких кругах.

Недавно появилась поддержка GUI (графического интерфейса), что сделало программу более привлекательной для менее опытных пользователей (особенно наличие версии программы под Windows). Хорошо это или плохо, сказать сложно. Мы выберем версию под Linux и GUI-интерфейс.

В качестве операционной системы взята недавно вышедшая Fedora 10. Конечно, она не без проблем. Скорее всего, через полгода – год мелкие проблемы будут решены, и она станет рабочей платформой для многих администраторов, а пока она очень подходит для наших экспериментов. Если взять более ранние версии (Fedora 8, 9), то принципиальных различий в установке быть не должно.

Для работы графического интерфейса необходима установка языка Ruby и библиотек:

- ruby-1.8.6.287-2.fc10.i386.rpm;
- ruby-libs-1.8.6.287-2.fc10.i386.rpm;
- ruby-gtk2-0.18.0-2.fc10.i386.rpm;
- ruby-libglade2-0.18.0-2.fc10.i386.rpm;
- ruby-atk-0.18.0-2.fc10.i386.rpm;
- ruby-cairo-1.8.0-1.fc10.i386.rpm;
- ruby-gdkpixbuf2-0.18.0-2.fc10.i386.rpm;
- ruby-glib2-0.18.0-2.fc10.i386.rpm;
- ruby-gnome2-0.18.0-2.fc10.i386.rpm;
- ruby-gnomecanvas2-0.18.0-2.fc10.i386.rpm;
- ruby-libart2-0.18.0-2.fc10.i386.rpm;
- ruby-pango-0.18.0-2.fc10.i386.rpm.



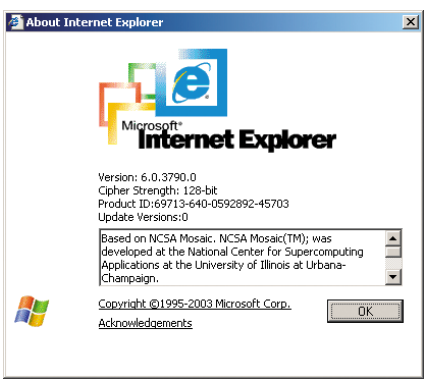


Рисунок 5. Версии ПО уязвимой машины: а) версия ОС; б) версия браузера

Сделать это можно либо вручную через команды:

```
rpm -ihv *.rpm
```

либо через:

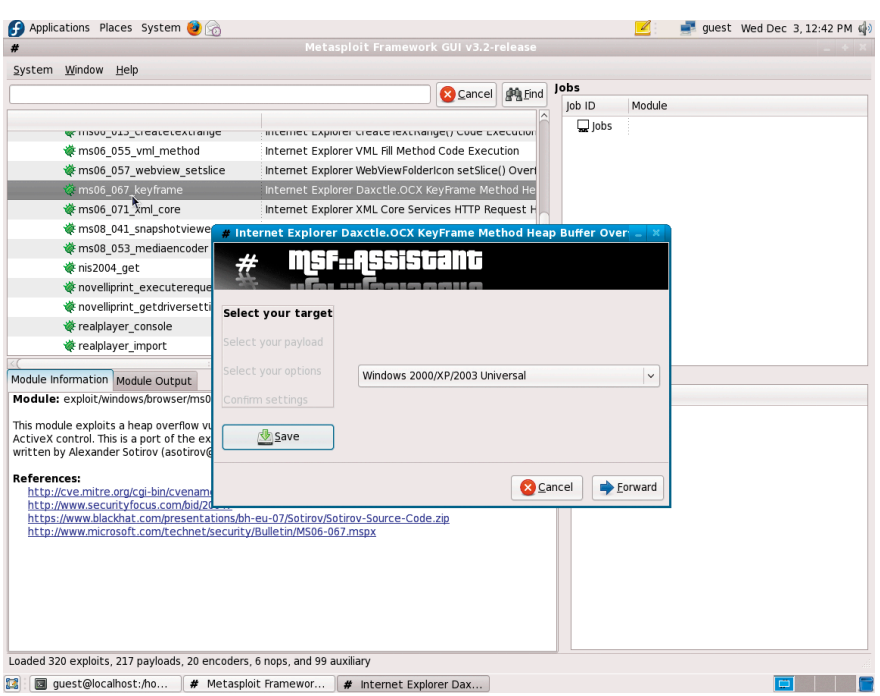


Рисунок 6. Настройка эксплоита под уязвимость MS06-067

```
yum install ...
```

тогда достаточно указать лишь первые четыре пакета, все остальные будут определены как зависимые и установятся сами.

Следующим этапом надо распаковать скачанный архив framework-3.2.tar.gz в какую-либо директорию, зайти в неё и с правами администратора запустить файл msfgui.

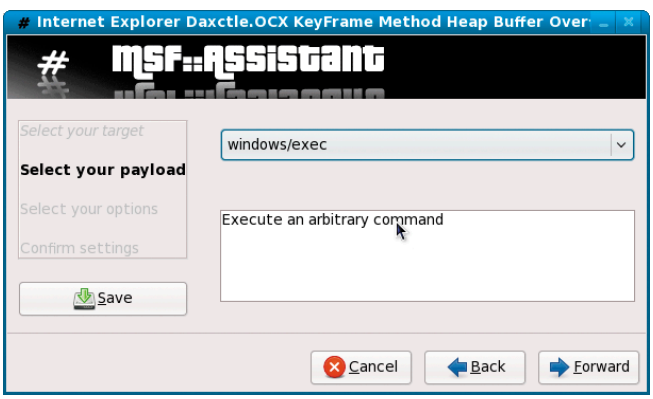


Рисунок 7. Выбираем windows/exec

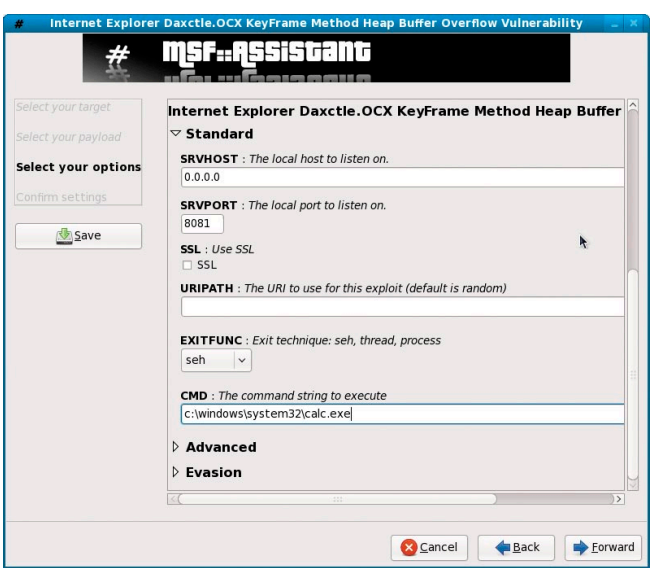


Рисунок 8. Настройка порта и ввод команды для запуска на удалённой машине

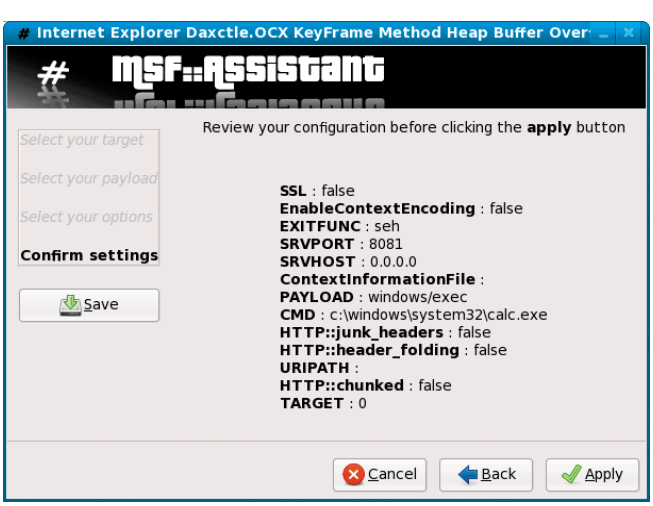


Рисунок 9. Окно подтверждения настроек задания

Права администратора (root) нужны для того, чтобы программа могла открывать сокеты на прослушивание на любом порту (например, на 80-м, протокол TCP).

Запуск программы

Загрузка длится около минуты (см. **рис. 2**), и на это время появятся логотип программы (см. **рис. 3**) и графическая среда (см. **рис. 4**). Программа готова к работе.

Теперь, выбирая уязвимости (в базе Metasploit Framework их немало), мы можем попытаться реализовать сервер, который сформирует код, который будет передан клиенту, для выполнения на его стороне. А далее выполним проверку клиента на уязвимость. В качестве уязвимой машины была выбрана первая находившаяся под рукой, а именно с Windows 2003 и IE 6.0 (см. **рис. 5**). Кстати, некоторые администраторы, не утруждая себя, часто ищут что-то в Сети по интересующим их вопросам прямо из консоли сервера, при этом ставить альтернативные браузеры они не собираются, мотивируя это тем, что подобные выходы в Интернет «на коленке из серверной» у них редки. Замечу, чтобы скомпрометировать сервер, достаточно одного случая!

А далее ситуация проста: главная задача – заманить жертву или всезнающего шефа на наш компьютер. В Интернете подобное решается социальным способом, то есть обходным путём. Например, с помощью размещения различных баннеров либо переадресацией с помощью popup-окошек с уже заражённых сайтов. Такое часто встречается на сомнительных сайтах (бесплатное скачивание коммерческих программ, порносайты и пр.), предлагающих кликнуть на какой-нибудь баннер.

В локальной сети, будучи её администраторами, мы можем завернуть обращение на шлюзе куда нам надо, а после показать шефу, что любой вполне безобидный сайт может творить чудеса с его компьютером (запускать другие приложения, копировать его документы и пр.), при условии что у него даже может быть запущен антивирус.

Конечно, всё это многообразие действий зависит от вашей фантазии, а цель статьи лишь показать направление и что такое возможно. Поэтому мы ограничимся лишь одной уязвимостью в качестве примера и запустим какую-нибудь безобидную программу на компьютере жертвы, например «Калькулятор». Не секрет, что для написания статьи, чтобы никого не обманывать, в течение получаса пришлось перебирать уязвимости, чтобы найти работающую в данной конфигурации.

В качестве уязвимости была выбрана описанная в Microsoft Security Bulletin MS06-067 [3] – выбираем эту уязвимость в базе программы (см. **рис. 6**).

Далее жмём forward и в следующем окне выбираем действие windows/exec, (см. **рис. 7**), также жмём forward и попадаем в настройки.

Прописываем порт 8081 и команду для запуска на машине с уязвимым бараузером «c:\windows\system32\calc.exe» (см. **рис. 8**).

Замечание: если вы хотите прописать 80-й порт, а у вас работает httpd-сервер, то не забудьте его остановить, например, командой:

```
# service httpd stop
```

или:

```
# /etc/rc.d/init.d/httpd stop
```

иначе непонятно, какая из двух программ должна прослушивать порт на входящие соединения. С этой целью в примере взят порт 8081, который заведомо будет свободен.

После подтверждаем настройки (см. **рис. 9**) и в списке висящих заданий (jobs) у нас появляется новая задача (см. **рис. 10**).

Далее мы можем посмотреть в логи – вкладка Output и попытаться обратиться с машины жертвы на наш сервер. Предварительно следует не забыть прописать разрешающие правила для пакетного фильтра, например:

```
# iptables -I INPUT -i eth0 -p tcp -sport 1024:65535 ↵
      -dport 8081 -j ACCEPT
# iptables -I OUTPUT-o eth0  -p tcp -dport 1024:65535 ↵
      -sport 8081 -j ACCEPT
```

Логи:

```
12:28:08 - Initialized the Metasploit Framework GUI.
12:45:38 - ms06_067_keyframe [*] Launching exploit windows/browser/ms06_067_keyframe...
12:45:39 - ms06_067_keyframe [*] Using URL: http://0.0.0.0:8081/
12:45:39 - ms06_067_keyframe [*]  Local IP: http://127.0.0.1:8081/
12:45:39 - ms06_067_keyframe [*] Server started.
12:46:04 - ms06_067_keyframe [*] Sending Internet Explorer Daxctle.OCX KeyFrame Method
Heap Buffer Overflow Vulnerability to 192.168.0.3:1603...
12:46:28 - [*] Stopping exploit:  windows/browser/ms06_067_keyframe
12:46:28 - ms06_067_keyframe [*] Server stopped.
```

Окно машины жертвы (см. **рис. 11**).

Заключение

Конечно, данный пример тривиален, и для того чтобы поразить окружающих или вашего шефа, лучше его модифицировать, учитывая специфику. Мы так устроены, что какое-либо действие (изменения) привлекают нас больше, поэтому для людей, не очень понимающих, как осуществляется переполнение буфера, лучше вместо калькулятора запустить архиватор с ключами, чтобы в окошке была анимация, например «бежало» число процентов сжатых файлов из папки «Мои документы\конфиденциально». Тогда и сказать, что этот сайт нацелен на сбор информации с компьютера вашего шефа, будет проще и ваши аргументы будут весомее. Раз сайт запустил архиватор, а не какой-нибудь калькулятор, то проблема намного серьёзнее. Хотя надеюсь, что большинство читателей, читая эти строчки, улыбнутся лишний раз.

Также эту статью и пример можно использовать в образовательных целях. Чем не пособие для преподавателей на курсах по безопасности или в вузах по проведению демонстраций или лабораторных работ? Выполнять такую лабораторную работу студентам будет куда интереснее, чем обсчитывать не всегда понятные результаты.

Если вы задумались, а не пора ли вам обновить/сменить систему или бразуер, то значит, вы на верном пути!

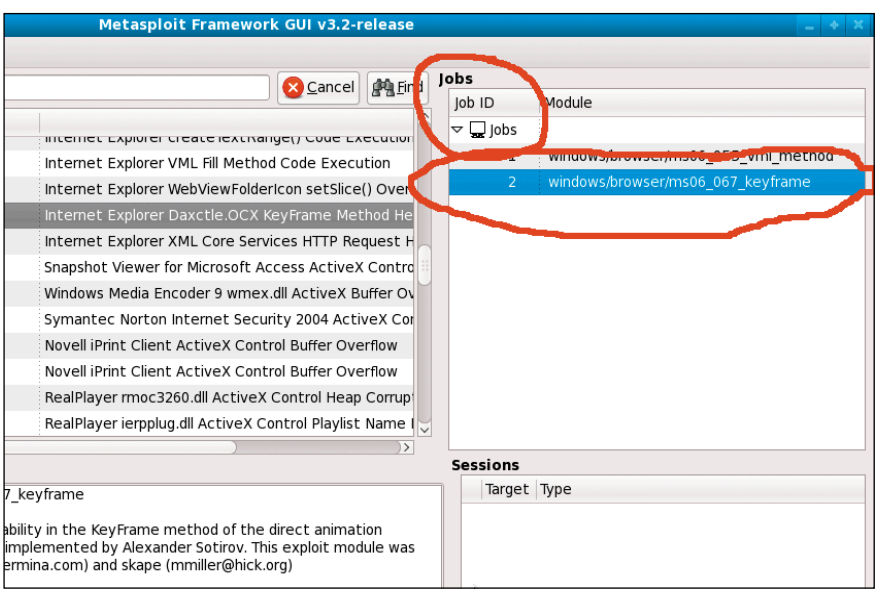


Рисунок 10. Запущена новая задача

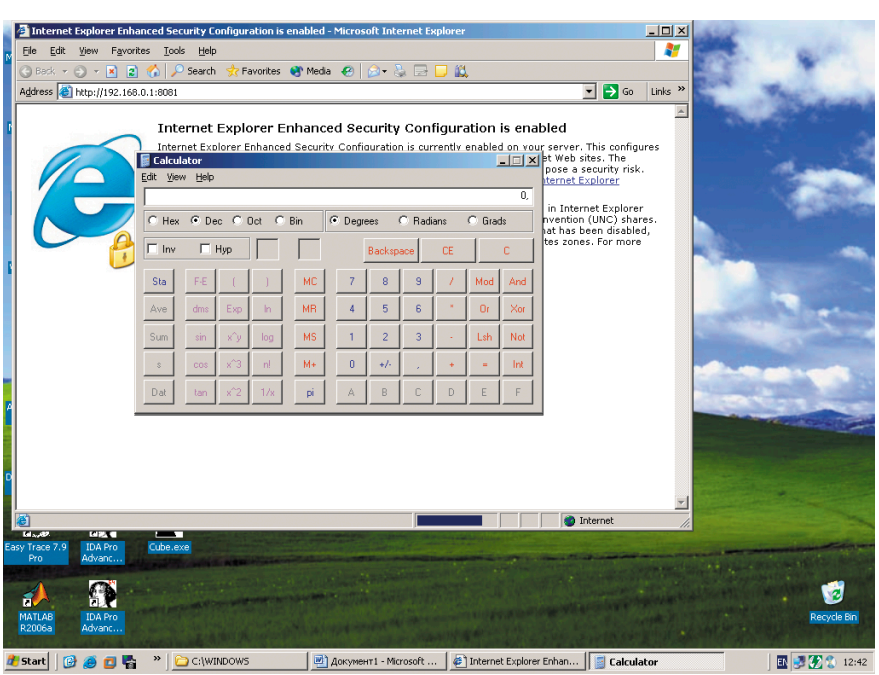
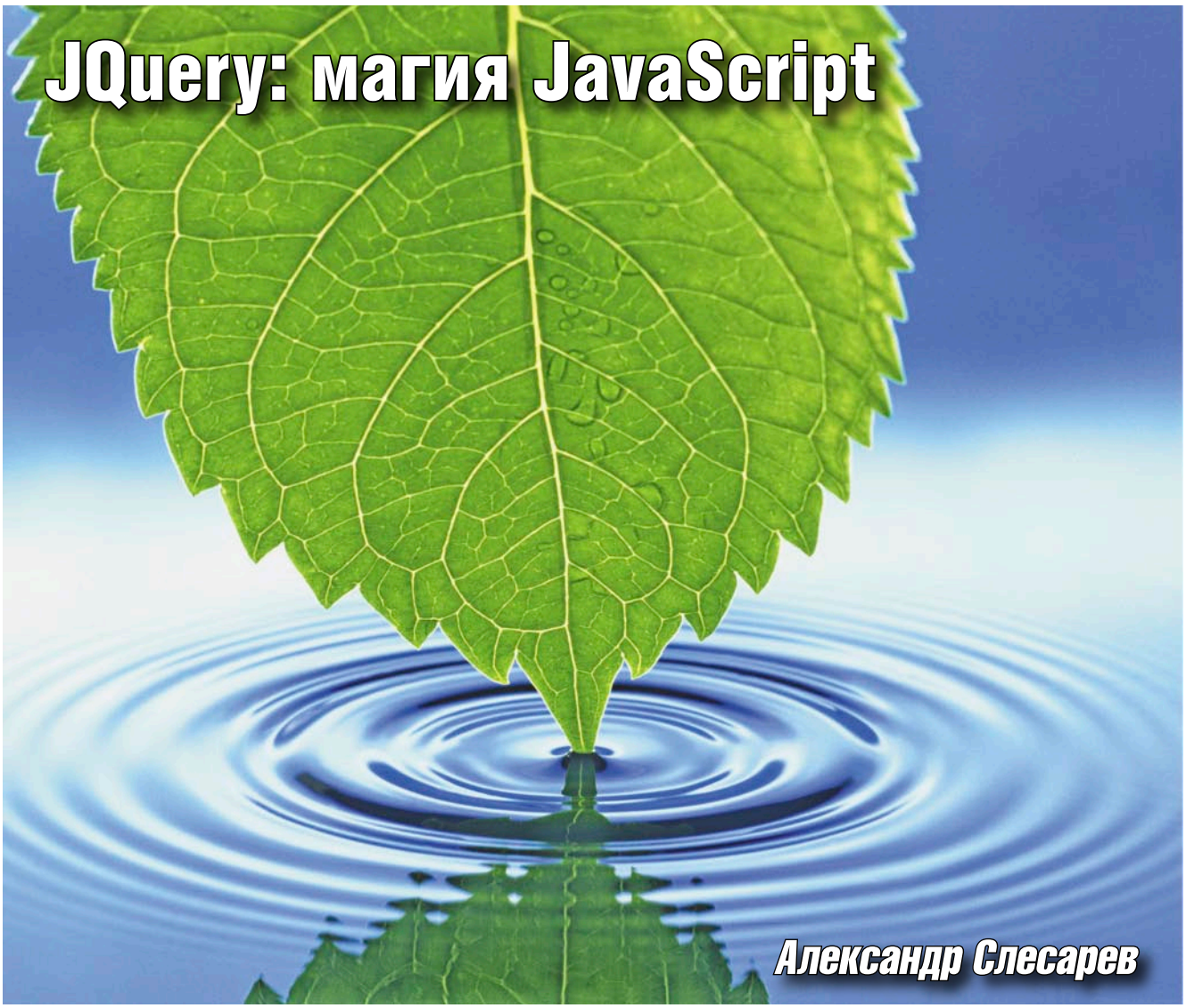


Рисунок 11. Окно уязвимой машины, на которой при обращении к серверу попутно запустилась сторонняя программа – калькулятор

1. Робачевский А. М. Операционная система UNIX. – СПб.: БХВ-Петербург, 2002, ISBN 5-8206-0030-4.
2. Сайт проекта The Metasploit Project, содержащего информацию и эксплоиты по различным уязвимостям, – http://metasploit.com.
3. Уязвимость Microsoft Security Bulletin MS06-067 – http://www.microsoft.com/technet/security/Bulletin/MS06-067.mspx.

JQuery: магия JavaScript



Александр Слесарев

Эпоха WEB 2.0 диктует разработчикам новые правила. Что же скрывается за функциональностью современных веб-приложений? Какие инструменты должен использовать разработчик для решения нестандартных задач при разработке клиентских приложений эпохи WEB 2.0? Ответ на эти вопросы есть – использование фреймворка, рассчитанного на решение этих задач. И такой фреймворк, который содержит богатейший набор методов для разработки современных веб-приложений, существует – JQuery.

В последние годы возникла тенденция повышения требований к функциональности веб-приложений, причем не столько к серверной части, а именно к клиентской. Появились элементы управления, которые до этого были доступны только прикладным программам: табы, деревья, слайдеры, прогрессбары и многое другое. Появилось очень много сайтов, которые по функциональности вполне могут соперничать с прикладными программами. Еще более усилило эту тенденцию появление технологии AJAX. Очень часто в различных информационных источниках мелькает термин WEB 2.0, определяющий приложения новой формации. Да, именно приложения, потому что большинство современных веб-ресурсов трудно назвать сайтами, об этом можно много дискутировать, но факт остается фактом – многие из современных «сайтов» по-другому назвать нельзя.

На фоне всего этого веб-разработчикам приходится прибегать к различным нестандартным приемам, искать новые пути решения задач. Приходится брать на вооружение все, что позволяет создавать новые приложения, объединяемые звучным термином WEB 2.0. Естественно, что для увеличения функциональности приходится использовать клиентские языки программирования, так как базовые технологии веб-разработки HTML и CSS являются статичными. Самым распространенным в данный момент языком программирования на клиентской части является JavaScript. Появилось множество JS-библиотек, позволяющих реализовать красивые графические эффекты, анимацию, общение с сервером без перезагрузки страницы, в общем, инструментарий для облегчения

жизни веб-разработчикам. Многие из них отличает либо большая сложность, либо ограниченность функциональности. Наибольшую популярность у разработчиков завоевали лишь несколько библиотек, одной из которых является фреймворк JQuery.

Не знаю, можно ли говорить о том, что JQuery самая лучшая библиотека, так как конкурирующие продукты (например, Prototype, Mootools и ExtJS) тоже имеют ряд удобных моментов, но к явным плюсам JQuery можно отнести следующие:

- небольшой объем (15 Кб в сжатом виде);
- совместимость с основными браузерами.

И еще одно несомненное преимущество – это то, что библиотека может претендовать на то, чтобы стать стандартом в веб-разработке. Ведь не спроста такой софтверный монстр как Microsoft собирается включить ее в состав своего набора инструментов Visual Studio.

Следует обратить внимание на еще один немаловажный момент. Дело в том, что одним из ключевых понятий программирования является пространство имен (namespacing). JavaScript предоставляет разработчику одно глобальное пространство имен – объект window. Зачастую при написании кода программисту приходится его «замусоривать», добавляя без надобности глобальные переменные. JQuery решает эту проблему, добавляя в это пространство лишь один объект – функцию jQuery. Все остальное является либо свойствами, либо методами этого объекта.

Первое знакомство

Библиотека JQuery была впервые опубликована на компьютерной конференции «BarCamp» в Нью-Йорке Джоном Ресигом (John Resig) в 2006 году. Спустя некоторое время она уже завоевала популярность у веб-разработчиков. Данный фреймворк базируется на взаимодействии JavaScript и DOM HTML-документа. К основным возможностям можно отнести следующие:

- переход по дереву DOM, включая поддержку XPath как плагина;
- обработка событий;
- визуальные эффекты;
- AJAX-дополнения.

В качестве базиса в нее заложен выбор CSS-селекторов, в том числе в стиле XPath, и не менее изящное решение, последовательный вызов методов в виде цепочек.

Для начала нам понадобятся дистрибутив фреймворка, который можно скачать на официальном сайте разработчика [1], и тестовая веб-страница. Для подключения библиотеки к нашей веб-странице нужно всего лишь добавить ссылку на сценарий в контейнере <head>:

```
<head>
<script type="text/javascript" ↵
      src="путь к файлу/jquery.js"></script>
</head>
```

Для первого знакомства давайте рассмотрим один интересный пример. В качестве этого можно привести плагин imgAreaSelect, распространяемый по лицензиям MIT и GPL (лицензии на свободное ПО). Его разработал польский программист Михал Войцеховски (Michal Wojciechowski) [4]. Для этого потребуется скачать сам плагин [5], разархивировать и подключить его к нашей странице в контейнер <head>, как было описано выше. Далее создаем в нашей странице код:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; ↵
      charset=windows-1251" />
<title>Jquery</title>
<script src="js/jquery-1.2.6.js"></script>
<script src="js/jquery.imgareaselect-0.6.1.js"></script>
<script language="JavaScript" type="text/javascript">
var $x1, $y1, $x2, $y2, $w, $h;

 function selectChange(img, selection)
 {
   $x1.text(selection.x1);
   $y1.text(selection.y1);
   $x2.text(selection.x2);
   $y2.text(selection.y2);
   $w.text(selection.width);
   $h.text(selection.height);
 }

 $(document).ready(function(){
   $x1 = $('#x1');
   $y1 = $('#y1');
   $x2 = $('#x2');
   $y2 = $('#y2');
   $w  = $('#w');
   $h  = $('#h');
  });

 $(window).load(function(){
   $('img#flower').imgAreaSelect({ selectionOpacity: 0, ↵
      onSelectChange: selectChange });
  });
</script>
</head>
<body>
<div style="float: left;">
  <img id="flower" src="flower.jpg" />
 </div>
 <div style="float: left; margin-left: 10px;">
  <p style="background: #eee; border: solid 1px #ddd; ↵
      margin: 0; padding: 10px;">
   <b>Координаты выделения:</b><br />

   <b>X<sub>1</sub>:</b> <span id="x1"></span><br />
   <b>Y<sub>1</sub>:</b> <span id="y1"></span><br />
   <b>X<sub>2</sub>:</b> <span id="x2"></span><br />

   <b>Y<sub>2</sub>:</b> <span id="y2"></span><br />
   <br />
   <b>Размеры выделения:</b><br />
   <b>Width:</b> <span id="w"></span><br />
   <b>Height:</b> <span id="h"></span>
  </p>
 </div>
</body>
</html>
```

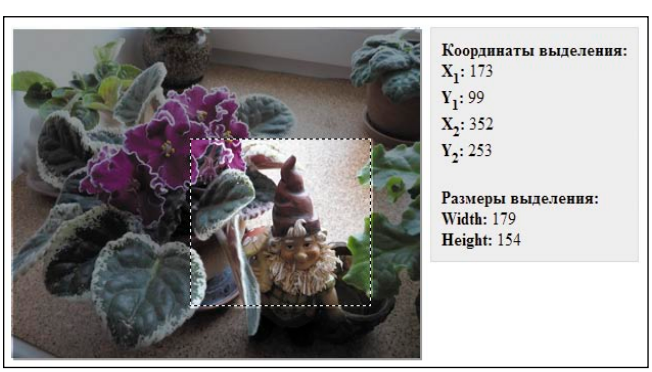


Рисунок 1. Пример работы плагина imgAreaSelect

В качестве тестового изображения подойдет любой, не слишком больших размеров рисунок. Результат работы плагина можно посмотреть на **рис. 1**.

На этом простом примере вы можете убедиться, с какой легкостью и простотой фреймворк позволяет создавать необычные эффекты.

Ну а теперь можно заняться изучением инструментария, который JQuery в огромном количестве предоставляет разработчику для манипуляции элементами документа и их свойствами. Давайте же кратко рассмотрим некоторые из них, а также ряд особенностей работы с ними.

Магическая функция $

Как говорилось выше, фреймворк JQuery вводит в глобальное пространство имен функцию jQuery. Но кроме этого используется также функция $, которая является алиасом вышеназванной функции и гораздо чаще используется при написании кода.

```
//Код:
jQuery('div.panel');

//Эквивалентен коду:
$('div.panel');
```

Посмотрите на эти примеры. Они полностью эквивалентны, но второй пример кода, несомненно, выглядит более изящно. Но как же быть, если вы используете в проекте еще одну библиотеку, например, Prototype, в которой также используется функция $? Чтобы не возникало конфликтов, в JQuery на этот счет предусмотрены следующие решения:

```
jQuery.noConflict();
```

После вызова этой функции все обращения к $ будут адресованы библиотеке Prototype. Другой способ – создание анонимной функции:

```
(function($) {
   // Внутри этого блока $ относится к jQuery
})(jQuery);
```

Внутри этого блока можно использовать функцию $, не опасаясь коллизий при использовании другой одноименной глобальной функции.

Готовим плацдарм

Большинство библиотек JavaScript часто используют событие window.onload. Оно вызывается после того, как документ полностью загрузился в окне браузера. Это значит, что вызываемый в обработчике этого события код не сработает, пока не загрузятся все изображения, флешбаннеры, видеоролики и другой мультимедийный контент страницы.

JQuery предлагает очень изящное решение этой проблемы, а именно функцию ready().

```
$(document).ready(function() {
   //Ваш код
});
```

Внутри этого блока код будет выполнен сразу после того, как будет готова объектная модель документа, но раньше, чем произойдет событие window.onload.

Выбираем элементы

В JQuery реализован очень интересный механизм поиска элементов, использующий CSS и XPath. То есть для нахождения требуемого элемента DOM вы можете воспользоваться как механизмом селекторов CSS, так и запросами по документу в стиле XPath.

XPath (XML Path Language) является языком для обращения к частям XML-документа. HTML, или, вернее, XHTML, является подмножеством XML, и совершенно логично, что не существует причин, по которым с помощью XPath нельзя было бы обращаться к частям HTML-документа. Вернее, их не существует для jQuery, так как эта библиотека поддерживает довольно большое подмножество XPath и легко объединяет его с некоторыми селекторами CSS для создания невероятно гибкого механизма поиска элементов на странице. Чтобы было более понятно, приведу несколько примеров.

Все элементы с атрибутом class="block":

```
$('.block');
```

Элемент p с атрибутом с id="plain":

```
$('p#plain');
```

Все видимые ссылки внутри элмента div с атрибутом id="content":

```
$('div#content a:visible');
```

Все четные строки в таблице с атрибутом class="orders":

```
$('table.orders tr:odd');
```

Все поля ввода с атрибутом name="email":

```
$('input[@name=email]');
```

Все внешние ссылки (то есть те, которые начинаются с http://);

```
$('a[@href^="http://"]');
```

Все элементы p, в которых есть хотя бы одна ссылка:

```
$('p[a]');
```

Все элементы span, являющиеся прямыми потомками элемента p, расположенные в блоке div с атрибутом id="container":

```
$('div#container p/span');
```

Как мы видим, в сочетании эти два метода дают веб-разработчику очень гибкий инструмент для выбора элементов.

Изменяем элементы

Объекты, которые возвращает функция jQuery, имеют некоторые интересные особенности.

С одной стороны, это набор элементов DOM, который обладает свойствами массива, имеет свойство lenght, к каждому элементу можно получить доступ по индексу.

С другой стороны, это объект JQuery, который имеет большой набор методов, с помощью которых можно изменять данные элементы.

Нет смысла описывать все доступные методы, это можно посмотреть в технической документации [3], приведу лишь несколько примеров.

Выставляет ширину блока div с атрибутом id="block" в 300 пикселей:

```
$('div#block').width(300);
```

Изменяет цвет элементов p с атрибутом class="title":

```
$('p.title').css('color', '#ff0000');
```

Применяет 2 CSS-правила для каждого нечетного пункта списка:

```
$('li:odd').css({color: 'white', backgroundColor: 'black'});
```

Добавляет стилевой класс external для всех внешних ссылок (то есть тех, которые начинаются с http://), затем добавляет для них атрибут target="_blank":

```
$('a[@href^="http://"]').addClass('external'). ↵
      attr('target', '_blank');\
```

Для каждого тега span на странице выводит сообщение alert() с его текстовым содержанием (включая HTML-теги):

```
$('span').each(function(el){alert($(this).text())});
```

Заменяет весь текст в ссылках на странице текстом «Нажми здесь!»:

```
$('a').html('Нажми здесь!');
```

Следует отметить, что методы JQuery обладают симметрией, то есть их можно использовать не только для изменения атрибутов элементов, но и для получения значений этих атрибутов.

Возвращает ширину первого элемента div на странице:

```
var width = $('div').width();
```

Возвращает значение атрибута src у первого элемента img на странице:

```
var src = $('img').attr('src');
```

Возвращает значение цвета первого элемента h1 на странице:

```
var color = $('h1').css('color');
```

Как было сказано выше, объект, возвращаемый функцией $, обладает свойствами массива, поэтому к любому элементу можно обратиться по индексу:

```
$('p')[0].className = "myclass";
```

В том случае, если вам необходимо пройтись по всем элементам коллекции и выполнить над ними какие-то действия, можно использовать метод each():

```
$('p').each(
    function(){
        //Действия над элементом
    }
);
```

В качестве параметра each() принимает функцию, которая работает в контексте найденного элемента, поэтому в ней можно использовать переменную this, указывающую на текущий элемент.

Магические цепочки (собираем все вместе)

Одной из важных особенностей JQuery является возможность объединять для преобразований в цепочки несколько вызовов селекторов. Это было показано в одном из вышеприведенных примеров. Давайте же рассмотрим эти возможности более подробно на примере связанной анимации. В нашей тестовой страничке создадим код:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; ↵
      charset=windows-1251" />
<title>Jquery</title>
<style type="text/css">
#run{
      border: solid 1px #000000;
      background-color: #8080ff;
      width: 100px;
      height: 100px;
      position: absolute;
      top: 40px;
      left: 20px;
}
</style>
<script src="js/jquery-1.2.6.js"></script>
<script language="JavaScript" type="text/javascript">
$(document).ready(function(){
      $('a').click(function(){
                $('div#run').
                 slideUp('slow').
                 slideDown('slow').
                 animate({opacity: 'hide', left: '+=400'}, ↵
                         500).
                 animate({opacity: 'show', left: '-=400'}, ↵
                         1000);
      });
```

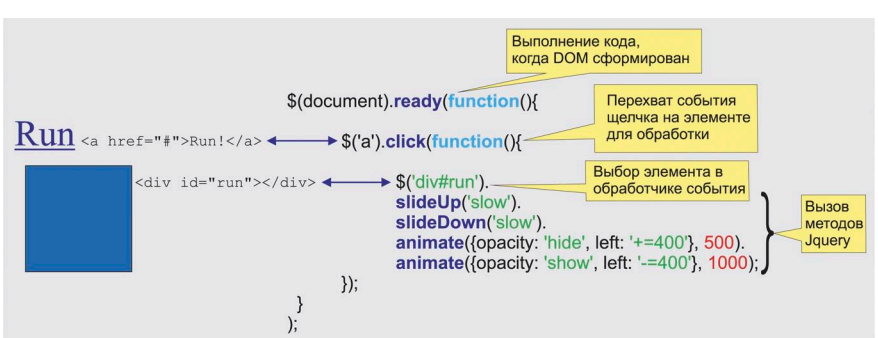


Рисунок 2. Пример реализации функций

```
  }
);
</script>
</head>
<body>
<a href="#">Run!</a>
<div id="run"></div>
</body>
</html>
```

И подробнее рассмотрим, что же происходит на этой странице (см. **рис. 2**).

Как видно из примера, к элементу div с атрибутом id="run" применяется сразу несколько методов, выстроенных в цепочку, которые будут выполняться один за другим:

- **slideUp** – медленно скрыть элемент вверх;
- **slideDown** – медленно отобразить элемент сверху;
- **animate** – применить к элементу анимацию.

Несомненно, что с помощью этого можно достичь высокой гибкости в разработке. Приблизительный результат работы этого сценария выглядит, как показано на **рис. 3**.

Магические превращения

В предыдущем примере мы затронули еще один интересный метод JQuery, а именно метод animate(). Давайте рассмотрим его более подробно. Он является одной из ключевых функций библиотеки, на которой базируются другие эффекты:

```
animate(params, speed, easing, callback);
```

Параметрами этой функции являются:

- **params** – обязательный параметр, свойства анимации в виде пар {ключ: значение};
- **speed** – обязательный параметр, скорость анимации в миллисекундах;
- **easing** – необязательный параметр, замедление анимации (easein – замедление к концу, easeout – ускорение);
- **callback** – необязательный параметр, функция, которая будет вызвана после завершения анимации.

Функция animate является основой большинства, если не всех, эффектов JQuery. Необходимо также отметить, что эффекты применяются к элементам не сразу, а по очереди. Например, если мы написали такой код:

```
for(var i = 0; i < 10; i++){
    $('mydiv').animate({opacity: 'hide'}, 300);
    $('mydiv').animate({opacity: 'show'}, 300);
}
```

мы получим плавное изменение прозрачности элемента независимо от скорости выполнения цикла. Также следует обратить внимание на то, что очередь эффектов составляется поэлементно, то есть эффекты, примененные к разным элементам одновременно, будут выполняться одновременно.

Рисунок 3. Результат работы сценария

Давайте вернемся к нашей тестовой странице и создадим в ней следующий код:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; ↵
      charset=windows-1251" />
<title>jQuery</title>
<style type="text/css">
.block{
      height: 100px;
      width: 100px;
      border: solid 1px #000000;
      background-color: #8080ff;
      margin: 5px;
}
#button{
      border: solid 1px #808080;
      background-color: #dfdfdf;
      height: 30px;
      width: 100px;
      margin: 5px;
      text-align: center;
      cursor: pointer;
      font-family: Arial;
}
</style>
<script src="js/jquery-1.2.6.js" ↵
      type="text/javascript"></script>
<script type="text/javascript">
$(document).ready(function(){
    $('#button').click(function(){
                $('#block1').
                 animate({opacity: 'hide'}, 500).
                 animate({opacity: 'show'}, 1000);
                $('#block2').
                 animate({opacity: 'hide'}, 500).
                 animate({opacity: 'show'}, 1000);
      });
});
</script>
</head>
<body>
<div id="button">Go</div>
<div class="block" id="block1"></div>
<div class="block" id="block2"></div> </body>
</html>
```

В приведенном примере к разным элементам '#block1' и '#block2' одновременно применены одинаковые методы animate(), которые будут выполняться также одновременно.

Манипуляция свойствами элементов на странице позволяет разработчикам получать такие визуальные эффекты, которые раньше были возможны только при использовании технологии Flash. Это и плавное появление, и сокрытие объектов, плавное изменение различных свойств (цвета, размеров), движение объектов, реализация всевозможных элементов интерфейса: деревьев, drag-drop объектов и сортируемых списков.

В базовой поставке jQuery предлагает лишь ограниченный набор таких эффектов. Остальные можно реализовать при помощи модулей расширения, о которых пойдет речь дальше.

Помоги себе сам

Одним из основных показателей качества библиотеки является ее расширяемость. Разумеется, эта особенность в полной мере присуща и JQuery. Она имеет очень удобный API для расширения собственной функциональности. Любой разработчик может с легкостью написать под нее свой

плагин, реализующий свои методы, эффекты и даже селекторы. Достаточно следовать некоторым простым правилам. Чтобы было более понятно, давайте рассмотрим это на простом примере.

Для начала придумаем назание нового плагина, например, myplugin. Далее создадим JavaScript файл jquery.myplugin.js. Для добавления в плагин нового метода, который будет доступен сразу из функции $, достаточно добавить его в объект fn.

Запишем код в созданный файл:

```
jQuery.fn.myplugin = function()
{
  alert("Мой плагин!");
  return this;
};
```

Теперь вернемся к нашей тестовой странице и создадим в ней код:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; ↵
      charset=windows-1251" />
<title>jQuery</title>
<script src="js/jquery-1.2.6.js" ↵
      type="text/javascript"></script>
<script src="js/jquery.myplugin.js" ↵
      type="text/javascript"></script>
<script type="text/javascript">
$(document).ready(
  function()
  {
       $("#mydiv").myplugin();
  }
);
</script>
</head>
<body>
<div id="mydiv"></div>
</body>
</html>
```

Плагин работает! Следует обратить внимание на то, что в конце функции мы написали return this. Это необходимо для того, чтобы можно было создавать цепочки из методов. Но это еще не все. Скорее всего, нам понадобится вызов метода с передачей в него параметров, например, в таком виде:

```
$("#mydiv"). myplugin(
  {
    key: "action",
    value: "test"
  }
);
```

Для этого можно использовать метод extend:

```
$.extend(target, property1, ..., propertyN)
```

В данном методе:

- **target** – начальный объект;
- **property1 – propertyN** – объекты, свойства которых дополняют или изменяют начальный объект.

Таким образом, мы можем хранить в плагине значения по умолчанию и заменять их параметрами, полученными от пользователя. Теперь код нашего плагина может иметь такой вид:

```
jQuery.fn.myplugin = function(options)
{
  // Начальные параметры
  var settings = {default: "Мой плагин!", value: ""};

  // Замена параметров
  settings = jQuery.extend(settings, options);

  // Вывод новых значений
     if(settings.value == "")
         alert("Значение по умолчанию: " + ↵
               settings.default);
     else
       alert("Полученное значение: " + settings.value);
  return this;
};
```

Заменив в нашей тестовой странице строку, чтобы вызвать плагин с новыми параметрами:

```
$("#mydiv").myplugin({value: "Новое значение"});
```

мы видим, что код нашего расширения также выполняется с учетом нововведений.

И снова AJAX

Эпоха WEB 2.0 обязывает разработчика использовать при создании интерактивных веб-интерфейсов подход, заключающийся в фоновом обмене данными с сервером. Разумеется, речь идет об AJAX – технологии, которая в JQuery поддерживается в полной мере. По мнению некоторых разработчиков, данная библиотека имеет самый удобный API для работы с AJAX.

Для тестирования работы AJAX нам потребуется настроенный веб-сервер с любым интерпретатором серверного языка программирования, в нашем случае это будет PHP. Базовыми функциями для работы с AJAX в JQuery являются функции post() и get():

```
$.post(url[, params[, callback]])
$.get(url[, params[, callback]])
```

В данных функциях:

- **url** – адрес страницы, на которую будет отправлен запрос;
- **params** – параметры, передаваемые в запросе в виде пар {ключ: значение};
- **callback** – функция, которая будет вызвана в случае успешного завершения вызова.

Эти функции очень похожи друг на друга, отличаются лишь методом отправляемого запроса: POST или GET соответственно. Например, POST-запрос к странице test.php с параметрами action и id и вызов функции onGetAjax в случае успеха:

```
$.post(
  '/test.php',
  {
    action: 'news',
    id: 5
  },
  onGetAjaxs
);
function onGetAjax(data)
{
  // Получение данных, отправленных сервером
  alert(data);
}
```

Асинхронный запрос к странице ничем не отличается от обычного ее вызова, например, через окно браузера, то есть переданные данные будут доступны в ней точно так же, как если бы они были переданы обычным GET- или POST-запросом.

Обратите также внимание на то, что иногда необходимо знать, каким образом была отправлена страница – запросом в браузер или через AJAX. Для этого при запросе через AJAX устанавливается HTTP заголовок HTTP_X_REQUESTED_WITH со значением XmlHTTPRequest.

На сервере при помощи PHP это можно узнать следующим образом:

```
<?php
if($_SERVER['HTTP_X_REQUESTED_WITH'] == 'XMLHttpRequest')
{
  // выполнение кода
}
?>
```

Еще один метод для работы с AJAX, который необходимо упомянуть, – это метод load():

```
load(url);
```

Здесь:

- **url** – адрес запрашиваемой страницы на сервере.

Он передает в какой-либо элемент результат работы серверного сценария. Рассмотрим это на небольшом примере.

Допустим, у нас на сервере есть файл test.php:

```
<?php
  echo 'Текст сформированный сервером';
?>
```

А в нашей тестовой странице следующий код:

```
$('div#mydiv').load('test.php');
```

В результате работы этого сценария в блок div с id="mydiv" будет записан текст, сформированный скриптом, содержащимся в файле test.php, а именно фраза «Текст, сформированный сервером».

Помимо вышеперечисленных методов работы с AJAX у разработчиков пользуется популярностью JSON. Это формат записи данных в виде пар {ключ1: значение1, ключ2: значение2}, который можно легко преобразовать в JavaScript объект. Вот пример записи данных в виде JSON:

```
{
   "firstName": "Иван",
   "lastName": "Иванов",
   "address": "streetAddress": "Московское ш., 101, кв.101",
   "phoneNumbers": "812 123-1234"
}
```

Для работы с ним в JQuery есть метод getJSON():

```
getJSON(url, params, callback)
```

Здесь:

- **url** – адрес серверной страницы;
- **params** – параметры в виде {ключ: значение};
- **callback** – вызываемая функция.

Чтобы было понятнее, воспользуемся опять простым примером. Код нашего тестового файла на сервере test.php:

```
<?php
if($_SERVER['HTTP_X_REQUESTED_WITH'] == 'XMLHttpRequest')
{
  echo '{param: '.$_REQUEST['param'].', response: ↵
      "Ответ сервера"}';
}
?>
```

В тестовую страницу вставьте код:

```
$(document).ready(function(){
      $.getJSON('test.php', {param: 10}, onGetAjax);
      function onGetAjax(data)
      {
          alert(data.param + ' ' + data.response);
      }
});
```

После прохождения запроса ответ с сервера обрабатывается функцией eval() и полученный объект передается в функцию onGetAjax().

Следует также обратить внимание на еще один метод, который предоставляет JQuery, это метод getScript(). С его помощью можно загрузить и выполнить любой JavaScript сценарий. Например, если у нас есть сценарий jstest.js:

```
$('a').css('color', '#ff0000');
```

то после выполнения кода:

```
$.getScript('jstest.js');
```

все гиперссылки страницы будут окрашены в красный цвет.

Эпилог

Разумеется, в рамках данной статьи невозможно охватить весь инструментарий, которым располагает библиотека JQuery. Вы в любой момент можете воспользоваться технической документацией на официальном сайте фреймворка [3], а также онлайн-документацией [6], но в любом случае это не будет пустой тратой времени. Познакомившись с JQuery ближе, вы, несомненно, поймете, насколько это удобный и гибкий фреймворк, покрывающий огромный диапазон функций, предоставляя при этом удобный API для расширения собственной функциональности, работы с AJAX, визуальными эффектами и многим другим.

1. http://jquery.com – официальный сайт разработчиков JQuery.
2. http://docs.jquery.com/License – лицензионное соглашение.
3. http://docs.jquery.com – техническая документация.
4. http://odyniec.net – Михал Войцеховски.
5. http://odyniec.net/projects/imgareaselect/imgareaselect-0.6.1.zip – плагин imgAreaSelect
6. http://www.visualjquery.com – онлайн-справочник библиотеки JQuery.

Множественные уязвимости в Sun Java JDK и JRE

Программа: Java Web Start 1.x; Java Web Start 5.x; Java Web Start 6.x; Sun Java JDK 1.5.x; Sun Java JDK 1.6.x; Sun Java JRE 1.3.x; Sun Java JRE 1.4.x; Sun Java JRE 1.5.x/5.x; Sun Java JRE 1.6.x/6.x; Sun Java SDK 1.3.x; Sun Java SDK 1.4.x.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за того, что Java Runtime Environment (JRE) создает временные файлы с предсказуемыми именами. Злоумышленник может записать произвольные JAR-файлы и произвести запрещенные действия на уязвимой системе.

2. Уязвимость существует из-за ошибки в библиотеке Java AWT при обработке моделей изображений. Удаленный пользователь может с помощью специально сформированной растровой модели изображения, используемой в операции ConvolveOp, вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за ошибки при обработке заголовков GIF-изображений в Java Web Start. Удаленный пользователь может с помощью специально сформированного GIF-изображения вызвать повреждение памяти.

4. Целочисленное переполнение обнаружено при обработке TrueType-шрифтов. Удаленный пользователь может вызвать переполнение динамической памяти и скомпрометировать целевую систему.

5. Уязвимость существует из-за ошибки в JRE, которая позволяет злоумышленнику создать сетевые соединения к произвольным хостам.

6. Уязвимость существует из-за ошибки при запуске Java Web Start-приложений. Злонамеренное недоверенное приложение может получить доступ на чтение, запись и выполнение приложений с привилегиями пользователя, запустившего приложение.

7. Уязвимость существует из-за ошибки, которая позволяет недоверенному Java Web Start-приложению получить имея текущего пользователя и данные о расположении Java Web Start-кэша на системе.

8. Уязвимость существует из-за ошибки в Java Web Start, которая позволяет злоумышленнику с помощью специально сформированного JNLP-файла изменить системные настройки (например, java.home, java.ext.dirs и user.home).

9. Уязвимость существует из-за ошибки в Java Web Start и Java-плагине, которая позволяет злоумышленнику внедриться в HTTP-сессию пользователя.

10. Уязвимость существует из-за ошибки в функционале загрузки классов JRE-апплетов. Удаленный пользователь может просмотреть содержимое произвольных файлов на системе и создать сетевые подключения к произвольным хостам.

11. Уязвимость существует из-за ошибки в Java Web Start BasicService, которая позволяет открыть произвольные локальные файлы в браузере пользователя.

12. Уязвимость существует из-за того, что механизм Java Update не проверяет цифровые подписи загруженных обновлений. Удаленный пользователь может с помощью атаки «человек посредине» или DNS-спуфинг атаки скомпрометировать целевую систему.

13. Уязвимость существует из-за ошибки проверки границ данных при обработке Main-Class-строк в JAR-файле. Удаленный пользователь может с помощью специально сформированного JAR-файла вызвать переполнение стека и выполнить произвольный код на целевой системе.

14. Уязвимость существует из-за ошибки при десериализации объектов календаря. Недоверенный Java-апплет может прочитать, записать и выполнить произвольные файлы на системе.

15. Целочисленное переполнение обнаружено в JRE. Удаленный пользователь может с помощью специально сформированного Pack200-сжатого JAR-файла вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

16. Уязвимость существует из-за того, что декодер UTF-8 принимает кодировки длиной более чем форма shortest. Злоумышленник может с помощью специально сформированного URI заставить приложение принять некорректные последовательности и получить доступ к важным данным.

17. Уязвимость существует из-за ошибки в JRE, которая позволяет злоумышленнику просмотреть содержимое домашней директории пользователя.

18. Уязвимость существует из-за ошибки при обработке публичных RSA-ключей. Удаленный пользователь может с помощью специально сформированного RSA-ключа потребить большое количество системных ресурсов.

19. Уязвимость существует из-за ошибки в механизме аутентификации JRE Kerberos. Удаленный пользователь может потребить большое количество системных ресурсов.

20. Уязвимость существует из-за различных ошибок в JAX-WS- и JAXB JRE-пакетах. Недоверенный Java-апплет может прочитать, записать и выполнить произвольные файлы на системе.

21. Уязвимость существует из-за ошибки при обработке ZIP-файлов. Злоумышленник может с помощью специально сформированного ZIP-архива получить доступ к произвольным участкам памяти на системе.

22. Уязвимость существует из-за ошибки, которая позволяет злонамеренному коду, загруженному из локальной файловой системы, получить сетевой доступ к локальному хосту.

23. Уязвимость существует из-за ошибки проверки границ данных при обработке TrueType-шрифтов. Удаленный пользователь может с помощью специально сформированного TrueType-шрифта вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

URL производителя: java.sun.com.

Решение: Установите исправление с сайта производителя.

Составил Александр Антипов

WinBinder PHP. Создаём GUI-интерфейс за 2 клика

Александр Майоров

Сегодня уже никого не удивить инструментами для создания приложений с GUI-интерфейсом на скриптовых языках. PHP не исключение, и об этом были статьи, в частности, про PHP-GTK. Но не все знают, что кроме PHP-GTK существуют другие библиотеки, одна из которых – WinBinder.

Что это?

WinBinder – это библиотека для создания приложений с графическим интерфейсом на языке программирования PHP. Наверное, не стоит говорить о том, какое большое распространение получил этот язык в настоящее время. PHP является очень популярным языком сценариев, который используется главным образом для веб-разработок, но также набирает популярность как язык скриптов общего назначения. Надёжно укрепив свои позиции на серверах, теперь переходит в другие секторы, и десктопы не исключение. Об этом свидетельствует появление таких библиотек, как PHP-GTK, PHP-Qt и собственно WinBinder, о котором мы собрались поговорить.

Препарируем WinBinder

Давайте теперь детально рассмотрим, что из себя представляет фреймворк WinBinder. Это расширение для PHP с открытым исходным кодом. Оно позволяет PHP-программистам быстро и легко разрабатывать Windows-приложения. Среди основных особенностей WinBinder можно упомянуть непосредственное взаимодействие с программным интерфейсом операционной системы Microsoft Windows, небольшой размер конечных файлов приложений (при компиляции скриптов с помощью утилиты bamcompile), обширную базу всевозможных PHP-функций, возможность как объектноориентированного, так и процедурного программирования, а также удобство использования.

WinBinder состоит из DLL-библиотеки, которая фактически является PHP-расширением небольшого набора вспомогательных скриптов и файлов. На **рис. 1** представлена схема работы приложения, написанного с использованием данного расширения.

Связь между компонентами в WinBinder реализована через механизм обратных вызовов. Windows-сообщения, генерируемые контроллерами и таймерами, транслируются в одиночные callback-события, которые можно легко перехватить в PHP-программе. Каждое сообщение имеет свой целочисленный идентификатор, по которому его можно идентифицировать.

Библиотека WinBinder фактически состоит из двух слоев, взаимодействующих между собой. Первый слой – это нижний уровень, называемый API-слоем. Данный слой напрямую связан с Windows API и предоставляет единый интерфейс для более высокоуровневого слоя – слоя PHP. Хотя функции на нижнем уровне представляют из себя обертки для Windows API вызовов, большинство из них являются больше чем просто обертки вокруг API. Они инкапсулируют работу Windows-функций и упрощают доступ к ним.

Например, Windows использует различные сообщения для установки числовых значений для таких компонент, как progress-bar, scroll-bar и т. д. И хотя существует явное сходство между этими элементами управления при генерации сообщений, их аргументы различны. Примеры генерации сообщений (см. **таблицу**).

Одна из целей WinBinder как раз заключается в том, чтобы изолировать программиста от всех этих сложностей, предоставляя функционал библиотеки. API-слой выполняет всю работу через единую функцию wbSetValue(), которая имеет

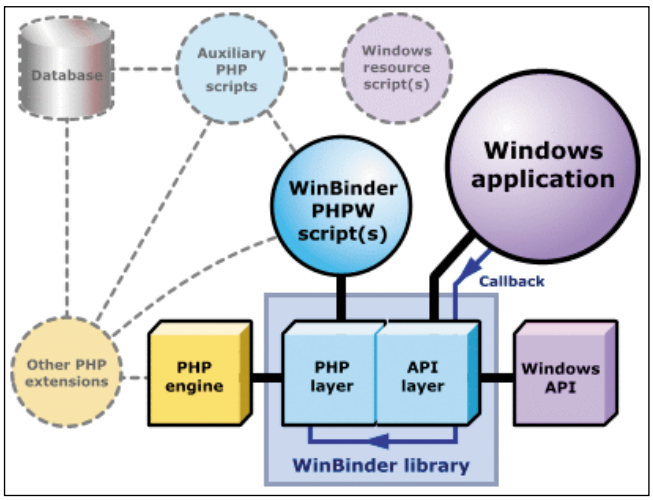


Рисунок 1. Схема взаимодействия компонентов в приложении на WinBinder

единый интерфейс для управления всеми объектами. Эта функция, кстати, применима ко всем без исключения компонентам Windows, начиная от простых лэйблов и полей ввода и заканчивая такими сложными компонентами, как компоненты для форматированного вывода текста, пунктов меню и прочего, устраняя тем самым необходимость использовать функции для каждого класса (к примеру, это были бы функции wbSelect, wbCheck и т. д.).

Собственно второй слой, который мы уже упоминали выше, – это слой PHP, который эффективно связывает Windows API с Zend Engine, создавая новый набор пользовательских функций PHP. Многие из этих функций имеют префикс wb_, например, wb_set_value(), которую вам придется часто использовать для установки значения объектам.

Результатом двухслойной архитектуры WinBinder является набор простых и удобных в использовании функций, упрощающих работу с Windows API-интерфейсом. Например, чтобы присвоить иконку для окна приложения, нужно вызвать функцию wb_set_image(). Её прототип выглядит следующим образом:

```
bool wb_set_image (int wbobject, mixed source, ↵
      int transparentcolor, int index, int param)
```

Достаточно передать идентификатор объекта и ресурс. В качестве ресурса может быть как графический файл, так и DLL-библиотека или исполняемый файл, содержащие в себе графические ресурсы (для этого указывается индекс ресурса внутри бинарного файла – index). Та же функция используется и для растровых изображений, применяемых к любому объекту, хоть списки, хоть проводник с деревом. Таким образом, программист освобождается от всех тонкостей работы с Windows API, с его множеством функций и сообщений, которые скрыты от глаз PHP-программиста.

Еще одним преимуществом такой архитектуры WinBinder является то, что можно создавать переплеты

Примеры генерации сообщений

Scroll bars	SendMessage(hCtrl, SBM_SETPOS, (WPARAM)dwValue, TRUE);
Track bars	SendMessage(hCtrl, TBM_SETPOS, TRUE, (LPARAM)(LONG)dwValue);
Progress bars	SendMessage(hCtrl, PBM_SETPOS, (WPARAM)dwValue, 0);
Up/down controls	SendMessage(hCtrl, UDM_SETPOS, 0, (LPARAM)MAKELONG((short)dwValue, 0));

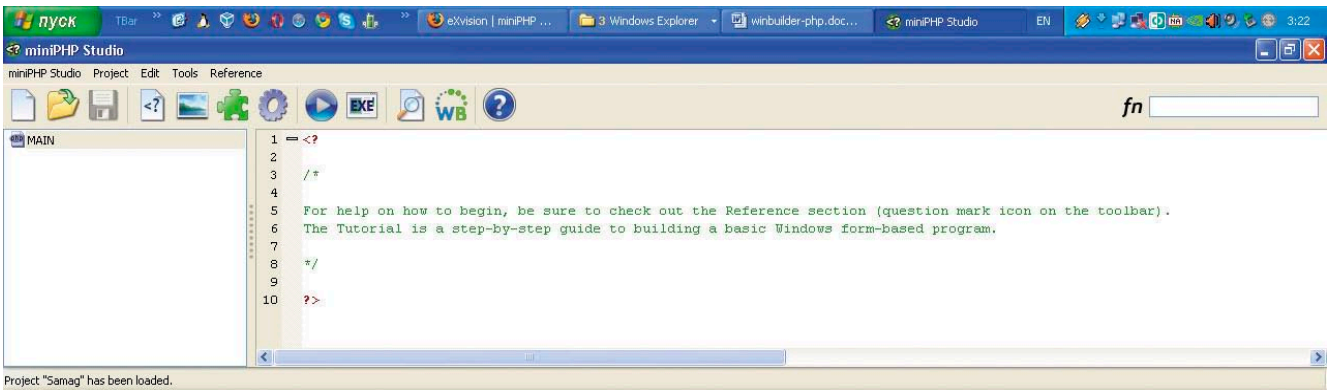


Рисунок 2. Рабочий стол студии

с другими скриптовыми языками программирования, заменив слой PHP на какой-то другой. В этом случае WinBinder будет действовать как основа, каркас, связывающий разнородные компоненты воедино.

Возможна даже замена Windows API-слоя, что позволит делать приложения для других операционных систем, отличных от Windows, но это только в теории. На практике вопросом на данный момент никто не занимается и это не входит в рамки развития проекта. Хотя никто не мешает вам подумать над этим, может быть, кто-то и заинтересуется. Все в ваших руках.

И опять, и снова да здравствует мир во всём мире!

Ну что же, мы разобрали, что такое WinBinder, давайте перейдем теперь к практической части. Библиотеку и нужные компоненты можно скачать с официального сайта http://winbinder.org. Этого достаточно, чтобы писать приложения, но есть одно «но». Как и в случае с PHP-GTK, на компьютере должен быть интепретатор PHP. И что же? Меняем шило на мыло? Не совсем. Да, WinBinder не кроссплатформенный, в отличие от того же PHP-GTK, но он более легок в освоении и программировании. В WinBinder есть графический редактор форм, который позволяет экспортировать их сразу в нативный PHP-код.

Но WinBinder мало чем отличался бы от аналогов, если бы не одна разработка от eXvision. Называется она miniPHP Studio. Эта студия представляет собой простой, но тем не менее удобный редактор PHP-кода, редактор ресурсов и компилятор кода в исполняемый файл. В качестве компилятора в ней используется bamcompile (http://www.bambalam.se/bamcompile). Это очень удобный и наиболее распространенный компилятор PHP в исполняемые exe-файлы. Скомпилированные бинарники сжимаются утилитой UPX (Ultimate Packer for eXecutables – упаковщик исполняемых файлов, поддерживающий несколько различных платформ и форматов файлов). На выходе получается компактная программка с графическим интерфейсом, написанная на PHP. Она готова к распространению, а главное, на компьютере пользователя не нужно что-то дополнительно устанавливать. Все необходимое уже будет включено в бинарный файл и готово к использованию. Также miniPHP Studio позволяет включать в исполняемый файл любой ресурс, будь то графический файл или текстовый, а также включать DLL-библиотеки и расширения PHP.

Теперь заходим на http://exvision.net. Качаем оттуда студию. Установка делается в 2 клика, так что нет смысла её расписывать. Запускаем студию и получаем главное окно – рабочий стол. Жмете в меню «Project → New», задаете имя проекта, пусть у нас будет это Samag. После создания проекта будет сгенерирован главный файл MAIN. Слева вы увидите его. Надо заметить сразу, что это не обозреватель файлов, а проводник ресурсов. Все, что отображается в этом списке, будет скомпилировано в исполняемый файл. Имена ресурсов автоматически генерируются на основе реальных имен файлов. Из имени исключается все лишнее (точки, пробелы, прочее), и оно приводится к верхнему регистру.

Итак. С чего начнем? Банальный «Привет, мир!» нам стоит написать, чтобы быстро показать идеологию проектирования на WinBinder. Сделаем простое окно с текстом и кнопкой Show message (см. **рис. 2**).

Как и в PHP-GTK, чтобы создать форму, нужно описать ее, инициализировать библиотеку и прочее. Но WinBinder тем и хорош, что он позволяет создать форму за два клика. Открываем редактор форм (WinBinder Form Editor). Создаем форму, какую захотим. Давайте кинем на форму кнопку. Назовите её как-нибудь. Теперь выберите из пункта меню File: Export PHP Code. Сохраните форму в файл, к примеру, mainform.php. Далее можно пойти несколькими путями. Самый простой, но не самый правильный – это скопировать содержимое файла mainform.php в нашу открытую рабочую область (файл MAIN). У вас должно получиться:

```
<?php

/*************************************************************

WINBINDER - form editor PHP file (generated automatically)

*************************************************************/

// Control identifiers
if(!defined('IDC_PUSHBUTTON1002')) ↵
      define('IDC_PUSHBUTTON1002', 1002);

// Create window
$winmain = wb_create_window(null, AppWindow, ↵
      'www.samag.ru', WBC_CENTER, WBC_CENTER, 317, 179, ↵
      0x00000000, 0);

// Insert controls
wb_create_control($winmain, PushButton, 'Show message', ↵
      105, 65, 90, 25, IDC_PUSHBUTTON1002, 0x00000000, ↵
      0, 0);

// End controls
?>
```

Этого, правда, недостаточно для запуска. Теперь нам надо инициализировать саму библиотеку, вызвав функцию wb_init() в самом начале файла. Далее нам надо написать и зарегистрировать функцию-обработчик для сообщений Windows. Выглядеть она может так:

```
// Main Window's processor
function main_events_handler($Sender, $id)
{
      switch($id)
      {
                case IDC_PUSHBUTTON1002:
                         wb_message_box($Sender, ↵
                            "Hello world!", ↵
                            "My first test programm");
                         break;

                case IDCLOSE:
                         wb_destroy_window($Sender);
                         break;
      }
}
```

Теперь регистрируем функцию через следующий вызов:

```
wb_set_handler($winmain, "main_events_handler");
```

И вызываем функцию wb_main_loop(), она создает главный цикл программы. Собственно все. Теперь запускаем программу кнопкой Preview project. Есть, правда, маленькое «но». Программа miniPHP Studio написана без разделения на потоки, поэтому при предварительной компиляции будет казаться, что студия повисла. На самом деле это не так. Кстати при компиляции всегда выскакивает окно с сообщением, что студия не может быть активна до окончания процесса компиляции. Делается это не очень быстро, но терпимо. Процесс сборки может достигать минуты, так что не спешите убивать процесс. Итак, делайте предварительную сборку приложения и смотрите, что у вас получилось. Если возникнут ошибки, то студия вам сообщит о них.

Полный исходный код нашего тестового приложения выглядит так (см. **рис. 3**):

```
<?php

wb_init();

/*****************************************************

WINBINDER - form editor PHP file (generated automatically)

*****************************************************/

// Control identifiers
if(!defined('IDC_PUSHBUTTON1002')) ↵
      define('IDC_PUSHBUTTON1002', 1002);

// Create window
$winmain = wb_create_window(null, AppWindow, ↵
      'www.samag.ru', WBC_CENTER, WBC_CENTER, 317, 179, ↵
      0x00000000, 0);
wb_set_handler($winmain, "main_events_handler");

// Insert controls
wb_create_control($winmain, PushButton, 'Show message', ↵
      105, 65, 90, 25, IDC_PUSHBUTTON1002, 0x00000000, ↵
      0, 0);

// End controls

wb_main_loop();

// Main Window's processor
function main_events_handler($Sender, $id)
{
      switch($id)
      {
                case IDC_PUSHBUTTON1002:
                         wb_message_box($Sender, ↵
                            "Hello world!", ↵
                            "My first test programm");
                         break;

                case IDCLOSE:
                         wb_destroy_window($Sender);
                         break;
      }
}

?>
```

Проведем краткий разбор приложения. Вначале мы инициализировали библиотеку, вызвав wb_init(). Затем объявили константу IDC_PUSHBUTTON1002, присвоив ей значение 1002. Это целочисленный идентификатор нашей кнопки. В WinBinder ко всем ресурсам и компонентам доступ происходит через целочисленные идентификаторы, будь то окно, контроллер или сообщение. После мы создали окно с заголовком www.samag.ru. Далее идет регистрация нашего обработчика сообщений wb_set_handler($winmain, "main_events_handler"). В качестве аргументов передается идентификатор окна и название функции обратного вызова. Функция принимает идентификатор объекта-родителя и целочисленный идентификатор сообщения. Внутри функции мы обрабатываем эти сообщения по номерам в конструкции switch. Вы видите нашу объявленную константу IDC_PUSHBUTTON1002 и неизвестную IDCLOSE. Вторая константа – это стандартная константа библиотеки. Подробнее оних можно прочесть в справке, которая идет в комплекте со студией. Ну и, наконец, происходит запуск бесконечного цикла функцией wb_main_loop(). Все. Теперь вы можете скомпилировать вашу программу и распространять ее на любом компьютере с операционной системой Windows.

После сборки на выходе получите исполняемый файл размером примерно полтора мегабайта, готовый к работе и включающий в себя все необходимые библиотеки и ресурсы.

Тестер регулярных выражений

Давайте теперь напишем более полезную программу и немного больше разберемся с WinBinder. Напишем утилиту, с помощью которой можно будет быстро протестировать регулярное выражение на пригодность. Итак, приступим.

Для начала накидаем простейший класс-отладчик, ибо без отладки немыслима разработка. Вся отладочная ин-

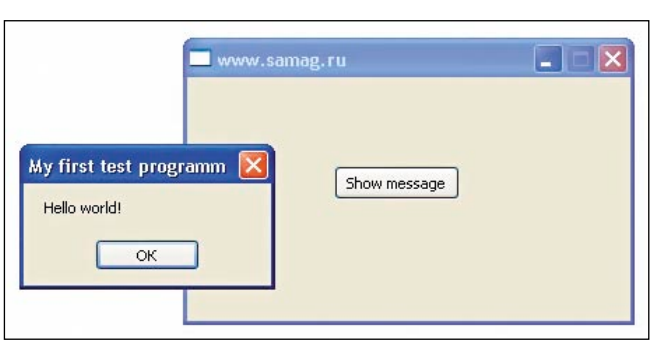


Рисунок 3. Пример работы нашего приложения

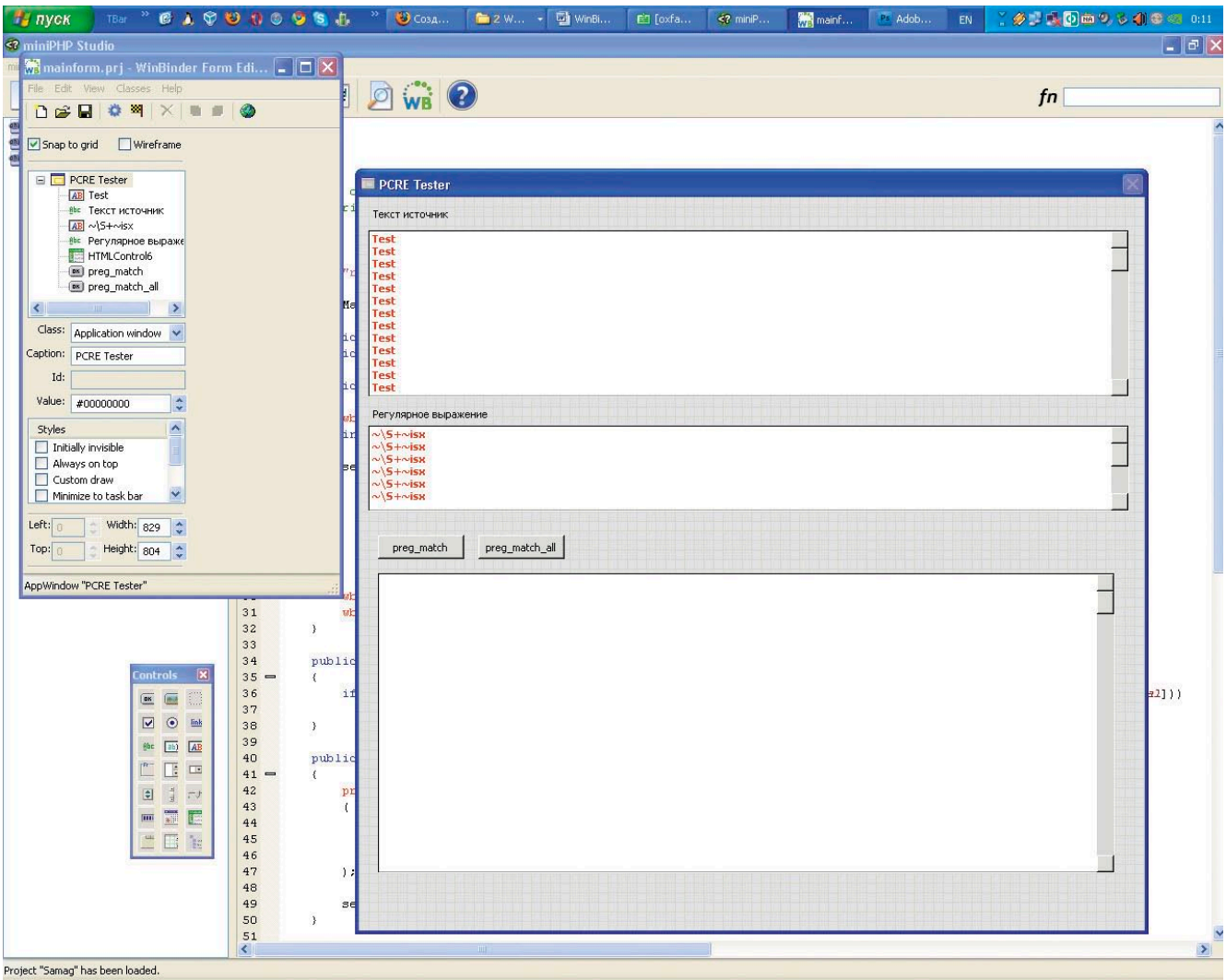


Рисунок 4. Форма будущей программы

формация будет кидаться в текстовый лог-файл, так как это лучший способ отладки. Код нашего отладчика будет следующим:

```
<?php

class Debug
{
      public static $dumpFile = 'dump.log';

      public static function var_dump()
      {
          $args = func_get_args();
          ob_start();
          call_user_func_array('var_dump', $args);
          error_log(ob_get_clean(), 3, self::$dumpFile);
      }

      public static function var_export()
      {
          $args = func_get_args();
          error_log(var_export($args,true), 3, ↵
               self::$dumpFile);
      }
}
?>
```

Это, по сути, обертка для двух функций var_dump() и var_export(), а класс выступает в роли пространства имен. Сохраняем этот код в файл debug.php и подключаем к нашему проекту. Для этого в проводнике ресурсов щелкаете правой кнопкой мыши и выбираете пункт Import a PHP Script. Выбираете файл debug.php и подключаете.

Ресурсы WinBinder

Прежде чем продолжить, я должен рассказать вам про ресурсы WinBinder и как с ними работать. Любой ресурс, импортированный в проект, будет храниться внутри бинарного файла. PHP-скрипты также являются текстовыми ресурсами. Чтобы обратиться к внутреннему ресурсу надо использовать схему res://. Общий прототип именования выглядит следующим образом:

```
"res:///RESOURCETYPE/RESOURCENAME"
```

Это описание внутреннего адреса включенного файла. Тогда, чтобы подключить наш файл debug.php, который стал ресурсом по имени DEBUG, нужно написать следующую строчку:

```
include "res:///PHP/DEBUG";
```

Таким образом, мы подключили внутренний файл. Мы могли этот файл оставить внешним, и тогда его подключать приходилось бы через указание пути к этому файлу.

Этого достаточно для нашего приложения. Более подробно обо всех видах ресурсов написано в справке к библиотеке.

Создаем каркас

Кинем на форму два текстовых поля, две кнопки и компонент для рендеринга HTML кода. Наша форма должна выглядеть примерно так (см. **рис. 4**).

Теперь давайте напишем каркас нашего будущего приложения. Лучше всего его оформить один раз в виде класса и впоследствии использовать во всех ваших приложениях с WinBinder. Каркас будет выглядеть так:

```
<?php

class WBMain
{
      public static $signalsBind = array();
      public static $components = array();

      public static function main()
      {
          wb_init();
          include "res:///PHP/MAINFORMFORM";

          self::$signalsBind =
                array
                (
                    IDCLOSE => 'close'
                ,   IDC_PUSHBUTTON1004 => 'pushButton1'
                ,   IDC_PUSHBUTTON1005 => 'pushButton2'
                );

          wb_set_handler($winmain, ↲
              'WBMain::callSignalHandler');
          wb_main_loop();
      }

      public static function ↲
                callSignalHandler($Window, $signal)
      {
          if (isset(self::$signalsBind[$signal]) && ↲
              is_callable($foo = 'WBMain::signal_' . ↲
              self::$signalsBind[$signal]))
                call_user_func($foo, $Window);
      }

      public static function signal_pushButton1($Window)
      {
          wb_message_box($Window, __METHOD__, '');
      }

      public static function signal_pushButton2($Window)
      {
          wb_message_box($Window, __METHOD__, '');
      }

      public static function signal_close($Window)
      {
          wb_destroy_window($Window);
      }

}

WBMain::main();

?>
```

Здесь мы оформили код приложения в виде класса, с набором статических свойств. Выделили общий контроллер сообщений callSignalHandler(), который, в зависимости от сообщения, вызывает нужную функцию обратного вызова, что удобнее и правильней, чем один большой switch на всю программу. Это почти весь текст программы, за исключением того, что в ней нужно описать логику для кнопок, это методы signal_pushButton1 и signal_pushButton2 соответственно. Можно оформить код программы таким образом, чтобы каждый обработчик представлял собой отдельный класс и хранился в отдельном файле. Это особенно удобно, если у вас очень большая программа. Вы сами решите, как вам удобнее и лучше.

Вернемся к нашим недописанным обработчикам сообщений. Код этих методов выглядит следующим образом. Для кнопки preg_match:

```
public static function signal_pushButton1($Window)
{
    preg_match
    (
          wb_get_text(self::$components ↲
                [IDC_RTFEDITBOX1002]),
          wb_get_text(self::$components ↲
                [IDC_RTFEDITBOX1001]),
          $arrayResults
    );

    self::setResult($arrayResults);
}
```

и аналогичная функция для кнопки preg_match_all:

```
public static function signal_pushButton2($Window)
{
    preg_match_all
    (
          wb_get_text(self::$components ↲
                [IDC_RTFEDITBOX1002]),
          wb_get_text(self::$components ↲
                [IDC_RTFEDITBOX1001]),
          $arrayResults
          );

    self::setResult($arrayResults);
}
```

В обеих функциях вы видите вызов функции setResult(). Это функция, обрабатывающая результат и выводящая его в красивом форматированном виде. Сделано это для сокращения размера программы, так как функционал вывода полностью идентичен для обеих кнопок. Код функции представлен ниже:

```
public static function setResult(array $arrayResults)
{
    $result =
          '<html><head><title>PCRETester</title> ↲
                    </head><body>'
          . highlight_string
                    (
                     "<?php\n\n"
                     . var_export($arrayResults,true)
                     ,true
                    )
          . '</body></html>'
          ;

    static $file;
    if (!$file) $file = getcwd() . '/render.tmp';

    $fp = fopen($file,'w+');
    fwrite($fp, $result);
    fclose($fp);

    wb_set_location(self::$components ↲
          [IDC_HTMLCONTROL1003], $file);
}
```

Вот таким вот нехитрым образом мы выводим дамп массива в формате HTML с результатами. Данные сохраняются во временный файл, который потом загружается в компонент HTMLControl, где происходит рендеринг. Таким вот образом за 5 минут была написана полезная утилита (см. **рис. 5**). Веб-разработчику нет необходимости пере-

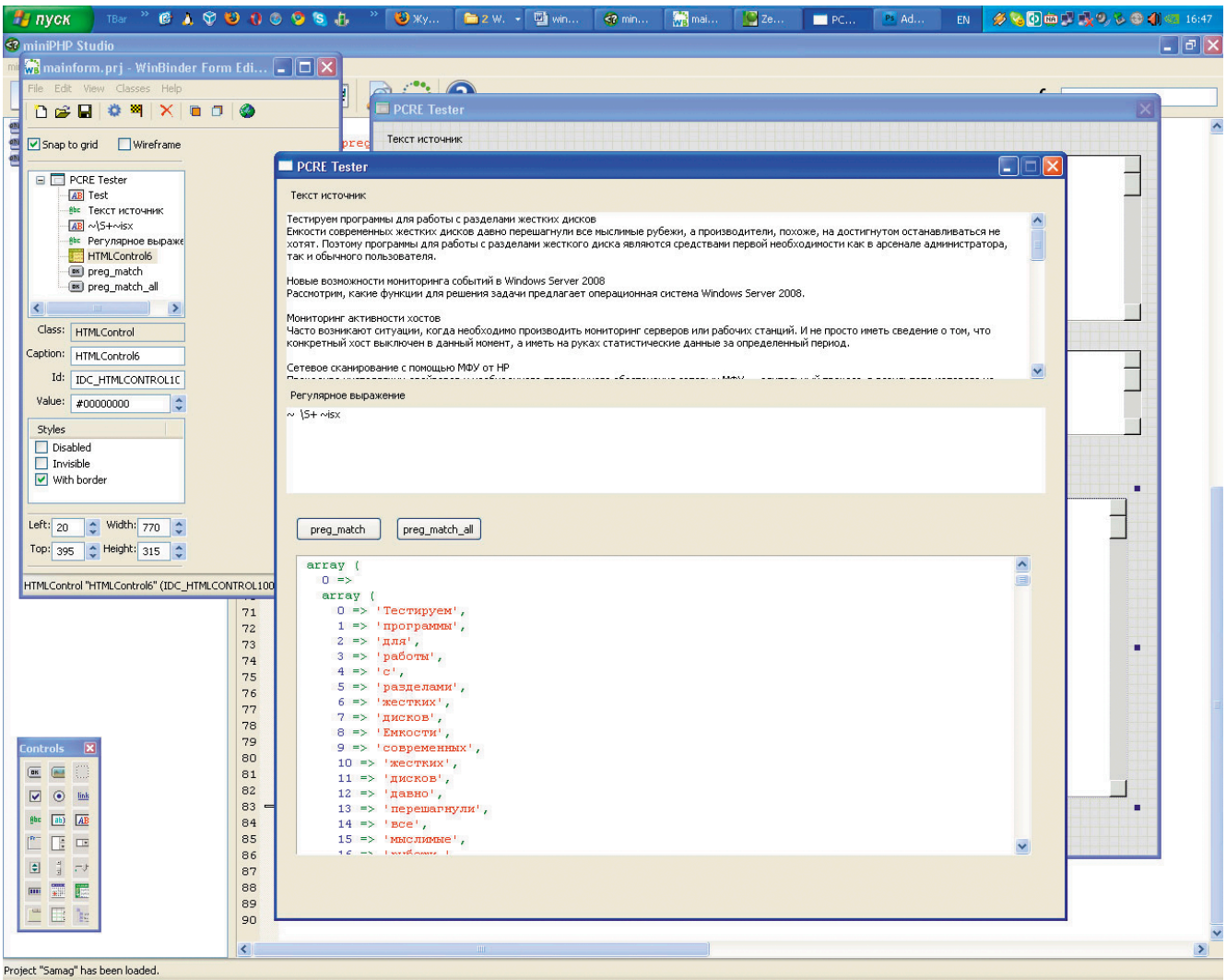


Рисунок 5. Наша программа в действии

учиваться и изучать что-то сложное. WinBinder очень легок в освоении, а на сайте есть очень подробная документация и хорошие примеры. Эта документация встроена и в саму студию, так что нет необходимости ходить на сайт.

Еще пару слов в пользу WinBinder

WinBinder настолько прост, что много о нём рассказывать не вижу смысла. Данной статьи достаточно для того, чтобы сесть и начать писать всякие утилитки для себя уже после тридцати минут знакомства. Можно написать легко и быстро редактор для базы данных SQLIte. Можно написать простой графический редактор, используя GD. К примеру, программу для визуального изменения размера изображений и их брендирования. И даже ICQ-клиент, благо есть библиотека, написанная на PHP, для работы с этим протоколом. Можно написать клиент для работы с почтой. Можно написать FTP-клиент. Да можно много чего еще написать. Была бы фантазия, прямые руки и свободное время, а инструмент у нас уже есть.

Конечно WinBinder не заменит вам C#/C++ или Java, но его возможностей достаточно для создания более-менее сложных приложений. Более того, сообщество программистов постоянно расширяет возможности WinBinder. Чего только стоит поддержка WinAPI, а также возможность чтения/записи памяти по произвольным адресам с помощью функций wb_peek() и wb_poke(). Например, таким образом был найден способ взаимодействия с буфером обмена.

Кстати, вот вам пример работы напрямую с памятью. Например, изменение содержимого строки в памяти:

```
<?php

$string = "Test string";
$addr = wb_get_address($string);
$peek = wb_peek($addr);
Debug::var_dump( $peek );

wb_poke($addr, "Replace");
$peek = wb_peek($addr);
Debug::var_dump($peek, $string);

?>
```

В результате в лог-файл будет записано следующее:

```
string(11) "Test string"
string(11) "Replacering"
string(11) "Replacering"
```

Мы получили адрес строковой переменной с помощью wb_get_adress(), затем получили её содержимое через wb_peek() и изменили, перезаписав начало строки через wb_poke().

Еще один плюс в корзину WinBinder – это то, что он поддерживает ресурсы из WinASM Studio (бесплатная среда разработки программного обеспечения для ОС Windows и DOS, изначально предназначенная для написания программ на языке Ассемблер) (см. **рис. 6**).

WinBinder умеет даже «на лету» работать с файлами ресурсов. К примеру, у вас есть файл с ресурсом окна. Вы можете его подключить прямо в программе, распарсить функцией parse_rc(), которая вернет нативный PHP-код и выполнить его. Пример приведен ниже:

```
<?php

$fp = fopen('myform.rc', 'rb');
$resource = fread($fp, file_size('myform.rc'));
fclose($fp);

$native_php_resource = parse_rc($resource, '$mainwin', ↵
      null, 'PopupWindow');
eval($native_php_resource);

?>
```

На сегодня поддерживаются только ресурсы, созданные WinASM Studio. Подробнее о данной функции вы можете прочесть на этой странице http://winbinder.org/manual/functions/auxiliary/parse_rc.html.

В WinBinder реализованы даже функции для работы с базой данных. Все они начинаются с префикса db_. Подробности их использования можно узнать тут: http://winbinder.org/manual/reference/functions_database.html.

Теперь давайте разберем пример работы с реестром, так как в операционных системах Windows это неотъемлемая часть. А серьезному приложению работа с реестром просто необходима. Например, мы хотим узнать, какие обои установлены в данный момент на рабочем столе:

```
<?php

$wallpaper = wb_get_registry_key('HKCU', ↵
      'Control Panel\\Desktop',  'Wallpaper');

?>
```

Нет ничего проще

В Winbinder встроены функции для проигрывания звуков (wb_play_sound()), для поиска файлов (wb_find_file()). Так же легко можно работать с COM-компонентами Windows, увеличивая функционал своих программ. Например, можно написать свой Skype-клиент, используя SkypeAPI. Достаточно пары строк кода, и у вас уже почти готовое приложение:

```
<?php

$Skype = new COM('SKYPEAPI.Access')
if ( !$Skype )
{
      wb_message_box($Window, "ERROR! Can not create ↵
            SKYPEAPILib.Access object!", "ERROR!");
      exit(1024);
}

$Com->Connect();
$data_array = $Com->GetFriendList();

?>
```

Думаю, на этом можно остановиться. Вы знаете достаточно, чтобы понять, нужен ли вам этот замечательный

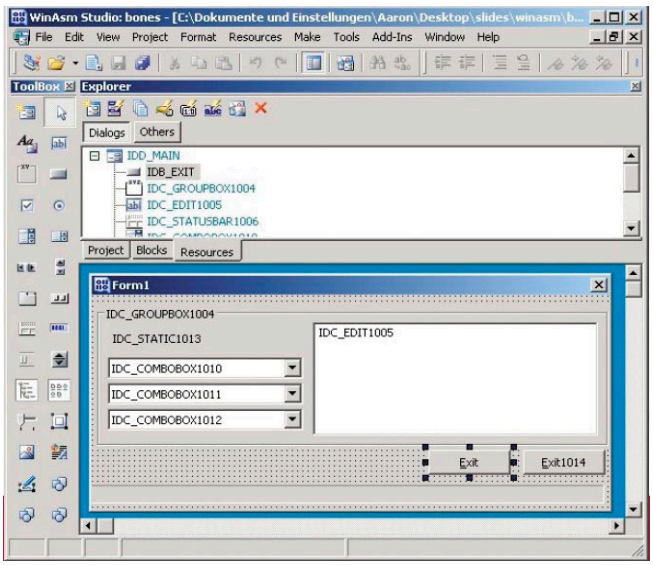


Рисунок 6. Ресурсы, созданные в WinASM Studio, можно подключать к Winbinder

фреймворк и хотите ли вы с ним ознакомиться поближе. Безусловно, он вам может пригодиться, если вы PHP-программист и, возможно, читая эту статью, уже придумали, какую программу, написанную для себя, вы давно хотели переписать с помощью PHP-GTK, но не хватало времени изучить все возможности и особенности. Разработка с применением GTK никогда не славилась легкостью, тут никто спорить не будет. Причем я говорю не только о PHP-GTK. Так почему бы не попробовать новый инструмент? Особенно если у вас стоит задача написать приложение именно под операционную систему Windows.

Итого

Возможности WinBinder достаточно велики. Он умеет работать с реестром Windows. Умеет работать с медиа-ресурсами и проигрывать *.wav-файлы. Достаточно взглянуть в справочную информацию, и вы поймете, что он умеет много чего. Тем не менее его функционал хоть и велик, но очень прост в изучении. Один тот факт, что WinBinder взаимодействует напрямую с Windows API, говорит о том, что он обладает достаточной мощью для разработки приложений под операционную систему Windows. Более того, он очень хорошо документирован (на мой взгляд, лучше, чем PHP-GTK). На официальном сайте вы найдете массу примеров, а также много информации можно почерпнуть с форума сообщества.

Если вы уже знакомы с PHP, то через пару часов вы сможете увидеть свою программу на PHP в виндовом окошке. Освоив документацию WinBinder и получив достаточное количество практики, вы поймете, что еще более простого прикладного программирования под Windows вы не находили. Кстати, WinBinder доступен в PECL-репозитории по адресу http://pecl.php.net/package/WinBinder.

1. Официальный сайт фреймворка WinBinder – http://winbinder.org.
2. Сайт miniPHP Studio – http://exvision.net.
3. WinBinder в репозитории PECL – http://pecl.php.net/package/WinBinder.

Доступ к данным на основе хранимых процедур в веб-приложениях

Большинство приложений вынуждено работать с базами данных, общаясь с СУБД на языке SQL-запросов. Иными словами, одни программы на языках высокого уровня составляют другие программы на SQL. Это выглядит привычным – поэтому кажется логичным и удобным, но так ли это на самом деле?

Рассмотрим два способа взаимодействия приложения и базы данных. Первый и на данный момент более популярный способ – генерация SQL-запроса в теле скрипта (здесь и далее приводятся примеры для PHP5 + MySQL 5 с установленным расширением mysqli):

```
/* Выбрать все города в стране с заданным кодом,
 * динамическая генерация запроса
 */
$countryCode = 'RU';
$result =  mysqli_query ($db, "SELECT Cities.name ↵
      FROM Countries, Cities WHERE Cities.countryId = ↵
      Countries.id AND Countries.code = ↵
      '".mysqli_real_escape_string($db, $countryCode)."'");
```

Второй способ – доступ к данным через хранимые процедуры. Хранимая процедура – объект базы данных, представляющий собой набор скомпилированных SQL-инструкций. Скрипт вызывает процедуру со списком параметров и обрабатывает полученный результат(ы).

Приведенный выше запрос (SELECT Cities.name FROM Countries, Cities WHERE Cities.countryId = Countries.id AND Countries.code = 'RU') можно сохранить в виде процедуры – getCities, с одним входным параметром – код страны (countryCode char(2)).

Приведу пример создания хранимой процедуры:

```
DELIMITER $$
CREATE PROCEDURE `getCities`(countryCode char(2))
    BEGIN
        SELECT Cities.name FROM Countries, Cities ↵
               WHERE Cities.countryId = Countries.id ↵
               AND Countries.code = countryCode;
    END$$
DELIMITER ;
```

В момент вызова хранимой процедуры СУБД подставляет значение параметра в тело запроса и возвращает результат выборки данных.

Для вызова хранимой процедуры 'getCities' на стороне сервера БД необходимо выполнить следующую команду:

```
CALL `getCities`('RU');
```

Вызвать процедуру getCities из PHP-приложения можно следующим образом:

```
/* Выбрать все города в стране с заданным кодом,
 * вызов хранимой процедуры
 */
$countryCode = 'RU';
mysqli_multi_query($db, "CALL getCities ↵
      ('".mysqli_real_escape_string ↵
      ($db, $countryCode)."');");
```

Работа с БД через хранимые процедуры в настоящий момент встречается реже, чем генерация SQL-запроса в теле программы. На мой взгляд, это происходит по следующим причинам:

- наиболее популярная связка для написания веб-приложений – PHP + MySQL, однако только в MySQL 5 стало возможно использовать хранимые процедуры;
- в большинстве пособий по программированию приведены примеры работы с БД, основанные на генерации запроса в теле скрипта, и начинающим программистам сложно отойти от книжных примеров;
- написание приложения с использованием хранимых процедур подразумевает умение программистов работать с хранимыми процедурами или наличие времени для изучения данной технологии (что не всегда допустимо в рамках конкретного проекта).

Преимущества использования хранимых процедур

- **Повышение скорости работы БД.** Процедуры хранятся в скомпилированном виде, а значит, СУБД не тратит время на компиляцию запроса при каждом его исполнении. Приложению не требуется тратить время на генерацию запроса. Команда для вызова хранимой процедуры значительно короче, чем запрос, содержащийся в теле процедуры, поэтому требуется меньше времени и трафика на передачу команд на сервер БД.
- **Большая степень свободы.** Хранимые процедуры поддерживают: входные и выходные параметры, локальные переменные, операторы условного ветвления, циклы, вызовы встроенных команд и других процедур, исполнение DDL-операторов. Во многом хранимые процедуры похожи на процедуры языков программирования высокого уровня.
- **Упрощение кода приложения.** В приложении нет SQL-запросов, а значит, программисту не нужно писать код для их генерации. Для вызова хранимой процедуры необходимо знать только имя и список параметров (аналогично вызову обычных функций/методов в теле приложения). Такой подход сокращает размер кода и улучшает его читабельность, что положительно влияет на качество конечного продукта.
- **Защита приложения от изменений структуры БД.** В процессе развития проекта может возникнуть необходимость в изменении структуры БД, например, добавить/удалить/переименовать таблицу или столбец. Если приложение генерирует SQL-запросы, то необходимо внести изменения во все фрагменты кода, отвечающие за генерацию запросов. Организация доступа через хранимые процедуры не требует внесения изменений в код приложения до тех пор, пока имя хранимой процедуры и список параметров (а также ожидаемый результат) остаются прежними.
- **Снижение количества ошибок и упрощение отладки.** Чаще всего ошибки в работе приложения с БД возникают по следующим причинам:
  - ☑ приложение использует некорректные значения для генерации SQL-запроса;
  - ☑ SQL-выражение некорректно описывает ожидаемый результат (т.е. ошибка в запросе);
  - ☑ фрагмент кода приложения, отвечающий за генерацию SQL-запроса, содержит ошибку и не способен правильно построить нужный запрос.

  Если доступ к БД построен на основе хранимых процедур, то:
  - ☑ легко узнать, какие значения попадают в хранимую процедуру, достаточно распечатать список аргументов в момент вызова хранимой процедуры;
  - ☑ вам не нужно гадать по коду приложения, какой именно запрос должен получиться в том или ином месте программы, достаточно посмотреть на тело хранимой процедуры, что значительно упрощает процесс отладки;
  - ☑ этой ошибки возникнуть не может, так как приложение вообще не генерирует SQL-запросов, все запросы находятся в БД в виде хранимых процедур.
- **Безопасность.** Использование хранимых процедур позволяет значительно снизить угрозу возникновения уязвимости типа SQL-injection. Кроме того, можно устанавливать права доступа к объектам базы данных для каждой хранимой процедуры, что также способствует повышению уровня безопасности приложения.

Трудности работы с хранимыми процедурами

Существует масса преимуществ, говорящих за использование хранимых процедур. Однако не стоит думать, что хранимые процедуры, безусловно, оптимальное решение для любого проекта. Чтобы сделать осмысленный выбор, давайте рассмотрим отрицательные стороны данного метода.

- **Проблема совместимости.** Если необходимо обеспечить легкую переносимость приложения на максимальное количество СУБД, то, вероятно, стоит отдать предпочтение динамической генерации запросов, так как хранимые процедуры поддерживаются не всеми СУБД.
- **Сложность внедрения хранимых процедур в существующий проект.** Внедрение хранимых процедур в приложение, использующее динамическую генерацию запросов, приведет к полной реорганизации кода работы с БД. Необходимость такой реорганизации не всегда просто объяснить заказчику.

- **Передача сложных типов данных.** Иногда в качестве аргумента процедуре требуется передать не просто строку или число, а массив данных (или более сложный объект). В этом случае данные необходимо преобразовать в строку и в таком виде передавать хранимой процедуре, внутри которой происходит обратное преобразование. Построение запроса в теле приложения в этом случае проще.

Особенности работы с хранимыми процедурами

- Хранимые процедуры служат только для доступа к данным (извлечение/обновление/удаление) и ни для чего больше. Использование процедур в иных целях (проверка данных или генерация HTML) является ошибкой.
- Процедура может вернуть более одного результата. В коде вызова хранимой процедуры необходимо делать итерацию по всем возвращаемым результатам и обрабатывать каждый из них в отдельности.
- Достаточно сложно передать в хранимую процедуру массив значений. Наиболее популярным решением является передача массива в хранимую процедуру в виде строки, содержащей элементы массива, разделенные специальным символом (вертикальная черта – «|»), далее параметр анализируется в теле хранимой процедуры.
- Если в теле хранимой процедуры необходимо динамически генерировать SQL-запрос (старайтесь всеми возможными способами избегать написания подобных процедур), не забывайте экранировать кавычки и спецсимволы во всех переданных в процедуру параметрах, участвующих в построении запроса, иначе процедура будет содержать потенциальную уязвимость типа SQL-injection.

Пример класса для работы с БД через хранимые процедуры

Как мы уже заметили, хранимые процедуры очень похожи на функции, наш класс будет реализовывать прозрачную работу с процедурами таким образом, чтобы с точки зрения приложения не было разницы между обычными функциями и хранимыми процедурами.

Чтобы стало понятно, о чем идет речь, начнем с примера:

```
<?php
include 'DBaccess.php';
// Создаем объект доступа к БД
$db = new DBaccess('main_db' , 'localhost', 3306, ↵
      'login', 'password', 'utf8');
// Вызываем хранимую процедуру GetCities и передаем
// в качестве параметра RU
$result = $db->getCities('RU');
// Обрабатываем полученный результат (массив данных)
var_dump($result);
?>
```

В приведенном выше примере для вызова хранимой процедуры getCities с параметром RU (код страны) используется объект класса DBaccess. С точки зрения приложения такой вызов процедуры выглядит как вызов обыкновенного метода, что позволяет отказаться от логики написания программы, которая в свою очередь составляет другую программу на SQL. Приведу далее код класса DBaccess (для работы класса требуется PHP5 с mysqli расширением, MySQL 5):

```
<?php
class DBConnection {
      private $db = null;
      public function __construct($dbName, $host, $port, ↵
            $login, $password, $charset) {
          $this->db = new mysqli($host, $login, ↵
                $password, $dbName, $port);
          $this->db->set_charset($charset);
      }
      public function __call($storeProcedureName, $params) {
          $quotedParams = array();
          foreach($params as $param)        {
                array_push($quotedParams, $param === ↵
                    null ? 'NULL' : '\''.$this->db-> ↵
                    escape_string($param).'\'');
                }
          $sql = 'CALL `'.$storeProcedureName.'` ↵
                ('.implode(',', $quotedParams).');';
          $this->db->multi_query($sql);
          $results = array();
                do {
                if ($result = $this->db->store_result()) {
                    $rows = array();
                    while ($row = $result->fetch_assoc()) {
                          array_push($rows, $row);
                    }
                    $result->close();
                    array_push($results, $rows);
                          }
          } while ($this->db->more_results() && ↵
                $this->db->next_result());
      return($results);
      }
}
?>
```

Внутри класса DBaccess не объявлен метод getCities, однако мы можем вызывать хранимую процедуру как «$db->getCities('RU');».

Это достигается за счет использования магического метода __call() (данная возможность появилась в PHP5), который работает следующим образом: при вызове метода, не объявленного в классе, имя вызываемого метода и список аргументов передается в __call($metodName, $params) для обработки (если метод объявлен).

Таким образом, мы можем вызывать любую хранимую процедуру на сервере, например «$db->loadUser($email, $password);».

В приведенном выше коде класса DBaccess отсутствуют необходимые проверки на ошибки, возможность работы с несколькими БД, проверка стабильности соединения с сервером, автоматическое переподключение и множество других полезных функций. Это сделано намеренно, дабы проиллюстрировать основную идею с использованием минимального количества кода.

Скачать полнофункциональную версию класса для изучения и использования можно здесь: http://www.vipidn.com/dbaccess.zip.

1. Полнофункциональная версия класса «DBaccess» – http://www.vipidn.com/dbaccess.zip.
2. Описание магического метода __call() – http://ru2.php.net/manual/ru/language.oop5.overloading.php.
3. Описание расширения mysqli – http://ru2.php.net/manual/ru/ref.mysqli.php.
4. Информация к размышлению – «Good and Evil in the Garden of Stored Procedures» (Jeremy D. Miller) – http://codebetter.com/blogs/jeremy.miller/archive/2005/07/05/130093.aspx.

Сисадминский Новый год

Лежу я, значит, со своей девушкой на диване дома 31 декабря 2008 года, в последний вечер года, и в самый интересный момент раздается звонок моей мобилы (звонят с работы), поднимаю трубку и слышу: «Приезжай скорей, у нас компьютер не включается, пишет, что, типа, не найден такой-то файл, дальнейшая работа Windows невозможна...»

Обслуживаю сеть круглосуточных супермаркетов. Надо ехать, но время 22:40, меньше чем через полтора часа Новый год! Приехал, спрашиваю: «Что произошло?» Отвечают: «Какое-то сообщение вылезло, ну мы там нажали на OK, комп завис, мы его перезагрузили кнопкой, а он и не загружается, вот мы тебе и позвонили...»

– Что в сообщении-то было написано?

Пожимают плечами.

– ???

– Мы же видели, что ты, типа, нажимаешь на OK, потом перезагружаешь сервак, и все пучком!

В общем, на кассовом сервере жесткий сдох, хорошо хоть BackUpы есть! Не стал с ними церемониться, ввел POS-терминалы в автономный режим, до утра потерпят!

В обед на следующий день (1.01.2009) с бодуна прилетаю в магазин, дабы поднять сервак. Сижу, ковыряюсь, мне звонок на мобилу (генеральная звонит): «Что там произошло?» Объясняю все доходчиво, что, типа, сервер упал – сижу, поднимаю. Она: «Может, прислать кого из грузчиков? Помогут поднять!» Я в шоке: «Зачем грузчиков? Сам справлюсь!» Потом сижу-догоняю: она же не в курсе, что падение сервера не обязательно означает его физическое изменение месторасположения в короткий промежуток времени...

В итоге Новый год встречать приехал без четверти двенадцать, девушка в шоке (она давно мою работу не любит)...

P.S.:

1. Почему серваки падают в такое время, когда ты совсем этого не ждешь, и в самый интересный момент (кстати, кому очень интересно, этот интересный процесс, все же я довел до своего логического конца)?
2. Я просто в шоке от юзверей, которые не читают сообщения...

С Новым годом вас, камрады!

ViRuZzz

Незаменимые у нас есть

В свете кризиса выгнали на 4-дневку за свой счет. И начинаются в пятницу звонки. Как оказалось, все (бухи, кадры, даже электрики) работают, выгнали только «избранных», и админы попали в их число. Разумеется, все были посланы далеко и надолго. Сами выгнали – работайте как хотите. После того как подох свитч в сервачной нам «разрешили» работать по пятницам до 2 часов.

Так, в пятницу, когда я сижу на минимуме поддержки, только критические ситуации, долбанутая кадровичка наметила перестановку и позвонила мне за 20 минут до конца рабочего дня с просьбой подключить компьютеры. О том, что подключать компы надо к розеткам и сети, а также о том, что у них есть провода, они даже не подумали. Также никто даже никто не читал инструкций о том, что к компам прикасаться нельзя и все перестановки делает только админ. Ровно в 14.00 я свалил. И тут же начались звонки начальнице, почему мы уходим точно по графику, а кадровичка сидит до 10 вечера, когда надо. Была послана, но...

Почему админ получает 35к, а кадровичка 150к за то, что сокращает народ? Где-нибудь ценят админов нормально? И как кого коснулся этот кризис?

Дмитрий Иванов

Кризисное

Работал я админом в офисе. Все было хорошо, цивильно – нормальная сеть, построенная по уму, – отдельная серверная, стойки-патчпанели, UPS. Разводка розеток (и сеть, и телефон, и питание) на каждое рабочее место с запасом. Никаких «ужасов» вроде серверов на полу или гирлянд из проводов, свисающих по стенам. Делал ее мой предшественник, за что ему великий почет и уважение. Офис большой, комфортный, в удобном для меня месте. Полгода работал и горя не знал. А потом пришел кризис.

И решили мы переезжать в офис поменьше и подальше, попутно разделяясь на две организации. Отделилось одно из направлений. Правда, от выбора до фактического переезда осталось две недели, но кого это волновало? А меня (админа) припахали заключать договора и запрашивать счета на подвод всего в это помещение. С постоянными отчетами «когда уже». На намек, что раньше надо было суетиться и в средине декабря телефонная компания закупает шампанское на корпоратив, а не тянет телефоны, реакции нет. Притом старый офис остался тоже на мне, да еще с постоянными левыми задачами, вроде «у меня компьютер гудит» или «поищи нам музыку на Новый год, мы не умеем».

В серверной нового офиса отсутствует охлаждение. Как класс. Только свисающая с разобранного фальшпотолка труба, отключенная от вентиляции здания. Из питания – розетки, 3 штуки. На стене. От общей группы. Сети фактически нет. Есть кое-где розетки, половина не рабочая. Но это ладно. Протянем-проложим, поставим-настроим, не впервой. Мягко намекнули, что пахать придется все праздники.

Дальше началось совсем смешно. Питания и розеток на все рабочие места не хватает. На вопрос руководству «???» ответ: «Подводи удлинителями». 19" стойку забрать не дали, отдали отделяющемуся направлению. Стоечный UPS – тоже. На вопрос «когда купим?» ответ: «ну, может быть к марту...» На вопрос «упадет, и сами будете плакать» ответ: «ну, раньше же не падало». Убеждения, что все когда-то бывает в первый раз, не помогли. А ежедневные изнасилования мозга отчетами и планами продолжались.

Апогеем стала новость, что забрать из старого офиса мы сможем только занятые машины. Свободные – нет. И мониторы 19" свободные – тоже нет, сидите на 15". А вообще посмотрим, может, мы вообще тебе с февраля зарплату понизим, ведь людей будет меньше. На вялый намек «основная часть моего времени уходит не на замену мышек, а на работу с сетью и серверами» ответа нет. В итоге я написал заявление ПСЖ. И ушел. И на меня все косились, как «бросил нас в кризисной ситуации».

Коллеги, подскажите – это я такой дурак, что ушел?

MInoy

По материалам сайта «Сисадмин тоже человек» – http://sysadmin.mail.ru

Редакционная подписка
для физических лиц

- Вы можете оформить подписку только на **российский** адрес.
- При заполнении квитанции **обязательно РАЗБОРЧИВО укажите фамилию, имя, отчество полностью, почтовый индекс и адрес получателя (область, город, улица, номер дома, номер квартиры), контактный телефон.**
- Журнал высылается почтой заказной бандеролью только после поступления денег на расчетный счет и **копии заполненного и оплаченного бланка, отправленной в редакцию по факсу: (495) 628-82-53 (доб. 120) или на электронный адрес: subscribe@samag.ru**.

ИЗВЕЩЕНИЕ

ООО "С 13" Форма № ПД-4
ИНН 7708654814 / КПП 770801001
Р. сч. 40702810300080001868 К. сч. 30101810100000000787
ОАО «УРАЛСИБ» г. Москва БИК 044525787
Коды: по ОКПО 84027582, по ОКОПФ 65

Вид платежа: Редакционная подписка на журнал "Системный администратор" за 2009 г.

01	02	03	04	05	06	07	08	09	10	11	12
X	X	X	X	X	X	X	X	X	X	X	X

Дата _____ Сумма платежа: 2400 руб. 00 коп.

Информация о плательщике:

_____
(Ф. И. О. почтовый индекс, адрес и телефон)

_____

_____

Подпись _____

Кассир

КВИТАНЦИЯ

ООО "С 13" Форма № ПД-4
ИНН 7708654814 / КПП 770801001
Р. сч. 40702810300080001868 К. сч. 30101810100000000787
ОАО «УРАЛСИБ» г. Москва БИК 044525787
Коды: по ОКПО 84027582, по ОКОПФ 65

Вид платежа: Редакционная подписка на журнал "Системный администратор" за 2009 г.

01	02	03	04	05	06	07	08	09	10	11	12
X	X	X	X	X	X	X	X	X	X	X	X

Дата _____ Сумма платежа: 2400 руб. 00 коп.

Информация о плательщике:

_____
(Ф. И. О. почтовый индекс, адрес и телефон)

_____

_____

Подпись _____

Кассир

Российская Федерация

- Подписной индекс: годовой – **20780**, полугодовой – **81655**
  Каталог агентства «**Роспечать**»
- Подписной индекс: годовой – **88099**, полугодовой – **87836**
  Объединенный каталог «**Пресса России**»
  Адресный каталог «**Подписка за рабочим столом**»
  Адресный каталог «**Библиотечный каталог**»
- Альтернативные подписные агентства:
  Агентство «**Интер-Почта**» (495) 500-00-60, курьерская доставка по Москве
  Агентство «**Вся Пресса**» (495) 787-34-47
  Агентство «**Курьер-Прессервис**»
  Агентство «**ООО Урал-Пресс**» (343) 375-62-74
  ЛинуксЦентр www.linuxcenter.ru
- Подписка On-line
  http://www.arzi.ru
  http://www.gazety.ru
  http://www.presscafe.ru

СНГ

В странах СНГ подписка принимается в почтовых отделениях по национальным каталогам или по списку номенклатуры «**АРЗИ**»:

- **Азербайджан** – по объединенному каталогу российских изданий через предприятие по распространению печати «**Гасид**» (370102, г. Баку, ул. Джавадхана, 21)
- **Казахстан** – по каталогу «**Российская Пресса**» через ОАО «**Казпочта**» и ЗАО «**Евразия пресс**»
- **Беларусь** – по каталогу изданий стран СНГ через РГО «**Белпочта**» (220050, г. Минск, пр-т Ф. Скорины, 10)
- **Узбекистан** – по каталогу «**Davriy nashrlar**» российские издания через агентство по распространению печати «**Davriy nashrlar**» (7000029, г. Ташкент, пл. Мустакиллик, 5/3, офис 33)
- **Армения** – по списку номенклатуры «**АРЗИ**» через ГЗАО «**Армпечать**» (375005, г. Ереван, пл. Сасунци Давида, д. 2) и ЗАО «**Контакт-Мамул**» (375002, г. Ереван, ул. Сарьяна, 22)
- **Грузия** – по списку номенклатуры «**АРЗИ**» через АО «**Сакпресса**» (380019, г. Тбилиси, ул. Хошараульская, 29) и АО «**Мацне**» (380060, г. Тбилиси, пр-т Гамсахурдия, 42)
- **Молдавия** – по каталогу через ГП «**Пошта Молдовей**» (МД-2012, г. Кишинев, бул. Штефан чел Маре, 134)
  по списку через ГУП «**Почта Приднестровья**» (MD-3300, г. Тирасполь, ул. Ленина, 17)
  по прайс-листу через ООО Агентство «**Editil Periodice**» (МД-2012, г. Кишинев, бул. Штефан чел Маре, 134)
- Подписка для **Украины**:
  Киевский главпочтамт
  Подписное агентство «**KSS**», тел./факс (044)464-0220

Ф.СП-1

Министерство связи РФ

АБОНЕМЕНТ на журнал _____ (индекс издания)

Системный администратор

Количество комплектов: _____

на 200 год по месяцам

1	2	3	4	5	6	7	8	9	10	11	12

Куда _____ (почтовый индекс) _____ (адрес)

Кому _____

(фамилия, инициалы)

ДОСТАВОЧНАЯ КАРТОЧКА

ПВ | место | литер

на журнал _____ (индекс издания)

Системный администратор

Стоимость: по каталогу _____ руб. _____ коп.; за доставку _____ руб. _____ коп.

Количество комплектов: _____

на 200 год по месяцам

1	2	3	4	5	6	7	8	9	10	11	12

Куда _____ (почтовый индекс) _____ (адрес)

Кому _____

(фамилия, инициалы)

Подписные индексы:

20780*
+ диск с архивом статей 2008 года

81655**
без диска

по каталогу агентства «Роспечать»

88099*
+ диск с архивом статей 2008 года

87836**
без диска

по каталогу агентства «Пресса России»

* Годовой
** Полугодовой
*** Диск вкладывается в февральский номер журнала, распространяется только на территории России

СИСТЕМНЫЙ АДМИНИСТРАТОР
№1(74), Январь, 2009 год

УЧРЕДИТЕЛИ
Частные лица

РЕДАКЦИЯ
Генеральный директор
Владимир Положевец
Главный редактор
Алексей Коршунов
chief@samag.ru
Ответственный секретарь
Наталья Хвостова
sekretar@samag.ru
Технический редактор
Владимир Лукин

Главный редактор электронного приложения «Open Source»
Дмитрий Шурупов

Внештатные редакторы
Алексей Барабанов
Кирилл Сухов
Александр Емельянов
Андрей Луконькин

РЕКЛАМНАЯ СЛУЖБА
тел./факс: (495) 628-8253
Евгения Тарабрина (доб. 120)
reclama@samag.ru

Верстка и оформление
maker@samag.ru

Дизайн обложки
Дмитрий Репин

По вопросам распространения обращайтесь по телефону:
Светлана Зобова
(495) 628-8253 (доб. 120)

107045, г. Москва,
Ананьевский переулок, дом 4/2, стр. 1
тел./факс: (495) 628-8253

Сайт журнала: www.samag.ru

ИЗДАТЕЛЬ
ООО «С 13»

Отпечатано типографией
ООО «Периодика»
Тираж 17000 экз.

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций (свидетельство ПИ № 77-12542 от 24 апреля 2002 г.).

Вы знаете, как бороться с «Просачивающейся Адварью»? Применяете «Чарующий скрипт»?

Редакция журнала «Системный администратор» представляет вам новый админский сувенир для истинных знатоков своего дела – карточную игру «АУТСОРСЕР».

В ходе игры участники тянут из колоды карты «Проблем», с которым им предстоит бороться один на один или с помощниками, используя подручные средства. Успешное решение «Проблемы» добавляет игроку уровни. Если вы не считаете себя добрым и милым, то для вас в игре предусмотрена специальная возможность – сделать гадость другому участнику и обойти его в погоне за уровнями.

Победителем становится тот, кто быстрее всех доберется до 10 уровня. Остальные подробности об игре, «Чарующем скрипте», «МегаУтилите» и «Клановом коктейле» вы сможете узнать из правил игры.

«АУТСОРСЕР» – это пародия на жизнь, которая позволит вам ощутить всю прелесть аутсорсинга... но без всей словесной мишуры, типа, «утром стулья, вечером деньги...»!

Приобретайте игру «АУТСОРСЕР» в редакции.