Системный администратор

ежемесячный журнал www.samag.ru

№11(84) ноябрь 2009

MyZCI – автоматическая инвентаризация

Виртуализируем предприятие

Черный экран тишины

Applocker: укрепляем безопасность сети

Решаем проблему внезапной блокировки учетной записи

А нужен ли банкам Linux?

Аутсорсинг: кто против?

Персональное дело IBM

ISSN 1813-5579

09011

9 771813 557005

Калиф на час или навсегда?

Когда мы опубликовали статью «Ищем сотру;:-/-:E или партнеров?» о плюсах и минусах аутсорсин-а (№9,2009), то невольно наступили на больную мозоль многих наших читателей - системных администраторов. Это на их место зачастую зовут айтишников со стороны, потому что так выходит дешевле для компании, особенно в кризис. А если админ сохраняет свою работу, то ему приходится непосредственно общаться с представителями аутсорсера, эмпирическим путем постигая все преимущества и недостатки этой услуги, которая набирает популярность.

Наверное, каждый системный администратор может рассказать хотя бы одну «страшную историю» о нечистоплотном аутсорсере, укравшем конфиденциальную информацию или халтурно исполнившем заказ. Обидно бывает вдвойне, когда приходит такой же, как ты, админ - представитель аутсорсера, отнюдь не суперпрофессионал, однако руководство почему-то верит, что именно он и наладит наконец работу, как надо. А когда иллюзии развеиваются, остается только грустно разводить руками - мол, я же предупреждал.

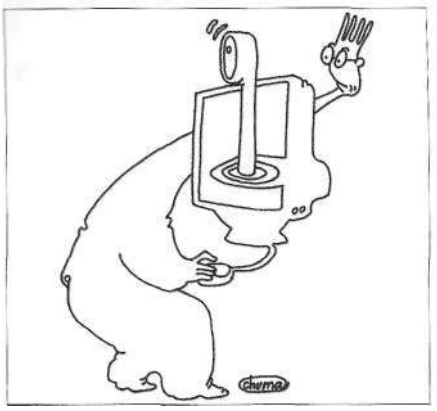
Так кто же аутсорсеры: партнеры или калифы на час? Этому посвящена наша главная дискуссия номера. В ней выступают на этот раз и топ-менеджеры аутсорсинговых компаний, и заказчики, и эксперты по информационной безопасности, и системные администраторы. У всех свои резоны, но в сущности участники обсуждения приходят к мнению, что аутсорсинг нужен, «просто он подходит не каждому», как написал один из наших читателей.

В России пока рынок аутсорсинга не слишком развит. Ясно, что так будет не всегда. К аутсорсингу прибегают все чаще, мир оценил эффективность разделения труда. Новые потребности растущих компаний заставляют их обращаться к аутсорсерам.

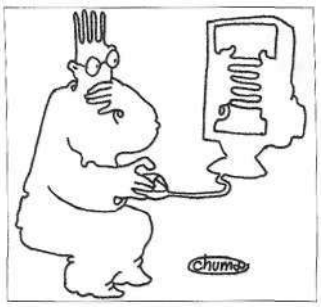
В конце концов, естественный отбор уберет с рынка тех, кто плохо зарекомендовал себя. А нормальные аутсорсинговые компании будут развиваться. Как сказал представитель одой из них, аутсорсинг - это процесс, он бесконечен. Поэтому, обращаясь за помощью к аутсорсерам, лучше сразу строить отношения с ними так, чтобы становиться партнерами надолго.

Галина Положевец.
главный редактор

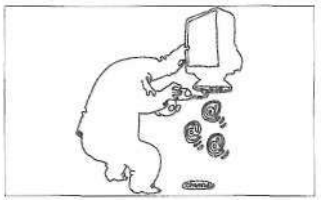
В номере



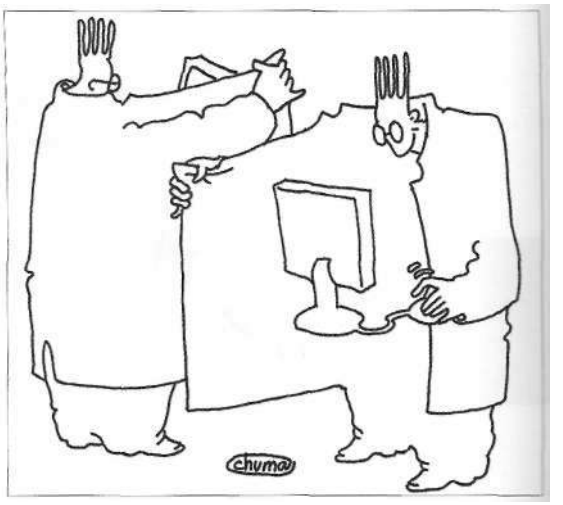
20



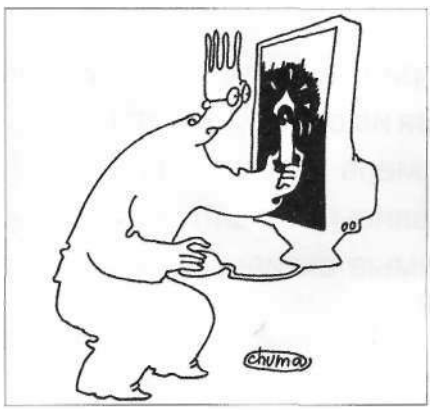
48

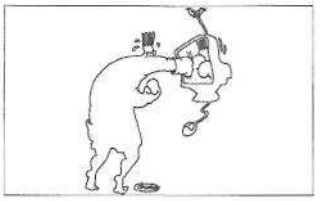


52



56





Волна недовольства среди энтузиастов и независимых разработчиков **вылилась в формирование нового альянса Open Android Alliance**

Визитка

ДМИТРИЙ ШУРУПОВ.

Лондонская фондовая биржа переходит с .NET на Linux/Solaris

Представители Лондонской фондовой биржи подтвердили информацию о том, что собираются сменить платформу TradElect, основанную на .NET, на разработку от MillenniumIT на базе Linux и Solaris. Стоимость использовавшейся до сих пор TradElect составляет 65 миллионов USD, а решения от компании MillenniumIT из Шри-Ланки - 30 миллионов USD. Ожидается, что с новой платформой LSE будет ежегодно экономить около 15 миллионов USD, начиная с 2011/2012 годов. На интеграцию разработки MillenniumIT, базирующейся на Linux и Solaris, потребуется около 1,5 лет. По словам Дэвида Лестера (David Lester), директора по информационным технологиям в LSE, переход на новую платформу поможет добиться «лучшего контролирования, меньших затрат и возможностей создавать и привносить инновации». При выборе новой платформы для LSE рассматривались 20 решений. Список четырех лучших (по мнению специалистов Лондонской фондовой биржи) был опубликован в августе. EOF

Появился альтернативный альянс разработчиков Android

Open Source-энтузиасты создали новый альянс Open Android Alliance, который задался целью создать полностью открытую версию мобильной Linux/Java-платформы Android. Как многие знают, компанию Google с самого появления Android обвиняли в том, что эта платформа недостаточно открыта. Ситуация усугубилась недавними событиями, связанными с альтернативной Android-прошивкой проекта CyanogenMod. Авторы CyanogenMod создавали прошивки на базе Android, куда включали новые возможности. При этом в них оставались закрытые компоненты Android - такие разработки Google, как приложения Android Market и Gmail, - распространение которых без согласия Google запрещено. Поэтому Google потребовала приостановить разработку и распространение прошивок с Android от CyanogenMod, в которых, по словам юристов компании, нарушаются права на ее собственность.

Реакция Open Source-сообщества на подобные действия интернет-гиганта не заставила себя ждать. Волна недовольства энтузиастов и независимых разработчиков вылилась з формирование нового альянса, который объединил желающих развивать альтернативную полнофункциональную версию Android. Ее код будет полностью открыт. Альянс получил название Open Android Alliance (OAA) и уже запустил официальный сайт - openandroidalliance.com. На нем расположился блог с новостями альянса, доступна общая /нформация о проекте и форумы для обсуждений. EOF

В Москве прошла конференция Highload++

12 и 13 октября в Москве прошла конференция разработчиков высоконагруженных систем Highload++ (www.highload.ru). Кроме докладов, были проведены мастер-классы. Благодаря этому каждый участник мог без труда выбрать **интересные** для себя темы. Помимо русскоязычных докладчиков выступали и зарубежные гости. Так, например, Морган Токер из Регсопа рассказал об основах оптимизации СУБД MySQL, проанализировав и сравнив три основных пути: наращивание мощи аппаратного обеспечения, правильная конфигурация сервера MySQL, оптимизация запросов. Магнус Хагандер из PostgreSQL Europe осветил улучшения производительности в другой популярной СУБД с открытым кодом - PostgreSQL версии 8.4. Известный Perl-гуру Тим Бане выступил с докладами об оптимизации Perl-приложений и модулях для их профилирования. Среди наших соотечественников, присутствовавших на Highload++, можно по праву выделить Дмитрия Завалишина, который на сей раз не только рассказал о разрабатываемой ОС Phantom OS, основанной на весьма интересных концепциях, но и продемонстрировал ее в действии. Правда, в показываемой сборке система еще была неспособна работать даже минуту, но, по словам автора, уже готова и более «зрелая» версия, где этот недостаток устранен. В очередной раз не дала скучать публике часовая серия пятиминутных блиц-докладов, которые стали хорошим дополнением к традиционным выступлениям. EOF

Визитка

*ЕВГЕНИЙ **ЩЕПИЛОВ**, директор Сервисного центра компании «Ай~Теко»*

Пять аргументов «за»

Антикризисные задачи ИТ-аутсорсинга

Аутсорсинг не только оптимизирует затраты на ИТ. Он позволяет использовать сегодняшние инвестиции для восстановления компании после кризиса

В непростой экономической ситуации перед российским бизнесом стоит не только задача выжить, но и много других, достаточно тесно с ней связанных. Каким же образом ИТ-аутсорсинг может способствовать решению актуальных задач?

Задача: оптимизировать расходы

Именно стремление заказчиков к сокращению затрат на информационные технологии определило ситуацию на ИТ-рынке в кризисный период. Заказчики были вынуждены пересмотреть свои ИТ-стратегии, перераспределить бюджеты, ранее выделенные на крупные проекты, уменьшить объемы внедрения новых технологий или вовсе отложить запланированные работы на неопределенный срок. Но одним махом отказаться от поддержки и развития корпоративных ИТ невозможно, поскольку такие действия нанесли бы бизнесу не меньший урон, чем собственно кризис. Понимая это, и ИТ-компании, и заказчики стали искать компромиссные пути и новые схемы взаимодействия. Так, в сфере ИТ-аутсорсинга наиболее актуальными и перспективными услугами стали предоставление инфраструктуры как сервиса (Infrastructure as a Service), программного обеспечения как сервиса (Software as a Service), аренда вычислительных мощностей или оборудования с определенным уровнем сервиса. Все они позволяют отказаться от единовременных капитальных затрат (на закупку оборудования, например) и воспользоваться необходимыми ИТ-ресурсами за фиксированную абонентскую плату.

По-прежнему актуальны и востребованы «классические» варианты ИТ-аутсорсинга, например поддержка и администрирование ИТ-ресурсов заказчика, также позволяющие снизить совокупные расходы на ИТ, в первую очередь за счет сокращения затрат на персонал. Многие компании, располагающие сложным специализированным оборудованием или комплексными ИТ-системами, считают рациональным не привлечение в штат дорогостоящего ИТ-персонала, а передачу обслуживания и поддержки вычислительных ресурсов на аутсорсинг.

Задача: повысить качество ИТ-сервисов

Кризис настойчиво диктует бизнесу необходимость сокращения расходов, но в то же время требует бороться за клиента, что неосуществимо без повышения эффективности работы. Актуальность ИТ-аутсорсинга объясняется тем, что он позволяет решить обе задачи одновременно: и сократить расходы на ИТ, и обеспечить необходимое качество ИТ-сервисов для бизнеса. Квалификация аутсорсера, его опыт и ресурсы гарантируют заказчику требуемый уровень качества сервисов и соответственно максимальную отдачу от инвестиций в ИТ. При этом качество аутсорсинговых услуг строго регламентировано соглашением об уровне сервиса (SLA).

Задача: обеспечить непрерывность бизнеса

Согласитесь, модернизация корпоративного ЦОД с целью повышения надежности существующих инженерных систем - дело весьма затратное. Поэтому помимо экономических выгод и повышения качества ИТ-сервисов заказчики ожидают от ИТ-аутсорсинга минимизации незапланированных простоев и операционных рисков. Оптимальным вариантом обеспечения необходимого уровня надежности и безопасности ИТ-ресурсов можно считать сотрудничество с коммерческими центрами обработки данных.

Сегодня на рынке достаточно много предложений по аутсорсингу ЦОД, различающихся уровнем и качеством услуг и, как следствие, их стоимостью. Но заказчику, планирующему разместить в коммерческом ЦОД критичные для бизнеса приложения, целесообразно сузить круг предложений к рассмотрению, ограничив его дата-центрами с уровнем доступности не ниже Tier 3. Напомню, что согласно классификации по стандарту Uptime Institute категория Tier 3 предполагает не более 1,5 часов простоя в год, при этом регламентные

Квалификация аутеорсера» его опыт и ресурсы гарантируют заказчику **требуемое качество сервиса**

работы проводятся без остановки работы инженерных систем дата-центра. В дата-центрах, соответствующих категории Tier 3 (и выше), действует служба эксплуатации, которая в круглосуточном режиме контролирует работу оборудования и устраняет сбои. Все это способствует обеспечению непрерывности бизнеса заказчиков.

Повысить надежность и получить дополнительную гарантию бесперебойной работы бизнес-приложений можно и за счет кастомизации клиентского ЦОД на базе коммерческого. Правда, пока такую услугу предлагает только дата-центр «Траст-Инфо» (ГК «Ай-Теко»). Он готов изменить параметры инженерной инфраструктуры серверного зала в соответствии с нуждами заказчика, то есть адаптировать площадку для размещения оборудования с учетом специфичных требований к кондиционированию, СКС и проч. Фактически заказчик получает собственный корпоративный ЦОД на основе инженерной инфраструктуры коммерческого дата-центра. При этом не нужно капитальных затрат и сохраняются все преимущества, предоставляемые поставщиком услуг согласно SLA.

Необходимый уровень безопасности в коммерческих ЦОД обеспечивается при наличии многоуровневой системы контроля доступа, нескольких контуров охраны, видеонаблюдения и проч. Если согласно корпоративным требованиям по информационной безопасности оборудование заказчика должно быть размещено в отдельном помещении, это не повод отказываться от сотрудничества с коммерческим дата-центром, но повод найти такой ЦОД, который готов предоставить возможности размещения оборудования клиентов в выделенных зонах, изолированных от общего машинного зала.

Задача: обеспечить гибкость сервисов

В сегодняшних условиях бизнесу важно оперативно реагировать на запросы рынка. Соответственно ИТ-среда должна быть гибкой, что не всегда достижимо: для разворачивания новых ИТ-сервисов зачастую требуются новые компетенции, новые ресурсы и время. С учетом этого вполне логично обратиться к услугам ИТ-аутсорсинга, традиционно обеспечивающим быстрый запуск ИТ-сервисов. Кроме того, аутсорсинг позволяет заказчикам четко планировать операционные расходы на поддержку информационной инфраструктуры, а значит, более эффективно расходовать ИТ-бюджеты при разворачивании новых сервисов.

Задача: построить базу для дальнейшего развития

ИТ-аутсорсинг не только способствует оптимизации затрат на ИТ и решению других актуальных задач в краткосрочной перспективе, но и позволит использовать сегодняшние инвестиции для восстановления компании после кризиса. В рамках аутсорсинговых проектов оптимизируются профильные бизнес-процессы, создаются возможности для планомерного масштабирования ИТ-ресурсов, и, таким образом, обеспечивается база для развития корпоративной ИТ-инфраструктуры.

Важно учесть, что сотрудничество с аутсорсером, как и любые договорные отношения, может быть прекращено по каким-либо причинам, и в этом случае заказчику потребуется либо принять проект на себя, либо передать его другому исполнителю, чтобы не потерять наработанную ИТ-базу. А это возможно только при условии документирования работ по проекту. Риски и последствия прекращения сотрудничества с аутсорсером лучше оценить еще на этапе выбора партнера. Крупные ИТ-компании заинтересованы в том, чтобы обеспечить беспроблемную передачу сервиса другой компании, поскольку некорректные действия в этом плане могут испортить их деловую репутацию.

ИТ-аутсорсинг уже доказал свою «боеспособность» в борьбе с кризисом. Но чтобы достичь необходимого уровня эффективности, надежности и безопасности своих ИТ-ресурсов, компаниям следует очень внимательно отнестись к выбору партнера-аутсорсера. Если проект не оправдал ожиданий, не стоит искать изъяны в самой схеме ИТ-аутсорсинга. Причины неудачи проектов в большинстве случаев кроются в действиях исполнителя, ведь от его компетенций и опыта напрямую зависит непрерывность бизнеса клиентов. EOF

Аутсорсинг в вашей компании

Это хорошо или плохо?

На вопрос «СА» отвечают ИТ-специалисты

«Аутсорсер - это сисадмин, выдавивший из себя лакея!»

Из народного творчества

Читатели «Системного администратора» отнеслись со всей серьезностью к предложению редакции рассказать о своем видении работы аутсорсеров. Они живо обсуждали эту тему на форуме сайта «СА». Делились обидами на «варягов», давали советы, как нужно вести дела с внешней ИТ-командой, чтобы был толк от совместной работы, а не сплошной убыток для родной компании. Прикидывали все плюсы и минусы решения переложить на кого-то другого свою головную боль. А в результате получился прелюбопытный коллективный взгляд изнутри на проблемы аутсорсинга.

Мы публикуем в этом номере выдержки из наиболее интересных высказываний наших читателей, включая и тех, кто из скромности не назвал себя.

Мнение пессимиста

Аутсорсинг хорош только для мелких

...Почему так мало людей пользуются аутсорсингом в ИТ-индустрии? Потому что если время на исправление/дополнение отчета для сотрудника->ограммиста варьируется от пяти **минут** до трех дней, то для аутсорсера - только от трех дней и начинается. Потому что задание программисту или руководителю отдела ИТ можно дать по внутреннему телефону, а с аутсорсером надо подписать техническое задание, предварительно его согласовав. И самое главное - перед этим надо согласовать расходы со службой финансов, получить от неё добро, убедить финанасового директора, что эти изменения необходимы.

ИТ-аутсорсинг применим для компаний с количеством сотрудников до 15 человек, где 8-10 компьютеров и один принтер. Все остальные компании, в силу того что они развиваются, требуют изменений в инфраструктуре, и соответственно им нужен специалист, который будет заниматься технической поддержкой бизнес-процессов, а не только администрированием. Элементарно - настроить телефон руководителю через wi-fi, проектор, поменять внутренние номера сотрудников в АТС, подготовить компьютер для нового сотрудника, отремонтировать сломавшийся, помочь с офисными приложениями и т.д. Причем для мелких компаний подойдут именно студенты, и чем крупнее компания, тем дороже специалист...

Мнения оппонентов

Для кого тогда работают крупные?

...Крупные аутсорсеры выигрывают тендеры не по качеству, а по портфолио, такие аутсорсеры допускают текучесть своих кадров, они без сожаления могут позволить расстаться и с капризным клиентом. Маленькие компании таким аутсорсерам неинтересны, да и эти компании не могут позволить себе работу с аутсорсерами, работающими как на конвейере...

Кстати

Элемент недоверия, безусловно, должен присутствовать. Так как аутсорсер - не сторона производственных отношений, а субъект отношений рыночных!

В маленькой компании не разовьешься

...Предположим, действительно можно зарабатывать на клиентах до 15 человек, где 10 ПК и один принтер. Только

«Это выгодна, если правильно договориться»

- Я придерживаюсь точки зрения, что использование данного сервиса выгодно компании. Правда, при соблюдении небольшого набора требований. Со стороны получателя - услуги: стандартизация, стабильность инфраструктуры, прозрачность, бюджетирование. Со стороны аутсорсера - квалифицированная команда и четко спланированный план работ. Выполнение перечисленных условий практически гарантирует получение положительного результата, экономию средств компании или успешное окончание проекта в установленные сроки».

Владислав Котусов, **директор по информационным технологиям компании Softline**

в этом случае возникнут резонные вопросы:

- Будет ли такой админ развиваться как специалист? Разве что в области тонкого тюнинга операционных систем и автоматизации рутинных задач своими силами, без привлечения поставщиков решений enterprise класса. Это несомненный плюс. Но юзеры могут иметь свойство съедать мозг на мелких проблемах, не оставляя времени на самосовершенствование, если дать сесть на шею.
- Если будет расти - долго ли он выдержит со столь скудной инфраструктурой? Даже если будет экспертом в операционных системах, он не сможет полностью реализовать их возможности.
- Какая текучесть таких специалистов?
- Можно ли такой вид работы называть полноценным ИТ-аутсорсингом, если он не подразумевает разграничения по компаниям-клиентам в соответствии с уровнем специалиста?..

Мнение реалиста

Занимаясь аутсорсингом, не забывай свою работу

...Аутсорсеров в чистом виде не бывает. Хотя бы потому, что в этом деле главное не как выполнить работу, а как верно построить отношения с заказчиком. И здесь правило - не терять клиентов. Первое, о чем должен позаботиться аутсорсер, - не бросать свою основную работу!..

Мнение мечтателя

А почему бы и не стать аутсорсером?

...С аутсорсерами важен совсем иной подход к управлению: вы не управляете ими как сотрудниками, а вы управляете результатом. Четко ставите задачи, четко добиваетесь их выполнения. Тогда всё хорошо, все работают, все довольны...

Все именно так. Аутсорсер не сотрудник - принеси, подай. Аутсорсер - это сисадмин, выдавивший из себя лакея! А начинается все с малого и простого. Задайте себе вопрос: «Как часто вы отзываетесь на нештатные просьбы коллег и руководства, как часто вы настраиваете им компьютеры и телефоны, устанавливаете им игрушки, собираете заказные системники?»...

Мнение бывалого

Локальный админ не прыгнет выше собственной сети

...Нужно учитывать, что компаний у аутсорсера много и они все разные. Например, у меня несколько компаний имеют своих локальных админов. Просто потому что там работы много. У всех разные технологические особенности, и только я один могу их сравнить и сделать выводы. Кроме того, у меня периодически возникают странного рода заказчики из совсем неожиданных отраслей. Когда я рассказываю одним, как сделано у других, это всегда воспринимается с интересом. Потому что никакой локальный админ не сможет прыгнуть выше уровня собственной сети. Даже публикация в журнале - это УЖЕ АУТСОРСИНГ!

Вот потому-то лучший способ упереться и загнить мозгом - это оставаться всю жизнь на фултайме. Вот потому-то эти админы не находят иного способа

Аутсорсинг — это как **ремонт** в квартире. Покрасишь-поклеишь, но кафель положить, сантехнику установить приглашаешь специалиста. **А потом убеждаешься: хочешь сделать хорошо — делай сам.**

«Негативное отношение - следствие грустного опыта»

- Первоначально ИТ-аутсорсинг появился в России в крупном бизнесе. Во-первых, крупный бизнес всегда проявлял большой интерес к ИТ-новинкам. Во-вторых, суммы, которые в нем задействованы, гораздо интереснее и привлекательнее для ИТ-компаний.

А сегодня ИТ-аутсорсинг гораздо интереснее малому бизнесу, чем большому. Небольшие компании привыкли считать деньги, в то же время они зачастую активно используют компьютерную технику и нуждаются в консультации и ее обслуживании.-Им невыгодно держать штат, а иногда даже одного системного администратора.

Правильный ИТ-аутсорсинг позволяет повысить одновременно качество обслуживания и снизить расходы, поэтому относиться негативно к аутсорсингу можно только в том случае, если он категорически не нужен компании или опыт общения с аутсорсерами **был** грустным... Аутсорсинг в крупных **и малых компаний** значительно отличается. **Для крупных характерны** масштабные уникальные **проекты с** дорогостоящим оборудованием **и программным** обеспечением, что в свою очередь предполагает труд дорогостоящих и **узконаправленных** ИТ-специалистов. Основная цель здесь, как правило, не экономия средств, **а** качественная реализация проекта, столь необходимого компании.

В последние годы **на** многих крупнейших предприятиях и в ряде ведомств стартовали мегапроекты, в которых сочетаются внедрение систем управления (ERP, документооборот, аналитика, хранилища данных) и активное развитие корпоративной инфраструктуры (ЦОД, почтовые сервисы, системы коллективной работы). Такие проекты требуют принципиально другого уровня управления, высокой квалификации внедряющего и сопровождающего персонала. Поэтому **для их реализации** привлекаются внешние сервисные компании, способные предоставить заказчику экспертизу в сложных технологических дисциплинах и располагающие большим числом консультантов для внедрения и тиражирования информационных систем. Все это приводит к ускоренному по сравнению с другими сегментами ИТ-рынка развитию сектора ИТ-услуг.

Что касается рисков при применении аутсорсинга, то, например, наша компания старается максимально обговорить все пункты в договоре с клиентом. Риск обращения к аутсорсингу, с точки зрения клиента, заключается в том, что он боится получить некачественные услуги. Кроме того, он хочет знать наверняка, что будут покрыты его насущные потребности в ИТ.

Константин Кузилин, руководитель отдела информационно-технической поддержки компании MASTERTELr

«Разделение труда - всегда плюс»

- Аутсорсинг в ИТ, на мой взгляд, очередная ступень эволюции в этой сфере. Давно уже замечено, что разделение труда несёт только положительный эффект. Важно, что это помогает прийти к лучшей стандартизации и шаблонности, что в свою очередь влияет на качество и скорость работы. Конечно, это справедливо только для хорошо организованного аутсорсинга - а его в нашей стране пока нет. Аутсорсер - это такой же ИТ-специалист, как и штатный, и причин его уважать или не уважать быть не может- в конце концов, какая разница, где работать, а точнее, где быть оформленным.

Владислав Листровой, начальник ИТ-отдела компании KLG Holding

развития, кроме кадрового - просто уходят в начальники. А куда им еще?..

Мнение практика

Главное - контроль и кураторы

1. Аутсорсинг всей инфраструктуры на своем оборудовании. Оборудование закупается на средства заказчика, устанавливается в помещении заказчика, технические работы по развитию и эксплуатации проводят специалисты сторонней компании, за что получают дополнительные деньги. Возможно использование в случае отсутствия ИТ-специалистов в компании.

Плюсы:

> Нет необходимости в наборе, содержании, развитии и обучении своего штата специалистов.

> В некоторых случаях может оказаться дешевле нанять стороннюю организацию, чем создавать свой ИТ-отдел/департамент/дирекцию.

> При юридическом закреплении соответствующих пунктов в договоре возможно взыскание с партнера, когда происходит сбой в работе ИТ-инфраструктуры, а также при действиях или бездействии аутсорсера, из-за чего и произошел простой.

Минусы:

> Аутсорсер получает доступ к конфиденциальной информации компании. Необходимы контроль, доверие либо принятие рисков.

>Разграчение ответственности за соблюдение аутсорсерами правил *охраны труда* электро- и пожарной безопасности (лучше описать в договоре), предоставление соответствующих закону условий для работы аутсорсера на своей территории.

> Необходимо компетентное курирование со стороны заказчика. Естественно, это менее затратно, чем содержание целого штата ИТ, однако требования к кураторам должны быть следующие:

» они должны хорошо понимать информационные технологии в применении к рынку, на котором они работают;

» знать требования регуляторов к информационным системам, контролировать их соблюдение аутсорсерами;

» быть «проверенными» людьми, в отношениях с аутсорсером контролировать выполнение аутсорсерами задач, необходимых для обеспечения бизнеса своей компании;

» контролировать доступ к конфиденциальной информации компании и возможность ее утечки;

» контролировать уровень компетентности специалистов подрядчика и соответствие их исполняемым обязанностям.

2. Аутсорсинг всей инфраструктуры на оборудовании партнера. В этом случае оборудование не закупается заказчиком, а сервисы на базе инфраструктуры аутсорсера включены в стоимость. Из вышеперечисленных проблем с заказчика снимается задача закупки оборудования, а если при этом все ИТ-ресурсы располагаются на территории аутсорсера, то организация пожарной безопасности и температурного режима помещений, соблюдение норм охраны труда тоже становятся заботой подрядчика. Но тут усугубляется проблема доступа аутсорсера к конфиденциальной информации компании-клиента.

3. Аутсорсинг определенных решений внутри инфраструктуры компании. Например, интегрировано в сеть решение, за которым нужно следить. On-site support и remote support в этом случае - тот самый аутсорс.

Плюсы такого аутсорса:

> перенесение ответственности за глюки решения, действия или бездействия при устранении аварии на аутсорсера;

> отсутствие необходимости выполнять рутинную работу штатным высококвалифицированным инженерам:

> реакция согласно SLA.

Минусы перечислены выше: нужны контроль и кураторы.

Мнение философа

Аутсорсинг не может быть плох, просто подходит он не всем

Аутсорсинг - это хорошо, если компания к нему готова и партнер-аутсорсер нормального уровня. В идеале вся непрофильная деятельность компании может быть отдана на аутсорсинг. А для небольших компаний/офисов, чем держать ИТ-шника в штате, лучше иметь хорошего спеца по вызову, который придет, настроит и вернется только когда что-то будет глючить. Иногда специалист со стороны может увидеть проблему или посмотреть на нее под другим углом. Своим многие вопросы просто приедаются, да и менять что-то, если сделано неправильно, - значит признать свои ошибки. Аутсорсинг не может быть плох, просто подходит он не всем. EOF

«Мы отдаем аутсорсерам только рутину»

- Бытует мнение, что привлечение аутсорсинговых ИТ-компаний приводит к утечке информации, поэтому организациям часто советуют как можно реже обращаться за помощью к сторонним ИТ-командам. На самом деле ситуация несколько иная. Поскольку ключевыми процессами в организации ведает собственный ИТ-департамент, который никогда не передаст критически важные приложения, ключи и пароли аутсорсерам, поэтому говорить о чрезмерных рисках при привлечении аутсорсинговых компаний было бы не совсем правильно. Проблемы могут возникнуть у компаний, в которых нет собственного ИТ-подразделения, но таких остается все меньше.

Наша компания прибегает к услугам аутсорсинговых ИТ-компаний, несколько десятков тысяч пользователей в Европе обслуживаются подобной компанией. Но у нас не возникало ситуаций с утечкой данных, поскольку сотрудники аутсорсинговых компаний заняты только рутинной работой, а жизненно важные для организации процессы - управление сетями,безопасностью и хранилищем данных - находятся в руках компетентных сотрудников в собственных ИТ-отделах компании.

Юрий Кушпетюк, специалист службы информационной безопасности компании APC by Schneider Electric

Доверяй, но проверяй

Как защититься от мнимым друзей

На вопросы «СА» отвечают эксперты по информационной безопасности

> **Какие риски информационной безопасности вы считаете наиболее опасными для компаний, которые пользуются аутсорсингом?**

> **Как системный администратор или ИТ-директор должен правильно строить отношения с аутсорсерами, чтобы обезопасить систему?**

НАТАЛЬЯ ЗОСИМОВСКАЯ, специалист отдела маркетинга компании «Информзащита»

Ищите лучших

Наиболее опасным я считаю риск утечки информации, а также нарушение целостности и доступности корпоративной сети. Говоря об аутсорсинге ИБ, я предлагаю рассматривать такие сервисы как удаленный мониторинг и управление средствами защиты клиента сторонней компанией, а также сервисы по сопровождению.

Что же традиционно представляют собой услуги по удаленному мониторингу и управлению? С подконтрольных средств безопасности клиента собираются все данные, необходимые для анализа, и передаются то выделенному защищенному каналу компании-аутсорсеру. Там они обрабатываются, анализируются, а на выходе клиент получает оповещения, касающиеся критичных событий в его сети. Такие оперативные оповещения являются руководством к действиям по устранению возникших проблем. Если клиент готов доверить компании-аутсорсеру не только мониторинг, но и элементы управления, то в этом случае можно говорить об услугах, касающихся управления IDS/IPS, а также устройствами межсетевого экранирования. Помимо функций мониторинга, сюда добавляются такие элементы управления, как изменение политик, а также проактивные обновления подконтрольных средств защиты и их мониторинг на предмет работы в штатном режиме.

Однако при всей видимой простоте и логичности этих услуг существует ряд обоснованных угроз и опасений клиентов. Это, прежде всего, риск утечки информации ограниченного доступа, касающейся самого проекта, а также получаемой ходе осуществления работ. Как с ним бороться?

Во-первых, естественно, необходимо закрепить юридическую ответственность путем подписания соглашения о конфиденциальности и SLA. В соглашении о конфиденциальности отражаются обязательства сторон по неразглашению и обеспечению режима защиты конфиденциальной информации. Service Level Agreement - это соглашение об уровне сервиса.

Во-вторых, нужно контролировать действия сотрудников аутсорсера. Зачастую одним из параметров сервиса по мониторингу и управлению средствами защиты является предоставление доступа клиенту на специализированный веб-портал. На нем фиксируются не только все события и выявленные инциденты ИБ, но и все действия аутсорсера. Если он совершает какие-то действия в отношении средств защиты клиента, то должен делать это только после подтверждения клиентом запланированных действий и в рамках оказываемого сервиса (это должно быть четко прописано в SLA).

В-третьих, не стоит забывать про разграничение прав доступа и своевременное удаление аккаунта аутсорсера (если такой заводился в сети).

В-четвертых, для безопасной передачи данных необходимо использовать технологию VPN, позволяющую передавать информацию в зашифрованном виде.

Помимо этого клиент может попросить исполнителя представить информацию об используемых технологиях физической безопасности центра, в котором будут храниться и обрабатываться данные, полученные с его средств защиты. Также желательно прояснить вопрос о средствах и методах обеспечения информационной безопасности.

Аутсорсинг - это проект, в котором не последнее место занимает доверие между исполнителем и заказчиком. Поэтому, выбирая аутсорсера, лучше ориентироваться на компании, которые уже хорошо себя зарекомендовали на рынке и имеют опыт осуществления аналогичных проектов. EOF

НИКОЛАЙ ЗЕНИН, руководите^ направления защиты коммерческих тайн LETA IT-company

Попробуйте DLP

Сегодня под ИТ-аутсорсингом часто понимают не только собственно передачу ИТ-сервисов на обслуживание сторонней компанией, но иногда и другие разновидности оказания услуг. Среди них:

- выполнение законченных проектов внедрения ИТ-систем по договору на оказание консультационных услуг;
- выполнение работ внешней организацией в рамках поставки ИТ-продуктов или предоставления других услуг (без договора на собственно выполняемые услуги);
- временная (по договору) аренда рабочей силы (ИТ-специалистов) сторонней организации с целью выполнения внутренних ИТ-проектов;
- заказная разработка программного обеспечения;
- абонентское обслуживание внешней организацией информационных систем, например, корпоративного веб-сайта, расположенных внутри предприятия;
- внешнее размещение ИТ-систем, например, создание и обслуживание системы управления персоналом, на стороне провайдера услуг (модель Software on-Demand, или Software as a service).

Естественно, у каждой из моделей - свои риски. Я подробнее остановлюсь на внешнем размещении ИТ-систем, например, создании и обслуживании системы управления персоналом, на стороне провайдера услуг (модель Software on-Demand, или Software as a service). Эта модель предоставления сервисов сейчас развивается наиболее интенсивно.

Опасения, которые испытывают заказчики, можно разбить на две группы.

К первой группе бизнес-рисков относятся:

1. Нерентабельность услуги (недостаточный возврат инвестиций).
2. Банкротство компании-провайдера.
3. Шантаж заказчика компанией-провайдером за счет конфиденциального характера обрабатываемых данных (гипотетически в результате нарушения отношений между компаниями).

Это важно!

Защищая информационные ресурсы от недоверенного подрядчика, определите уровень и зону его доступа. Возможно, достаточно предоставить доступ к части аппаратного обеспечения (на конфигурирование, не к данным), так как силами организации это более сложно или менее неэффективно.

Определите порядок доступа к важным данным. Объедините всех людей, которые работают с ними от внешней организации, в единый блок.

Выстроив защищенную инфраструктуру, назначьте ответственных за выдачу, отзыв и обновления сертификатов и ключей шифрования от вашей организации и полностью передайте все права на шифрование им.

4. Опасения, связанные с новизной формы оказания услуг.
5. Возможные затруднения в получении лицензии на обработку персональных данных.

Риски 2-4 компании снижают, выбирая надежную компанию-провайдера, имеющую опыт оказания этой же услуги компаниям схожего размера. Между заказчиком и провайдером должно быть подписано адекватное соглашение конфиденциальности.

К технологическим рискам (вторая группа) относятся:

Подходы, которые можно использовать для контроля над аутсорсером

№ пп	Подход к защите конфиденциальной информации	Примеры реализации
1.	Фильтрация исходящей информации по ключевым словам, регулярным выражениям для идентификации конфиденциальных данных	Системы фильтрации трафика (MIMEsweeper, «Дозор Джет», «Контур безопасности»)
2.	Установка грифов конфиденциальности на защищаемые документы и слежение за жизненным циклом помеченного документа	Системы мандатного доступа к документам и протоколирования обращений (SecretNet, SecrecyKeeper)
3.	Слежение за манипуляциями с конфиденциальными данными и протоколирование действий пользователя на рабочем месте	Системы контроля действий пользователя (StaffCop, «Инфоперiметр», ТКБ Мониторинг)
4.	Управление доступом к устройствам ввода-вывода	Системы контроля сменных носителей (DeviceLock, ZLock, Device Control)
5.	Ретроспективный анализ базы отправленной корреспонденции для расследования инцидентов безопасности	Хранилища почтовой и веб-корреспонденции («Дозор Джет», InfoWatch *Storage, Symantec Enterprise Vault)
6.	Исполнение всего комплекса вышеперечисленных подходов и сведение управления политиками и событиями к единой консоли	Системы Data Loss Prevention (Websense DSS, Symantec DLP, InfoWatch Traffic Monitor, McAfee DLP)
7.	Анализ протоколов разнообразных систем безопасности в унифицированном виде и выявление аномальных активностей со стороны сотрудников и внешних злоумышленников	Системы Computer Forensics (netForensics, RSA enVision, Symantec SIM)
8.	Контроль доступа пользователей к компьютерам и информационным системам с дополнительными элементами контроля	Системы двухфакторной аутентификации, системы с использованием биометрических методов опознавания
9.	Разветвленная система управления правами доступа к конфиденциальным документам	Системы класса Enterprise Rights Management (Microsoft RMS) и защищенного документооборота
10.	Шифрование носителей конфиденциальной информации	Системы шифрования хранилищ, дисков, накопителей

- случайная утечка от компании-провайдера услуг;
- нарушение целостности информации в связи с выходом из строя оборудования;
- недоступность информации в связи с нарушениями канала связи на стороне провайдера или на стороне заказчика.

Все риски этой группы снижают посредством контроля исполнения заключенного между сторонами соглашения об уровне сервиса.

Надо учитывать, что компания-провайдер финансово заинтересована в качественном исполнении услуг. Она серьезно рискует своей репутацией, если не приложит все силы для сохранения конфиденциальности, целостности, доступности информации заказчика. От компаний-провайдеров случаются утечки информации, но по существующей статистике, гораздо большее число утечек происходит все-таки из-за деятельности внешних злоумышленников и собственных сотрудников.

Неправомерно воспользоваться служебной информацией может и внешний подрядчик, и доверенный сотрудник организации.

Специализированную функцию по защите данных от «кражи» можно обеспечить с помощью системы защиты от утечек, контролирующей основные операции с критичной информацией - копирование, изменение (включая подмену символов), а также контроль перемещения за границы подконтрольной вычислительной сети.

Наряду с системой контроля утечек защита может быть реализована с помощью дополнительных технических средств и решений несколькими способами:

Первый способ - создание внутренней защищенной сети. В ней обрабатывается конфиденциальная информация (включая создание нескольких периметров безопасности, компании-аутсорсеру доступ предоставляется только к конкретным из них, не содержащим критичную информацию).

Второй способ - шифрование любых данных, выходящих за пределы вычислительной сети, сертификатами, к которым аутсорсер не получает доступа. При этом доступ к сертификатам строго учитывается, а сами сертификаты регулярно обновляются.

Третий способ - система передачи данных через почтовый сервер ЛВС в зашифрованном виде (это также можно автоматизировать).

Четвертый способ - использование технологий ограничения прав доступа - RMS и т.п., при котором внешнему подрядчику опять же не предоставляется доступ к сертификатам.

Пятый способ - резервное копирование конфиденциальной информации, при котором данные из ЛВС передаются только в зашифрованном виде, а при невозможности - с помощью аппаратного шифрования (без передачи ключей внешнему подрядчику).

Шестой способ - шифрование всех дисков рабочих станций и серверов.

Подходы, которые можно использовать для контроля над аутсорсером см. в таблице.

Из перечисленных подходов первые пять обеспечивают закрытие единичных сценариев защиты конфиденциальных данных от утечки.

От компаний-провайдеров случаются утечки информации, но гораздо большее число утечек происходит из-за деятельности внешних злоумышленников и собственных сотрудников

Подход 7 требует длительного кропотливого внедрения и отладки (1-3 года), чтобы начать получать качественные результаты.

Только подход 6 позволяет получать значимый результат (выявление источников утечки информации, предотвращение распространения стратегических планов компании) в первые же недели после внедрения системы Data Loss Prevention (DLP).

Оставшиеся подходы 8-10 дополнят системы DLP за счет снижения рисков утечки в результате кражи/потери ноутбуков или дисков. При этом совместно с DLP-системами используют также подходы 4 для дополнительного контроля над портами компьютеров и 5 для ретроспективного анализа инцидентов. EOF

«Считайте затраты»

Павел Ерошкин, начальник Управления информационной безопасности компании «Техносерв»:

- Передавая систему информационной безопасности компании на аутсорсинг, следует учитывать стоимость контракта, риски оттока специалистов в компанию-аутсорсер, и соответственно, количество времени и денег, которые придется потратить на поиск новых сотрудников, а также затраты на ведение договора. Кроме того, нужно принимать во внимание стоимость контроля исполнителя, особенно в случае аутсорсинга информационной безопасности. Существует три основных этапа передачи системы ИБ на аутсорсинг. Это - проектирование комплексной системы информационной безопасности (КСИБ). Совместный процесс проектирования дает обеим сторонам необходимые данные для понимания проблем и задач, связанных с управлением ИБ.

Следующий этап - внедрение КСИБ. Проведение пуско-наладочных работ позволяет узнать все особенности внедренной системы, что дает обеим сторонам детальное понимание принципов работы компонентов КСИБ, а также позволяет эффективно распределить роли участников.

И, наконец, техническое обслуживание КСИБ. Этот этап позволяет заказчику понять, насколько целесообразной и обоснованной будет передача процесса управления ИБ на аутсорсинг. Сюда также необходимо добавить процессы написания проектов, организационно-распорядительной документации, инструкций, регламентов и т.д. Написание политики информационной безопасности компании,как правило, является самостоятельным процессом, в котором, впрочем, есть место и для аутсорсинга ИБ.

Павел Бетсис:

"ОТКАЗАТЬСЯ ОТ ИННОВАЦИЙ— ЗНАЧИТ ПЕРЕСТАТЬ РАЗВИВАТЬСЯ"

На вопросы «Системного администратора» отвечает генеральный директор 000 «Сиско Системс» Павел Бетсис

Галина Положевец

Павел Бетсис руководит деятельностью 000 «Сиско Системе». Он возглавляет коллектив более чем из 300 сотрудников и отвечает за все деловые операции компании в России. Работая в мировой ИТ-индустрии с 1985 года, П. Бетсис приобрел обширный опыт успешной деятельности в ключевых областях ИТ-индустрии (аппаратное и программное обеспечение, различные сервисы, а также венчурное инвестирование) за счет сотрудничества, как с крупными корпорациями, так и стартапами в Канаде, США, Австрии, Италии, Голландии и ряде стран Азии. Свою карьеру он начал в IBM, где вырос от программиста до руководителя отдела продаж. Затем Павел работал региональным руководителем отдела продаж компании Sterling Software, а до прихода в 000 «Сиско Системе» был главным исполнительным директором pVeiocity, Inc. - успешной компании-поставщика программного обеспечения ERP, которая входит в состав крупной венчурной компании Edgestone Capital, широко представленной на рынках Северной Америки и Европы. Павел Бетсис родился в 1962 году в Украине. Выпускник Торонтского университета, также получил образование в области административного управления в Гарвардском университете.

- **Павел, скажите, пожалуйста, с чем связаны изменения в стратегии Cisco в России?**

- Мы хотим привести работу нашей компании в соответствие с приоритета'.'.- самой России. Cisco сегодня уделяет особое внимание развитию программ, способствующих созданию инновационной экономики в стране. По ряду направлений мы уже добились немал= •• успехов. Например, сетевые академии Cisco в России давно готовят специалистов по теории и практике проектирования, строительства и эксплуатации локальных и глобальных сетей. Вместе с тем некоторые направления мы только собираемся развивать.

- **Правда ли, что компания намерена укреплять сотрудничество с государственными структурами, чтобы получить статус доверенного советника Правительства РФ?**

- Да, тесное взаимодействие с правительством страны - один из наших главных приоритетов. Мы активно работаем с федеральными органами, министерствами и в дальнейшем планируем только укреплять эти отношения. Cisco участвовала и участвует в реализации ряда инфраструктурных проектов в России. Практически всегда они курируются госструктурами и финансируются из госбюджета. Для участия в подобных проектах наше оборудование должно иметь соответствующие сертификации и лицензии.

- **Вы хорошо знаете российский рынок?**

- Кое-кто считает, что российский ИТ-рынок кардинально отличается от дру-

гих. Более того, существует мнение, будто в России все кардинально отличается от остальных стран. Думаю, это не так. Различия, конечно же, есть, но все-таки гораздо больше общего с зарубежными ИТ-рынками.

Используемые в России технологии достаточно похожи на те, что распространены везде. Отличия же связаны, в первую очередь, с «ландшафтом» партнеров и системных интеграторов. По сравнению с западными странами, в России их намного больше, причем они специализируются в различных направлениях в рамках одной компании. Если же говорить о работе с отечественными заказчиками, то приоритеты практически такие же, как во всем мире. Иным может быть уровень развития, возможно, здесь сложнее работать в каких-то направлениях, но в целом я не разделяю мнение о том, будто в России все не так.

- **Информационные технологии - это одно из стратегических направлений. Но участники ИТ-отрасли считают, что их развитие могло бы быть более успешным. Например, федеральный проект «Электронная Россия» фактически провалился.**

- Не вдаваясь в подробности, могу привести целый ряд примеров крупных государственных проектов в таких странах, как Голландия, Италия, Канада, США, Швеция, которые были признаны неудачными. Так что и в этом плане Россия не слишком отличается от других стран.

- **Вы ставите амбициозную задачу - увеличить вдвое бизнес компании в России за три года. Но на дворе кризис. В каких направлениях будете двигаться?**

- Цель нашей компании - создание технологий, меняющих способы человеческого общения, связи и совместной работы, поэтому Cisco работает со всеми сегментами ИТ-рынка. Но ключевое направление для нас - все, что связано с государственными проектами.

Наши планы действительно амбициозные, и мы понимаем, что их будет нелегко осуществить.

Что касается кризиса, то, как и многие, я считаю, что он еще не закончился. Тем не менее мы рассчитываем уже в 2010 году добиться позитивных изменений на базе нашей стратегии.

- **По вашему мнению, какие направления ИТ-отрасли будут развиваться в России в ближайшие годы?**

- На мой взгляд, одна из перспективных тенденций - это создание центров обработки данных. Виртуализация в России пока недостаточно развита, хотя технология, позволяющая делать это успешно, уже существует, и у нас есть решения, позволяющие повысить эффективность ЦОД.

С точки зрения бизнеса, наиболее перспективным сегментом можно назвать малый и средний бизнес. Наша компания выводит на рынок предназначенные специально для МСБ новые продукты и решения высокого качества, но по приемлемым ценам. Кроме того, Cisco активно поддерживает своих закачиков и партнеров, работающих в данном сегменте. Так, например, в сентябре мы провели в Екатеринбурге, Санкт-Петербурге и Москве серию семинаров о решениях Cisco для предприятий малого и среднего бизнеса под названием Cisco Business Solution Workshop.

Наша компания не сокращает бюджет, несмотря на трудности. Мы просто не можем себе это позволить, **потому что это все равно, что перестать развиваться**

- **Однако малые предприятия, как правило, бедны, далеко не все из них имеют даже компьютеры.**

- Это общемировая проблема. Перспективы малого и среднего бизнеса зависят от того, как идут дела в больших организациях. Когда происходит насыщение рынка, наступает кризис, малые и средние предприятия начинают играть основную роль. Но в ИТ-отрасли это неразвитый сегмент. ООО «Сиско Системе» ведет активную деятельность в данном сегменте. В конце июля 2009 года мы ввели в России в действие программу «Клуб ИТ-директоров» для ключевых заказчиков, работающих в сегменте МСБ. Проект предусматривает организацию веб-конференций, семинаров и встреч, подготовленных Cisco специально для членов клуба. Основная задача программы - с помощью технологий виртуального общения Cisco регулярно информировать заказчиков о последних разработках и решениях нашей компании.

- **Рассказывая о видеотехнологиях, вы назвали их одними из самых перспективных и востребованных. Почему?**

- Видео все шире используется на всех уровнях. По данным организованного компанией Cisco исследования под названием Visual Networking Index (VNI) Research («Индекс развития визуальных сетевых технологий»), к 2012 году объем использования видео в деловых целях увеличится почти на 78 процентов. Мы не ожидаем в ближайшее время особого бума, связанного с ростом бизнеса: все компании стремятся сократить свои расходы - такова общемировая тенденция. Видео же помогает решить многие проблемы. Одна из наших технологий - Cisco TelePresence - позволяет проводить удаленные переговоры с эффектом присутствия, избавляя от необходимости по каждому случаю ездить в командировки. Поэтому мы ежедневно используем эту технологию в 45 странах, включая Россию, сэкономив таким образом более 275 миллионов долларов за счет резкого сокращения служебных поездок.

- **Каков ваш прогноз развития ИТ-отрасли на ближайшие пять лет?**

- Давайте посмотрим на этот вопрос философски. Более двадцати лет назад, когда я только начинал работу в этой отрасли, все в ней было построено на огромных мэйнфреймах IBM - компании, где я тогда работал. Такие корпорации, как Cisco, в то время еще только вставали на ноги. Затем развитие ИТ-отрасли стало двигаться в направлении программного обеспечения, потом начали развиваться услуги.

Особое мнение

Многие из читателей «Системного администратора» постоянно внедряют технические решения разных компаний. И нередко находят и пытаются исправить ошибки разработчиков. Учитывает ли Cisco в своей работе мнение сисадминов? На вопрос «СА» отвечает технический директор компании ООО «Сиско Системе» **Андрей Кузьмич:**

«Каждый заказчик уникален»

- В нашей компании на корпоративном уровне проводится ежегодный электронный опрос заказчиков, в том числе специалистов, занимающихся эксплуатацией. Это не просто участие в опросе по принципу: выбери ответ, который тебе больше нравится. Предполагается и даже приветствуется, что респонденты могут еще и оставлять свои комментарии. Таким образом, результаты опроса позволяют тщательно проанализировать ситуацию, в том числе технических и эксплутационных аспектов применения технологий и решений Cisco. В дальнейшей работе с заказчиками, особенно с крупными, всегда учитывается информация, которую они нам предоставляют. Все замечания обобщаются, и если они превышают определенный порог по тем же техническим требованиям, то, безусловно, вводится модификация.

Впрочем, мой опыт свидетельствует о том, что все заказчики уникальны. У каждого из них может быть свое, особое требование, и все выполнить просто невозможно. Я еще ни разу не видел, чтобы система внедрялась так, как она спроектирована разработчиками. Люди всегда хотят чего-то еще. Например, мы даем рекомендации по эксплуатации нашего оборудования, но в компаниях хотят повысить эффективность системы. Люди прилагают усилия, чтобы система работала так, как мы проектируем ее в пике, но при этом, чтобы в пике она стабильно работала. Ничего подобного на развитых западных рынках не происходит. Там службы эксплуатации прислушиваются к тому, что говорит производитель. Конечно, тоже с определенной долей скепсиса, но с гораздо меньшей, чем у нас.

Прошло время, и вектор развития вновь изменился. То, что мы видим сегодня, - это комбинация ПО и услуг. Мы создаем необходимые сервисы для своих заказчиков, используя свое оборудование и даже технические решения наших партнеров или других компаний. Это направление, полагаю, и будет развиваться в ближайшем будущем.

- **Какую технологию Cisco вы считаете наиболее удачной?**

- Все технологии, связанные не столько с передачей информации, сколько с совместной работой, очень перспективны. Скажем, меня приглашают принять участие в виртуальном совещании в пятницу вечером. Я с удовольствием присоединюсь к нему, поскольку теперь это возможно делать у себя дома, пользуясь компьютером или мобильным телефоном. Для этого мы используем технологию Cisco WebEx - инновационное решение, которое позволяет в режиме реального времени проводить интерактивные семинары, тренинги, конференции, избавляя участников от необходимости тратить время и средства на поездки.Таким образом, ты можешь, если захочешь, работать в неделю уже не 40, а 80 часов.

- **Вы трудоголик?**

- Нет. Но если есть возможность принять участие в важной встрече, всего лишь нажав кнопку на мобильном телефоне или ноутбуке, почему бы ею не воспользоваться? Технология Cisco WebEx может применяться как на работе, так и в частной жизни. Она дает уникальные возможности для личного общения между людьми практически всюду и в любой ситуации. У нас много сотрудников, которые не ездят каждый день в офис, но работают очень успешно.

- **Тема инноваций популярна в последние годы в России. Удается ли вам сегодня заниматься технологическими инновациями?**

- Создание инновационных технологий никак не зависит от кризиса. Cisco тратит более четырех миллиардов долларов в год на развитие инновационных технологий и, несмотря на общемировые проблемы, не сокращает ассигнования на эти цели. Да мы и не можем себе это позволить, потому что это все равно, что перестать развиваться. Урезают бюджеты наши заказчики. Cisco же даже в условиях кризиса предлагает своим клиентам гибкие условия финансирования, благодаря чему заказчики могут приобрести любое оборудование.

- **Вы собираетесь создавать собственное производство. Почему вы так решили?**

- Прежде всего, хочу заметить, что мы нигде в мире не занимаемся производством, вернее, нам не принадлежат те заводы, на которых производится наша продукция. Но мы занимаемся логистикой. Россия представляет для Cisco большой интерес и входит в список важнейших приоритетов компании. А для дальнейшего стратегического развития на внутреннем рынке очень важно иметь собственное производство.

- **Все бизнес-сообщество в России обсуждает сегодня «Закон о персональных данных». Многие считают его несовершенным. Ваше отношение к нему?**

- Знаю, что закон был принят достаточно давно, хотя ИТ-отрасль не восприняла его серьезно. Но я абсолютно согласен с тем, что закон необходим, тем более, что подобные законы ее ; во многих странах. И отрасль должна отнестись к нему со всей ответственностью.

Все, что связано с незапланированными инвестициями, обычно воспринимается негативно. В таких случаях участники рынка всегда просят, даже требуют отсрочки. Это характерно для любой страны. Но закон «О защите персональных данных» важен и для компаний, и для любого гражданина.

- **Информационная безопасность, мне кажется, с каждым годом приобретает все большую остроту и в бизнесе,и в частной жизни.**

- Согласен. Именно поэтому наша компания придает такое значение соответствующим технологиям. До конца года мы сделаем несколько официальных объявлений и анонсируем новые решения в области ИБ.

- **Почему девизом десятой юбилейной конференции Cisco стало выражение «Знание - сила»?**

- Во-первых, этот девиз хорошо звучит, а во-вторых, рекордное число участников конференции - 2298 и небывалое число партнеров, спонсоров и медиапартнеров форума наглядно подтвердило его верность. Знание - действительно сила.

- **А у вас есть свой личный девиз?**

- Был когда-то - в мои пионерские годы. «Будь готов! Всегда готов!». И, знаете, этот девиз для меня до си> пор актуален. EOF

Уязвимость в URJ-обработчике в Google Apps

Программа: Google Apps 1.1.110.6031, возможно, другие версии.

Опасность: Высокая.

Наличие эксплоита: Нет.

Описание: Уязвимость существует из-за ошибки в googleapps.exe при обработке аргументов, полученных через «googleapps.url.mailto:» URI. Удаленный пользователь может с помощью специально сформированного Web сайта передать произвольные аргументы приложению chrome.exe и выполнить произвольные приложения из сетевой папки посредством опции -renderer-path.

URL производителя: pack.google.com

Решение: В настоящее время способов устранения уязвимости не существует.

Уязвимость при обработке «iim:» URI в IBM installation Manager

Программа: IBM Installation Manager 1.3.2, возможно, другие версии.

Опасность: Высокая

Наличие эксплоита: Нет

Описание: Уязвимость существует из-за ошибки в IBMIM.exe при обработке аргументов, полученных через «iim:» URI. Удаленный пользователь может с помощью специально сформированного аргумента -vm загрузить произвольную библиотеку с сетевого общедоступного ресурса.

URL производителя: www-01.ibm.com/software/rational/installmgr/faq.html.

Решение: В настоящее время способов устранения уязвимости не существует.

Множественные уязвимости в Cisco Unified Presence

Программа: Cisco Unified Presence версии до 6.0(6) и 7.0(4); Cisco Unified Presence Server 1 .x.

Опасность: Средняя.

Наличие эксплоита: Нет

Описание: 1. Уязвимость существует из-за ошибки в TimesTenD-процессе. Удаленный пользователь может создать большое количество подключений к TCP-портам 16200 и 22794 и аварийно завершить работу процесса.

2. Уязвимость существует из-за ошибки в строенном МСЭ при отслеживании сетевых подключений. Удаленный пользователь может создать большое количество TCP-подключений и заполнить всю таблицу отслеживания подключений, что не позволит создать новые сетевые подключения к устройству.

URL производителя: www cisco.com

Решение: Установите исправление с сайта производителя.

Переполнение буфера в rpc.cmsd в IBM AIX

Программа: IBM AIX 5.3 и 6.1; IBM Virtual I/O Server (VIOS) версии 1.4, 1.5 и 2.1, возможно, более ранние версии.

Опасность: Средняя.

Наличие эксплоита: Нет.

Описание: Уязвимость существует из-за ошибки проверки границ данных в библиотеке libcsa.a. Удаленный пользователь может с помощью специально сформированного RPC-запроса к Calendar Manager Service Daemon (rpc.cmsd), содержащего слишком длинный аргумент для удаленной процедуры 21, вызвать переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: www.ibm.com.

Решение: Установите исправление с сайта производителя.

Переполнение буфера в Noveil NetWare

Программа: Novell NetWare 6.5, возможно, другие версии.

Опасность: Средняя.

Наличие эксплоита: Нет.

Описание: Уязвимость существует из-за ошибки в portmapper-демоне PKERNEL.NLM при обработке RPC-запросов. Удаленный пользователь может с помощью специально сформированного CALLIT RPC-вызова вызвать переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: www.novell.com/products/netware.

Решение: Установите исправление с сайта производителя.

Повышение привилегий в Microsoft Windows

Программа: Microsoft Windows 2000; Microsoft Windows XP; Microsoft Windows 2003; Microsoft Windows Vista; Microsoft Windows 2008.

Опасность: Низкая.

Наличие эксплоита: не-

Описание: 1. Уязвимость **существует из-за** ошибки в ядре Windows при преобразовании 64-битного значения в 32-битное. Локальный пользователь может вызвать целочисленное переполнение и выполнить произвольный код на системе с повышенными привилегиями.

2. Уязвимость существует из-за ошибки разыменования нулевого указателя в ядре Windows при обработке некоторых данных в исполняемых файлах. Локальный пользователь может с помощью специально сформированного файла выполнить произвольный код на целевой системе с повышенными привилегиями.

3. Уязвимость существует из-за ошибки при обработке исключений в ядре Windows. Локальный пользователь может аварийно завершить работу системы.

URL производителя: www.microsft.com.

Решение: Установите исправление с сайта производителя.

Составил Александр Антипов

Визитка

ИГОРЬ ШТОМПЕЛЬ, инженер, системный администратор. Сфера профессиональных интересов - GNU/Unux, функциональное программирование

Продукты для виртуализации

Возможности свободного программного обеспечения

С каждым годом расширяется применение виртуализации вычислительных процессов. Появляются новые технологии. А на что способно свободное программное обеспечение в данной области?

Ключевые термины и типы виртуализации

Итак, **виртуализация** - это абстракция каких-либо ресурсов в вычислительных целях (например, запуск одной операционной системы из-под другой). С данным определением тесно связаны такие понятия, как хост, гостевая операционная система, гипервизор.

Хост - операционная система, в которой осуществляется виртуализация, а **гостевая операционная система** - это та, которая виртуализируется. Например, на компьютере установлены операционная система gNewSense GNU/Linux и программное обеспечение Virtualbox OSE (об этой версии подробнее далее), в котором запущен Trisquel GNU/Linux. Так вот, gNewSense в данном случае - хост, Trisquel - гостевая операционная система.

Гипервизор - это программное обеспечение, которое позволяет гостевой операционной системе взаимодействовать с физическими (не эмулируемыми, которые использует хост) аппаратными средствами.

В разных источниках выделяются разные типы виртуализации. Например, в Википедии: виртуализация серверов, аппаратная виртуализация, виртуализация уровня ОС и паравиртуализация, виртуализация ресурсов и виртуализация приложений. А Тим Джонс, инженер-консультант Emulex (http://www.emulex.com), в своей статье «Виртуальный Linux» выделил следующие типы - эмуляция оборудования, полная виртуализация, паравиртуализация и виртуализация уровня операционной системы [1].

Рассмотрим, что представляют собой выделенные типы. Итак, **эмуляция оборудования** - это процесс представления программой виртуализации того или иного программного обеспечения как аппаратного составляющего для гостевой операционной системы. Таким образом, с помощью программы виртуализации, предоставляется возможность работы с виртуальным (эмулирующим работу оригинального) оборудованием.

Например как частный случай выбор объема оперативной памяти на этапе создания гостевой системы. Среди свободных программ подобного типа можно выделить Bochs (http://bochs.sourceforge.net), QEMU (http://www.qemu.org) и FAUmachine (http://www3.informatik.uni-erlangen.de/Research/FAUmachine).

Полная виртуализация отличается от эмуляции оборудования тем, что между гостевой операционной системой и аппаратной частью появляется «посредник». Этот «посредник» - гипервизор, который обеспечивает взаимодействие последних. В мире свободных программ данной функциональностью обладает VirtualBox OSE (http://www.virtuaibox.org/wiki/Editions).

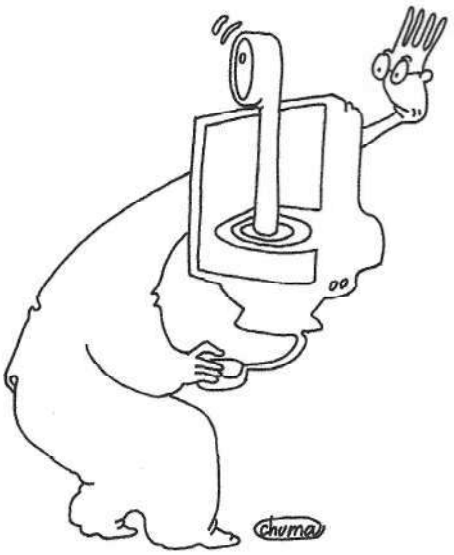
Паравиртуализация имеет сходство с полной виртуализацией. При данном подходе гипервизор ответственен за разделение доступа к основным аппаратным средствам. Гостевой операционной системе через гипервизор доступен специализированный API. Последний позволяет «гост-; взаимодействовать с аппаратным обеспечением. Поскольку код, необходимый для осуществления виртуализации, добавлен в ядро Linux (библиотеки и приложения user-space не модифицируются), то отпадает необходимость в дополнительной перекомпиляции. Последнее может иметь место. например, при использовании метода полной виртуализации. Примером свободного программного обеспечения для реализации данного метода может служить Xen (http: www.cl.cam.ac.uk/research/srg/netos/xen).

Эмулятор Bochs

Основателем проекта, как и одним из разработчиков, до сих пор (помимо него изменения в проект вносили несколько сотен человек) является Кевин Лоутон (Kevin Lawton, http: www.linkedin.com/in/kevinlawton). Сегодня у проекта шесть мейнтейнеров.

В основе названия программы лежит игра слов - фонетически оно произноситься так же, как английское слове «box» (технические специалисты любят называть свои машины - «box» (например, «Linux box»), вот и получается что Bochs эмулирует «box» внутри «box»). Кстати, это отражает и логотип проекта.

Программа (лицензия GNU LGPL) представляет собой эмулятор аппаратного обеспечения архитектуры IA-32 (x86: написанный на языке программирования C++. Bochs досту-



Виртуализация - это абстракция каких-либо ресурсов **в вычислительных** целях **(например, запуск одной ОС из-под другой)**

пен для таких операционных систем, как GNU/Linux, BSD-системы, Windows 95/98/NT/2000/XP/Vista и DOS. Среди поддерживаемых платформ - x86 (эмуляция процессоров - 386, 486, Pentium/PentiumII/PentiumIII/Pentium4, x86-64 с поддержкой инструкций MMX, SSEx и 3DNow!), Alpha, Sun и MIPS. В программе возможна работа со следующими гостевыми системами: GNU/Linux, BSD-системы, Windows и DOS (см. рис. 1).

Bochs поддерживает эмуляцию CD-ROM для операционных систем Linux, Windows, BeOS и большинства BSD-систем. В программе доступна эмуляция Sound Blaster 16 (SB16) - MPU401 (MIDI-процессор) с поддержкой режимов UART (Universal Asynchronous Receiver/Transmitter, Универсальный асинхронный приемопередатчик- перевод данных в/из последовательной в/из параллельную форму). Эмулятор также обладает поддержкой сетевых карт NE2000.

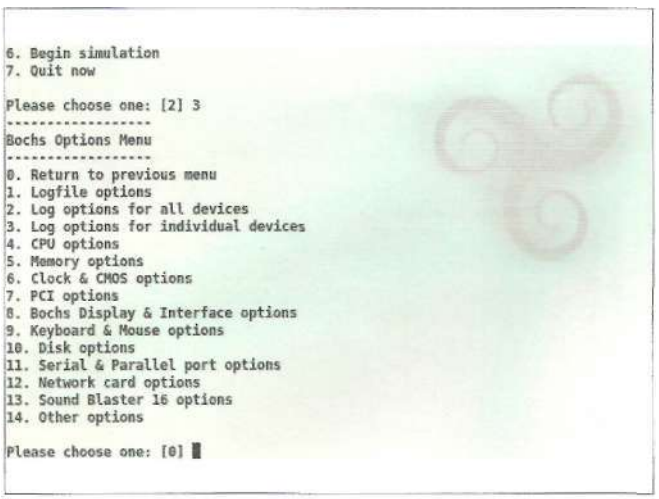
QEMU

Рассмотрим еще один эмулятор аппаратного обеспечения. Проект QEMU был зарегистрирован на http://savannah.nongnu.org 9 апреля 2003 года. Официальный сайт, посвященный QEMU - http://www.qemu.org, был запущен в 2005 году. Сегодня активных участников проекта насчитается 11 человек, а права на торговую марку принадлежат активному разработчику с первых дней проекта Фабрису Беллару (Fabrice Bellard, http://bellard.org) - ведущему разработчику Ffmpeg (создал библиотеку libavcodec). Любопытно, что именно он является автором формулы Беллара, которая позволяет наиболее быстро вычислить единичный разряд числа Пи в двоичном представлении (http://bellard.org/pi).

QEMU в качестве хост-платформ поддерживает x86, x86_64 и PowerPC, а в тестовом режиме - Sparc32 и ARM [2]. Имеет два режима работы. Первый - это «пользовательская эмуляция» (User emulation), при которой возможен запуск бинарных файлов для различных платформ. Второй - это «полная эмуляция» (System emulation), при которой эмулируются платформа полностью (похоже на Bochs) и соответственно операционные системы. Например, на рис. 2 показан запуск gNewSense GNU/Linux 2.3 Deltah с использованием одной из графических оболочек (о них чуть позже), созданных для данного эмулятора, - QtEmu и QEMU.

В качестве гостевых платформ для «пользовательской эмуляции» доступны x86, ARM, SPARC, MIPS, m68k (Coldfire) и CRIS. Кроме того, x86_64, PowerPC, PowerPC64, SH-4 и MicroBiaze поддерживаются в тестовом режиме, а поддержка SPARC64 и Alpha находится в стадии разработки. Например, QEMU позволяет запустить на x86 бинарный файл для ARM в Linux (т.е. ПО, включая и операционные системы, разработанное для одной платформы в другой) путем реализованной в нем технологии динамического транслятора (подробнее можно прочитать в статье Беллара, описывающей его внутреннее устройство, - http://www.usenix.org/publications/library/proceedings/usenix05/tech/freenix/full_papers/bellard/bellard.pdf). Помимо динамического транслятора для усовершенствования эмуляции в QEMU был реализован специальный акселератор. Последний позволяет выполнить эмулируемый код на процессоре хоста, что значительно повышает эффективность и скорость эмуляции.

Рисунок 1. Настройка Bochs



Что касается «полной эмуляции», то доступны x86, x86_64, **ARM,** SPARC, MIPS, MIPS64, m68k (Coldfire); PowerPC, CRIS и MicroBlaze в тестовом режиме; SPARC64, PowerPC64, SH-4 и Alpha - в стадии разработки. При работе с данным эмулятором гостевыми системами могут являться GNU/Linux, FreeBSD, Mac OS X, Windows, BeOS.

Тонкая конфигурация QEMU производится из консоли. Но в то же время для работы с эмулятором доступны различные графические интерфейсы: QtEmu, Qemulator, Qemu Launcher.

FAUmachine

С проектом QEMU связан проект FAUmachine, который создан в Университете Эрланген-Нюрнберг имени Фридриха-Александра на отделении компьютерных наук технического факультета. Официальная страница проекта доступна по адресу http://www3.informatik.uni-erlangen.de/Research/FAUmachine.

FAUmachine - это виртуальная машина, которая запускается как обыкновенный пользовательский процесс (в пространстве пользователя) и работает без привилегий суперпользователя. Процессор FAUmachine основан на эмуляторе QEMU, что, как было отмечено выше, и связывает эти два проекта. Начиная с релиза 20090922, добавлен дополнительный процессор, который использует KVM-модуль ядра Linux для выполнения кода гостевых систем на процессоре хоста вместо эмуляции.

FAUmachine поддерживает эмуляцию следующих аппаратных компонентов: процессоров x86 и x86_64; контроллеров IDE и SCSI; сетевых адаптеров NE2000 и Intel еергоЮО; звуковой карты SB16; общего VGA-адаптера и графического адаптера Cirrus GD5446; 24 и 48 контактных PCI-карт ввода-вывода. А из периферии - сетевых концентраторов и маршрутизаторов; модемов.

Кроме того, виртуальная машина, как показано на рис. 3, обладает возможностью делать скриншоты эмулируемых систем и снимать видео их работы. В рамках проекта разработан экспериментальный интерпретатор и компилятор языка VHDL - fauhdlc, доступный по адресу - http://www3.informatik.uni-erlangen.de/Research/fauhdlc. Например, с помощью этого языка, по словам разработчиков, можно создавать скрипты, автоматизирующие инсталляцию дистрибутивов Linux и других операционных систем с использованием дисковода компакт-дисков или файлов-образов.

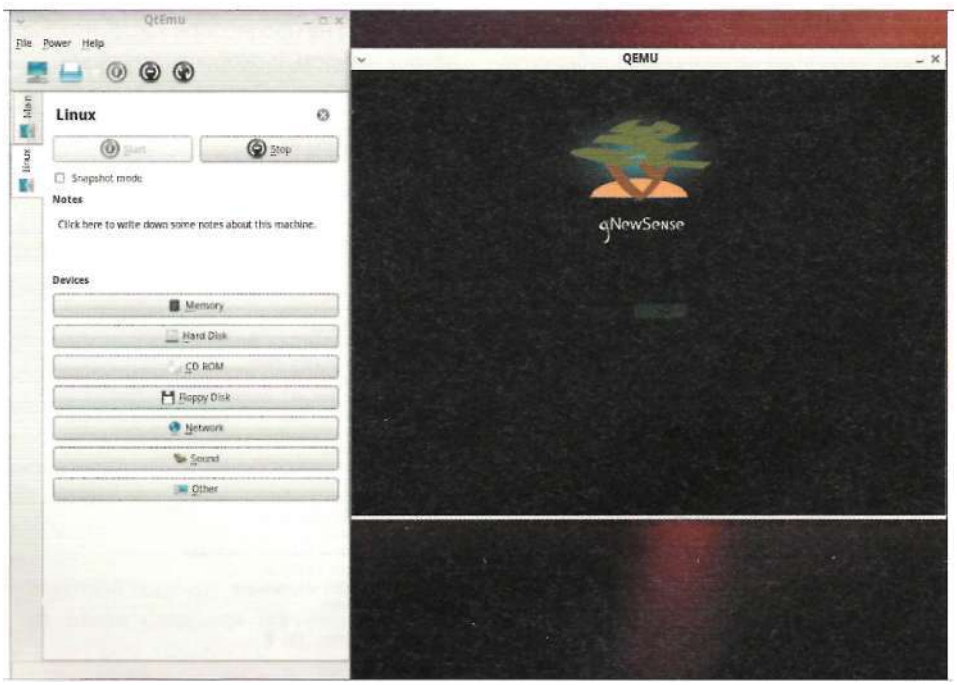
VirtualBox OSE (Open Source Edition)

Об этом программном продукте в мартовском номере «СА» за 2007 год была размещена статья Валентина Синицына «VirtualBox - виртуализация под GPL». Сейчас отметим изменения, которые претерпел продукт за это время.

Список функций, доступных только в закрытой версии VirtualBox, сократился и включает в себя следующее: сервер удаленного доступа к гостевой машине (Remote Display Protocol Server), поддержка USB (в том числе возможность предоставить доступ удаленным машинам к локальным USB-устройствам - USB over RDP). Основная проблема в том, что эти функции востребованы как в корпоративной среде, так и домашними пользователями (последним, конечно же, интересна в первую очередь поддержка USB, которая значительно облегчает вывод данных из виртуальной машины).

Таким образом, в VirtualBox OSE появилась возможность работать с разделяемыми папками (Shared Folders - но при попытке установки для их использования «Дополнений гостевой ОС» программа предлагает произвести загрузку дополнительного файла в формате .iso, лицензионное соглашение для которого мне обнаружить не удалось как на сайте www.virtualbox.org, так в самом файле-образе) и инициатором iSCSI. Последний необходим, чтобы иметь

Рисунок 2. Запуск gNewSense с использованием QEMU



возможность клиентского доступа к интерфейсу SCSI. Разработчики по-прежнему заверяют, что данный список функций будет меняться с течением времени и некоторые станут доступны в свободной версии программы [3].

Гипервизор Хеп

Хеп - это гипервизор для реализации паравиртуализации. Его разработка была начата исследовательской группой из компьютерной лаборатории (http://www.cl.cam.ac.uk) Кембриджского университета (http://www.cam.ac.uk) как часть проекта Xenoservers (http://www.cl.cam.ac.uk/research/srg/netos/xeno/index.html), финансируемого британским правительством в лице EPSRC (http://www.epsrc.ac.uk/default.htm). Релиз 1.0 был выпущен в октябре 2003 года. В настоящее время над проектом также работают в RedHat, IBM, HP, XenSource, Intel, AMD, Novell.

Основные сферы его применения следующие. Запуск нескольких изолированных (большой плюс в случае сбоя одного из них) друг от друга виртуальных серверов на одном физическом хосте; достижение аппаратной независимости (перенос операционных систем и приложений при переходе на новое оборудование); тестирование различных версий операционных систем, в том числе и параллельно; тестирование и отладка ядра операционной системы (не требуется отдельная машина); достижение большей гибкости кластерных вычислений (например, лучший контроль и изоляция за счет «живой миграции» машин для балансировки нагрузки кластера); необходимость в широкой аппаратной поддержке таких операционных систем, как GNU/Linux.

Что касается аппаратной поддержки, то Хеп работает на архитектуре x86 (процессоры P6 и новее - Pentium Pro, Celeron, Pentium II, Pentium III, Pentium IV, Xeon, Athlon и Duron от AMD). Полный список поддерживаемых процессоров доступен по адресу http://wiki.xensource.com/xenwiki/HVM_Compatib!e_Processors. Имеется возможность работы с многопроцессорными машинами. Кроме того, есть поддержка Hyper-Threading (SMT) и портов на IA64 и PowerPC.

32-битный гипервизор Хеп по умолчанию предоставляет возможность работы с Intel's Physical Addressing Extensions (PAE), который обеспечивает адресацию оперативной памяти до 64 Гб (архитектура x86). Без использования PAE адресация гораздо меньше - 4 Гб. Адресация оперативной памяти до 1 Тб доступна для платформ - Intel EM64T и AMD Opteron.

Хеп поддерживает работу с таким операционными системами, как GNU/Linux, NetBSD, FreeBSD, Solaris. Если используется процессор без поддержки аппаратной виртуализации, то потребуется модификация ее ядра для использования Хеп. При использовании процессоров с поддержкой технологий Intel VT (Intel(R) Virtualization Technology) или AMD SVM (Secure Virtual Machine) изменение ядра гостевой операционной системы не требуется.

KVM или Linux в роли гипервизора

Впервые KVM (Kernel-based Virtual Machine) была включена в ядро Linux версии 2.6.20. KVM - это технология, которая позволяет превратить ядро Linux в гипервизор путем инсталляции модуля ядра kvm.ko. Последний имеет специальные файлы поддержки процессора (kvm-intel.ko - для Intel и kvm-amd.ko - для AMD), другими он использует расширения HVM (Hardware Virtual Machine) процессоров (Intel VT и AMD SVM).

Основная особенность виртуальной машины ядра заключается в том, что она, превращая ядро в гипервизор, обеспечивая высокую скорость виртуализации, позволяет запускать другие операционные системы (например, другие ядра Linux), которые будут **иметь** изолированное аппаратное обеспечение (сетевую **карту,** графический адаптер и другое) [4]. Список поддерживаемых гостевых операционных систем обширен. Ознакомиться с **ним можно** по адресу: http://www.linux-kvm.org/page/Guest_S „zz :'t_Status. Он включает дистрибутивы GNU/Linux, **операционные** системы семейства BSD, UNIX (Darwin, MINIX, **GNU/Hurd), Solaris**/OpenSolaris, Windows и ряд других.

KVM тесно связана с QEMU. QEMU осуществляет операции ввода-вывода с «гостем». Так, все запросы на **ввод-**вывод со стороны последнего перехватываются и направляются в пространство пользователя для эмулирования процессом QEMU (последний в свою очередь незначи'е.~=-но для этого модифицирован) [5].

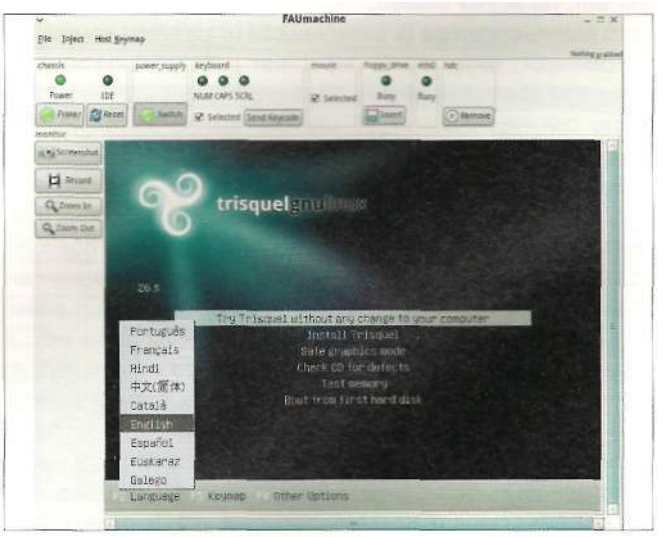
***

В статье было рассмотрено свободное программное обеспечение, используемое для виртуализации. Из отмеченных типов последней, наиболее проблемной областью, применительно как к корпоративным требованиям, так и требованиям домашних пользователей, является полная виртуализация и VirtualBox OSE. Кроме того, QEMU способствовал развитию ряда из рассмотренных проектов, а технология KVM стоит особняком и предоставляет более гибкие возможности для осуществления виртуализации.

Стоит отметить, что данная статья не претендует на полноту охвата всех доступных сегодня продуктов для реализации виртуализации - внимание было сконцентрировано только на свободных решениях. EOF

1. http://www.ibm.com/developerworks/ru/library/l-linuxvirt/index.html.
2. http://www.qemu.org/status.html.
3. http://www.virtualbox.org/wiki/Editions.
4. http://www.linux-kvm.org/page/Main_Page.
5. http://www.ibm.com/developerworks/ru/library/l-linux-kvm.

Рисунок 3. Интерфейс FAUmachine наделен кнопками Screenshot и Reset



Визитка

СЕРГЕЙ КРУТСКИХ, старший системный администратор компании «ИНФИН», занимается администрированием серверов, работающих под управлением Windows Server 2003, FiveBSD, openSuSe, OpenBSD

Виртуализируем предприятие

Чтобы заработала бргалтерия

Ожидания и уверения правительств разных стран в том, что кризис вот-вот закончится (или уже где-то закончился], как-то не укладываются в реальную ситуацию

Системный администратор, как собака: всё понимает, только сказать не может...

Из устного фольклора

Что делать, когда не знаешь, что делать?
А реальная ситуация такова: все ещё больше стали экономить на всем (даже правительство «ненавязчиво» предлагает всем нам дружно перейти на энергосберегающие лампочки), бюджеты ИТ-отделов, и не только, срезают, людей увольняют или отправляют в бессрочный неоплачиваемый отпуск пачками. Программы по обновлению и расширению компьютерного парка заморожены.

Самое интересное и парадоксальное в этой ситуации - работы для всех стало больше, и это, на мой взгляд, прямое следствие изменений в штатных расписаниях предприятий и организаций, но сейчас не об этом.

Как гласит одна поговорка: «Хороший начальник - это тот начальник, о котором вспоминают только в день зарплаты». Так вот, по моему мнению, про службу ИТ или про системного администратора (в зависимости от размера компании) вспоминают, когда что-то перестает работать или хочется уменьшить расходы за счет ИТ-отдела.

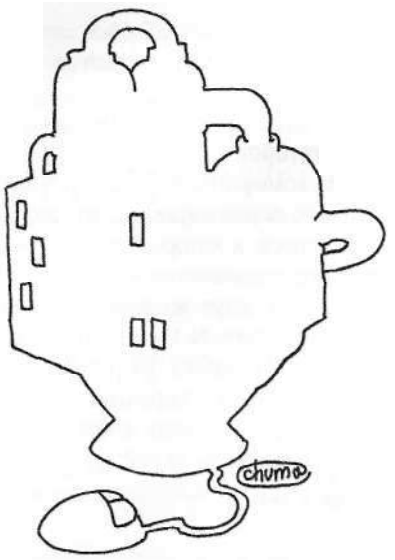
До сих пор существует мнение, что «они» - это что-"о среднее между завхозом, кладовщиком и электриком (уборщицей, поваром, охранником и т.п. - нужное подчеркнуть). Чем занимаются - непонятно, а значит, не очень нужны, и деньги давать им не стоит. Переломить эту позицию ,~ае^ся не всем. Приговор часто выглядит примерно так: '.'ы же в прошлом году новый сервер покупали, разве -егззя на нем бухгалтерию «крутить», сейчас денег нет...» .' -а-инаются долгие объяснения про то, что «новый сервер ~: -г.ˆ/ для контроллера домена, так как старый девяти-~е~-а/ разности, HP уже ну никак не справлялся - ни памя-" - *1 :•* эвого пространства», что «бухгалтерию в целях :аз:~асности необходимо выделить в отдельную подсеть, :: а- ;:аав :се^ствами коммутатора VLAN» и что им в этой сети необходим сервер баз данных. При этом умалчивая, что еще желательно DNS + DHCP. В итоге, как обычно, все остается по-прежнему за исключением того что «бухгалтерия должна работать!».

И вот в такой непростой ситуации для администратора вопрос, что делать, становится главным: отказаться от своих лучших побуждений - отделения бухгалтерской подсети от основной массы пользователей, тем самым защищая конфиденциальную информацию, или искать другие решения?

Недавно и мне пришлось искать решение подобной задачи, о чем и хочу рассказать. В общих чертах я уже обрисовал задачу, теперь уточню:

- Локальная сеть класса С на 60 рабочих мест (в основной массе Windows XP) - 192.168.1.0/24, состоящая из двух коммутаторов, к которым подключены все рабочие места пользователей и сервер. Деления на подсети нет.
- Необходимость трех сетевых хранилищ с разными правами доступа для подразделений - сетевые диски W, V, P.
- Контроллер домена AD + DHCP + DNS, сервер kdc.firma.ru.
- Корпоративный портал - portal.firma.ru.
- Необходимость ограничения сетевого доступа к компьютерам, используемым отделом бухгалтерии со стороны других отделов. Для чего предполагается разделение всей сети на две VLAN2 (для бухгалтерии) и VLAN1 (для всех остальных). На рис. 1 представлена схема сети, которую предполагается построить. Отдел бухгалтерии сейчас состоит из восьми рабочих мест и использует подключение к базе данных, расположенной на контроллере домена.
- В сети отдела бухгалтерии необходим сервер баз данных Adaptive Server Anywhere (ASA) 9-й или 10-й версии. Рабочая группа или домен с сервером buh.firma.ru для авторизации пользователей и желательно DNS + DHCP-серверы.

Имеющееся оборудование и лицензии на программное обеспечение:



Отказаться от отделения бухгалтерской подсети от основной массы пользователей **или искать другие решения?**

- Сервер - TYAN Thunder i7520/S5360 - 1 шт.
- Управляемый коммутатор №1 - 3Com Switch 4200G - 1 шт.
- Управляемый коммутатор №2 - 3Com Switch 430 - 1 шт.
- Лицензия Windows Server Standard Release 2 - 1 шт.
- Windows Server CAL2003 - 60 шт.
- Windows XP Professional Service Pack 3 - 60 шт.
- SQL Anywhere Studio 9.0 - 10 лицензий.

На сервере была развернута служба AD и все необходимые сервисы, а также сконфигурированы и настроены сетевые диски.

Все прекрасно, если бы не бухгалтерия. Где взять еще один сервер? Вспоминаю, что сервер поддерживает аппаратную виртуализацию, и принимаю решение виртуализировать. Вопрос только, на какой платформе. Начинаю перебирать: VMware Server, VirtualBox, Microsoft VirtualPC, Parallels Workstation, Xen, Hyper-V, Citrix XenServer, KVM.

VirtualBox, Microsoft VirtualPC, Parallels Workstation - сразу отвергаю как платформы, в основном «заточенные» для рабочих станций, а VirtualBox 3.0 еще и сыроват - проблемы с виртуализацией сети. VMware Server и Hyper-V отпадает из-за платности.

В чистом остатке - Xen, Citrix XenServer, KVM. С Xen и Citrix XenServer я уже давно имел дело, поэтому свой выбор остановил на них, а вот KVM решил не рассматривать в связи с тем, что с ней пока не работал.

Подготовка

В начале мая 2009 года компанией Citrix Systems был анонсирован Citrix XenServer 5.5.0, который основан на третьей ветке Xen. Сейчас он доступен для загрузки по адресу http://www.citrix.com/lang/English/lp/lp_1688615.asp. Также нам понадобится ISO-образ с драйверами для Windows и Linux-гостевых систем Linux Guest Support и XenCenter, которые тоже доступны для загрузки с этой страницы.

Как контроллер домена DHCP и DNS для сети бухгалтерии (buh.firma.ru) будем использовать openSUSE 11.1 Скачиваем по адресу http://download.opensuse.Org/distribution/11.1/

Рисунок 1. Схема сети после модернизации

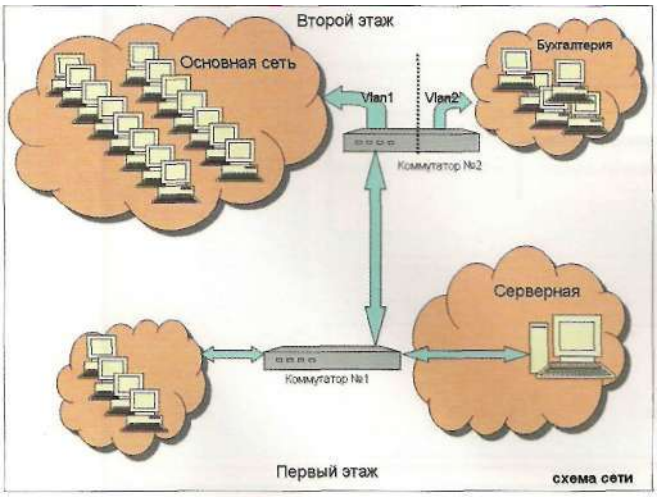
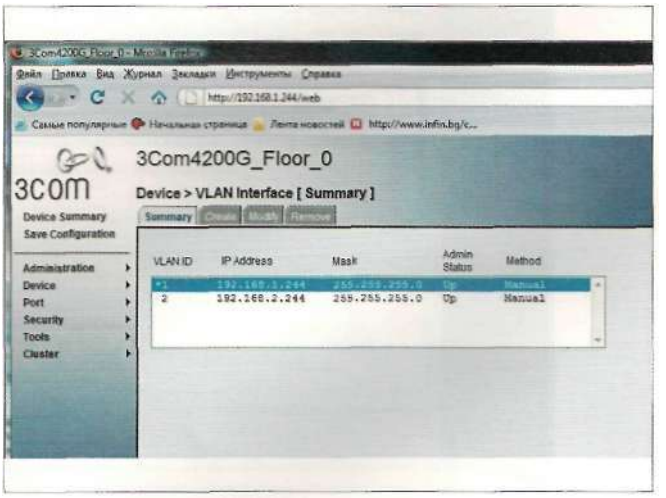


Рисунок 2. Две подсети в коммутаторе



iso/openSUSE-11.1-DVD-x86_64.iso. Мне эта ОС нравится за немецкое качество и замечательный инструмент настройки и конфигурирования Yast.

Для переноса физического сервера в виртуальную среду Citrix Systems рекомендует воспользоваться утилитой XenConvert 2.0.2, которую можно скачать по адресу http://citrix.com/English/ss/downloads/results. asp?productID=683148. Но воспользоваться ею можно, только если в вашей сети уже есть установленный Citrix XenServer.

Ещё один минус, который был обнаружен - утилита не в состоянии скопировать блокированные системой DAT-файлы AD с работающего сервера. И, как следствие, мы можем с ее помощью получить неработающий контроллер AD.

В связи с этим было принято более сложное решение - установить уже в виртуальной машине сервер, а затем восстановить резервную копию AD. Минус решения - пришлось устанавливать все необходимые программы заново и делать некоторые настройки. Плюс - система чиста от ненужных теперь драйверов физических устройств.

Еще один вариант: использовать Acronis True Image для создания vdi-образа, а затем этот образ импортировать в Citrix XenServer (для такого решения удобно использовать Live CD - Yurkesha BartPE, который можно скачать по адресу http://yurkesha.seclorum.ru/main_ru.html).

Были еще несколько вариантов, но все они занимают примерно одно и то же время и одинаковы по трудоемкости. В конкретной ситуации для меня оказалось проще так.

Все работы были запланированы на субботу, поэтому к окончанию работы в пятницу был сделан бэкап всех данных сервера на внешний жесткий диск емкостью 1 Тб. Затем на этот жесткий диск копируем в корень ISO-образы Windows Server 2003 R2, openSUSE 11.1, Linux Guest Support и Yurkesha BartPE, они нам понадобятся для установки виртуальных систем.

Настройка коммутаторов

Создаем на обоих коммутаторах подсеть VLAN1. Добавляем в эту подсеть все порты первого и второго коммутатора за исключением портов, к которым подсоединены компьютеры бухгалтерского отдела.

Свичи подключены друг к другу по порту 1 Гбит (свитч №2 - 49 порт и свитч №1 - 3 порт), поэтому для проброса тегированного трафика их необходимо добавить в сеть VLAN2 и тегировать трафик на порту первого свича, к которому подключен сервер, в моем случае порт №4. Для этого подключаемся к свичу №2:

```
#  telnet 192.168.1.242
```

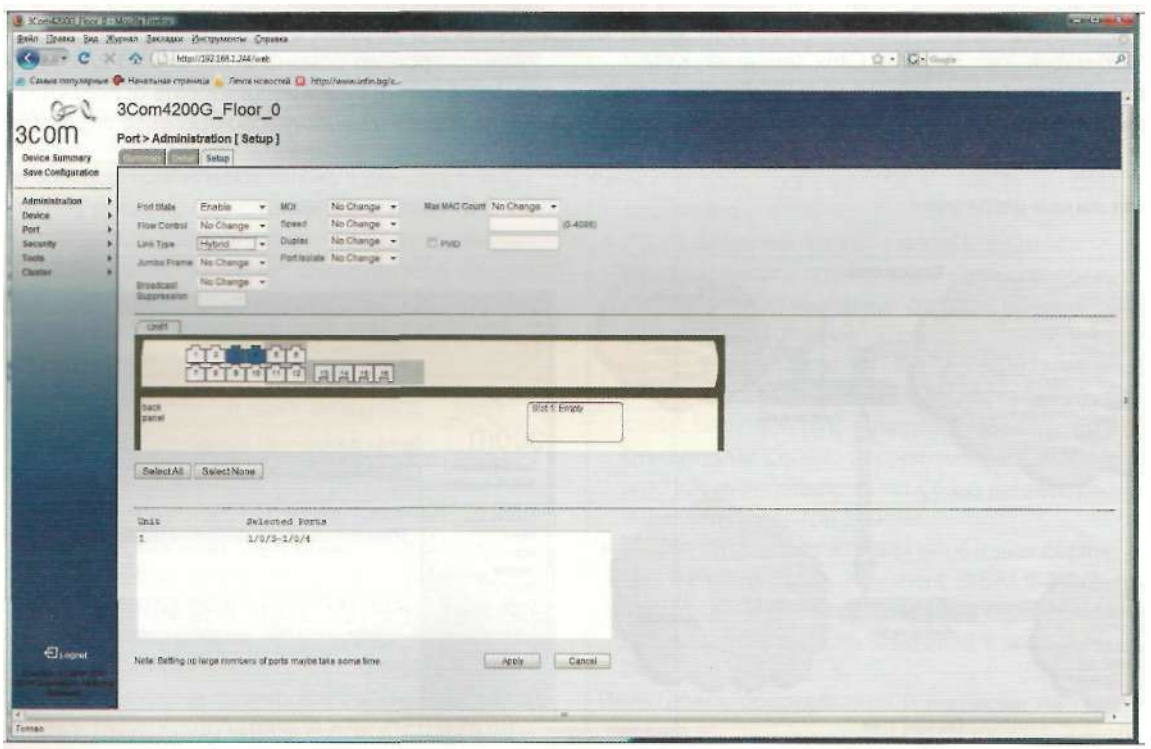
Вводим логин и пароль, переходим в меню bridge, а затем в меню vlan:

```
----------------------3Com Switch (1)----------------------
Select menu option: bridge
Menu options: --------3Com SuperStack 3 Switch 4300--------
vlan                - Administer VLANs
Type "q" to return to previous menu or ? for help.
----------------------3Com Switch (1)----------------------
Select menu option (bridge): vlan
```

Выбираем создать VLAN (create), вводим номер VLAN - 2 и имя:

```
Select menu option (bridge/vlan): create
Select VLAN ID (2-2048): 2
Enter VLAN name [VLAN 2]: Buh
```

Рисунок 3. Подготавливаем тегированные порты



После этого при помощи modify добавляем необходимые порты в подсеть VLAN2:

```
----------------------3Com Switch (1)----------------------
Select menu option (bridge/vlan): modify
----------------------3Com Switch (1)----------------------
Select menu option (bridge/vlan/modify): addPort
Select VLAN ID (1-2)[1]: 2
Select bridge port (1-49,all)[all]: 49
```

По окончании добавления портов в подсеть VLAN2 на втором свиче должно получиться что-то вроде этого:

```
Select menu option (bridge/vlan): detail
Select VLAN ID (1-2)[1]: 2
VLAN ID: 2          Name: Buh
Unit     Untagged Member Ports          Tagged Member Ports
-------------------------------------------------------------
1              42-48                                  49
Select menu option (bridge/vlan):
```

Здесь порты с 42 по 48 - это и есть подсеть бухгалтерии, они подключены только в VLAN2. С этим коммутатором все. На свиче №1 добавляем VLAN2. Порты, которые необходимо включить в эту сеть (порт 3, идущий из свича №2, и порт 4, который подключен к серверу виртуальных машин), переводим в режим hibrid, а затем добавляем их в VLAN2. Все эти действия достаточно удобно производить через веб-управление. В итоге должна получиться такая картина, как показана на рис. 2, 3, 4.

Подключаем сетевые интерфейсы сервера соответственно eth0 в любой порт, а eth1 в порт 3, который «смотрит» в VLAN2 (см. рис. 4).

Объясню, почему нельзя было подсоединить сразу во второй свитч, он просто банально находится не в серверной, а на другом этаже, и к нему подключены не только машины бухгалтерии, но и основная масса остальных рабочих станций.

Устанавливаем Citrix XenServer, при установке не забываем указать «Установить xen-tools» и задать для eth0 IP-адрес в диапазоне первой (существующей) сети VLAN1. По окончании установки и перезагрузке проверяем в консольном меню IP-адрес и остальные параметры конфигурации сервера. Если все в порядке, то можем переходить к своему рабочему месту.

Все остальные операции будем производить удаленно с помощью XenCenter. Инсталлируем на рабочем компьютере администратора XenCenter и подключаемся к серверу по указанному при установке IP-адресу (см. рис. 5).

Подключаем внешний диск к машине администратора и расшариваем для доступа на чтение весь диск под именем iso или как кому нравится. Вызываем вкладку New Storage в XenCenter, создаем репозиторий типа ISO library - Windows File Sharing (CIFS) и жмем Next (см. рис. 6).

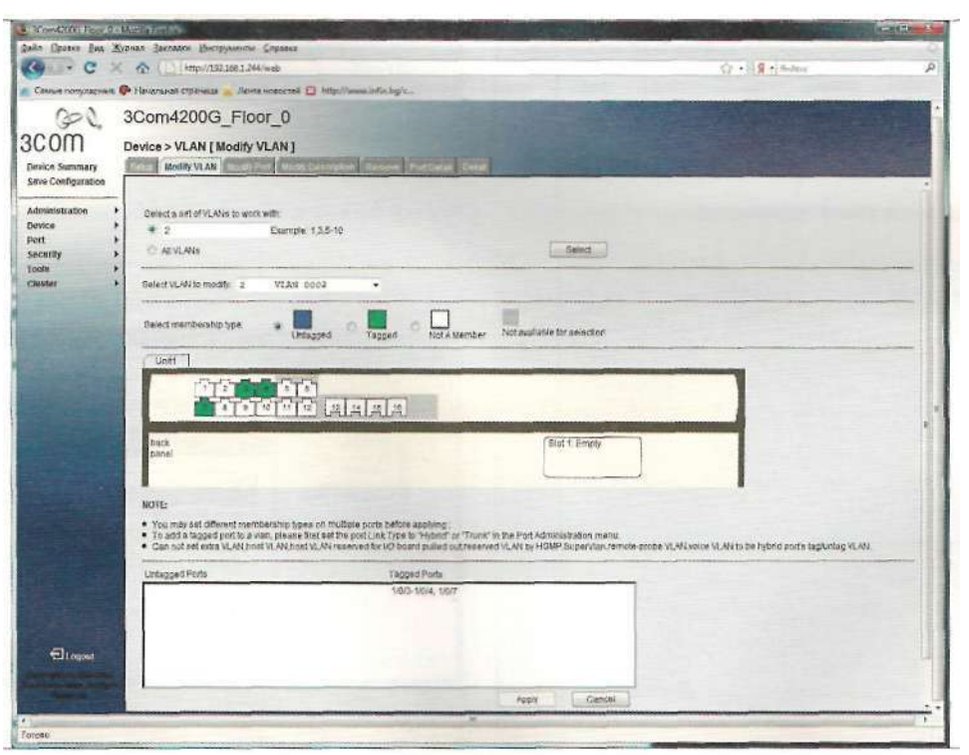
На следующей вкладке указываем IP-адрес машины администратора, название директории, имя и пароль пользователя для подключения и жмем Finish (см. рис. 7).

Теперь в центре управления должен появиться локальный ISO-репозиторий, содержащий дистрибутивы (см. рис. 8), используя который будем создавать виртуальные машины.

Создаём виртуальную машину, выбрав шаблон Windows 2003-32, подключив ISO-образ дистрибутива и изменив размер локального диска по своему усмотрению. Я посчитал, что для моей системы для диска «C» вполне хватит 30 Гб. Остальные диски для рабочих групп добавим и настроим позже.

Затем переключаемся на вкладку Console виртуальной машины и выполняем установку системы. По окончании

Рисунок 4. Зеленые порты тегированы тегом 2 (VLAN002)



установки выбираем из раскрывающегося списка в качестве DVD Drive образ xs-tools.iso и устанавливаем драйвера системы для улучшенной поддержки виртуальной машины.

Перегружаемся и добавляем роли dhcp и dns, не настраивая, затем выполняем восстановление AD. Операция восстановления или создания контроллера домена из резервной копии подробно описана на сайте microsoft.com, а также на многих сайтах в Интернете. Потому не буду подробно останавливаться на этом вопросе. Перегружаем сервер, проверяем работу служб, затем выключаем.

Виртуальный коммутатор в Citrix XenServer позволяет создавать виртуальные сети VLAN. С помощью XenCenter делать это одно удовольствие.

Заходим на вкладку меню Network. Отмечаем тип External Network, указываем имя сети - Buh, выбираем физический интерфейс (NIC), указывая на ту сетевую карту (в нашем случае eth1), которая смотрит в тегированный порт, и назначаем ей VLAN, равный 2 (см. рис. 9).

Вот и все! Теперь у нас есть виртуальный сетевой адаптер, который видит только сеть VLAN2. Его и используем при создании виртуальной машины для бухгалтерии.

В стандартных шаблонах XenCenter нет openSUSE 11.1 - выбираем SUSE Linux Enterprise Server 11 x64 или создаем конфигурацию сами, как кому нравится, исключение составляет только размер виртуального диска, нам понадобится не меньше 30 Гб (20 Гб под базы данных и бэкапы и 10 Гб под систему, по умолчанию - всего 8 Гб).

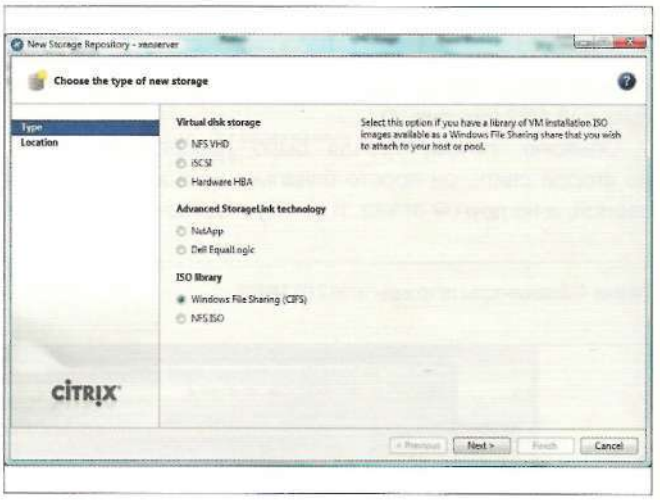
Установка openSUSE 11.1 описана много раз и не представляет никакой сложности, поэтому не будем на ней подробно останавливаться, за исключением нескольких моментов.

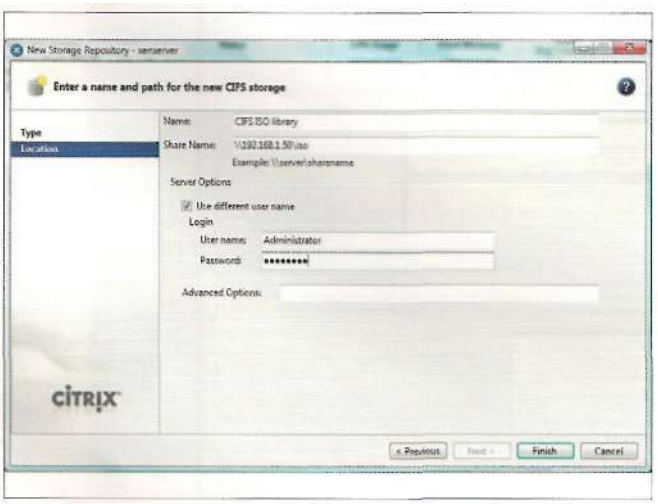
При стандартном автоматическом разбиении дискового пространства утилита установки предложит создать отдельные разделы для корня файловой системы, папки home и диска подкачки swap.

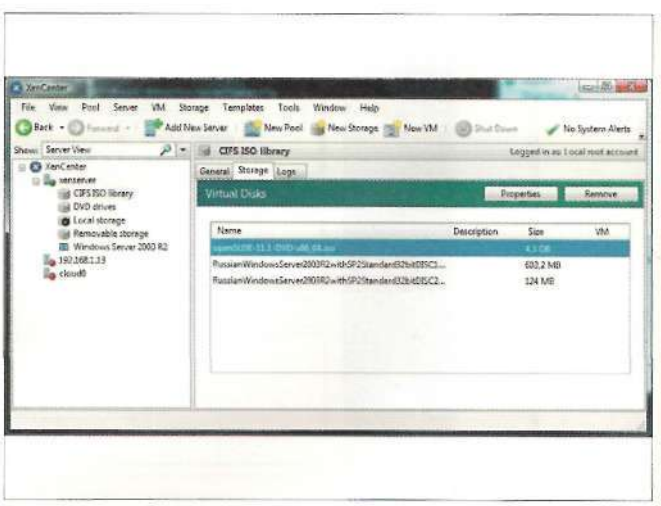
Я, исходя из собственного опыта, предпочитаю создавать разметку для openSUSE 11.1 на основе LVM приблизительно с такими параметрами: 1-2 Гб - под swap, 30-70 Мб - для boot, 8-10 Гб - для /, остальное распределяю между /srv и /var. Я не претендую на то, что это лучший вариант, просто мне так удобней, у вас может быть все по вашему желанию.

Рисунок 5. Подключение к Citrix XenServer

Рисунок 6. Добавление ISO-репозитория







Важное преимущество при использовании LVM - возможность в любой момент добавить еще один физический том в любую группу томов, а также свободно менять размеры разделов. Причем все операции можно производить «на горячую», не останавливая работы сервера. Такой вариант разметки очень удобен для виртуальной машины - когда возникнет необходимость, всегда можно увеличить размер дискового пространства любого раздела.

При выборе устанавливаемого программного обеспечения обязательно отмечаем для установки:

- файловый сервер;
- сервер DHCP;
- сервер DNS.

Устанавливать или нет графику - это решать вам, но мое мнение, что с Yast-ом быстрее и удобнее работать при помощи мыши, хотя все действия можно выполнять с помощью функциональных клавиш, <TAB> и <Shift>. Для серверов можно ограничиться минимальным набором «графики» XFCE.

Также на время настройки сразу при установке советую отключить файервол.

По окончании установки и перезагрузке выполняем установку xs-tools.iso, подключив в DVD xen-tools. Для этого проверяем существование устройства командой;

```
fdisk -l
```

затем монтируем найденное устройство и запускаем скрипт установки install.sh (см. рис. 10).

Если в вашей версии скрипт завершится с ошибкой, то просто установите соответствующий ргрл-пакет:

```
rpm -ivh xe-guest-utilities-5.5.0-458.x86_64.rpm
```

После установки обязательно требуется перезагрузка системы.

Имя сервера устанавливаем buh, домен firma.ru. В настройках сетевой карты присваиваем статический IP-адрес 192.168.2.1 и переходим к настройкам DNS. Создаем с помощью Yast прямую firma.ru и обратную 2.168.192.in-addr.arpa зоны. Добавляем NS- и A-записи, указывающие на сервер 192.168.2.1 с именем buh. Не забываем указать или заново создать TSIG Key для дальнейшего динамического обновления с помощью DHCP. Сохраняем настройки.

Заходим в настройку DHCP, задаем диапазон раздаваемых адресов и обязательно указываем синхронизировать данные с DNS-сервером. При выборе этой опции Yast предложит автоматически или в режиме мастера создать (модифицировать) DNS-зону - смело соглашайтесь.

Выбираем расширенную конфигурацию, затем необходимую зону и в ней управление динамическим DNS (Configured Declarations -> Subnet -» Edit -> Dynamic DNS), включаем динамическое обновление, указываем TSIG Key для зон и их название, жмем Save.

Перезапускаем серверы. Все, связка DHCP + DNS настроена. Перед дальнейшей настройкой желательно проверить их работу, включив любой компьютер из VLAN2, и убедиться, что IP-адрес и имя компьютера появятся в DNS и будут резол виться.

Переходим в Yast на вкладку Network Services и справа выбираем закладку Samba Server. На вопрос о типе выбираем контроллер домена и заполняем необходимые поля, здесь же можно включить Wins для поддержки старых систем. Запоминаем пароль суперпользователя root на Samba - с его помощью будем добавлять компьютеры в рабочую группу, и сохраняем настройки (см. рис. 11).

В стандартной конфигурации Samba профили пользователей Windows хранятся на сервере, нам это не нужно, поэтому сразу правим файл /etc/samba/smb.conf.

Строку:

```
logon home= \\%L\%U\.9xprofile
```

меняем на:

```
logon home= ''
```

Строку:

```
logon path =...
```

комментируем.

В строке:

```
logon scrip = start.bat
```

Рисунок 9. Создание тегированного сетевого интерфейса

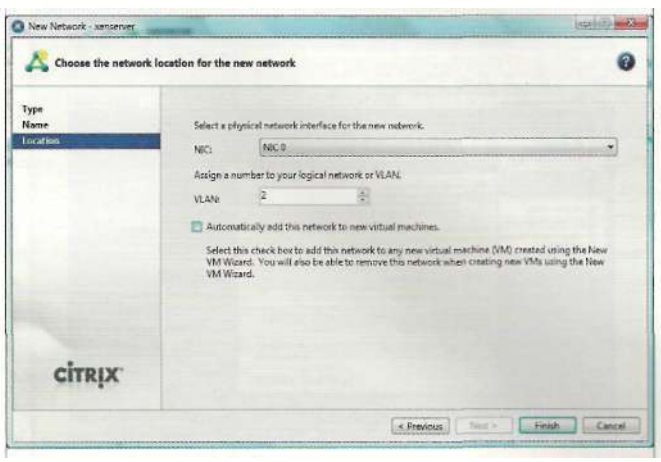
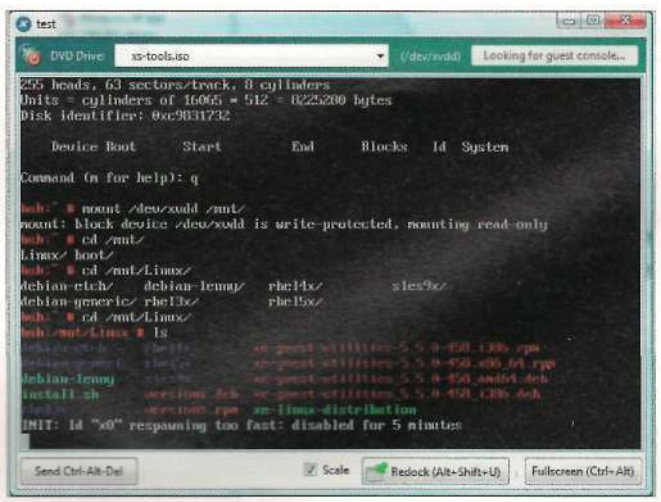


Рисунок 10. Установка xen-tools на гостевую машину



указываем имя файла, который будет запускаться при старте системы. Этот файл должен располагаться в каталоге: /var/lib/samba/netlogon. У меня он просто монтирует общий для всех пользователей каталог и содержит:

```
net use W: \\buh\distrib
```

Для осуществления желаемого необходимо создать папку/HOME/distrib. Выставить на нее права:

```
chmod 755 /home/distrib
```

и изменить группу владельцев на нее:

```
chown -R root:users /home/distrib
```

В файле /etc/samba/smb.conf этот каталог описываем как общий для чтения и доступный всем группам и пользователям, за что отвечает директива public:

```
# Описываем шары
[distrib]
   comment = all users share
   path = /home/distrib
   public = yes
   writable = yes
   valid users = firma.ru\users
   create mask = 0744
```

В такой конфигурации подразумевается, что ограничения прав записи на файловую систему не дадут простым пользователям изменять или записывать файлы, а администратор домена всегда сможет изменить любой файл или каталог.

Сейчас Samba имеет огромное количество параметров настройки, таких как выполнение скриптов загрузки, динамические изменения в реестре, установка и публикация принтеров, поддержка расширенных прав на файловую систему и т.д. Если хотите быть в курсе последних изменений, стоит заново перечитать документацию на нее.

Добавление пользователей происходит в два этапа. Сначала добавляем через Yast - «Управление пользователями» всех пользователей сети «Бухгалтерия», а затем, запуская из командной строки скрипт:

```
smbpasswd <имя пользователя>
```

который создает пары логин-пароль в файле /etc/samba/smbpasswd, в нем также можно прописать дополнительные алиасы имен пользователей. Компьютеры в домен добавляем как обычно, за исключением использования логина администратора, вместо него используем root, как показано на рис. 12. Из консоли XenCenter запускаем первый сервер kdc.firma.ru. На этом основная настройка окончена.

Осталось создать и добавить дополнительные диски для групп пользователей, а также назначить им права. Скопировать данные с переносного жесткого диска. Установить на сервер бухгалтерии SQL Anywhere Studio для Linux и запустить на нем базу данных бухгалтерии. Подключить принтер к серверу бухгалтерии, и можно работать.

***

Модифицировать и развивать эту конфигурацию очень просто. Можно легко создавать полные резервные копии установленных серверов. В любой момент делать снимки состояния систем. Создать и скопировать на внешний носитель шаблоны работающих систем для быстрой установки ОС, на которых можно отрепетировать определенные критические действия, такие как установка сервис-паков и т.п. Все ограничено только вашей фантазией, а простор для экспериментов открывается огромный. Удачи, буду рад вопросам и отзывам на форуме журнала по адресу www.samag.ru/forum. EOF

1. Installation Guide - http://www.citrix.com/lang/English/lp/lp_1688622.asp#top.
2. Virtual Machine Guide - http://www.citrix.com/lang/English/lp/lp_1688622.asp#top.
3. Reference Manual - http://www.citrix.com/lang/English/lp/lp_1688622.asp#top.
4. openSUSE 11.1 Reference Guide - http://www.novell.com/documentation/opensusel 11/pdfdoc/opensuse11 preference/opensusel 11_reference.pdf.
5. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2003. СПб. : БХВ-Петербург, 2006.
6. Samba-3 by Example - http://us1.samba.org/samba/docs/man/Samba-Guide.

Рисунок 11. Создание рабочей группы с помощью Yast

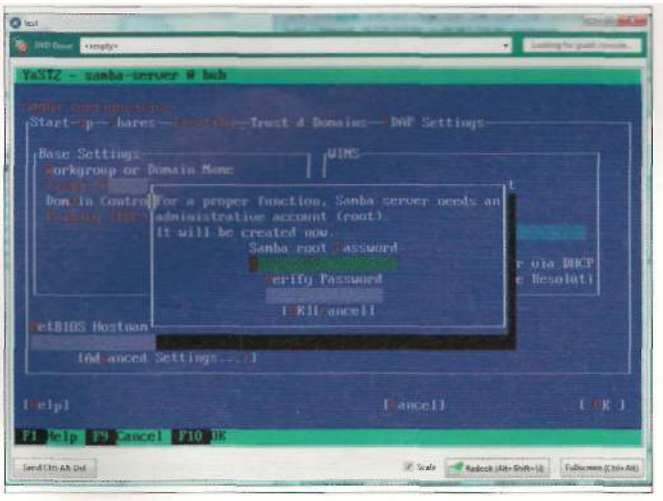
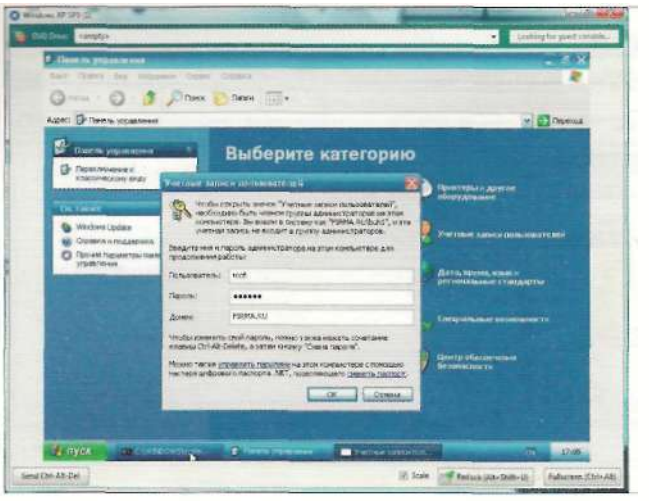


Рисунок 12. Ввод машины в рабочую группу



МИХАИЛ ФИЛИППЕНКО, выпускник Южно-Российского государственного технического университета. Сооснователь и генеральный директор компании Fast Reports

FastReport Server 2.2

Построй свой собственный SaaS

Организация работы распределённого офиса - задача актуальная, однако новая и трудная

Как создать работающую систему информационного взаимодействия. Перед системным администратором возникают следующие проблемы:

- Обеспечение оперативного доступа к актуальной информации в соответствии с уровнем компетенции сотрудника. Например, вашему коллеге на другом континенте важно знать, как идут дела в головном офисе, чтобы проконсультировать клиентов.
- Необходимость поддержки актуального программного обеспечения и новых шаблонов на всех рабочих местах. К примеру, обновить корпоративную систему отчётности на двух тысячах персональных компьютеров коллег по всему миру за одну ночь - это страшный сон для любого системного администратора.
- Защита канала передачи данных.

Будет неверно говорить, что все эти проблемы легко решаемы, тем не менее относительно недавно была сформулирована концепция SaaS (Soft as a Service - программное обеспечение как услуга), позволяющая развернуть решение этих задач в новом ключе. Идеология SaaS не предполагает владения конечным пользователем чем-то большим, чем интернет-браузер и умение обращаться с ним:

- Всё программное обеспечение находится на централизованном компьютере. Таким образом, персоналу достаточно иметь хоть какой-то веб-браузер.
- Сотрудники всегда работают с актуальной версией как программного обеспечения, так и данных,
- Более того, сами данные не передаются, а передаётся только результат их обработки.

Таким образом, отпадает необходимость в первоначальном централизованном долгом и трудоёмком внедрении, а также постоянной поддержке актуальности программного обеспечения одновременно на многих рабочих местах. Также плюсами такого подхода являются низкие требования к каналам передачи данных и к конечному оборудованию как таковому. Следует также отметить возможность централизованного управления доступом к корпоративным документам.

За использование стороннего SaaS-решения приводится и такой дополнительный аргумент, как оплата только за использование по числу рабочих мест.

Минус SaaS - психологически далеко не все готовы отдавать обработку своей собственной внутрикорпоративной информации сторонним сервисам. И это касается не только и не столько самих сервисов, сколько защищённости каналов передачи данных сервису.

Компания Fast Reports представляет новую версию своего решения для создания системы корпоративной отчётности FastReport Server 2.2 как внутри предприятия, так и в качестве элемента SaaS-платформы. Причём в случае внутрикорпоративного использования компании-пользователю не придётся платить арендную плату за количество подключаемых пользователей или, что заставляет некоторых потенциальных клиентов относиться к Saas настороженно, отдавать внутрикорпоративные данные «на сторону» и беспокоиться о внешнем канале передачи данных - сервер баз данных не может никоим образом отдавать информацию «наружу» - будет виден только результат и только зарегистрированным пользователям.

Возможна совместная работа с уже работающими веб-серверами IIS и Apache с помощью идущего в комплекте с FastReport Server CGI-приложения или в качестве ISAPI-модуля. Применение последнего вообще делает запуск службы собственного сервера ненужной - вся функциональность сервера отчетов сосредоточена в ISAPI DLL. Все настройки сервера хранятся в xml-файле. снабжены комментариями и могут быть изменены с помощью программы-конфигуратора только администратором системы. Особо стоит отметить возможность FastReport Server создавать несколько подключений к базам данных в одном отчете и собирать информацию из разных источников данных.

Использование встроенной в MS Windows аутентификации даёт возможность тесной интеграции в домены Active Directory и упрощает управление учётными записями и группами пользователей - каждой группе пользователей назначаются отчёты, нужные именно этой группе: руководству - одни, бухгалтерии - другие. И каждый пользователь может быть абсолютно спокоен за актуальность получаемой информации - отчёт будет сформирован по его запросу именно в тот момент, когда понадобится.

Fast Reports предлагает вам построить свой собственный SaaS! EOF

Визитка

ИГОРЬ АНТОНОВ, профессиональный программист. Автор множества статей в журналах «IT-Спец» и «Хакер». В настоящее время работает начальником отдела разработки программного обеспечения в компании ОАО «ЦальЖАСО»

Возможности VMBitrix

Разгадка виртуальной машины

Сегодня все больше компаний делают выбор в пользу виртуализации, нежели увеличения парка аппаратных машин. И на это есть объективные причины

Управлять и поддерживать виртуальные машины гораздо проще, и стоить это будет значительно дешевле, чем приобретение оборудования. На этом преимущества виртуальных машин не заканчиваются. Итак, вперед, в виртуальную реальность!

VMBitrix - виртуальная машина от«1С-Битрикс»

Не так давно линейка продуктов компании «1С-Битрикс» пополнилась интересной новинкой - VMBitrix. Данный продукт представляет собой полностью сконфигурированный и готовый к работе веб-сервер. Основными его преимуществами являются наличие всех необходимых веб-разработчику серверных компонентов, быстрое развертывание виртуальной машины, наиболее оптимальные настройки всех компонентов и моментальная готовность к работе. VMBitrix - не просто очередное решение для быстрой установки WAMP/LAMP-сервера. Это возможность почувствовать себя «хостером», в распоряжении которого полноценный виртуальный сервер, работающий под управлением Linux и напичканный всем необходимым серверным программным обеспечением.

Как это выглядит?

VMBitrix - это образ виртуальной машины, созданный с помощью программы виртуализации от VMware. Для того чтобы приступить к его использованию требуется зайти на официальный сайт компании [1] и скачать образ виртуальной машины. После завершения загрузки от вас также потребуется загрузить VMPlayer (см. рис. 1) - «плеер» виртуальных машин и открыть в нем загруженный образ. После выполнения последнего действия начнутся загрузка виртуальной машины и старт всех демонов (nginx, MySQL и т.д.). Для продолжения работы вам потребуется вбить IP-адрес виртуальной машины в адресной строке своего браузера и приступить к работе (либо к конфигурированию, либо к установке «1С-Битрикс»).

Главное - производительность

Все компоненты, входящие в состав виртуальной машины, максимально оптимизированы и сконфигурированы для комфортной работы. Системных ресурсов для корректного функционирования виртуальной машины требуется минимум. Например, если говорить об оперативной памяти, то из host-системы зарезервируется 256 Мб. Сравнив работу PHP-сценариев в VMBitrix и в win-окружении хостовой машины, получили, что в VMBitrix на выполнение тратится меньше времени (в качестве скриптов использовались система управления контентом «1С-Битрикс» и бесплатный фреймворк -Drupal).

Как еще можно использовать VMBitrix

На VMBitrix возможно возложить ряд задач и придумать десятки способов его применения. Например, использовать его в качестве полигона для разработки и тестирования собственных веб-приложений/сервисов.

На развертывание и запуск системы требуется очень мало времени и системных ресурсов. Ее запросто смогут использовать разработчики, работающие на ноутбуках, - производительности хватит.

Достоинства и недостатки

Главные плюсы:

Сокращение финансовых затрат. Использование виртуальной инфраструктуры, позволяет сэкономить на покупке нового оборудования. Например, вам требуется развернуть несколько серверных приложений. Представим, что часть этих приложений предназначена для работы на UNIX-like-платформах, а другая - на Windows. Если предполагается, что на эти приложения будет приходиться большая нагрузка, то скорее всего воспользоваться виртуализацией вам будет невыгодно. Если же нет, то ситуация меняется с точностью наоборот. В этом случае проще и выгоднее приобрести один производительный сервер и развернуть на нем несколько виртуальных машин с нужными операционными системами. В итоге у вас получится один физический сервер, а в вашей виртуальной сети будет видно несколько отдельных серверов.

Более легкая техническая под- Сбоям всегда есть место. Последствия этого могут быть самыми разными. Одним из главных

будет время простоя. Представим себе, что на вашем сервере вышла из строя материнская плата. ОС обычно тяжело переживают такие ситуации, и есть большая вероятность, что ее придется полностью переустанавливать. Если дело в одной ОС, но мы же помним, что у нас хитрым способом настроена куча сервисов, переподнятие которых с нуля займет много времени. Ситуация не из приятных. Особенно если из резервных копий есть только бэкапы данных, а не настроек. В случае использования виртуальных машин развитие событий может происходить по-другому. Как? Позаботившись о резервных копиях виртуальных машин, в случае краха вам потребуется лишь установить ОС на сервер, а после развернуть программу для работы с виртуальными машинами. И все! Подсовываем ей бэкапы ОС и стартуем. Пара минут, и все работает в прежнем состоянии. Даже если конфигурация (в железном плане) вашего нового сервера полностью изменилась, виртуальной машине все равно.

Сверхбыстрое развертывание. Это один из самых важных плюсов виртуальных машин. Представим, что нам нужно открыть новый филиал компании. Сосредоточим внимание на информационной инфраструктуре. Развернуть все сервисы, которые функционируют в головном офисе, можно будет за считанные минуты. Весь процесс развертывания будет сводиться к переносу файлов с виртуальными машинами и запуску программы, отвечающей за виртуализацию. Никаких лишних настроек. Никаких рутинных действий. Все будет работать так же, как вы и настроили. Добавим к этому, что присутствие высококвалифицированного специалиста не требуется, и выгода становится более чем очевидной.

Полный контроль **над** ресурсами. Например, у вас установлен сервис, который потребляет малое количество системных ресурсов, в то время как сервис на другом сервере работает как папа Карло и с жадностью глотает каждый мегабайт памяти. Теоретически обе эти службы возможно установить на одном компьютере и ограничить им ресурсы. Например, наиболее активной выделить побольше Мгц процессора и памяти, а вторую ограничить. Тогда обоим сервисам будет хорошо, а у вас освободится один компьютер. Разве не здорово? Решить эту задачу опять же можно с помощью виртуализации.

Виртуальная машина - полигон для опытов. Требуется проверить работу разрабатываемого продукта на разных платформах? Убедиться в корректности и работоспособности свеженького пакета заплаток? Презентовать клиенту проект (web, сетевые сервисы и т.д.)? Для всех этих и многих других схожих задач использование виртуальных машин окажется более чем предпочтительно. На развертывание виртуальных машин много времени не нужно и после запуска они будут выглядеть так, как вы их настроили. Так почему бы не воспользоваться этой простотой и мощью в целях тестирования и банальной презентации?

У виртуализации есть свои минусы. Эдин из таких минусов - общее снижение надежности всей виртуальной инфраструктуры. Например, не стоит 100% полагаться на виртуальные машины и вешать все сервисы на один физический сервер (путем разворачивания нескольких виртуальных машин). Особенно, если от работоспособности виртуальных сервисов зависит общее функционирование всей сети. Так что скорей всего это даже не минус, а требование, о котором не стоит забывать.

VMBitrix - это

- Операционная система Ubuntu Linux 8.04.
- Двухуровневая конфигурация NGINX + Zend Server CE.
- СУБД MySQL 5 (поддержка InnoDB).
- Настроенный файервол.
- Поддержка протокола https.
- Почтовый клиент msmtp.
- Автоматизация производительности.

***

Компания «1С-Битрикс» представила удобный продукт, позволяющий развернуть полноценный виртуальный и готовый к работе веб-сервер. Их разработка пригодится не только пользователям, остановившись на системе управления контентом «1С-Битрикс», а всем веб-разработчикам.

Дистрибутив VMBitrix распространяется совершенно бесплатно. Для тех, кто оценит преимущество использования виртуальных машин, компания «1С-Битрикс» готова предложить вариант аренды виртуальной машины на серверах хостера. Удачи вам в ваших виртуальных исследованиях! EOF

1. http://www.1c-bitrix.ru - официальный сайт компании «1С-Битрикс». Описание, демонстрационные версии продуктов и т.д.

Рисунок 1. Загрузка виртуальной машины

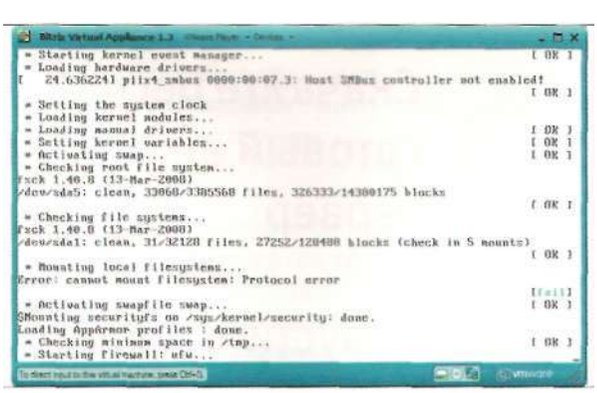
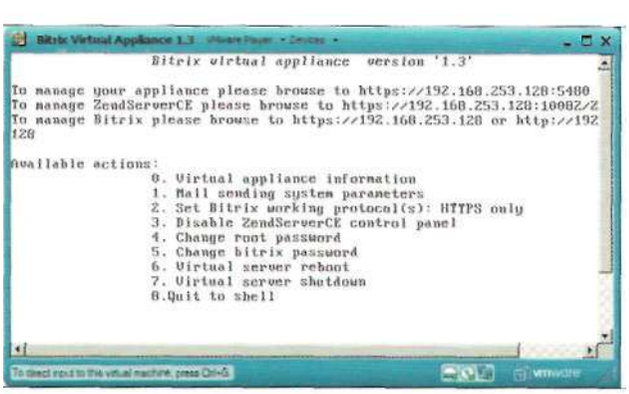


Рисунок 2. Основные функции управления



Уязвимость при обработке SiP-пакетов в Cisco Unified Communications Manager

Программа: Cisco Unified Communications Manager 5.x версии до 5.1(3g); Cisco Unified Communications Manager 6.x версии до 6.1 (4); Cisco Unified Communications Manager 7.0.x версии до 7.0(2a)su1; Cisco Unified Communications Manager 7.1.x версии до 7.1(2).

Опасность: Средняя.

Наличие эксплоита: Нет

Описание: Уязвимость существует из-за ошибки в реализации SIP. Удаленный пользователь может с помощью специально сформированных SIP-пакетов вызвать перезагрузку главного Cisco Unified Communications Manager-процесса.

URL производителя: www.cisco.com.

Решение: Установите последнюю версию с сайта производителя.

Разыменование нулевого указателя в Devfs и VFS в FreeBSD

Программа: FreeBSD версии 6.3, 6.4, 7.1, 7.2.

Опасность: Средняя.

Наличие эксплоита: Нет.

Описание: Уязвимость существует из-за ошибки разыменования нулевого указателя вследствие ошибки состояния операции при работе devfs и VFS. Локальный пользователь может выполнить произвольный код на системе с привилегиями ядра.

Примечание: Производитель выпустил дополнение, которое не позволяет эксплуатацию уязвимостей разыменования нулевого указателя.

URL производителя: www.freebsd.org.

Решение: Установите исправление с сайта производителя.

Спуфинг-атака в Windows CryptoAPi

Программа: Microsoft Windows 2000; Microsoft Windows XP; Microsoft Windows 2003; Microsoft Windows Vista; Microsoft Windows 2008; Microsoft Windows 7.

Опасность: Средняя.

Наличие эксплоита: Нет.

Описание: 1. Уязвимость существует из-за ошибки при обработке ASN.1-данных в X.509-сертификатах. Удаленный пользователь может с помощью нулевого байта в поле Common Name подменить доверенный сертификат.

2. Целочисленное переполнение обнаружено при обработке идентификаторов ASN.1 объектов в X.509-сертификатах, Удаленный пользователь может с помощью специально сформированного Object Identifiers (OID) подменить доверенный сертификат.

URL производителя: www.microsft.com.

Решение: Установите исправление с сайта производителя.

Множественные уязвимости в VMware Fusion

Программа: VMware Fusion 2.0.5 и более ранние версии.

Опасность: Низкая.

Наличие эксплоита: Нет

Описание: 1. Уязвимость существует из-за неизвестной ошибки в расширении ядра vmx86. Локальный пользователь может выполнить произвольный код на системе в контексте основной ОС.

2. Целочисленное переполнение обнаружено в расширении ядра vmx86. Локальный пользователь может вызвать отказ в обслуживании.

URL производителя: www.vmware.com/products/fusion.

Решение: Установите последнюю версию 2.0.6 build 196839 с сайта производителя.

Множественные уязвимости в IBM 0B2

Программа: IBM DB2 **9.x.**

Опасность: Низкая.

Наличие эксплоита: Нет

Описание: 1. Уязвимость существует из-за неизвестной ошибки, которая позволяет вставить, изменить и удалить строки, не имея необходимых привилегий. Уязвимость распространяется на версии DB2 9.1 до FP8 и DB2 9.5 до FP4. -

2. Уязвимость существует из-за неизвестной ошибки, относящейся к таблице функций. Уязвимость распространяется на версии DB2 9.1 до FP8 и DB2 9.5 до FP4.

3. Уязвимость существует из-за ошибки при обработке команды SET SESSION AUTHORIZATION. Злоумышленник может выполнить запрос не имея необходимых привилегий. Уязвимость существует в версии DB2 9.1 до FP8.

URL производителя: www-306.ibm.com/software/data/db2/9.

Решение: Установите последнюю версию DB2 9.1 FP8 или DB2 9.5 FP4 с сайта производителя.

Целочисленное переполнение в службе LSASS в Microsoft Windows

Программа: Microsoft Windows XP; Microsoft Windows 2003; Microsoft Windows Vista; Microsoft Windows 2008; Microsoft Windows 7.

Опасность: Средняя .

Наличие эксплоита: Нет.

Описание: Целочисленное переполнение существует из-за ошибки в реализации NTLM при обработке пакетов в процессе аутентификации в службе Local Security Authority Subsystem Service (LSASS). Удаленный пользователь может с помощью специально сформированного аутентификационного NTLM-фрейма аварийно завершить работу службы и вызвать перезагрузку системы.

URL производителя: www.microsft.com.

Решение: Установите исправление с сайта производителя.

Визитка

ЮРИЙ ВИННИК, сисадмин в информационном центре Львовской железной дороги с 2001 года. Занимается программированием на языках PHP, Perl Pascal, Bash Script

MyZCl поможет

Моя система автоматической инвентаризации

Существует много программ инвентаризации компьютерной техники, но большинство из них являются коммерческими и стоят денег. Я же расскажу, как решить эту задачу, не потратив ни копейки

При наличии большого количества компьютеров в корпоративной сети очень полезно иметь полную и регулярно обновляемую информацию о каждом компьютере в электронном виде. В этой же базе удобно хранить инвентарные номера устройств, информацию об установленном ПО, историю изменений конфигурации и многое другое.

Для этих целей я решил использовать систему zCl [1]. Эта система хорошо подходит для проведения инвентаризации корпоративной сети. Она проста в использовании, бесплатна, открыта.

Но поэксплуатировав её некоторое время , я отметил ряд недочётов.

Во-первых, в системе отсутствовали поля для хранения инвентарных номеров и информации о размещении компьютеров в том или ином подразделении организации.

Во-вторых, система не допускала ручного ввода устройства, и такие важные узлы сети, как маршрутизаторы, невозможно было добавить в базу данных системы.

В-третьих, внесённую в систему информацию нельзя удалить тривиальным способом, а только вручную, удаляя данные из таблиц. И наконец, интерфейс системы был написан на английском языке, который, увы, не все понимают в нужном объеме.

Поэтому я решил устранить **все эти** недостатки системы инвентаризации **zCl радикальным методом - написал форк** под названием MyZCl и разместил **его** HaSorceForge.net [2]. В этой статье я хочу рассказать **об опыте установки и** применения этой системы **для инвентаризации** компьютерной техники.

Доработка продукта

В этой главе я расскажу об изменениях, которые я произвёл над исходным кодом проекта **zCl. Если** читателя не интересуют эти подробности, он может смело опустить главу и сразу же переходить к следующей.

Вначале я решил перевести интерфейс на русский и украинский языки. Исходный проект zCl был написан на PHP, поэтому был произведён перевод всех фраз на английском языке в командах echo.

Чтобы повысить читаемость выводимой из таблиц информации, при выводе названий столбцов таблиц пришлось операторы SQL типа:

```
SELECT b.hostname,b.user FROM computer_system b
```

заменить на:

```
SELECT b.hostname as 'Хост',b.user as 'Имя пользователя' .
       FROM computer_system b
```

В скрипте registered_device.php добавил переменные $dev_name и $zak, в которых хранились название типа устройств (периферия или мониторы) и суффикс прилагательного «Зарегистрированный» («~ые» или «~ая» в зависимости от типа устройства).

К таблицам computer_system, monitor, peripheral добавлено поле invn типа varchar(31), в котором будет храниться инвентарный номер соответствующих устройств.

В таблицу computer_system также были добавлены поля place типа varchar(IOO) и comment типа varchar(200), которые могли бы содержать место размещение компьютера и примечания.

В PHP-скриптах computer_details.php и computer_details_spvisor.php, отвечающих за отображение и изменение информации о компьютере, были добавлены вывод инвентарного номера, места размещения и примечания, а также возможность их изменения. В скрипт computer_details_spvisor.php добавил кнопку «Удалить» и написал метод удаления информации об устройстве из системы - del .comp.php.

Для автоматического обновления информации я написал несколько скриптов для установки на стороне клиента. Ссылки для скачивания архивов с этими скриптами я вынес на главную станицу системы, а сами архивы разместил в подкаталоге add-ons.

В случае сбора информации с ОС семейства Windows при помощи пакетного файла install.bat происходит запрос сетевого адреса и пути к системе MyZCl, после чего эта информация вносится в файл takedata.js, который, собственно, и собирает и регистрирует информацию об инвентаризируемой системе. Далее создаётся фоновый процесс с помо-

щью run.vbs, который и регистрируется в реестре для автоматического выполнения при каждом старте системы.

В случае ОС семейства GNU/Linux при запуске на строне клиента скрипта install.sh происходит проверка наличия необходимых для корректной работы клиентской части пакетов: sun-jdk, lshw, read-edid. Далее будет запрошена и внесена в файл lshwclient.java информация о сетевом адресе и пути к системе MyZCI, после чего с помощью компилятора Java будет создана программа, собирающая информацию о системе. Эта программа будет внесена в планировщик заданий cron для периодического выполнения каждый час - для регулярного обновления информации об инвентаризируемой системе.

Рекомендации по установке и настройке системы

Система инвентаризации MyZCI является многоплатформенной. Она с успехом может выполняться на сервере как под управлением ОС Windows, так и под управлением GNU/Linux. Главные требования системы - это веб-сервер с поддержкой PHP и сервер баз данных MySQL.

После скачивания и распаковки архива прочитайте документацию по установке и использованию системы. Она располагается в подкаталоге docs и переведена мной на русский и украинский языки. В ней достаточно подробно описан процесс установки и настройки, я же расскажу о некоторых дополнительных моментах, не вынесенных в документацию.

Во-первых, в самом конце SQL-скрипта по созданию базы данных и таблиц мной была для универсальности доступа к БД добавлена следующая строка:

```
grant select,delete,insert,update on zci.* to 'zci'@'%' ↵
      identified by 'zci';
```

Если вы собираетесь систему инвентаризации MyZCI и сервер БД MySQL установить на одном компьютере и не планируете наблюдать за базой с других компьютеров в сети, то я бы рекомендовал эту строку перед выполнением скрипта удалить или закомментировал!.

Во-вторых, для безопасности желательно закрыть паролем доступ к подкаталогу manage. Сделать это можно в конфигурационном файле веб-сервера Apache. Ниже привожу фрагмент моего конфигурационного файла:

```
<Directory /var/www/myzci/manage>
        AuthType basic
        AuthUserFile /var/www/myzci/manage/.htaccess
        AuthName "Access"
        require valid-user
</Directory>
```

Здесь я указываю серверу, что при доступе к каталогу /var/www/myzci/manage нужно требовать авторизацию по паре пользователь/пароль, что хранится в файле /var/www/myzci/manage/.htaccess. Кроме того, не забудьте, что нужно создать файл .htaccess с парами пользователь/пароль с помощью утилиты htpasswd.

При установке PHP также обратите внимание, что обязательно должен быть установлен пакет расширений PECL. Если он отсутствует в репозитории вашего дистрибутива, то, скорее всего, придётся пересобрать PHP из исходных кодов с включенными опциями -enable-dbx и -enable-mysqi.

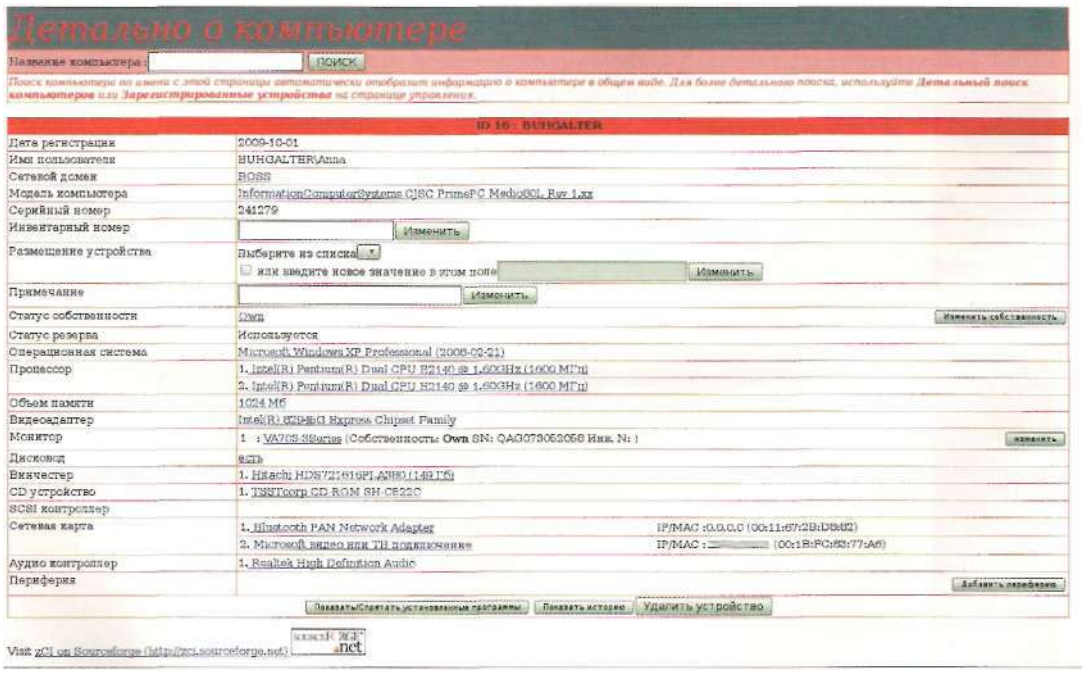
Для ОС семейства Windows пакет PECL для PHP 5.2.6 можно скачать с сайта разработчиков [3].

Если в качестве сервера вы будете использовать систему, базирующуюся на Debian GNU/Linux, то расширения PECL можно добавить так, как описано здесь [4].

Сбор данных с компьютеров

Когда система MyZCI установлена и настроена, то можно приступать к сбору данных с пользовательских машин. Для периодического автоматического обновления инфор-

Рисунок 1. На администровной странице мы можем изменить некоторую информацию о компьютере



мации с зарегистрированных систем мной были разработаны специальные скрипты, которые устанавливаются на стороне клиента и регистрируются в системе.

Ссылки для скачивания архивов с этими скриптами размещены на главной странице системы. Для того чтобы попасть на эту станицу достаточно в адресной строке браузера ввести сетевой адрес и путь в вашей системе MyZCI, например: http://localhost/myzci.

В случае установки скриптов в Windows нужно в произвольный каталог скачать с главной страницы архив win_zci_client.zip и распаковать его. Запустить пакетный файл install.bat и ввести адрес и путь к системе MyZCI.

Для ОС семейства GNU/Linux нужно скачать архив lin_zci_client_deb.tar.gz или lin_zci_client_rpm.tar.gz в зависимости от используемого в вашей инвентаризируемой системе пакетного менеджера. Далее нужно запустить скрипт install, sh и ввести два параметра: адрес сервера и относительный путь к системе MyZCI. Если в системе отсутсвуют пакеты sun-jdk, lshw или read-edid, то их придётся доустановить.

Для ОС семейства Windows я бы рекомендовал следующий алгоритм по регистрации компьютеров:

- В адресной строке браузера на регистрируемой машине ввести сетевой адрес и путь к системе MyZCI, чтобы попасть на главную страницу системы. Попытаться зарегистрировать компьютер с помощью кнопки на главной странице MyZCI - «Зарегистрировать компьютер».
- Если на страницах управления появилась информация о вносимом в базу компьютере (Меню «Зарегистрированные устройства», пункт «Все компьютеры»), то можно скачивать с главной страницы и устанавливать скрипт автоматического сбора информации - win_zci_client.zip.
- Если же информация не появилась, то возможны два варианта решения проблемы:
  - возможно, проблема **связана с** настройками браузера IE. Нужно установить уровень безопасности как самый низкий либо же внести сервер MyZCI в доверенные узлы;
  - также может по какой-то причине не работать механизм MS Windows Scripting Host (у меня такое случалось не так уж и редко). В этом случае нужно просто скачать с главной страницы и установить этот пакет на инвентаризируемый компьютер.

Для ОС семейства GNU/Linux особых проблем со сбором информации не отмечалось. Отмечу только одно, что для получения полной информации с системы нужно запускать и устанавливать скрипт от имени администратора root. При запуске от имени обычного пользователя не сохраняется информация об установленном в системе мониторе, и ее нужно вводить вручную.

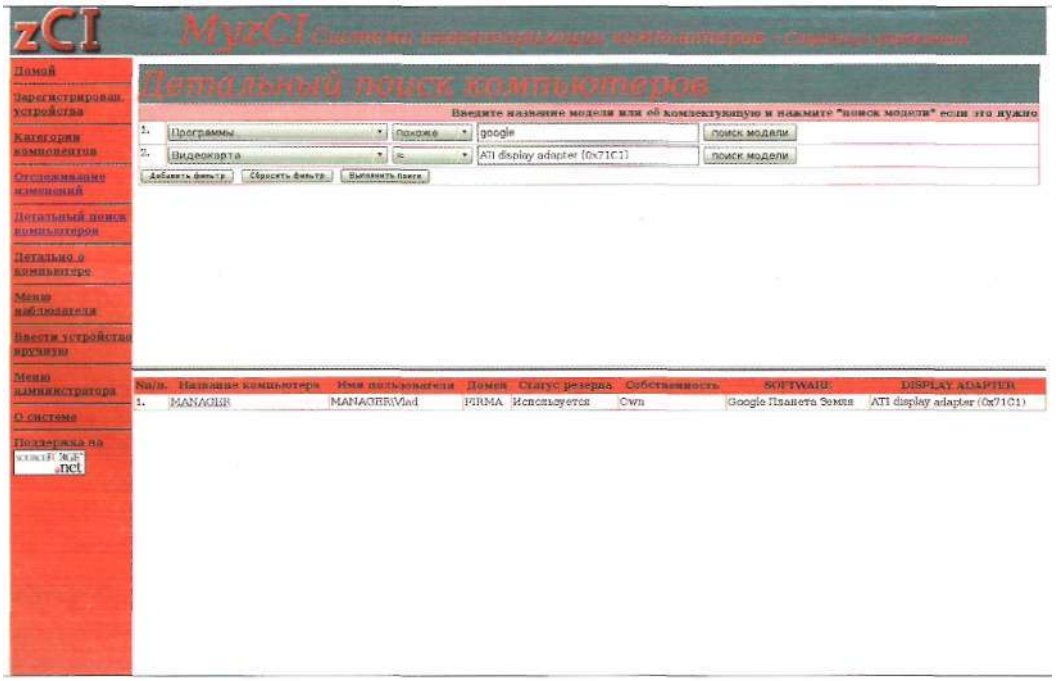
Если устройство невозможно добавить с помощью методов, описанных выше, то его параметры можно ввести вручную на странице «Ввести устройство вручную».

Использование интерфейса

Все основные действия над зарегистрированными устройствами осуществляются со страниц управления. Для входа на страницы управления введите в адресной строке браузера адрес вида: гтИр://<адрес_вашего_сервера/путь_к_MyZCb/manage, например: http://localhost/myzci/manage.

В «Зарегистрированных устройствах» можно получить список всех компьютеров с группировкой по типам собственности и резерва. С помощью кнопок «Монитор» и «Периферия» можно переключить список на отражение информации о данных типах устройств. Поиск можно проводить для компьютеров по названию хоста, членству в домене и имени пользователя. Для периферии и мониторов поиск производится за серийным номером или названием устройства.

Рисунок 2. Страничка расширенного поиска по многим параметрам



Просмотреть детальную информацию о компьютере можно, щёлкнув по имени хоста, тогда мы перейдём на страницу с характеристиками данного устройства. Для того чтобы изменить некоторую информацию о компьютере: инвентарный номер, место размещения, тип собственности, добавить периферию или монитор или же просто удалить эту запись из системы, нужно нажать на кнопку «Страницы Администрирования» (см. рис. 1).

В «Категориях компонентов» можно посмотреть общее количество установленных в ваших компьютерах устройств. Для просмотра списка компьютеров с установленными однотипными компонентами, нужно нажать на ссылку «(просмотр)», размещённую справа возле номера по порядку компонента.

Для того чтобы отследить вносимые в конфигурацию системы изменения, можно воспользоваться пунктом «Отслеживание изменений». Из списка «Тип устройства» выбираем интересующий вас компонент, потом тип изменений «Старые/Неактивные записи» и корректируем, если нужно, дату поиска. После этого нажимаем кнопку «Запрос» и получаем список компьютеров, по которым данные компоненты удалялись. В списке будут отмечены дата установки и дата удаления компонента.

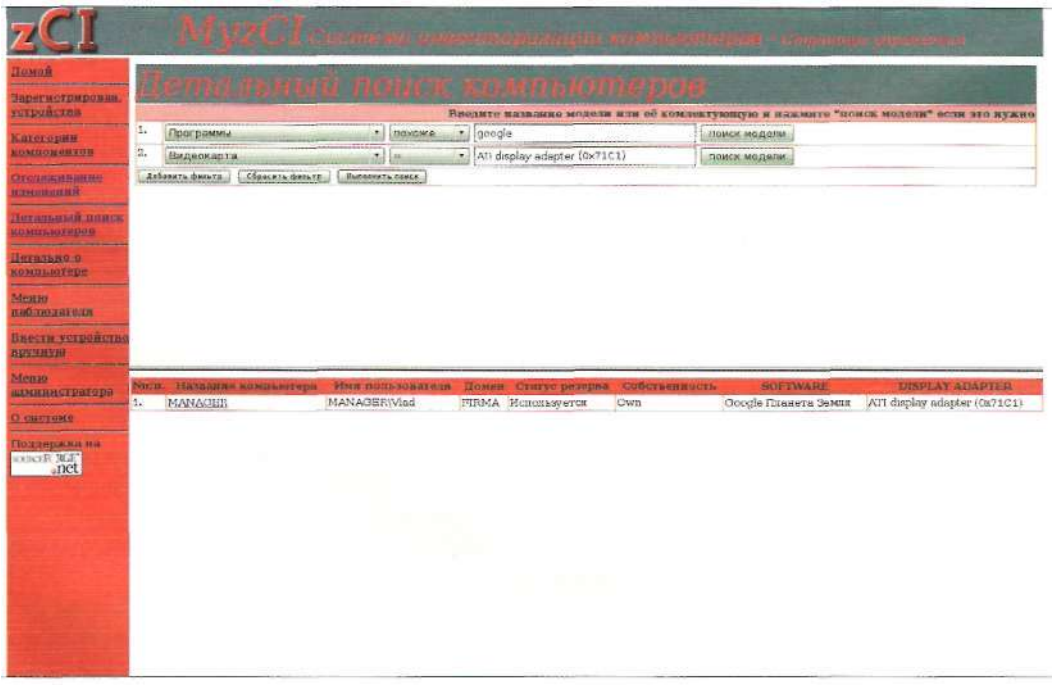
Если нужно произвести сложный поиск компьютеров с использованием характеристик установленных на нём компонентов, то нужно использовать пункт меню «Детальный поиск компьютеров». Поиск можно проводить не только по одному параметру, а по нескольким. Для этого нужно нажать кнопку «Добавить фильтр» и ввести дополнительный параметр поиска в текстовое поле (см. рис. 2). Чтобы определить, существует ли вообще такой параметр поиска, нужно ввести его (либо его часть) в текстовое поле и начать кнопку «Поиск модели». Откроется дополнительное экно, в котором будет список параметров поиска, которые соответствуют введённому вами, либо будет выдан пустой список, если таковых в системе не зарегистрировано. Если щёлкнуть мышкой в этом списке **на нужном вам** параметре, то его значение будет скопировано в текстовое поле для поиска.

В «Меню администратора» можно изменить статус собственности и резерва для зарегистрированных в системе устройств. Для этого нужно выбрать пункт «Изменить статус компьютера» или «Изменить статус устройства», Изменение типа собственности производится в зависимости от текущего состояния собственности устройства или компьютера. Например, если устройство (или компьютер) находится в состоянии «Собственный», то его собственность можно изменить на «Аренда» или «Окончание собственности», а если в состоянии «Аренда», то на «Собственный» или «Окончание аренды». Аналогично производится изменение статуса резерва. Поиск компьютеров производится по имени хоста, имени пользователя или по членству в домене. Поиск устройств производится по их имени или серийному номеру. Если в обоих случаях категорию поиска не вводить, а просто нажать кнопку «Поиск», то мы получим список всех зарегистрированных компьютеров или устройств в системе с последующей возможностью изменения их статуса (см. рис. 3).

Вот кратко и всё, что я хотел рассказать о возможностях системы сетевой инвентаризации MyZCI. Если у вас возникнут конструктивные замечания и пожелания по модернизации системы MyZCI, пишите на форум журнала - www.samag.ru/forum. Удачи! EOF

1. http://www.zci.sourceforge.net.
2. http://www.myzci.sourceforge.net.
3. http://museum.php.net/php5/pecl-5.2.6-Win32.zip,
4. http://www.jejik.com/articies/2008/07/howto_build_andjnstali_the_intl_pecl_extension_for_php5_in_debian.

Рисунок 3. Изменение типа собственности и резерва производится очень просто



Визитка

СЕРГЕЙ УНАГАЕВ, генеральный директор компании Database Harbor

Учет компьютеров
с Hardware Inspector

В компаниях ИТ-подразделения часто обязаны проводить ежегодно инвентаризацию компьютерного парка. Как это сделать?

Многие начальники проходят тернистый путь, начиная с попыток учета компьютеров и программного обеспечения в Excel и заканчивая созданием приложения для учета своими силами. Но гораздо эффективнее использовать специализированные программные продукты. Рынок предлагает достаточно большой ассортимент решений. Рассмотрим продукт, который действительно занимается инвентаризацией устройств, а не просто отображает текущую конфигурацию компьютеров, прочитав ее по WMI. Речь идет о Hardware Inspector.

Важность полноценной базы данных

Тот факт, что приложение заводит в базе данных паспорт на каждый учетный объект (устройство, лицензия и прочее), определяет высокий потенциал и величину экономического эффекта от его использования. Ведь это позволяет вести историю обслуживания, перемещения и инвентаризации объектов. На основе этих данных возможно построение самых разнообразных отчетов и аналитик.

Скорость внедрения

Благодаря интеграции Hardware Inspector с программами ASTRA32 и EVEREST, предназначенными для анализа конфигурации компьютеров, процесс формирования базы данных перестает быть трудоемким. Они анализируют конфигурацию именно на низком уровне, а не получая ее по WMI. Это позволяет получить гораздо более качественные и достоверные данные об устройствах.

Перечень рабочих мест может быть импортирован из сетевого окружения, список сотрудников - из Active Directory или базы отдела кадров.

Устройства могут быть импортированы пошагово, либо «одной кнопкой» с помощью аудита рабочих мест.

О компании

Компания является лидером на российском рынке в сфере учета компьютеров и автоматизации деятельности ИТ-подразделений. Отличительной . : - : запагаемых решений является высокая производительность = : _ - = : : т :•;•= простота внедрения и доступная цена.

Инвентаризация с помощью штрихкодов

Hardware Inspector предлагает инструменты организации учета и проведения процедур инвентаризации оборудования с использованием сканеров штрихкода.

Аудит рабочих мест

Данный механизм предназначен для ежедневного контроля отклонений в составе устройств компьютеров на рабочих местах.

Он позволяет оперативно отслеживать следующие виды отклонений: появление новых и исчезновение старых устройств, выполненные перемещения, которые забыли отразить в базе данных.

Поиск запрещенного ПО

В последнее время особенно актуальной стала проблема контроля использования на рабочих местах запрещенного и нелицензионного ПО. Данный механизм позволяет системному администратору видеть целостную картину по легитимности использования ПО пользователями. Также имеется инструмент распределения ответственности за перечень установленного программного обеспечения.

Прочие функции

Помимо учета компьютеров как такового, Hardware Inspector позволяет решать целый ряд задач по автоматизации деятельности ИТ-структур:

- учет заявок от пользователей;
- кроссировка сети;
- учет лицензий и мониторинг запрещенного ПО;
- учет расходных материалов;
- сервисные и профилактические работы;
- возможность работы всех удаленных филиалов компании в единой базе данных;
- более 30 встроенных отчетов с возможностью их модификации пользователем;
- гибкое разграничение прав доступа на уровне функционала, оргструктуры, карты и типов устройств. ECF

Визитка

АЛЕКСАНДР ГЕРНГРОСС, системный администратор турфирмы «Лабиринт».
МАКСИМ ЛОБОВ, руководитель технического отдела турфирмы «Лабиринт

Сетевая версия SQL под Linux

Перевод серверной части «1С:Предприятие 7.7»

Практика показывает, что при переходе компаний на использование Linux на своих компьютерах программное обеспечение бухгалтерии обычно становится камнем преткновения

Несмотря на то что продукт «1С:Предприятие8» имеет больше возможностей работать под Linux [18], бухгалтеры средних и крупных фирм не спешат переходить с версии 7.7 на 8. Не дожидаясь светлого будущего, системные администраторы уже сейчас вынуждены запускать «1С:Предприятие 7.7» под Linux. Можно ответить, что существует много способов запуска «1С:Предприятие» под Linux, данная тема не раз обсуждалась на форумах [3, 4], а об одном из них было написано на страницах журнала [1], однако все эти способы описывают запуск клиентских приложений, оставляя в тени серверную часть.

Получается, что переход на Linux осуществляется наполовину? Не совсем так. Давайте разберёмся, что же понимать под серверной частью и как её перевести под Linux? Локальную версию (не сетевую) мы не рассматриваем, так как этот случай тривиален.

Сетевая версия «1С:Предприятия» может работать в двух режимах:

- с использованием общих файлов для хранения всей базы в формате dbf;
- с использованием SQL-сервера для хранения переменных данных и dbf файлов для различных постоянных форм и шаблонов.

Небольшие фирмы обычно используют общие файлы. В качестве протокола обмена используется SMB или CIFS. В Windows поддержка этих протоколов выглядит как использование «Сетевого окружения», а в Linux используется пакет Samba.

По мере роста базы и увеличения числа одновременно работающих бухгалтерских работников в системе фирмы сталкиваются с тем, что при общем хранении файлов операции, ранее выполнявшиеся за 10-15 секунд, требуют нескольких минут ожидания.

Связано это с неоптимальной организацией базы, что приводит к возникновению множества взаимных блокировок. Выход из ситуации есть - это переход на использование SQL-сервера, который изначально рассчитан на одновременную работу большого числа пользователей и позволяет оптимально работать с данными.

Какой SQL-сервер выбрать? У большинства предприятий размер бухгалтерских баз не очень велик, чтобы переходить на Oracle, это всё равно что из пушки стрелять по воробьям. Наиболее простые базы, вроде mSQL или MySQL, не поддерживают триггеры и процедуры в полном объёме, как это может понадобиться. Да, и не стоит забывать: когда 10 лет назад вышла версия 7.7, у большинства фирм стояли пиратские ОС, доступность которых, как и дистрибутивов СУБД, определялась низкой ценой и безнаказанностью их использования. В таких условиях логичнее всего было сделать поддержку СУБД Microsoft SQL.

Сейчас наша экономика входит в цивилизованное русло, фирмы начинают задумываться о легальности используемого ПО, эффективнее оценивают функциональную необходимость, затраты и риски. Если где-то ещё не перешли на полностью лицензионное программное обеспечение, то, по крайней мере, стараются умалчивать об этом. Возможно, что не все знают об альтернативных решениях, об одном из которых сейчас и пойдёт речь.

PostgreSQL альтернатива Microsoft SQL

Покупка СУБД Microsoft SQL - это дорого, плюс надо вложить деньги в покупку серверной ОС, так как под пользовательской ОС или под Linux данная СУБД не работает. Также необходимо обучить персонал для работы с этими продуктами. PostgreSQL - это объектно-реляционная система управления базами данных, разработка которой в различных формах ведётся с 1977 года [5]. PostgreSQL считается самой совершенной СУБД, распространяемой на условиях открытых исходных текстов.

Несмотря на глубокие исторические корни и более чем 32-летние наработки, грустная действительность современного мира такова, что редко какие технические решения развиваются без рекламы и массового использования. Возьмите пример с операционной системой OS/2 или стандартом Betacam. В таких условиях самым главным направлением в популяризации преимуществ PostgreSQL может быть только практическое применение данной СУБД. Что интересно, многие разработчики программного обеспечения понимают

это и, например, восьмая версия «1С:Предприятия» умеет изначально работать с PostgreSQL. Но как быть тем, у кого версия 7.7? Не для них ли написана эта статья?

Для тех программных продуктов, которые «не знают» о существовании СУБД PostgreSQL (т.е. не могут работать с ней напрямую), следует использовать конвертор запросов. Предполагая, что все существующие приложения укладываются в рамках клиент-серверной модели, зададимся вопросом: а где расположить конвертор - на сервере или на клиенте?

Несомненно, более прозрачным решением было бы установить один конвертор на стороне сервера. Технически это сложная задача, готовые проекты нам неизвестны, но работы в этом направлении ведутся. Более простой вариант - это конвертирование на стороне клиента. Мнимая простота компенсируется другими затратами, конвертор необходимо не только устанавливать на каждом из клиентов, но он ещё должен учитывать особенности реализаций на всём множестве клиентов. Если количество клиентов конечно, их вариативность небольшая или вообще отсутствует, задача получается не такой сложной.

Именно по второму пути сейчас развивается проект универсального транслятора SQL-запросов из диалекта T-SQL в pgSQL с названием SELTA@Etersoft [6]. Первоначально существовала задача сделать максимально простой транслятор, главным образом для «1С:Предприятия 7.7», сейчас же проект перерастает в создание более универсального инструмента. На выбранном направлении есть и подводные камни из-за особенностей проекта. Так, предполагается, что на клиентской стороне используются Windows или программы, работающие под эмулятором wine. Логично спросить: а как быть тем, у кого клиент под UNIX, например, используется связка FreeBSD + FreeTDS [14] + Apache + PHP?

С этим вопросом мы обратились к **Станиславу Коробейникову,** главному идеологу проекта. Его ответ был следующим: «Данная ситуация скорее редкость, чем правило, но несмотря на это в ближайших планах развития есть создание серверного варианта. Как бы то ни было, быстрый старт SELTA был невозможен благодаря простоте и включению функций парсера SQL-запросов в ODBC-драйвер. Начни мы по-другому, возможно, не было бы этого проекта вообще». Из ответа стало ясно, что структурная схема работы транслятора запросов следующая (см. рис. 1).

Рассмотрим, что представляет данный проект сегодня.

SELTA@Etersoft

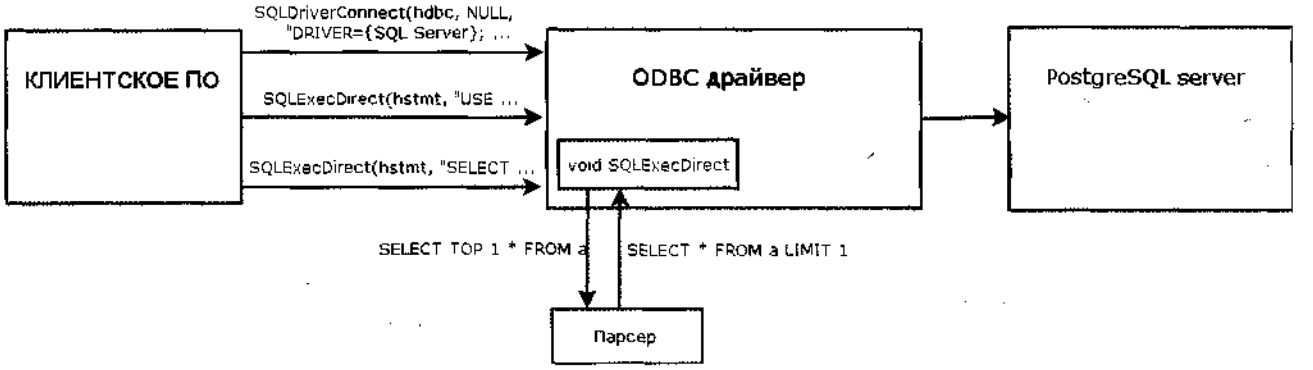
Идея проекта такова, что SELTA + PostgreSQL фактически выступают эмулятором сервера MS SQL. Несмотря на то что данный транслятор запросов изначально разрабатывался с целью запуска «1С:Предприятие» под Linux, его возможности постоянно расширяются, вводится поддержка новых приложений. Даже если вы не используете продукты «1С» в своей работе, а применяете какие-то другие, использующие MS SQL, или планируете приобрести, например, программу «САМО-Тур», то вам пора задуматься о миграции на PostgreSQL и возможной экономии.

Транслятор SELTA@Etersoft является коммерческим продуктом, к которому прилагается техническая поддержка. Но если вы не намерены что-то покупать сразу, а просто хотите изучить возможности транслятора перед покупкой, то фирма лояльно относится к просьбам о тестировании, требуя лишь гарантийное письмо о том, что вы сотрёте продукт со своего компьютера после завершения тестирования.

В описании продукта [6] можно встретить фразу: «Создать универсальный транслятор запросов практически невозможно, поэтому данный продукт предназначен только для некоторых приложений». Задавшись вопросом, почему конвертор не всегда работает, какие проблемы возникают при его реализации и каков же полный список поддерживаемых сегодня приложений, мы обратились к разработчику и получили следующий ответ:

«SQL-серверы отличаются друг от друга не только и не столько синтаксисом. Ключевыми моментами являются механизмы блокировок, версионность, уровни изоляции транзакций, типы данных и, как следствие, работа с ними. PL/pgsql, используемый в Postgres, сильно отличается от t-sql, с которым работает MS SQL Server. Есть и мелкие отличия, с которыми постоянно сталкиваются разработчики. Например, в t-sql, если переменной присвоить значение поля запроса, не возвращающего строк, переменная не изменит своего значения. В plpgsql в том же случае переменная станет NULL. Таких отличий множество, поэтому чаще всего для каждого нового ПО, поддерживаемого SELTA, требуется доработка. Тем не менее SELTA универсальна и может работать с разными продуктами. На данный момент она

Рисунок 1. Структурная схема работы транслятора запросов SELTA



ориентирована на «1С:Предприятие 7.7». Однако если вы заинтересованы во включении в список программ, поддерживаемых SELTA, конкретного приложения, использующего MS SQL, вы можете обратиться к разработчикам Etersoft».

От себя добавим, что сейчас SELTA@Etersoft полностью поддерживаются следующие программы:

- «ЮПредприятие 7.7» SQL;
- конфигурация «Бухгалтерия»;
- конфигурация «Зарплата»;
- конфигурация «Торговля и Склад»;
- конфигурация «Производство и Услуги»;
- расширение «1С++».

В ближайшее время планируется поддержка:

- «WinCMeTaSQL»;
- MonitorCRM;
- «КМ-Школа»;
- MarkSQL.

Чаще проверяйте список поддерживаемых программ по адресу [11]. Недалёк тот день, когда вы в списке полностью поддерживаемых программ обнаружите какой-нибудь «САМО-Тур»[1] или другое используемое вами ПО, а если хотите ускорить процесс, то пишите разработчикам проекта и присоединяйтесь.

Несмотря на оптимизм разработчиков, мы всё же копнули глубже и задались научной стороной вопроса трансляции запросов.

Что из запросов перевести нельзя, или Какие проблемы встречаются ?

Ответ **Станислава Коробейникова** был следующим: «Боль_шая проблема изначально была вызвана отсутствием у Postgres динамических курсоров (на странице с неподдерживаемыми функциями [9] можно видеть: B034 Dynamic specification of cursor attributes). Программы же, работающие с MS SQL Server, очень активно используют именно динамические курсоры. Первым шагом к добавлению этого функционала было пересоздание простых курсоров при каждом обращении. Метод имеет несколько минусов. Один из них - время, затрачиваемое на пересоздание курсора. От этого частично удалось уйти в версии SELTA 1.0.5. через триггеры, отслеживающие **изменения** в таблицах. Недостаток такого подхода-лишние накладные расходы при изменении данных. Чтобы избежать замедления, в SELTA была включена таблица с масками имён таблиц, требующих наличие триггеров [10]. Для «1С» была собрана статистика, и эти маски создаются при загрузке данных. Но этот подход также требует доработки. Немаловажен в работе с СУБД механизм блокировок. В MS SQL возможен такой принцип работы: для целостности данных и получения только актуальной информации при множественном изменении блокируются все участвующие таблицы. При этом доступ к информации без требования актуальности может быть обеспечен с помощью механизма, называемого «грязным чтением». «Чистое чтение» будет ожидать, пока блокировка таблицы закончится.

Философия работы с PostgreSQL иная, и такой механизм не реализован. Чтобы имитировать подобное поведение, SELTA блокирует таблицы при «чистом чтении», исключая возможность взаимного изменения данных и разрешая при этом чтение данных, ставшее таким образом «грязным».

Получив достаточно сведений о проекте с разных сторон, мы решили попробовать SELTA@Etersoft в действии и перевести серверную часть программы «ЮПредприятие» на Linux.

Практическая часть

Первым делом необходимо выбрать дистрибутив Linux для тестирования. Приоритетными при тестировании и для сборки новых версий являются платформы ALT Linux Server и Ubuntu Server. Связано это с широкой распространённостью последнего дистрибутива и тесными связями с производителями первого. Сама же SELTA, по заверениям разработчиков, тестируется под различные ОС Windows (от 2000 вплоть до 2008 Server) и WINE@Etersoft. Можно сделать вывод, что принципиальных предпочтений того или иного дистрибутива у разработчиков SELTA@Etersoft нет, поэтому среди десятка поддерживаемых был выбран уже установленный на сервере Linux Fedora 11. Вполне вероятно, что всё описанное ниже также заработает и под вашим дистрибутивом с небольшими поправками. В качестве wine использовался WINE@Etersoft 1.0 SQL 1.0.11-eter8/3.

Рисунок 2. Окно программы SELTA@Etersoft

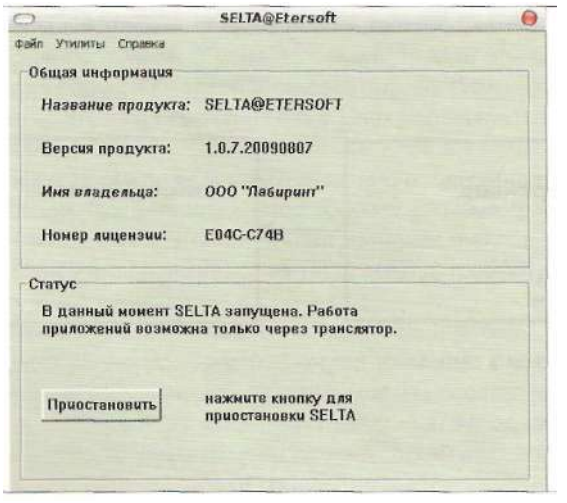
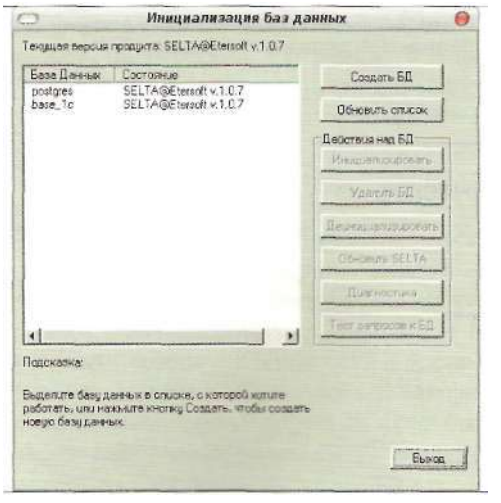


Рисунок 3. Окно «Инициализация Баз Данных»



Вся настройка «1С» для работы с серверной частью под Linux сводится к четырём несложным этапам:

- установка и запуск PostgreSQL;
- установка SELTA на стороне клиента;
- установка и запуск клиента «1С»;
- конвертирование или перенос базы данных «1С».

Пройдём подробнее по всем этапам. Пошаговую инструкцию по установке и настройке компонентов можно найти тут [7].

Установка PostgreSQL на сервер

Если на вашем компьютере уже установлен PostgreSQL-зервер, то, к сожалению, его придётся удалить. Проверить, установлены пакеты или нет, можно командой:

```
# rpm -qa|grep postgresql
```

Удалить можно через команду:

```
# rpm -e имя_пакета
```

или через:

```
# yum remove имя_пакета
```

Удалять - не самое хорошее решение, но, к сожалению, патчей для наиболее популярных готовых сборок не существует. Те же, кто могут разобраться с исходными кодами, и так разберутся, обратившись к [8]. Для всех остальных существуют бесплатные сборки PostgreSQL (Postgres® Etersoft), размещённые по адресу: ftp://updates.etersoft.ru/pub/Etersoft/Postgres@Etersoft/stable.

По полученной информации от разработчиков SELTA, в сборку Postgres@Etersoft входят все последние патчи [8], включая патч от «1С» (Бартунова и Сигаева) со строковыми типами, делающими работу со строками идентичной MS SQL.

Итак, скачав для своего дистрибутива необходимые установочные пакеты PostgreSQL компании Etersoft, начинаем установку, подробнее см. [15].

```
# rpm -ih vpostgresql-8.3eter-8.3.7-eter4fedora.i586.rpm
```

```
postgresql-8.3eter-contrib-8.3.7-eter4fedora.i586.rpm
postgresql-8.3eter-server-8.3.7-eter4fedora.i586.rpm
```

Перед первым запуском СУБД необходимо поменять настройки в файле /etc/sysctl.conf: общий размер shared memory в страницах (kernel.shmall) и максимальный размер сегмента shared memory в байтах (kernel.shmmax), установив:

```
kernel.shmall=134217728
kernel.shmmax=134217728
```

Чтобы внесенные изменения вступили в силу без перезагрузки системы, выполняем команду:

```
# sysctl -p
```

Инициализация базы производится автоматически при первом запуске PostgreSQL, файлы баз данных будут храниться в каталоге /var/lib/pgsql/data, владельцем каталога и процессов PostgreSQL устанавливается системный пользователь с учётной записью postgres, который создаётся автоматически, при установке пакетов. Для того **чтобы** иметь возможность подключиться к СУБД, мы должны **задать** пароль главному пользователю СУБД - владельцу всех баз данных - postgres. Это выполняется следующим образом.

Перед первым запуском в файле конфигурации /var/lib/pgsqi/data/pg_hba.conf изменяем строчку:

```
local   all       all       ident     sameuser
```

на:

```
local   all       all       trust
```

Данное изменение позволит локальным пользователям подключаться к СУБД без пароля. (В целях безопасности не забудьте вернуть значение обратно, когда всё будет настроено.)

Запускаем PostgreSQL командой:

```
# service postgresql start
```

или:

```
# /etc/rc.d/init.d/postgresql start
```

После удачного старта необходимо подключиться к СУБД и задать пароль главному пользователю СУБД (владельцу всех баз данных - postgres), выполнив в консоли следующую команду:

```
$  psql -U postgres -d template1 -c "ALTER USER postgres ↵
      PASSWORD 'новый пароль' "
```

Установив пароль для пользователя СУБД postgres, отключаем локальным пользователям возможность подключаться к базе без пароля. Для этого в файле var/lib/pgsql/data/pg_hba.conf возвращаем настройки обратно и перезапускаем СУБД PostgreSQL командой:

```
# /etc/rc.d/init.d/postgresql restart
```

или:

```
# service postgresql restart
```

Проверить, что всё работает правильно, можно, попытавшись подключиться к PostgreSQL с помощью консольного клиента psql командой:

```
$ psql -U postgres -h localhost
```

В случае удачного подключения вы увидите на консоли примерно следующее приглашение от СУБД:

```
Welcome to psql 8.3.7-eter4, the PostgreSQL interactive
terminal.

Type:  \copyright for distribution terms
       \h for help with SQL commands
       \? for help with psql commands
       \g or terminate with semicolon to execute query
       \q to quit

postgres=#
```

Отключаемся от базы, набрав \q. При необходимости прописываем PostgreSQL в стартовые скрипты системы в /etc/rc.d/rc?.d, например, командой:

```
# chkconfig postgresql on
```

Подробнее о настройках и как работать с PostgreSQL можно прочитать в книге [5], об оптимальных настройках см. [16].

Установка программы SELTA на стороне клиента

Так как программа SELTA работает на стороне клиента, то она может быть установлена как на комьютере с Windows, так и на компьютере с Linux под эмулятором wine. Принципиальных отличий в установке нет. Заметим, что PostgreSQL и SELTA обычно устанавливаются на разных компьютерах, но могут работать и на одном.

Скачиваем с сайта Etersoft установщик selta.msi или английскую версию seltaEng.msi.

```
$ wget ftp://updates.etersoft.ru/pub/Etersoft/ ↵
       SELTA@Etersoft/1.0.7/Windows/selta.msi
```

Далее запускаем под обычным пользователем установку командой:

```
$ wine start selta.msi
```

Выбираем директорию установки для программы. После установки запускаем SELTA под учётной записью установившего её пользователя:

```
$ wine "c:/Program Files/Selta/Selta.exe"
```

При первом запуске программы нужно будет указать путь к файлу лицензии. Его можно получить на сайте Etersoft, выбрав необходимую программу (в данном случае SELTA® Etersoft) и пройдя регистрацию на сайте. Получить лицензию на тестирование продукта на пару месяцев не так и сложно. После того как файл лицензии был указан, появится окно программы (см. рис. 2).

В появившемся окне выбираем меню «Утилиты -» Инициализация БД». И заполняем данные для подключения к базе PostgreSQL, после чего жмём кнопку «Соединение». Если соединение прошло удачно, появится окно «Инициализация Баз Данных» (см. рис. 3). В нем будут отображены существующие базы, к ним имеет доступ пользователь, которого вы указали при подключении. Для того чтобы создать базу, нужно нажать кнопку «Создать БД» и в появившемся окне написать название будущей базы.

Данная установка SELTA должна быть проведена на всех клиентских машинах, где планируется работа «1С:Предприятие» с сервером PostgreSQL.

Более подробную информацию по установке программы SELTA можно найти тут [12].

Установка клиента «1С:Предприятие 7.7» на компьютер с Linux

Запускаем установку «1С:Предприятие» под учётной записью обычного пользователя:

```
$ wine 1CSetup27.exe
```

На предложение выбрать компоненты программы для установки оставляем всё по умолчанию (см. рис. 4).

После того как «1С:Предприятие» установилось, устанавливаем путь к месту хранения конфигурации и запускаем режим конфигуратора. Далее заходим в меню «Окна -> Панель Окон -> Показать». И снимаем галочку с меню «Показать»; если этого не сделать, то в некоторых случаях программа будет аварийно завершать работу [1]. После чего осталось только прописать настройки подключения. Заходим в меню «Администрирование -> Параметры базы данных SQL» и в появившемся окне вписываем необходимые значения для подключения к базе данных.

Перенос данных в PostgreSQL для «1С:Предприятия 7.7»

Существует два наиболее простых варианта переноса данных из MS SQL в Postgres@Etersoft:

Вариант 1: воспользоваться конвертором [13] программы SELTA@Etersoft для создания дампа старой базы и загрузки его в новую базу.

Вариант 2: выгрузить базу через конфигуратор «ЮПредприятия» в zip-файл все настройки и базы, будучи подключёнными к MS SQL, затем переподключиться к PostgreSQL через SELTA и восстановить из ранее сохранённого zip-файла информацию, используя всё те же штатные возможности конфигуратора.

Рассмотрим эти варианты подробнее:

Перенос данных с помощью конвертора программы SELTA@Etersoft

Перенос начинается с создания новой информационной базы при помощи программы SELTA@Etersoft.

Рисунок 4. Установка «1С:Предприятие 7.7». Выбор компонентов

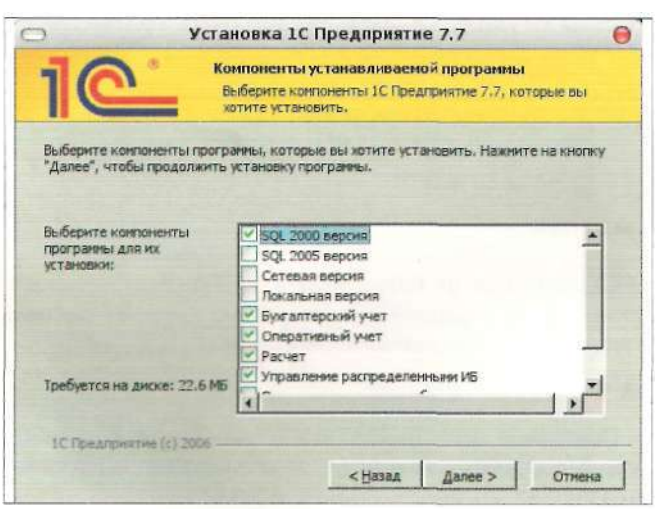


Рисунок 5. Выбор формата хранения данных

Запускаем программу (см. рис. 2). В появившемся окне выбираем меню «Утилиты -» Инициализация БД». И заполняем данные для подключения к базе PostgreSQL, после чего жмём кнопку «Соединение». Если соединение прошло удачно, появится окно «Инициализация Баз Данных» (см. рис. 3).

Для того чтобы создать базу, нужно нажать кнопку «Создать БД» и в появившемся окне написать название будущей базы.

Запускаем «1С:Предприятие» в режиме конфигуратора. Далее появится окно, предлагающее выбрать вам формат хранения данных. Выбираем MS SQL Server и жмём кнопку ОК (см. рис. 5). В меню «Администрирование -> Параметры базы данных SQL» указываем параметры для подключения к PostgreSQL, в качестве имени базы укажите ту базу, которую создали ранее.

Далее необходимо загрузить .md-файл конфигурации, для которой вы переносите данные, и выполнить её сохранение.

Заходим в меню «Администрирование -> Загрузить данные» и указываем путь к файлу .md. При этом будут созданы все необходимые таблицы, индексы и хранимые процедуры - создание структуры базы данных завершено.

Для переноса самих данных воспользуйтесь графической утилитой «Конвертор» [13]. Для этого запускаем SELTA@Etersoft и в меню выбираем «Утилиты -» Конвертор» (см. рис. 6).

Выберите кнопку MS SQL Server -> CSV, в открывшемся окне укажите параметры подключения к MS SQL Server, на котором лежит база данных, из нее вы переносите данные. А в качестве пути для дампа укажите папку на машине клиента, в которую будут скопированы данные. Нажмите «Выполнить» и дождитесь выполнения операции, копирование всех таблиц может занять продолжительное время.

Далее полученный CSV-дамп необходимо загрузить з PostgreSQL@Etersoft. Запустите «Конвертор», выберите кнопку CSV -> PostgreSQL. В открывшемся диалоге необходимо указать параметры подключения к базе, в которой до этого была сохранена ваша конфигурация. Нажмите «Выполнить» и дождитесь выполнения операции, копирование всех таблиц может занять продолжительное время для больших баз - до нескольких часов).

После окончания копирования база готова к работе, можете запускать «1С» и работать с ней в обычном режиме!

Загрузка CSV-дампа в MS SQL Server выполняется аналогично. Подробнее с переносом данных при помощи конвертора можно ознакомиться тут [17].

Перенос данных с помощью штатных средств программы «1С:Предприятие»

Создаём базу данных при помощи утилиты SELTA@Etersoft, лак было описано выше. Затем запускаем«1 С:Предприятие» з режиме конфигуратора, предварительно указав путь -: хранению файлов. После чего нажимаем кнопку ОК.

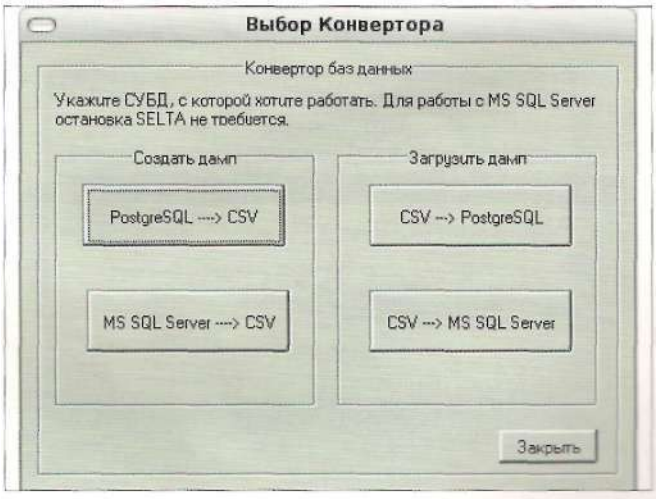
Далее появится окно, предлагающее выбрать вам формат хранения данных. Выбираем MS SQL Server и жмём -кнопку ОК. Выбираем меню «Администрирование -> Выгрузить данные» и делаем полную выгрузку старой базы. После ~эго как выгрузка будет завершена в меню «Администрирование -> Параметры базы данных SQL», прописываем параметры для подключения к PostgreSQL, в качестве имени базы укажите ту базу, которую создали ранее.

Далее необходимо загрузить выгруженные файлы в новую базу PostgreSQL. Заходим в меню «Администрирование -» Загрузить данные» и указываем путь к файлам.

После завершения загрузки можно запустить программу в обычном режиме. «ЮПредприятие» готово к использованию. EOF

1. Барановский С. Квартет: «CAMO», «1С», wine и Etersoft. //Системный администратор, №1, 2009 г. - С. 52-60.
2. Факты внедрения Linux в компаниях - http://www.etersoft.ru/component/option,com_wrapper/Itemid,192.
3. Запуск комплекса «ЮПредприятие» под Linux - http://gloomka.livejournal.com/35655.html.
4. Запуск «1С» под эмулятором в Linux - http://www.opennet.ru/base/sys/run_1 c_on_linux.txt.html.
5. Уорсли Дж., Дрейк Дж. PostgreSQL. Для профессионалов. - СПб.: Питер, 2003. ISBN 5-94723-337-1.
6. SELTA. Универсальный транслятор SQL-запросов из диалекта T-SQL в pgSQL- http://wiki.etersoft.ru/SELTA.
7. «SELTA@Etersoft - Пошаговая инструкция по установке и настройке» - http://wiki.etersoft.ru/SELTA/SeltaDoc.
8. Изменения, внесённые в PostgreSQL - http://wiki.etersoft.ru/PostgreSQL/Patch.
9. http://developer.postgresql.org/pgdocs/postgres/unsupported-features-sql-standard.html.
10. http://wiki.etersoft.ru/SELTA/cursorstriggers.
11. http://wiki.etersoft.ru/SELTA/applications.
12. http://wiki.etersoft.ru/SELTA/Install.
13. http://wiki.etersoft.ru/SELTA/SELTAEXECONVERT.
14. FreeTDS-http://freetds.org.
15. Установка и настройка PostgreSQL - http://wiki.etersoft.ru/PostgreSQL.
16. Оптимизация работы Postgre SQL - http://wiki.etersoft.ru/PostgreSQL/Optimum.
17. Перенос данных из MS SQL Server в Postgre SQL для «ЮПредприятия 7.7» - http://wiki.etersoft.ru/SELTA/CSVDump.
18. Системные требования «ЮПредприятия 8.2» - http://v8.1c.ru/requirements.

Рисунок 6. Графическая утилита «Конвертор»



Визитка

МИХАИЛ ДАНЬШИН, эксперт в области Ш. Специализируется на Exchange и смежных технологиях. Ведет блог (http://danshin.ms}, выступает на конференциях и в MCP-клубе.Награжден премией Microsoft MVP

Решаем проблему

внезапной блокировки учетной записи

Доводилось ли вам сталкиваться с тем, что пользователи не могут войти в компьютер? Что же делать, если учетная запись существует, она не отключена, да еще и пароль правильный?

Иногда возникают ситуации, когда при попытке входа в компьютер пользователь получает сообщение:

```
Unable to log you on because your account has been
locked out, please contact your administrator
```

Это уведомление говорит о том, что акаунт заблокирован (locked). Это не то же самое, что отключен (disabled). В первом случае учетная запись нейтрализуется на некоторое время, и это происходит автоматически, без участия администратора. А во втором отключается системным администратором вручную.

Оказалось, что данная тема актуальна до сих пор. И мне постоянно приходится отвечать на вопросы не только начинающих, но и опытных администраторов.

Сообщение о блокировке учетной записи выглядит, как показано на рис 1.

Природа этого явления заключается в том, что было предпринято несколько попыток ввода неверного пароля. В домене вы можете настроить групповую политику, которая будет регламентировать количество попыток ввода паролей и время, на которое акаунт будет заблокирован. В случае если правильный пароль не будет введен, акаунт будет заблокирован, а пользователь получит уведомление, как показано выше, на рис. 1.

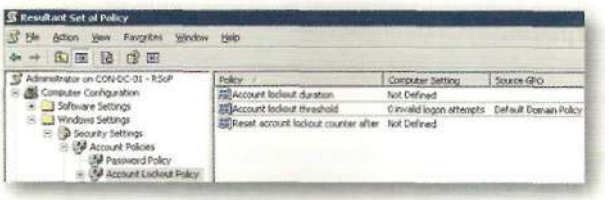
Для того чтобы определить политику, запустите Group Policy Management Console*). По умолчанию политика выглядит так, как показано на рис. 2.

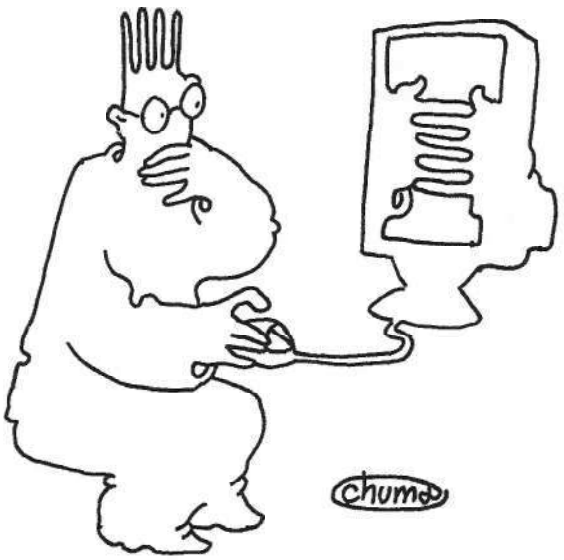
Предположим, что вы хотите ограничить количество неправильных вводов пароля пятью попытками, а потом блокировать акаунт на 30 минут. Для этого вам нужно отредактировать Default Domain Policy (помним, что политики паролей в доменах Win 2003 применяются к уровню домена). Выберите Computer Configuration -> Windows Settings -> Security Settings -» Account Policy -» Account Lockout Policy. Затем отредактируйте параметры групповой политики. Значение параметров:

Account lockout duration - определяет время, на которое акаунт будет заблокирован.

Рисунок 1. Сообщение об ошибке, которое получает пользователь с заблокированной учетной записью

Рисунок 2. Политика Account Lockut Policy по умолчанию





Иногда блокировка акаунта происходит без видимых причин. Определить их **бывает довольно сложно**

Account lockout threshold - определяет количество попыток ввода, после которого акаунт будет заблокирован.

Reset account lockout counter after - определяет время, по истечении которого будет сброшен счетчик попыток. Например, если вы определили, что после пяти попыток акаунт будет заблокирован, а сделали только две попытки входа, а потом, например, ушли пить чай, то по истечении этого установленного времени счетчик обнулится, и у вас опять будет пять попыток.

Попробуйте изменить любой из параметров, и система предложит вам оптимальные с ее точки зрения значения остальных параметров (см. рис. 3).

Вы можете согласиться, а потом при необходимости изменить их по своему усмотрению. Например, если вы установите значение параметра Account lockout threshold, соответствующее 5, а затем нажмете OK, то система предложит вам 30-минутное значение для остальных параметров, как показано на рис. 3.

После того как политика будет определена, вы можете известить ваших пользователей о том, что после того как они введут неверный пароль несколько раз, их учетная запись будет заблокирована (locked). Чтобы снять блокировку, нужно снять галочку Account is locked out в свойствах пользователя, как показано на рис. 4.

Иногда блокировка акаунта происходит без видимых причин. И несмотря на то что блокировка так просто снимается, в некоторых случаях это не решает проблему. Через некоторое время пользователь может обнаружить, что его учетная запись опять заблокирована.

Причин тому может быть несколько, и я опишу их далее. Иногда определить причины бывает довольно сложно. Основная сложность в определении компьютера, с которого происходят попытки ввода неверных паролей.

В журнале безопасности для отслеживания подобных событий существует запись с кодом 680 от источника Security категории Account Logon. В этой записи (см. рис. 5) показана информация о том, в какое время и с какого компью-

Рисунок3. Значения, которые предлагает система

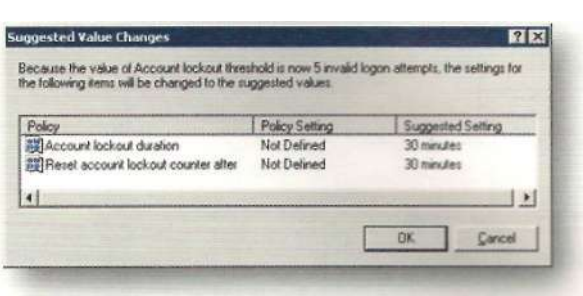
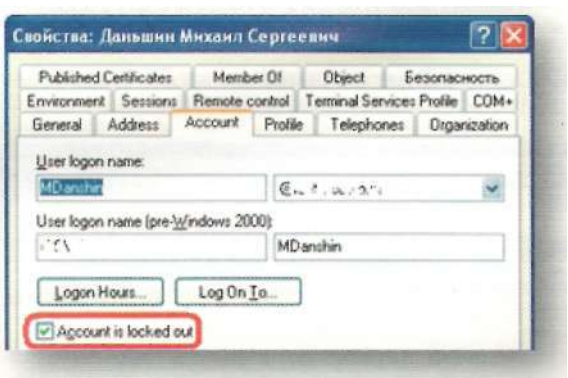


Рисунок 4. Account is locked out в свойствах пользователя



тера была предпринята попытка ввода неверного пароля. Конечно, есть способ реагировать на событие немедленно. Я писал о нем в статье «Как отреагировать на событие?» [1].

Если вы отслеживаете появления подобных записей и своевременно реагируете на них, то определить источник проблемы будет просто. Но, как правило, таких записей может быть огромное множество. И никто не реагирует на них немедленно, а расследует инцеденты потом.

Пользователи часто ошибаются с вводом пароля. И не существует простого способа определить точное время того, когда акаунт был заблокирован. Как правило, мы узнаем об этом через некоторое время от самого пользователя.

В решении проблемы нам может помочь утилита Microsoft Account Lockout Status, которая входит в пакет утилит Account Lockout and Management Tools. Получить этот пакет можно на сайте Microsoft3. Утилита была выпущена еще в 2003 году. Удивительно, что спустя много лет она все еще востребована.

Принцип работы утилиты заключается в том, что она анализирует журналы событий на всех контроллерах домена в сети и определяет, на каком контроллере произошла блокировка, в какое время, а также предоставляет дополнительную информацию, которая может помочь нам в расследовании.

Также утилита может помочь снять блокировку с учетной записи и многое другое.

Чтобы приступить к работе с утилитой, вам нужно запустить файл LockoutStatus.exe. Когда программа запустится, выберите меню File, а затем Select Target. В появившемся диалоговом окне (см. рис. 6) в поле Target User Name введите имя пользователя, у которого возникает проблема с учетной записью, а в поле Target Domain Name введите имя домена, в котором находится учетная запись пользователя.

Обратите внимание на галочку - Use Alternate Credentials. В случае если программа запущена с правами обычного пользователя, то, установив эту галочку, вы можете запустить проверку от имени другого пользователя, входящего в группу «Администраторы домена». Если же вы запустили программу от имени пользователя с правами доменного администратора, то устанавливать галку не нужно.

Рисунок 5. Вид сообщения из «Журнала Событий»

Рисунок 6. Окно ввода данных о пользователе, учетная запись которого блокируется

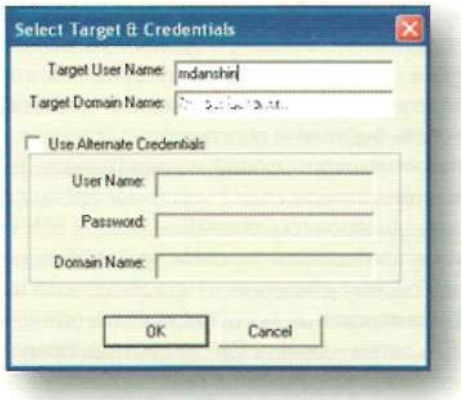


Рисунок 7. Результат работы программы

Рисунок 8. Снимаем блокировку с учетной записи

После непродолжительного процесса сбора информации вы увидите результаты работы, в которых будет отражено, на каком контроллере домена была заблокирована запись, в какое время, сколько попыток ввода неверного пароля было предпринято и т.д. Все это показано на рис. 7.

Из меню этой же программы вы можете снять блокировку с учетной записи. Для этого выберите контроллер домена, нажмите правую кнопку мыши и в контекстном меню выбирите Unlock Account (см. рис. 8).

Это изменение моментально будет реплицировано на все контроллеры домена, и пользователь может тут же повторить попытку входа. Если пользователь забыл пароль, то, выбрав Reset User's Password, вы можете его сменить.

Иногда возникают ситуации, когда после удачного входа в систему проблема возвращается. Пользователь не может получить доступ к сетевому ресурсу, не может повторно войти в систему и т.д. Причин такого поведения может быть несколько. Я приведу лишь несколько самых популярных из них. Но помните, что универсального решения нет и каждый случай нужно расследовать индивидуально.

Например, в сети может действовать злоумышленник, который пытается подобрать пароль от учетной записи пользователя.

Второй распространенный вариант - это использование одной учетной записи несколькими пользователями одновременно. В этом случае кто-то может постоянно вводить неверный пароль и тем самым мешать работе остальных пользователей.

Начиная расследование, первое, что мы должны установить, - это точное время происшествия. Установив время, мы легко сможем найти запись в журнале безопасности и понять, с какого компьютера в сети производились попытки ввода неверного пароля.

Как видно на рис. 7, программа сообщает нам эти сведения. Надо щелкнуть правой кнопки мыши по контроллеру домена и выбрать в контекстном меню Open Event Viewer (открыть журнал событий). Так как мы теперь знаем точное время, когда была попытка входа, которая привела к блокировке учетной записи, мы без труда сможем найти событие и определить, с какого компьютера было произведено действие, повлекшее блокировку. Проблема решена - виновные наказаны!

Но кроме человеческого фактора, есть еще и другие причины. Пожалуй, самая распространенная причина-это когда вы настраиваете «Назначенное Задание», которое выполняется от имени пользователя, затем меняете пароль этого пользователя, а ваше задание все еще пытается выполнить вход со старым паролем. Естественно, у него это не получается, и акаунт блокируется.

Надеюсь, что после прочтения этой статьи у вас появилась ясность, чем может быть вызвана обозначенная в начале статьи проблема и как ее решить. EOF

1. http://www.danshin.ms/2008/06/blog-post.html.
2. http://www.microsoft.com/downloads/detaiis.aspx?displaylang=en&familyid=7af2e69c-91f3-4e63-8629-b999adde0b9e.

Визитка

МАКСИМ БОЧКИН, и.о. ИТ-директора Управляющей компании АИН. Активно изучает Linux/UNIX ПО. Имеет несколько собственных проектов по переходу (внедрению! компании на ПО Open Source. Любимая ОС - GNUVunux Debian

Больше, чем почта

Zimbra Collaboration Suite Б.0

Основой для обеспечения электронного документооборота служит корпоративный почтовый сервер. Но иметь просто сервер с почтовыми службами в наше время мало

Гораздо удобнее, когда в компании есть средство для организации коллективной работы. Общая почта, задачи и календари - это малая часть того, что можно сделать. А главное, быстро и совершенно бесплатно. Я опишу, как организовать сервер коллективного документооборота на Zimbra Collaboration Suite 6.0.

Почему именно Zimbra?

- Сервер легко развернуть, а также управлять им.
- Разработан с использованием Open Source (Linux, Apache Tomcat, Postfix MTA, MySQL, OpenLDAP и т.д.).
- Используются стандартные открытые протоколы (SMTP, LMTP, SOAP, XML, IMAP, POP, iCal, CalDAV).
- Имеется бесплатная версия.
- Имеет общие календари, задачи, удобный мессенджер, а также систему общего доступа.
- Мощная система плагинов (Zimlet). Плагины разрабатываются сообществом Zimbra, а также самими пользователями (необходимы знания XML и Java).
- Веб-интерфейс к почте. Можно обеспечить доступ к своему ящику с любой точки мира и почти с любой операционной системы (версии: AJAX, Html, Mobile).
- Возможна интеграция с Active Directory.
- Взаимодействие с Microsoft Exchange Server.
- Антивирусная/антиспамная защита прямо «из коробки» (ClamAV, SpamAssassin и другие).
- Существует свой собственный стационарный клиент для работы с почтой, даже в офлайн-режиме (версия для Windows, Linux, MacOS), а также мини-агент (Toaster).

Сервер Zimbra Collaboration Suite можно развернуть на большинстве Linux-систем, также имеются версия для MacOS и версия для разработчиков.

Установка ZCS на Debian Etch

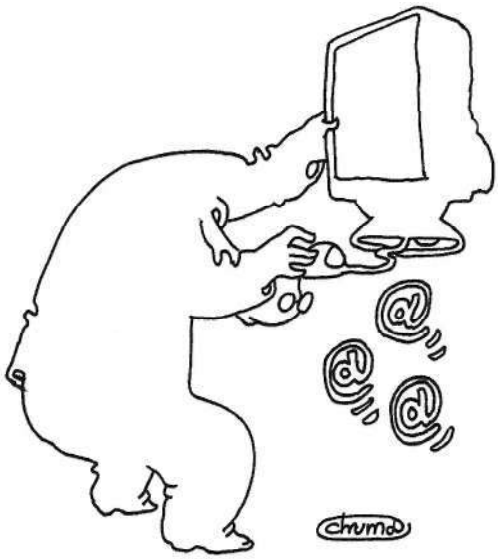
2 сентября 2009 года вышла 6.0 версия Zimbra Collaboration Suite (далее - ZCS). Сервер получил кодовое название в честь одной из рок-групп 80-х годов Guns'N'Roses. Дан-

Рисунок 1. Таблица мапинга портов в ZCS

Table 1 Zimbra Port Mapping

	Port
Remote Queue Manager	22
Postfix	25
HTTP	80
POP3	110
IMAP	143
LDAP	389
HTTPS	443
Mailboxd IMAP SSL	993
Mailboxd POP SSL	995
Mailboxd LMTP	7025

Рисунок 2. Раздел администратора ZCS



Хотелось бы отметить работу Zimbra в корпоративной среде. У него есть **практически весь функционал MS Exchange**

ная сборка официально стала поддерживать инсталляцию на Debian Lenny, но, к сожалению, как говорят в сообществе, сборка для Debian 5 пока ещё активно не тестировалась и содержит ряд мелких неисправностей (на момент написания статьи). Поэтому целесообразнее будет поставить ZCS на Debian Etch.

Перед установкой очень важно убедиться, что ваш DNS-сервер правильно сконфигурирован и доменное имя имеет MX и A. Zimbra проверяет это перед установкой.

Также рекомендую при разметке диска учесть, что всё программное обеспечение, почтовые ящики, системные настройки и прочие данные Zimbra хранит в /opt, советую выделить под этот раздел приличное пространство.

Для начала подготовим сам сервер.

Необходимо удалить устанавливаемый по умолчанию в Debian почтовый агент Exim:

```
apt-get remove --purge exim4 exim4-base exim4-config ↵
        exim4-daemon-light
```

А также поставить пакеты, которые использует ZCS:

```
apt-get install libc6-i686 sudo libidn11 curl fetchmail ↵
        libgmp3c2 libexpat1 libgetopt-mixed-perl libxml2 ↵
        libstdc++6 libpcre3 libltdl3
```

Теперь всё готово к установке непосредственно ZCS-сервера. Сам процесс занимает не более 10 минут, без учёта загрузки архива самого сервера. Переходим на сайт Zimbra для закачки свежей версии - http://www.zimbra.com/community/downloads.html. Находим в платформах Debian 4, копируем ссылку на архив и закачиваем на нашем сервере, используя wget. По окончании загрузки необходимо извлечь архив:

```
cd /tmp
wget http://h.yimg.com/lo/downloads/6.0.0_GA/ ↵
        zcs-6.0.0_GA_1802.DEBIAN4.0.20090830152935.tgz
tar xvf zcs-6.0.0_GA_1802.DEBIAN4.0.20090830152935.tgz
```

Теперь можно перейти в директорию, куда мы извлекли архив с ZCS, и запустить скрипт установки.

Рисунок 3. Настройки класса обслуживания

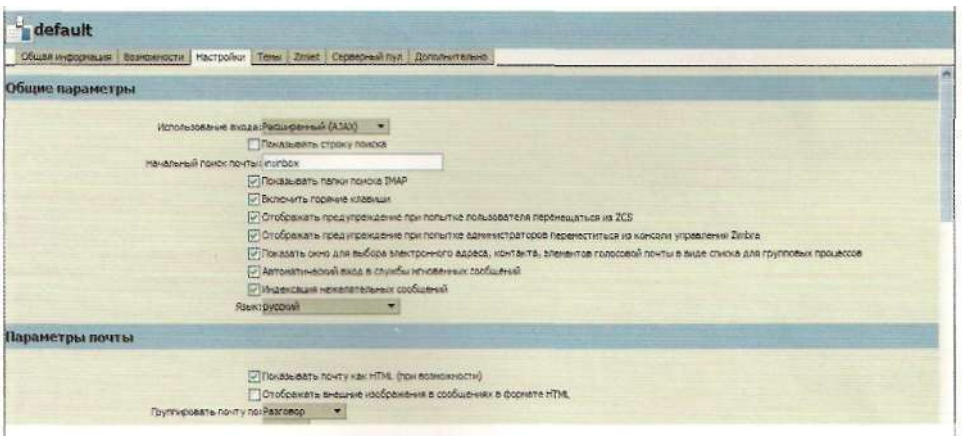


Рисунок 4. Включённые службы сервера

```
cd  zcs-6.0.0_GA_1802.DEBIAN4.0.20090830152935
./install.sh
```

После просмотра лицензий и проверки всех необходимых дополнительно установленных пакетов нам нужно сделать выбор служб для инсталляции. Обычно это все имеющиеся службы, кроме proxy и memcached.

```
Install zimbra-ldap [Y] Y
Install zimbra-logger [Y] Y
Install zimbra-mta [Y] Y
Install zimbra-snmp [Y] Y
Install zimbra-store [Y] Y
Install zimbra-apache [Y] Y
Install zimbra-spell [Y] Y
Install zimbra-memcached [N] N
Install zimbra-proxy [N] N
```

После этого начнётся установка deb-пакетов выбранных компонентов, а также частичная перенастройка всей системы в целом. Крайне рекомендую в консольном меню (раздел 3) после инсталляции сменить пароль администратора и ознакомиться со всеми использующимися в Zimbra портами, их не так уж много (см. рис. 1).

Настройка

Этап базовой настройки Zimbra в целом несложен и проходит в тёплой и уютной обстановке удобного веб-интерфейса. В него можно зайти через SSL порт 7071. (к примеру https://vash-domen:7071) (см. рис. 2).

Для начала необходимо подредактировать уже имеющийся класс обслуживания. Это некая групповая политика для почтовых ящиков, позволяющая тонко настраивать буквально каждый параметр пользователя. Используя настройки класса, можно хорошо выиграть время при развёртывании почтового сервера, просто выставив один раз настройки для всех почтовых ящиков (см. рис. 3).

Также будет полезно заглянуть в разделы «Домены», «Серверы» и «Глобальные настройки». Там содержатся более глубокие настройки сервера, такие как: проверка подлинности, Gal, настройки почтовых протоколов и программ для защиты от вирусов и спама.

Важно знать, что настройки сервера имеют приоритет перед глобальными настройками (см. рис. 4).

После всех операций приступайте к созданию учётных записей пользователей. Имеются два варианта создания.

Рисунок 5. Раздел мониторинга дисков

Рисунок 6. Почтовый веб-клиент

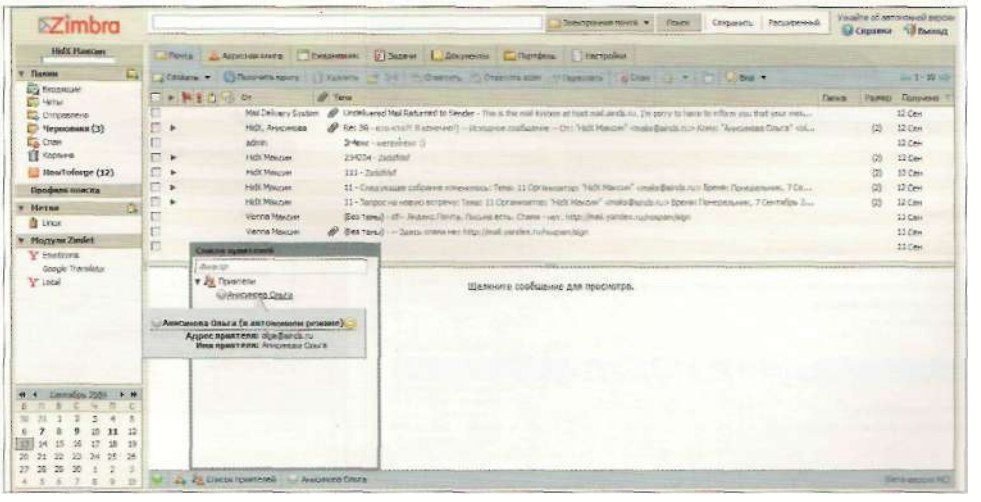
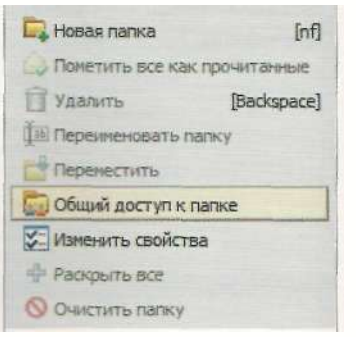


Рисунок 7. Общий доступ



Во-первых, пользователей можно создавать по отдельности, через удобный мастер. Тут в принципе вопросов не должно возникать, всё очень даже понятно и просто. Во-вторых, можно использовать массовую загрузку.

Для массовой загрузки учётных записей необходимо подготовить cvs файл. Каждая строка в файле представляет одну учетную запись. Она должна состоять из трех столбцов, разделенных запятыми (,) и содержащих имя учетной записи, экранное имя и пароль. Пример:

```
user@domain.ru,Максим,password
```

Если пароль не будет задан, то учётной записи выдаётся «случайный пароль». При первом входе в систему пользователь будет должен сменить пароль.

Для удобства рекомендую использовать Excel.

Что в итоге?

А в итоге мы с вами получили отличный почтовый сервер для совместной работы как внутри компании, так и снаружи. Вообще, хотелось бы отметить работу Zimbra CS в корпоративной среде. У сервера, который мы установили, есть практически весь функционал MS Exchange.

С точки зрения администрирования вы получаете мощный интерфейс управления всеми службами почтового сервера, а также встроенные средства диагностики и настройки на консольном уровне (см. рис. 5).

С точки зрения пользователя - приятный глазу интерфейс, общие календари, задачи и даже мини-мессенджер. Функционал совместной работы в Zimbra реализован хорошо.

Из собственного опыта могу сказать, что сейчас сервер с ZCS у меня обслуживает порядка 200 пользователей, которые регулярно используют не только почту, но и средства коллективной работы (общие календари, документы и задачи). Также в помощь пользователям я установил несколько zimlet-модулей, такие как переводчик текста/писем и wiki-поиск. Особых претензий к ZCS у меня нет. Сервер работает вполне стабильно и сообщает обо всех неисправностях своими ежедневными отчётами (см. рис. 6, 7).

Казалось бы, «идеальный почтовый сервер»? Но знаете, почему-то я не могу сказать так про Zimbra CS 6. Несмотря на её достоинства и плюсы, есть несколько мелких минусов.

Из основных недоработок можно отметить периодические проблемы с кодировкой и службой статистики сервера. Также есть несколько претензий к русскому переводу, к отображению «админки» в Internet Explorer 8.

Весь список недоработок можно найти на странице разработки Zimbra (http://pm.zimbra.com). Разработчики обещали исправить все недочёты в версиях 6.0.1 и 6.0.2. Будем надеяться, что так оно и будет.

Дерзайте! EOF

1. Сайт проекта Zimbra - http://www.zimbra.com.
2. Страница Wiki - http://wiki.zimbra.com/index.php?title=Main_Page.
3. Форум проекта Zimbra - http://www.zimbra.com/forums.
4. Спецификация версий ZCS - http://www.zimbra.com/products/product_editions.html,
5. Демо-версия веб-клиента - http://www.testzimbra.com/zimbraDemo/public/ValidateDemoCreation.jsp.

Визитка

ВЛАДИМИР ЗАКЛЯКОВ, инженер, экономист, советник налоговой службы 2-го ранга

А нужен ли банкам Linux?

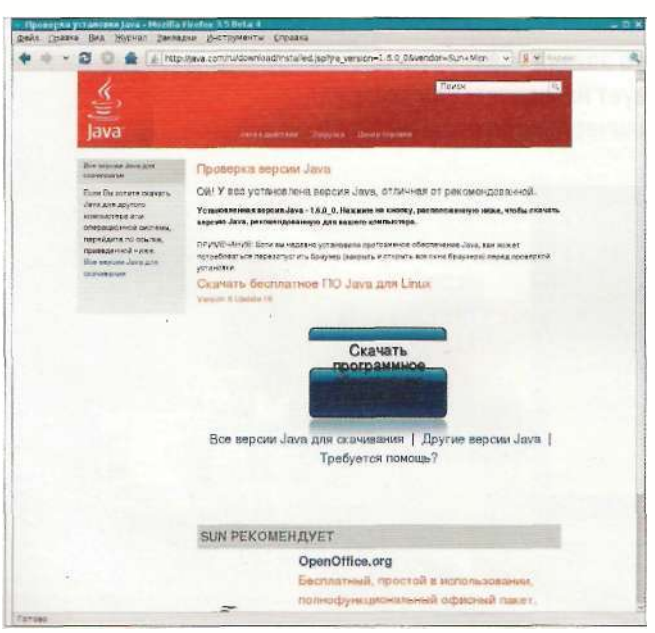
Как правильно запустить банк-клиент iBank 2

Вы думаете найти в статье ответ на поставленный вопрос? Частично его найдёте, но по большей части предстоит ответить самостоятельно. Именно ваше мнение может изменить ход истории

Чтобы быть хорошим человеком, следует совершать благие дела постоянно. Так и с программным обеспечением: создав кросс-платформенный продукт, важно не только его выпустить в свет, но и поддерживать. Так о чём же будет статья? О жизни и о банковских технологиях.

Сегодня многие бухгалтеры идут в ногу со временем и предпочитают работать с корпоративными банковскими счетами удалённо в режиме on-line. Технологии позволяют в течение банковского дня совершать операции по счёту, а также видеть их историю и знать остаток 24 часа в сутки 7 дней в неделю без участия сотрудников банка. Несомненно, это плюс, но есть ли единые пользовательские стандарты в этой сфере? Увы, нет, и виной тому безопасность. Из-за конкуренции банки не доверяют друг другу, не видят смысла договариваться, и поэтому техническое исполнение от одного банка к другому сильно варьируется. Подчас используются не только разные программные продукты, но и аппаратные.

Рисунок 1. Альтернативная версия Java не работает с банк-клиентом



Видно, что проблема находится за пределами интересов конкретных банков, поэтому решение её будет извне, либо централизованно через изменения в законодательстве, то есть придёт «сверху», либо жизнь со временем расставит всё на свои места, то есть «снизу».

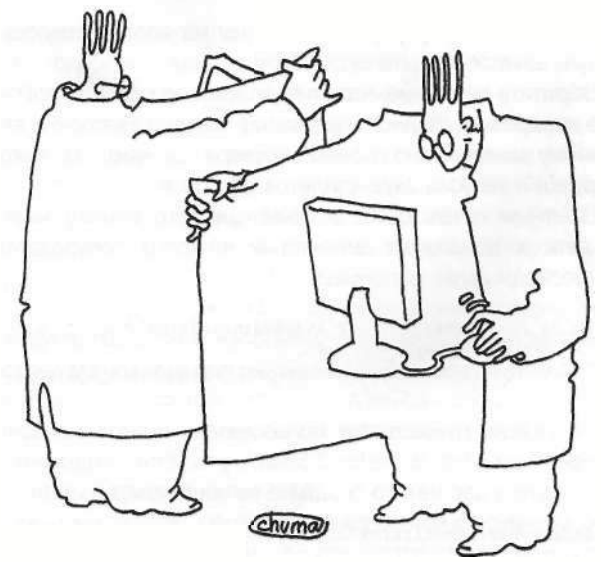
Возможно, попытку в решении проблемы «снизу» предприняла фирма «БИФИТ» [1], основное направление деятельности которой - разработка, внедрение и сопровождение программного обеспечения для электронного банкинга - системы iBank 2. Этот коммерческий продукт предлагается для продажи банкам, а те в свою очередь, купив этот продукт, делают выбор за своих клиентов. Не знаю, то ли случайно, то ли подумав на будущее, в качестве основы системы iBank 2 была выбрана среда Java. Использование Java позволило создать кросс-платформенное приложение, не привязанное к операционной системе на стороне клиента, но в то же время породило ряд проблем, связанных с поддержкой.

С одной стороны, клиентам не навязывается выбор ОС Windows, Linux или Solaris, с другой - поддержка ни одной платформы не осуществляется на должном уровне.

Если бы не один случай из жизни, возможно, не было бы этой статьи. В одной фирме до поры до времени использовался Java-клиент для ОС Windows, но случилось так, что сначала в стране были майские праздники, а в фирме вынужденные отпуска, потом смена кадров, а уже в июне выяснилось, что система перестала работать.

Сложно определить дату и точную причину, почему это произошло: то ли в банке что-то поменяли, то ли клиент обновил у себя OpenOffice (и, как следствие, обновилась Java), то ли установили очередное исправление на операционную систему... Но загруженное Java-приложение от банка после выбора файла ключей на стороне клиента начало переводить компьютер в состояние BSOD с перезагрузкой.

Долгая переписка с технической поддержкой банка затянулась на месяцы. Поставьте то, попробуйте это, при-



Многие бухгалтеры предпочитают работать с корпоративными банковскими счетами **удалённо в режиме on-line**

шлите вывод msinfo32, а за одно и файлы minidump-а..., а в конце очередной ответ «... причина перезагрузки пока неизвестна».

Первые несколько дней простоя в работе бухгалтерии привели к тому, что проблема через руководство вернулась в технический отдел, где было принято решение: пока не будет устранена проблема с Windows, «пересадить» несговорчивую бухгалтерию вместе с неработающим банк-клиентом iBank 2 под Linux. Учитывая, что практика запуска клиента iBank 2 в фирме ранее имелась, а запуск других приложений вроде «1С» под Linux не раз обсуждался на форумах и страницах журнала, долго ждать не пришлось. В почте быстро нашлось письмо от бывшего ИнвестСберБанка (сейчас ОТП-Банк) с инструкциями по установке и файлом криптобиблиотеки libibank2agava.so. Переустановка операционной системы и профильного программного обеспечения в отделе бухгалтерии из непосильной задачи стала делом техники.

Установка банк-клиента iBank 2 под Linux (32-бит)

Замечание: Данное руководство не является рекламой конкретного решения, наоборот, освещаются проблемы и нерешённые вопросы. Возможно, используемая методика будет интересна с целью переноса применяемых методов к другим программным продуктам, использующим Java.

Присланная ранее инструкция была неточной и неполной, поэтому привожу полную последовательность действий по запуску iBank 2-клиента под Linux со своими комментариями. В качестве рабочего дистрибутива был выбран уже использующийся на фирме Linux Fedora 11 (i386).

Для работы клиента требуется браузер с поддержкой Java. В качестве браузера мы выбрали используемый по умолчанию Firefox 3.5, а поддержку Java можно выполнить несколькими способами [1]. Наиболее простой и быстрый - это установка пакета Java-1.6.0-openjdk-plugin через:

```
# rpm -ihv ↵
   java-1.6.0-openjdk-plugin-1.6.0.0-22.b16.fc11.i586.rpm ↵
   java-1.6.0-openjdk-1.6.0.0-22.b16.fc11.i586.rpm
```

или:

```
# yum install java-1.6.0-openjdk-plugin
```

Но, увы, почему-то работать с этой версией банк-клиент не хочет. При первом же обращении в ОТП-Банк за помощью там предложили проверить версию на сайте Java.com, а после озвучивания увиденного (см. рис. 1) настоятельно посоветовали использовать версию Java от Sun Microsystems. В связи с этим пришлось удалить установленный пакет командой:

```
# yum remove java-1.6.0-openjdk-plugin
```

или:

```
# rpm -ihv м
    java-1.6.0-openjdk-plugin-1.6.0.0-22.b16.fc11.i586.rpm
```

Уточнить имя пакета можно с помощью команды:

```
# rpm -qa|grep java
```

Далее заходим на сайт Java.com [3] или [4] и скачиваем последнюю версию Java Runtime Environment (Linux RPM, самораспаковывающийся файл). В то время, когда писалась

статья, это был файл jre-6u16-linux-i586-rpm.bin. Инструкцию по загрузке и установке исполнительной среды Java в Linux можно найти в [5].

Скачанному bash-файлу необходимо передать управление либо как:

```
#chmod +x jre-6u16-linux-i586-rpm.bin
#./jre-6u16-linux-i586-rpm.bin
```

либо:

```
#sh jre-6u16-linux-i586-rpm.bin
```

На консоли будет отображено лицензионное соглашение, которое следует прочитать, пролистав до самого конца. Для чтения следующей строки нажимайте клавишу «пробел». Чтобы завершить установку, после прочтения вам придётся подтвердить соглашение, набрав yes и нажав <Enter>. В рабочей директории будет создан rpm-файл,

```
Do you agree to the above license terms? [yes or no] yes
Unpacking...
Checksumming...
Extracting...
UnZipSFX 5.50 of 17 February 2002, by Info-ZIP
(Zip-Bugs@lists.wku.edu).
  inflating: jre-6u16-linux-i586.rpm
Подготовка...      ########################################### [100%]
   1:jre           ########################################### [100%]
Unpacking JAR files...
        rt.jar...
        jsse.jar...
        charsets.jar...
        localedata.jar...
        plugin.jar...
        javaws.jar...
        deploy.jar...

Done.
```

После установки среды Java необходимо установить модуль для браузера, то есть создать мягкую ссылку в директории, где браузер ищет плагины на соответствующий модуль Java.

Обратите внимание, что следует именно сделать ссылку, а не копировать файл. Копирование приведёт к сбою и аварийному завершению работы браузера при каждой попытке загрузки и запуска Java-апплетов [6].

Опытным путём было установлено, что ссылку можно создать в домашней директории каждого пользователя (—/.mozilla/plugins), например:

```
$ ln -s /usr/java/jre1.6.0_16/plugin/i386/ns7/ ↵
        libjavaplugin_oji.so ↵
        /home/buh/.mozilla/plugins/libjavaplugin_oji.so
```

или согласно руководству пользователя централизованно в директории /usr/lib/firefox-3.5b4/plugins. Если поддиректории plugins у вас нет, то создайте её командой:

```
# mkdir /usr/lib/firefox-3.5b4/plugins
```

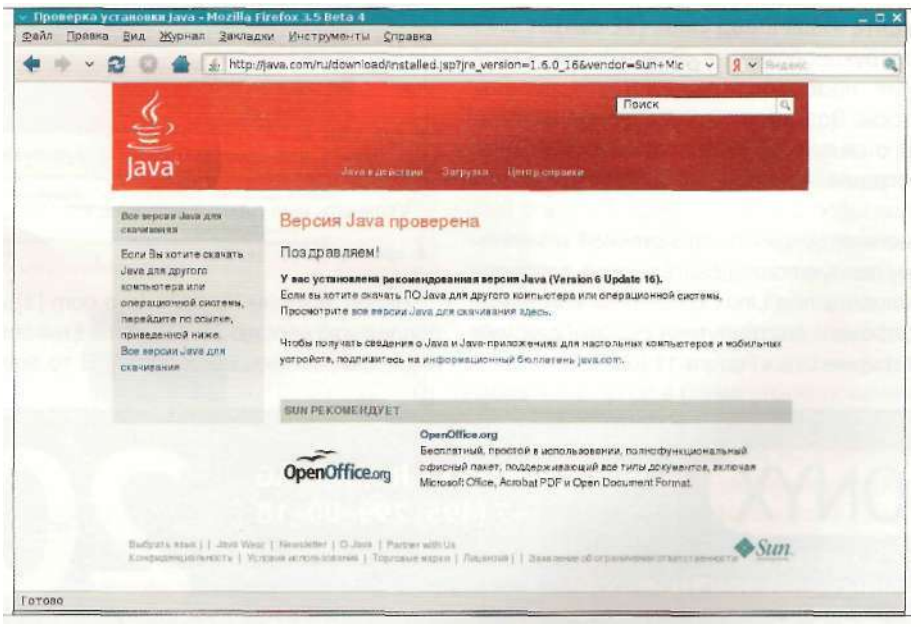
Директория /usr/lib/firefox-3.5b4 должна у вас уже быть. При необходимости внесите коррективы, указав используемую вами версию браузера. Затем создайте ссылку:

```
# ln -s /usr/java/jre1.6.0_16/plugin/i386/ns7/ ↵
        libjavaplugin_oji.so ↵
        /usr/lib/firefox-3.5b4/plugins/libjavaplugin_oji.so
```

После установки модуля перезапустите браузер, зайдите на сайт Java.com и проверьте версию. В случае успеха вы увидите примерно следующую картинку (см. рис. 2).

Замечание: если вам по каким-то причинам необходимо использовать пакет OpenJDK, идущий по умолчанию с операционной системой и удалённый нами в начале этого раздела, то рекомендую использовать alternatives. (Идёт в составе пакета chkconfig.) Данная программа была создана на основе идеи аналогичной утилиты из дистрибутива Debian и позволяет иметь несколько различных версий одного и того же программного обеспечения, помогая бы-

Рисунок 2. Проверка установки Java, установлена последняя рекомендованная версия



стро и удобно переключаться между ними с помощью ссылок. Подробнее, как это можно сделать, написано в [2].

После того как вы увидели надпись «У вас установлена рекомендованная версия Java» (см. рис. 2), с помощью браузера заходим на страницу банка https://ibank.isb.ru/iBank2 или https://ibank.tfbank.ru или https://212.57.108.118:444 (адрес получен 1 октября 2009 года от поддержки ТФ-Банка) и щёлкаем по изображению человечка «Обслуживание юридических лиц».

Далее у вас, скорее всего, откроется окно предупреждения безопасности с вопросом, доверяете ли вы загружаемому Java-апплету или нет. Жмём Run. В результате загрузки и запуска апплета должно появиться сообщение о том, что у вас не установлена криптобиблиотека (см. рис. 3).

Установка криптобиблиотеки

Далее вам следует обратиться в банк (или фирму «Бифит») и получить от него файл libibank2agava.so (размер файла 83105 байт). Что интересно, поисковая система Google среди первого десятка ссылок нашла этот файл в сети по адресу: ftp://ftp.masterbank.ru/pub/IBank2/crp/linux-i586/libibank2agava.so.

На поверку файл оказался идентичным, такой же файл был получен и от ИнвестСберБанка, ОТП-Банка и Банка торгового финансирования.

Файл следует скопировать в домашнюю директорию пользователя (определено опытным путём) либо в директорию /lib или любую другую, указанную в переменной, как рекомендуется банком:

```
java.library.path = /usr/java/jre1.6.0_16/lib/i386/ ↵
        client:/usr/java/jre1.6.0_16/lib/i386:/usr/lib/ ↵
        firefox-3.5b4:/usr/lib/firefox-3.5b4/plugins:/ ↵
        usr/lib/firefox-3.5b4:/usr/java/packages/lib/ ↵
        i386:/lib:/usr/lib
```

Значение переменной Java.library.path можно узнать с помощью Java-консоли.

Замечание: для того чтобы попасть в Java-консоль, следует выполнить любую из команд:

```
$/usr/java/jre1.6.0_16/bin/ControlPanel
```

или:

```
$/usr/java/jre1.6.0_16/bin/jcontrol
```

В появившемся окне (см. рис. 4) следует выбрать вкладку Advanced, а параметр Java console установить в Show console.

После загрузки любого Java-апплета вы увидите окно Java-консоли (см. рис. 5), где будет выводиться отладочная информация. Нажав на клавиатуре <S>, выбрав пункт s dump system and deployment properties, вы сможете увидеть все переменные и настройки.

После копирования криптобиблиотеки перезагрузите браузер и повторите вход на страницу банка. В случае успеха должно появиться окно выбора ключа шифрования, (см. рис. 6).

Если вы включали Java-консоль с отладочной информацией, её можно выключить. Вход в систему и проверку работы апплета можно осуществить с тестовым ключом. Взять его можно, например, тут: https://ibank.isb.ru/iBank2/test.dat, пароль 123123.

Что в итоге?

Дочитав до этих строк, половина из вас наверняка задастся вопросом, почему статья называется «А нужен ли банкам Linux?» А называется она так потому, что получить вышеописанную последовательность действий по установке от ранее упомянутых банков не предоставлялось возможным.

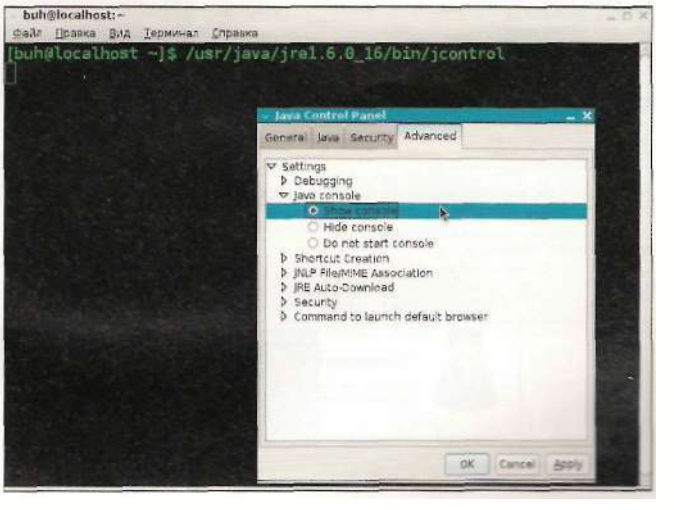
Руководство по установке банк-клиента iBank 2 под Linux пришлось написать самому. Что интересно, на этом проблемы по использованию интернет-банкинга в Linux не закончились, а лишь начались.

Если вы заметили, то был выбран 1386-дистрибутив. Жизнь не стоит на месте, почти всё новое «железо» 64-битное. Логично спросить: а как быть, если у вас x86_64-аппаратная платформа и аналогичный дистрибутив Linux? Решений много, но нет ни одного оптимального. Рассмотрим возможные варианты:

1. Установить 1386-дистрибутив и не использовать 64-битные возможности операционной системы.

Рисунок 3. Сообщение о том, что не установлено сертифицированное криптосредство

Рисунок 4. Включение показа Java-консоли



2. Установить x86_64-операционную систему, но i386-сборку браузера Firefox, отказавшись от 64-битных плагинов и некоторых возможностей браузера.

3. Установить nspluginwrapper [8], но он почему-то не желает работать с 32-битными плагинами Java, по крайней мере в файле /etc/sysconfig/nspluginwrapper можно увидеть следующее:

```
# List of plugins what are excluded from wrapping
# Names of plugins are separated by ':'
export IGNORE_WRAP="libtotem*:libjavaplugin*: ↵
       gecko-mediaplayer*:mplayerplug-in*:librhythmbox*"
```

4. Использовать wine или другие эмуляторы.

5. Установить 64-битную версию ОС, браузера и Java, запросив у фирмы «Бифит» 64-битную версию криптобиблиотеки.

Наиболее простым решением будут первый и второй варианты, третий и четвёртый будут более сложными и изощрёнными, пятый является наиболее правильным и перспективным, но фирма «Бифит» не считает данный путь востребованным.

Именно сейчас ваше мнение может изменить историю. Скажите своё слово на форуме журнала или напрямую фирме «Бифит», что вам ближе именно этот способ использования интернет-банкинга.

Так нужен ли банкам Linux?

Предполагаю, что ОТП Банку не нужен, в подтверждение данного вывода привожу цитату из переписки с технической поддержкой банка:

«Проблема в том, что нет 64-битных Java-плагинов для браузеров. Об этом можно получить информацию на сайте www.java.com. Грубо говоря, даже если будут криптобиблиотеки на 64 бита, то их негде будет использовать».

Это притом что 64-битная версия плагина Java уже стоит на моём компьютере. Выводы сделайте сами. На ваш выбор доступны как OpenJDK. так и Sun-версия. Не говоря уже о том, что можно вспомнить, с чего вообще началась эта история установки интернет-банкинга в Linux. А вашему банку и вашему бизнесу нужен Linux?

Поддержит ли Sun Java?

Просьбу о помощи с установкой Java можно отнести к SUN Microsystems, которым был задан вопрос на сайте Java (http://www.java.com/en/download/support.jsp) в разделе Consumer Java Feedback: «Как заставить работать i386 Java-плагин в браузере x86_64-сборки без замены последнего на i386-BepcnK>. Популярность и актуальность данного вопроса определяются числом отзывов (вопросов), так что спешите оставить своё сообщение! Если технология Java настолько перспективна, то резонно спросить: поддержит ли Sun пользователей Java в данном вопросе?

Подождём, посмотрим. Описание проблем и решений по использованию интернет-банкинга в 64-битных сборках Linux так и просится во вторую часть статьи.

Хотите присоединиться - пишите на форум журнала http://www.samag.ru/forum. БОТ

1. Фирма «Бифит» -http://www.bifit.ru.
2. Установка Java-плагина для Linux Fedora 10 - http://www.mjmwired.net/resources/mjm-fedora-f10.html#java.
3. Страница загрузки Java под Linux - http://Java.com/ru/download/linux_manual.jsp?locale=ru&host=java.com
4. Страница загрузки Java - http://java.sun.com/javase/downloads/index.jsp.
5. Инструкции по загрузке и установке исполнительной среды Java в Linux - http://iava.com/ru/download/help/5000010500.xml.
6. Mozilla Plugin Support on Linux (x86) - http://plugindoc.mozdev.org/linux.html#Java.
7. Плагин Java для Firefox-http://linuxforum.ru/index.php?s=d5a4997a7b1ac7ab41ed12dfa6a51f68&showtopic=60873&st=0&p=593491&#entry593491.
8. Nspluginwrapper is an Open Source compatibility plugin - http://gwenole.beauchesne.info/en/projects/nspluginwrapper.

Рисунок 5. Java-консоль

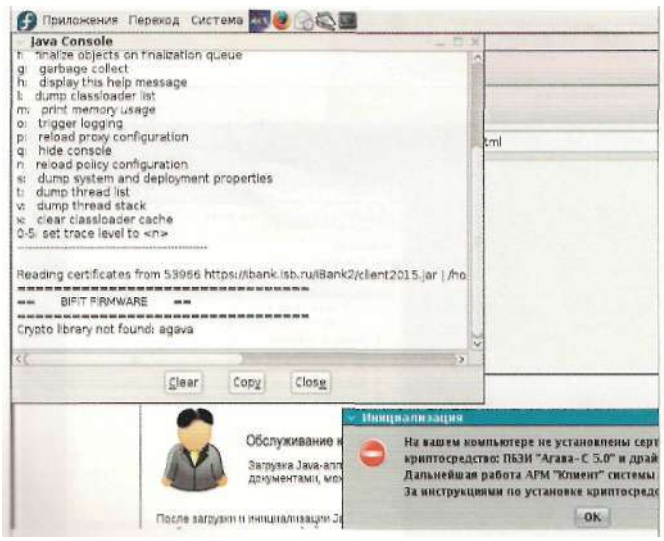


Рисунок 6. Окно выбора ключа шифрования, вход в систему интернет-банкинга

Визитка

НИКИТА ПАНОВ, работает в корпорации Microsoft техническим инженером, модерирует русскоязычный сектор портала TechNet, является лидером MCP-клуба в Воронеже. Любит преподавать и взаимодействовать с аудиторией

Черный экран тишины

Десять способов, как избавиться от него

Все началось с того, что мне понадобилось установить на рабочий ноутбук Windows Server 2008, чтобы смоделировать ситуацию для пользователя портала TechNet. Я решил это сделать дома

Уходя с работы, я перевел свою Vista Business в режим гибернации, как я обычно делаю. Как часто пишут в сводках «ничто не предвещало беды». Мой винт имеет 2 раздела - логических диска. Так что сервер я со спокойной душой установил на второй раздел. При первом же перезапуске выяснилось, что начисто «слетел» загрузчик! Нельзя сказать, что это такая уж нештатная ситуация - загрузчик довольно легко восстанавливается при помощи стандартного инструмента с recovery-диска (см. рис. 1).

Думаю, многим знаком этот скрин. Итак, с помощью пункта Startup Repair я стал восстанавливать загрузчик. На жестком диске были обнаружены обе установленные ОС, и я получил сообщение о том, что ошибки при загрузке Microsoft Vista были успешно исправлены.

Действительно, при перезагрузке я выбрал в меню необходимую мне ОС (Microsoft Vista), и загрузка началась. Сразу отмечу, что Windows Server 2008 после установки запускался абсолютно штатно.

Однако Microsoft Vista была «другого мнения», и я получил т.н. черный экран тишины. Думаю, есть пользователи, которые знакомы с этим понятием. Иллюстрировать его я не считаю нужным, ибо достаточно просто представить черный экран и курсор мыши.

Компьютер ни на что не реагировал: не открывался диспетчер задач, не срабатывали сочетания «горячих» клавиш - очень тихо и страшно. Поскольку я не лыком шитый, то принял решение восстанавливать Microsoft Vista до последнего.

Далее приведу способы восстановления, которые я успел найти за три дня упорных попыток восстановить работоспособность ОС, а не переустанавливать её, как делают очень многие.

Примечание: попытки загрузить систему в различных формах Safe Mode приводили точно к такому же «экрану тишины». Откат к последней рабочей конфигурации также не помог.

Рисунок 1. Загрузочное меню System Recovery

Рисунок 2. Диспетчер задач Windows Vista

Компьютер ни на что не реагировал: не открывался диспетчер задач, не срабатывали сочетания «горячих» клавиш — **очень тихо и страшно**

Способ номер «раз»

Когда я начинал поиски ответов, то даже не догадывался о том количестве пользователей, которые пострадали от такой напасти. И еще меня поразило то, насколько люди, попавшие в одинаковое положение, способны к взаимопомощи.

Итак, самый частый и первый способ восстановления, который я обнаружил, это попытаться запустить процесс explorer.exe вручную, используя диспетчер задач. Напомню, что в Microsoft Vista он открывается сочетанием <Ctrl> + <Shift> + <Esc>. Далее в диспетчере задач нужно выбрать меню «Файл -> Новая задача» и ввести explorer.exe (см. рис. 2).

Существует достаточно много отзывов от пользователей, которые именно таким образом смогли инициировать загрузку рабочего стола. После чего проводились мероприятия по очистке компьютера от вредоносного ПО или вирусов (в которых чаще всего и кроется причина подобного сбоя). Либо если пользователь точно знает о том ПО, установка которого повлекла появление «черного экрана тишины», то данное ПО либо удаляется, либо отключается его запуск (если это служба) через msconfig.

Примечание: есть много сведений о том, что это могут быть драйвера к звуковому контроллеру или контроллеру Wi-Fi.

Способ номер два

Оговорюсь, что специально не привожу здесь способы восстановления с использованием резервных копий раздела либо Complete PC Restore, ибо у меня такой возможности не было. Но если у вас есть сохраненная точка восстановления и т.п., то в первую очередь нужно воспользоваться именно ею.

Второй способ подразумевает использование диска с установленной Windows PE. Необходимо с этого диска загрузиться и запустить редактор реестра: «Пуск -> Выполнить -» regedit».

Если у вас нет диска с Windows PE, то запустите консоль восстановления с вашего recovery-диска и выберите работу с командной строкой. Введите regedit.exe, и у вас откроется редактор реестра (см. рис. 3).

Далее нужно найти раздел HKLM и в меню «Файл» выбрать «Загрузить куст» (Load Hive). Затем вам необходимо зайти на ваш жесткий диск, где установлена Microsoft Vista, и пройти в %systemdrive%\Windows\System32\config. Именно тут хранится требуемый нам куст Software, который и нужно добавить.

При этом редактор спросит вас о том, под каким именем будет добавлен данный куст. Введите любое имя, например Vista_crash. Вы увидите, как в разделе HKLM добавился новый куст. По сути, это копия раздела Software из реестра испорченной Microsoft Vista.

В этом кусте вам нужно найти раздел \Microsoft\Windows NT\CurrentVersion\Winlogon. В правой части окна отобразится содержимое выбранной папки.

Обратите внимание на параметр Shell. По умолчанию там должно находиться значение explorer.exe. Если это не так, то вручную измените значение этого параметра на explorer.exe. На самом деле этот способ перекликается со способом номер «раз». Просто в данном случае мы делаем изменения для того, чтобы рабочий стол появлялся автоматически.

Теперь прокручиваем список вверх до названия нашего куста (Vista_crash), выделяем его и в меню «Файл» выбираем пункт «Выгрузить куст» (Unload Hive). Теперь можно перезагрузиться и проверить работоспособность.

Способ номер три

Этот способ я считаю самым необычным из тех, что нашел! Оказывается, нас может спасти «залипание клавиш»! Для этого предлагается на фоне «черного экрана тишины» 5 раз нажать на правый <Shift>. При этом появляется окно с предложением включить либо отключить данный сервис, но нас интересует ссылка в этом окне (см. рис. 4), при нажатии на которую запустится «Проводник»! Откуда мы можем запустить либо regedit, либо msconfig, чтобы отредактировать список автоматически стартующих программ и служб.

Способ номер четыре

Очень простой. Есть сообщения о том, что получить «черный экран тишины» можно, установив обновление KB915597. Поэтому просто воздержитесь от его установки. Или же в случае, если данное обновление уже установлено на ваш компьютер, просто удалите его. Как вариант - выполните «откат» к точке восстановления до установки данного обновления.

Способ номер пять

Кстати, возможна ситуация, когда ваш компьютер является членом домена и при запуске у вас выполняется ряд скриптов, например по подключению сетевых дисков, и т.п. При этом состояние очень напоминает подобный «экран тишины». Проконсультируйтесь с администратором вашей сети, возможно, вам нужно просто подождать, пока все скрипты при загрузке завершат свою работу.

Способ номер шесть

Еще один способ, связанный с реестром. Для этого вам необходимо выполнить способ номер два, но в папке %systemdrive%\Windows\System32\config выбрать для подключения куст System. После чего в подключенном кусте ищем папку CurrentControlSet и в ней подпапку Services\RpcSs, где проверяем параметр ObjectName. Он должен иметь значение NT AUTHORITYXNetworkService. Если значение другое, то вручную установите именно это значение. Не забудьте выгрузить куст!!!

Способ номер семь

Если на вашем компьютере установлен смарт-карт-ридер или просто карт-ридер, то попробуйте отключить его и перезагрузиться. Бывали случаи, что это возобновляло работу системы.

Способ номер восемь

Довольно спорный, но может помочь. Однако это вариант для случая, когда у вас осталась возможность запуска через Safe Mode. Есть мнение, что Microsoft Vista мешают запуститься «плохие» лог-файлы событий. Предлагается следующий способ. Запустите систему в Safe Mode, далее «Пуск -> Выполнить -» msconfig» выберите вкладку «Службы», в ней снимите галочку со службы «Журнал событий Windows» (Windows Event Log). После чего перезапуститесь в нормальном режиме.

Способ номер девять

Отключение учетной записи администратора. Применение опять-таки возможно в случае, когда у вас осталась возможность запуска через Safe Mode. Запустите систему, используя учетную запись администратора, зайдите в панель управления и выберите «Управление учетными записями». Нажмите на ссылку «ВключениеХотключение UAC» и отключите данную службу. Затем «Пуск -> Выполнить -» cmd», там набираем;

```
Net User administrator /active:no
```

Этим вы отключите учетную запись администратора. Перезагрузите компьютер.

Способ последний, официальный

To work around this problem, perform a clean installation or a parallel installation of Windows Vista (для решения этой проблемы выполните «чистую» установку Windows Vista, либо установите новую копию Windows Vista параллельно имеющейся) - http://support.microsoft.com/kb/946532.

***

От себя могу сообщить, что ни один из способов в моем случае не сработал. Пришлось пользоваться последним. Увы!

Однако очень много из способов, которые я вам описал, реально помогли людям. Возможно, моя проблема была связана именно с тем, что моя Microsoft Vista находилась в состоянии гибернации, когда я начал установку Windows Server 2008.

Последнее, что могу посоветовать, - регулярно создавайте резервные копии!!! EOF

Рисунок 3. Редактор реестра

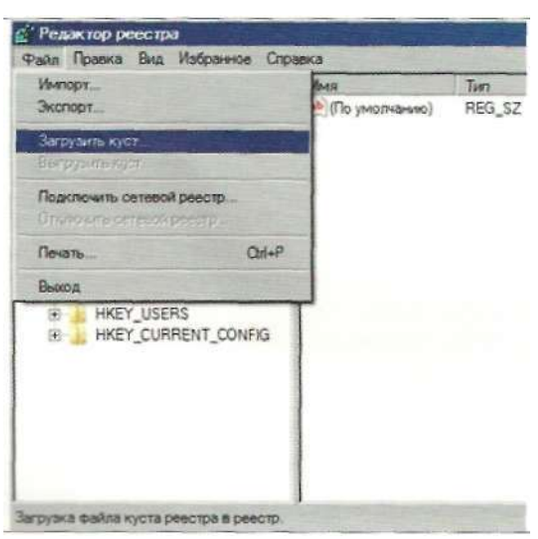
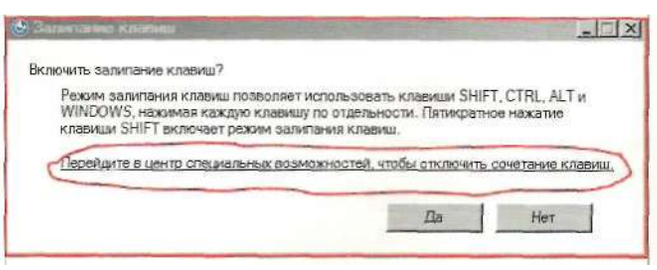


Рисунок 4. Диалоговое окно режима «залипания клавиш»



Визитка

ВИТАЛИЙ ВЕРЕЩАГИН, руководитель практики IBM Cognos компании ND Group

Управляем эффективностью компании

Акценты сместились, приоритеты уточнились

Любой кризис — это экономическая база, на которую можно будет опереться для последующего роста, потому что без падений не бывает роста

Неправильное решение ведет к потере бизнеса

Важно понимать, в каком состоянии будет компания, когда этот экономический рост возобновится, и каким образом с пользой для себя можно воспользоваться текущей ситуацией и открывшимися возможностями. Ответ лежит на поверхности: необходимо обратить внимание на качество оборотного капитала, выявить слабые управленческие звенья в структуре компании, понять, в каком направлении движется бизнес. Очевидно, что стратегические и тактические задачи, которые стояли перед компаниями до кризиса, с его приходом никуда не исчезли, а именно:

Эффективная работа с пулом существующих клиентов. Хорошо известно, что привлечение новых клиентов обходится компании в разы дороже, чем удержание имеющихся.

Грамотное управление продуктовым портфелем. Правило Парето применительно к этой тематике гласит, что 20% продуктового портфеля приносит 80% прибыли компании, а это значит, что надо сконцентрироваться на этих 20% наиболее прибыльных и эффективно работать с ними.

Повышение финансовой устойчивости компании. Необходимо четко понимать в различных сценариях, что для компании будет означать увеличение отсрочки по платежам с контрагентами и переход на предоплату с поставщиками, и, как результат, - работа по управлению кассовыми разрывами.

Оптимизация бизнес-процессов. Средняя эффективность работы в пересчете на единицу готовой продукции в России ниже в 3-5 раз, чем аналогичные показатели в странах Западной Европы, что дает большие возможности для повышения эффективности бизнес-процессов компании, с учетом имеющейся best practice по отраслям экономики.

Таким образом, ничто не отменяет целей компании в системном подходе к решению стоящих перед ней задач: всего лишь сместились акценты и уточнились приоритеты. В силу высокой динамики изменений рыночной ситуации существенно сократилось время на принятие решений и качественно возросла стоимость неправильного решения. Ошибка в таких условиях может означать потерю бизнеса, что мы наблюдали на примере ряда отечественных компаний в последнем полугодии.

«Магический квадрант» для реальной практики

Каким же образом решаются эти комплексные задачи на практике?

При классическом подходе задачи управления компанией группируются по трем уровням: операционный, управление эффективностью и стратегический (см. рис.1). На каждом из уровней исполнение задач поддерживается определенным классом ИТ-систем,

Уровень операционного управления поддерживает основные бизнес-процессы компании, и без его автоматизации деятельность предприятия существенно затруднена, а в отдельных случаях просто невозможна. Операционное управление, как правило, автоматизируется системами класса Enterprise Resource Planning (ERP), такими как SAP R/3, Oracle EBS, MS Dynamics AX, «1С» и т.д.

Уровень стратегического управления решает задачи стратегического планирования. ИТ-средства поддержки решения таких задач, как правило, имеют различные встроенные алгоритмы поиска оптимальных решений, например, наиболее эффективные алгоритмы генетической оптимизации. В качестве примеров таких нишевых продуктов можно привести PowerSim, iThink и т.д.

На уровне управления эффективностью решаются задачи финансового анализа, планирования и бюджетирования, построения управленческой и консолидированной финансовой отчетности по международным стандартам, управления ключевыми показателями деятельности. Концепция Corporate performance management (CPM по классификации Gartner), с помощью которой решаются задачи управления эффективностью, представляет собой набор методов и средств, позволяющих оптимизировать эффективность управления в компании. Технология реализации концепции

CPM на практике представляет собой автоматизацию бизнес-процессов компании, поддерживающих принятие решений на всех уровнях ее управления с применением специализированных ИТ-решений.

Существует ряд продуктов, с помощью которых успешно решаются задачи такого класса. Среди лидеров согласно отчету Gartner по рынку CPM «Magic Quadrant for Corporate Performance Management Suites» (см. рис. 2), датированному апрелем 2009 года, можно выделить три ключевых игрока, которые остаются в первом квадранте на протяжении последних лет (с учетом слияний и поглощений), это Oracle Hyperion, SAP (Business Object) и IBM Cognos Performance Management. Согласно тому же источнику большая тройка вендоров (Oracle, SAP, IBM) контролирует порядка 70% рынка CPM-решений, при этом предпосылки для существенного изменения ситуации отсутствуют.

Остановимся более подробно на IBM Cognos Performance Management - интегрированной платформе поддержки принятия решений, реализующей концепцию CPM.

Платформа IBM Cognos 8 Performance Management построена на основе открытой сервисно-ориентированной (SOA) веб-архитектуре, представляющей собой интеграционную основу для всех компонентов платформы. Использование такой архитектуры отвечает стратегии IBM Information on Demand и обеспечивает быстрое развертывание системы и широкие возможности для масштабирования решения, а также гарантирует заказчику совместимость с уже используемыми в компании бизнес-приложениями с открытым интерфейсом. Платформа IBM Cognos 8 Performance Management позволяет решать следующие задачи, критичные для бизнеса в любой ситуации:

моделирование и выбор оптимального управленческого решения в кратчайшие сроки: моделирование сценариев и вариантов оптимизации расходов, текущих активов, развитие новых направлений и т.д.;

- анализ «что если...»: многоверсионность сценариев развития событий, многомерность аналитического пространства, быстрое создание различных отчетов по брендам, бизнес-направлениям, подразделениям, продуктовым линейкам и т.д.;

прогнозирование на основе фактических данных: создание оптимистичного, пессимистичного и реалистичного прогнозов, гибкое построение бизнес-моделей и отчетов, интеграция с учетными системами;

планирование денежных потоков: расчет и сравнение инвестиционных проектов, варианты привлечения инвестиций, кредитов, прогнозирование дебиторской и кредиторской задолженностей и т.д.;

возможности финансового анализа, расчет всех необходимых показателей с помощью встроенных экономических функций.

взаимосвязь управленческих решений со стратегическими целями компании, которая планирует продолжать деятельность после кризиса;

Когда заказчик не прав

Зачастую приходится слышать следующие **тезисы при** обсуждении целесообразности внедрения аналитических решен:/ -га::; "'.' ~ <смпании:

> «Сейчас важно контролировать, а с анализом... **разберемся потом».**

> «У нас «сократили» инвестбюджеты, поэтому сейчас денег нет - вернемся к этому вопросу через год».

> «Ситуация сейчас слишком неопределенная, надо подождать полгода-год, пока все не прояснится, что делать и как v= -=::-£- ем - вот тогда и поговорим».

«У нас есть ERP-система, она все умеет, а ИТ-решения в области бизнес-аналитики -дело необязательное».

> «Есть MS Excel, у нас все пользователи на нем работают. Зачем нам нужен IBM Cognos?»

«У нас работают умные и талантливые люди, поэтому либо они разберутся во всем сами, либо им никакая система не поможет».

«На рынке появляются недорогие фрилансеры - они все сделают, что мы захотим, и будет в два раза дешевле».

«Быть бережливым - это прекращать все ИТ-проекты, а не ввязываться в новые».

Компании, которые не решили для себя все эти вопросы, существенно повышаю риск того, что когда придет время для роста, они будут к этому не готовы. Сэр Уинстон Черчилль говорил, что нужно «уже сегодня делать то, о чем другие будут думать завтра». Согласитесь, это хороший повод задуматься о том, где компания может оказаться уже в ближайшее время, если просто будет ждать «у моря погоды».

Рисунок 1. ИТ на различных уровнях управления компании

Рисунок 2. «Магический квадрант» для решений Corporate Performance Management (Gartner, апрель 2009)

быстрая экономическая отдача от внедрения системы.

Решение большинства задач при внедрении и использовании любых компонентов IBM Cognos 8 Performance Management, в том числе создание сложных параметрических отчетов и внесение изменений в плановые или консолидационные модели, осуществляется без программирования. Этот факт, а также открытость архитектуры IBM Cognos 8 и высокая степень интеграции компонент обеспечивают простоту внедрения и освоения платформы конечными бизнес-пользователями.

Что на выходе?

У нас, как у консультантов с большим проектным опытом, очень часто спрашивают:

- «А сколько людей мы сможем уволить после внедрения вашей системы?»
- «Все понятно, система хорошая, но вот только как быстро ваша система окупится?»

  «Покажите нам экономическую целесообразность внедрения, посчитайте TCO и R01»

В качестве примера бенефитов, которые компания может получить от внедрения системы класса Performance Management, можно привести проект в Группе Компаний Genser,

В компании поставили перед собой задачу автоматизировать систему репортинга в сжатые сроки, с учетом ограничений по бюджету и необходимости формирования входящего сальдо, то есть создание системы отчетности «с нуля». По результатам тендера для решения задач автоматизации консолидации по стандартам МСФО был выбран продукт IBM Cognos Controller. Проект внедрения длился порядка 2 месяцев до получения бета-версий консолидации за 2005-2006 гг. в новой системе, при этом настройка функционала системы производилась внутренним ресурсом компании с точечным привлечением экспертизы автора.

В результате успешного внедрения помимо повышения качества входных данных можно говорить о повышении эффективности подготовки отчетности, так как объемы бизнеса за 2008 год выросли на 70% (за 2007 год - в 2 раза), при этом скорость подготовки отчетности выросла, затраты на подготовку и аудит остались прежними. Таким образом, экономическая целесообразность проекта автоматизации, на наш взгляд, очевидна. EOF

Оцените преимущества

Все компоненты в рамках IBM Cognos 8 Performance Management полностью интегрированы между собой. ИТ-службы по достоинству оценят все преимущества столь тесной интеграции, это:

- централизованное администрирование через портал;
  единые средства безопасности;
  единая модель метаданных;
  единый пользовательский портал;
- унифицированный веб-ориентированный интерфейс.

На практике высокая степень интеграции позволяет, например, пользователю системы использовать в режиме реального времени результаты процесса планирования и финансовой консолидации для целей анализа или связать любой отслеживаемый показатель эффективности (KPI) с тем или иным отчетом.

Множественные уязвимости в Cisco IOS

Программа: Cisco IOS 12.x, R12.x; Cisco IOS XE 2.1.x, 2.2.x, 2.3.x. _

Опасность: Средняя.

Наличие эксплоита: Нет

Описание: 1. Уязвимость существует из-за ошибки в секции входа в функционале Extension Mobility компонента Cisco Unified CME (Communications Manager Express). Удаленный пользователь может с помощью специально сформированного HTTP-запроса вызвать переполнение буфера и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки в реализации IKE. Удаленный пользователь может потребить все доступные Phase 1 SA и предотвратить возможность установки новых IPSec-сессий. Для успешной эксплуатации уязвимости требуется, чтобы для аутентификации использовались IKE-сертификаты.

3. Уязвимость существует из-за множественных ошибок в реализации IP-туннелей при коммутации сетевых пакетов. Удаленный пользователь может с помощью специально сформированных пакетов вызвать перезагрузку устройства. Для успешной эксплуатации уязвимости устройство должно быть сконфигурировано для использования PPTP, GRE, IPinIP, Generic Packet Tunneling в IPv6, или IPv6 поверх IP-туннелей и Cisco Express Forwarding.

4. Уязвимость существует из-за ошибки в реализации Object Group для списков контроля доступа. Удаленный пользователь может обойти установленные политики доступа.

5. Уязвимость существует из-за ошибки в реализации H.323. Удаленный пользователь может с помощью специально сформированных TCP-пакетов вызвать перезагрузку устройства. Для успешной эксплуатации уязвимости H.323 должен быть включен (не является настройкой по умолчанию).

6. Уязвимость существует из-за ошибки в реализации SIP, относящейся к функционалу Cisco Unified Border Element. Удаленный пользователь может вызвать перезагрузку устройства.

7. Уязвимость существует из-за ошибки в функционалах SSLVPN, SSH и IKE Encrypted Nonce. Удаленный пользователь может вызвать перезагрузку устройства с помощью специально сформированных пакетов, отправленных на TCP порты 22 (SSH) и 443 (VPNSSL). и UDP-порты 500 или 4500 (IKE Encrypted Nonce).

8. Уязвимость существует из-за ошибки состояния операции в Authentication Proxy для HTTP(S), Web Authentication и Consent. Удаленный пользователь может обойти Authentication Proxy Services и страницу принятия соглашения при наличии аутентифицированной сессии или принятого соглашения.

9. Уязвимость существует из-за ошибки в функционале Cisco IOS Zone-Based Policy Firewall SIP Inspection. Удаленный пользователь может с помощью специально сформированного транзитного SIP-пакета вызвать перезагрузку устройства.

10. Уязвимость существует из-за ошибки в реализации NTPv4 при создании NTP-ответов. Удаленный пользователь может с помощью специально сформированного NTP-пакета вызвать перезагрузку устройства.

URL производителя: www.cisco.com

Решение: Установите исправление с сайта производителя.

Повышение привилегий в OpenSSH в Red Hat Linux

Программа: Red Hat Enterprise Linux (RHEL) 5.4.

Опасность: Низкая,

Наличие эксплоита: Нет.

Описание: Уязвимость существует из-за недостаточной проверки директорий, передаваемых через конфигурационную опцию ChrootDirectory. Локальный пользователь может с помощью специально сформированных жестких ссылок на setuid-приложения, использующие конфигурационные файлы внутри chroot директории, выполнить произвольные команды на системе с привилегиями другого пользователя.

URL производителя: www.redhat.com.

Решение: Установите исправление с сайта производителя.

Уязвимость при обработке XMM-исключений в OpenBSD

Программа: OpenBSD 4.4, 4.5 и 4.6, возможно, другие версии.

Опасность: Низкая

Наличие эксплоита: Нет

Описание: Уязвимость существует из-за ошибки при обработке XMM-исключений. Локальный пользователь может вызвать панику ядра системы на 1386-ядре.

URL производителя: www.openbsd.org.

Решение: Установите исправление с сайта производителя.

Уязвимость в реализации TCP в продуктах Check Point

Программа: Check Point VPN-1 Power NGX; Check Point VPN-1 UTM NGX: Check Point VPN-1/FireWall-1 VSX NG; Check Point Connectra Appliances.

Опасность: Низкая.

Наличие **эксплоита:** Нет.

Описание: Уязвимость существует из-за ошибок в реализации TCP при обработке ресурсов. Удаленный пользователь может потребить всю доступную память ядра и вызвать отказ в обслуживании.

URL производителя: www.checkpoint.com.

Решение: Установите исправление с сайта производителя.

Визитка

ДМИТРИЙ НЕСТЕРКИН, инженер, системный администратор ООО «Телисет-С», имеет сертификат Microsoft MCOST. Сфера интересов: сетевые технологии, программное обеспечение с открытым исходным кодом

Настройка интернет-шлюза

с авторизацией через AD по протоколу Kerberos

Едва ли есть организация, компьютерная сеть которой не имела бы собственного шлюза для доступа в Интернет. Различных решений здесь масса, я опишу то, которое было выбрано в нашей организации

Были поставлены следующие задачи:

- обеспечение безопасности сети посредством файервола;
- прокси-сервер для организации доступа пользователей в Интернет с возможностью контроля и учета доступа, запрета посещения сайтов согласно политике компании;
- интеграция с Active Directory;
- надежное и безопасное решение, не подверженное большинству угроз.

В результате мы пришли к следующей конфигурации ПО:

- Debian Lenny 5.0;
- Squid 2.7 STABLE3, аутентификация через Kerberos;
- Apache2 (для вывода страниц с сообщениями о запрете доступа);
- Rejik 3 для ограничения доступа к запрещенным сайтам.

Преимущества данного решения:

- как любая Linux-система, Debian мало подвержена вирусным атакам;
- гибко настраиваемый прокси-сервер, для которого доступны различные анализаторы логов и сторонние модули;
- Kerberos-аутентификация абсолютно прозрачна для пользователя и является одной из самых безопасных схем аутентификации.

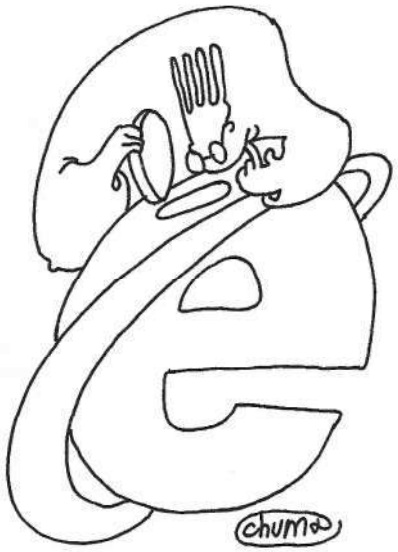
Немного устаревшая версия Squid выбрана из-за того, что она, по нашему опыту, максимально корректно работает с протоколом Kerberos. В Squid версии 3 модуль авторизации squid_kerb_auth на момент написания статьи отсутствовал.

Настройка

После этапа непосредственной установки операционной системы, описанного уже много раз, приступаем к конфигурированию.

Для упрощения настройки файервола был составлен следующий скрипт, автозапуск которого потом был прописан через rc-update:

```
#!/bin/sh
# Конфигурация внешнего интерфейса
INET_IP="11.22.33.44"
INET_IFACE="eth0"
INET_BROADCAST="255.255.255.0"
#
# Конфигурация внутреннего интерфейса
LAN_IP="192.168.100.253"
LAN_IP_RANGE="192.168.100.0/24"
LAN_IFACE="eth1"

# Конфигурация localhost
LO_IFACE="lo"
LO_IP="127.0.0.1"

# Конфигурация IPTables
IPT="/sbin/iptables"
# Номера непривилегированных  портов
NONPRIPORTS="1024:65535"
# Модули IPTables
/sbin/modprobe ip_tables
/sbin/modprobe ip_conntrack
/sbin/modprobe iptable_filter
/sbin/modprobe iptable_mangle
/sbin/modprobe iptable_nat
/sbin/modprobe ipt_LOG
/sbin/modprobe ipt_limit
/sbin/modprobe ipt_state
/sbin/modprobe ipt_REJECT

# Включаем форвардинг
echo "1" > /proc/sys/net/ipv4/ip_forward
/sbin/sysctl -w net.ipv4.ip_forward=1

# Сбрасываем правила и удаляем цепочки
$IPT -F
$IPT -X

# Политика по умолчанию
$IPT -P INPUT DROP
$IPT -P OUTPUT DROP
$IPT -P FORWARD ACCEPT

# Разрешаем прохождение любого трафика по loopback-интерфейсу
$IPT -A INPUT -i $LO_IFACE -j ACCEPT
$IPT -A OUTPUT -o $LO_IFACE -j ACCEPT

# Если интерфейс не loopback, то запрещаем входить в список
# его адресов
$IPT -A INPUT -s 127.0.0.1/255.0.0.0 ! -i $LO_IFACE -j DROP

# Отбрасываем все некорректно сформированные пакеты
$IPT -A INPUT   -m state --state INVALID -j DROP
$IPT -A FORWARD -m state --state INVALID -j DROP
```



Мы получили интернет-шлюз, **работающий прозрачно для пользователей и соответствующий всем требованиям**

```
# Принимаем все пакеты, принадлежащие уже установленным
# (ESTABLISHED) соединениям
$IPT -A INPUT   -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# Правила для внутренней сети
$IPT -A INPUT -p ALL -i $LAN_IFACE -s $LAN_IP_RANGE -j ACCEPT
$IPT -A OUTPUT -p ALL -o $LAN_IFACE -d $LAN_IP_RANGE -j ACCEPT
$IPT -A INPUT -p tcp -i $LAN_IFACE --dport 3128 -j ACCEPT

# Правила защиты от некоторых распространенных атак снаружи
# и изнутри сети(Внимание! Данные правила могут нарушить
# работу части прграмм и сервисов)
#SYN Flood
$IPT -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
$IPT -A OUTPUT -p tcp ! --syn -m state --state NEW -j DROP
#UDP Flood
$IPT -A INPUT -p UDP -i $INET_IFACE --dport 138 -j DROP
$IPT -A INPUT -p UDP -i INET_IFACE --dport 113 -j REJECT
$IPT -A INPUT -p UDP -i INET_IFACE --sport 67 --dport 68 ↵
       -j REJECT
$IPT -A INPUT -p UDP -j RETURN
$IPT -A OUTPUT -p UDP -o $INET_IFACE -j ACCEPT
#ICMP-перенаправление
$IPT -A INPUT --fragment -p ICMP -j DROP
$IPT -A OUTPUT --fragment -p ICMP -j DROP

# Разрешаем ICMP-соединение
$IPT -A INPUT -p icmp -m icmp -i $INET_IFACE --icmp-type ↵
       source-quench -j ACCEPT
$IPT -A OUTPUT -p icmp -m icmp -o $INET_IFACE --icmp-type ↵
       source-quench -j ACCEPT

# Разрешаем  ping и весь ICMP-трафик внутри нашей сети
$IPT -A INPUT -p icmp -m icmp -i $INET_IFACE --icmp-type ↵
       echo-reply -j ACCEPT
$IPT -A INPUT -p icmp -m icmp -i $LAN_IFACE -j ACCEPT
$IPT -A OUTPUT -p icmp -m icmp -o $INET_IFACE --icmp-type ↵
       echo-request -j ACCEPT
$IPT -A OUTPUT -p icmp -m icmp -o $LAN_IFACE -j ACCEPT
$IPT -A INPUT -p icmp -m icmp -i $INET_IFACE --icmp-type ↵
       echo-request -j ACCEPT
$IPT -A OUTPUT -p icmp -m icmp -o $INET_IFACE --icmp-type ↵
       echo-reply -j ACCEPT

# Разрешаем передачу пакета «некорректный параметр» -
# используется, если в заголовке пакета содержится
# недопустимая запись или CRC пакета не совпадает с указанной
$IPT -A INPUT -p icmp -m icmp -i $INET_IFACE --icmp-type ↵
       parameter-problem -j ACCEPT
$IPT -A OUTPUT -p icmp -m icmp -o $INET_IFACE --icmp-type ↵
       parameter-problem -j ACCEPT
```

```
# Разрешаем запросы к DNS
$IPT -A OUTPUT -p udp -m udp -o $INET_IFACE --dport 53 ↵
       --sport $NONPRIPORTS -j ACCEPT
$IPT -A OUTPUT -p tcp -m tcp -o $INET_IFACE --dport 53 ↵
       --sport $NONPRIPORTS -j ACCEPT
$IPT -A INPUT -p udp -m udp -i $INET_IFACE ↵
       --dport $NONPRIPORTS --sport 53 -j ACCEPT
$IPT -A INPUT -p tcp -m tcp -i $INET_IFACE ↵
       --dport 1024:65353 --sport 53 -j ACCEPT

# Разрешаем AUTH-запросы на удаленные сервера,
# на свой - запрещаем
$IPT -A OUTPUT -p tcp -m tcp -o $INET_IFACE --dport 113 ↵
       --sport $NONPRIPORTS -j ACCEPT
$IPT -A INPUT -p tcp -m tcp -i $INET_IFACE ↵
       --dport $NONPRIPORTS --sport 113 -j ACCEPT ! --syn
$IPT -A INPUT -p tcp -m tcp -i $INET_IFACE ↵
       --dport 113 -j DROP

# Открываем необходимые нам порты
# FTP (21)
$IPT -A OUTPUT -p tcp -m tcp -o $INET_IFACE --dport 21 ↵
       --sport $NONPRIPORTS -j ACCEPT
# SMTP (25)
$IPT -A OUTPUT -p tcp -m tcp -o $INET_IFACE --dport 25 ↵
       --sport $NONPRIPORTS -j ACCEPT
# POP3 (110)
$IPT -A OUTPUT -p tcp -m tcp -o $INET_IFACE --dport 110 ↵
       --sport $NONPRIPORTS -j ACCEPT
# HTTP/HTTPS клиент (80, 443)
$IPT -A OUTPUT -p tcp -m tcp -m multiport -o $INET_IFACE ↵
       --sport $NONPRIPORTS -j ACCEPT --dports 80,443
# PROXY (3128)
$IPT -A OUTPUT -p tcp -m tcp -o $LAN_IFACE --dport 3128 ↵
       -j ACCEPT
$IPT -A INPUT -p tcp -m tcp -i $LAN_IFACE --dport 3128 ↵
       -j ACCEPT
#ICQ (5190)
$IPT -A OUTPUT -p tcp -m tcp -o $INET_IFACE --dport 5190 ↵
       --sport $NONPRIPORTS -j ACCEPT
#QIP-аккаунт (5222)
$IPT -A OUTPUT -p tcp -m tcp -o $INET_IFACE --dport 5222 ↵
       --sport $NONPRIPORTS -j ACCEPT

# Включаем NAT
$IPT -t nat -A POSTROUTING -o $INET_IFACE -j SNAT ↵
       --to-source $INET_IP
```

Таким образом, мы контролируем трафик по различным протоколам и организовываем трансляцию адресов для нашей сети.

Конечно, данный скрипт не может претендовать на абсолютную универсальность, он приведен здесь скорее в качестве примера, а не руководства к действию.

Установливаем Squid

Стандартная установка пакета через менеджер пакетов компилируется не совсем так, как нам нужно. Поэтому нам необходимо скачать пакет с исходными текстами командой dpkg-source и отредактировать файл debian/rules так, чтобы там были прописаны следующие параметры:

```
--enable-auth="basic,negotiate"
--enable-negotiate-auth-helpers="squid_kerb_auth"
--enable-external-acl-helpers="ldap_group"
```

После этого Squid собирается командами:

```
debian/rules build
debian/rules binary
```

Вы получите 3 бинарных пакета, однако установить достаточно только два: squid и squid-common.

Однако и это еще не все. Необходимый нам хелпер squid_kerb_auth поддерживает как реализацию MIT Kerberos, так и Heimdal Kerberos, и поэтому в итоге скомпилированный хелпер не работает корректно. Для решения данной проблемы в исходниках ищем файл ,/helpers/negotiate_auth/squid_kerb_auth/readme.txt и копируем оттуда кусок кода, отвечающий за реализацию MIT kerberos, в файл и запускаем получившийся скрипт.

Вот что нужно скопировать:

```
#!/bin/sh
DEFINE_SPNEGO=-DHAVE_SPNEGO
#HEIMDAL
# DEFINE="-DHEIMDAL $DEFINE_SPNEGO -d__LITTLE_ENDIAN__"
# INCLUDE=-I/usr/include/heimdale -Ispnegohelp
#LIBS="-Lgssapi -lkrb5 -lcom_err -lasn1 -lroken"
#MIT
 DEFINE="$DEFINE_SPNEGO -D__LITTLE_ENDIAN__"
 INCLUDE=-Ispnegohelp
 LIBS="-lgssapi_krb5 -lkrb5 -lcom_err"
#
SPNEGO="spnegohelp/derparse.c spnegoelp/spnego.c ↵
        spnegohelp/spnegohelp.c spnegohelp/spnegoparse.c"
SOURCE="squid_kerb_auth.c base64.c"
qcc -o squid_kerb_auth $DEFINE $INCLUDE $SOURCE $SPNEGO $LIBS
```

Скомпилированный хелпер копируем в /usr/lib/squid с заменой исходного файла.

Устанавливаем Rejik

В принципе установка сводится к простым командам:

```
make
make install
```

За исключением пары тонкостей:

> Необходима библиотека pcre.

> В makefile нужно прописать переменные SQUID_USER и SQUID_GROUP, значения которых должны совпадать со значением переменных cache_effective_user и cache_effective_group файла squid.conf.

После установки редактируем конфигурационный файл /usr/local/rejik3/redirector.conf - там необходимо прописать правила блокировки сайтов и пути к HTML-страницам с сообщениями о запрете доступа.

Теперь на контроллере домена необходимо создать билет для учетной записи, под которой будут проверяться учетные данные пользователя при доступе в Интернет. Учетная запись должна иметь неограниченный срок действия пароля и не должна блокироваться. Например:

домен - mydomain.local;
имя пользователя - proxyuser;
пароль-password.
сервер - squidproxy.mydomain.local.
Наша команда:

```
C:\Program Files\Support Tools>ktpass ↵
    -princ HTTP/squidproxy.mydomain.local@MYDOMAIN.LOCAL ↵
    -mapuser proxyuser -crypto des-cbc-md5 ↵
    -pass "password" -ptype KRB5_NT_SRV_HST ↵
    -out squid.keytab
```

Поскольку мы не вводим прокси-сервер в домен, то в DNS должны быть внесены данные о нашем сервере (A- и PTR-записи). Создаем группу пользователей, которым разрешен доступ в Интернет (например, группа INET_ALLOW в OU Internet). Копируем .keytab-файл в папку /etc/squid. Меняем права доступа:

```
chmod 400 /etc/squid/squid.keytab
chown proxy /etc/squid/squid.keytab
```

В файл /etc/init.d/squid вносим строки для подключения ключа:

```
KRB5_KTNAME=/etc/squid/squid.keytab
export KRB5_KTNAME
```

Если у вас много пользователей и Squid тратит много ресурсов на их аутентификацию, то можно отключить проверку кэша использованных тикетов, добавив в /etc/init.d/squid следующие строки:

```
KRB5RCACHETYPE=none
export KRB5RCACHETYPE
```

Настраиваем Kerberos

Несмотря на то что пакет krb5-user (клиент Kerberos) в стабильной версии Lenny должен быть совместим с Kerberos V5, у нас он работал некорректно, и потребовалось установить данный пакет (со всеми зависимостями) из ветки testing.

Основным файлом настроек является /etc/krb5.conf. Необходимо отредактировать его следующим образом:

```
[libdefaults]
default_realm = MYDOMAIN.LOCAL
dns_lookup_realm = no
dns_lookup_kdc = no
default_keytab_name = /etc/squid/squid.keytab
default_tgs_enctypes = des-cbc-crc rc4-hmac des-cbc-md5
default_tkt_enctypes = des-cbc-crc rc4-hmac des-cbc-md5
permitted_enctypes = des-cbc-crc rc4-hmac des-cbc-md5
ticket_lifetieme = 24000
clock_skew = 300
# The following krb5.conf variables are only for MIT Kerberos
krb4_config = /etc/krb.conf
krb4_realms = /etc/krb.realms
kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true
# The following libdefaults parameters are only for Heimdal
# Kerberos
v4_instance_resolve = false
v4_name_convert = {
```

```
host = {
rcmd = host
ftp = ftp
}
plain = {
something = something-else
}
}
fcc-mit-ticketflags = true
#
[realms]
MYDOMAIN.LOCAL = {
kdc = dc.mydomain.local
admin_server = dc.mydomain.local
default_domain = mydomain.local
}
#
[domain_realm]
.linux.local = MYDOMAIN.LOCAL
.mydonain.local = MYDOMAIN.LOCAL
mydomain.local = MYDOMAIN.LOCAL
#
[logging]
default = FILE:/var/log/krb5lib.log
kdc = FILE:/var/log/kdc.log
kdc = SYSLOG:INFO AEMON
admin_server = FILE:/var/log/kadmin.log
```

Проверяем ключ:

```
$ kinit -V -k -t /etc/squid/squid.keytab ↵
        HTTP/squidproxy.mydomain.local
```

Вы должны получить в ответ:

```
Authenticated to Kerberos V5
```

Настраиваем Squid

Редактируем файл /etc/squid/squid.conf так:

```
auth_param negotiate program ↵
        /usr/lib/squid/squid_kerb_auth ↵
        -d -s HTTP/squidproxy.mydomain.local@MYDOMAIN.LOCAL
auth_param negotiate children 10
auth_param negotiate keep_alive on
acl all src all
#Recommended minimum configuration:
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8
#
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method GET
# Тут проверяем группу, к которой принадлежит пользователь
# (вся конструкция пишется в одну строку, хотя и разбита
# при печати)
external_acl_type ldap_ad_check ttl=1200 %LOGIN ↵
    /usr/lib/squid/squid_ldap_group ↵
   -R -b "dc=mydomain,dc=local" ↵
    -f "(&(objectclass=user)(sAMAccountName=%v ↵
    (memberof=cn=%a,ou=internet,dc=mydomain,dc=local))" ↵
    -D "proxyuser@mydomain.local" -w "password" ↵
    -K -d 192.168.100.
#192.168.100.2 - адрес DC
acl inet_access external ldap_ad_check @INET_ALLOW
acl AUTHENTIC proxy_auth REQUIRED
#
http_access allow inet_access
http_access deny !AUTHENTIC
http_access allow AUTHENTIC
http_access deny all
#
http_port 3128
#
redirect_program /usr/local/rejik3/redirector ↵
        /usr/local/rejik3/redirector.conf
```

На клиентских машинах необходимо прописать прокси-сервер в виде FQDN: squidproxy.mydomain.local, порт 3128. Использование IP-адреса или сокращенного имени компьютера недопустимо. Также был выявлен необычный баг, связанный с длиной имени хоста прокси-сервера. В случае слишком короткого имени (у нас вначале было 5 букв) Kerberos-авторизация не работает.

Просмотр статистики доступа к интернет-ресурсам можно организовать с помощью различных утилит, генерирующих отчеты на основе журналов Squid. Мы используем для этой цели lightsquid. Это очень удобное решение, генерирующее подробные html-отчеты, которые доступны через веб-интерфейс. Для установки достаточно скачать архив с официального сайта http:// lightsquid.sourceforge.net, распаковать его в каталог var/www//<каталог lightsquid> и изменить права доступа ко всем файлам так, чтобы они стали исполняемыми, а их владельцем стал пользователь Apache.

В файле httpd.conf необходимо добавить строки:

```
<Directory "/var/www/<каталог lightsquid>">
        AddHandler cgi-script .cgi
        AllowOverride All
</Directory>
```

Настройка осуществляется через файл lightsquid.cfg. Соответствие учетных записей пользователей, групп и их реальных имен - через файлы group.cfg и realname.cfg.

***

Итак, мы получили интернет-шлюз, работающий абсолютно прозрачно для пользователей (учетные данные берутся из Windows-сессии) и соответствующий всем поставленным в начале статьи требованиям. При этом нам не потребовались дополнительные сервисы вроде Samba, что экономит ресурсы сервера. Однако у данного решения есть один минус: Kerberos-аутентификация поддерживается не всеми браузерами. Поэтому их использование в компании должно быть регламентировано.

В настоящий момент совместимость браузеров такова:

Internet Explorer 6 **и более ранние** - Kerberos не поддерживается;

Internet Explorer 7 - поддержка заявлена, однако из-за имеющейся ошибки аутентификация пропадает через полчаса, и требуется перезапуск браузера;

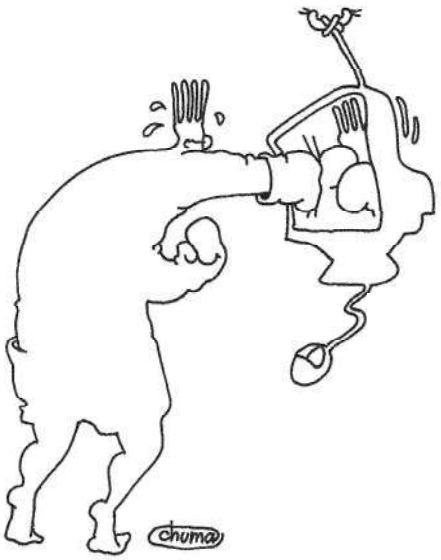
Internet Explorer 8 - полная поддержка;

Mozilla Firefox 3.5 - полная поддержка;

Opera - не поддерживается ни в одной версии, включая 10 (представители Opera Software заявляют, что данный тип авторизации редко востребован, а внесение его поддержки требует серьезных изменений в коде браузера);

Apple Safari - поддержка заявлена, но я не проверял;

Google Chrome - не поддерживается ни в одной версии. включая 3.0 (на момент написания статьи актуальной была версия 3.0.195.21). EOF



Зловредное ПО нарушает нормальную работу ПК, **из-за чего сотрудники не могут полноценно выполнять свои задачи**

Для каждого типа правил можно выбрать один из двух режимов работы.

Enforced - правила принудительно применяются к пользователям. И любой файл, для которого нет подходящего правила, будет заблокирован для запуска.

Audit Only - режим аудита. Он полезен для определения списка ПО, которое используется пользователями. Когда включен этот режим, политики AppLocker не ограничивают запуск приложений. Но если для запускаемого файла (сценария или приложения) задано правило в политике, в журнал событий AppLocker будет добавлена соответствующая запись. Этот журнал можно просмотреть через оснастку Event Viewer по адресу Applications and Service logs -» Microsoft -> Windows -> AppLocker (см. рис. 2).

На вкладке Advanced того же окна вы можете отдельно настроить применение политик AppLocker к файлам типа Application extension - динамически загружаемым библиотекам с расширением dll. Однако используйте эту функцию с осторожностью, так как после её включения вам придётся создавать отдельные правила для файлов библиотек. А в результате проверки всех библиотек на соответствие правилам скорость работы системы может существенно снизиться (см. рис. 3).

Обратите внимание, что для применения правил в системе должна быть запущена служба Application Identity. Для создания и редактирования правил это не требуется.

Создание правил

После краткого обзора консоли управления политикой мы можем приступать к созданию правил (см. рис. 4). К этой задаче существуют три подхода:

- создание правил вручную;
- автоматическая генерация правил;
- автоматическое создание правил по умолчанию.

В большинстве случаев я рекомендую комбинировать ручное создание правил с автоматической генерацией правил по умолчанию. Это позволит сразу создать относительно безопасную среду. Для этого нажмите правой кнопкой на

Рисунок 1. Внешний вид консоли AppLocker

Рисунок 2. Окно управления режимом работы политики для каждой категории правил

каждой категории и выберите элемент Create Default Rules, после чего система создаст несколько правил по умолчанию. Пример результата для типа Executable Files показан на рис. 5.

Правила по умолчанию позволяют всем пользователям запускать любые исполняемые файлы из каталогов Windows и Program Files. А локальным администраторам разрешают запускать вообще всё. Это достаточно щадящие правила, которые впоследствии могут быть отредактированы под ваши нужды. Так же здесь хочу отметить один достаточно важный момент - пока в конкретной категории правил политики нет ни одного правила, вы можете запускать любые файлы, которые подпадают под эту категорию. Создав хоть одно правило, вы сможете запускать только те файлы, которые подпадают под разрешения в созданных правилах.

В результате если мы работаем под учётной записью обычного пользователя, нам будет разрешено запускать файлы только из системных каталогов. Это относится только к тем расширениям, которые проверяются политикой. Но очень часто этого будет недостаточно, именно поэтому придётся создавать и свои правила. Для этого в контекстном меню нужной категории выберите пункт Create New Rule..., после чего вы увидите окно создания нового правила. Правила создаются пошаговым мастером, поэтому разобраться в них будет достаточно просто (см. рис. 6).

В секции Before You Begin вы можете прочитать вступление к мастеру и основные инструкции. В секции Permissions вы можете задать действие для правила - разрешить или запретить запуск подходящих файлов, а также выбрать группу безопасности, на которую это правило будет распространяться. Это намного удобнее, чем механизм применения политик в SRP. Теперь мы можем создать всего одну политику на уровне домена вместо того, чтобы иметь несколько отдельных политик и управлять их применением с помощью Security Filtering. Важно знать, что политики AppLocker не действуют на служебные учётные записи, например, LocalSystem. Дальше в секции Conditions вы выбираете тип правила. Прежде чем выбрать что-то из этого списка, следует рассмотреть каждый тип правил.

Правила пути

Правила пути достаточно простые, но их нужно использовать осторожно. Правила этого типа следует использовать только для тех путей, по которым пользователи не имеют права на запись. Ни в коем случае не допускается создание правил путей для каталогов, в которые пользователи могут записывать свои файлы. Ведь в результате им ничего не будет стоить подменить легитимные файлы своими и запускать их. Правила пути обычно используются для приложений, которые установлены не в стандартный каталог (Program Files), а находятся по другому адресу - например, в сетевой папке или на другом томе. Вы можете использовать подстановочные знаки - такие, как «?» и «*», а также специальные переменные окружения (см. таблицу).

Несмотря на синтаксическое совпадение с некоторыми системными переменными окружения, они таковыми не являются. К сожалению, мы лишены возможности использования системных переменных окружения во избежание их подмены. Например, при настройке SRP системные администраторы в качестве пути к сценариям входа в систему зачастую использовали такие переменные как %LogonServer% (в конструкции вроде %LogonServer%\Netl_ogon\Scripts). Это даёт гарантию подключения к сетевой папке NetLogon работающего контроллера домена. Сейчас же для создания подобных правил придётся использовать абсолютные пути вместо относительных.

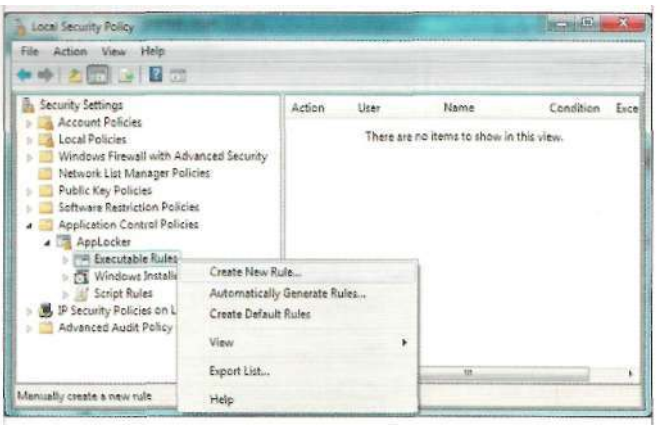
Но это неудобство было немного компенсировано другой полезной особенностью - теперь мы можем использовать отдельные переменные для съёмных и оптических носителей.

Правила хешей

Это один из наиболее популярных типов правил как в SRP, так и в AppLocker. Правило хеша просто создаёт хеш для файла (с использованием алгоритма SHA256) и записывает его в правило. Данный тип правил следует использовать для файлов, которые расположены в разрешённых для записи пользователям каталогах. Действительно, некоторые программы для корректной работы требуют прав на создание файлов в той же папке, в которой находится сам исполняемый модуль. Для таких сценариев целесоо-

Рисунок 3. Окно управления проверкой файлов библиотек на соответствие правилам

Рисунок 4. Создание новых правил из контекстного меню каждого типа



бразно использовать правило хеша. В этом случае при повреждении файла, подмене, заражении вирусом его хеш будет также изменён, и файл окажется заблокирован для запуска. Однако при частом обновлении программ вам с такой же периодичностью придётся обновлять и соответствующие правила хеша.

Правила издателей

Правила издателей - это следующая ступень эволюции классических правил сертификатов в SRP, которая привнесла несколько удобных нововведений. Правило издателей вы можете создавать, просто указав файл с цифровой подписью. Следует учесть, что для этого файл должен иметь целостную подпись, а корневой сертификат подписи должен быть помещён в контейнер «Trusted Root Certification Authorites». Если хоть одно из этих условий не выполняется, то создать правило издателя не получится (см. рис. 7).

Если посмотреть на примере Microsoft Office, то мы видим достаточно информации, чтобы достоверно идентифицировать приложение. Такое правило включает поле Subject сертификата цифровой подписи, сведения о продукте, внутреннее имя файла и внутреннюю версию файла. Используя ползунок, мы можем задать и более общее правило, которое, например, будет разрешать запускать любой подписанный файл с указанным полем Subject (в правиле это поле называется Publisher) и внутренним именем без ограничения по версии. Или даже любой файл, который подписан таким сертификатом. Также вы можете использовать и вовсе произвольные настройки правил издателей. Для этого установите флажок Use custom Values - и все поля станут доступны для редактирования вручную. В том числе вы можете указывать степень соответствия версии файла как Exact match, And above и And below. Это можно использовать, когда вы хотите запретить использовать любые версии Excel младше, чем Excel 2003. Тогда вы указываете версию 11.0.0.0 и степень соответствия выставляете в And above. В таком случае запустятся только версии Excel 2003 и более новые.

Правила издателей удобны для часто обновляемых программных файлов (например, бизнес-приложения или ваши собственные подписанные сценарии). Если после обновления файлы проходят повторный процесс подписывания, они подпадут под уже существующее правило и будут запускаться.

Много правил в одном правиле

Следующим удобством является то, что при использовании правил путей или правил хеша вы можете добавлять не только по одному файлу, но и группу файлов в одном каталоге. Технологически вы не имеете возможности добавить группу файлов на основе правила издателя, поскольку правило издателя не опирается на физическое местоположение файлов, а их целостность проверяется только при запуске. Когда вы выбрали правило пути или правило хеша, в следующем окне мастера вы можете нажать Browse Folders, и тогда для правила пути мастер разрешит запускать всё из указанного каталога (это будет заметно по символу подстановки - «*» в конце пути). А для правила хеша мастер найдёт все подходящие файлы в указанной папке и подсчитает для них хеш. При этом важно отметить, что поиск не будет рекурсивным (т.е. не станет включать файлы во вложенных каталогах).

Если вы хотите исключить какие-то файлы из полученного списка, достаточно выделить нужные файлы и нажать кнопку Remove. Вы не можете использовать отдельные исключения для правила хеша, поскольку любой хеш уникально идентифицирует конкретный файл. Иными словами, под одно правило хеша может подпадать только один файл. А добавляя несколько файлов (например, все файлы в каталоге), вы создаёте целый набор отдельных правил хеша. Это следующий положительный момент в организации правил в AppLoker, поскольку эти составляющие правила вы можете группировать по какому-либо принципу. Например, создать одно общее правило хеша, которое будет называться Microsoft Office, и внутри этого правила добавить по хешу несколько исполняемых файлов из программного пакета. Зачастую бизнес-приложения так же состоят из нескольких исполняемых модулей. Таким образом, значительно повышается читабельность политик, удобство управления правилами и снижается вероятность ошибки.

Я рекомендую именно такой сценарий группировки правил - по типу приложений. Для каждого приложения вы создаёте свою коллекцию правил, в которую включаете все необходимые исполняемые модули. Таким образом, при из-

Рисунок 5. Правила, созданные по умолчанию

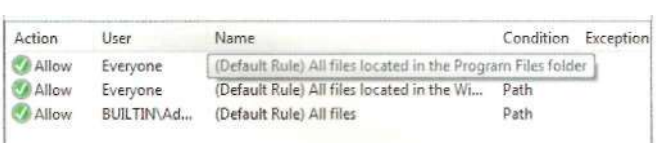


Таблица. Правила пути

Переменная пути в AppLocker	Аналог переменной окружения в Windows	Пример
%WinDir%	%WinDir%, %SystemRoot%	"C:\Windows\"
%System32%	n/a	"C:\Windows\System32\"
%OSDrive%	%SystemDrive%	"C:\"
%ProgramFiles%	%ProgramFiles%, %ProgramFiles(x86)%	"C:\Program Files", "C:\Program Files (x86)"
%Removable%	n/a	CD or DVD (съёмные накопители)
%Hot%	n/a	Накопители USB (носители данных с «горячим» подключением)

менении определённого приложения вам будет очень просто найти нужное правило и отредактировать его.

Исключения из правил

В отличие от правила хеша правила пути и издателя не позволяют уникально идентифицировать файл и обладают достаточно большой областью действия. Поэтому возможны ситуации, когда вы хотите запретить запуск некоторых файлов, которые подпадают под разрешающее правило. Для этого в секции Exceptions мастера создания правила вы можете указать исключения.

Как вы видите на рис. 8, исключения можно создавать, используя все возможности AppLocker. В порядке исключения вы можете добавлять исключаемые пути, хеши файлов и даже цифровые подписи. Например, вы разрешили все файлы по маске %PROGRAMFILES%\Microsoft OfficeV, используя правило пути. Однако вы хотите запретить запуск программы PowerPoint. Для этого вы можете создать исключение по правилу пути вида %PROGRAMFILES%\Microsoft Office\Office12\POWERPNT.EXE или по правилу хеша, указав конкретный файл PowerPnt.exe.

Другой сценарий может подразумевать, что у вас есть приложение, исполняемые модули которого подписаны различными сертификатами. В таком случае правило издателя будет не очень эффективным решением, и вы хотите создать правило пути или правило хеша для всего каталога. Но вы хотите запретить запуск файлов, которые подписаны определённым сертификатом. В данном случае в секции Exceptions вы указываете тип исключения Publisher и в диалоговом окне поиска выбираете файл с необходимой цифровой подписью. Таким образом вы сможете запускать все файлы из каталога - кроме тех, которые подписаны указанным сертификатом.

Исключения или запреты?

Внимательные читатели могут задать вопрос: а зачем делать исключения, если их можно вынести в отдельные правила запрета? Действительно, на первый взгляд может показаться, что это более простое решение. Однако запреты всегда являются краеугольным камнем в настройке прав.

Применительно к AppLocker здесь есть несколько нюансов, которые следует учитывать при создании запретов. Самый главный из них - порядок применения правил. Для определения возможности запуска файла AppLocker при сортировке правил использует принцип первого попадания (First Match). Это означает, что правила к файлу применяются в строго определённом порядке, и действующим окажется то, которое сработало (т.е. под которое подпал файл) первым. Поэтому знание принципа сортировки правил в AppLocker может сэкономить вам время.

Все правила сортируются отдельно по запретам и разрешениям и проверяются в следующем порядке:

- Сначала проверяются все явные запреты (в произвольном порядке).
  - Если файл подпал под явный запрет, то для этого запрета отрабатываются все исключения. Если файл всё ещё подпадает под явный запрет, то файл блокируется для запуска.
  - Если после обработки исключений файл больше не подпадает под явный запрет, то берётся следующее запрещающее правило, и так продолжается, пока не будут проверены все явные запреты.
- Если ни одного явного запрета не обнаружено, то проверяются все явные разрешения.
  - Если файл подпал под явное разрешение, то для этого разрешения отрабатываются все исключения. Если файл всё ещё подпадает под разрешение, то файл будет разрешён для запуска.
  - Если после обработки исключений файл больше не подпадает под явное разрешение, то берётся следующее разрешающее правило, и процесс повторяется до тех пор, пока файл после фильтрации исключений не подпадёт под разрешение.
- Если ни одна из итераций не дала однозначный ответ вида разрешено/не разрешено, то файл блокируется для запуска.

Чтобы понять, как это работает, рассмотрим один пример. На компьютере в каталог по умолчанию установлен пакет Microsoft Office, которым можно пользоваться всем. Но группе Accountants необходимо разрешить запускать

Рисунок 6. Окно мастера создания правил

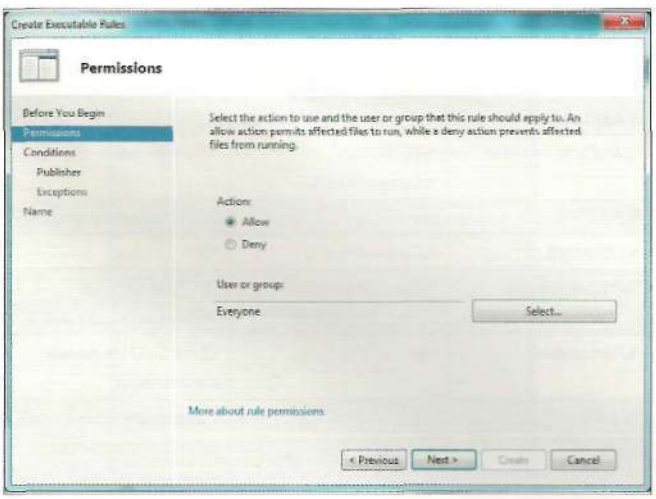


Рисунок 7. Окно со свойствами правила издателя

только программы Word и Excel. Запуск остальных файлов из Program Files разрешён без ограничений.

Для решения этой задачи мы должны разрешить весь каталог Program Files по правилу пути для группы Everyone. Поскольку доступ к программам Microsoft Office будет ограничен только для группы Accountants, мы создаём новое запрещающее правило (с действием Deny), которое применяется только к группе Accountants. Теперь программы из пакета Microsoft Office будут разрешены для запуска всем, кроме группы Accountants. Чтобы обеспечить запуск только необходимых приложений из этой папки, мы редактируем запрещающее правило и добавляем два исключения (по правилу пути, хеша или издателя) для файлов Excel.exe и Word.exe.

Исходя из порядка сортировки правил, в первую очередь файлы будут проверены на соответствие запрещающему правилу (запрет на каталог Microsoft Office) с учётом исключений. После этого под запретом остаётся весь каталог Mictosoft Office, но без Word.exe и Excel.exe. Если у нас запретов больше нет, то применяется разрешение на каталог Program Files для группы Everyone. Поскольку указанные файлы подходят под это разрешающее правило, они и будут разрешены для запуска. (Разумеется, при условии, что в этом разрешающем правиле нет исключений, действующих на эти файлы).

А вот если члены группы Accountants попытаются запустить PowerPoint, то ситуация окажется совершенно другой. Мы снова начинаем с первого шага. Из запрещающего правила отрабатываются исключения, т.е. Word и Excel, а затем файл снова проверяется на соответствие правилу. И даже после удаления исключений PowerPoint всё ещё подпадает под запрет. В таком случае остальные правила не проверяются, а запуск блокируется.

Импорт и экспорт правил AppLocker

В процессе эксплуатации AppLocker вы можете захотеть зафиксировать конфигурацию политик на отдельной рабочей станции перед изменением существующих правил. Одной из причин такого шага может служить необходимость отката к заведомо работоспособной конфигурации на случай, если изменения приведут к непредвиденным последствиям, а также для использования шаблонов правил. При использовании SRP это зачастую было неразрешимым вопросом, поскольку стандартные шаблоны безопасности (Security Templates) не позволяют заранее настроить правила для SRP и сохранить их в каком-то состоянии. В AppLocker этот недостаток также решён (см. рис. 9).

В контекстном меню AppLocker вы можете выбрать команду Export Policy для экспорта и Import Policy для импорта политик. AppLocker сохраняет все правила и настройки в файле XML, который вы можете редактировать даже без доступа к редактору групповой политики. Если в доменной среде вы можете делать резервные копии политик с помощью GPMC, то в условиях рабочей группы (например, домашнего использования) эта возможность будет очень удобным и простым средством сохранения ваших правил AppLocker.

***

В данной статье мы рассмотрели ключевые возможности нового инструмента защиты ПК от выполнения нежелательного (и потенциально злонамеренного) ПО -AppLocker. Также мы рассмотрели методику создания правил на нескольких практических примерах. Изложенный материал является достаточным для начала эффективной работы с AppLocker с целью обеспечения безопасности ваших систем. Если вы заинтересовались данной технологией и хотели бы испытать её в действии, то вы можете загрузить ознакомительную версию Windows 7 Enterprise с сайта Microsoft. Также более глубокое изучение особенностей работы политики AppLocker вы можете прочитать в блоге автора статьи - http://www.sysadmins.lv. BKP

1. Поданс В. На страже безопасности - Software Restriction Policies. //Системный администратор, №9, 2008 г. - С. 54-59.
2. AppLocker Technical Documentation for Windows 7 and Windows Server 2008 R2 - http://www.microsoft.com/downloads/details.aspx?FamilyID=025cf2e8-b0ab-4419-b5bb-86ab2d5eca83.
3. AppLocker Step-by-Step Guide - http://technet.microsoft.com/library/dd723686.aspx.
4. Windows 7 Enterprise 90-day Trial - http://technet.microsoft.com/evalcenter/cc442495.aspx.

Рисунок 8. Окно Exceptions мастера создания правил

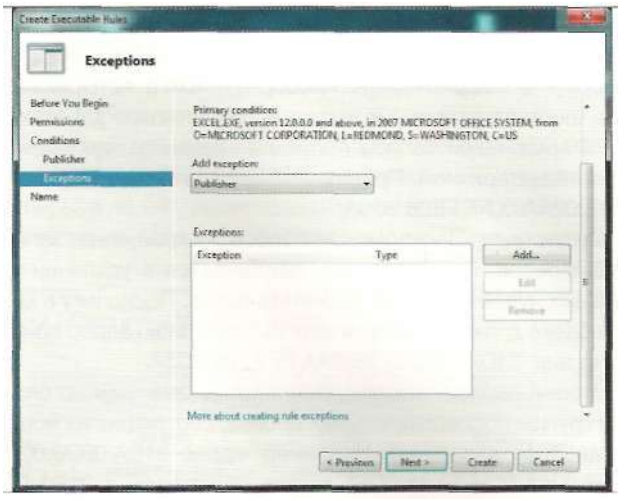
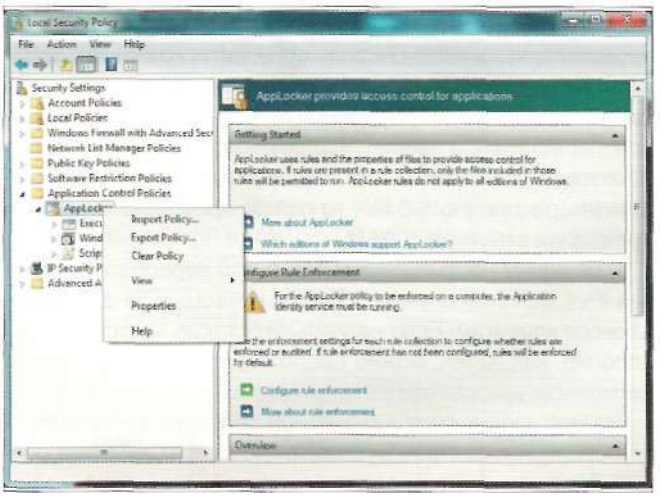


Рисунок 9. Контекстное меню импорта и экспорта политики AppLocker



Визитка

ИЛЬЯ РУДЬ, сертифицированный тренер Microsoft, специализируется на технологии Active Directory, один из основателей ресурса itband.ru

Гость из будущего

Протокол IPv6 - новая версия

Многие стандарты передачи данных были разработаны более 30 лет назад, и современному администратору пора начинать обновление багажа знаний

С выходом новых версий ОС Windows и соответственно обновленных служб нередко в списке изменений встречаются такие фразы, как «Добавлена поддержка IPv6» или «IPv6-совместимо». Большинству администраторов понятно, что речь идет о новой версии протокола IP, но, как правило, этим познания и заканчиваются. Я предлагаю немного разобраться с данным вопросом, ибо, если верить прогнозам, довольно скоро IPv6 перейдет из статуса таинственной новинки в повседневную реальность. Но для начала давайте поймем, чего не хватает IPv4 сегодня.

Проблемы IPv4

Одной из основных проблем называют истощение адресного пространства. Напомню, что размер адресного пространства IPv4 равен 232, а это более чем 4 млрд узлов. С этим можно поспорить, фактически при использовании технологии NAT адресное пространство растягивается до бесконечности, но тогда появляется другая проблема, связанная со строго ограниченным количеством портов. Ясно одно - свободные, незарегистрированные адреса в ближайшие десять лет подойдут к концу, а по некоторым подсчетам «Время X» наступит в течение ближайших двух-трех лет.

Другим камнем в огород IPv4 считается неэффективная маршрутизация, которая заложена в самой идеологии протокола, что в свою очередь приводит к хранению на магистральных маршрутизаторах десятков тысяч маршрутов и, как следствие, чрезмерную их нагрузку, особенно при перестроении таблиц маршрутизации. Если в начале 90-х годов для размещения маршрутной таблицы в маршрутизаторе хватало 4-8 Мб, то сейчас требования к памяти превысили отметку в 100 Мб.

Еще одним неотъемлемым атрибутом корпоративных сетей IPv4 является служба DCHP, отвечающая за выдачу IP-адресов клиентам. Если не учитывать такую «детскую» технологию, как APIPA, можно смело сказать, что встроенное автоконфигурирование в IPv4 отсутствует.

На мой взгляд, самой серьезной проблемой IPv4 является безопасность. Несмотря на то что стек TCP/IP был разработан по инициативе Министерства обороны США, своим появлением он во многом обязан академической университетской среде, которую в то время возможность передачи данных волновала гораздо больше, чем сохранение их конфиденциальности. Появившиеся впоследствии протоколы IPsec, SSL, TLS были призваны решить проблему безопасности и отчасти ее решили, к сожалению, усложнив при этом управление передачей данных.

После появления протокола IPv4 большую популярность получили потоковые мультимедиаприложения, VoIP и видеоконференции, которые требуют гарантированной пропускной способности и непревышения максимальной задержки, т.е. обеспечения качества обслуживания (Quality of Service). В IPv4 существует специальное поле Type of service, но механизм интерпретации и резервирования его определен не был, поэтому абсолютное большинство существующих маршрутизаторов попросту игнорируют это поле в заголовке IPv4.

Список этот можно продолжить напоминанием о недостаточном размере заголовка IPv4 , но, я думаю, и этого вполне достаточно, чтобы будущее обратило внимание на IPv6. Так что же изменится с переходом на новый протокол?

Новый протокол

Прежде всего это размер IP-адреса, в IPv6 он составляет 128 бит, что в четыре раза превышает размер адреса в IPv4. 128-битный адрес IPv6 делится на части по 16 бит, которые в свою очередь преобразуются в четырехзначные шестнадцатеричные числа и разделяются двоеточиями. Форма такой записи получила название двухточечно-шестнадцатеричной. Пример IPv6-aflpeca: 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A.

Существует несколько способов сокращения записи 1Pv6-адресов. Первый из них заключается в удалении начальных нулей в каждом 16-битном блоке. Поскольку в каждом блоке должен остаться хотя бы один знак, адрес приобретет вид: 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A.

Второй вариант заключается в замещении одного блока или группы последовательных блоков, состоящих из нолей, на двойное двоеточие. Например, адрес 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A можно превратить в 21DA:D3::

Если верить прогнозам, довольно скоро **IPv6** перейдет **из статуса таинственной новинки в повседневную реальность**

2F3B:2AA:FF:FE28:9C5A, убрав начальные ноли и заменив нулевой блок на (::). Важно то, что в адресе может быть только одно двойное двоеточие, поэтому заменять следует либо какой-то один разряд, либо группу последовательных.

Хорошим примером служит сокращение адреса многоадресной рассылки FF02:0000:0000:0000:0000:0000:0000:0002, который после применения правила принял вид FF02::2.

Следующее изменение связано с отсутствием такого понятия, как маска подсети. IPv6-aflpec делится на три части:

Глобальный префикс (Global Routing Prefix) - аналогичен идентификатору сети (Network ID) в IPv4 и присваивается провайдерам. Определяется он тремя первыми блоками.

Идентификатор подсети **(Subnet ID)** - представлен четвертым блоком и, по сути, очень похож на идентификатор подсети (Subnet ID) в IPv4.;

Идентификатор интерфейса (Interface SD) - аналог Host ID в IPv4, определяет уникальный адрес хоста вашей сети.

Существует несколько способов получения уникального 64-битного идентификатора интерфейса: он может быть настроен вручную, определен DCHP-сервером или получен путем преобразования MAC-адреса сетевой карты. Вместо маски в IPv6 указывается префикс - это количество бит, которые определяют часть блоков, отвечающих за Global Routing Prefix. Пишется префикс через косую черту после самого адреса.

Возьмем для примера IPv6-aflpec: 2001:0f68:0000:0000:0000:0000:1986:69af/48. Поскольку префикс (/48) указывает на первые 48 бит, можно сделать вид, что 2001:0f68:0000 будет являться частью Global Routing Prefix. Следующее поле, 0000, указывает на идентификатор подсети. Оставшиеся блоки 0000:0000:1986:69af-это идентификатор интерфейса.

В IPv6 существует три различных типа адресов:

Unicast-определяет конкретный уникальный хост в сети;

Multicast - идентифицирует группу хостов или интерфейсов, при отправке пакета на этот адрес он доставляется на каждый хост группы;

Anycast - тоже объединяет несколько хостов, но имеет существенное отличие от Multicast - пакет, посланный на Anycast-адрес, доставляется только ближайшему к отправителю участнику группы.

Еще одно существенное отличие заключается в появлении нового протокола канального уровня модели OSI Neighbor Discovery, который призван заменить IPv4 широковещательные пакеты типа Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and ICMPv4 Redirect на более эффективные Unicast- и Multicast-пакеты. Поскольку функций у Neighbor Discovery довольно много, их принято делить на функции Host-Router Discovery и Host-Host Communication.

В первую группу попадает задача Router Discovery, как понятно по названию, это метод обнаружения хостом маршрутизаторов в своей локальной сети. Далее на ND висит задача определения префикса сети (Prefix discovery), который дает понять клиенту, в какой сети он находится. Кроме этого с помощью ND клиент получает от маршрутизатора информацию о том, как производится получение IP-адреса (через DHCPv6 или через роутер), и дополнительные параметры, такие как максимальный размер пакета (Parameter Discovery).

Задачи группы Host-Host Communication - это разрешение имен, замена тех функций, которые в IPv4 выполнялись протоколом ARP (IP в MAC), а также определение доступно-

Рисунок 1. Схема IPv6-адреса (Global Unicast)

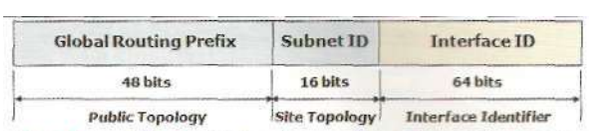


Рисунок 2. Схема IPve-адреса (Link Local Unucast)

сти партнера по передачи данных и выявление нарушения уникальности IP-адресов, то есть появления одинаковых IP.

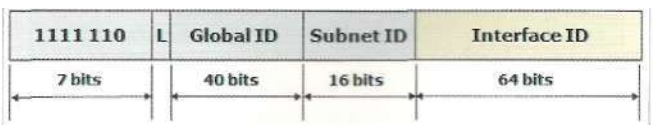
Плюсов у ND довольно много. Если резюмировать, то, во-первых, можно забыть о broadcasts-пакетах, ибо разрешение имен идет через Multicast. Во-вторых, устройства, использующие маршрутизатор, в случае если он перестает быть достижим, обнаруживают это и автоматически переключаются на другой (при его наличии). Поскольку ND работает на сетевом уровне, это дает возможность аутентифицировать и шифровать средствами IPSec такие задачи, как разрешение имен или обнаружение адреса маршрутизатора. И, конечно, автоконфигурация, несмотря на появление DHCPv6, значимость этой службы может оказаться под большим вопросом.

Итак, мы определились с типами IPv6-адресов. На одном из типов, а именно на Unicast, следует остановиться подробней. Он бывает трех видов:

Global Unicast - эквивалентен «белому» IPv4-адресу, он маршрутизируется в Интернете и доступен в IPv6-участке Глобальной сети. Первые 48-бит адреса являются уникальными по всему Интернету (Global Routing Prefix), а провайдер, используя следующие 16 бит (идентификатор подсети), может создать до 65536 подсетей (см. рис. 1). Пример сокращения нолей был показан на Global Unicast-адресе.

Link Local **Unicast**-уникальный IP-адрес, автоматически получаемый хостом вне зависимости от наличия в сети маршрутизаторов и DHCPv6-серВероВ. Генерируется адрес довольно просто. Глобальный префикс (Global Routing Prefix) изначально определен (fe80) и занимает лишь первые 10 бит адреса. Так как префикс стал короче (по сравнению с Global unicast-адресом), то пространство, отведенное под идентификатор подсети, увеличилось с 16 бит до 54 бит. А поскольку адрес LLU создан только для локальной сети, то данные биты не используются и выражаются нолями. Оставшиеся 64 бита (идентификатор интерфейса) получаются путем несложного преобразования 48-битного MAC-адреса компьютера (см. рис. 2). Пример такого преобразования: Узел А имеет MAC-адрес Ethernet 00-AA-00-3F-2A-1C. Сначала этот адрес преобразуется в формат EUI-64 путем вставки разрядов FF-FE между третьим и четвертым байтами: 00-AA-00-FF-FE-3F-2A-1C. Затем инвертируется бит U/L (седьмой бит в первом байте). Первый байт в двоичной форме имеет вид 00000000. При инвертировании седьмого бита он принимает вид 00000010 (0x02). Конечный результат, 02-AA-00-FF-FE-3F-2A-1C, после преобразования в двухточечно-шестнадцатеричную нотацию становится идентификатором интерфейса: 2AA:FF:FE3F:2A1C. Таким образом, сетевому адаптеру с MAC-адресом 00-AA-00-3F-2A-1C соответствует адрес локальной связи FE80::2AA:FF:FE3F:2A1C.

Рисунок 3. Схема IPv6-адреса (Unique Local Unicast)



Одной из главных задач Link Local Unicast является поддержка работы протокола Neighbor Discovery, именно поэтому адрес конфигурируется в любом случае. Передача данных внутри локальной сети осуществляется с использованием Link Local Unicast , даже при наличии сконфигурированного Global Unicast-адреса.

Unique Local Unicast - идеологически напоминает IPv4-адрес из зарезервированных диапазонов (10.0.0.0/8 или 192.168.0.0/24). Они также предназначены для работы в сетях, напрямую не связанных с Интернетом. Global Routing Prefix определяется первыми 8 битами и уже изначально задан (FD00::/8). Следующие 40 бит формируют Global ID - уникальный идентификатор, который представляет организацию. Он должен быть случайным, чтобы минимизировать возможность совпадения с другими организациями. Такая уникальность позволит осуществить объединение сетей и настроить маршрутизацию без их переконфигурирования. Еще 16 бит дают возможность создать 65536 подсетей и настроить маршрутизацию для внутреннего использования. Ну и наконец, последние 64 бита отданы под уже знакомый идентификатор интерфейса (см. рис. 3).

Одна из задач разработчиков протокола IPv6 состояла в предоставлении возможности автоконфигурирования интерфейсов. Важно понимать, что один интерфейс может иметь множество различных адресов IPv6. (В принципе, и при IPv4 интерфейс может иметь несколько адресов.) Таким образом, интерфейс может одновременно иметь Link Local и Global IPv6-адреса.

Процесс автоконфигурации начинается с получения Link Local-адреса, проверки его уникальности и определения того, какая информация должна быть получена автоматически (адреса, дополнительные параметры или и то, и другое). В случае если надо автоматически получить адрес, то через какой механизм он должен быть сконфигурирован: stateless или stateful?

Механизм stateless требует минимального конфигурирования маршрутизатора, при этом дополнительные серверы не нужны. При stateless механизме хост генерирует собственный адрес из локальной информации (MAC-адрес) и информации, предоставленной маршрутизатором. Маршрутизатор объявляет префикс, идентифицирующий подсеть, а хост использует уникальный идентификатор интерфейса. Соединив их вместе, хост получает адрес IPv6. В отсутствии маршрутизатора хост может сформировать только Link Local-адрес. Однако даже такой адрес дает ему возможность работать с машинами, находящимися в его подсети.

Автоконфигурирование по механизму stateful производится с помощью DHCPv6. В случае stateful хост получает адрес интерфейса и/или другую информацию с сервера (адреса DNS, как вариант). Администратор сети может определить, какой способ будет использоваться при помощи специальных ЮМРуб-сообщений Router Advertisement messages. Механизмы stateless и stateful могут дополнять друг друга и использоваться совместно.

Stateless может использоваться, когда точные адреса непринципиальны. Stateful, наоборот - когда требуется выдача конкретных адресов конкретным хостам.

Адрес IPv6 выдаётся на фиксированное (либо бесконечное) время. Каждый адрес привязан к интерфейсу в течение

времени жизни. По истечении времени жизни адрес теряет связь с интерфейсом и может быть присвоен другому хосту в Интернете. Чтобы избежать возможных проблем, время жизни адреса делится на две стадии:

preferred - использование адреса предпочтительно;
deprecated - адрес, который вскоре будет утрачен.

Новые соединения должны использовать адрес в состоянии preferred. Адрес deprecated может использоваться только приложениями, которые уже используют его и пока не могут переключиться на новый адрес. Для решения проблем с уникальностью 1Ру6-адресов существует механизм Duplicate Address Detection. Маршрутизаторы также имеют Link Local-адрес, полученный аналогичным образом.

Взаимодействие в смешанных средах

Поскольку осуществить переход с IPv4 на IPv6 в короткий срок - задача неосуществимая, было разработано несколько технологий взаимодействия в смешанных средах. Это: туннелирование, двойной стек и трансляция протоколов.

Суть туннелирования состоит в том, что пакет данных IPv6 инкапсулируется в данные пакета IPv4. Такой пакет IPv4 содержит в себе два заголовка IPv6 и IPv4, что в свою очередь позволяет передавать его через обычные IPv4-сети. Он доставляется к узлу декапсуляции, где производится отбрасывание заголовка IPv4 и передача данных к 1Ру6-устройству. В зависимости от того, где происходит инкапсуляция и декапсуляция, выделяют три вида туннелирования: «Маршрутизатор - Маршрутизатор», «Хост - Маршрутизатор»,«Маршрутизатор - Хост».

Реализация двойного стека подразумевает поддержку устройством одновременно протоколов IPv6 и IPv4. Первая поддержка двойного стека появилась в Windows XP и Windows Server 2003, где администраторы могли дополнительно установить компонент протокола IPv6.

И последний вариант - трансляция протокола. Сама трансляция не что иное, как согласование двух протоколов путем преобразования сообщений, поступающих от одной сети в формат другой сети. Один из вариантов заключается в использовании протокол-шлюзов, размещенных на границах между 1Руб-сетями и 1Ру4-сетями.

Зло или неизбежность?

Пару лет назад, после публикации предварительного RFC, согласно которому переход на IPv6 должен завершиться до 2011 года, на одном из форумов был проведет опрос. Системным администраторам было задано два вопроса: планируют ли они переход на IPv6 и как они к нему относятся.

Самыми популярными ответами стали: «Я еще не размышлял на эту тему» и «IPv6 - это неизбежное зло, с которым придется мириться». Результаты очень хорошо отражали развитие IPv6 в России. Хотя с того времени прошло около двух лет, ситуация кардинально не изменилась. Если верить сайту ipv6.ru, сегодня по количеству выделенных блоков 1Ру6-адресов Россия занимает 19-е место в Европе и 29-е место в мире. Посмотрев за пределы России, можно увидеть отсутствие поддержки IPv6 на большинстве популярных ресурсов, что явно не ускорит переход.

В любом случае набором минимальных 1Ру6-знаний системный администратор должен обладать, дабы не впадать в ступор при виде результата ipconfig в Windows 7. EOF

Визитка

АНДРЕЙ БИРЮКОВ, специалист по информационной безопасности. Работает в крупном системном интеграторе. Занимается внедрением решений по защите корпоративных ресурсов

Обзор технологии Geneva

Построение распределенным гетерогенным систем

Построение распределенных гетерогенных систем на базе федеративных отношений — важная задача в крупных корпоративных сетях. Рассмотрим решение Microsoft Geneva Server

Суть технологии

Современная корпоративная сеть может содержать десятки и даже сотни различных бизнес-приложений, каждое из которых, как правило, наделено встроенной системой аутентификации. Большинство из этих приложений можно интегрировать с каталогом ШАР и, в частности, со службой Active Directory. Возможность аутентификации через AD позволяет избавить пользователя от необходимости многократного ввода паролей при входе в различные приложения.

Однако нередко возникает необходимость в предоставлении доступа к корпоративным приложениям сторонних компаний (схема Business To Business, B2B). Более того, возможны ситуации, когда на стороне пользователя установлена операционная система, не принадлежащая к семейству Windows.

Если для небольших компаний это, как правило, не так актуально, то для организаций с численностью пользователей более 100 человек средство управления доступом просто необходимо, так как иначе существенная часть рабочего времени у системных администраторов будет уходить на решение проблем, связанных с доступом пользователей к приложениям. Например, сброс забытых паролей или разблокирование учетных записей после нескольких попыток некорректного входа.

Для решения задач управления доступом и идентификацией существует ряд приложений от различных производителей, представляющих собой единую точку входа (Single Sign On).

На практике это выглядит примерно так: вы один раз вводите свои учетные данные и затем получаете доступ ко всем приложениям без повторной авторизации, а система SSO осуществляет подстановку ваших учетных данных в приложение. При этом вы можете посещать как локальные ресурсы, так и веб-сайты, а также ресурсы компаний-партнеров, с которыми установлены доверительные отношения в рамках домена Active Directory.

Одним из продуктов по управлению идентификацией является решение компании Microsoft, которая выпустила вторую бета-версию системы Geneva. Данный продукт предназначен для контроля личности пользователей при регулировании доступа к приложениям и системам под названием Geneva Server. По информации разработчика, на более ранних стадиях этот проект носил кодовое наименование Zermatt (Церматт, известный курорт в Швейцарии на северном склоне г. Маттерхорн).

Технология Geneva - это один из важнейших компонентов для соединения службы каталогов Active Directory с другими платформами управления всеобщей идентификацией. По словам разработчиков, Geneva является открытой платформой, которая облегчает доступ пользователей к самым разным приложениям и системам, установленным в локальной сети или в так называемом облаке.

Облачные вычисления на сегодня - одно из наиболее перспективных направлений, разработкой приложений для которых сейчас занимается множество компаний, поэтому неудивительно, что Geneva поддерживает данную технологию.

Прежде чем приступить к описанию непосредственно технологии Geneva, мне хотелось бы рассказать о технологических решениях Microsoft, на основе которых построена система управления доступом.

Учетные данные, которые система управления доступом предоставляет приложению, это так называемый токен (Token), то есть набор байтов, в котором закодированы имя пользователя, группа, к которой он принадлежит, и другие сведения, необходимые приложению. Данный токен подписывается цифровой подписью администратора информационной безопасности, который отвечает за создание и контроль целостности токена.

Также система управления доступом использует службу Security Token Service (STS), которая осуществляет выпуск и отзыв токенов. Взаимодействие с STS проиллюстрировано на рис. 1.

Архитектура и описание компонентов

Сегодня существует ряд открытых решений, позволяющих осуществлять взаимодействие с различными приложения-

ми. Поэтому перед Microsoft стоит непростая задача, так как необходимо предложить решение для взаимодействия с различными приложениями, которое бы позволяло дорабатывать Microsoft Geneva для работы со специфичными приложениями.

Однако если Microsoft предложит удобный способ миграции на свою новую технологию, масштабы использования Geneva могут оказаться огромными - ведь с помощью Geneva пользователь сможет употреблять свой единый «паспорт» формата Windows LiveID для доступа к любым корпоративным приложениям и публичным системам как внутри сети, так и с домашнего компьютера или мобильного терминала.

По собственному опыту могу отметить, что для решений Single Sign On важнейшим элементом является возможность их доработки под конкретные приложения. Дело в том, что большинство решений по умолчанию поддерживают интеграцию с такими системами, как Active Directory, Lotus Domino, Novell EDirectory и другими широко распространенными приложениями. Но при этом в любой крупной организации всегда найдутся «самописные» программы, которые применяются только в данной организации, и требующие интеграции с SSO. Здесь и начинаются проблемы, потому что, как правило, «самописное» приложение не поддерживается. В таких случаях обычно разработчики предлагают осуществить интеграцию с требуемым приложением за дополнительную (немалую) плату. Это не всегда устраивает заказчиков, в результате продукты SSO не приобретаются. Поэтому Single Sign On решение должно не только поддерживать набор определенных приложений, но и включать в себя средства для интеграции с приложениями заказчика.

Для решения таких задач в Geneva Server Microsoft предлагает разработчикам технологию Geneva Framework для быстрого создания .NET-приложений, умеющих работать с «удостоверениями на предъявителя» (claims-based application), и вынесения механизмов идентификации пользователя за рамки приложений. Конечно, есть опасения, что данный Framework позволит интегрироваться далеко не со всеми приложениями в силу различных программных ограничений, традиционно используемых Microsoft.

Еще одним ключевым компонентом платформы Geneva является технология Windows CardSpace. Она управляет непосредственно пользователями и приложениями, с которыми устанавливается контакт. В дополнение к этому в платформе Geneva реализована поддержка протокола SAML 2.0 (Security Assertion Markup Language - язык, предназначенный для описания и разметки различных параметров безопасности и ограничения доступа) и общая модель идентификации пользователей, которые являются частью комплексного подхода к установлению и проверке личности пользователей.

Отдельно следует отметить тесную интеграцию с «облачными вычислениями». Для этого предназначена разработка Microsoft под названием Azure. К сожалению, этот продукт пока не вышел. Однако уже анонсирована тесная интеграция с «облачной» платформой Azure, которая вскоре позволит разработчикам создавать свои приложения, размещаемые в собственном или внешнем «облаке». В этом случае технология Geneva станет незаменимым инструментом для единой авторизации пользователей при доступе к любым локальным и «облачным» приложениям.

Пакет Geneva Server Beta 2 содержит семь новых функций. В частности, новая версия Geneva поддерживает единый механизм коллективной работы с документами в SharePoint 2007 - теперь пользователям не придется вводить массу дополнительных паролей при защищенном доступе к приложениям извне корпоративной сети. Также в новой версии появились шаблоны для среды разработки Visual Studio, которые предлагают разработчикам готовую логику безопасности, необходимые инструменты и компоненты для .NET-приложений.

Кроме того, в пакете Geneva Beta 2 разработчики и администраторы могут устанавливать «федеративные» отношения между Geneva Server и шлюзом Microsoft Federation Gateway одним щелчком мыши: в этом случае действие локальных удостоверений, созданных в Active Directory, можно распространить на «облачные» сервисы. Также Geneva Server Beta 2 предоставляет сквозное управление процессом выпуска, обращения и отзыва удостоверений. Если администратор создает такие удостоверения, то лю-

Рисунок 1. Схема работы с STS

Рисунок 2. Аутентификация с использованием Geneva Server

Кстати

Облачные вычисления (cloud computing, также используется термин «Облачная обработка данных») - технология обработки данных, в которой программное обеспечение предоставляется пользователю как интернет-сервис. Пользователь имеет доступ к собственным данным, но не может управлять и не должен заботиться об инфраструктуре, операционной системе и собственно программном обеспечении, с которым он работает.

бой авторизованный пользователь автоматически получает клиентский модуль CardSpace при входе в «федеративное» приложение. Процесс загрузки CardSpace-клиента выполняется незаметно для пользователя, обеспечивая единую регистрацию для доступа ко всем разрешенным ресурсам.

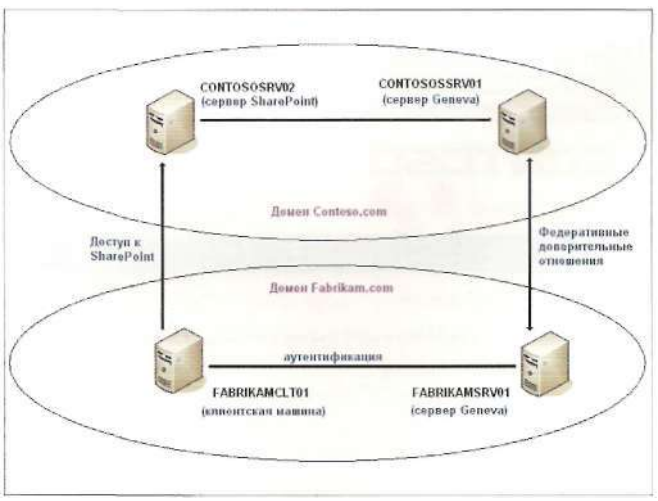
Новая бета-версия Geneva Server поддерживает федеративные сервисы управления правами доступа. Новый механизм преобразования заявок авторизации в Geneva Server позволяет расширить перечень источников таких заявок на службу каталогов Active Directory, базы данных SQL и другие нестандартные хранилища атрибутов. Заключительным новшеством стала расширенная поддержка протокола SAML - теперь в Geneva Server реализованы механизмы WS-Trust и WS-Federation для согласования и обмена ключами в веб-сервисах.

Демонстрируя широкую совместимость со сторонними системами и приложениями, требующими надежной авторизации пользователей, компания Microsoft заявила о своих планах по тестированию Geneva Server вместе с такими продуктами, как CA Federation Manager, CA SiteMinder, Novell Access Manager, SAP NetWeaver, Sun OpenSSO Enterprise и Fedlet.

Сейчас компания SAP уже ведет тестирование SAML-ключей безопасности, которые генерирует Geneva Server, для установки соединений между веб-сервисами и .NET-приложениями.

Компании Novell, Sun и CAтоже предлагают возможности взаимодействия со своими системами для контроля идентификации и доступа с использованием протоколов SAML 2.0 MWS.

Рисунок 3. Схема взаимодействия



Ранее компания Microsoft сообщала о тесном сотрудничестве с разработчиками пакетов IBM Tivoli и Shibboleth для обеспечения их совместимости с Geneva Server.

Существующая реализация

Желающие развернуть и протестировать данную технологию могут скачать стенд, расположенный по адресу [1], состоящий из виртуальных машин, имитирующих рабочую среду, необходимую для Geneva Server. Правда, полный архив данного стенда имеет размер порядка 14 Гб и требует для запуска Hyper-V, что накладывает некоторые ограничения на тестирование в домашних условиях. По адресу [2] можно найти достаточно подробное, русскоязычное описание работы данного стенда и реализации взаимодействия Geneva и Sharepoint.

Если рассматривать вкратце то, реализацию виртуальной среды для Microsoft Geneva, то она состоит из двух доменов Active Directory (contoso.com и fabrikam.com), каждый из которых принадлежит отдельной организации. Между этими доменами установлен Federated Trust, также в Contoso развернут Sharepoint (см. рис. 3).

В результате развертывания данной виртуальной среды решаются следующие задачи:

- С помощью сервера Geneva обеспечивается ролевая и пользовательская аутентификация на сайте SharePoint внутри домена Contoso.
- Установлены доверительные отношения между двумя компаниями с помощью серверов Geneva и обеспечен аналогичный доступ некоторых сотрудников из Fabrikam.
- SQL Server используется в качестве альтернативного (по отношению к AD) хранилища информации о ролях и пользователях.
- Защита документов и библиотек в SharePoint с помощью Active Directory Rights Management Services.

При этом для входа в консоль Sharepoint можно будет использовать Windows Integrated Authentication. Хотя возможность использовать для входа в систему доменных учетных данных остается (см. рис. 2).

Конечно, для подключения Single Sign On на основе Geneva необходимо выполнить ряд нетривиальных действий, однако единая точка входа позволяет существенно упростить работу как пользователям, так и системным администраторам.

***

В заключение хочу отметить, что новый продукт обладает большим количеством возможностей и будет весьма полезен для крупных компаний. Пока доступна только бета-версия данного продукта. По заявлениям разработчиков, финальную версию Geneva Server планируется выпустить до конца 2009 года. EOF

1. http://technet.microsoft.com/ru-ru/dd440951 (en-us).aspx - виртуальные машины со стендом для Geneva Server (общий объем около 14 Гб).
2. http://alexlomakin.spaces.live.com/blog/cnsIFC35D86765D2ECDC!256.entry - русскоязычная документация по развертыванию стенда Geneva Server.

Переполнение буфера в avast! Home/Professiona!

Программа: avast! Home/Professional 4.8.1351, возможно, другие версии.
Опасность: Низкая.
Наличие эксплоита: Да.
Описание: Уязвимость существует из-за ошибки проверки границ данных в драйвере ядра aswMon2.sys при обработке IOCTL. Локальный пользователь может с помощью специально сформированного 0xB2C80018 IOCTL вызвать переполнение стека и выполнить произвольный код на системе с привилегиями учетной записи SYSTEM.
URL производителя: www.avast.com/eng/desktop_protection.html.
Решение: В настоящее время способов устранения уязвимости не существует.

Повышение привилегий в FreeBSD

Программа: FreeBSD 6.3, 6.4.
Опасность: Низкая.
Наличие эксплоита: Да.
Описание: Уязвимость существует из-за ошибки после освобождения, вызванной ошибкой состояния операции в реализации канала close(), относящегося к kqueues. Локальный пользователь может выполнить произвольный код на системе с привилегиями ядра.
Примечание: Производитель выпустил дополнение, которое не позволяет эксплуатацию уязвимостей разыменования нулевого указателя.
URL производителя: www.freebsd.org
Решение: Установите исправление с сайта производителя.

Отказ в обслуживании в IBM Informix Dynamic Server

Программа: IBM Informix Dynamic Server версии до IDS 10.00.xC11, 11.10.xC4 и 11.50.XC5.
Опасность: Низкая.
Наличие эксплоита: Нет
Описание: Уязвимость существует из-за неизвестной ошибки при обработке JDBC-подключений. Удаленный пользователь может отправить приложению слишком длинный пароль (более 511 символов) и аварийно завершить работу приложения.
URL производителя: www-306.ibm.com/software/data/informix/ids.
Решение: Установите последнюю версию IDS 10.00.xC11, 11.10.xC4 или 11.50.xC5 с сайта производителя.

Уязвимость в реализации WebDAV в riginx

Программа: nginx 0.7.62 и более ранние версии.
Опасность: Низкая.
Наличие эксплоита: Нет
Описание: Уязвимость существует из-за того, что nginx недостаточно проверяет пути для WebDAV-методов MOVE и COPY. Удаленный пользователь может записать файлы за пределы корневой директории сервера. Для успешной эксплуатации уязвимости требуется, чтобы сервер был собран с поддержкой http_dav_module и атакующий должен иметь привилегии на использование методов MOVE или COPY.
URL производителя: nginx.net.
Решение: В настоящее время способов устранения уязвимости не существует.

Использование небезопасной AH-функции OleLoadFromStreamO в Microsoft Windows ActiveX-компонентах

Программа: Microsoft Windows 2000; Microsoft Windows XP; Microsoft Windows 2003; Microsoft Windows Vista; Microsoft Windows 2008; Microsoft Windows 7.
Опасность: Критическая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за того, что различные ActiveX-компоненты используют небезопасным образом уязвимую ATL-функцию OleLoadFromStream().
Примечание: согласно Microsoft, эта уязвимость используется в целевых атаках в настоящий момент.
URL производителя: www.microsft.com.
Решение: Установите исправление с сайта производителя.

Уязвимость форматной строки в службе авторизации в VMware

Программа: VMware Workstation 6.5.3 build 185404, возможно, другие версии; VMware Player 2.5.3 build 185404, возможно, другие версии.
Опасность: Низкая.
Наличие эксплоита: Да.
Описание: Уязвимость существует из-за ошибки форматной строки в VMware Authorization Service (vmware-authd.exe версия 6.5.3.8888) при обработке запросов на авторизацию. Удаленный пользователь может отправить процессу vmware-authd (порт 912ДСР) специально сформированную строку и аварийно завершить работу службы.
URL производителя: www.vmware.com.
Решение: В настоящее время способов устранения уязвимости не существует.

ВЛАДИМИР ГАКОВ, журналист, писатель-фантаст, лектор. Окончил физфак МГУ. Работал в НИИ. С1984 г. на творческой работе. В 1990-1991 гг. - Associate Professor, Central Michigan University. С 2003 г. преподает в Академии народного хозяйства. Автор 8 книг и более 1000 публикаций

Персональное дело IBM

Вся правда об империи «Голубого гиганта»»

Долгим и полным драматизма оказался путь от первых электромеханических счетных машин, с которых начинали создатели компании, до суперкомпьютера RS/BOOO SP

Перепись населения как двигатель прогресса

Последний год XX века ознаменовался сразу двумя юбилеями в компьютерном мире. В 2000 году исполнилось 90 лет корпорации, со временем принявшей название International Business Machines (IBM). И 20 лет - созданной ею же первой «персоналке», персональному компьютеру. Долгим и полным драматизма оказался путь от первых электромеханических счетных машин, с которых начинали создатели IBM, до суперкомпьютера RS/6000 SP (в просторечии - Deep Blue), уже обладающего достаточным «интеллектом», чтобы победить за шахматной доской чемпиона мира.

У истоков «Голубого гиганта» (Big Blue), как называют IBM во всем мире, стоял выходец из Германии Герман Холлерит. Он работал в Федеральном агентстве по переписи населения (U. S. Census Bureau) и на протяжении многих лет пытался построить электромеханическую машину для оптимизации трудоемкого процесса - обработки результатов этой самой переписи.

В 1890 году такая машина, работавшая с использованием перфокарт, была построена и сразу же прошла боевое крещение. Если обработка результатов переписи населения в 1880 году потребовала семи лет и труда 1500 сотрудников, то на сей раз изобретение Холлерита позволило его ведомству справиться всего за три года! За это время всего 700 человек заполнили учетные карточки на 63 миллиона американских граждан.

Результаты оказались столь многообещающими, что окрыленный успехом Холлерит спустя шесть лет основал собственную фирму Tabulating Machine Company, главным направлением которой стали производство и продажа специального оборудования для перфорирования карточек. 15 июня 1911 года компания слилась с двумя другими, созданными чуть раньше, - Bundy Manufacturing Company и Computing Scale Company of America. Новая корпорация была зарегистрирована в штате Нью-Йорк как Computing-Tabular-Recording Company (CTR) и занялась выпуском разнообразных счетных машин и измерительных приборов. В 1924 году она окончательно поменяла название на ныне всем известное International Business Machines.

Хотя мало кто сегодня именует лидера компьютерного бизнеса полным именем, предпочитая краткое - IBM. А как же иначе - изделия со знакомой латинской аббревиатурой давно перестали быть только офисной техникой, превратившись для миллионов людей в друзей, собеседников, помощников, партнеров.

Начав с выпуска устройств для изготовления и чтения перфокарт, IBM затем переключилась на пишущие машинки. Их в свою очередь сменили электромеханические калькуляторы, а в 1950-е годы - компьютеры. К тому времени число сотрудников корпорации перевалило за 40 тысяч человек, а фабрики и отделения IBM, кроме нью-йоркской штаб-квартиры, были разбросаны в десятке стран Европы, Азии и Южной Америки.

Во имя отца и сына

Своими успехами компания была обязана двум Томасам Уотсонам - отцу и сыну. Старшего пригласили в CTR на должность исполнительного директора в 1914 году - одновременно с рождением сына. И уже год спустя 41-летний Томас Уотсон-старший занял президентское кресло.

В первый же год своего президентства он распорядился вывесить на стенах всех кабинетов и прочих помещений компании таблички, на которых заглавными буквами было написано всего одно слово - THINK (думай). Этот фирменный девиз будущей IBM стал своего рода священной мантрой для персонала, постоянно напоминая сотрудникам, что в этой организации от них ждут прежде всего творческого отношения к порученной работе, интеллектуальных усилий и только во вторую очередь - исполнительности.

Кроме того, Уотсон обогатил словарь корпоративных лозунгов XX века принципом: «Успех клиента - наш успех». Сегодня это кажется настолько очевидным для создателей «средств производства» для бизнеса - компьютеров, что многие даже не представляют себе, что и у этой крылатой фразы был конкретный автор. Позже к афоризмам президента компании прибавился еще один корпоративный слоган: «Тех, кто покупает продукты IBM, с работы не увольняют».

С именем Уотсона-старшего связано еще несколько революционных нововведений, преобразивших лицо компании. С фанатичным упорством истинного протестанта он старался привить всем сотрудникам, от руководителя до последней уборщицы, чувство корпоративной лояльности, организуя спортивные команды и общие пикники и торжества. Даже в черные для американского бизнеса годы Великой депрессии корпорация IBM под руководством Уотсона думала не только о прибылях, но и о том, как удержать персонал на рабочих местах. Она одной из первых внедрила систему групповой пожизненной страховки (в 1934-м) и оплачиваемого отпуска (в 1936-м). И продолжала наращивать производство, невзирая на катастрофическое падение спроса на счетные устройства. В 1931 году - в самый разгар кризиса, когда о развитии бизнеса мог думать только умалишенный, компания Уотсона представила публике новую серию счетных машин - IBM 600.

Правда, спустя год небо над IBM заволокло другим «облаком»: конкуренты подали на компанию в суд за нарушение антимонопольного законодательства. Тогда дело удалось замять - в ситуации, когда практически весь бизнес в Америке «стоял», вопрос о монополизации рынка был явно неактуальным. Но первый тревожный звонок оказался далеко не последним - повторение последовало, правда, спустя три десятилетия.

Зато поразительное упрямство и жизнестойкость корпорации IBM и ее президента принесли свои плоды на другом направлении - речь идет о правительственных заказах.

В 1935 году конгресс принял закон о социальной помощи (Social Security Act), и для оформления миллионов документов в качестве подрядчика нужна была солидная компания, имеющая опыт в обработке данных. Правительство остановило свой выбор на IBM, подписав с компанией контракт на составление досье занятости для 26 миллионов человек.

В 1937 году титаническая работа была успешно завершена.

Запуск компьютера

После этой «крупнейшей счетной операции в истории» на IBM один за другим посыпались заказы. Уже на следующий год компания переехала на престижную нью-йоркскую Мэдисон-авеню, что для всех стало сигналом: IBM уверенно влилась в элиту американского бизнеса.

Со вступлением США во Вторую мировую войну компания вынуждена была перепрофилироваться - теперь она выпускала авиационные прицелы для бомбометания, стрелковое оружие, детали к моторам (всего более 40 наименований). Уотсон (до войны, кстати, весьма симпатизировавший Гитлеру!) установил на эти изделия номинальную прибыль в 1%, а на вырученные деньги основал фонд помощи вдовам и сиротам - жертвам войны.

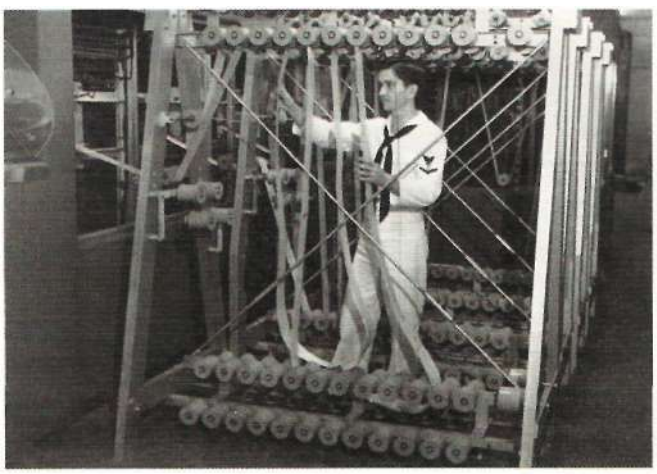
В 1956-м президентскую эстафету от Томаса Уотсона-старшего принял его сорокалетний сын. Уотсон-младший поступил работать в компанию отца еще в 1937 году, а электроникой «заболел» в начале 1946-го. Тогда его пригласили вместе с другими специалистами в университет штата Пенсильвания на демонстрацию новейшего чуда техники - первого электронного компьютера ENIAC. «Я был поражен, - вспоминал Уотсон, - скоростью работы электронных схем, но меня беспокоило, что в наших лабораториях не было специалистов, которые бы в этом разбирались».

Действительно, ни один американский университет в ту пору не готовил специалистов-компьютерщиков - просто за неимением специальности! Новый глава IBM первым из коллег озаботился созданием «кузницы кадров», выбрав в качестве таковой знаменитый Массачусетский технологический институт (MIT). Компания передала в дар институту большой компьютер и профинансировала его эксплуатацию. А спустя пять лет IBM приняла на работу сразу несколько десятков свежеиспеченных специалистов.

И меткие тоже мажут

«Я думаю, мировой рынок компьютеров вряд ли превысит пять штук». Удивительно, но этот приговор вынесен в 1943 году никем иным, как Томасом Уотсоном-старшим. Впрочем, он знал, о чем говорил. Первые электронные вычислительные машины были огромны, необычайно прожорливы (в смысле потребления электроэнергии) и капризны - после решения конкретной задачи их приходилось вручную переключать на решение следующей. И все же «попадание в молоко» одного из лучших прогностических «снайперов» эпохи по-своему показательно: от ошибок не застрахованы даже самые проницательные.

«Стол Холлерита»



Компьютер во времена Второй мировой

Кто кого учит

Сегодня может показаться забавной информация о том, что одной из главных сенсаций брюссельской Всемирной ярмарки 1958 года была новинка от IBM - первый жесткий магнитный диск RAMAC. А забавно то, что посетители на десяти языках экзаменовали «железяку» по истории - не подозревая, что сами присутствуют при одном из ее драматичных поворотов.

В первое послевоенное десятилетие спрос на вычислительные машины превысил все мыслимые прогнозы: ежегодный прирост (заявок, а не машин) достигал 22%. IBM без особых проблем перешла на выпуск компьютеров, «приучив» рынок к своему бренду, под которым продавалась ее электромеханическая вычислительная техника. К тому же еще Уотсон-старший заложил в компании основы системы, которую вскоре приняли многие производители - поставлять не только «железо», но и весь спектр сервиса к нему.

Первые компьютеры IBM были, естественно, ламповыми, но уже к концу 1950-х годов лампы оказались полностью вытеснены транзисторами. «Голубой гигант» не сплоховал и тут - первым в мире наладил их промышленное производство, открыв соответствующую фабрику в Нью-Йорке.

В 1959 году компания выпустила свой первый полностью транзисторный mainframe - модель IBM 7090 с быстродействием 220 тысяч операций в секунду. Она использовалась как военными, так и на «гражданке». ВВС оснастили ею систему раннего оповещения о запусках баллистических ракет, а авиакомпания American Airlines на базе двух 7090-х машин первой внедрила автоматизированную систему бронирования билетов (SABRE), связавшую пункты продажи билетов в 65 городах страны.

В 1961 году сотрудники упомянутого Массачусетского технологического института на базе компьютера IBM 7094 совершили еще один технологический скачок - создали систему, способную одновременно обслуживать до 30 удаленных пользователей (позже это назвали «системой с разделением времени»). Теперь любой пользователь мог подключаться со своего пульта к большой ЭВМ, находившейся хоть в другом городе.

IBM вместе с MIT продолжила развивать наступление на этом направлении, и успехи не заставили себя ждать. Если к 1965 году в мире насчитывалось восемь таких систем (пять в США и три во Франции), то в следующем году - уже более 30, причем половина из них предназначалась для коммерческих расчетов. Это привело к резкому удешевлению компьютерного времени: в следующем году средняя стоимость часа работы на терминале составляла в США около $15, а средняя арендная месячная плата за него не превышала $200.

За пять лет IBM собиралась продать около 250 тысяч «микрокомпьютеров» (так именовались будущие PC). Пятилетний план был выполнен за месяц!

«Железный» век

Другим направлением, на котором IBM добилась значительных результатов, стало увеличение объемов машинной памяти. В 1956 году специалисты исследовательской лаборатории корпорации в Сан-Хосе, штат Калифорния, создали первый жесткий магнитный диск RAMAC 305 с емкостью памяти 5 Мб.

В апреле 1964 года IBM представила новую модель - IBM/360, которой также было суждено войти в историю. Журнал Forbes назвал ее «азартной игрой с $5 млрд на кону» - ровно столько вложила компания в разработку новинки, занявшую четыре года. Эта сумма превышала затраты правительства США на реализацию знаменитого проекта Manhattan - создание атомной бомбы - и была беспрецедентной для частной компании в то время.

Фактически речь шла о шести моделях, принадлежавших к одному семейству компьютеров на интегральных схемах. А главным новшеством стало то, что все члены этого семейства были совместимы - иначе говоря, допускали постоянное обновление как программного оборудования, так и периферии. Теперь вместо того чтобы каждый раз покупать новую машину, достаточно было заменить лишь ряд существенных элементов на более «продвинутые».

Вообще в сфере информационных технологий 1960-е годы вошли в историю как эпоха бурно прогрессирующего «железа» - за десять лет сменилось два поколения компьютеров! Если первую половину декады на рынке доминировало «второе поколение» с транзисторами вместо ламп и магнитными лентами и дисками вместо перфолент, то появление 360-й модели знаменовало собой приход «третьего». Его отличительными особенностями стали интегральные схемы на микрочипах и управляющие ресурсами компьютера операционные системы.

В эти годы позиции «Голубого гиганта» на рынке больших машин стали практически неуязвимыми. Компьютеры IBM обслуживали научные центры и промышленные предприятия, а также трудились на американскую оборону на земле, на воде (и под водой) и в воздухе. И даже за пределами земной атмосферы - бортовые ЭВМ для космических аппаратов Gemini и Apollo, а также машины для систем управления полетами в Хьюстонском центре управления полетами были изготовлены специалистами IBM.

В 1971 году Уотсон-младший покинул IBM, но до середины 1980-х бывший глава корпорации оставался членом совета директоров. Он много сделал, чтобы вывести IBM в лидеры американского бизнеса: годовой доход компании вырос с $900 млн в 1965 году (когда сын заменил отца) до $8 млрд, а число сотрудников - с 72 тысяч до 270 тысяч. Во времена, когда Билл Гейтс еще осваивал арифметику в школе, такой взлет одной отдельно взятой компании, причем не сырьевой - высокотехнологичной! - представлял собой явление беспрецедентное.

Из достижений IBM этого десятилетия можно отметить первый жесткий диск типа «винчестер» и принципиально новое печатающее устройство на основе лазерной технологии. Однако в последнем случае лавры первопроходца компания делит с фирмой Xerox, вырвавшейся в итоге вперед. Исследователи до сих пор расходятся во мнении, какая модель появилась на рынке раньше - Xerox 9700 или IBM 3800, во всяком случае оба лазерных «динозавра» стоили друг друга. В том числе буквально: цена каждого доходила до $350 тыс.

Но к концу 1970-х небо над «Голубым гигантом» снова заволокло тучами. Внешне все обстояло как нельзя лучше - заказы на большие машины для правительства и крупной промышленности обеспечивали годовой оборот свыше $30 млрд. Однако и конкуренты не дремали. Не имея возможности открыто бросить вызов гиганту на рынке, они усилили давление на IBM через суд.

Руководство компании понимало, что рано или поздно антимонопольное ведомство возьмется за нее всерьез - и срочно начало разрабатывать эффектную контрмеру против обвинений в монополизме.

Кошмар архитектора

Конкретно перед сотрудниками компании была поставлена на первый взгляд неразрешимая задача. А именно - создать нечто доселе невиданное. С одной стороны, это «нечто» открывало бы рынок для конкурентов (только и ждущих своего часа), а с другой - сохраняло бы для IBM шансы и самой заработать на новинке!

На выполнение задачи была брошена группа из двенадцати сотрудников во главе с Уильямом Лоуи. Чуть больше года - с июля 1980 года по август 1981-го - его «спецкоманда» провела в лаборатории специально созданного отделения микрокомпьютерных систем IBM во флоридском городе Бока-Бэтоне. В результате добровольного «заточения» 17 августа родился первый в мире персональный компьютер.

В тот день вряд ли даже сами разработчики отдавали себе отчет, что только что совершили настоящую технологическую революцию. И не только технологическую. Потому что с приходом в нашу повседневную жизнь «персоналок» мир разительно изменился.

Модель IBM 5150 Personal Computer (IBM PC) представляла собой собственно вычислительное устройство (без жесткого диска, но с 16 Кб оперативной памяти - и возможностью расширения до 256 Кб), черно-белый монитор и выносную клавиатуру. Система строилась на своеобразной «триаде», состоявшей из процессора 8088 малоизвестной тогда компании Intel, поставляемой на отдельной дискете операционной системы DOS 1.0 (ее создала вообще никому не известная фирма во главе с каким-то гарвардским студентом-недоучкой) и, самое главное, системной платы с разъемами, позволявшими подключать к машине дополнительные устройства. Все вместе реализовало концепцию так называемой открытой архитектуры - она-то и поставила крест на монополии IBM.

Компьютерный десант за «железный занавес»

В 1979 году президент Джеймс Картер назначил экс-главу IBM... послом в Советском Союзе. На этом посту Томас Уотсон-младший проработал три года и, наверное, дорого бы отдал за то, чтобы разузнать, что же такого наработали в компьютерной отрасли его советские коллеги. А они, начиная с 1960-х, следовали господствующим тогда установкам свыше - «не изобретать велосипед», старательно копируя те же «забугорные» IBM 360/370 (у нас это называлось ЕС - «Единой серией»). Хотя более ранние советские разработки 1950-х - серия БЭСМ («Большая электронно-счетная машина») - были вполне достойным продуктом для своего времени даже по мировым меркам.

Если не вдаваться в дебри, то «открытая архитектура» означала, что теперь производить комплектующие и писать программы для «персоналки» IBM мог кто угодно.

Итак, задача была решена, но решение оказалось весьма противоречивым, если не сказать больше. С одной стороны, IBM приобретала рекламу, о какой не могла и мечтать. Теперь покупатель персонального компьютера, пусть даже изготовленного другим производителем, первым делом интересовался у продавца: а совместима ли модель с IBM PC? С другой стороны, подобные машины отныне мог выпускать любой - «открытая архитектура» не оставляла никаких надежд на защиту торговой марки в виде патентных заслонок.

Так и случилось. Начался бурный процесс электронного клонирования. Не прошло и года, как на рынке поя-

Томас Уотсон-старши?

Томас Уотсон-младший

вились первые IBM PC-совместимые компьютеры - портативный Hyperion компании Dynalogic и настольный MPC фирмы Columbia Data Products. Чуть позже к дележу «персонального» пирога подоспели будущие гиганты компьютеростроения - Compaq и Dell, после чего процесс размножения «клонов» пошел лавинообразно. Именно тогда две короткие аббревиатуры IBM и PC в сознании миллионов превратились в синонимы.

Конечно, и IBM урвала себе солидный кусок - и даже больше, чем рассчитывала! Пока команда Лоуи творила историю под жарким солнцем Флориды, исследовательский центр IBM в Соммерсе, штат Нью-Йорк, выпустил отчет «Следующие пять лет» - своего рода бизнес-план компании на текущую пятилетку. О персональных компьютерах там не было ни слова - что и понятно: еще не успели изобрести термин. Но и роль создаваемых «микрокомпьютеров» (так именовались будущие PC) представлялась создателям отчета малозначимой - всего лишь «терминалы нижнего уровня» в иерархической системе, управляемой большими машинами. Тем не менее IBM собиралась за пять лет продать около 250 тысяч таких «малышек».

Пятилетний план был выполнен... за один месяц! За первой ласточкой последовали модели PC XT (на базе того же 8088-го процессора Intel), PC AT (с встроенным жестким 40-мегабайтовым диском и цветным монитором EGA), PS/2... И так далее, вплоть до относительно недавних настольных NetVista и ноутбуков ThinkPad.

Однако и оснований кусать локти от досады хватало. Первый миллионный персональный компьютер «Голубой гигант» продал, вопреки оптимистическим прогнозам, лишь в 1987 году, постепенно уступая рынок другим производителям - их IBM-совместимые модели зачастую превосходили машины самой IBM. А потом пошла волна пресловутой «желтой» сборки из Тайваня и Малайзии, и о былом гордом одиночестве на рынке компьютерного «железа» пришлось забыть раз и навсегда.

Голубая фишка

К тому же «открытая архитектура» позволила максимально нажиться на новинке совсем не производителям компьютеров, но иным участникам рынка. Последующие модели «персоналок» IBM уже никто не называл по имени - только по номеру процессора фирмы Intel: «386-й», «486-й», «пентиум».

И, конечно, максимум прибыли получила компания, создавшая операционную систему для первой «персоналки» - и еще множество других программ для новых поколений компьютеров. Вряд ли сегодня на планете найдется пользователь, которому были бы неизвестно название той компании - Microsoft. А имя и фамилию того студента-недоучки, возглавлявшего ее до самого последнего времени, полагаю, называть не обязательно (о нем можно прочитать в одном из номеров журнала за этот год).

Потом была затяжная война между IBM и компанией Apple (о которой журнал также писал). И недавняя продажа китайцам всего «персонального» хозяйства IBM. а именно сектора персональных компьютеров, которые теперь выходят под брендом Lenovo. Вряд ли кто-то мог предвидеть подобное и за год до исторической сделки...

Уступив лидерство на рынке производства компьютеров, IBM не пала духом, а продолжала открывать новые перспективные рынки. Эту стратегию наметил еще Уотсон-старший: искать направления, на которых возможен технологический прорыв, и именно на них развивать наступление, пока не подоспели конкуренты. Не случайно журналисты часто сравнивали IBM с айсбергом, вкладывая в это слово разные значения: и «большой», и «голубой», и не тонет, и не тает, и дрейфует по всем широтам!

Так, в самые последние годы компания выбилась в лидеры на сверхперспективном направлении ИТ-бизнеса. По данным опросов, сегодняшние пользователи ИТ-услуг рассматривают «Голубого гиганта» в качестве ведущего бренда - совсем как пользователи «персоналок» десятилетиями раньше.

А накануне миллениума - в декабре 1999 года - IBM объявила о выделении $100 млн на исследовательские работы по созданию в течение ближайших пяти лет самого мощного суперкомпьютера за всю историю. Будущий компьютерный монстр получил название Blue Gene («Голубой ген»), а его планируемая производительность должна была превзойти 1 квадриллион операций в секунду, то есть в 500 раз превысить возможности тогдашнего лидера - модели ASCI Red компании Intel.

В партнерстве с Национальной лабораторией имени Лоуренса в Ливерморе и министерством энергетики сотрудники IBM справились с поставленной задачей. Суперкомьютер был построен и приступил к работе. Слово «ген» в названии намекает на основной круг задач, которые должен решать преемник упомянутого Deep Blue, - Blue Gene будет не в шахматы играть, а помогать ученым моделировать белковые структуры человеческого организма.

Оглядываясь на пройденный путь, руководство IBM считает, что это как раз то, что корпорации удается лучше всего: «постоянно делать ставку на крупные прорывные технологии, которые изменят будущее компьютерных вычислений». EOF

Сергей Анциферов:
«Ваша изюминка - «болты и гайки»

На вопросы «СА» отвечает ведущий инженер отдела информационного обеспечения Читинского регионального филиала ОАО «Россельхозбанк»

- Почему вы читаете журнал?

- Несомненно, сейчас много полезной информации можно почерпнуть в Интернете, однако самую свежую и уникальную информацию можно найти только на страницах периодических изданий. Журнал «Системный администратор», как никто другой, лучше и детально освещает разные технические аспекты. Кроме того, я остаюсь приверженцем печатных изданий, с ними удобно узнавать новости, находясь в длительной поездке.

- Какая изюминка, на ваш взгляд, должна быть у «СА»?

- Мне кажется, что изюминка журнала присутствует со дня его первого выпуска. В журнале четко и конкретно идет описание решения той или иной задачи. С 1997 года я подписывался на многие издания по компьютерной тематике. Но практически у всех журналов статьи несут обобщенный информационно-рекламный характер. Хотелось бы и в дальнейшем видеть в «СА» больше конкретики, потому что именно за счет описания «болтов и гаек» видна целостная картина о функциональности того или иного ПО.

- Какой рубрики не хватает в журнале?

- Ко мне часто обращаются молодые специалисты, пришедшие в сферу ИТ с разными вопросами из категории для начинающих. Было бы вполне неплохо открыть цикл статей в этом направлении. Кроме того, на страницах журнала хотелось бы видеть темы, касающиеся телефонии и учрежденческих АТС, которые также лежат на плечах системных администраторов.

- Кто ваши друзья, чем увлекаетесь?

- Мои друзья разносторонние люди, но всех их объединяет одна черта - они творческие личности. Несомненно, большинство друзей работают в сфере ИТ, однако среди них есть и музыканты, и даже электрики, и монтажники пластиковых окон. Сам я тоже человек разносторонний. Помимо ИТ увлекаюсь рыбалкой и спортом. С недавних пор начал заниматься автолюбительством. В перспективе хочу начать собственный бизнес в сфере разработки прикладного ПО, можно сказать, что это мечта всей моей жизни.

Мечта моей жизни — собственный бизнес в сфере разработки прикладного ПО

- Как вы стали сисадмином?

- В школе меня всегда интересовали точные предметы, поэтому по остальным были в основном тройки, но с 8-го класса я, можно сказать, на спор подтянулся и окончил школу исключительно на «4» и «5». Первый компьютер - Yamaha я увидел в 9-м классе и буквально по уши ушел в основы изучения программирования и освоения радиоэлектроники. Написал множество программ, а на первом курсе института спаял собственный компьютер «Специалист» по материалам журнала «Моделист-Конструктор».

В нашем городе, когда я учился в школе, не было вузов, выпускающих программистов, поэтому я окончил ЧГТУ по специальности «геофизик». Один год отработал в ЗабНИИ. Принимал активное участие в научной работе «Измерение вызванной поляризации методом спада тока в питающей линии», основанной на новейшей по тем временам измерительной аппаратуре и буквально только запущенной в эксплуатацию GPS навигации.

Потом из-за финансовых трудностей в геологии я перешел в отделение Пенсионного фонда, которому посвятил восемь лет сначала в качестве программиста, а затем и в роли системного администратора. Сейчас работаю в Читинском РФ ОАО «Россельхозбанк» и выполняю задачи по сопровождению локальных и корпоративных сетей, серверов и телефонии. EOF

Системный администратор

ежемесячный журнал www.samag.ru

№11(84) ноябрь 2009

MyZCI – автоматическая инвентаризация

Виртуализируем предприятие

Черный экран тишины

Applocker: укрепляем безопасность сети

Решаем проблему внезапной блокировки учетной записи

А нужен ли банкам Linux?

Аутсорсинг: кто против?

Персональное дело IBM

ISSN 1813-5579

09011

9771813557005

Linux center