Так видит журнал читатель, который забыл оформить подписку:

НОВОГОДНИЕ КАНИКУЛЫ ЗАТЯНУЛИСЬ

БЫСТРО РАСКУПИЛИ ТИРАЖ

УЕХАЛ В ОТПУСК

ПОСЛЕ ОТПУСКА АВРАЛ НА РАБОТЕ

НЕОЖИДАННО ЗАКОНЧИЛИСЬ ДЕНЬГИ

Так видит журнал читатель, оформивший подписку:

ПОДПИШИТЕСЬ И ЧИТАЙТЕ!

Роспечать – 20780, 81655

Пресса России – 88099, 87836

Интер-почта – тел. (495) 500-00-60

№7 (80) июль 2009 Системный администратор

Системный администратор

ежемесячный журнал www.samag.ru

№7(80) июль 2009

Тратим меньше, спим больше с VMware Sphere 4.0

Профилактическое обслуживание Active Directory

Осваиваем нововведения Windows PowerShell 2.0

Кто мы: цари природы, энергобатарейки или биокомпьютеры

Дисковое хранилище NETGEAR ReadyNAS – альтернатива файловому серверу

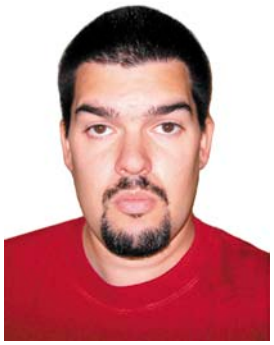
FreeBSD tips: periodic на службе сисадмина

Шифруемся на лету при помощи TrueCrypt

Понять Билла, на это способен далеко не каждый

ISSN 1813-5579

Linux Center www.linuxcenter.ru



Уважаемые читатели!

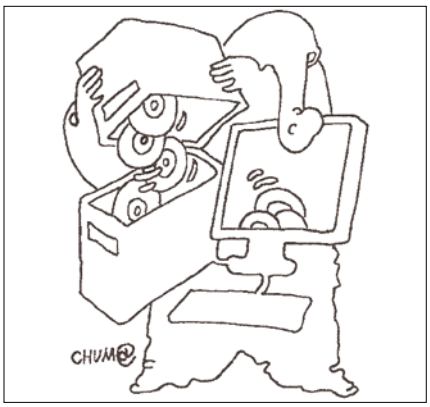
Вы, конечно, знаете, что в этом году «Системному администратору» исполняется семь лет. Детсадовский возраст позади – пора овладевать школьными премудростями.

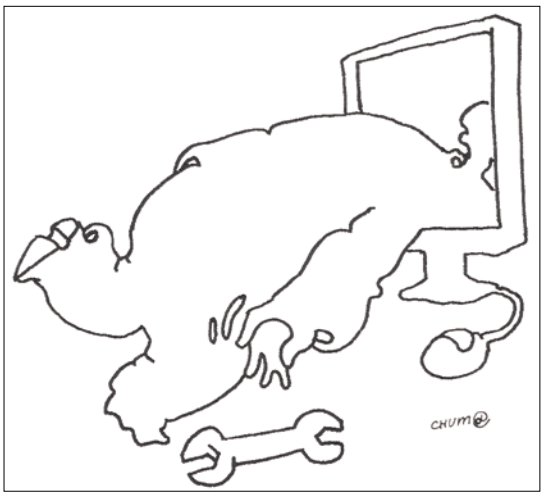
Эти первые семь лет мы прожили не впустую. О том, что получилось, судить, безусловно, вам. Но без ложной скромности хочу отметить, что нам удалось найти многих верных друзей среди системных администраторов, и, надеюсь, быть вам полезными. Об этом свидетельствует хотя бы то, что нас читают около 60 тысяч человек! А по проверенным данным, из отраслевых СМИ наш журнал предпочитают 42 процента системных администраторов.

Короче: пора двигаться дальше! Растете вы, а мы хотим расти вместе с вами. Мы отдаем на ваш суд обновленный седьмой (что символично!) номер журнала. В нем появились новые темы и рубрики, изменились макет и оформление.

Ругайте, хвалите, спрашивайте – главное, не оставайтесь равнодушными! Критикуя – предлагайте, предлагая – действуйте. И помните, что «Системный администратор» – это открытая дискуссионная площадка для всех и каждого.

Владимир Положевец,
Генеральный директор журнала «Системный администратор»





Все знают, что в редакции нашего журнала живет Админский приз. Мы называем его просто Приз. Случилось так, что к 2009 году Админский приз приобрел необыкновенные свойства. Он так и тянется к самым любознательным, опытным и общительным системным администраторам. А еще Приз стал очень капризным: он утверждает, что достанется только тем, кто даст правильные ответы на его загадки. Приз также обожает слушать истории. Любит интересные рассказики и с удовольствием сидит на форумах.

Приглашаем вас принять участие в розыгрыше призов «Админский приз 2009». Вам понадобится собрать коды из журналов и получить дополнительные коды за активность на форуме, за победы на чемпионате по игре «Аутсорсер», за правильные ответы на задачки. Дополнительные коды увеличивают ваши шансы на победу!

Админский Приз

Розыгрыш будет проходить в три этапа:

I — участвуют коды из журналов №7, 8, 9 и дополнительные коды, полученные с июля по август 2009 г.

II — участвуют коды из журналов №10, 11, 12 и дополнительные коды, полученные с октября по декабрь 2009 г.

III — участвуют коды из всех шести номеров журнала за 2-е полугодие 2009 г. и дополнительные коды, полученные участниками за весь период проведения конкурса

Ближайший чемпионат по игре «Аутсорсер», на котором вы сможете получить дополнительные коды, состоится в День системного администратора в рамках Четвертого Всероссийского Слета Сисадминов под Калугой (31 июля — 2 августа). Также вы можете получить дополнительные коды за активное участие в форуме нашего журнала.

Админский Приз

Админский Приз

Призы:

I этап:
1 место — приз-сюрприз
2 место — учебные курсы
3 место — пакет программного обеспечения
4 место — почтовый сервер на 50 пользователей
5 место — виртуальные выделенные серверы

II этап:
1 место — приз-сюрприз
2 место — учебные курсы
3 место — пакет программного обеспечения
4 место — почтовый сервер на 50 пользователей
5 место — виртуальные выделенные серверы

III этап:
1 место — приз-сюрприз
2 место — учебные курсы
3 место — пакет программного обеспечения
4 место — почтовый сервер на 50 пользователей
5 место — виртуальные выделенные серверы

Специальный утешительный приз — электронная книга

Ваш код для участия
в розыгрыше призов:

Админский Приз

Визитка

АНДРЕЙ БИРЮКОВ, специалист по информационной безопасности. Работает в крупном системном интеграторе. Занимается внедрением решений по защите корпоративных ресурсов

Углубляйте знания
с Cisco Expo Learning Club

Новая инициатива компании Cisco нацелена на повышение уровня квалификации отечественных ИТ-специалистов.

Форум Cisco Expo Learning Club был посвящён последним решениям Cisco в области информационной безопасности, унифицированных коммуникаций и центров обработки данных. На мероприятие пришло большое число посетителей – технических специалистов, активно работающих с оборудованием и технологиями Cisco.

Открыл конференцию директор по развитию бизнеса и работе с партнерами Cisco Михаил Кристев. Докладчик отметил, что корпорация Cisco, несмотря на кризис, расширяет ряд своих технологий, направленных на экономию средств заказчиков. Собственно, этот доклад задал тон всей конференции.

Новое в информационной безопасности

Доклад Владимира Иванова, системного инженера-консультанта Cisco, был посвящен угрозам информационной безопасности и способам их преодоления. Была подробно рассмотрена одна из наиболее актуальных угроз – ботнеты. Для борьбы с ними Cisco использует межсетевые экраны Cisco ASA и устройства предотвращения вторжений Cisco IPS. Для контроля угроз корпорация развернула аналитический центр. В него стекаются сведения от партнеров компании о различных вредоносных воздействиях. Далее эта информация обрабатывается аналитиками, и производится динамическое обновление правил защиты, наиболее полно отражающее текущую ситуацию.

На примере ботнета Srizbi докладчик продемонстрировал работу Cisco ASA по обнаружению вторжений. Ботнет инфицировался через спам, полностью исполнялся в ядре ОС Windows, его файлы не были видны в системе. В результате антивирусное ПО не могло вылечить зараженную машину. Аппаратное решение Cisco ASA содержит динамическую базу данных, обновляемую из центра борьбы с заражениями Cisco. Таким образом, как только в аналитическом центре изучили способы заражения, используемые этим ботнетом, было выпущено правило защиты, позволяющее заблокировать активность Srizbi. Принципиальное различие с антивирусными системами заключается в том, что здесь анализируется сетевой трафик до того, как он достигнет инфицируемой машины. Появляется возможность предотвращать вирусную активность на лету до того момента, как она проникнет на рабочую станцию и попытается её загрузить.

Владимир Иванов привел пример внедрения Cisco ASA в американской медицинской компании, имеющей филиальную сеть по всей стране. После внедрения ASA было обнаружено до полуторамиллиона подключений к сети ботнета в месяц, наличие в сети узла, управляющего ботнетом и распространяющего вредоносный код.

Затем в докладе было рассмотрено средство предотвращения вторжений Cisco IPS. Посредством глобальной корреляции IPS появляется возможность быстрого предотвращения распространения вредоносного кода по всему миру. То есть если в одной точке земного шара сенсоры обнаруживают новый тип зловредного кода, сенсор в другом регионе выявляет подключение к управляющему серверу ботнета, и наконец третий сенсор детектирует попытку вторжения с помощью данного ботнета в корпоративную сеть организации и принимает необходимые действия по ее предотвращению.

Также докладчик рассказал о методике анализа Cisco IPS – введении понятия «репутации». Например, в проходящем HTTP-трафике обнаружены команды SQL. Вполне возможно, это широко распространенный тип атаки – SQL-инъекция. Что делает Cisco IPS? Система анализирует следующие четыре параметра: Что? Как? Откуда? Почему? Ответ на первый вопрос – это SQL-команды внутри веб-трафика. Это само по себе очень подозрительно, так как обычно SQL-команды выполняются на стороне веб-сервера и передаются по своему собственному протоколу, а не по HTTP. Ответ на второй вопрос – первое HTTP-соединение. Тоже странно, при первом же обращении к веб-узлу сразу запрос к базе. Ответ на третий вопрос – динамический IP-адрес, динамический DNS. И наконец, почему – источник находится в сети азиатского провайдера и о нём известно, что из его автономной системы (AS) уже были атаки и встречались ботнеты.

На основании полученных ответов IPS делает вывод, что «репутация»

у источника соединения плохая, соответственно SQL-команды являются инъекцией, и данное соединение необходимо отклонить.

Решения Cisco и S-Terra

Директор по специальным проектам компании «С-Терра СиЭсПи» Алексей Афанасьев привел типовые проблемы с безопасностью при подключении филиалов. Прежде всего это ограничение филиалов в ИТ-ресурсах по сравнению с центром, защита соединений, проблемы с расширением зоны охвата, унаследованные приложения и инфраструктура безопасности. Еще одной важной проблемой является спам. Пользователи тратят больше времени на чтение электронной почты. Повышается нагрузка на почтовые сервера. В связи с этим возникает необходимость в более мощных и интеллектуальных решениях, предназначенных для борьбы с нежелательными почтовыми рассылками. Для защиты филиалов компаний необходимы межсетевые экраны, IPS, сетевые антивирусы и средства IPSec/SSL VPN. Однако такое решение требует много устройств, что для большого числа филиалов получается очень дорого. Для решения проблемы Cisco предлагает маршрутизаторы ISR, которые содержат все функции безопасности, необходимые для работы с WAN, в одном устройстве.

Далее докладчик продемонстрировал новые возможности модуля NME-RVPN – совместной разработки Cisco и S-Terra, первой специализированной прикладной платформы, предназначенной для маршрутизаторов Cisco ISR. Данный модуль реализует российские стандарты криптографической защиты для протоколов TCP/IP. Модуль может интегрироваться в маршрутизаторы серий 2800 и 3800 и предназначен для поддержки IPsec VPN с российскими криптографическими стандартами. При необходимости могут использоваться и другие криптографические алгоритмы.

Затем были представлены продукты Cisco VPN, предназначенные для применения в инфраструктуре безопасности Cisco SDN. Продукты могут самостоятельно использоваться и в сетях других производителей. В целом продукты CSP VPN включают полный набор средств защиты сетевого уровня, таких как CSP VPN Client – продукт для защиты индивидуального рабочего места; CSP VPN Server – продукт для защиты отдельного сервера; масштабируемый набор шлюзов безопасности CSP VPN Gate, в том числе модуль NME-RVPN, о котором говорилось ранее.

Также в состав модуля входит ряд решений для защиты от вирусов и спама, построенных на базе продуктов «Лаборатории Касперского»: Kaspersky Mail Gateway и Kaspersky Antivirus for Proxy Server. При этом возможны два варианта работы модуля: шлюз фильтрации вредоносного ПО и спама, и то же самое плюс VPN-шлюз.

Взаимодействие с системами виртуализации

Менеджер по развитию бизнеса Cisco Олег Коверзнев рассказал об основных направлениях деятельности Cisco в сегменте центров обработки данных (ЦОД), о главных аспектах виртуализации ЦОД и о новом решении Cisco UCS, призванном стать платформой для виртуальных сред.

Кроме того, Олег представил новый продукт – программный коммутатор Cisco Nexus 1000V. Коммутаторы предназначены для обслуживания ЦОД. А как известно, виртуализация – одно из лучших средств оптимизации работы ЦОД. Поэтому в отличие от аналогичных программно-аппаратных решений по коммутации это полностью программный коммутатор, предназначенный для работы с виртуальными машинами на платформе VMware. При этом каждая виртуальная машина подключается к порту коммутатора и получает свои настройки по безопасности, QoS и т.д. В случае перемещения виртуальной машины на другой сервер все сетевые настройки также переедут вместе с виртуальной машиной. Таким образом обеспечивается мобильность виртуальных серверов и их настроек. К тому же сохраняется эксплуатационная модель ЦОД. Что касается поддерживаемых Cisco Nexus версий VMware, то поддерживается только VMware ESX Enterprise 4. Однако докладчик упомянул, что сейчас ведутся разработки другого решения, которое будет поддерживать виртуальные машины не только на базе VMware, но и на базе MS Windows, в частности технологии Hyper-V. Учитывая широкое распространение виртуальных серверов и тех экономических и технических выгод, которые предоставляются тех-

В зале не было свободных мест

Системный инженер-консультанат Cisco Владимир Иванов рассказал об угрозе ботнетов

нологией виртуализации, у коммутаторов семейства Cisco Nexus большое будущее.

Решение Cisco WebEx

Менеджер по развитию бизнеса Cisco Павел Теплов рассказал об инструментах Cisco, созданных специально для успешной совместной работы, в частности, о решении Cisco WebEx, которое было приобретено компанией в 2006 году. Будучи частью системы унифицированных коммуникаций Cisco, интернет-сервис Cisco WebEx дает возможность существенно расширить функционал совместной работы, позволяя устраивать разнообразные виртуальные мероприятия в режиме реального времени. При этом виртуальное взаимодействие удобно в настройке и безопасно, к тому же WebEx не требует существенных изменений в настройках безопасности сети. Также в WebEx имеется функционал, позволяющий осуществлять коллективное взаимодействие с приложением, интегрироваться с VoIP-решениями. При этом на стороне клиента может использоваться как Windows, так и ОС семейства Linux. Решения WebEx получили широкое распространение в мире. Так, например, в последние месяцы компания Cisco провела с помощью решения Cisco WebEx более 50 различных онлайн-семинаров (вебинаров) для заказчиков и партнеров из России и других стран СНГ. Вебинары с использованием технологии Cisco WebEx, позволяющие проводить интерактивное онлайн-обучение, не отходя от рабочего места, организованы и в рамках программы Cisco Expo Learning Club. По заявлениям Cisco, в них уже приняли участие более 1300 членов клуба, тогда как традиционные семинары, проводимые в офисе Cisco, собрали 425 человек.

Обучение Cisco

Далее на конференции речь пошла об обучении Cisco. Следующий докладчик – Дэнни Гурис (Danny Gooris), менеджер подразделения Learning@Cisco по развитию бизнеса в России, рассказал о новшествах в обучении технологиям Cisco. По утверждению докладчика, в России и СНГ число специалистов по сетевым технологиям пока крайне мало, и в ближайшие два-три года потребуется их существенное увеличение. Cisco Learning Network – это учебная сеть, являющаяся основой технологий обучения Cisco. Также докладчик уделил большое внимание сертификации специалистов. На сегодняшний день наличие сертификатов Cisco уровня CCNA, CCNP и других зачастую является необходимым требованием при приеме на работу сетевых специалистов для многих крупных организаций. Также докладчик привел весьма интересный слайд, на котором сравнивались заработные платы для сертифицированных и несертифицированных специалистов. Различие составило порядка 30% в пользу сертифицированных специалистов. Но эти данные были приведены, естественно, для США, так что для России картина будет несколько иная, хотя наличие сертификата также является преимуществом, позволяющим сертифицированным специалистам претендовать на более высокую заработную плату.

Были представлены способы сдачи экзаменов. Что касается экзаменов уровней Associate и Professional, то тут ничего не изменилось, их по-прежнему можно сдавать в авторизованных центрах тестирования. Экзамены уровня Expert теперь можно сдавать в России, для этого проводятся выездные лабораторные работы CCIE в Москве. Преимущество мобильных лабораторий очевидно – нет необходимости ехать в другую страну для сдачи экзамена. Также докладчик сообщил, что среди стран с развивающимися рынками в России самое большое число CCIE.

Оксана Барсукова, менеджер по работе с авторизованными учебными центрами – партнерами Cisco в России и других странах СНГ, рассказала об образовательных программах подразделения Learning@Cisco. В России более 20 учебных центров-партнеров. Большинство из этих центров читает так называемые Fast-треки, то есть авторизованные курсы, продолжающиеся 3-5 дней. Такие курсы всегда читают авторизованные специалисты.

Менеджер по маркетингу Cisco Ирина Куманина подвела промежуточные итоги работы Cisco Expo Learning Club. Программа стратовала 1 февраля 2009 года. За прошедшее время было проведено множество бесплатных семинаров и веб-трансляций. В этих семинарах смогли принять участие несколько тысяч пользователей. Основной целевой аудиторией Cisco Expo Learning Club стали постоянные участники Cisco Expo. По словам докладчицы, сравнивая состав участников московских конференций Cisco Expo за последние четыре года, организаторы заметили, что многие посетители приходят на данное мероприятие регулярно, в течение нескольких лет. Поэтому и родилась идея создать клуб специалистов, объединенных стремлением совершенствовать свои знания в области информационных технологий. Успех программы Cisco Expo Learning Club очевиден: стартовав четыре месяца назад, она привлекла уже более 3400 профессионалов ИТ-индустрии из ста с лишним населенных пунктов России, Азербайджана, Беларуси, Казахстана, Кыргызстана, Молдовы, Таджикистана, Узбекистана и Украины. Постоянно увеличивающийся число членов клуба позволяет надеяться, что данное мероприятие будет развиваться и далее.

Конференция удалась

На этом официальная часть конференции завершилась. Далее организаторы продемонстрировали сетевое оборудование, о котором шла речь на конференции.

Внимание участников форума привлекли технологические новинки Cisco в таких областях, как информационная безопасность, унифицированные коммуникации и центры обработки данных, а также с решением Cisco WAAS Mobile, которое представляет собой одну из последних разработок в рамках стратегии Cisco Data Center 3.0.

Также в холле конференции были представлены стенды учебных центров – партнеров Cisco: «Ланит», «Специалист», «Редцентр. Учебные центры» представили свои программы обучения, которые, несмотря на глобальные экономические трудности, были довольно разнообразны. При этом на стенде «Ланит» всем желающим предлагалось пройти тест на знание сетевых технологий.

В целом мероприятие явно удалось. В зале практически не было свободных мест на протяжении всей конференции. Доклады привлекли внимание аудитории и были действительно интересны и полезны. Хочется надеяться, что организаторы продолжат практику подобных конференций. EOF

Визитка

ДМИТРИЙ ШУРУПОВ, ведущий рубрики, главный редактор электронного приложения «Open Source», автор российских веб-порталов nixp.ru и linuxphone.ru, технический директор Open Source-стартапа TrueOffice

Canonical намерена устранить недостатки в юзабилити Ubuntu

Авторы одного из популярнейших Linux-дистрибутивов Ubuntu объявили о запуске инициативы One Hundred Paper Cuts (https://launchpad.net/hundredpapercuts), направленной на сбор и устранение незначительных недочетов в юзабилити операционной системы, что в конечном итоге должно улучшить «ощущения от использования».

Проектом руководит команда Canonical Design and User Experience с целью улучшения ощущений от использования Ubuntu путем идентификации и исправления сотни проблем, которые испытывают рядовые Linux-пользователи при работе с системой. Стоит отметить, что все эти недочеты должны решаться весьма просто (например, за счет изменения какого-то устоявшегося в UNIX-среде термина в интерфейсе). И ожидается, что работа будет завершена уже к ближайшему релизу Ubuntu 9.10, который состоится в октябре этого года.

Вся работа разделена на 10 этапов, в каждом из которых устранят по 10 проблем. Ожидаемая дата выполнения последнего этапа – 30 августа.

Обновился ряд Open Source-средств для разработчиков

Конец июня ознаменовался чередой заметных обновлений различных инструментов с открытым исходным кодом для разработчиков. Среди значимых релизов стоит выделить интегрированные среды разработки Eclipse 3.5 и NetBeans 6.7, а также интерпретаторы скриптовых языков PHP 5.3 и Python 3.1.

Релиз Eclipse Galileo назван самым крупным за всю историю этой IDE: в него вошли 33 проекта и более 24 миллионов строк кода. Три главных направления, которыми руководствовались авторы при создании Eclipse 3.5: улучшение применения Eclipse в корпоративном секторе, инновации в области технологии моделирования с помощью Eclipse, расширение возможностей технологии запуска приложений EclipseRT. Среди новых возможностей, представленных в релизе, отмечается: обновленная поддержка 32- и 64-разрядных сборок интерфейса Mac OS X Cocoa; новый инструмент анализа памяти (Memory Analyzer) для анализирования потребления памяти Java-приложениями; PDT (PHP Development Tools) 2.1 с поддержкой PHP 5.3; поддержка WikiText в Mylyn для редактирования и парсинга wiki-разметки; новая XSL-утилита для редактирования и отладки XSL; Xtext – новый проект Eclipse, предназначенный для создания предметно-ориентированных языков (Domain Specific Languages, DSL).

Одним из главных новшеств в NetBeans IDE 6.7 стала интеграция с хостингом для Open Source-приложений Project Kenai от компании Sun. Кроме того, в Maven появился просмотрщик графа зависимостей библиотек, в PHP – поддержка PHPUnit и автодополнение SQL-кода в редакторе. Также отмечается поддержка Groovy and Grails 1.1 «из коробки» и автоматическое дополнение для Groovy and Grails, удаленная отладка для Ruby and Rails, инструменты профилирования DLight для проектов C++ и интегрированную поддержку популярных библиотек и утилит Qt.

Среди изменений в Python 3.1 выделяются: новый тип данных – упорядоченный словарь (ordered dictionary), оптимизации в типе данных int, новые возможности в модульном тестировании (unittest), а также новый модуль importlib с полностью документированной реализацией выражения import.

В PHP 5.3.0 представлена долгожданная поддержка пространств имен, а также лямбда-функции и замыкания, ограниченная версия оператора goto (jump label), родной MySQL-драйвер mysqlnd как замена libmysql и улучшенная поддержка платформы Windows. Кроме того, некоторые расширения были включены в состав основного дистрибутива интерпретатора, а некоторые – наоборот, вынесены в хранилище PECL.

Veracode признала высочайший уровень безопасности Sendmail

Компания Veracode, известная своей платформой управления рисками приложений, объявила о завершении тестирования на безопасность популярнейшего почтового агента (MTA) с открытым исходным кодом – Sendmail. Проект Sendmail удостоился самого высокого балла – уровня «A».

Тестирование Sendmail проводилось независимо и по инициативе Veracode. В нем были использованы такие индустриальные стандарты, как OWASP Top 10 и SANS-CWE Top 25. По словам Мэтта Мойнахана (Matt Moynahan), исполнительного директора Veracode, результаты тестирования подтверждают, что Open Source-решения готовы для серьезного промышленного использования, где безопасность критичных для бизнеса приложений выходит на первый план.

Sendmail – самый популярный MTA во всем Интернете. На сегодняшний день Open Source- и коммерческие редакции этого почтового агента можно обнаружить на значительной части серверов (35%), которые в совокупности доставляют более 65% электронной почты в мире. EOF

Визитка

ИЛЬЯ АЛЕКСАНДРОВ, постоянный автор ряда ИТ-журналов, студент исторического факультета СпбГУ. Специально – для «Системного администратора»

Праздник, который придумал Тед

В последнюю пятницу июля каждый сисадмин в России произносит тост за коллег по цеху. А как отмечают профессиональный праздник в других странах?

> И каждый жив в надежде
> На то, что пинг пройдет:
> Админы сервер держат –
> Даст бог, не упадет!
>
> **(Из неофициального гимна админов)**

Однажды Тед Кекатос листал компьютерный журнал и наткнулся на рекламу принтеров Hewlett-Packard. На картинке были изображены пользователи, задаривающие подарками своего системного администратора. Тед, двадцать лет занимающийся компьютерной техникой, подумал, что неплохо бы в действительности отмечать день админа. В ближайшую пятницу он с коллегами по компании организовал пикник на окраине родного Чикаго, в шутку назвав мероприятие «The sysadmin day». И вот уже десять лет у сисадминов есть свой день в календаре. И празднуют его не только в Чикаго.

Канада

Особенность: кидаться клавиатурами на дальность – эта интернациональная забава известна, кажется, любому компьютерщику в любой стороне света. Но, как утверждают жители Торонто (точнее, ИТ-ориентированная их часть), «throwing keyboards» придумали именно они. Без швыряния клавиатур канадский День сисадмина будет уже не тот.

Атрибуты праздника: админы в Канаде преимущественно мужчины, как нетрудно догадаться. А одно из любимых зрелищ канадцев – это хоккей. На стадион не сходить из-за межсезонья в НХЛ, но местом отмечания всегда является спортбар.

Напиток: пиво хоть и остается самым популярным админским напитком, но в столь важный день безоговорочно уступает виски.

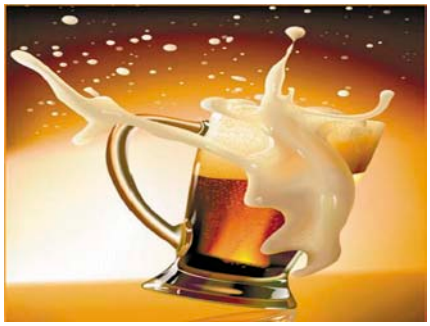
Что дарить канадскому админу: большую кружку с нарисованным на ней Туксом, чтобы было из чего испить кофе.

Голландия

Особенность: в Стране тюльпанов сисадмины организуют вечеринки в честь своего праздника либо на работе (здравствуй, моя любимая серверная!), либо у кого-то дома. Хорошим тоном считается на таких вечеринках запустить какой-нибудь олдскульный ПК; отдельные любители электронного раритета притаскивают «Спектрумы» и «Амиги». Это и повод поговорить об истории технологий, и способ создания нужного антуража.

Атрибуты праздника: как правило, День системного администратора приходится на время, когда в Эйндховене проходит крупнейшая в мире велосипедная выставка. Эйндховен – самый технологичный город страны, а велосипеды являются главным способом передвижения в Нидерландах. Неудивительно, что многие админы отмечают свой праздник на этой выставке.

Напиток: джин, фруктовое пиво.



Что дарить голландскому админу: USB-прикуриватель, чтобы вместе посмеяться над стереотипами.

Германия

Особенность: приход нового профессионального праздника в Германии совпал с бумом социальных сетей. Многие админы стараются провести вечер не только в кругу коллег, но и среди тех, вместе с кем получили профессиональное образование. Этакое объединение встречи однокурсников и дня работников отрасли.

Атрибуты праздника: место встреч неизменно – классическая немецкая пивная. Да и странно, если бы админы выбирали другие места.

Напиток: пиво. Тут конкуренции быть не может.

Что дарить немецкому админу: приставку Xbox или Sony Playstation. Чтобы проходить «Cult of duty».

Япония

Особенность: в последнюю пятницу июля местные сисадмины устраивают флэшмоб. Все аватары в социальных сетях меняются на тематические картинки, разные иллюстрации на тему «Sysadmin day». Подобные картинки вывешиваются в блогах, и о событии сообщается в Сети везде, где общаются админы. Таким образом в Японии пытаются популяризировать праздник.

Атрибуты праздника: фраза о том, что даже атомная бомба не может прервать партию в го, справедлива и для профессиональных дат. Го – это национальная настольная игра, где нужно передвигать по карте специальные камушки. Игра в главную интеллектуальную игру страны стала неотъемлемой составляющей праздничных вечеринок.

Только факты

Премия. Неутомимый Тед Кекатос на внесении профессиональной даты в календарь не успокоился. Он основал собственную премию «Лучший системный администратор года». Тед создал эту премию, чтобы сисадмины тоже получили признание – есть же «Грэмми» для музыкантов. Для участия в конкурсе нужно записать двухминутный видеоролик, где будет показано, как админ обеспечивает надежность работы компьютеров в своей организации. Лучших награждают ноутбуками Apple, а фотографию победителя размещают на сайте www.sysadminoftheyear.com.

К сожалению, пока этот конкурс проводится только для жителей США и Канады.

Даты. Среди компьютерщиков также принято отмечать 256-й день в году, он выпадает на 13 сентября в обычный год, и на 12-е – в високосный. Обычно этот день считают своим праздником программисты, но и многие сисадмины не упускают случая поднять бокалы по этому поводу.

В 2006 году Генеральная Ассамблея ООН провозгласила Всемирный день информационного общества, он закреплен за 17 мая. Это первый официальный праздник, который компьютерщики могут считать своим.

В Fidonet Днем администратора считалась каждая пятница, 13-е. Дело в том, что однажды в это сочетания числа и дня недели активировался опасный вирус, и в ту пятницу сисадминам в разных городах пришлось задержаться на работе допоздна. Тогда и решили в «Фидо» каждую пятницу, тринадцатого, поздравлять сисадминов.

Фестивали. Самым большим фестивалем в России, приуроченным к празднику, является слет сисадминов под Калугой. В этом году он пройдет с 31 июля по 2 августа. Надо сказать, что подобных мероприятий в мире совсем немного, самое крупное из которых – Linuxfest в американском Огайо. Это фестиваль линуксоидов, где выступают известные в Open Source-персоны. Linuxfest приурочен как раз к последней пятнице июля.

Напиток: местное пиво, особенно котируется «Саппоро». Ближе к вечеру – сакэ.

Что дарить японскому админу: сборник советских мультфильмов с субтитрами. Чтобы они узнали, что помимо аниме есть еще что-то.

Австралия

Особенность: свой праздник админы в шутку называют «днем апгрейда». Ближе ко дню X все стараются обновить технику, которую давно собирались менять. Со временем обновить компьютер на удачу начинает становиться традицией. Если ПК и так новый, то ограничиваются приобретением мышки.

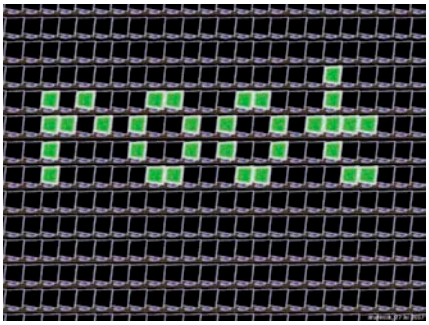
Атрибуты праздника: торт со взбитыми сливками. Австралийская привычка закупать торт на все праздники не обошла стороной и админов. Хотя, казалось бы, как сладкое сочетается с соответствующими напитками?

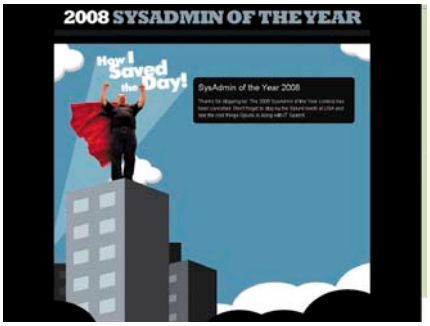
Напиток: светлый лагер и эль. Из элей наибольшим спросом пользуется яблочный.

Что дарить австралийскому админу: цифровую фоторамку с подборкой зимних русских пейзажей. Чтобы знал, что не везде коралловые рифы и курорт круглый год.

***

Автор благодарит Якоба Кларка (Jacob Clark), Эдвина Фриза (Edwin Friz), Андрея Климентьева и Виктора Шакирова за помощь по сбору информации для статьи, а также сайт facebook.com, без которого связаться с сисадминами разных стран было бы невозможно. EOF





Визитка

АНДРЕЙ ПОГОДИН, был сисадмином. Окончил высшую школу КГБ СССР, работал в структурах МИД СССР, был зампредом правления Сбербанка, зам. гендиректора ФГУП «Почта России», лауреат премии «IT-ЛИДЕР» 2003 и 2006 годов. Председатель Совета директоров компании «Эн Ди Групп»

Цари природы, энергобатарейки или биокомпьютеры?

Искусственный разум не появится до тех пор, пока мы не поймем, как работает человеческий мозг

…Это случилось много лет назад, когда я был просто системщиком, так тогда называли сисадминов. Рядом с моей работой находился книжный магазин, куда я часто заходил в поисках новинок по информатике, прежде всего операционной системы. Ее я знал до битика и до байтика и очень этим гордился.

Да, я считал себя профессионалом. И вдруг, однажды, перебирая, как обычно, новинки на полке, прочитал на корешке книги: Хьюберт Дрейфус «Чего не могут вычислительные машины». Я посчитал это провокацией! Как? Я был уверен, что машины могут все. Но, купив и прочитав эту книгу, понял, что ничего не знаю о своей профессии. Дрейфус подтолкнул меня к изучению смежных областей: потом много лет я занимался вопросами искусственного интеллекта. Его книга перевернула мое сознание. До этого я считал, что надо быть очень узким специалистом, досконально знать свой предмет. Конечно, подобные специалисты необходимы. Однако информатика – это область, в которой постоянно появляется что-то новое. Когда умерла IBM OC 360, на которой я работал в то время, мои знания стали никому не нужны. Моя ценность для социума исчезла. Это заставило меня крепко задуматься и двигаться дальше.

Люди – не боги, а жалкие плагиаторы

Что касается выводов, сделанных Дрейфусом, то я с ними и согласен, и нет. Согласен потому, что автор исходил из состояния, в котором находилась информатика 30-35 лет назад. Тогда его выводы были абсолютно верными.

Не согласен, так как за прошедшие десятилетия горизонты информатики сильно расширились, правда, оптимизма у нас заметно поубавилось. В 60-70 годах XX века термин «искусственный интеллект» был на слуху, казалось, вот-вот и у нас появятся роботы-помощники. Однако мы по-прежнему не понимаем, как работает человеческий мозг, не решили множество фундаментальных проблем с точки зрения вычислительной техники, поэтому, думаю, что в ближайшее время не надо ждать прорыва.

Тем не менее я уверен: наступит время, когда появятся человекоподобные машины, которые начнут выполнять не просто узкоспециализированные функции, а существовать в той среде, в которой существуем мы с вами. Они будут обладать способностью к обучению, эвристическим мышлением, целеполаганием. Я бы все-таки называл их не роботами, а биокомпьютерами. Это будет что-то очень похожее на нас, если не высказать крамольную мысль – это будем мы. Похоже, что человек стремится создать искусственный интеллект по образу и подобию своему. И здесь возникают не только технические задачи.

Когда Дрейфус утверждал, что машина никогда не сможет заменить человека, он исходил не просто из текущих достижений информатики, но также из чисто философских проблем. Дрейфус объяснял свой вывод так: у компьютеров в отличие от людей отсутствует целеполагание, а оно определяется нашими насущными потребностями. Правда, Дрейфус почему-то не затрагивал проблему совести, которая тоже присуща только людям.

С точки зрения религии это объясняется достаточно просто. Господь на шестой день сотворения мира создал человека по образу и подобию своему и вдохнул в него дух. В принципе это то, что отличает нас от животных. Соответственно у компьютера сегодня нет ни духа, ни целеполагания, у него отсутствует контекст. Пока мы не решим эти проблемы, мы, наверное, не сможем создать человекоподобное существо, о котором все так давно мечтают. Однако будет ли нам это позволено? Если исходить из тезиса, что человек– это биокомпьютер, то до тех пор, пока не поймем, как работает человеческий мозг, мы всего лишь жалкие плагиаторы, которые замахнулись на роль Творца в этом мире.

О безграничности стремлений и мере ответственности

Адам и Ева, как вы помните, были изгнаны из рая именно за то, что они сорвали плод с древа познания добра и зла. С той поры наши прародители стремились узнавать о мире все больше и больше. Мысль человеческая безгранична не

в своих возможностях, а в своих стремлениях. Безусловно, все, о чем пишут писатели-фантасты, что показывают в фантастических фильмах, – рано или поздно произойдет только потому, что все это уже когда-то было.

Я считаю, что мы не первая и не последняя цивилизация. Ученые всего мира бьются над доказательствами того, что мы не одиноки во Вселенной. На самом деле может оказаться, что мы не цари природы, а всего лишь энергобатарейки для кого-то и чего-то. Например, ученые-биологи высказывают мнение, что миром правят вирусы и бактерии, а люди лишь среда существования для них.

Человек в своем стремлении к безграничности знаний и удовлетворению собственного тщеславия и возможностей идет все дальше и дальше. Им движет любопытство: а что там, за дверью? Вспомните легенду о ящике Пандоры – его открыли из любопытства, а в результате выпустили ядовитых змей, расползшихся по всему свету. То же самое, с моей точки зрения, происходит с любыми научными открытиями, которые создаются прежде всего для военно-промышленного комплекса. Если люди обладают знаниями, которые напрямую отражаются на жизни общества, возникает вопрос об ответственности этих людей.

Американский физик Тесла долгое время проводил очень интересные опыты с электричеством, но потом вдруг уничтожил все результаты. В его поступке я вижу проявление ответственности профессионала. Наверное, Тесла понял: его открытия могут использоваться другими людьми против человечества.

Совершая те или иные поступки, мы формируем свое будущее. Нильс Бор сказал как-то про Оппенгеймера, создателя атомной бомбы, что он был его самым гениальным учеником, но далеко не самым нравственным человеком. Возможно, Оппенгеймер не думал о последствиях, к которым приведет его открытие. В конце концов, кроме атомной бомбы, мы получили и атомные электростанции – при исчезновении органического топлива они становятся основным источником энергии.

Однако ни для кого не секрет, что сейчас идут эксперименты в военных целях с ноосферой. Речь идет уже не о ядерной войне, а о климатических войнах. На это тратятся миллиардные средства, нанимаются тысячные армии ученых. Задумываются ли они о своей ответственности? Вряд ли. Здесь, наверное, срабатывает эффект стада: каждый считает, что если он откажется, все равно это будут делать другие. «Я только выполняю свою работу, решаю свои житейские проблемы», – возможно, утешает себя человек. Но в итоге может получиться результат, который будет угрожать и существованию всего человечества, и лично ему и его близким.

Есть такой анекдот. Марс спрашивает Землю: «Как ты там?» – Она отвечает: «Ох, тяжело, люди гадят везде, засорили окружающую среду, все разрушают». – Марс: «Да, может скинуть их с себя?» – Земля: «Зачем? Сами вымрут!»

Действительно, достаточно какого-нибудь «открытия» или серьезного катаклизма, чтобы наша цивилизация навсегда исчезла. И если когда-нибудь все повторится, ее следов уже никогда не найдут.

От сисадмина до хакера – только шаг

К сожалению, прогресс человечества в области технологий не сопровождался прогрессом духовным, а скорее наоборот, деградацией. Взаимозависимость профессионализма и ответственности – это, наверное, главный вопрос, на который любой специалист должен найти свой ответ.

Для этого необязательно быть ученым-физиком, создающим атомную бомбу или андронный колайдер, который поможет открыть частицу Хигса – «частицу бога», и тогда с миром, может, произойдет что-то невероятное.

Системный администратор на самом деле – очень широкое понятие. Возможно, его роль скромна в небольших организациях. Но в крупных компаниях, где системные администраторы отвечают за все информационные системы, он может либо сделать много хорошего для окружающих, либо испортить им и работу, и жизнь. Все зависит от его целеполагания, потому что мы живем по определенным принципам и законам и, повторяю, сами творим свою судьбу.

Думаю, что человек – это социальный биокомпьютер. Я хотел бы, чтобы большие профессионалы никогда не забывали о нравственных категориях. Нужно четко понимать, где нужно применять свои знания, а где не нужно. Это как в восточных единоборствах – «учителя», обучающие им, мудры и осторожны, потому что понимают, что дают знания и навыки, дающие их владельцам большие преимущества. То же относится и к системному администратору: применение его знаний должно быть оправдано. Это во многом определит его профессиональную карьеру.

Мне хотелось бы пожелать своим бывшим коллегам, сисадминам, смотреть чуть шире своих профессиональных интересов. Соизмерять поступки со своими внутренними моральными ограничителями и не замыкаться в рамках профессии, чтобы иметь возможность развиваться дальше. Ведь большинство системных администраторов – очень талантливые люди. EOF

Когда умерла IBM OC 360, на которой я работал в то время, мои узкоспециализированные знания стали никому не нужны. Моя ценность для социума исчезла. Это заставило меня крепко задуматься и двигаться дальше.

Визитка

АЛЕКСЕЙ БЕРЕЖНОЙ, системный администратор, главные направления деятельности: виртуализация и гетерогенные сети. Еще одно увлечение, помимо написания статей, – популяризация бесплатного ПО

Альтернатива файловому серверу
это – дисковое хранилище NETGEAR ReadyNAS

Что делать, когда требуется быстрое экономичное решение для небольшой компании, а системного администратора в штате не предвидится? Использование сетевых хранилищ в качестве файлового сервера – неплохой вариант решения проблемы.

Предыстория

В нашей компании было принято решение выделить бухгалтерию и финотдел в отдельное предприятие. Все как полагается: с отдельным уставом, реквизитами, офисом, руководством и, конечно же, отдельной ИТ-структурой.

Встал вопрос: как это организовать? Вопрос касательно сервера СУБД (в нашем случае это «1С8») решился сам собой. Есть приходящий администратор баз данных (DBA), способный взять на себя функции по управлению сервером с MS SQL 2005 и серверной частью «1С:Предприятие». Вопрос с контроллером домена решился крайне просто. Так как пользователей в сети осталось одиннадцать человек, решено было организовать рабочую группу (Workgroup). А вот с файловым сервером дело обстояло сложнее. Помимо обычных функций предоставления папок в общий доступ по CIFS-протоколу возникла необходимость предоставления доступа извне, так как некоторые сотрудники изъявили желание работать с документами из дома. Открывать для них CIFS-протокол? С точки зрения безопасности мысль не совсем удачная. Можно, конечно, дополнительно поднять и настроить, к примеру, доступ по HTTPS. Но следует учесть, что это дополнительная задача, требующая участия квалифицированного администратора. Не стоит также забывать об обслуживании данного сервиса в процессе работы. Кроме того, остался открытым вопрос о создании и размещении резервных копий. Если к этому присовокупить тот факт, что отвечать за эксплуатацию нового «хозяйства» некому, то ситуация представляется весьма пикантной. И в дополнение ко всему прочему маячившая «перспектива» приобрести еще одну дополнительную лицензию Windows Server 2003 не слишком радовала руководство компании. Оплачивать услуги еще одного администратора в случае использования бесплатных продуктов на базе UNIX-подобных систем руководству тоже не хотелось.

Поэтому было решено приобрести оборудование, которое:

- Способно выполнять роль файлового сервера, работающего по нескольким протоколам, включая FTP и HTTPS.
- При настройке не требует специальных знаний системного администратора.
- Не нужно приобретать дополнительное дорогостоящее программное обеспечение, такое как операционная система MS Windows 2003 (2008).
- Устойчиво к заражению вирусами, сбоям электропитания и другим факторам, способным вывести файловый сервер из строя.

На нашу удачу, мы вспомнили о сетевых хранилищах от NETGEAR. Первоначальное изучение возможностей ReadyNAS Pro, найденное в Интернете, подсказало, что устройство способно удовлетворить все наши требования. Связавшись с представительством компании в обмен на гарантийное письмо мы получили на тестирование искомое хранилище ReadyNAS Pro и приступили к изучению нового для нас оборудования.

Выбор жестких дисков и организация RAID

Очевидно, сетевое хранилище не работает без жестких дисков. По предварительным расчетам, чтобы удовлетворить практически все нужды по хранению рабочих материалов наших бухгалтеров и финансистов, а также делать резервные копии баз данных, дискового массива размером 2,5 Тб должно хватить с большим запасом. Поэтому были приобретены 4 винчестера Seagate ST31000340NS по 1 Тб. С учетом потерь на организацию дискового пространства этого объема вполне должно хватить на первое время.

Стоит отдельно сказать о технологии X-RAID, применяемой в хранилищах ReadyNAS.

X-RAID – это разработка, запатентованная фирмой Infrant. Технология организации RAID-массивов значительно упрощает процесс управления RAID. Вы можете установить в хранилище, к примеру, два диска по 1 Тб. В этом случае вы получаете «зеркало» из двух дисков, аналог RAID1. Позже, если понадобится дополнительное дисковое пространство, можно добавить еще один диск указанной емкости и получить размер массива, равный суммарному объему двух дисков аналогично ситуации с RAID5. Точно таким же образом добавляются и другие диски, увеличивая тем самым объем

используемого пространства, пока не заполнятся все отсеки. Но даже когда все отсеки заполнены, X-RAID позволяет увеличить объем и дальше. Если заменить все диски, то после замены последнего диска том автоматически расширится за счет дополнительной емкости новых дисков. Естественно, заменять диски нужно по одному, чтобы успешно выполнилась операция rebuilding по перестройке массива.

Важное замечание: после каждой смены диска необходимо обязательно дождаться окончания процедуры синхронизации. Это может занять продолжительное время (для диска объемом 750 Гб процедура может занимать до 7 часов). При этом устройство будет доступно для выполнения всех необходимых операций, как при обычной работе.

Надо отметить, что дисковые хранилища ReadyNAS поддерживают и обычный RAID5. В случае замены обычного офисного файлового сервера этот вариант является даже предпочтительней, так как X-RAID оптимизирован для операций чтения больших блоков данных. Такая оптимизация хороша, например, при воспроизведении потокового видео или восстановления системы при помощи программ блочного резервного копирования, например Acronis True Image, но теряет смысл при обычных операциях чтения-записи при работе с офисными приложениями.

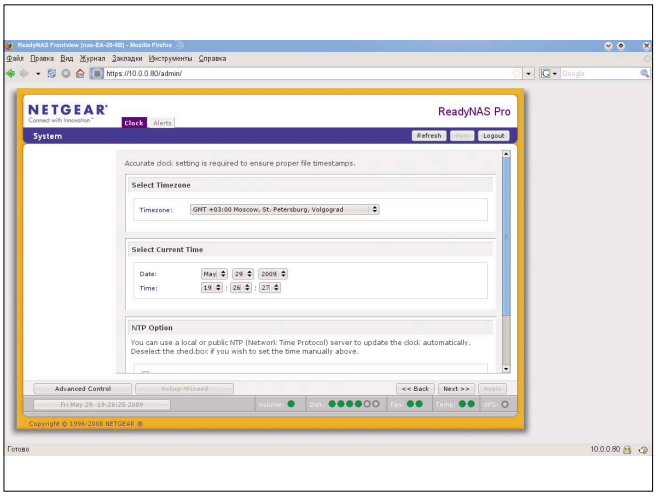
Но все-таки выбор был сделан в пользу технологии X-RAID в связи с оптимизацией затрат и дальнейшей необходимостью делегировать полномочия другому лицу. В этом случае появляется возможность наращивать объем хранилища постепенно, не прибегая к услугам высококвалифицированного системного администратора. Кроме того, система X-RAID имеет возможность в автоматическом режиме перестроить RAID-массив при замене вышедшего из строя жесткого диска.

Первоначальная настройка

Установка дисков в хранилище производится обычным путем. Диск устанавливается в корзину, корзина с диском вставляется в хранилище. Здесь, как говорится, ничего нового не придумано (см. рис. 1).

Рисунок 1. Сетевое хранилище NETGEAR ReadyNAS Pro с наполовину извлеченной корзиной

Рисунок 2. Первое окно настройки – System, вкладка Clock



После включения хранилища сразу высветилась надпись Ready NAS и появилась полоска индикатора. Следом появилось сообщение: Factory Reset installing. После этого буквально через несколько минут на индикаторе появилась новая информация Create disk C: с указанием количества процентов от выполненной операции. После создания диска C показалась надпись: Requesting IP. По умолчанию дисковые хранилища ReadyNAS настроены на получение IP-адреса по DHCP, и наш случай не стал исключением. DHCP-сервер в сети был, поэтому ReadyNAS, как ему и полагается, получил свой IP-адрес, который высветился на табло. Далее началась синхронизация дисков. К установке программы для настройки дискового хранилища можно приступать, не дожидаясь конца этого процесса.

К сожалению, на мой компьютер с OpenSUSE Linux 11.1 программа RAIDar (точнее, ее версия для Linux), предназначенная для поиска сетевых хранилищ и их настройки, устанавливаться категорически не захотела. К счастью, в прилагаемом CD присутствует документация на английском языке (в формате PDF), где есть раздел, связанный с установкой программы на Linux. Там предлагалось в подобных случаях использовать веб-интерфейс программы, введя в браузере адрес: http://_адрес_хранилища_/admin. (Кстати, веб-интерфейс управления хранилищем ReadyNAS называется FrontView.) Логин для входа по умолчанию admin, пароль по умолчанию netgear1. Воспользовавшись этим мудрым советом, я смог получить доступ к веб-интерфейсу. При входе сразу стартовал мастер настройки (Setup Wizard), который выдал первое окно System, вкладку Clock, где предлагается установить системное время (см. рис. 2).

Примечание: веб-интерфейс NETGEAR ReadyNAS Pro имеет 2 режима: режим мастера настройки (Wizard) и основной. Первый раз автоматически предлагается Wizard. Но пользователь в любой момент может переключиться в основной режим по кнопке Advanced Control. После первоначальной настройки при каждом новом сеансе будет автоматически предложен основной режим, но точно так же можно легко переключиться в режим мастера настройки, нажав кнопку Setup Wizard.

В следующей вкладке Alerts нас просят ввести адрес E-mail для приема уведомлений. Далее появляется окно Network, в котором можно либо задать получение IP-адреса по DHCP – Use values from DHCP server, либо выбрать пункт Use values below и вручную установить IP-адрес и маску подсети. Так как у хранилища два сетевых интерфейса, то на следующем шаге появляется возможность произвести аналогичную настройку второго сетевого подключения. Потом программа переходит на вкладку Global Settings, где задаются такие важные параметры, как имя хоста (Hostname), название рабочей группы (Workgroups), а также указывается шлюз по умолчанию (Default Gateway) и настройка DNS (DNS Setting) (см. рис. 3). Последние два параметра доступны для ввода только в случае, когда сетевые настройки устанавливаются вручную, а не присваиваются посредством DHCP.

После этого открывается окно Security, где предлагается сменить пароль администратора, а также задать реквизиты для восстановления пароля (см. рис. 4). В случае если реквизиты восстановления пароля заданы корректно, для выполнения данной операции достаточно обратиться на страничку http://ip_address_of_readynas/password_recovery. Если данные были введены неправильно или данная функция не была включена, то процедура восстановления несколько усложняется – потребуется переустановка ПО, которая сбросит пароль, но сохранит основные настройки.

Далее перед нами откроется вкладка Accounts, где можно создать учетные записи остальных пользователей.

Следующее окно Services, вкладка Standard File Protocols. Собственно, то, из-за чего и понадобилось сетевое хранилище в нашем случае. Здесь представлен перечень протоколов, по которым будет осуществляться доступ к хранилищу. В нашем случае будет использоваться только протокол CIFS для доступа Windows клиентов внутри сети и HTTPS для доступа снаружи (этот протокол разрешен по умолчанию, так как используется для управления хранилищем). Поддержку всех остальных протоколов следует отключить, сняв соответствующие галочки (см. рис. 5).

Следующая вкладка Streaming Services касается мультимедийных приложений и в данном случае неактуальна. Далее за ней идет вкладка Installed Add-Ons, показываю-

Рисунок 3. Окно настройки – Network, вкладка Global Setting

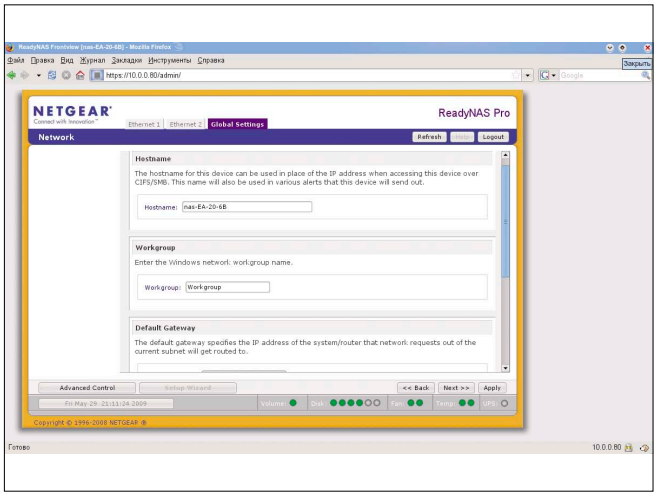
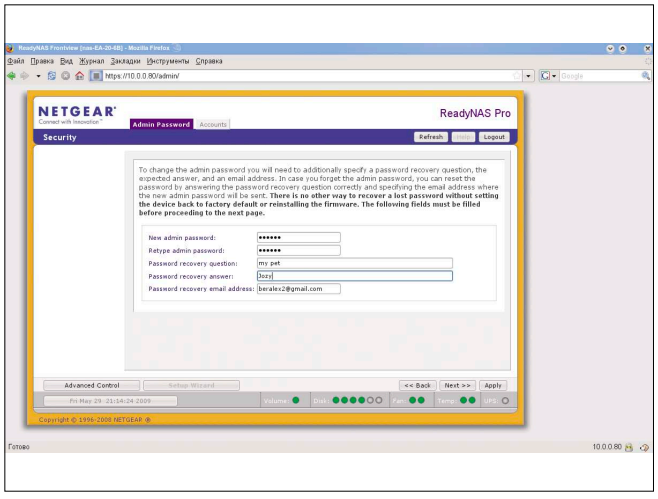


Рисунок 4. Окно Security, вкладка Admin Password



щая проинсталлированные дополнения. Так как устройство только что установлено и дополнений нет, поэтому список пуст.

Окно Shares, вкладка Share List. Демонстрирует список общих ресурсов и предоставляет возможность отредактировать параметры, например, по каким протоколам будет предоставляться доступ. Следует также добавить, что ReadyNAS позволяет предоставлять в общий доступ не только внутренние диски, но и сменные носители, подключенные по USB (см. рис. 6).

Следующая вкладка Add Shares позволяет создавать новые общие ресурсы.

Следующее окно USB Printers позволяет управлять принтерами в общем доступе, подключенными по USB-интерфейсу. Довольно полезная возможность. Список совместимых принтеров можно посмотреть по адресу http://readynas.su/compatibility_list/usb_printers. В нашем случае сетевое хранилище было решено разместить подальше от любопытных пользователей, поэтому сетевую печать придется организовать другим способом.

Далее появляется окно Registration, где нам предлагается зарегистрировать наше сетевое хранилище для получения поддержки со стороны производителя.

Примечание: что касается Windows-платформ, то установка программы RAIDar прошла без особых проблем. Необходимо запустить инсталляционный файл (на тот момент это был RAIDar_Win_4_1_5.exe) и по итогам установки получить рабочее окно программы. Она не только помогает осуществить поиск сетевых хранилищ ReadyNAS в сети, но также облегчает доступ к административному веб-интерфейсу соответствующих устройств (хранилищ), а кроме того, служит для мониторинга их состояния (см. рис. 7). После выбора соответствующего хранилища и нажатия на кнопку Setup запустится уже знакомый нам веб-интерфейс программы настройки хранилища.

Создание учетных записей пользователей

При работе с мастером (Wizard) настройки мы произвели только первичную настройку сетевого хранилища. Но нам необходимо создать из этого агрегата полноценный файловый сервер, завести несколько пользователей и предоставить в общий доступ несколько каталогов.

Прежде чем приступить к процессу, необходимо понять идеологию работы сетевого хранилища. Дело в том, что встроенная операционная система NETGEAR ReadyNAS Pro базируется на ядре Linux, что наложило соответствующий отпечаток на организацию прав доступа, хотя существующая система имеет свои отличия, которые будут рассмотрены дальше.

Примечание: в качестве операционной системы ReadyNAS PRo служит Linux Debian. В качестве ПО для организации файлового сервера – Samba. Версия Debian и Samba обновляются по мере выхода нового ПО для ReadyNAS. В нашем случае используется версия, доработанная инженерами NETGEAR: Linux version 2.6.27.6.RNx86.2.0 (дистрибутив Debian 4.1.1-19). Samba версии 3.0.28.

Поэтому вначале нужно определить, является ли наш ресурс (общая папка) по умолчанию только для чтения, для чтения-записи, или по умолчанию доступ к нему запрещен. Если ресурс только для чтения, то необходимо определить список пользователей и групп, которые могут осуществлять операции чтения-записи в каталог. Если ресурс по умолчанию открыт для чтения-записи, то при необходимости определяется список лиц, которым установлен доступ только в режиме чтения. Если же доступ к ресурсу по умолчанию запрещен, то можно определить оба типа доступа: только для чтения и для чтения-записи – и указать пользователей и группы, которым предоставлен тот или иной тип доступа.

Для начала создадим учетную запись пользователя, пусть это будет некий readwriter. Как видно из названия, пользователь будет иметь доступ для чтения и записи в общий каталог. Для этого обратимся к соответствующему разделу веб-интерфейса управления хранилищем. Обратите внимание, что после первоначальной настройки внешний вид веб-приложения выглядит несколько иначе. Итак, мы снова набираем в строке браузера http://_адрес_хранилища_/admin/, вводим имя пользователя admin и соответствующий пароль, после чего с левой стороны выбираем пункт меню Security, далее – подпункт User & Group Account и попадаем в нужный раздел программы. Далее переходим на вкладку Add User

Рисунок 5. Окно Services, вкладка Standard Files Protocols. Отключаем все, кроме CIFS и HTTPS, по умолчанию

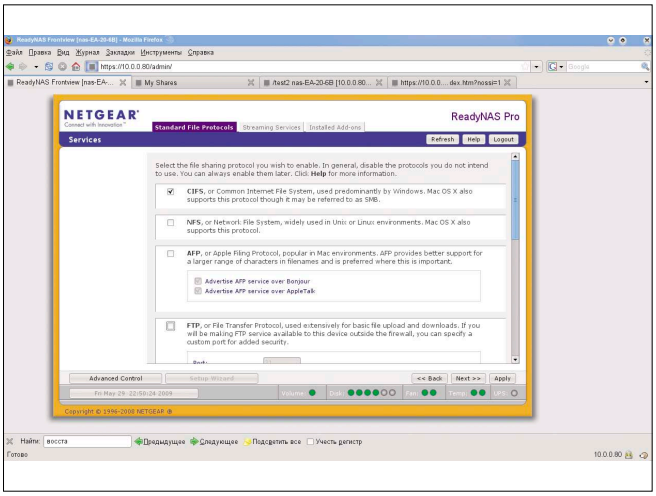
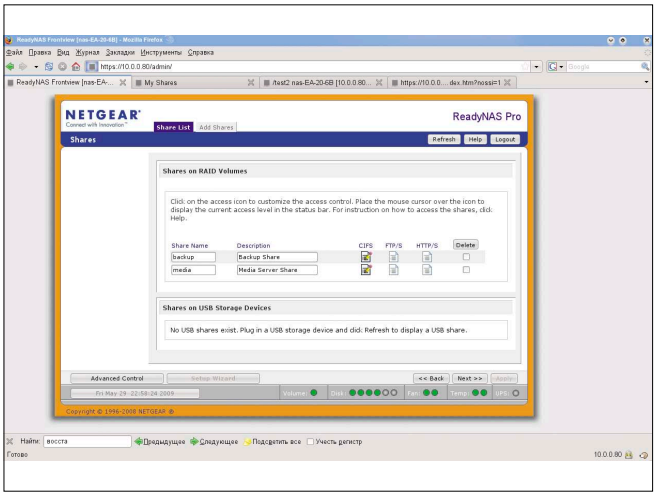


Рисунок 6. Окно Share, вкладка Share list – список ресурсов



и заполняем поля, необходимые для создания новой учетной записи:

User – имя пользователя.

E-mail – почтовый адрес, используется для отправки уведомлений, например, о заполнении выделенного дискового пространства.

UID – уникальный идентификатор пользователя. Поле лучше оставить пустым, программа сама проставит нужное значение.

Primary Group – первичная группа пользователя. В нашем примере оставлено значение по умолчанию.

Password – пароль пользователя.

Quota – выделенная квота для данного пользователя.

Аналогичным образом создаем пользователя reader, который будет иметь права только для чтения (см. рис. 8).

После заполнения реквизитов учетной записи пользователя нажимаем кнопку Apply, и новая учетная запись будет создана.

Аналогичным образом создается соответствующая запись для группы. Для создания группы необходимо посредством ниспадающего меню в правом верхнем углу окна выбрать соответствующий раздел.

Далее в появившемся окне необходимо заполнить следующие поля:

Group Name – имя группы.

GID – уникальный идентификационный номер группы, лучше оставить пустым, тогда система присвоит ему необходимое значение.

Quota MB – квота для группы.

После того как учетная запись для группы будет создана, необходимо приписать к данной группе необходимых пользователей. Для этого нужно, ориентируясь по алфавитному перечню, перейти на вкладку настройки свойств данной группы и ввести имена пользователей в поле Secondary Members.

Теперь создадим общий ресурс. Процесс создания проходит довольно просто. Переходим в раздел Shares, добавляем раздел Add Share. Теперь необходимо заполнить форму, в которой указать имя ресурса и примечание к нему. После нажатия кнопки Apply ресурс будет создан.

Настройка доступа по протоколу CIFS

Для настройки доступа клиентов сети Windows по протоколу CIFS переходим раздел Shares → Share List. Кликаем мышкой по значку протокола CIFS созданного нами общего ресурса и попадаем в окно настройки доступа по CIFS. Окно хоть и небольшое, но содержит весьма внушительное число параметров и снабжено полосой прокрутки (см. рис. 9).

В целях безопасности определим доступ по умолчанию (Default Access) к нашему ресурсу как Disabled, то есть доступа к нему без аутентификации не будет. А пользователей и группы, которым необходимо иметь доступ на чтение или чтение-запись, укажем отдельно, заполнив поля Read-only users, Read-only groups, Write-enabled users, Write-enabled groups соответственно. Следует также упомянуть о поле Hosts allowed access, в котором задается список IP-адресов или имен хостов для разрешения доступа к ресурсу только этим клиентам. Если же данное поле не активировано, доступ осуществляется с любого адреса.

Следующий пункт, очень важный в организации файловых ресурсов: Share Display Option. Если сделать активным параметр Hide this share when a user browses the ReadyNAS for available shares (скрывать этот ресурс, когда пользователь просматривает ReadyNAS в поиске общих ресурсов), то данный общий каталог становится невидимым для клиентов.

Настройка Recycle Bin, то есть «Корзины», заключается в первую очередь в возможности активации настройки корзины, а также в указании временного периода в днях, по истечении которого нужно удалять файлы (Remove files older than: .. days), и размера самой корзины в мегабайтах (Limit Recycle Bin to: … MB).

Еще один раздел, заслуживающий внимания: Advanced CIFS Permission. Здесь предлагается настроить права доступа для вновь создаваемых файлов.

Установка флажка Automatically set permissions on new files and folders разрешает установку разрешений по умолчанию для вновь создаваемых файлов или каталогов.

Do not allow ACL changes to be more restrictive than this – не позволять ACL устанавливать более ограниченные параметры, нежели эти.

Рисунок 7. Запущенная программа RAIDar

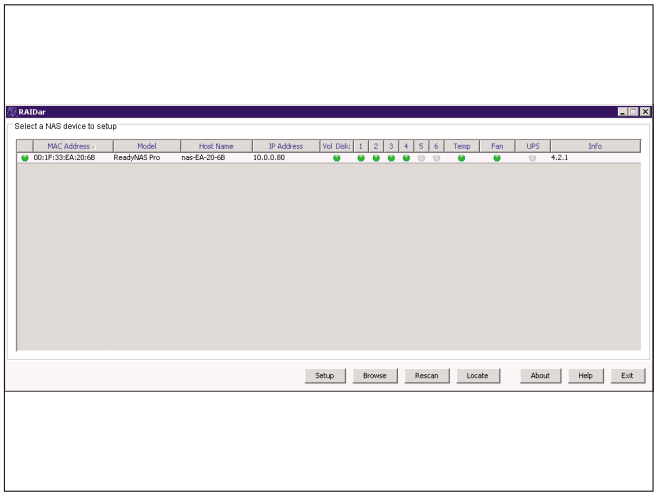
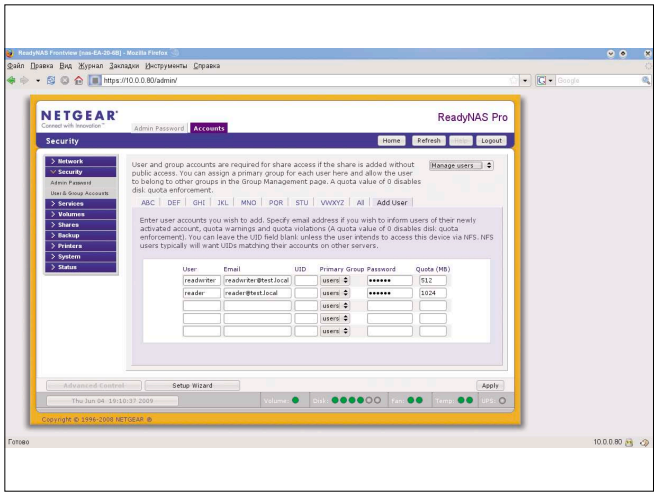


Рисунок 8. Создание нового пользователя на сетевом хранилище



Далее идет краткое пояснение, основной смысл которого заключается в том, что когда создается новый файл посредством доступа через протокол CIFS, то устанавливаются следующие типы разрешений: разрешения для владельца файла или каталога, разрешения для группы и разрешения для всех остальных (данная схема организации прав доступа является стандартной для UNIX-систем).

После установки флажка Automatically set permissions on new files and folders становится доступным меню выбора для групп (Group rights), где предлагается выбрать следующие значения: чтение-запись (Read/write), только чтение (Read-only) и доступ запрещен (Disabled). Список с такими же значениями доступен и для всех остальных (Everyone).

В нашем случае установим следующие значения: чтение-запись для группы и запрет на доступ для всех остальных.

Полностью аналогичные действия предлагается произвести и для вновь создаваемых каталогов.

Еще один интересный параметр – Opportunistic Locking. Увеличивает производительность CIFS, позволяя использовать кэширование файлов на Windows-клиентах.

Флажок Enable oplocks for this share, который разрешает кэширование, включен по умолчанию.

Настройка доступа по HTTPS

Чтобы более эффективно вести бизнес, зачастую необходим доступ к внутренним ресурсам сети извне. Также иногда бывает необходимо быстро обеспечить быстрый просмотр документов для клиентов на другой платформе (MacOS, Linux). Для решения данной задачи будем использовать протоколы: HTTPS или WebDAV через защищенное соединение HTTPS.

Настройка доступа по протоколу HTTPS

Снова переходим в Share Listing и щелкаем мышкой по значку в колонке HTTP/HTTPS.

После этого мы попадаем в окно настройки (см. рис 10).

Самое первое, что необходимо сделать, – установить по умолчанию параметр, разрешающий использовать доступ по HTTPS в режиме чтения-записи. Для этого выберем из ниспадающего меню Default Access пункт Read/write. Для получения возможности ограничить доступ пользователей отметим флажок Hosts allowed access. Станут доступны поля Users allowed access и Groups allowed access, куда мы введем имя учетной записи пользователя и группы, которым позволено осуществлять доступ к ресурсу по HTTPS. (В нашем случае это пользователь readwriter и группа writegroup.) Остается разрешить использование WebDAV установкой соответствующего параметра Enable WebDAV support и нажать кнопку Apply для применения настроек.

Пример использования доступа по HTTPS можно видеть на рис. 11.

Настройка протокола WevDAV

WebDAV (Web Distributed Authoring and Versioning) – протокол доступа к файлам и папкам, работающий поверх HTTP/HTTPS. В нашем случае протокол удобен тем, что можно организовать доступ к сетевым ресурсам извне, при этом достаточно один раз настроить клиента на ноутбуке с Windows (в нашем случае это Windows XP).

Для включения поддержки WebDAV необходимо включить параметр Enable WebDAV support в разделе настройки протокола HTTPS и подтвердить свой выбор (см. рис. 11).

Далее необходимо настроить клиента WebDAV на компьютере Windows XP.

- Открываем «Сетевое окружение» (My Network Place).
- В разделе Network Tasks («Сетевые задачи») кликаем Add A Network Place («Добавить новый элемент в сетевое окружение»). Windows XP запустит «Мастер добавления в сетевое окружение» (Add Network Place Wizard).
- После нажатия кнопки Next в окне приветствия появится окно «Мастера добавления в сетевое окружение» (Add Network Place Wizard), в котором нужно указать, где будет создаваться сетевое размещение (Where Do You Want To Create This Network Place).
- Далее в окне What is the adress of this network place («Укажите адрес этого сетевого размещения») необходимо в поле Internet or network adress («Сетевой адрес или адрес в Интернете») указать адрес для под-

Рисунок 9. Окно настройки доступа к общему ресурсу по протоколу CIFS

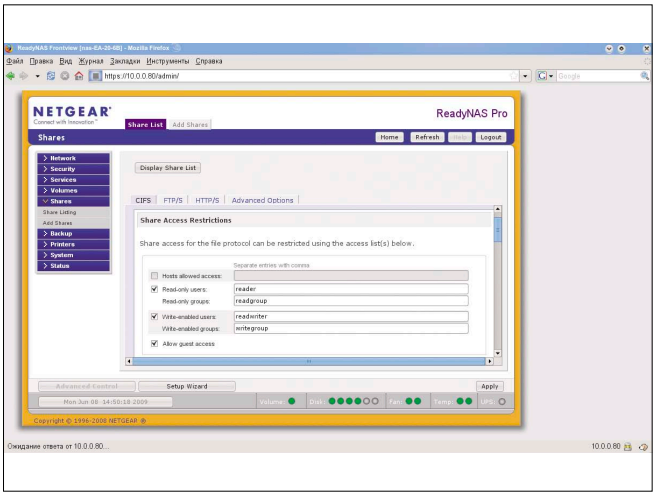
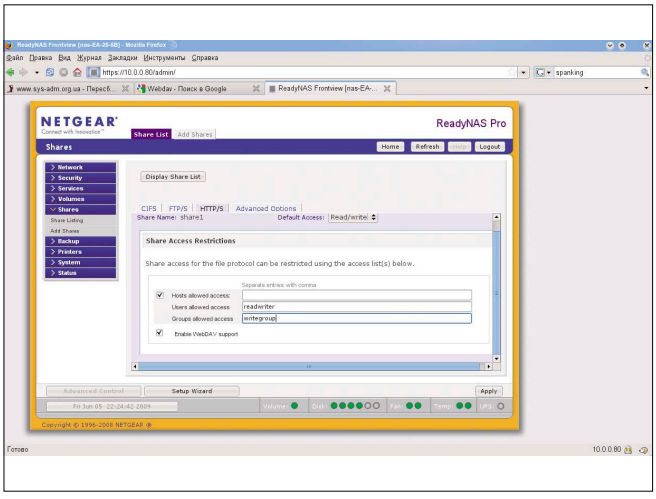


Рисунок 10. Настройка HTTPS (WebDAV)



ключения сетевой папки формата: https://_имя_сервера_/_имя_ресурса_/ (см. рис. 12).

- После нажатия кнопки Next появится окно Security Alert, в котором предлагается сохранить сертификат: This page requires a secure connection which includes server authentication. The certificate issuer for this site is intrusted or unkhow. Do you wish to proceed? («Эта страница требует безопасного подключения, включающего проверку подлинности сервера. Поставщик данного узла неизвестен или ненадежен. Продолжить?»). Подтверждаем наше доверие сертификату сетевого хранилища, нажав кнопку «Да».
- Следующее окно Enter Network Password («Ввод сетевого пароля») предлагает ввести информацию для аутентификации: Please enter your authentication information» («Введите сведения для проверки»). Вводим наши Username и Password (пользователь и пароль). Можно установить галочку Save this password in this password list («Сохранить пароль в списке паролей»).
- Нажимаем OK и переходим в окно What is the name of this network place («Укажите имя для этого сетевого размещения»). В поле «Введите имя для этого места в сетевом окружении» вводим соответствующее имя и далее по клавише Next в окно Completing the add Network Wizard. После нажатия кнопки «Финиш» будет создано новое подключение к WebDAV-ресурсу.

Пример подключения к сетевому хранилищу с помощью Internet Explorer показан на рис. 13. Для копирования файла на сетевой ресурс достаточно перетащить документ в окно браузера.

Примечание: при включении поддержки WebDAV при обычном доступе через браузер пропадает верхнее меню для работы с дополнительными функциями (см. рис. 14, сравните с рис. 12).

Можно приступать к работе с нашим сетевым хранилищем. В следующем номере я расскажу, как, имея NETGEAR ReadyNAS Pro, организовать резервное копирование рабочих станций, а также информации на сетевом хранилище. EOF

1. Официальный сайт NETGEAR – http://www.netgear.com.
2. Официальный сайт NETGEAR в России – http://www.netgear.ru.

Рисунок 11. Иллюстрация доступа по протоколу HTTPS. Открыто окно Upload для демонстрации возможности выбора загружаемых файлов

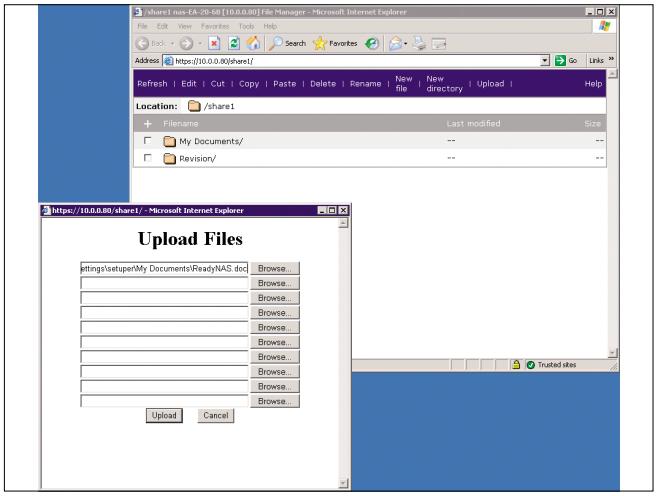


Рисунок 12. Настройка клиента WebDAV в Windows XP

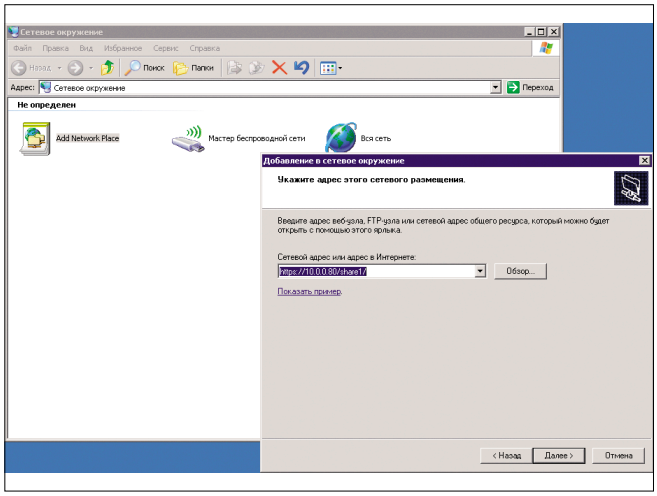


Рисунок 13. Подключение к сетевому ресурсу по WebDAV

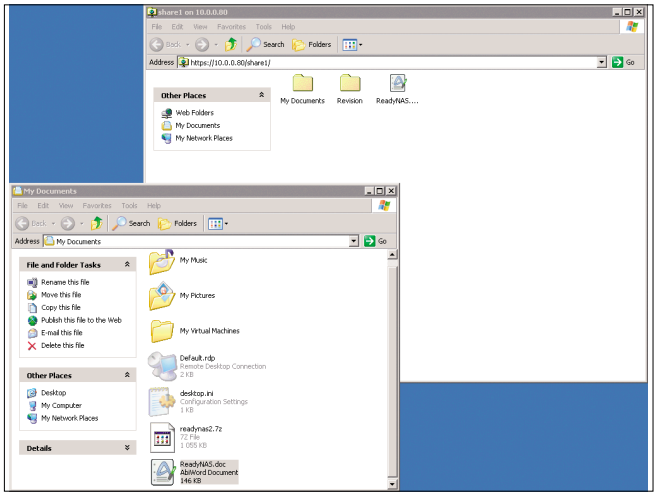
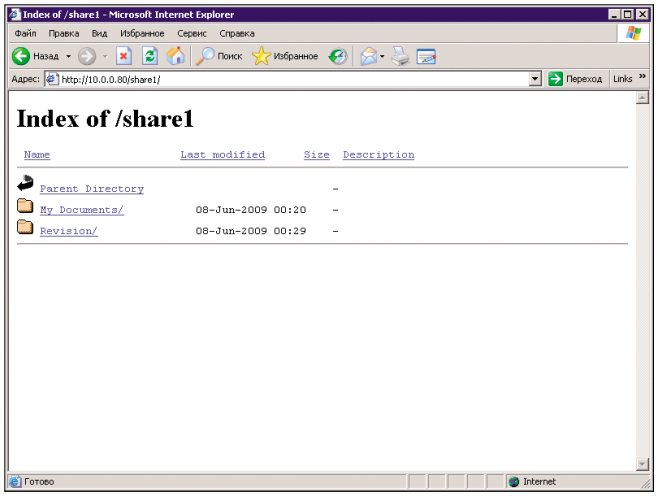


Рисунок 14. Окно веб-интерфейса при доступе через браузер. Отсутствует верхнее веб-меню



Mandriva Linux

Сертифицированная ФСТЭК версия

Дружественный и удобный интерфейс, Простота работы и настройки, Большой спектр поддерживаемого оборудования, Гарантия безопасности: дистрибутивы сертифицированы ФСТЭК.*

Офисная рабочая станция

Mandriva Powerpack 2008 Spring — надежное решение для рабочей станции. Включает в себя офисный пакет OpenOffice.org: текстовый редактор, электронные таблицы, редактор презентаций, конструктор баз данных, почтовый клиент, браузер, другие интернет-приложения, графические редакторы, приложения для работы со звуком и видео, другое ПО для офисного компьютера.

Мобильное рабочее место

Mandriva Flash — защищенное рабочее место для мобильных сотрудников. Mandriva Flash загружается и работает прямо с USB-накопителя. Mandriva Flash содержит необходимые офисные приложения и достаточно места для хранения ваших настроек и данных. Все, что нужно для загрузки защищенного рабочего места — это любой компьютер, поддерживающий загрузку с USB-носителя.

Надежный сервер

Mandriva Corporate Server 4 Update 3 — надежное решение для сервера. На базе Mandriva Corporate Server можно создать: интернет-сервер, почтовый сервер, сервер баз данных, сервер приложений, сервер печати, и т.д.

* Сертификат ФСТЭК по 5 классу для СВТ и 4 уровню контроля НДВ.

Сертифицированные ФСТЭК продукты рекомендуются к использованию в государственных организациях и организациях, обрабатывающих персональные данные граждан.

Приобрести сертифицированные ФСТЭК продукты вы можете в ГНУ/Линуксцентре.

www.linuxcenter.ru | Телефон в Москве: (499)271-49-55 | Телефон в Санкт-Петербурге: 8(812) 309-06-86

Визитка

АЛЕКСЕЙ ТАРАНЕНКО, MCTS SCCM 2007, Microsoft Certified IT Professional: Server. Один из создателей сайта itband.ru

SCCM 2007 R2

резервное копирование и восстановление

Рано или поздно настанет день, когда даже самая стабильная система поведет себя неправильно, и ее придется восстанавливать. Важно встретить этот момент во всеоружии.

Лето – пора отпусков. Ничто так не восстанавливает нервы, как несколько недель на море. Но отпуск рано или поздно заканчивается. Иногда возвращение на работу может быть омрачено авариями ИТ-инфраструктуры, которые случились во время вашего отсутствия. Максимально ускорить процесс восстановления работоспособности информационных систем призваны резервные копии.

Для начала необходимо определиться, от каких угроз помогут уберечься резервные копии. Их можно разделить на два класса: нежелательная (несанкционированная) модификация и полное или частичное уничтожение информации. В первом случае мы можем говорить как о халатности обслуживающего персонала, так и о непреднамеренной ошибке в настройке сайта SCCM, когда была произведена нежелательная модификация базы данных или настроек сайта. Во втором, скорее, о выходе из строя аппаратной части сервера, на котором установлена одна из систем сайта Configuration Manager 2007 .

В зависимости от этих классов угроз рассмотрим несколько решений для резервного копирования данных сайта SCCM 2007.

Рассмотрим пример следующей инфраструктуры: Windows Server 2003 (WSUS, WDS, ISS) – центральный сайт SCCM 2007, включая следующие роли: OS Deployment, Software Delpoyment, Update point, Report point. База данных сайта хранится на отдельном сервере, под управлением SQL 2005.

Backup ConfigMgr

Для защиты от ошибок в настройках сайта или базе данных лучше всего подойдет встроенный механизм резервного копирования Configuration Manager 2007 – Backup ConfigMgr. Он позволяет архивировать следующие данные:

- база данных сайта Configuration Manager (база данных сервера SQL);
- каталог установки Configuration Manager на сервере сайта;
- основной файл параметров сайта (.\Inboxes\Sitectrl.box\Sitectrl.ct0);
- разделы реестра (HKLM\Software\Microsoft\SMS и HKLM\Software\Microsoft\NAL) на сервере сайта.

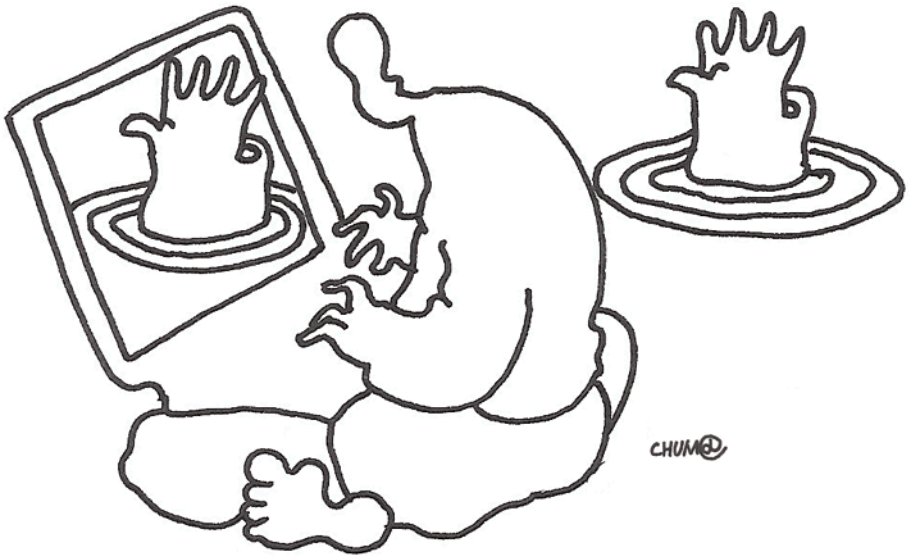
Все остальные данные (включая стандартные точки распространения и точки распространения филиала, точки управления, точки формирования отчетов и точки обнаружения серверов и прочее) считаются легко восстановимыми и поэтому не подлежат копированию в задаче Backup ConfigMgr.

Стоит отметить, что для нормального восстановления информации через Backup ConfigMgr необходимо строго соблюдать синхронизацию данных. То есть, обладая только резервной копией базы данных сайта, будет невозможно произвести восстановление сайта SCCM 2007.

Мастер резервного копирования Configuration Manager 2007 использует в своей работе Volume Shadow copy Service (VSS), добиваясь создания актуальных теневых копий.

Задание резервного копирования сайта SCCM 2007 доступно из консоли администрирования Configuration Manager Console. Для настройки расписания резервного копирования необходимо перейти в консоли администрирования к пункту Site Database → Site Management → Site Code → Site Setting → Site Maintenance → Task → Backup ConfigMgr Site Server (см. рис. 1). Для активирования задания необходимо отметить параметр Enable this task, задать расписание архивирования, а также место хранения архивных файлов. Папку архивирования можно указывать в локальном формате (например, C:\backup) или в формате UNC (например, \\server\sharebackup). Таким образом вы можете сохранять резервную копию как на переносной USB-диск, подключенный локально, так и на централизованное сетевое хранилище. Если указанный путь не существует, он будет создан задачей. Для успешной архивации данных необходимо, чтобы учетная запись сервера SCCM имела разрешение на запись и удаление для данного ресурса, кроме того, учетная запись сервера SQL также должна иметь такие разрешения. Работа задания регистрируется в лог-файле ./smsbkup.log.

Важно! Задача Backup ConfigManager Site Server – считывать параметры запуска раз в сутки. Поэтому если задание архивирования данных отработало некорректно, необходи-



мо исправить неверно заданные параметры задачи, ориентируясь на записи в лог-файле, а затем вручную запустить службу Backup ConfigManager Site Server командой:

```
net start SMS_Site_Backup
```

При выполнении задания Backup ConfigManager Site Server создает моментальный снимок системы. При повторном выполнении задания резервного копирования этот снимок будет перезаписан. Таким образом, по умолчанию будет сохранен только один, последний снимок сайта. Рекомендуется хранить несколько моментальных снимков системы сайта, поскольку вы можете пропустить момент нежелательной модификации настроек сайта, и таким образом эти данные попадут в архив. Кроме того, поскольку задача Backup ConfigManager Site Server вначале удаляет старый снимок, а только потом записывает новый, в случае сбоя задачи резервного копирования моментальный снимок не будет создан, а предыдущий будет утрачен. Для решения этих проблем предназначен файл AfterBackup.bat. Мастер резервного копирования запускает файл после успешного снятия снимка системы сайта. Отсутствие файла не вызывает ошибок в работе Backup ConfigManager Site Server. Вы должны самостоятельно создать файл AfterBackup.bat и сохранить его в папке ConfigMgrInstallPath>\inboxes\smsbkup.box. Файл может содержать любую произвольную последовательность команд, например, таких как архивирование моментального снимка с помощью WinRAR или 7zip на сторонний носитель.

После выполнения задачи резервного копирования в папке-получателе будет создана структура папок, как на рис. 2.

Хотя по умолчанию Backup ConfigManager Site Server копирует только самые необходимые данные, этот список можно расширить. В этом нам поможет файл Smsbkup.ctl, который находится в папке <ConfigMgrInstallPath>\inboxes\smsbkup.box. Этот текстовый файл содержит настройки копирования задачи Backup ConfigManager Site Server. Вы можете отредактировать файл, указав для резервного копирования дополнительные каталоги и ключи реестра.

Рисунок 1. Настройка расписания архивирования с помощью Backup ConfigMgr Site Server

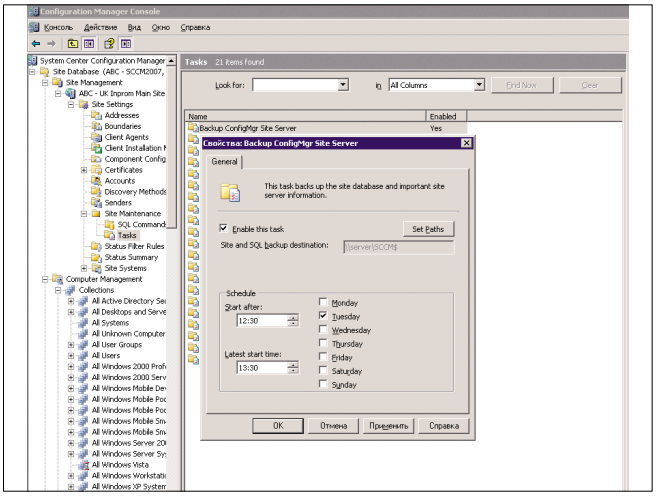
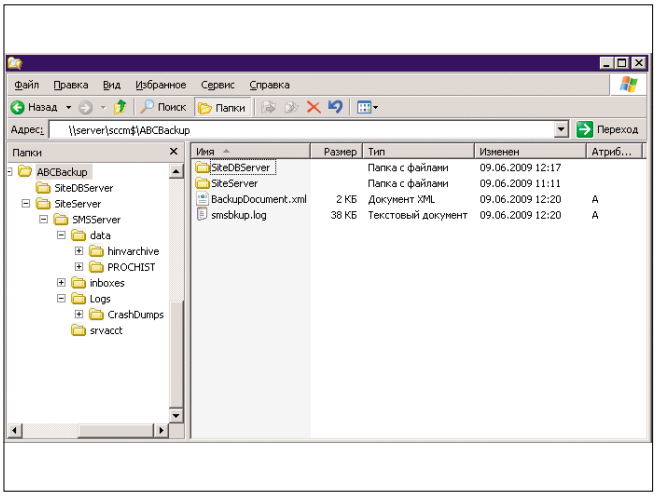


Рисунок 2. Структура папок резервной копии



Внимание! Никогда не пытайтесь удалить или переопределить настройки, которые уже прописаны в файле по умолчанию. Это может привести к полной неработоспособности механизма резервного копирования.

Резервное копирование всех систем сайта

Не очень удобно указывать в данном файле копирование дополнительных компонентов, таких как файлы на точке распространения или файлы обновлений Windows. Поскольку время копирования этих файлов будет велико, и все это время сайт SCCM 2007 будет отключен. Поэтому для копирования остальных систем сайта Configuration Manager 2007 воспользуемся сторонними средствами, например штатной утилитой Windows Server 2003 NTBackup.

Для начала определимся, какие данные нам необходимо архивировать дополнительно. Разумеется, если мы можем себе позволить архивировать сервер SCCM целиком через образы дисков, то лучше так и поступить. Но часто сайт SCCM 2007 совмещают с некоторыми другими ролями (например, файл-сервером), и архивирование через снятие образов дисков не желательно. В любом случае крайне важно архивировать системный диск, а также состояние системы (system state). В идеале на сервере SCCM 2007 должно быть два раздела: первый – основной системный, на нем хранятся файлы Windows и Configuration Manager 2007. Второй – для хранения точки распространения, образов WIM, файлов обновлений WSUS и т.д. В зависимости от того, какие из ролей установлены на сервере, можно составить список необходимых к архивации каталогов (см. таблицу 1).

Чаще всего в уже настроенной среде файлы в этих каталогах изменяются довольно редко. В основном, когда происходит загрузка новых обновлений или добавление какой-либо новой программы на точку распространения. Поэтому копирование этих данных можно делать реже, чем архивацию конфигурационных данных. Например, можно делать полную копию данных каждое второе воскресенье месяца (поскольку каждый второй вторник месяца корпорация Microsoft проводит выпуск обновлений), а в остальные воскресенья делать дифференциальную копию данных. Разумеется, вам необходимо самостоятельно оценить частоту создания резервных копий.

Таблица 1. Примерный список каталогов для резервного копирования

Роль	Каталог
Сервер SCCM	Системный диск (C) Состояние системы (system state)
Точка распространения	SMSPKGx$, x- буква диска
Software Deployment	Папка с исходными файлами для распространяемых программ
Operation System Deployment	SMSSIG$ – точка распространения загрузочных образов RemoteInstall – папка RemInst WDS сервера Папка с WIM-файлами Папка, содержащая исходные файлы драйверов Папка с пакетами драйверов
Software Update	WSUSContent – папка файлов обновления WSUS Папка пакетов обновлений SCCM

Восстановление работоспособности сайта

Теперь пора рассмотреть процедуру восстановления работоспособности сайта SCCM 2007. Мы будем восстанавливать сервер Configuration Manager 2007 с тем именем и кодом сайта, которые были до «падения» сервера. Различается две задачи восстановления работоспособности сайта SCCM 2007: восстановление базы данных сайта и восстановление систем сайта.

Восстановление базы данных сайта SCCM 2007

Воспользуемся консолью SQL Server Manager Console для восстановления базы данных сайта. В первую очередь необходимо закрыть все консоли управления сайтом Configuration Manager Console и остановить на сервере SCCM службы SMS_Executie и SMS_Site_Component_Manager. Затем в консоли SQL Server Manager Console необходимо отключить существующую базу данных сайта SCCM 2007 и, воспользовавшись командой восстановления, указать файлы .mdf и .ldf, созданные задачей Backup ConfigManager Site Server для восстановления. После этого необходимо запустить остановленные службы и проверить работоспособность базы данных.

Важно! Процесс переноса базы данных сайта SCCM с одного сервера SQL на другой не сильно отличается от процесса восстановления. Восстанавливаете базу данных на новом сайта SQL, а затем в консоли администрирования SCCM 2007 используйте мастер Database Connection Wizard (корень консоли → щелчок правой кнопкой → All task → Connect to Site Database) для указания нового местоположения базы данных сайта.

Восстановление систем сайта

Для использования резервных копий, созданных задачей Backup ConfigManager Site Server, воспользуемся мастером Configuration Manager Site Repair Wizard. И хотя мастер автоматически устанавливается на сервер SCCM, а также на все компьютеры, на которые устанавливается консоль администрирования Configuration Manager consol, мастер восстановления сайта необходимо запускать только с консоли, установленной на сервере восстанавливаемого сайта.

Нажмите кнопку «Пуск» и перейдите к пункту Microsoft System Center → Configuration Manager 2007 → Configuration Manager Site Repair Wizard. В стартовом окне мастера убедитесь, что в поле Site server to be repaired отображается имя сервера сайта, который требуется восстановить. На следующей странице выберите место расположения резервной копии. Если база данных сайта не требует восстановления, то выберите Do not restore database. Выполните восстановление сайта. Затем на странице «Параметры родительского сайта (Parent Site Settings page) необходимо проверить настройки и убедиться, что они не менялись со времени создания резервной копии. Если восстанавливаемый сайт входил в иерархию сайтов SCCM, необходимо на странице проверки иерархии сайта убедиться, что адреса всех связанных (родительского и дочернего) сайтов указаны правильно. Если данные не верны, исправить их можно с помощью кнопок «Добавить» (Add) и «Удалить»(Remove).

Важно! Вы можете создать дочерний сайт, который будет выполнять функции эталонного сайта в случае сбоя основного сайта системы. В таком случае с этого сайта можно будет восстановить любые объекты, созданные с момента

снятия резервной копии основного сайта. Для этого необходимо выбрать поле «Восстановить данные с указанного сайта» (Recover data from reference site).

На странице «Панель объектов» (Object Pad) укажите количество коллекций, пакетов и объявлений, созданных на сайте с момента последней резервной копии. Это необходимо, чтобы идентификаторы этих объектов, создаваемых в будущем, не совпадали с уже созданными пакетами. На следующем шаге «Восстановление пакета» (Package Recovery) можно проверить состояние локальной точки распространения программ.

Важно! Лог работы мастера восстановления сохраняется в c:\SMS\Logs\sms_srw.log.

После восстановления сервера сайта мастером Site repair wizard дополнительные роли на сервере сайта не будут переустановлены до тех пор, пока не будет выполнен сброс сайта SCCM. Для сброса настроек сайта Configuration Manager 2007 закройте все открытые подключения консоли Configuration Manager к серверу сайта. На сервере основного сайта нажмите кнопку «Пуск», последовательно выберите «Все программы → Microsoft System Center → Configuration Manager 2007 → Configuration Manager Setup» или перейдите в каталог .\bin\i386 установочного носителя Configuration Manager 2007 и дважды щелкните мышкой файл Setup.exe.

На странице приветствия мастера установки Configuration Manager нажмите кнопку «Далее».

На странице «Параметры установки» мастера установки Configuration Manager выберите элемент «Выполнить обслуживание сайта» или «Сброс сайта». На странице «Обслуживание сайта» выберите «Повторно применить заданный по умолчанию файл и разрешения реестра на этом сервере сайта». В диалоговом окне подтверждения сброса сайта нажмите кнопку «Да». Программа установки Configuration Manager выполнит сброс сайта.

Preinst.exe

Средство обслуживания иерархии устанавливается автоматически при установке Configuration Manager 2007. Программу preinst.exe можно найти в общем каталоге \SMS_<код сайта>\bin\i386\<код языка> на сервере сайта, а также в каталоге \SMSSETUP\BIN\I386\<код языка> в файлах установки Configuration Manager 2007.

С помощью средства обслуживания иерархии можно диагностировать проблемы на сайте, восстановить сайт или остановить все службы Configuration Manager 2007 сайта. Например, предположим, что сайт Configuration Manager 2007 был некорректно удален путем отключения дочернего сайта от его родительского сайта без предварительного удаления дочернего сайта из базы данных родительского сайта. Это приведет к проблемам, поскольку родительский сайт будет по-прежнему пытаться отправлять данные отключенному дочернему сайту и получать от него данные. Для устранения такой ситуации можно с помощью средства обслуживания иерархии обойти консоль Configuration Manager и удалить некорректно удаленный дочерний сайт из базы данных родительского сайта.

Подробнее о preinst.exe можно прочитать: http://technet.microsoft.com/ru-ru/library/bb693624.aspx.

Восстановление связанных с SCCM файлов

Если сервер SCCM был полностью уничтожен, то для максимально быстрого введения в строй выполните следующие действия:

- Используйте файлы резервных копий, созданные программой ntbackup, для восстановления системного диска и состояния системы.
- Восстановите папки данных, при этом буква диска должна совпадать с буквой диска на старом сервере.
- Воспользуйтесь мастером Configuration Manager Site Repair Wizard для восстановления актуального состояния конфигурационных данных сайта SCCM 2007.

Рекомендуется использовать встроенный мастер восстановления (Backup ConfigMgr Site Server) для защиты от нежелательных изменений в параметрах сайта, поскольку такой подход позволит экономить дисковое пространство, занимаемое резервными копиями.

В то же время важно не забывать и об остальных частях сайта SCCM 2007: файлах WIM, содержащих в себе образы операционных систем, подготовленных к автоматической инсталляции дистрибутивов программ и файлов обновлений. Восстановление этих данных с нуля из-за выхода из строя аппаратной части сервера может потребовать значительных усилий от администратора и большого количества времени.

Но поскольку эти данные занимают большие объемы дискового пространства, достигая порой нескольких сотен гигабайт, и зачастую почти не меняются или меняются очень редко, то для архивирования такой информации можно порекомендовать делать образ системного диска и важных каталогов раз в месяц. EOF

Визитка

АРТЕМ ХАЗОВ, директор по продажам. Работает в компании Aflex software – официальном представительстве западных разработчиков программных решений на территории России и СНГ

Безопасность бизнеса *

Защищаем информационные активы

За последние пять лет 93% компаний, утративших особо важные данные, ушли с рынка. Как избежать этого и обеспечить безопасность своего бизнеса?

Финансовый кризис, не утихающий по сей день, затронул большинство как российских, так и международных компаний. Сокращение бюджетов вынуждает руководство ИТ-департаментов максимизировать использование имеющихся в их распоряжении ресурсов, а также экономить на приобретении новых программно-аппаратных комплексов. Однако именно в период кризиса особенно важно обеспечить непрерывность бизнес-процессов всего предприятия и каждого его подразделения в отдельности. Соответственно одной из главных задач ИТ-службы становится поддержание работоспособности корпоративных информационных систем и запущенных на них приложений, а также реализация практических мероприятий по защите информационных активов от утраты или хищения. Обеспечить непрерывность бизнес-процессов и работы информационной системы в целом можно разными способами. Например, можно создать физически защищенную систему хранения данных, использовать кластерные системы с репликацией данных между серверами кластера, хранить данные в RAID-массивах и т.д. Однако все эти меры не отменяют необходимости применения специальных программных решений, обеспечивающих резервное копирование данных и возможность их последующего восстановления. Причем в ряде случаев этот метод окажется наименее затратным.

На разработке таких решений специализируется международная компания Acronis. Ее флагманский продукт, Acronis True Image Enterprise Server, успешно зарекомендовал себя во множестве российских и зарубежных компаний. Это решение позволяет предприятиям комплексно решить задачи резервного копирования и восстановления данных ИТ-инфраструктуры современных предприятий, включающей в себя любое сочетание физических и виртуальных серверов под управлением Windows и Linux. Пользователю Acronis True Image Enterprise Server доступно создание полных образов жесткого диска сервера, включая операционную систему, все настройки и данные методом посекторного резервного копирования, а также резервирование отдельных файлов и папок. Технологии Acronis позволяют восстановить систему с установленными приложениями и пользовательскими данными без переустановки вручную, сократив время восстановления работоспособности сервера после сбоя до нескольких минут. Кроме того, при использовании отдельно лицензируемого модуля Universal Restore пользователь системы резервного копирования и восстановления серверов под управлением Windows может разворачивать резервный образ на оборудование, конфигурация которого отлична от эталонного. При этом Acronis True Image Enterprise Server предоставляет на выбор разные варианты резервирования: полное – с включением в резервную копию содержимого жесткого диска или раздела целиком, дифференциальное и инкрементное – только для новых и измененных файлов, а также различные варианты фильтров и масок по типам файлов, чтобы включать в резервные образы только действительно необходимые данные. Встроенные средства удаленного администрирования позволяют централизованно управлять резервированием данных всех серверов в локальной сети. Отмечу, что резервное копирование и восстановление данных происходит в фоновом режиме, позволяя обеспечить непрерывность бизнес-процессов компании. Резервное копирование, восстановление и другие операции выполняются с помощью «мастеров», поэтому внедрение программы требует минимальной подготовки персонала. С центральной консоли управления производится удаленное администрирование всех компьютеров, на которых установлен агент Acronis, независимо от их принадлежности к домену и рабочей группе.

Рассмотрим подробно процедуру создания резервной копии и ее развертывания на примере решения Acronis True Image Enterprise Server. Взаимодействие пользователя с системой Acronis True Image Enterprise Server осуществляется через интегрированную консоль управления – специальный инструмент для удаленного доступа к компонентам Acronis. С консоли администратор удаленно устанавливает и конфигурирует компоненты, управляет их работой. С ее помощью пользователь может удалённо запускать процедуры создания резервных копий и их развертывания, создавать и модерировать планы резервирования отдельных серверов и серверных групп, а также управлять другими функциями.

Встроенный планировщик Acronis True Image Echo Enterprise Server поможет создать для разных групп компьютеров различные задания по резервному копированию, регулярно запускаемые в определенное время или при наступлении определенных событий.

Для подтверждения успешного завершения копирования или при необходимости вмешательства пользователя Acronis True Image Echo Enterprise Server может отправлять оповещения по электронной почте или с помощью сервиса Winpopup. Также программа может оставлять записи в Журнале событий Windows или автоматически посылать их клиентам SNMP.

Программа позволяет задать команды, которые будут выполняться до и после резервного копирования или восстановления. Например, перед созданием образа диска можно автоматически запускать антивирус, а после создания образа – проверять целостность данных в нем. Поскольку все эти события можно планировать, нет необходимости каждый раз заново составлять сценарии, достаточно один раз создать задание, и в дальнейшем оно уже будет выполняться автоматически.

Установив систему на сервер, рекомендуется незамедлительно создать резервные копии всех дисков сервера. Сделать это можно, запустив специальный инструмент – Мастер резервного копирования. Здесь пользователю предлагается выбрать тип данных, резервная копия которых будет создана. При выборе опции «Мой компьютер», система создаст полные образы логических дисков сервера. Выбрав опцию «Мои данные», пользователь сможет самостоятельно назначить папки с наиболее ценными файлами, которые будут помещены в резервный архив. При первичном выполнении операции резервирования данных предпочтительно выбрать опцию «Мой компьютер» и создать загрузочный диск аварийного восстановления Acronis. В дальнейшем для сохранения актуальности созданных архивов образы дисков необходимо периодически обновлять.

Помимо инкрементного и дифференциального, применяется также полное резервное копирование серверов. В первом случае записывается только информация, изменившаяся с момента создания последней резервной копии. Такие архивы создаются быстро и, как правило, имеют небольшой размер. Для полного восстановления системы необходимо сохранять все последовательно созданные инкрементные копии. Дифференциальные архивы представляют собой единый файл, куда записываются все изменения, сделанные с момента создания полной резервной копии. При этом инкрементные архивы по мере их накопления можно объединять в один дифференциальный. Поскольку полное резервирование данных со временем будет занимать все больше и больше времени, рекомендуется регулярно создавать архивы изменений, например, инкрементные – ежедневно, а дифференциальные – раз в неделю.

Затем пользователь может выбрать логические диски, которые будут резервироваться, и место хранения резервных копий. Администратор может выбрать удобный ему способ хранения: резервные копии можно записывать в специальный скрытый защищенный раздел жесткого диска (так называемая Acronis Secure Zone) или хранить на жестком диске, в сетевых папках и хранилищах данных (SAN, NAS), ленточные накопители, FTP.

Назначив диски для резервирования и место для хранения копий, пользователь может выбрать тип создаваемого образа диска: полный, инкрементный или дифференциальный. В случае когда необходимо зарезервировать все содержимое жесткого диска, целесообразно создать полный его образ. Далее пользователю предлагается принять параметры создания резервной копии по умолчанию (например, степень сжатия данных, быстродействие, а также параметры безопасности файлов) или же назначить их по своему усмотрению.

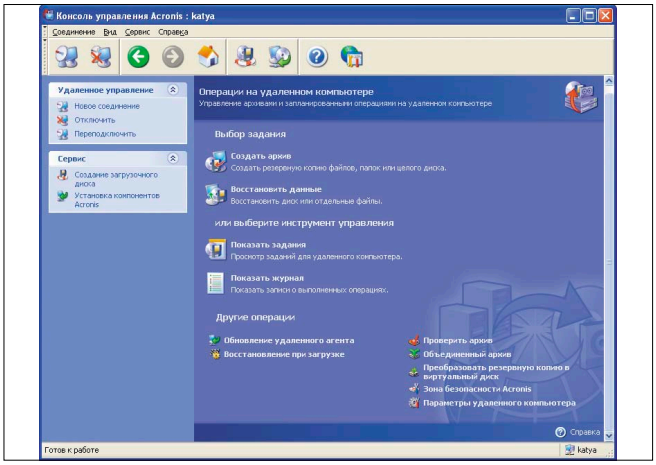
Теперь, проверив напоследок все параметры будущего резервного архива, пользователь может приступить к его созданию. Время сохранения резервной копии зависит от объема данных и от того, куда вы ее записываете. Запись 10 Гб на тот же самый физический диск займет около 10 минут.

Продукты линейки Acronis Recovery разработаны специально для посекторного резервного копирования и восстановления баз данных и наряду с этой функцией позволяют сохранять записи журнала транзакций. Благодаря этому база данных сохраняется в максимально актуальном состоянии, а пользователь получает возможность восстановить ее в предельно сжатые сроки. Сегодня линейка Acronis Recovery включает в себя решения для базы данных MS SQL и для Microsoft Exchange Server. В ближайшее время планируется выпустить на российский рынок специализированное решение для баз данных Oracle.

Производители систем резервирования и восстановления данных постоянно совершенствуют свои решения, расширяя их функционал и упрощая пользовательский интерфейс. Уже сейчас успешно работать с такими решениями может даже специалист, обладающий даже минимальными знаниями о резервировании данных и критически важных приложений, а большинство операций архивирования и вовсе автоматизировано. Широкий спектр представленных на рынке продуктов позволяет заказчикам выбирать оптимальные именно для себя, с учетом политики лицензирования и функциональных особенностей решений разных вендоров. EOF

* На правах рекламы

Консоль управления Acronis True Image Enterprise Server



Визитка

ИВАН КОРОБКО, сертифицированный специалист MCP, автор более 50 статей и двух книг. Занимается созданием различных приложений для Active Directory

Active Directory

Проводим профилактическое обслуживание

Ядро контроллера домена — база данных AD, которая нуждается в обслуживании. Благодаря специально созданному для этого сервисному режиму, задача решается просто.

Данные в Active Directory автоматически оптимизируются каждые 12 часов в режиме реального времени. В ходе этой процедуры осуществляется перемещение данных из временных файлов непосредственно в файл базы ntds.dit. Но этого недостаточно, поскольку размер базы данных постоянно увеличивается при условии, что в Active Directory вносятся различные изменения: создаются новые учетные записи, изменяются их свойства и т.д.

Во время работы базы данных никаких работ по ее управлению провести невозможно, поскольку доступ к ней закрыт. Все работы по восстановлению, дефрагментации базы, проверки ее целостности можно провести в специально созданном сервисном режиме. Не стоит забывать о том, что любая база данных – это всего лишь набор файлов, а с другой стороны – набор таблиц, которые взаимосвязаны друг с другом.

Таблица 1. Файлы каталога NTDS

Название файла	Описание
NTDS.DIT	База данных Active Directory
EDD.CHK	Проверочный (checkpoint) файл
EDB.LOG	Журнал транзакций (событий). Все изменения, происходящие с каталогом Active Directory, содержатся в этом файле. Размер файла ограничивается 10 Мб.
EDBxxxx.LOG	Вспомогательные журналы событий, которые создаются, когда файл EBD.LOG уже достиг 10 Мб, а данные еще не выгружены в файл NTDS.DIT. Соответственно каждый файл занимает не более 10 Мб дискового пространства
RES1.LOG	Резервный файл журнала событий
RES2.LOG	Резервный файл журнала событий
TEMP.EDB	Временный журнал, который содержит информацию о событиях, происходящих в настоящий момент
SHEMA.INI	Необязательный файл, используемый для инициализации файла NTDS.DIT во время загрузки контроллера домена

Active Directory как часть файловой структуры

База данных Active Directory хранится на контроллере домена в файле NTFS.DIT, который находится в папке %SYSTEMROOT%\NTDS.

Файл базы данных имеет ряд особенностей, о которых всегда необходимо помнить:

- Размер файла NTFS.DIT увеличивается фиксированными порциями, занимая целое число страниц, во избежание их дробления. Из-за этого размер каталога Active Directory всегда больше, чем он есть на самом деле.
- В нормальном режиме функционирования домена файл базы данных всегда открыт и не может быть скопирован.
- Размер открытого файла не обновляется. Фактический размер базы данных можно определить исходя из свободного пространства на жестком диске.
- В подключенном состоянии база данных не может быть дефрагментирована. Для использования утилиты дефрагментации NTDSUTIL.EXE необходимо перезапустить домен в сервисном режиме.

Кроме файла NTDS.DIT в каталоге %SysytemRoot%\NTDS находятся вспомогательные файлы (см. рис. 1), функция которых кратко описана в таблице 1. Все перечисленные файлы обеспечивают две важных функции: отказоустойчивость базы данных и ее дефрагментацию в режиме реального времени.

Active Directory как база данных

Файл NTDS.DIT представляет собой базу данных, состоящую из трех таблиц:

Схема каталога. В этой таблице хранится описание объектов: их атрибуты, соответствующие им типы данных и другая служебная информация. Схема Active Directory расширяется только в случае крайней необходимости, поэтому можно считать, что это статическая таблица.

Таблица ссылок. Здесь зафиксированы сопоставления полей, которые выполняются во время просмотра тех или иных значений администратором. Ярким примером явля-

ется список групп, членами которых является выбранный пользователь (см. рис. 2). В каталоге Active Directory значением поля member является distinguishedname объекта. Администратор же видит не относительный составной путь к группе, а его отображаемое имя (поле cn). Таблица ссылок самая маленькая среди существующих и не поддается изменению.

Таблица данных. Это самая большая таблица, доступ к которой осуществляется с помощью мастеров Active Directory Users and Computers, Active Directory Sites and Services. В ней находится вся информация об объектах в домене: пользователях, группах и других сущностях, описанных в схеме. Также из этой таблицы осуществляется обращение к таблице ссылок и вывод значений, удобных для чтения.

Резервное копирование Active Directory

Перед дефрагментацией каталога Active Directory необходимо сделать резервную копию. Не стоит полагаться на собственный опыт и пренебрегать элементарными правилами работы системного администратора, ведь самое страшное, что может случиться, – это потеря данных, а не выход сервера из строя, как многие думают.

Резервное копирование, а точнее слепок состояния системы (System state), выполняется в нормальном режиме работы контроллера домена с помощью утилиты NTBACKUP.EXE. Эта процедура включает в себя копирование таких элементов как:

- каталог Active Directory (файлы NTDS.DIT, EDB.CHK, EDB*.LOG, RES1.LOG, RES2.LOG);
- системные компоненты (реестр, база зарегистрированных классов COM+, SYSVOL, кластер);
- сервисы, связанные с функционированием Active Directory (сервер сертификатов, DNS).

Перечень компонентов зависит от конфигурации вашего домена.

Запуск утилиты осуществляется из командной строки с помощью команды NTBACKUP. Для создания резервной копии системы (System State) необходимо запустить соответствующий мастер, вызвав Backup Master в меню Tools

Рисунок 1. Содержимое каталога %SystemRoot%/NTDS

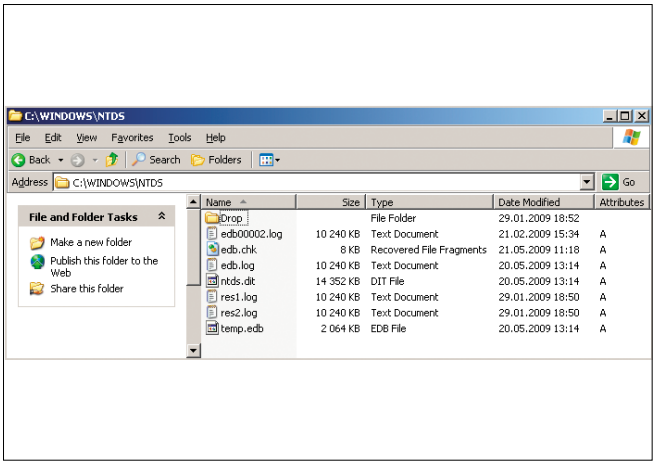
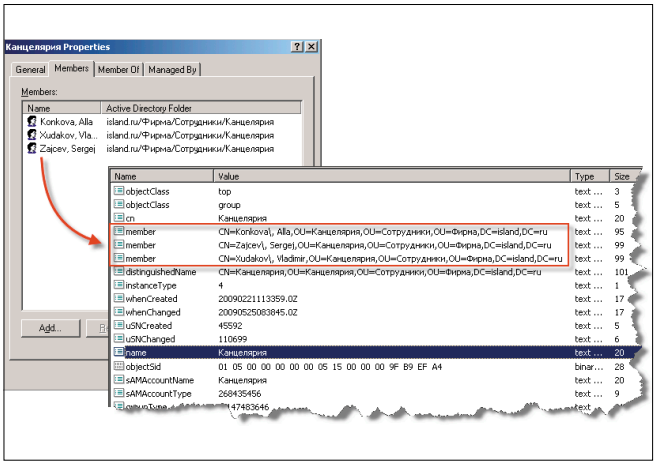


Рисунок 2. Пример использования таблицы ссылок



и в предлагаемом меню выбрав вариант Only back up the System State data (см. рис. 3).

Далее остается выбрать путь резервного копирования системы и инициализировать процесс. Результатом работы мастера является файл с расширением BKF. По умолчанию предлагается имя backup.bkf.

Запуск контроллера домена в сервисном режиме

Для входа в сервисный режим контроллера домена его необходимо перезагрузить и вызвать меню загрузки с помощью клавиши <F8>, в появившемся меню (см. рис. 4) выбрать Directory Services Restore Mode. Режим представляет собой еще одну модификацию Safe Mode, созданного специально для управления базой данной Active Directory в сервисном режиме. Большинство манипуляций с базой Active Directory осуществляется с помощью утилиты NTDSUTIL.EXE, входящей в комплект операционной системы.

Возможности оболочки NTDSUTIL

Восстановление, дефрагментация и другие сервисные манипуляции с базой данных Active Directory осуществляются с помощью оболочки NTDSUTIL.EXE, лишенной графического интерфейса. По умолчанию файл NTDSUTIL.EXE находится в каталоге %SystemRoot%\System32.

После запуска оболочки необходимо инициализировать нужный режим работы с помощью одной из команд, приведенной в таблице 2.

Управление файлами NTDS базы данных

Для входа в режим управления файлами базы данных необходимо войти в режим FILES (см. таблицу 2). Для этого наберите FILES и нажмите клавишу <ENTER> в командной строке оболочки NTDSUTIL.

Все профилактическое обслуживание Active Directory осуществляется в этом режиме. Работы состоят из нескольких этапов, которые могут исключаться, переставляться и т.д. В случае серьезных проблем с каталогом Active Directory приведенный регламент не подходит.

Проводимые работы можно разбить на три этапа:

- получение информации о базе данных;
- резервное копирование базы данных;
- проверка на наличие ошибок в Active Directory.

Рисунок 3. Запуск мастера создания резервной копии

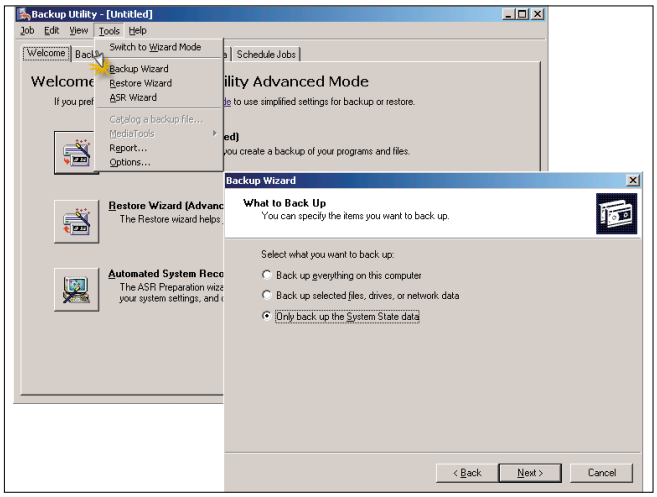


Рисунок 4. Вызов Directory Services Restore Mode

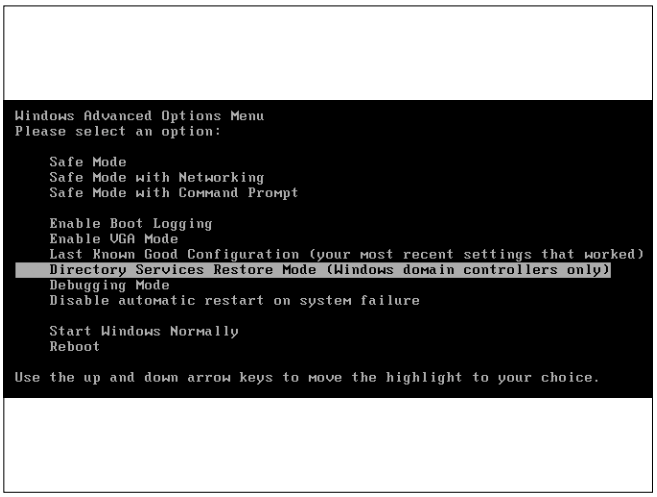


Рисунок 5. Пример работы команды INFO

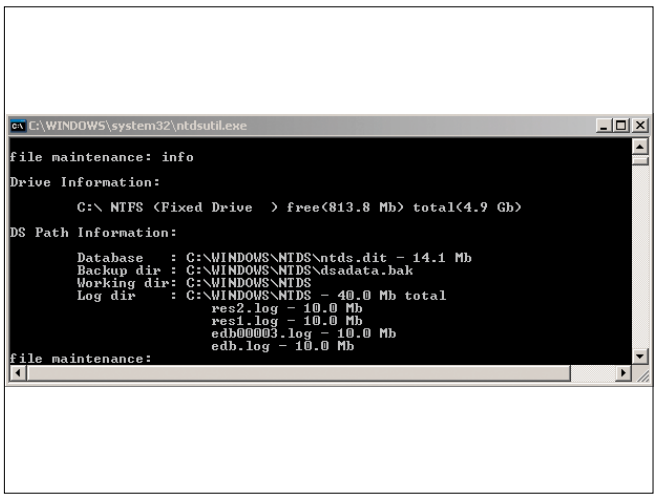
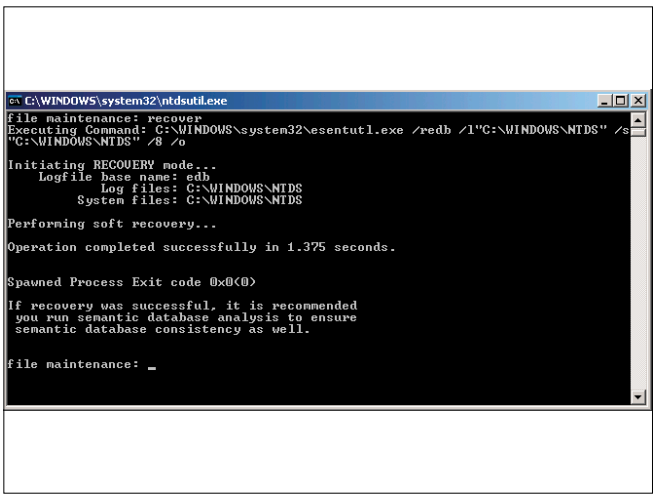


Рисунок 6. Проверка базы данных Active Directory



Получение информации

Получаемая в ходе проверки информация позволит проконтролировать состояние файлов базы данных, внутренних взаимосвязей и получить реальный размер базы данных Active Directory. Для получения информации используются три команды:

CHECKSUM. Определяет контрольную сумму файла базы данных NTDS.DIT. Одновременно определяется размер файла, количество страниц в Active Directory.

INFO. С помощью этой команды осуществляется анализ всех файлов (см. рис. 5), участвующих в процессе работы Active Directory (см. таблицу 1).

INTEGRITY. Осуществляется логическая проверка взаимосвязей в базе данных Active Directory.

Дефрагментация базы данных

Дефрагментация базы данных позволит сократить размер базы и убрать из нее «пустые» страницы. Для выполнения этой процедуры используют команду COMPACT TO %S, %S – путь к каталогу, в который будет записана дефрагментированная база данных Active Directory. Таким образом, используя дефрагментацию, администратор параллельно создает резервную копию Active Directory.

Проверка базы данных Active Directory

Для проверки и восстановления базы данных Active Directory используется команда RECOVER, которая инициализирует вызов утилиты esentutl.exe. После выполнения команды на экране появляется отчет (см. рис. 6).

Каждый новый пакет обновлений для сервера (service pack), каждая новая версия Windows Server таят в себе потенциальную опасность для целостности Active Directory. Регулярная проверка состояния базы данных позволит предотвратить неприятные последствия, а резервное копирование – восстановить ее максимально быстро. Вдобавок ко всему дефрагментация базы данных позволит увеличить скорость работы контроллера домена. EOF

Таблица 2. Режимы работы утилиты NTDSUTIL

Команда	Описание режима работы
Authoritative restore	Надежное восстановление DIT базы данных
Configurable Settings	Настройка параметров соединения с доменом
Domain management	Подготовка к созданию нового домена
Files	Управление файлами NTDS базы данных
Group Membership Evaluation	Управление идентификаторами безопасности SID пользователей групп и пользователей
LDAP Policies	Управление политиками протокола LDAP
Metadata cleanup	Очистка метаданных
Roles	Управление ролями контроллера домена
Semantic database analysis	Семантический анализ базы данных
Set DSRM Password	Сброс пароля учетной записи администратора для безопасного режима восстановления каталога

Визитка

ВАДИМ АНДРОСОВ, ассистент ВНУ, специалист МСР. Занимается анализом архитектур организаций с защищаемыми бизнес-процессами

Проводим реализацию
тонкого делегирования прав в Active Directory

Создаем надстройку, позволяющую перемещать учетные записи пользователей между подразделениями только усилиями администраторов организационных единиц.

Графический интерфейс сценариев

Пришло время разработать оставшиеся элементы надстройки (начало см. в СА №3,4,5,6 за 2009 г.). Поскольку речь здесь идет уже о работе с очередями переводимых пользователей, стандартный интерфейс сценариев, основанный на простейших диалоговых окнах, мало подходит. В то же время надстройка слишком проста для того, чтобы ради ее создания использовать сложную коммерческую интегрированную среду разработки.

Существует возможность создания для сценариев более изощренных пользовательских графических интерфейсов, основанных на языке разметки html. Это гипертекстовые приложения (hyper-text applications). По сути это обычная html-страничка со сценарием, которая сохранена с расширением hta. При запуске таких приложений используется графический движок (rendering engine) Internet Explorer. Однако по своей сути они гораздо ближе к обычным программам, чем к веб-страницам. Стандартная модель безопасности IE не распространяется на hta-приложения, что дает возможность свободно работать со всеми объектами операционной системы.

Кроме особого расширения hta-приложения должны иметь в разделе заголовка специальный тег hta:application. Все остальное оформляется как обычный html-документ. Рассмотрим каркас hta-приложения.

Листинг 1. Каркас hta-приложения

```
<head>
<title>Move</title>
<hta:application
contextmenu = "no"
minimizebutton = "no"
/>
<script language = "VBScript">
'Текст сценария
</script>
</head>
<body>
<h1>Some caption<h1>
<i>Some text<i>
</body>
```

Тег hta:application может содержать параметры, на самом деле их гораздо больше [1], но для текущей надстройки этих вполне достаточно. Рассмотрим подробнее используемые параметры.

contextmenu – позволяет отключить стандартное контекстное меню Internet Explorer, так как его содержание (выбор кодировки, просмотр исходного кода приложения и др.) обычно неуместно для программы;

minimizebutton – с помощью этого свойства включается и отключается кнопка минимизации окна.

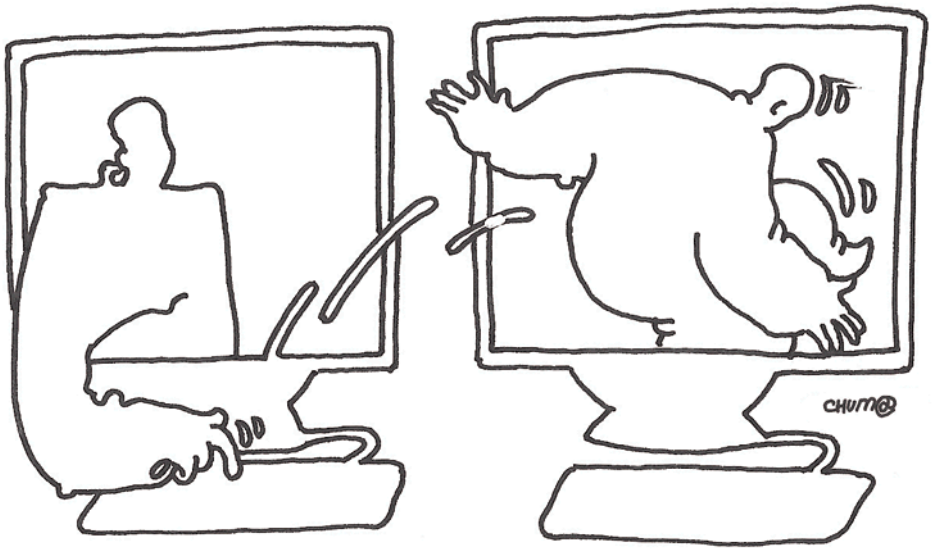
Рассмотрим пример разработки гипертекстового приложения. Основная функциональность будет реализована в последующих разделах. Здесь же обеспечим отображение окна в центре экрана. По умолчанию окно появляется в левом верхнем углу экрана, что совсем неудобно. Дальнейший исходный код должен быть помещен в тело тега script каркаса hta-приложения. Итак, цель – располагая предпочтительным размером приложения, обеспечить его корректное центрирование.

```
Const PREFERRED_WIDTH = 400
Const PREFERRED_HEIGHT = 300
```

Сначала с помощью констант задаем предпочтительные размеры окна. Далее определяется специальная функция window_onLoad. Подпрограмма с таким именем будет автоматически вызвана при загрузке приложения.

```
function window_onLoad()
dim x, y, w, h, scrW, scrH
  Set objWMIService = GetObject("winmgmts:" & ↵
        "{impersonationLevel=impersonate}!\\.\root\cimv2")
 Set colItems = objWMIService.ExecQuery ↵
        ("Select * from Win32_DesktopMonitor")
```

Затем подключаемся с помощью WMI-запроса к объектам типа Win32_DesktopMonitor. Теоретически мониторов может быть несколько, здесь было решено пользоваться первым. То есть цикл ниже выполнится только один раз для первой записи благодаря директиве exit for. Конечная цель – получить разрешение монитора, которое запоминается в переменных scrW (ширина) и scrH (высота).



```
  For Each objItem in colItems
    scrW = objItem.screenWidth
    scrH = objItem.screenHeight
    exit for
  next
```

Переменные x, y будут содержать итоговое положение окна (координаты его левого верхнего угла), w, h – соответственно его ширину и высоту. Изначально эти значения устанавливаются в соответствии с предпочтительными.

```
  w = PREFERRED_WIDTH
  h = PREFERRED_HEIGHT
  x = (scrW - PREFERRED_WIDTH) / 2
  y = (scrH - PREFERRED_HEIGHT) / 2
```

Но предпочтительный размер окна может не поместиться в экран. Для обработки этой ситуации предназначены два условных оператора. Если ширина приложения превосходит ширину рабочего стола, то размер окна устанавливается равным ширине экрана, а координата x – началу экрана (т.е. значению 0). Аналогично решается проблема слишком большой высоты.

```
  if scrW < PREFERRED_WIDTH then
    w = scrW
    x = 0
  end if
  if scrH < PREFERRED_HEIGHT then
    h = scrH
    y = 0
  end if
```

В конце концов окно устанавливается в заданную позицию посредством метода moveTo и масштабируется (метод resizeTo).

```
  window.moveTo x, y
  window.resizeTo w, h
end function
```

Окно с такой стартовой функцией будет всегда или располагаться по центру экрана, или занимать максимум возможного места при превышении размеров экрана. Отдельно упоминать эту функцию я больше не буду, но она будет применяться во всех hta-приложениях надстройки.

Как можно увидеть из этой подпрограммы сценарии в hta-приложениях имеют обычный доступ к инструментам операционной системы (включая WMI). В обычных веб-страницах подобные операции существенно ограничены, несмотря на возможность применения того же языка программирования.

Начало перемещения пользователя

Рассмотрим первое приложение (см. рис. 1). Оно будет вызываться из контекстного меню пользователя оснастки Active Directory Users and Computers для начала операции перемещения. Программа должна позволять пользователю указать целевую организационную единицу, т.е. предоставить средства перемещения по каталогу. Итак, интерфейс достаточно прост. Сверху написано имя перемещаемого пользователя (Gomer J.Simpson), ниже – текущий контейнер (отображается полный путь). Далее идет основной управляющий элемент. Список организационных единиц, входящих в текущую. Нажатие на <ENTER> или двойной щелчок должны производить вход в контейнер. Выбор самого верхнего элемента (<..) позволяет подняться к родительскому контейнеру, если таковой существует. Выбор второй строчки (> <) обозначает команду «Переместить сюда». Как только она выбрана, пользователь ставится в очередь на перевод, а приложение закрывается. Реализуем эту логику.

Общий каркас hta-приложения уже рассматривался. Сначала приведем описание внешнего вида на языке разметки HTML. Все, что нам нужно, это два поля под текст и список. Выглядеть это может так:

Листинг 2. Пользовательский интерфейс, созданный с помощью HTML

```
<body>
<div id = "userToMove"></div>
<hr>
<div id = "curPathShow"></div>
<form name = 'st artMove'>
<select style="width: 350px; height: 200px"
  size=2 name=ouList ondblclick = "itemSelected()"
```

```
  onkeypress = "onKey()">
</select>
</form>
</body>
```

Обоим разделам, куда будет выводиться текст (тег div), сопоставляются идентификаторы (id), благодаря которым к элементам можно будет обращаться из сценария. Для списка (тег select) назначаются обработчики двух типов событий: двойного нажатия кнопки мыши (функция itemSelected) и нажатия клавиши (функция onKey). Но сначала рассмотрим инициализацию приложения. Для работы программы понадобится ряд глобальных переменных:

```
dim curPath, backPath, prevPath, user, engine
```

curPath – путь к текущей организационной единице;
backPath – путь к родительской организационной единице, используется для выхода «наверх»;
prevPath – предыдущая организационная единица, т.е. та, из которой мы попали в текущую;
user – перемещаемый пользователь;
engine – экземпляр основного класса надстройки User Move.Engine, который был создан в предыдущих частях статьи.

Функция инициализации создает экземпляр класса надстройки, устанавливает фокус ввода на список и подключается к объекту перемещаемого пользователя. Что перемещать передается приложению через командную строку и извлекается из нее с помощью функции extractArg, которая будет рассмотрена далее. Затем имя пользователя выводится над списком. В конце устанавливается текущий каталог – тот, в котором находится пользователь.

Листинг 3. Функция инициализации приложения

```
function window_onLoad()
  set engine = createObject("UserMove.Engine")
  startMove.ouList.focus
  set user = getObject(extractArg)
  userToMove.innerhtml = "<b>" & user.cn & "</b>"
  setCurPath(engine.getParent(user.distinguishedName))
end function
```

Для hta-приложений не существует удобного способа получения параметров командной строки, аналогичного обычным сценариям. Однако можно использовать свойство приложения commandline, содержащее полную командную строку вызова: название приложения и параметры. Все что нужно – отделить параметр. Следующая функция возвращает только выделенный параметр.

Свойство commandline имеет вид, подобный следующему:

```
"\\marklar.ua\UserMoveSupport\exec\enqueue.hta" ↵
       "LDAP://main.marklar.ua/cn=Gomer J. Simpson, ↵
       OU=South Park,DC=marklar,DC=ua" user
```

Командная строка состоит из трех частей: полный путь к приложению, выбранный объект пользователя (тот объект, контекстное меню которого использовалось для вызова сценария) и класс объекта. Поскольку вызвать приложение можно только для объектов типа user, проверку типа можно не делать. То есть нам нужно извлечь вторую часть.

Для выделения параметра используется следующее регулярное выражение:

```
".+" "?([^"]+)"? .+
```

Первая часть («.+») обозначает путь к приложению: «один и больше произвольных символов, заключенных в кавычки». Затем следует пробел и вторая часть («?([^»]+)»?), путь к объекту пользователя: «любое количество не кавычек, которое может быть заключено в кавычки». Обратите внимание, второй параметр в случае, когда он не содержит пробелов, передается без кавычек. Именно поэтому в выражении используются знаки вопроса после кавычек, обозначающие один или ноль символов. Затем описывается третья часть после пробела: любое количество любых символов (.+).

Нам необходима вторая часть, поэтому именно ее берем в скобки, чтобы захватить (capture) результат. В VBScript строка не может содержать двойных кавычек, поэтому в программе я написал выражение, используя одинарные, а потом заменил их нужными с помощью функции replace. Символ двойной кавычки был получен по его коду с помощью функции char.

Рисунок 1. Приложения начала перемещения пользователя

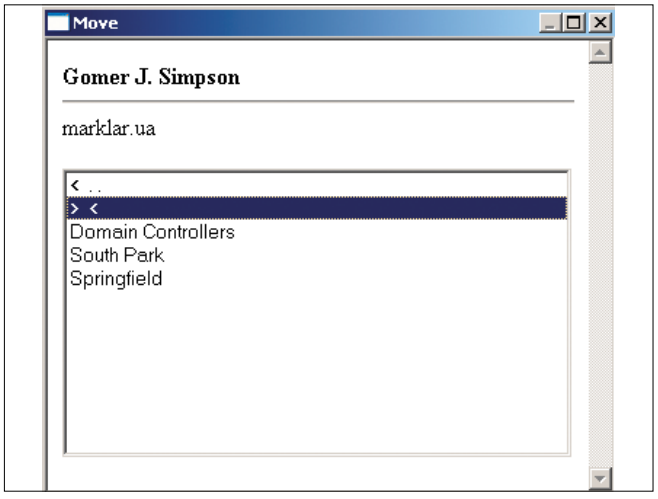
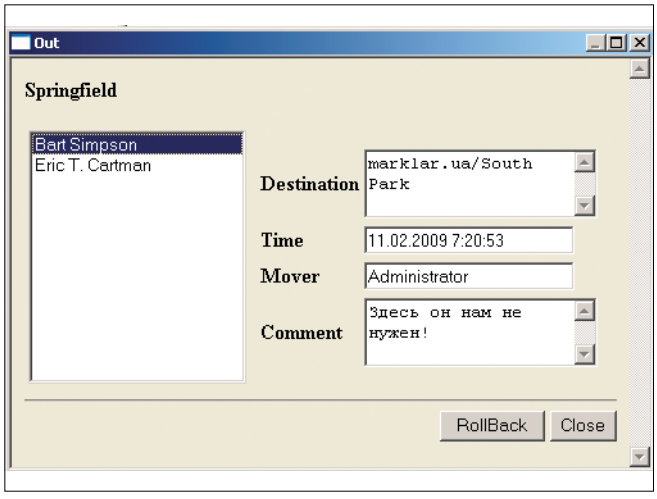


Рисунок 2. Приложение для отмены перевода пользователя



```
function extractArg
  dim re, aMatch, q
  set re = new Regexp
  re.pattern = _
    replace("'.+' '?([^']+)'? .+", "'", chr(34))
  re.ignoreCase = True
  set aMatch = re.execute(app.commandline)
  if aMatch.count > 0 then
    if  aMatch(0).subMatches.count > 0 then
```

Извлекаем захваченную часть регулярного выражения, которую я взял в круглые скобки. Поскольку захватывалась только одна часть, то и извлекаем ее как нулевой элемент массива совпадений (aMatch) и вложенных совпадений (subMatches).

```
      extractArg = aMatch(0).subMatches(0)
```

Путь к объекту передается сценарию в несколько непривычном виде: «LDAP://main.marklar.ua/cn=Gomer….». Обратите внимание на участок между названием протокола и начало отличительного имени. Это имя компьютера, на котором находится пользователь (один из контроллеров домена). Эту часть удаляем с помощью регулярного выражения:

```
      re.pattern = "\/\/[^\/]*/"
```

Здесь две наклонные, и текст за ними вплоть до следующей наклонной линии заменяется двумя прямыми слешами. То есть в результате мы получаем более привычный путь к объекту: «LDAP://cn=Gomer….». В таком виде результат и возвращается из функции.

```
      extractArg = re.replace(extractArg, "//")
    end if
  end if
end function
```

Основная подпрограмма приложения – заполнение списка организационными единицами текущего контейнера. Он должен обновляться каждый раз при смене родителя. Также список должен содержать два особых элемента: для выхода на уровень выше (< ..) и начала перемещения (> <).

```
sub populateList
```

Вначале очищаем список, установив количество его элементов равным нулю. Далее создаем два верхних элемента выхода на родителя и начала перемещения. Для этого используется функция newOption. Ей передается два параметра: видимая надпись элемента и путь к нему (т.е. путь к контейнеру). Для начала перемещения в качестве пути задается пустая строка.

```
  startMove.ouList.options.length = 0
  startMove.ouList.add newOption("<  . .", backPath)
  startMove.ouList.add newOption(">  <", "")
  dim curOU, subOU
```

В глобальной переменной curPath хранится путь к текущему контейнеру, содержимое которого и требуется отобразить в списке.

```
  set curOU = getObject(curPath)
  for each subOU in curOU
```

Перебираем все организационные единицы текущего контейнера и добавляем их в список с помощью той же функции newOption.

```
    if subOU.class = "organizationalUnit" then ↵
      startMove.ouList.add newOption( ↵
      subOU.ou, subOu.ADSPath)
    end if
  next
```

Для удобства пользователей выделим контейнер, из которого мы пришли в текущий. Путь к нему хранится в переменной prevPath. Такой подход используется в большинстве файловых менеджеров: при выходе из папки на уровень выше она становится выделенной, чтобы можно было вернуться назад, нажав на <Enter>.

```
  dim selectIt, opt
  selectIt = 0
  for each opt in startMove.ouList.options
    if opt.value = prevPath then selectIt = opt.index
  next
```

Для выделения заданного элемента списка используется свойство selectedIndex.

```
  startMove.ouList.selectedIndex = selectIt
end sub
```

Вот функция создания нового элемента списка. Сначала создается элемент документа типа option, затем инициализируются его поля: text (надпись на элементе), value (значение элемента, на экране оно не обращается, но может быть получено с помощью свойства списка value).

Листинг 4. Создание нового элемента списка

```
function newOption(oText, oValue)
  set newOption = document.createElement("option")
  newOption.value = oValue
  newOption.text = oText
end function
```

Перейдем к функции, которая назначена на событие двойного щелчка мышкой по элементу списка. Если значение выбранного элемента – пустая строка, начинается перемещение пользователя, в противном случае происходит переход в выбранный контейнер.

Листинг 5. Обработка события выбора элемента списка

```
function itemSelected()
  dim newPath
  newPath = startMove.ouList.value
  if newPath <> "" then
    setCurPath(newPath)
  else
    moveUserTo
  end if
end function
```

Сначала рассмотрим переход в контейнер. Процедура устанавливает переданный ей путь в качестве текущего, запоминает предыдущее положение, если оно существует, отображает новый путь в удобочитаемом виде и обновляет содержимое списка.

Листинг 6. Переход в заданную организационную единицу

```
sub setCurPath(path)
  if not isEmpty(curPath) then
    prevPath = curPath
  else
    prevPath = path
  end if
```

```
  curPathShow.innerhtml = engine.ADSPath2Readable(path)
  curPath = path
  backPath = engine.getParent(path)
  populateList
end sub
```

Для обработки нажатия клавиш используются те же подпрограммы. При нажатии <Enter> (код клавиши 13) вызывается та же процедура, что и при двойном щелчке мышью. В ответ на нажатие клавиши <Backspace> происходит установка родительского каталога в качестве текущего.

Листинг 7. Обработка нажатий клавиш

```
function onKey()
  select case window.event.keyCode
    case 13: itemSelected
    case 8:  setCurPath(backPath)
  end select
end function
```

Теперь посмотрим на начало перемещения пользователя.

```
function moveUserTo()
  dim comment, ans
```

Сначала нужно запросить у менеджера подтверждение на начало операции (диалоговое окно, содержащее параметры перемещения и кнопки OK и Cancel). Если положительного ответа не получено, функция завершает работу.

```
  ans = msgbox("Moving " & user.cn & " to " & ↵
    vbLF & engine.ADSPath2Readable(curPath), ↵
    vbOKCancel + vbQuestion)
  if ans = vbCancel then exit function
```

Если менеджер подтвердил начало операции, появляется диалоговое окно с просьбой ввести комментарий к перемещению. Затем вызывается метод move основного класса надстройки, который выполняет все необходимые действия.

```
  comment = inputBox("Post your comment here")
  msgbox engine.move(user.ADSPath, curPath, comment)
```

В конце приложение закрывается, поскольку вызов этой функции – единственная его цель.

```
  window.close
end function
```

Отмена перемещения

Следующее приложение – отмена операции перемещения. Менеджер, поставив пользователя в очередь, должен иметь возможность его вернуть. Для этого потребуется следующее приложение (см. рис. 2).

Слева отображается список исходящих пользователей. То есть тех, которые были перемещены из этого подразделения, но еще не приняты в другие. Все эти операции можно отменить с помощью кнопки RollBack. При выборе конкретного пользователя появляется возможность посмотреть некоторые параметры перемещения (пункт назначения, время операции, кто перемещал и комментарий).

Рассмотрим реализацию основных функций приложения. В правой части окна расположен исходящий список пользователей. Рассмотрим подпрограмму его заполнения.

```
sub populateList
```

Сначала список очищается. Затем для текущего контейнера устанавливается фильтр для выбора только комнат ожидания (класс userMoveWaitingRoom).

```
  viewOut.outcomingList.options.length = 0
  ou.filter = Array("userMoveWaitingRoom")
  dim room, roomFound
  roomFound = false
  for each room in ou
```

Получив указатель на первую (и единственную) комнату ожидания текущего контейнера, выходим из списка, установив флаг существования группы в значение «истина».

```
    roomFound = true
    exit for
  next
```

Если у текущей организационной единицы нет комнаты ожидания, процедура завершает работу. В этом случае исходящих пользователей также не существует, и список остается пустым.

Рисунок 3. Управление очередью входящих пользователей

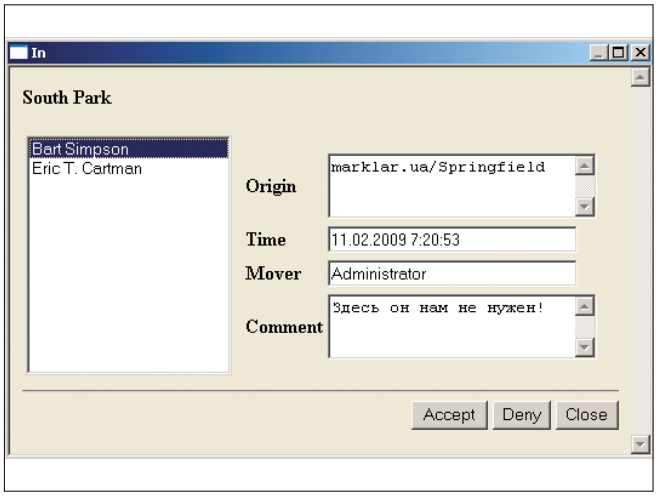
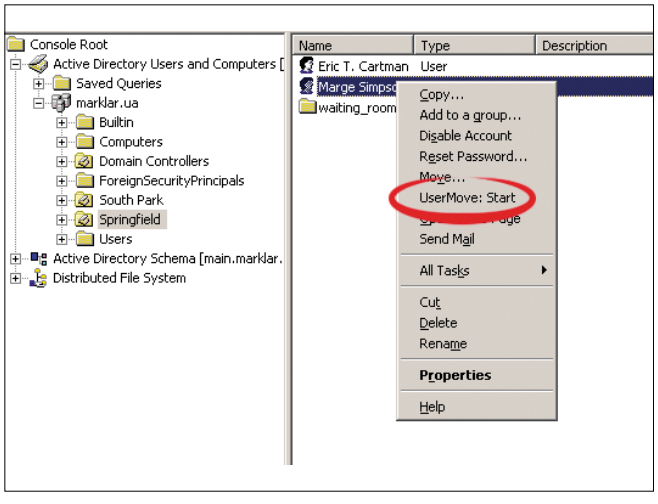


Рисунок 4. Дополнительный пункт меню для объектов пользователей



```
  if not roomFound then exit sub
```

Затем выбираем из комнаты ожидания ссылки на отправленных пользователей. Тип userMoveChairLink был специально введен в надстройку для упрощения и ускорения выполнения этой операции. Благодаря этому она сводится к простому перебору элементов одного контейнера.

```
  room.filter = Array("userMoveChairLink")
  dim li, user, commanded, cmd
  for each li in room
    set user = getObject(li.userMoveLink)
    ou.filter = Array("UserMoveCommand")
```

Затем просматриваем текущую организационную единицу на предмет наличия в ней невыполненных команд для текущего исходящего пользователя (их существование возможно, поскольку команды выполняются не мгновенно, их появление проверяется раз в 5 секунд, но может быть установлен и больший период).

```
    commanded = false
    for each cmd in ou
      if cmd.userMoveTarget = user.ADSPath then
        commanded = true
        exit for
      end if
    next
```

Если для пользователя найдена невыполненная команда, то в список исходящих он уже не попадает. Нельзя отменить перемещение пользователя, для которого в очереди ожидания находится невыполненная команда. В противном случае произойдет сбой при попытке ее выполнения позже.

```
    if not commanded then
      viewOut.outcomingList.add newOption( ↵
        user.cn, li.userMoveLink)
    end if
  next
```

Теперь список заполнен, но ни один его элемент пока не выбран, поэтому поля с дополнительной информацией очищаем.

```
  viewOut.iDest.value = ""
  viewOut.iTime.value = ""
  viewOut.iMover.value = ""
  viewOut.iComment.value = ""
end sub
```

Заполнение списка происходит из функции инициализации приложения. Здесь все практически то же, что и для предыдущего приложения: создается экземпляр главного класса надстройки, устанавливается фокус ввода на список, инициализируется текущий каталог.

Листинг 8. Инициализация приложения отмены перемещения

```
function window_onLoad()
  set engine = createObject("UserMove.Engine")
  viewOut.outcomingList.focus
  set ou = getObject(extractArg)
  ouName.innerhtml = "<b>" & ou.ou & "</b>"
  populateList
end function
```

При выборе элемента списка поля справа от него должны отобразить дополнительную информацию.

```
function selChanged()
 dim chair, s, mover, moverCN
```

Необходимые данные находятся в объекте стула ожидания, поэтому к нему и подключаемся. Стул является родительским контейнером по отношению к перемещаемому пользователю. Практически все свойства записываются в текстовые поля напрямую.

```
  set chair = getObject( ↵
    engine.getParent(viewOut.outcomingList.value))
  viewOut.iDest.value = engine.ADSPath2Readable( ↵
    engine.getParent(chair.parent))
  viewOut.iTime.value = ↵
   engine.fromUTC(CDate(chair.userMoveWhen))
  viewOut.iComment.value = chair.userMoveComment
```

Объект инициатора перемещения может уже не существовать в системе. Это не должно привести к аварийному завершению подпрограммы, поэтому временно отключаем завершение при ошибке.

```
  on error resume next
```

Затем делаем попытку подключиться к объекту инициатора.

```
  set mover = getObject(chair.userMoveWho)
```

Если значение переменной err не равно нулю, операцию выполнить не удалось, и в поле отправителя помещается текст «Не найден» (Not found).

Затем опять включаем стандартную реакцию системы на ошибки:

```
  on error goto 0
  viewOut.iMover.value = moverCN
  end function
```

И, наконец, рассмотрим процедуру отмены перемещения. Она вызывается при нажатии на кнопку RollBack.

```
function doRollBack()
dim userPath, ans
```

Вначале получаем путь к выбранному в списке перемещаемому пользователю. Если ничего не выбрано, выводится соответствующее сообщение, и процедура завершает работу.

```
userPath = viewOut.outcomingList.value
if userPath = "" then
  MsgBox "Nothing is selected"
Else
```

Если что-то выбрано, задается уточняющий вопрос менеджеру, при положительном ответе на который и начинается отмена. Отмена перемещения реализована в методе rollback основного класса надстройки.

```
  ans = msgbox("Do you want to rollback the transfer?", ↵
    vbYesNo + vbQuestion)
  if ans = vbNo then exit function
  MsgBox engine.rollback(userPath)
end if
```

В конце заново заполняем список с исходящими пользователями. Отмененной операции там уже быть не должно.

```
populateList
end function
```

Приложение для менеджера целевого отдела

Менеджер по персоналу целевого отдела должен иметь возможность просмотра очереди входящих пользователей, подтверждения или отказа в перемещении. Приложение выглядит следующим образом (см. рис. 3).

Пользовательский интерфейс здесь практически аналогичен предыдущему, поэтому его html-код приводить не буду. Подпрограмма вывода дополнительной информации о выбранном элементе в текстовые поля справа рассмотрена не будет по той же причине. Заполняется список следующим образом.

```
sub populateList
```

Сначала подключаемся к комнате ожидания (переменная room) текущей организационной единицы. Делается это так же, как в функции populateList предыдущего приложения, поэтому полный листинг повторно приводиться не будет.

```
  room.filter = Array("UserMoveChair")
  dim ch, user, cmd, commanded
```

Затем из каждого стула ожидания получаем ссылку на объект пользователя (переменная user).

```
  for each ch in room
    for each user in ch
      exit for
    next
```

Дальнейшая реализация аналогична программе из предыдущего приложения. Нужно проверить, нет ли ожидающей команды для текущего пользователя, и, если нет, добавить его в список.

```
end sub
```

Чтобы согласиться на перевод пользователя в свое подразделение, менеджер нажимает кнопку Accept. Вызывается обработчик:

Листинг 9. Функция подтверждения перемещения выбранного пользователя

```
function doAccept()
dim userPath, ans
userPath = viewOut.incomingList.value
if userPath = "" then
  MsgBox "Nothing is selected"
else
  ans = msgbox("Do you want to accept the transfer?", ↵
    vbYesNo + vbQuestion)
  if ans = vbNo then exit function
  MsgBox engine.accept(userPath)
end if
populateList
end function
```

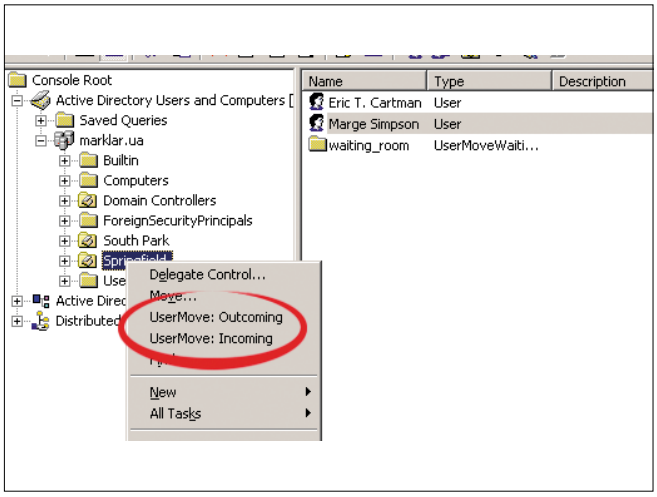
Здесь проверяется, выбран ли какой-то элемент списка, задается уточняющий вопрос. Подтверждение осуществляется вызовом метода accept основного класса надстройки. Функция отказа от перевода полностью аналогична, за исключением того, что нужно вызвать метод deny класса UserMove.Engine.

Что в итоге?

Итак, была разработана надстройка, позволяющая разбить процесс перемещения пользователя с одной организационной единицы в другую на два этапа, каждый из которых можно делегировать менеджеру в конкретном подразделении. Надстройка массивна, но в результате вся работа с ней заключается в использовании трех элементов контекстного меню: UserMove: Incoming и UserMove: Outcoming для организационных единиц и UserMove: Start для объектов пользователей (см. рис. 4 и 5).

В результате отпадает необходимость в использовании администратора с правами в обеих организационных единицах для перемещения профилей пользователей, что снижает общее количество сотрудников с «лишними» правами. EOF

Рисунок 5. Дополнительные элементы меню для организационных единиц



1. Don Jones, Jefferey Hicks «Advanced VBScript for Microsoft Windows Administrators». – Washington: Microsoft Press, 2006. – 537 p.
2. Чарли Рассел, Шарон Кроуфорд, Джейсон Джеренд. «Windows server 2003 +SP1 и R2. Справочник администратора». – М.: Издательство «ЭКОМ», 2006. – 1424 с.

2009

www.infosecuritymoscow.com

infosecurity RUSSIA

6-я международная специализированная выставка-конференция по информационной безопасности

29 сентября – 1 октября 2009

МОСКВА, Экспоцентр на Красной Пресне
Павильон №7

Одновременно
на одной площадке
с Infosecurity Russia:

STORAGE EXPO

DOCUMATION

РАЗДЕЛЫ ВЫСТАВКИ

- Антиспам
- Антивирусы
- Безопасность приложений
- Биометрические системы
- Непрерывность бизнеса/восстановление бизнеса после катастроф
- Соответствие требованиям регуляторов и стандартам
- Системы мониторинга и фильтрации контента
- E-mail безопасность / Безопасность средств оперативной пересылки сообщений или Безопасность мгновенного обмена сообщениями (систем типа ICQ)
- Шифрование, PKI (инфраструктура открытых ключей), Цифровые сертификаты
- Межсетевые экраны (брандмауэры)
- Управление идентификацией и доступом
- Безопасность Интернет/сетевая безопасность
- Выявление и предупреждение вторжений
- Расследование компьютерных инцидентов
- Техническая поддержка/системы helpdesk
- Законодательство и стандарты/BS7799/Сертификация
- Сертификационные центры
- Управление внесением исправлений
- Тестирование безопасности системы путем имитации атак / Оценка риска и уязвимости
- Физическая безопасность
- Удаленный доступ
- Безопасность хранения данных
- Политика безопасности
- Маркеры доступа
- Обучение и повышение осведомленности в области безопасности
- Безопасность Веб-сервисов
- Система «Доступ за один шаг» (Single Sign-On)
- Смарт-карты
- Системы унифицированного управления защитой от угроз
- Безопасность IP телефонии
- VPN (виртуальные частные сети)
- Безопасность мобильных/беспроводных систем

ВЫСТАВОЧНОЕ ОБЪЕДИНЕНИЕ РЕСТЭК™ Reed Exhibitions®

Дирекция выставки:
Санкт-Петербург, Петрозаводская ул., д.12
Тел.: +7 (812) 320-8098, факс: +7 (812) 320-8090, E-mail: itcom@restec.ru

Визитка

ВАСИЛИЙ ГУСЕВ, системный администратор ЗАО «УК «ЕвразФинанс», обладает статусами Microsoft MVP: PowerShell, MCSE, MCITP

Осваиваем нововведения
языка сценариев Windows PowerShell 2.0

Приближается долгожданное событие — выход Windows PowerShell 2.0. Что принесёт изменение цифры в версии молодого языка сценариев?

С одной стороны, синтаксис языка практически не претерпел изменений, переучиваться не придётся – сценарии, написанные для PowerShell 1.0, будут прекрасно работать и в PowerShell 2.0. С другой стороны, приятных нововведений так много, что я сразу предупреждаю – рассказать обо всех в одной статье невозможно. Так что я сделаю лишь краткий обзор нового функционала.

Компонент системы

PowerShell 2.0 сначала появится в составе операционных систем Windows 7 и Windows Server 2008 R2. Это значительный шаг для молодого языка сценариев, ведь теперь он является неотъемлемым компонентом системы. Да что там говорить, в Windows Server 2008 R2 значок PowerShell вынесен на панель задач сразу после Server Manager! И это не просто из-за того, что Microsoft хочет продвинуть новую технологию – немало функционала в новых системах основано на PowerShell. Взамен же PowerShell предоставляет богатые возможности по управлению различными компонентами этих систем. Кроме того, теперь вы сможете легко использовать PowerShell в групповых политиках, будучи уверены в том, что он установлен на системе, и сценарий будет выполнен.

Отдельная ситуация с Server Core. Несмотря на то что PowerShell теперь официально поддерживается в этом режиме установки системы, по умолчанию он не установлен, и это связано с самой идеологией Server Core – минимум всего.

Но несмотря на это, установить PowerShell в Server Core несложно, за пару минут, одной командой:

```
start /w ocsetup MicrosoftWindowsPowerShell
```

Удалённое выполнение команд (Remoting)

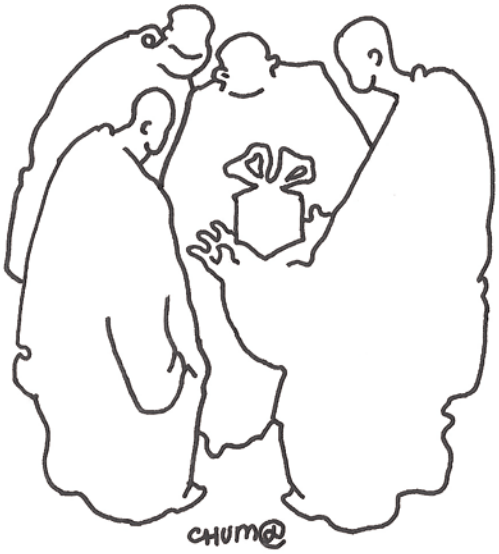
Одна из самых ожидаемых возможностей Windows PowerShell 2.0 – это, конечно, Remoting. Стоит, однако, заметить, что в это понятие авторы PowerShell вкладывают гораздо больший смысл, нежели «запустить команду на другом компьютере». PowerShell Remoting позволит вам не просто выполнять команды на одном или нескольких удалённых компьютерах, но и отслеживать их выполнение и получать результаты их работы. Причем это обычно для PowerShell и необычно для остальных – результаты работы по сети будут передаваться не в виде простого текста, а в виде объектов. Разумеется, многие объекты потеряют некоторые качества в отрыве от систем, на которых они были созданы, – все их методы будут удалены. Но свойства останутся (и даже будут добавлены новые, такие как PSComputerName, указывающий, с какого компьютера был получен объект), и с ними можно будет работать, как с остальными объектами PowerShell.

Гибкость Remoting тоже не разочарует. Можно как выполнять отдельные команды, так и установить постоянную сессию или сессии на несколько компьютеров, и выполнять в них серии команд. Это позволит, во-первых, сэкономить ресурсы за счет того, что не будет создаваться и уничтожаться отдельное окружение PowerShell для каждой команды, а во-вторых, команды из последовательности будут иметь доступ к переменным и другим объектам, созданным в этой сессии предыдущими командами.

Если вы захотите использовать интерактивные сессии, как в Telnet, SSH или PSExec, то возможно и это с помощью командлета Enter-PSSession (см. рис. 1, 2).

Разумеется, Remoting отключён на системах по умолчанию. Хоть это и прекрасное средство управления, безопасность остаётся превыше всего. Впрочем, включить его несложно, достаточно выполнить командлет Enable-PSRemoting, который спросит подтверждение (от которого можно избавиться с помощью ключа Force) и затем выполнит все необходимые действия для предоставления удалённого доступа для учетных записей, являющихся администраторами компьютера.

Этот метод хорош, когда вам надо включить Remoting на одном или нескольких компьютерах, но что делать, если их десятки, сотни, тысячи? Всего лишь несколько дополнительных манипуляций. Все действия, что производит командлет Enable-PSRemoting, можно сделать с помощью групповой политики.



Во-первых, надо включить настройку Computer Configuration/Administrative Templates/Windows Components/Windows Remote Management (WinRM)/WinRM Service/Allow automatic configuration of listeners. В ней же можно задать диапазоны адресов, с которых разрешены подключения.

Во-вторых, нужно создать необходимые исключения в брандмауэре Windows.

Ну и наконец, установить для службы Windows Remote Management (WS-Management) автоматический режим запуска.

Так как PowerShell Remoting использует технологию WinRM (реализацию стандарта WS-Management), он наследует множество её преимуществ. Например, возможность подключаться к системам даже через прокси-серверы. Или выдающаяся безопасность – все соединения Remoting шифруются в обязательном порядке, с использованием SSL. Разумеется, шифруются и передаваемые учетные данные. Кстати, поддерживается несколько механизмов аутентификации – Kerberos, NTLM, Digest и Basic. Разумеется, самым безопасным является Kerberos и по умолчанию, при возможности используется именно он.

По умолчанию подключение можно установить, лишь используя учетную запись, обладающую правами администратора на удаленном компьютере. Но вы вполне можете изменить эти разрешения или даже создать отдельные конфигурации подключений для разных групп пользователей. У разных конфигураций – разные ограничения. Лимитирование объема передаваемых данных или времени выполнения команд позволит в некоторой степени защититься от пожирания ресурсов сервера одним чересчур активным пользователем. Но главное это, конечно, возможность ограничить список разрешенных команд, их параметров и конструкций языка. То есть вы можете разрешить определенной группе пользователей выполнять на сервере лишь командлеты Get-* для получения информации, но внести в систему изменения они не смогут. Другой группе можно дать право исполнения командлета Get-Process с параметром -Id, а все остальные параметры и команды будут недоступны.

За другими подробностями можно обратиться во встроенную справку, выполнив команду:

```
help about_remoting
```

Фоновые работы (Jobs)

Не менее важно и другое нововведение – фоновые работы. Те, кто работал с UNIX-подобными системами, наверняка знают, что это такое, для остальных же поясню. Это команды, которые выполняются в отдельной сессии, параллельно основной. То есть вы можете запустить команду, требующую много времени, в качестве фоновой работы, и продолжать заниматься другими делами. Можно просматривать статус выполнения работ и при необходимости получать их результаты.

В PowerShell 2.0 это реализуется с помощью командлетов с существительным Job, которое позволяет:

Start-Job – запустить новую работу.

Get-Job – получить список работ текущей сессии и посмотреть их статус.

Receive-Job – получить результаты выполнения команды.

Стоит обратить внимание, что после того как Receive-Job передаст вам данные, она тут же уберёт их из стека вывода работы, и, вызвав командлет второй раз, вы получите лишь новые данные. Чтобы этого не происходило, используйте ключ Keep.

Впрочем, я не буду рассказывать о действии каждого командлета *-Job, уверен, вы прекрасно справитесь сами с помощью встроенной справки. Лучше упомяну о другом методе запуска фоновых работ, параметре -AsJob. Он присутствует у многих разных команд. Например, Invoke-Command -AsJob позволит вам запустить продолжительную команду на нескольких компьютерах в виде работ, а затем отслеживать процесс их выполнения и результаты с помощью командлетов *-Job. Get-WmiObject -AsJob делает примерно то же самое, но для WMI-запросов. Например, эта команда запрашивает значение Win32_ComputerSystem для всех компьютеров из списка Computers.txt, но не более чем на двух одновременно.

```
PS C:\> $Comps = Get-Content Computers.txt
PS C:\> $Job = Get-WmiObject Win32_ComputerSystem `
-Computer $Comps -AsJob -ThrottleLimit 2
PS C:\> $job.ChildJobs
Id Name State     HasMoreData Location  Command
-- ---- -----     ----------- --------  -------
2  Job2 Completed True        comp1
3  Job3 Failed    False       comp2
4  Job4 Running   False       comp3
5  Job5 Running   False       comp4
```

Результаты, разумеется, можно получить командлетом Receive-Job. Раздел справки, посвященный фоновым работам, – About_Jobs.

ISE

Хоть появление графической оболочки и среды разработки для PowerShell и не является прорывом (уже давно существует немало решений от сторонних производителей), тем не менее ISE всё-таки принесёт немало полезных нововведений.

Во-первых, это полноценный интерпретатор PowerShell, подобный самому PowerShell.exe, но в отличие от него не использующий консольную подсистему Windows, которая не изменялась уже много лет. Это даёт прекрасную возможность начать всё сначала и не повторять ошибок прошлого. PowerShell ISE не испытывает вообще никаких проблем с отображением Unicode и любых локальных символов. Текст можно удобно выделять, копировать и вставлять, как в любом другом приложении Windows. Разумеется, нет никаких сложностей с изменением размеров окна, это делается лишь перетаскиванием края окна, без необходимости залезать в какие-либо настройки. Также легко можно поменять размер шрифта.

Кажущаяся обычной подсветка синтаксиса всё же отличается от аналогичной в других продуктах тем, что для разбора текста сценариев и команд используется оригинальный механизм PowerShell, а не сложные правила, пытающиеся повторить его функционал. Теперь вы можете быть уверены – если редактор не подсвечивает какой-то участок или подсвечивает его не так, как вы хотите, значит, где-то вкралась ошибка.

Разумеется, работает и автоматическое дополнение команд, параметров, переменных и свойств объектов, так же как и в обычном PowerShell.exe. Причем для этого также используется обычная функция TabExpansion, а следовательно, стандартный функционал можно расширить.

Вполне естественным для такого редактора выглядит и наличие прекрасного отладчика с возможностью установки точек останова, просмотра содержимого переменных в процессе выполнения и всего остального, что может пригодиться для поиска ошибок при выполнении сценария.

Кроме обычных, для многих текстовых редакторов закладок, в которых можно открыть разные текстовые файлы, в PowerShell ISE можно еще открывать отдельные сессии PowerShell, не соприкасающиеся друг с другом. А благодаря технологии Remoting некоторые из этих сессий могут выполняться даже на других компьютерах!

Но главный момент для графической среды разработки – это, конечно, удобство. В PowerShell ISE вы можете выбрать расположение панелей редактора, командной строки и области вывода результатов. Можно даже скрыть всё, кроме редактора, и полностью погрузиться в процесс разработки своего сценария (см. рис. 3).

Если бы этим редактор ограничивался, он бы не смог стать хорошей альтернативой конкурентам. Но, к счастью, ISE обладает прекрасными возможностями для расширения своего функционала... с помощью сценариев PowerShell! С помощью специальной переменной $PsIse можно получить доступ к управлению интерфейсом PowerShell ISE, добавить свои пункты меню, обрабатывать текст из панелей редактора и командной строки и так далее. Я уверен, что вскоре после релиза появится множество пользовательских сценариев, приумножающих функционал ISE.

Соответствующий раздел справки называется about_Windows_PowerShell_ISE.

Advanced Functions

Те, кто серьезно занимался написанием своих сценариев или создавал командлеты в Windows PowerShell 1.0, навер-

Рисунок 1. Использование интерактивной сессии PowerShell Remoting

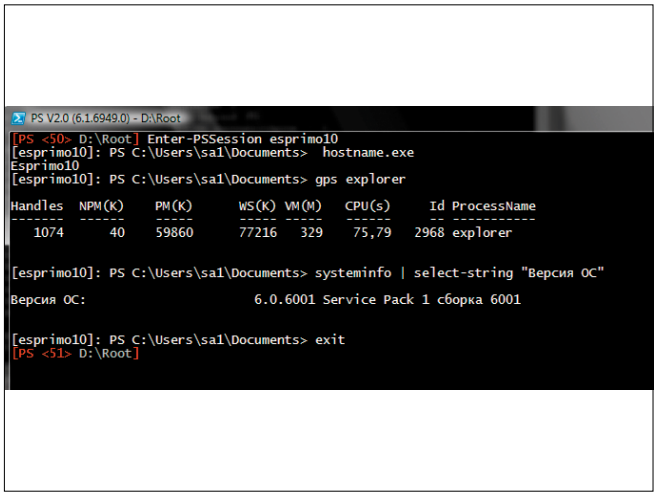
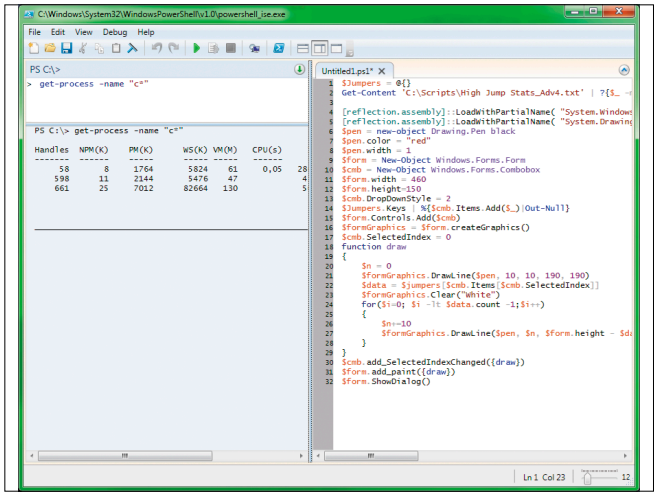


Рисунок 2. PowerShell Integrated Scripting Environment (ISE)



няка обратили внимание на то, что у последних есть некоторые достаточно большие преимущества. Так, например, в сценарии .ps1 вы не сможете использовать несколько различных наборов параметров, создавать для параметров псевдонимы и указывать другие атрибуты, такие как ValueFromPipeline и ValidateSet. Даже использование специальных параметров -WhatIf и -Confirm было невозможным в обычных файлах сценариев, лишь в командлетах, написанных на C# или VB.Net.

Что ж, теперь все будут находиться в равных условиях. Командлеты, написанные непосредственно на PowerShell, называются Advanced Functions, их синтаксис лишь немного отличается от обычных функций, но зато даёт гораздо большие возможности для создания качественных сценариев для долговременного использования. Подробности в about_functions_advanced.

Встроенный отладчик

По мне, и в PowerShell 1.0 была прекрасная возможность отладки сценариев из командной строки, которой могли позавидовать многие языки сценариев. Достаточно было добавить в текст сценария строку $Host.EnterNestedPrompt(), и при её достижении сценарий приостанавливался, предоставляя вложенную консоль, из которой можно было посмотреть и даже изменить состояние переменных, попробовать выполнить команду вручную и т.п. Для выхода достаточно было набрать Exit.

Но в 2.0 консольный отладчик вышел на совершенно новый уровень. Теперь можно создавать точки останова, которые будут срабатывать не только на некоторых строках, но и по достижении определенного столбца, команды или файла сценариев или переменной. Причем для последних можно задать, при каких действиях над переменной нужно срабатывать: чтение значения из переменной, изменение значения или и то и другое.

Есть возможность создать точки останова, которые вместо прерывания выполнения, будут выполнять любое указанное вами действие.

При срабатывании точки останова консоль переходит в специальный режим отладки, который можно отличить по префиксу [DBG]: в приглашении командной строки. Тут доступны специфичные для данного режима команды: stepInto, stepOver, stepOut, continue, list и некоторые другие, которые вы можете посмотреть, введя в командную строку вопросительный знак и нажав <Enter>.

Управляют точками останова с помощью командлетов *-PSBreakpoint. Для переключения различных опций, относящихся к режиму отладки, служит командлет Set-PSDebug. Кроме того, выполнив этот командлет с ключом -Strict, вы включите Strict Mode, специальный режим, аналогичный Option Explicit в Visual Basic.

Еще много интересного об отладке вы сможете прочитать в разделе встроенной справки about_Debuggers.

Новые командлеты

В PowerShell 2.0 добавилось множество новых командлетов. Я кратко расскажу о наиболее интересных.

Командлет Add-Type пригодится для использования в сценарии кода других .Net-языков. Это бывает очень полезно, если какая-то операция в сценарии должна выполняться максимально быстро или если вдруг вам понадобится какая-то из возможностей этих языков, которая недоступна в PowerShell. Например, Win32 API. Это низкоуровневые функции для управления различными аспектами системы, зачастую с их помощью можно сделать вещи, недоступные иными методами.

Вот простой пример вызова функции Win32API ShowWindowAsync:

```
$type = Add-Type @"
[DllImport("user32.dll")]
public static extern bool ShowWindowAsync( ↵
       IntPtr hWnd, int nCmdShow);
"@ -name "Win32ShowWindowAsync" -namespace ↵
       Win32Functions -passthru

#Скрывает окно PowerShell
$type::ShowWindowAsync(( ↵
       get-process -id $pid).MainWindowHandle,2)

#Снова показывает окно
$type::ShowWindowAsync(( ↵
       get-process -id $pid).MainWindowHandle,10)
```

Определения других функций Win32 API вы можете посмотреть на сайте http://www.pinvoke.net.

Команда разработчиков PowerShell, видимо, решила прибрать к рукам большую часть функционала утилиты net.exe, создав соответствующие командлеты, и это здорово! Просто посмотрите на названия командлетов, уверен, что мне не придётся объяснять их назначение:

- Add-Computer;
- Remove-Computer;
- Reset-ComputerMachinePassword;
- Test-ComputerSecureChannel.

Еще больше команд появилось для работы с журналами событий Windows:

- Clear-EventLog;
- Limit-EventLog;
- New-EventLog;
- Remove-EventLog;
- Show-EventLog;
- Write-EventLog.

С их помощью легко производить любые операции с журналами, например, создать для своего сценария журнал событий, установить его параметры и записывать в него отладочную информацию. Согласитесь, ведь текстовые журналы мы использовали лишь из-за того, что это было проще. Теперь также просто использовать системный функционал, предназначенный специально для этого. Журналы событий можно легко фильтровать, передавать на другой компьютер с помощью подписок или отслеживать, используя решения, подобные SC Operations Manager.

Отдельно стоит упомянуть командлет Get-WinEvent. Он работает только на системах Windows Vista, Windows Server 2008 и выше из-за того, что использует новые возможности механизма журналов событий. Кроме обычного извлечения событий, соответствующих вашим критериям из журнала, он может, например, показать список зарегистрированных в системе поставщиков событий и события, которые они могут писать:

```
$Provider = Get-WinEvent -ListProvider *update*
$Provider.Events | Format-Table Id, description -AutoSize
```

Чтобы увидеть другие примеры применения этого командлета, рекомендую вызвать команду:

```
Get-Help Get-WinEvent -Examples
```

Их там весьма немало.

Командлеты для работы с журналами событий легко спутать с другим набором команд. Эти предназначены для привязки своих действий к событиям, вызываемым другими объектами .Net или WMI:

- Register-EngineEvent;
- Register-ObjectEvent;
- Register-WmiEvent;
- Get-Event;
- New-Event;
- Remove-Event;
- Unregister-Event;
- Wait-Event;
- Get-EventSubscriber.

С их помощью можно, например, сделать, чтобы в созданной вами форме при нажатии на кнопку выполнялась ваша команда. Или назначить выполнение своего сценария на событие создания определенного файла в определенной папке, тогда вам не придется постоянно проверять список файлов – система сама оповестит сценарий при изменениях. Или вызывать код при завершении/старте процесса Windows.

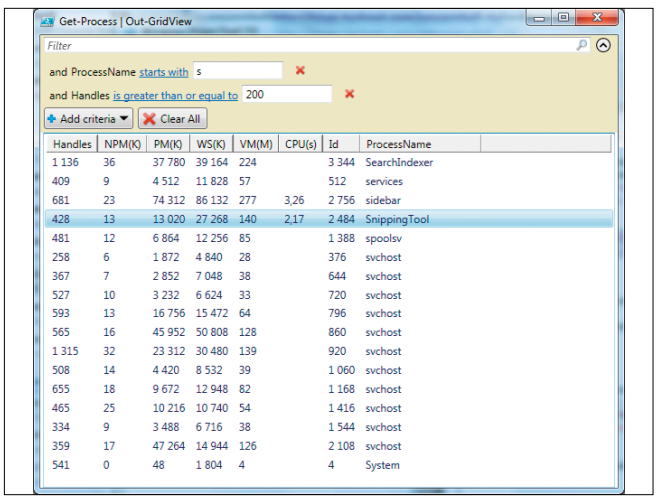
Get-Counter даст возможность легко и непринуждённо получать данные различных счетчиков производительности Windows. Ну и как можно догадаться, Export-Counter и Import-Counter позволяют экспортировать показания этих счетчиков и импортировать их в другую сессию для анализа.

Пусть в PowerShell 1.0 и так было несложно получить произвольное число или выбрать уникальное значение из группы, в 2.0 это стало еще проще и удобнее благодаря командлетам Get-Random и Get-Unique.

Воспользоваться всеми благами новой технологии вебслужб позволит командлет New-WebServiceProxy, который может подключаться к соответствующим сервисам и управлять ими или получать данные.

Out-GridView – командлет, который выводит возможности PowerShell за пределы командной строки. Он может показать данные, полученные по конвейеру в виде красивой и удобной таблицы, в которой работает мгновенный поиск, и можно даже фильтровать показанные результаты с помощью графического интерфейса для создания правил отбора.

Рисунок 3. Результат работы командлета Out-GridView



Функционал командлетов Send-MailMessage и Test-Connection вряд ли кого-то удивит. Первый позволяет отправлять почтовые сообщения по протоколу SMTP, а второй является аналогом Ping для PowerShell с массой новых возможностей, таких как многопоточность или выполнение пинга с другого компьютера.

Подробно обо всех этих командах можно прочитать во встроенной справке, вызвав ее следующей командой:

```
Help ИмяКомандлета
```

Чтобы увидеть примеры использования, добавьте ключ Examples, а для просмотра максимально полной версии справки с описанием всех параметров и примерами – ключ Full.

Новые параметры у старых команд

В процессе добавления новых команд не были забыты и старые друзья. Хотя основной функционал старых командлетов почти не изменялся для сохранения совместимости, ко многим командлетам были добавлены новые параметры, расширяющие их возможности.

Import-Csv и Export-Csv получили крайне необходимые в российских условиях параметры -Delimiter и -UseCulture, позволяющие задать используемый разделитель символов.

Командлет Get-Help, если не находит команды или раздела справки соответствующего переданному аргументу, выполняет поиск упоминаний этого аргумента по всем разделам. Попробуйте выполнить, например, команду:

```
Get-Help "regular expression"
```

и вы увидите все разделы справки, где упоминаются регулярные выражения.

Новый параметр командлета Select-String -Context позволяет получить не только ту строку, в которой было найдено вхождение искомого текста, но и несколько предыдущих и/или последующих строк. Например, следующая команда выведет все строки, в которых встречается слово Error, одну предыдущую строку и две последующие:

```
Get-Content Log.txt | select-string "Error" -Context 1,2
```

Другие улучшения языка

Как я уже сказал, в статье не хватит места рассказать обо всех нововведениях, и, разумеется, я не упомянул о многих новых командах и улучшениях, но некоторые вещи заслуживают хотя бы пары слов.

Так, теперь вы можете использовать в своих сценариях Windows Presentation Foundation, технологию возможности которой для простого создания красивых графических интерфейсов уже оценили многие Windows-программисты.

В PowerShell 2.0 вы сможете легко создавать обертки для команд, добавляя/изменяя/удаляя параметры, при этом сохраняя оригинальный функционал команды. Пример можно посмотреть в блоге разработчиков http://blogs.msdn.com/powershell/archive/2009/03/13/dir-a-d.aspx.

Благодаря новому подъязыку – data language – будет легко создавать сценарии, говорящие на разных языках, или отделить в сценарии данные от исполняемого кода.

Модули позволят хранить, распространять и подключать ваши наборы функций с гораздо большим удобством. О них можно прочитать в разделе справки About_Modules.

Другой раздел, About_Transactions, поведает вам о технологии, которая впервые появилась в языках сценариев, и даст нам совершенно новые возможности.

Оператор -Split легко разделит строку на компоненты, а -Join соберет ее заново, и все это используя указанные вами разделители.

Конструкция Try Catch Finally сделает обработку ошибок приятным делом. Если вы не знакомы с ней по другим языкам, то сможете научиться ее использовать, прочитав раздел справки about_Try_Catch_Finally.

Используя добавившиеся во второй версии многострочные комментарии, вы сможете легко создавать полноценную справку для своих сценариев и функций. Затем конечный пользователь сможет увидеть эту справочную информацию, даже не заглядывая в исходный код сценария, с помощью командлета Get-Help.

Кстати, о справке, не поленитесь и вызовите команду «Get-Help about_*». В PowerShell 2.0 было добавлено много новых разделов, которые позволят узнать еще больше о функционале этого языка и дадут вам еще больше возможностей.

Что дальше?

Рекомендую вам не останавливаться после прочтения этой статьи. Загрузите PowerShell 2.0 и попробуйте нововведения самостоятельно. Хоть доступная на момент написания статьи версия CTP3 и не рекомендуется к применению в реальном окружении, надо заметить, что она достаточно стабильна. Для использования Remoting и фоновых работ понадобится установить еще и WinRM 2.0 CTP3, который пока распространяется отдельно. Ссылки на загрузку находятся тут – http://xaegr.wordpress.com/2008/12/24/powershell-20-ctp3. Если же, когда вы будете читать эту статью, уже появится финальная версия PowerShell 2.0, то вы наверняка сможете его загрузить со страницы http://microsoft.com/powershell/download. Впрочем, если вы используете Windows 7, или Windows Server 2008 Release Candidate, или финальную версию, то вам не стоит себя утруждать никакими загрузками – PowerShell 2.0 и WinRM 2.0 уже интегрированы в эти системы.

Ну и конечно, не забывайте посещать мой блог (http://xaegr.wordpress.com) и блог команды разработчиков PowerShell (http://blogs.msdn.com/powershell), где вы найдете множество информации о PowerShell 2.0 и примеров кода. Также существует русскоязычная версия блога команды PowerShell – http://blogs.technet.com/powershell_ru. Еще обязательно загляните на TechDays.Ru, там уже накопилось немало видеодокладов, посвященных PowerShell – http://www.techdays.ru/Category.aspx?Tag=PowerShell. EOF

Визитка

ВИТАЛИЙ БАНКОВСКИЙ, технический директор, автор более 20 статей, главный двигатель прогресса в одной из интернет-компаний

Тратим меньше, спим больше
с VMware Sphere 4.0: установка

При развертывании нескольких ОС у сисадминов возникает два вопроса — как упростить установку, абстрагировавшись от аппаратного обеспечения, и как улучшить отказоустойчивость. Рассмотрим один из способов решения обеих задач.

Начнем с самого простого – изучим базовые понятия VMware, проведем установку и основные настройки этой системы виртуализации. В дальнейших статьях я планирую осветить такие важные аспекты, как:

- развертывание виртуальных серверов и перенос операционных систем с физических серверов на виртуальные;
- создание резервных копий виртуальных серверов;
- развертывание отказоустойчивых кластеров;
- административные задачи.

Выбор системы виртуализации

При выборе системы виртуализации я изучил несколько из них, а именно: XEN, VMware, OpenVZ, KVM. При этом я учитывал следующие критерии:

- поддержка на коммерческом уровне;
- активность разработки;
- полная виртуализация;
- возможность создания отказоустойчивых систем;
- встроенная система резервных копий;
- легкость обучения;
- удобное разделение ролей пользователей;
- качественная документация.

Также мне нужна была полная виртуализация, чтобы не нужно было модифицировать уже используемые системы на момент переноса их под систему виртуализации. После субъективного анализа рынка современных систем виртуализации я выбрал VMware ESX.

Таблица 1. Основные варианты версий и лицензий VMware

	VMware server	VMware ESXi	VMware Sphere (VMware ESX)
Тип сервера	Устанавливается на типовой дистрибутив Linux	Bare metal*	Bare metal*
Система управления	Командная строка	Текстовая консоль управления	Графическая система управления
Стоимость	Бесплатно	Бесплатно	От 995 долларов
Назначение	Домашнее использование	Системы начального уровня	Датацентры и системы масштаба предприятия

*Bare metal подразумевает установку гипервизора на аппаратный уровень сервера, без промежуточной операционной системы. Например, VMware ESX устанавливается на какой-либо существующий дистрибутив Linux.

Основные возможности VMware ESX Server 4.0

VMware предлагает богатые возможности по созданию систем от начального уровня до систем масштаба предприятия:

- поддержка 64-битных серверов и поддержка 32- и 64-разрядных гостевых систем;
- поддержка до 512 Гб памяти;
- детализированное управление пулом серверов с помощью VMware vCenter, включая установку обновлений;
- виртуальный коммутатор с реализацией VLAN с возможностью создания отказоустойчивых подключений к физическому коммутатору;
- развертывание отказоустойчивых кластеров;
- встроенная система создания резервных копий, возможность интеграции с решениями сторонних компаний;
- поддержка систем хранения на основе технологий SATA, NAS, iSCSI, Fibre Channel;
- использование шаблонов для быстрого развертывания типичных виртуальных серверов;
- перенос виртуальных серверов с одного хоста VMware на другой без остановки (технология VMware);
- создание мгновенных снимков виртуальных машин (snapshots);
- эффективное управление ролями;
- динамическое перераспределение ресурсов между серверами;
- консоль KVM для доступа к виртуальным серверам.

Установка

Компания VMware, Inc. предоставляет несколько вариантов лицензий, начиная с бесплатных версий для создания сис-

тем начального уровня до лицензий масштаба предприятия. В таблице 1 показаны основные варианты версий и лицензий.

Я использовал VMware vSphere 4 Essentials Bundle стоимостью 995 долларов. Компания VMware предоставляет пробную версию, работоспособную в течение 60 дней, которую можно скачать с сайта производителя в виде образов DVD. В качестве хоста vmware использовалось следующее аппаратное обеспечение:

- сервер Tyan TN68;
- 4 процессора AMD Opteron™ 8350 2.0 Ггц, 4 ядра в каждом процессоре;
- 64 Гб памяти;
- два встроенных массива RAID1 (для системы и для виртуальных машин);
- хранилище SAN HP MSA 1000, подключенных к хосту с помощью fiber channel.

Установка с DVD не отличается особой оригинальностью. Несколько моментов, на которые нужно обратить внимание:

- Хранилище, где будет установлена программа VMware ESX. Для этого я использовал небольшой встроенный массив RAID1, тогда как дисковые образы виртуальных машин я расположил на отдельном внутреннем массиве RAID10.
- При установке на шаге Network configuration необходимо указать идентификатор VLAN, в котором находится адрес IP управляющей консоли, причем идентификатор должет соответствовать идентификатору VLAN на физическом коммутаторе, куда подключен хост VMware, как показано на рис. 1.

Немного подробнее о внутренней сетевой архитектуре программы WMware, которая предоставляет так называемый «виртуальный коммутатор». Виртуальный коммутатор позволяет создавать виртуальные сети VLAN, назначение которых – изоляция трафика серверов одной VLAN от трафика серверов, расположенных в другом VLAN. Разумеется, при этом порты коммутатора, куда подключен хост VMware, должны быть в режиме транка с использованием протокола dot1q.

После завершения установки и перезагрузки сервера графическая консоль управления будет доступна по адресу https://<адрес сервера>. С этой страницы можно загрузить VMware Sphere Client – программа для Windows, которая предоставляет богатые возможности для управления серверами. К сожалению, этот клиент не работает под связкой Linux/Wine, а клиент для Linux находится в «зародышевом» состоянии.

Рисунок 1. Задание VLAN ID для управляющего интерфейса

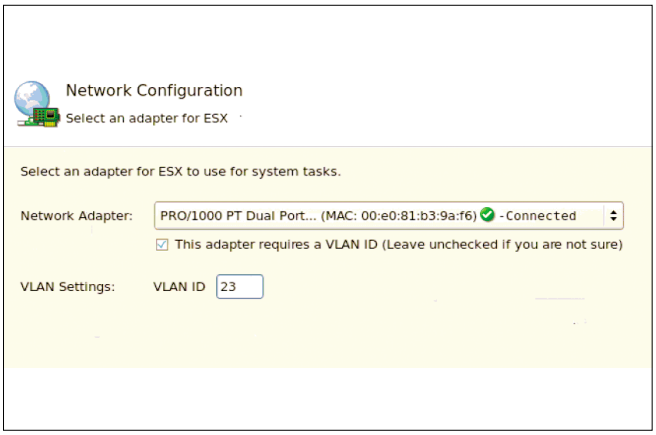


Рисунок 2. Графическое представление виртуального коммутатора

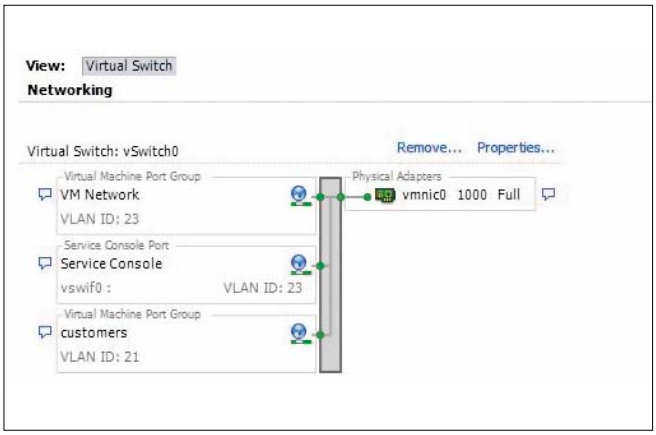


Рисунок 3. Создание VLAN

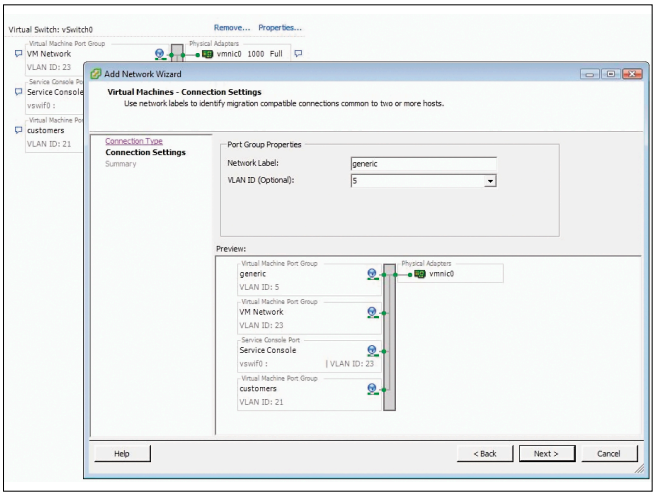
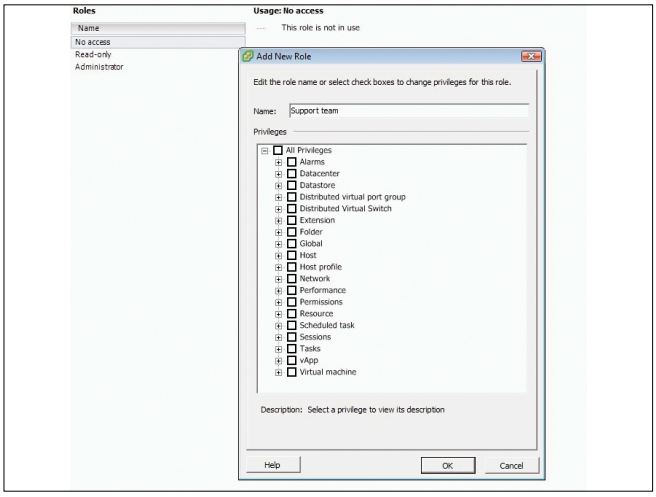


Рисунок 4. Управление ролями



Настройка виртуального коммутатора

Как я упоминал ранее, программа VMware предоставляет виртуальный коммутатор, в котором можно создавать раздельные VLAN для каждой группы серверов. В этом разделе я наглядно покажу, как это можно сделать.

Для настройки виртуального коммутатора необходимо выделить наш сервер с VMware, затем перейти в раздел Configuration и выбрать закладку Networking. При этом откроется визуальное представление коммутатора, как показано на рис. 2.

На этом рисунке можно увидеть, что на нашем коммутаторе настроены три VLAN:

- VM network.
- Service Console.
- VLAN customers для компьютеров из группы customers.

Теперь можно добавить еще одну VLAN generic. Для этого нажимаем Properties и указываем название и идентификатор VLAN, причем VLAN ID должен совпадать с номером VLAN, настроенной на нашем главном коммутаторе, куда подключен хост VMware.

В данном случае название нашего нового VLAN generic и VLAN ID равен 5.

Управление правами

Программа VMware предоставляет пользователям богатые возможности по созданию дополнительных пользователей и назначению прав по управлению всей системой или отдельным сервером. Привилегии сгруппированы, как показано в таблице 2.

Каждая группа имеет собственную подгруппу, например, можно дать возможность пользователю включать/выключать определенную виртуальную машину или только просматривать производительность.

Для нашей компании я определил следующие группы пользователей (см. таблицу 3).

Причем права конкретного пользователя можно назначать какому-либо объекту в иерархии программы VMware:

- датацентр;
- кластер;
- хост с программой VMware;
- конкретный виртуальный сервер.

У читателя наверняка возникает вопрос – можно ли создать какую-то роль с определенными правами и назначить пользователю эту роль? Конечно, компания VMware продумала решения и для этой ситуации. Для создания ролей нужно перейти в раздел Roles, который доступен из меню View, подменю Administration. Далее необходимо нажать на кнопку Add role, указать имя и права, например, как показано на рис. 4.

Далее, выбираем какой-либо объект, например, наш хост vmware, переходим в раздел Permissions, где видны пользователи, затем нажимаем правую клавишу мыши и в разделе Properties указываем роль этого пользователя.

Использование пула ресурсов

VMware поддерживает две интересные возможности – поддержка пула ресурсов и выделение виртуальных ресурсов больше, чем доступно на физическом сервере. Эти две

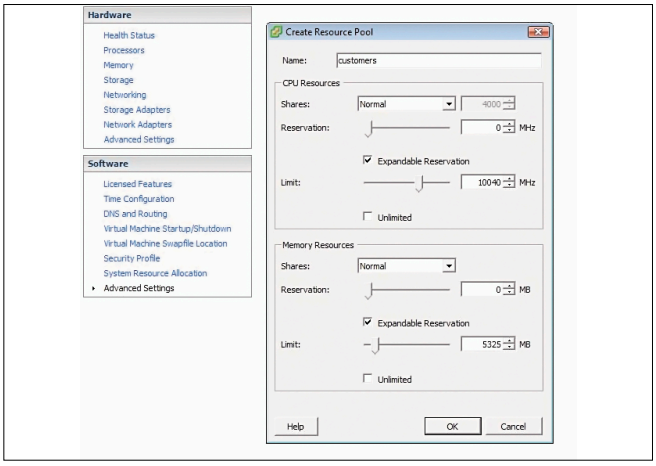
Таблица 2. Группа привилегий

Alarms	Работа с предупреждениями
Datacenter	Изменения параметров объекта «датацентр»
Datastore	Управления хранилищами
Distributed virtual port group	Настройки отказоустойчивых сетевых соединений
Distributed Virtual Switch	Управление виртуальным коммутатором
Extension	Установка/удаление расширений
Folder	Просмотр каталогов на хранилищах
Global	Глобальные настройки
Host	Настройки сервера, где установлена программа VMware
Host profile	Аналогично
Network	Управление сетью
Performance	Анализ производительности
Resource	Управление доступными ресурсами
Scheduled task	Создание/удаление задач
Sessions	Просмотр и управление сессиями авторизированных пользователей
Tasks	Создание/Удаление задач
vApp	Подключение и настройка приложений сторонних производителей
Virtual machine	Управление виртуальными машинами

Таблица 3. Группы пользователей

Администратор	Может все
Группа мониторинга	Анализируют производительность, предупреждения, могут перегружать виртуальные машины
Администраторы второго уровня	Могут создавать виртуальные машины и управлять, назначать им ресурсы
Владельцы виртуальных машин	Имею все права по управлению собственных виртуальных машин, кроме удаления

Рисунок 5. Создание пула ресурсов



возможности позволяют динамически распределять ресурсы между серверами в пулах. Таким образом, если какой-то виртуальный сервер в пуле использует мало ресурсов, то VMware будет выделять неиспользованные ресурсы в пользу другого сервера, требующего больше процессорных мощностей.

Причем, если ресурсы какого-то пула исчерпываются, то можно выделить дополнительные мощности этому пулу и соответственно виртуальным серверам без остановки последних.

При задании ресурсов пула указываются два параметра – зарезервированные ресурсы и ресурсы по требованию, причем последних можно выделить больше, чем доступно на физическом сервере, что позволяет оперировать динамически распределяемыми виртуальными ресурсами.

Пул ресурсов можно создать из верхнего меню View → Add → Pool. При этом откроется окно, показанное на рис. 5.

Как видите, можно задать параметры выделения памяти и ресурсов процессора, а именно:

- размер ресурсов процессора и памяти;
- размер расширяемых ресурсов процессора и памяти.

После создания пула новые виртуальные серверы можно создавать уже не на самом хосте VMware, но и в пуле ресурсов.

Установка сертификата

При подключении к серверу VMware с помощью интернет-обозревателя или VMware Sphere Client происходит проверка сертификата сервера VMware. При инсталляции программы VMware создается и устанавливается самоподписанный сертификат, который неизвестен клиентскому копьютеру, соответственно то будет выдано предупреждение о недействительности сертификата. Есть несколько решений этой ситуации:

Регистрация сертификата в операционной системе пользователя. Это решение подходит когда к серверу подключается ограниченное количество клиентов. Для установки сертификата, при получения предупреждения, нужно последовательно нажать на кнопки View certificate, Install certificate (зависит от ПО пользователя).

Подписание в собственном центре сертификации. Это решение подходит для компаний с собственным центром сертификации. Процедуры создания CA и подписания сертификата хорошо освещены в Интернете, например по адресу http://citforum.ru/security/cryptography/certificate_authority.

Покупка сертификата. Используется для ситуаций когда подключается много клиентов. Процедура также подробно освещена в сети Internet, например по адресу https://knowledge.geotrust.com/support/knowledge-base/index?page=content&id=AR876&actp=LIST. По завершению процедуры, необходимо скопировать сертификат rui.crt и ключ rui.key в папку /etc/vmware/ssl/ на сервере VMware и перезапустить последний.

Сертификаты можно подписать в одном из центров сертификации по адресам http://thawte.com, http://verisign.com, http://geotrust.com.

(Продолжение читайте в следующем номере.) EOF

Визитка

СЕРГЕЙ СУПРУНОВ, инженер электросвязи широкого ИТ-профиля. В свободное время изучает FreeBSD и Python и пытается осмыслить свою нелюбовь к KDE

FreeBSD tips:
periodic на службе сисадмина

Вы всегда должны знать, что происходит во вверенной вам системе. В обычной жизни следить за событиями помогают газеты и интернет-сайты. Во FreeBSD такую роль играет подсистема periodic.

Система periodic ежедневно, еженедельно и ежемесячно поставляет информацию обо всех важных событиях, происходящих в операционной системе, но системные администраторы почему-то редко уделяют ей должное внимание.

Ничего магического в ней нет – фактически задача утилиты /usr/sbin/periodic сводится к запуску всех скриптов в лексикографическом порядке из указанного в качестве аргумента каталога. Принято имя скрипта предварять трехзначным числом, задающим порядок выполнения. Таким образом, если в каталоге имеются скрипты с именами 100.script1, 200.script1, 300.script1, то порядок их запуска будет следующий: 100.script1, 200.script1, 300.script1. Нужно также учитывать, что скрипты выполняются строго последовательно, то есть каждый следующий запускается только после полного завершения предыдущего. Утилита periodic запускается подсистемой cron – в /etc/crontab можно найти следующие строки:

```
$ grep periodic /etc/crontab
1       3       *       *       *       root    periodic daily
15      4       *       *       6       root    periodic weekly
30      5       1       *       *       root    periodic monthly
```

Время исполнения подобрано таким образом, чтобы минимизировать «пересечение» с другими заданиями. Для большинства серверов, работающих круглосуточно, эти значения достаточно удачны, но если ваша система используется только в рабочее время или же на ночь приходится пик нагрузки, то расписание имеет смысл пересмотреть.

Вывод скриптов в общем случае, как и подобает заданиям cron, направляется соответствующему пользователю по электронной почте (по умолчанию это root; указать другого можно в переменной MAILTO crontab-файла, но это скажется на всех заданиях из /etc/crontab). Однако при необходимости это нетрудно изменить – в /etc/periodic.conf для каждого обрабатываемого каталога можно указать параметр вида <ИмяКаталога>_output, например:

```
daily_output="admin"
weekly_output="amsand@rambler.ru"
monthly_output="/var/log/monthly.log"
myscripts_output=""
```

При таких настройках результат выполнения скриптов из каталога daily будет направлен локальному пользователю admin, из weekly – по адресу на стороннем сервере, вывод monthly-сценариев уйдёт в указанный файл, а для скриптов из каталога myscripts будут использоваться текущие правила подсистемы cron.

Обратите внимание, что без дополнительной настройки periodic будет искать переданный ей в качестве параметра каталог в /etc/periodic и каталогах, указанных в конфигурации в параметре local_periodic (по умолчанию /usr/local/etc/periodic). Но при желании утилите можно передать и полное имя к каталогу со скриптами: /usr/sbin/periodic /usr/home/amsand/myscripts.

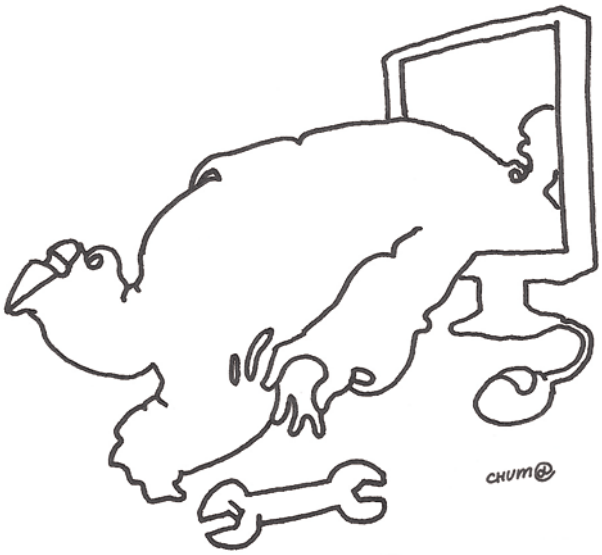
Все «умолчальные» параметры сосредоточены в /etc/defaults/periodic.conf, для внесения изменений в поведение подсистемы предназначен файл /etc/periodic.conf (изначально отсутствует). Конфигурационные параметры группируются по именам каталогов и скриптов, к которым относятся – если вывод того или иного сценария вас не вполне устраивает, загляните в /etc/defaults/periodic.conf, возможно, его работу можно будет подстроить под ваши потребности.

Как ни странно, но многие удовлетворяются возможностями, заданными по умолчанию, а иногда и вообще не задумываются о возможности подстроить periodic под свои задачи и тем самым повысить эффективность использования инструмента. Конечно, параметры по умолчанию работают неплохо, и для некоторых систем они действительно будут оптимальными. Но в общем случае индивидуальная подстройка periodic имеет смысл, и мы рассмотрим все возможности, предоставляемые этим инструментом.

Начнём с рассмотрения скриптов, представленных в /etc/periodic/daily.

100.clean-disks

Этот скрипт удаляет все файлы, имена которых соответствуют заданным шаблонам (по умолчанию это [#,]*, .#*, a.out,



*.core, *.CKP и .emacs_[0-9]*) и возраст которых больше заданного в параметре daily_clean_disk_days числа дней. По умолчанию не выполняется, и особой нужды в ежедневном выполнении я не вижу. Хотя у вас может быть по-другому.

110.clean-tmps
Удаляет все «временные» файлы (по умолчанию из /tmp, задаётся переменной daily_clean_tmps_dirs), старше указанного возраста (daily_clean_tmps_days), кроме соответствующих шаблонам, указанным в daily_clean_tmps_ignore. По умолчанию не выполняется, но если используемое вами ПО часто «забывает» подчищать за собой временный каталог, то имеет смысл включить выполнение этого файла, установив в /etc/periodic.conf переменную daily_clean_tmps_enable в YES.

120.clean-preserve
Удаляет старые файлы из /var/preserve, куда редактор vi в давние времена сохранял служебные файлы при аварийном завершении работы (например, при разрыве соединения) для последующего восстановления. По умолчанию выполняется, что несколько странно, так как «бэкапные» файлы vi уже давненько пишет в /var/tmp/vi.recovery, а изменить каталог /var/preserve, кроме как прямым редактированием сценария, нельзя. Рекомендую этот скрипт отключить.

130.clean-msgs
Очищает устаревшие msgs-сообщения (см. man msgs). Утилита msgs позволяет пользователям системы оставлять короткие сообщения всем остальным пользователям и читать такие сообщения. То есть играет роль доски объявлений. По умолчанию выполняется, но если вы не используете механизм msgs-сообщений, то нет смысла каждую ночь впустую вызывать скрипт, так что установите daily_clean_msgs_enable в NO.

140.clean-rwho
Очищает каталог /var/rwho – в нём накапливается информация, собираемая демоном rwhod. Этот демон собирает рассылаемую другими машинами UNIX-сети информацию, аналогичную той, которую возвращает команда who (аптайм, средняя загрузка, список подключенных пользователей). По умолчанию выполняется, но, поскольку такие доверительные отношения между машинами сети сейчас редко встречаются, скорее всего, смысла в этом сценарии на большинстве систем нет.

150.clean-hoststat
Sendmail в процессе своей работы может собирать статистику доступности хостов, чтобы не тратить время на попытки соединиться с теми, которые недавно были недоступны. Эта статистика со временем устаревает и начинает впустую расходовать память и место на диске. Задача скрипта заключается в вызове утилиты purgestat, которая очищает устаревшие данные. По умолчанию выполняется, но если вы не используете Sendmail, то в запуске этого скрипта не будет особого смысла.

200.backup-passwd
Копирует в /var/backups файлы master.passwd и group из каталога /etc. С одной стороны, такое копирование создаёт дополнительную «точку ответственности» для администратора, но с другой – позволяет восстановить случайно испорченные файлы, являющиеся жизненно важными для работы системы. По умолчанию выполняется.

210.backup-aliases
Ещё один пример копирования важных файлов. На этот раз в /var/backups будет сохраняться /etc/mail/aliases. По умолчанию выполняется.

300.calendar
Запускает утилиту calendar с ключом -a, которая обрабатывает файлы «календарей» всех пользователей и отсылает им по электронной почте сегодняшние и завтрашние задачи. По умолчанию не выполняется, и разработчики планируют удалить эту функцию из periodic, предлагая при необходимости использовать задания cron непосредственно.

310.accounting
Выполняет ротацию acct-файлов в /var/account. Учёт процессов (см. man acct(2)) позволяет сохранять в файл статистику всех запускавшихся процессов, такую как число вызовов процесса, израсходованное им процессорное время, среднее число операций ввода-вывода и т.п. По умолчанию выполняется, но, учитывая, что сбор подобной статистики на «боевых» серверах выполняется нечасто, над необходимостью выполнения этого сценария стоит задуматься.

330.news
Когда-то предназначался для запуска сценария /etc/news.expire сервера новостей. В базовой системе я уже давно news-сервера не наблюдаю, тем не менее по умолчанию этот сценарий выполняется (если в /etc/periodic.conf выставить daily_show_badconfig в YES, то ежедневно вы будете получать сообщение об отсутствии файла /etc/news.expire; по умолчанию сообщения об ошибках не отсылаются). Однозначно нужно отключать (задав конфигурационной переменной daily_news_expire_enable значение NO).

400.status-disks
Этот сценарий выводит информацию о состоянии локальных файловых систем (выполняя команду «df -l -h») и о последних дампах. Очень полезно для контроля за свободным пространством на дисках. Кроме того, позволяет обнаружить «лишние» файловые системы (скажем, забытую флешку или диск с резервной копией). По умолчанию выполняется.

404.status-zfs
Выводит информацию о состоянии пулов ZFS. По умолчанию не выполняется, но если вы используете ZFS, то имеет смысл выставить в /etc/periodic.conf параметр daily_status_zfs_enable в значение YES.

405.status-ata-raid
Возвращает данные о статусе RAID-контроллеров (по результатам вывода утилиты atacontrol). По умолчанию не выполняется.

406.status-gmirror, 407.status-graid3, 408.status-gstripe, 409.status-gconcat
Эти скрипты выводят информацию о состоянии соответствующих дисковых массивов, управляемых подсистемой GEOM. По умолчанию не выполняются.

420.status-network
Выводит результат работы команды «netstat -i», позволяя контролировать состояние интерфейсов на момент выполнения скрипта (интерфейсы, находящиеся в состоянии down, будут отмечены звёздочкой «*»), а также число переданных и принятых пакетов, в том числе ошибочных. По умолчанию выполняется.

430.status-rwho
Выводит информацию о времени непрерывной работы (uptime) машин UNIX-сети, которую собирает rwhod. По умолчанию выполняется, но по тем же причинам, о которых шла речь при обсуждении сценария 140.clean-rwho, на большинстве систем он фактически не нужен.

440.status-mailq
Скрипт выполняет команду mailq, возвращающую информацию о почтовой очереди. Выставив переменную daily_status_mailq_shorten в YES, вы будете получать сводную статистику вместо информации по каждому сообщению в очереди. По умолчанию выполняется.

450.status-security
Это своего рода «мета-скрипт» для запуска заданий из /etc/periodic/security. Как вы видели, в заданиях cron присутствуют вызовы только для daily, weekly и monthly, поскольку проверка безопасности предполагается как ежедневное задание. Можно было бы все security-сценарии разместить и непосредственно в daily, но разработчики приняли решение, что для такой ответственной задачи лучше выделить отдельный каталог. Вы тоже вполне можете использовать этот приём для выполнения «пакетных» задач.

460.status-mail-rejects
Этот сценарий выполняет анализ почтового лог-файла (/var/log/maillog) и выводит статистику по отклонённым письмам (с указанием причины). Вывод группируется по хостам-отправителям и сортируется в порядке убывания числа отклонённых соединений. Параметр daily_status_mail_rejects_logs задаёт число «архивных» файлов, полученных в ходе ротации (maillog.0.bz2 и т.д.), которые также будут обрабатываться. Если ротация почтовых логов в вашей системе выполняется ежедневно, имеет смысл выставить данный параметр в 0 (по умолчанию используется значение 3), чтобы не обрабатывать одни и те же данные несколько раз. Если вы используете другую политику ротации (например, по достижении определённого размера файла), подберите число обрабатываемых файлов таким образом, чтобы полностью охватить все логи, накапливаемые за сутки (если, конечно, для вас достоверность информации представляет какую-то ценность). По умолчанию выполняется.

470.status-named
Выбирает из файлов /var/log/messages записи процесса named, сообщающие о той или иной ошибке (failed, REFISED), а также о пересылках зон (transfer). По умолчанию выполняется.

480.status-ntpd
Выводит список известных NTP-серверу соседей (peer). По умолчанию не выполняется, но если стабильная работа системы времени для вас важна, можете включить эту проверку.

500.queuerun
Запускает обработку почтовой очереди (командой «sendmail -q»). По умолчанию выполняется, но подумайте о его отключении, если используете другой почтовый сервер.

Недельные задачи носят в основном сервисный характер:

310.locate
Проводит обновление базы locate (утилитой /usr/libexec/locate.update). База позволяет выполнять быстрый поиск

файлов в системе, не прибегая каждый раз к глобальному просмотру всех каталогов. Периодическое обновление необходимо, чтобы поддерживать базу в актуальном состоянии. По умолчанию выполняется, но если возможности locate вам не требуются или создаваемая утилитой locate.update нагрузка на файловую систему нежелательна даже раз в неделю, запуск этого сценария можно отключить.

320.whatis
Аналогично предыдущему сценарию, этот скрипт поддерживает в актуальном состоянии базу whatis (которая осуществляет контекстный поиск по содержимому man-страниц). По умолчанию выполняется, однако если состав man-страниц меняется редко (что верно для большинства рабочих серверов), то имеет смысл вызов скрипта отключить, а обновление базы whatis выполнять по мере необходимости вручную.

330.catman
Выполняет переформатирование man-страниц (командой catman). По умолчанию не выполняется, и на большинстве систем необходимости в нём не возникает.

340.noid
Ищет файлы и каталоги, не принадлежащие ни одному из пользователей и групп. По умолчанию не выполняется, хотя в некоторых случаях (особенно при обновлении ОС до другой версии) может быть полезным для поиска «осиротевших» файлов.

400.status-pkg
Выводит список установленных пакетов, требующих обновления. По умолчанию не выполняется. Однако, если ваша система настроена на автоматическое обновление коллекции портов (например, по cron с помощью portsnap), то данная информация может быть полезна – установите в /etc/periodic.conf переменную weekly_status_pgk_enable в YES.

Ежемесячно в текущих версиях FreeBSD исполняется только один сценарий:

200.accounting
Он собирает статистику по использованию пользователями процессорного времени. По умолчанию выполняется, но на большинстве серверов особой необходимости в этом нет. Разве только в порядке соц. соревнования – кто из администраторов сильнее нагружает систему?

И, наконец, наиболее важный каталог – security (все сценарии по умолчанию выполняются, так что я не буду указывать это отдельно):

100.chksetuid
Скрипт проверяет изменения в составе файлов, для которых установлен бит suid или sgid. Поиск выполняется утилитой find по всем файловым системам, кроме смонтированных с опцией nosuid или noexec, результат сравнивается с предыдущим значением (обычно сохраняется в /var/log/setuid.today). Обнаруженные отличия отправляются админи-

Локальные задания periodic

Некоторые сторонние программы используют систему periodic в своих целях. Например, postgresql при установке из Портов помещает в /usr/local/etc/periodic/daily файл 502.pgsql. В зависимости от настроек (которые выполняются, как и для остальных periodic-сценариев, в /etc/periodic.conf) этот скрипт ежедневно может выполнять дефрагментацию баз данных (командой vacuumdb) и их резервное копирование.

Так что, устанавливая ту или иную программу, обращайте внимание и на этот момент – чтобы не было сюрпризов в виде резко подскакивающей нагрузки на систему в неудачное время или пропажи архивных файлов, которые вы собирались неспешно обработать в конце месяца.

стратору. И хотя такой поиск довольно сильно может нагружать файловую подсистему, лучше от него не отказываться. Впрочем, если вы ведёте аудит безопасности другими средствами, проверку можно отключить.

200.chkmounts

Сравнивает текущий список смонтированных систем (возвращаемый командой «mount -p») со вчерашним списком, сохранённым в /var/log/mount.today.

300.chkuid0

Проверяет наличие в master.passwd пользователей с идентификатором 0, отличных от root и toor. Поскольку права суперпользователя определяются именно нулевым значением UID, а не символьным именем, такая проверка позволяет выявить опасные опечатки (или «чёрный ход», оставленный взломщиком или предыдущим администратором).

400.passwdless

Ищет пользователей с пустыми паролями.

410.logincheck

Проверяет права на файл login.conf (должен принадлежать пользователю root и группе wheel).

500.ipfwdenied, 510.ipfdenied, 520.pfdenied

Эти три скрипта выводят информацию о запрещающих правилах пакетных фильтров (соответственно ipfw, ipf и pf), изменившихся с момента предыдущей проверки.

550.ipfwlimit

Выводит список правил ipfw, по которым были превышены заданные лимиты.

700.kernelmsg

Отображает изменения вывода dmesg, произошедшие с момента последней проверки. Например, если за предыдущие сутки к серверу подключалась флешка, результат проверки может выглядеть следующим образом:

```
 kernel log messages:
+++ /tmp/security.mc0L61TV         2009-06-08 21:14:25.000000000 +0400
+umass0: <Kingston DataTraveler 2.0, class 0/0, rev 2.00/1.10, addr 2> on uhub1
+da0 at umass-sim0 bus 0 target 0 lun 0
+da0: <Kingston DataTraveler 2.0 PMAP> Removable Direct Access SCSI-0 device
+da0: 40.000MB/s transfers
+da0: 984MB (2015232 512 byte sectors: 64H 32S/T 984C)
+GEOM_LABEL: Label for provider da0s1 is msdosfs/KINGSTON.
+umass0: at uhub1 port 2 (addr 2) disconnected
+(da0:umass-sim0:0:0:0): lost device
+(da0:umass-sim0:0:0:0): removing device entry
+GEOM_LABEL: Label msdosfs/KINGSTON removed.
+umass0: detached
```

800.loginfail

Выводит информацию обо всех ошибках входа в систему, зафиксированных в /var/log/auth.log за прошедшие сутки.

900.tcpwrap

Возвращает предупреждения системы TCP Wrappers, найденные в файлах /var/log/messages.

Помимо рассмотренных сценариев в каталогах daily, weekly и monthly вы найдёте файлы 999.local. Их назначение – запуск скриптов /etc/daily.local, /etc/weekly.local и /etc/monthly.local соответственно. По умолчанию эти скрипты отсутствуют, но если хотите запускать свои команды вместе с другими periodic-задачами, вы можете их создать.

Например, чтобы ежедневно получать данные о доступности некоторого сервера и среднем времени передачи пакетов к нему, можно создать файл /etc/daily.local следующего содержания:

Ну и, безусловно, вы всегда можете поместить в /etc/periodic/* свои собственные скрипты (хотя для этого всё же рекомендуется использовать каталоги /usr/local/etc/periodic/*).

Пример

В заключение приведу пример своего файла /etc/periodic.conf (только не нужно рассматривать его как эталон – ваши потребности могут отличаться от моих):

```
daily_clean_preserve_enable="NO"
daily_clean_msgs_enable="NO"
daily_clean_rwho_enable="NO"
daily_accounting_enable="NO"
daily_news_expire_enable="NO"
daily_status_rwho_enable="NO"

daily_status_disks_df_flags="-l -h -i"

weekly_locate_enable="NO"
weekly_whatis_enable="NO"

weekly_noid_enable="YES"
weekly_status_pkg_enable="YES"
```

То есть я отключил все сценарии, которые мне не нужны (или периодический запуск которых неэффективен), включил контроль «осиротевших» файлов (noid_enable), поскольку часто экспериментирую, в т.ч. и с учётными записями. Также включил еженедельный вывод информации о статусе установленных пакетов. Ну и добавил флаг «-i» для утилиты df (по умолчанию 400.status-disks запускает её как df -l -h), чтобы получать также и данные о свободных индексных дескрипторах (inode). Всё остальное остаётся по умолчанию (согласно /etc/defaults/periodic.conf).

Как видите, по умолчанию periodic выполняет много лишнего (хотя это и не смертельно), так что желательно вдумчиво подходить к её настройке. Это позволит вам регулярно получать массу полезной (и только полезной) информации о жизнедеятельности ваших серверов. Так что, устанавливая новую систему, не ленитесь уделять подсистеме periodic пару минут. EOF

Удаленное выполнение команд оболочки в NAGIOS

Программа: Nagios 3.1.1.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Сценарий statuswml.cgi недостаточно фильтрует данные в параметре ping перед выполнением команды PING. В результате возможно внедрить и выполнить произвольные команды оболочки. Для успешной эксплуатации требуется доступ к функции PING через Wap-интерфейс.
URL производителя: http://www.nagios.org.
Решение: Обновите до версии 3.1.1.

Переполнение буфера в обработке TCP-пакетов в Bopup Communication Server

Программа: Bopup Communication Server 3.2.26.5460 и более ранние версии.
Опасность: Средняя.
Наличие эксплоита: Да.
Описание: Специально обработанный TCP-пакет, посланный на 19810-й порт, может вызвать стековое переполнение буфера и привести к выполнению произвольного кода на уязвимой системе.
URL производителя: http://www.blabsoft.com.
Решение: В настоящее время способов устранения уязвимости не существует.

Уязвимая OpenSSL-библиотека в SSVNC

Программа: SSVNC до версии 1.0.23.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Как сообщается, прекомпилированная версия программы содержит уязвимую версию OpenSSL-библиотеки.
URL производителя: http://www.karlrunge.com/x11vnc/ssvnc.html.
Решение: Обновите до версии 1.0.23.

Неавторизованный SMTP-релей в F-Secure Messaging Security Gateway

Программа: F-Secure Messaging Security Gateway 5.5.x.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Уязвимость обнаружена в запрете релея e-mail-сообщений при использовании SMTP turbo-модуля. В результате уязвимая система может использоваться как ретранслятор почтовых сообщений через специально созданный SMTP-запрос.
URL производителя: http://www.f-secure.com/products/fsmsgp.
Решение: Установите исправление 739 .

Переполнение буфера в библиотеке ToolTalk в IBM AIX

Программа: IBM AIX версии 5.2.0, 5.3.0, 5.3.7, 5.3.8, 5.3.9, 5.3.10, 6.1.0, 6.1.1, 6.1.2 и 6.1.3.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки проверки границ данных в функции _tt_internal_realpath() в библиотеке ToolTalk (libtt.a). Удаленный пользователь может с помощью специально сформированного запроса к серверу баз данных ToolTalk, содержащего слишком длинную XDR-кодированную строку в кодировке ASCII, вызвать переполнение стека и выполнить произвольный код на целевой системе. Для успешной эксплуатации уязвимости rpc.ttdbserver должен быть включен в etc/inetd.conf.
URL производителя: www.ibm.com.
Решение: Установите исправление с сайта производителя.

Множественные уязвимости в DB Top Sites

Программа: DB Top Sites 1.x.
Опасность: Высокая.
Наличие эксплоита: Да.
Описание: 1. Уязвимость в параметре u в full.php, index.php и contact.php позволяет включить произвольные локальные файлы, используя технику обхода каталога и URL-кодирования.
2. Сценарий add_reg.php создает несколько PHP-файлов, содержащих значения передаваемых параметров. В результате можно выполнить произвольный PHP-код через специально созданный параметр location.
URL производителя: http://www.jnmsolutions.co.uk/index.php?act=scripts&page=topsites.
Решение: В настоящее время способов устранения уязвимости не существует.

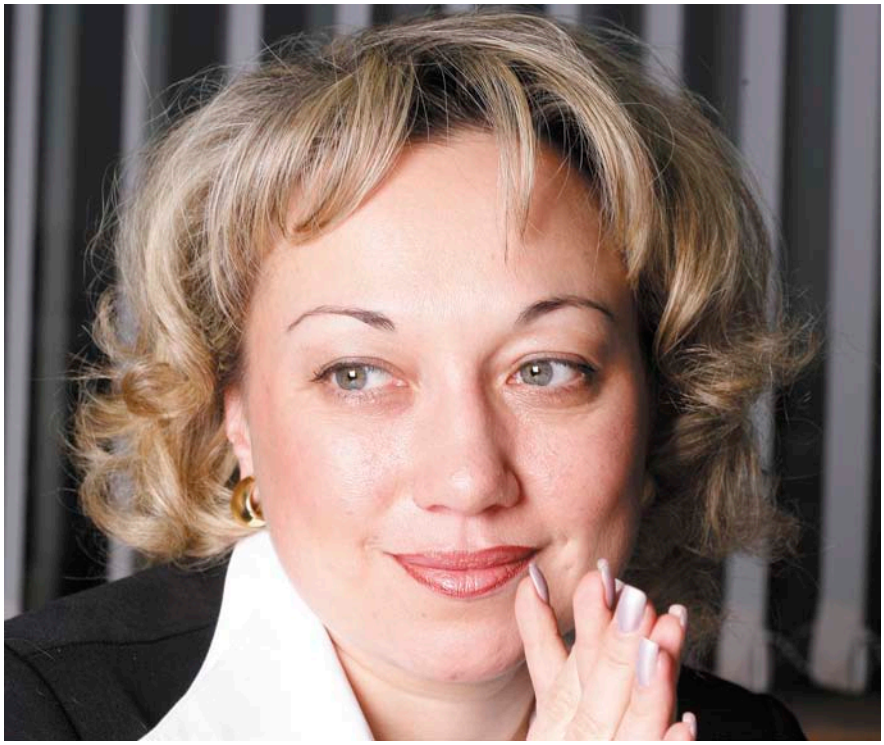
Множественные уязвимости в CA ARCserve Backup

Программа: CA ARCserve Backup 12.0 и 12.0 SP1.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: 1. Уязвимость существует из-за ошибки в модуле ASCORE механизма сообщений. Удаленный пользователь может отправить специально сформированный RPC-пакет на порт 6503/TCP и аварийно завершить работу приложения.
2. Уязвимость существует из-за ошибки в механизме сообщений. Удаленный пользователь может отправить специально сформированный RPC-пакет на порт 6503/TCP и аварийно завершить работу приложения.
URL производителя: www.ca.com.
Решение: Установите исправление Service Pack 2 RO08383 с сайта производителя.

Составил Александр Антипов

Оксана Глущенко:
«ИТ-ландшафты: бизнес-эволюция или бизнес-революция?»

На вопросы «Системного администратора» отвечает Директор по развитию бизнеса РОССВИФТ, независимый член Совета директоров консалтинговой компании ЗАО «Эн Ди Групп» Оксана Глущенко.



Оксана Глущенко имеет два высших образования, кандидат экономических наук, сочетает практику банкира и топ-менеджера. С 1994 по 2002 г. прошла путь от экономиста до топ-менеджера «Промстройбанка», г. Санкт-Петербург. В 2005-2008 гг. была директором Департамента по работе с финансовыми институтами в компании «САП СНГ», отвечала за взаимодействие с банками, страховыми и финансовыми организациями на территории России и СНГ. В 2002-2005 гг. руководила в швейцарской компании «Теменос» внедрением проектов автоматизированных систем для банков на территории СНГ и стран Балтии. С 2008 г. – директор по развитию бизнеса РОССВИФТ, одновременно является с 2009 г. независимым членом Совета директоров консалтинговой компании ЗАО «Эн Ди Групп».

– Оксана, сегодня все, обсуждая кризис, ищут аналогии с событиями десятилетней давности. Как, по-вашему, повлияли кризисы 98-99-х годов и нынешний на ИТ-сообщество, на пользователей, системщиков?

– Тот первый кризис лишь потрепал сознание ИТ-сообщества. В конце 90-х уже стартовал процесс технологической модернизации во всех бизнесах, в том числе и банковском. Кризис лишь укрепил эту тенденцию.

Что я имею в виду? Во-первых, ERP-системы с индустриальным контентом стали тогда своего рода стандартом для многих производств. Во-вторых, в то время CRM-решения только начинали прокладывать себе путь как самостоятельные системы. В результате внедрения западных систем, таких как SAP, Oracle, IBM, Microsoft, в России произошла эволюция сознания, усилившаяся под влиянием кризиса в 98-99-х годах.

По существу, рынок программного обеспечения (и внедрений тоже!) испытывает влияние, правда, не всегда сбалансированное, таких тенденций, как:

– отход от стандартов, когда подразумевалось внедрение единой монолитной системы, все компоненты которой приобретаются у одного поставщика. Такой подход был очень популярен в прошлом, а сейчас на арену уже

вышел компонентный подход, когда для каждой бизнес-задачи, функционального направления бизнеса выбирается интегрируемое решение, лучшее в своем классе;

– реализация в системах возможности индустриального и преднастроенного контента и функционала;

– достаточно осознанная ориентация в развитии ландшафтов ИТ с применением SOA;

– процессно-ориентированного управления и мощных средств и инструментария бизнес-аналитики;·

– распространение тенденций глобализации и стандартов бизнеса не только на крупные компании, но и на средних игроков;

– и, наконец, слияния и поглощения, в том числе не только компаний клиентов, но и объединение усилий и технологий самих вендоров ПО.

Сегодня (важный штрих нынешнего кризиса!) управленческие решения становятся очень востребованными. Кстати, скорость (быстрота) принятия управленческих решений буквально за последние годы, я полагаю, выросла в разы. Отсюда стремление переориентировать ИТ-политику на решения класса бизнес-анализа и поддержку принятия решений. Поскольку банки и предприятия стали гораздо ближе к западным стандартам бизнес-процессов и соглашений по обслуживанию систем, заметно выросла потребность в квалифицированных специалистах, обученных таким технологиям. Рынок ИТ-кадров оказался даже перегрет из-за такой нагрузки. А шла она именно от изменения условий и потребностей бизнеса. Это вхождение западного капитала, IPO российских компаний, рост конкуренции в сфере услуг и торговли.

Все это революционным образом повлияло на сознание ИТ-сообщества: от системного администратора до CIO. Полагаю, что и сейчас кризис лишь поверхностно зачистит ряды стремящихся заниматься ИТ и бизнес-технологиями и переориентирует ИТ-менеджмент, заставит его адаптироваться к новым условиям и искать иные пути для дальнейшего развития.

Иными словами, ИТ сейчас выходят на качественно новый уровень, когда верхи (топ-менеджмент компаний) не могут жить по старому, а низы не хотят.

– Вы много лет работаете в банковской области, а также в сфере бизнес- и информационных технологий. Скажите, как менялись требования заказчиков, топ-менеджеров компаний, банков в последние годы?

– Мне посчастливилось не только наблюдать, но и активно участвовать в выработке требований как на стороне заказчика, так и в качестве руководителя коллективов, которые продвигали стандартные программные продукты – бизнес-приложения. Что изменилось?

Во-первых, с точки зрения функциональных требований к системе, они претерпели как структурные, так и качественные изменения. Теперь все четко выделяют клиентский блок. Например, с развитием и внедрением CRM-решений пришло осознание, что набор требований к клиентской информации, процессам ее обработки в подразделениях компании надо существенно расширить.

Если говорить о банках, то произошло и существенное изменение представлений о том, каким должен быть ландшафт современной современной автоматизированной банковской системы (АБС): от единой системы, построенной вокруг до компонентной сервисной архитектуры, построенной по принципам SOA (сервисно-ориентированной архитектуры).

Во-вторых, с точки зрения системотехнических требований значительно выросли запросы к скорости обработки транзакций, производительности продуктивных систем и объемам хранимой информации.

Важно отметить, что самостоятельное развитие и бизнес-значение получает ПО промежуточного слоя, или Middleware, что является необходимой платформой для гарантированной доставки транзакций в гетерогенных, распределенных и мультикомпонентных системах. В последние годы слияния в банковской системе неизбежно ведут либо к перекраиванию всей клиентской политики и перезаключению договоров с клиентами объединивших-ся банков (а это высокий риск!), либо к грамотной работе по увязке клиентов, продуктовых систем и сервисов по бухгалтерии и обязательной отчетности через Middleware.

Главная причина в трансформации представлений и требований – это время! Необходимо быстро реагировать на изменения и иметь возможность оперативно запускать новые сервисы как с технической, так и с бизнес-стороны. Здесь, кстати, в последний год наметилась еще одна тенденция, которая, на мой взгляд, будет определять развитие ландшафтов и бизнес-требований в ближайшие пару лет. Это SaaS (Software as a Service) – новый сервисный подход к распространению ПО – как услуги, а не как продукта. Эта модель уже применяется на мировом рынке, но в России она только начинает формироваться.

– Какие преимущества она дает ИТ-директорам, финансистам, гене-

Компания ND-Group, оказывающая услуги консалтинга и системной интеграции, основана в 2006 году. Первым крупным проектом ND-Group стала локализация решения SAP for banking, которая была проведена в 2006-2007 гг. и была признана успешной. ND-Group обладает статусами партнерства SAP: Localization partner и SAP Preferred partner для финансовой сферы.

Кризис лишь поверхностно зачистит ряды стремящихся заниматься ИТ и бизнес-технологиями и переориентирует ИТ-менеджмент, заставит его адаптироваться к новым условиям, искать иные пути для дальнейшего развития

Согласно Уставу SWIFT (Society for Worldwide Interbank Financial Telecommunication) – в каждой стране, представленной в сообществе, создаются Национальная группа членов SWIFT и Группа пользователей SWIFT. В России их интересы представляет организация РОССВИФТ, которая была создана в 1994 году. РОССВИФТ является членом Европейского SWIFT Альянса, объединяющего более 30 стран внутри SWIFT, на долю которых приходится около трети мирового трафика.

ральным директорам и собственникам бизнеса?

– Что нужно сегодня, в кризисных условиях, CEO, акционерам, генеральному директору? Прежде всего, чтобы технологические задачи были решены как можно быстрее и по возможности за небольшие деньги. Скажем, компания собирается развивать новое направление или готовится к процедуре слияния. Время и скорость выхода на рынок, равно как и вопрос получения консолидированной отчетности, играют в этой ситуации немаловажную роль.

Финансисту говорят, что нельзя допускать лишней иммобилизации средств акционеров на покупку решения и его внедрение в течение одного-двух лет. Налоговый пресс также заставляет финансистов искать свежие решения – от оформления своих новых бизнес-процессов консолидации отчетности, как know how с последующей капитализацией затраченных средств, так и нематериальный актив аренды приложений систем хранения, лишь бы не увеличивать капитальные затраты сейчас.

Представители ИТ отличаются консервативностью, они не всегда хотят отдавать сторонней компании свою потенциальную часть работ по внедрению и сопровождению. Но это всего лишь временный аспект, как и аргументы по поводу рискованности схем аутсорсинга. Кстати, иногда зависимость от собственного всесильного ИТ гораздо более рискованна, чем услуги, оказанные со стороны.

Необходимо добавить несколько слов про ПО с открытым кодом. Это очень важный вопрос, особенно в контексте того, что всякое ПО должно проходить сертификацию. Это очень актуально для государственных структур. Ориентация президента страны Дмитрия Медведева на отечественные разработки также заставляет всех, кто принимает решения в области ИТ, уделять самое пристальное внимание ПО с открытым кодом.

– Меняется ли роль системного администратора сегодня?

– Безусловно! Прежде всего он должен, как никогда, быть квалифицированным специалистом в области информационной безопасности и обладать широким кругозором. Также я уверена он должен обладать высокоморальными качествами.

– Предположим, компания решила переходить на SaaS. С чего должен начать в таком случае ИТ-руководитель?

– Во-первых, начните с простого – с функционирования электронной почты сотрудников, внутреннего портала компании.

Во-вторых, выделите наиболее срочные задачи и сопоставьте их с предлагаемыми возможными решениями по SaaS:

- ERP-функции;
- управление кадрами;
- консолидация, если таковая требуется в бизнесе компании;
- управление недвижимостью;
- CRM-функции.

В-третьих, ведите переговоры и старайтесь подсчитать, как выгоднее использовать такие решения.

Если в конечном счете решение приживется, то, возможно, ваша компания сможет выкупить его у поставщика услуг. Поэтому хочу повторить еще раз – это процесс переговоров. Я бы обязательно предусматривала в договорах, в вариантах оплаты услуг возможность выкупа решения, удаленное администрирование ваших настроек и данных.

В-четвертых, смотрите, на какой платформе решение.

И наконец, необходимо обратить внимание на то, как осуществляется работа сервис-провайдера по соглашению обслуживания и какие у него подключены Data Center. Кстати, небольшие компании, возможно, будут более гибкими, а их подходы – более релевантными вашим запросам. Уровень сервиса таких компаний при вполне приемлемой цене нередко оказывается выше, чем у признанных старых игроков, что является ключевым требованием сегодняшнего дня.

– В чем же небольшие провайдеры могут дать фору крупным игрокам?

– Давайте проанализируем. Если небольшая компания имеет квалифицированный штат, высококлассных спрециалистов, если у нее есть хорошие контакты не с одним Data Center, то я бы выбирала такого поставщика услуг.

Такие компании сегодня очень часто исповедуют кооперативные стратегии, позволяющие минимизировать возможные трения и принимать решения, учитывающие цели всех заинтересованных сторон. Они будут развивать решения, пусть и по вашим подсказкам.

И ничего плохого тут нет. Главное – достигнуть синергии, тогда процесс, как говорится, пойдет.

Я бы отметила в заключение, что современные ИТ-ландшафты, находятся ли они в больших компаниях или нет, претерпевают поистине революционные изменения. Меняется спрос и на ИТ-услуги. Да, кризис заставляет крутиться и заказчиков, и поставщиков, что уже само по себе неплохо. EOF

Уже наметилась тенденция, которая будет определять развитие ландшафтов и бизнес-требований в ближайшие годы. Это SaaS – новый сервисный подход к распространению ПО – как услуги, а не как продукта

Как на вас и на вашей компании сказался кризис?

На вопрос «Системного администратора» отвечают ИТ-специалисты.

Сергей Лопутнёв, директор ООО «Программные Решения», г. Калининград

Наша компания предлагает на рынке Калининградской области услуги по развёртыванию и сопровождению крупных программно-аппаратных комплексов, а также услуги ИТ-аутсорсинга.

Текущая экономическая ситуация сильно сказалась на жизнедеятельности компании. Мы ориентировались в основном на крупные фирмы и предприятия. Сейчас большинство крупных заказчиков находятся в крайне тяжёлом финансовом положении, некоторые компании закрылись, а у тех кто работает, новые проекты заморожены или закрыты.

Для того чтобы сохранить обороты фирмы и персонал, мы диверсифицировали свою деятельность и стали предлагать отраслевые решения, которые помогают клиентам в минимальные сроки существенно сократить издержки, повысить эффективность работы, а сотрудникам нашей компании сохранить свою квалификацию.

Андрей Шетухин, г. Москва

Я считаю, что кризис – отличный предлог. Предлог для чего угодно.

Пришло время выгнать бездельников – выгоняем, ведь кризис!

Надо поставить на место зарвавшийся офисный планктон – лишаем премий ни за что, ведь кризис! Кризис – отличная возможность избавиться от бездельников, лентяев и тупиц.

И заняться, наконец, делом.

технический директор, г. Москва

Прекращено расширение компании (найм нового персонала), увеличилась средняя нагрузка на одного сотрудника: если до кризиса можно было работать хорошо, чтобы получать на выходе «хорошо», то сейчас приходится работать «отлично», чтобы получать «хорошо» или «удовлетворительно». Мы зависим от внешнего рынка. Сейчас коммерческие партнеры а) не хотят подписывать долгосрочные (годовые) контракты; б) нормальной стала ситуация отказа от предварительных договоренностей: т.е. мы что-то планируем делать в следующем месяце, а по достижении срока клиент отказывается или переносит на более долгий срок. В результате – избыток метаний вида «давай попробуем это или вот еще вот это». Какое-то планирование на два месяца вперед стало нереальным – ситуация (точнее метание в ситуации) меняется от недели к неделе.

разработчик веб-проектов, г. Москва

Я два года занимаюсь развитием собственных веб-проектов. В кризис сильно упали доходы от рекламы, приходится на всем экономить. Хотел на кризис найти временную работу в ИТ (поскольку до смены деятельности я работал сисадмином и сетевым инженером), чтобы совмещать со своим делом, но это оказалось гиблой затеей по многим причинам. Поэтому я сконцентрировал усилия на своем деле…

ИТ-директор, г. Москва

Бюджет закладывался из расчета 25,5 за доллар. Поэтому от некоторых вещей пришлось отказаться. В остальном – все прекрасно.

программист, г. Москва

Упала ЗП и исчезли некоторые сотрудники.

системный администратор, г. Новосибирск

Мне, собственно, написать нечего. Никак кризис на мне не сказался, тьфу-тьфу-тьфу. Наша компания работает, зарплаты никому не снижали, сокращений не проводили, даже магазин новый открываем.

Алексей Барабанов, г. Москва

Вообще никак. Проблемы только у компаний с кредитовым оборотом или у тех, что попали в кризисные отрасли – добывающие (но они просто жировали, а теперь пришли в норму).

Всякие «промывочные» околобюджетные компании не входят в число моих клиентов по той причине, что там деньги делят между своими, а я с 90-х прошлого века никому не плачу откатов. Так что в нормальной экономике для сисадминов КРИЗИСА НЕТ!

инженер-программист, г. Нижний Новгород

Был автопром: сокращение 50% персонала, задержка выплаты даже урезанной з/п. Результат: нашел более «правильную» компанию.

Визитка

АЛЕКСАНДР ЕМЕЛЬЯНОВ, *инженер группы информационных технологий Владимирского филиала ООО «Татнефть-АЗС-Запад»*

Шифруемся на лету
при помощи TrueCrypt

Нередко мы владеем информацией, важность которой очень велика. TrueCrypt — инструмент, позволяющий частично решить задачу защиты данных.

Почему частично? Разберемся в вопросе по порядку. Предположим, у фирмы есть некоторая информация, вызывающая «живой» интерес у конкурентов. Первостепенная задача – не допустить попадание этих данных в руки интересующихся. Не секрет, что в массе своей такими вопросами занимается бдительная служба безопасности. Более того, поскольку значительная часть секретной информации хранится на электронных носителях, а доступ к ней осуществляется посредством компьютеров, СБ в своей работе зачастую плотно взаимодействует с отделом информационных технологий. Однако, как бы четко ни был выстроен комплекс мероприятий по защите от утечек данных, практика показывает, что почти любая система имеет уязвимые места. Попросту говоря, рано или поздно информация может попасть в руки злоумышленников, и, если она хранилась в открытом виде, они без труда смогут ею воспользоваться. Предположение бредовое с той точки зрения, что вероятность возникновения такой ситуации минимальна. Так или иначе оно объясняет причину использования систем шифрования данных уровня предприятия.

Мы немного сузим область рассмотрения, а именно до единичного пользователя компьютера, который также вполне может располагать некоторой конфиденциальной информацией. Тем более что неосторожно забытая или выпавшая из кармана флешка может стать добычей, например, недоброжелателей или вымогателей. Продолжать список примеров можно долго, поэтому предположим, что существуют некоторые данные, которые нужно защитить так, чтобы воспользоваться ими мог только владелец либо доверенное лицо.

Для решения такой задачи существует множество программ шифрования данных. Мы рассмотрим одну из них, которая стоит в первых строках списка лидеров. К тому же подкупает тот факт, что она бесплатна, имеет открытый исходный код и может использоваться на платформах MS Windows, Linux и MacOS (не везде полноценно). В статье речь пойдет о Windows-версии. Даже несмотря на то что речь идет о шифровании, воспользоваться возможностями этого продукта сможет даже мало что смыслящий в криптографии человек. Стоит заметить, однако, что приобретение начальных знаний по предмету лишним не будет.

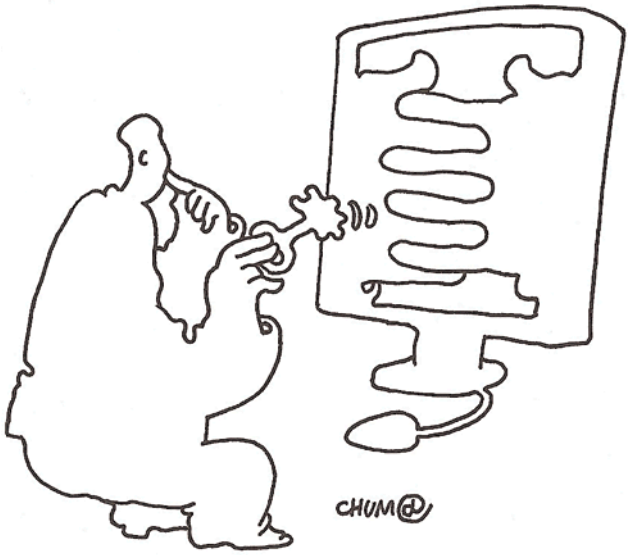
Речь пойдет о программе TrueCrypt. Актуальная версия на момент написания статьи была обозначена номером 6.2. Среди «одноклассников» она позиционируется как инструмент для шифрования данных «на лету». Это означает, что с ее помощью пользователь может зашифровать раздел диска, весь диск, USB-накопитель либо создать отдельный файл-контейнер и, единожды введя пароль, работать с файлами без дополнительных манипуляций. Все операции шифрования будут происходить незаметно для него. Хорошим примером для этого может служить воспроизведение файлов музыкального или видеоформата, которые находятся на зашифрованном диске. Файлы перетаскиваются в плейлист и воспроизводятся так, как будто они находятся на незашифрованном разделе. Понятно, что ничего не мешает помещать в такие разделы любые файлы и работать с ними в режиме on-line, не задумываясь о шифровании.

Процесс обзора TrueCrypt построен следующим образом. Для начала пройдемся по общему функционалу и посмотрим, что ставит данный продукт на ступень выше своих соратников. Затем разберем основные операции по созданию шифрованных контейнеров, разделов и USB-накопителей и работе с ними.

Основные достоинства

Не секрет, что для русского ИТ-сообщества свободное распространение программы будет если не главным, то едва ли не определяющим фактором в выборе «шифровальщика». Однако если эта свобода не будет подтверждаться высокой функциональностью продукта, выбор пользователей вряд ли падет на нее. К TrueCrypt это не относится.

Начнем с того, что она имеет достаточно высокую скорость шифрования данных. Технология параллелизации (parallelization), которая появилась в версии 6.0, дает прирост в скорости при работе TrueCrypt на многопроцессорных системах или многоядерных процессорах. Возрастание скорости шифрования прямо пропорционально количеству процессоров или ядер процессора, а также его тактовой ча-



стоте. То есть при использовании двухядерного процессора скорость приблизительно увеличится вдвое по сравнению с аналогичным одноядерным. Такая же ситуация и с двумя процессорами. Помимо этого, технология конвейеризации (pipelining), которая появилась в версии 5.0, увеличивает быстродействие при работе приложений с файлами, находящимися в зашифрованных разделах (работает только на Windows-системах).

Очень грубо, но для наглядности можно заметить, что по тестам скорости алгоритмов шифрования данных (тест встроен в интерфейс программы) на системе с двумя процессорами Intel Xeon 3,0 ГГц, 4 Гб оперативной памяти (DDR2) и RAID-массивом SAS-накопителей было отмечено десятикратное увеличение показателей по сравнению с машиной, на борту которой находился один процессор Intel Pentium 1800 ГГц, 1 Гб ОП (DDR) и жесткий диск с IDE-интерфейсом.

Пользователь TrueCrypt имеет возможность использовать несколько алгоритмов блочного симметричного шифрования данных на выбор: AES, Serpent и Twofish (во всех размер ключа шифрования составляет 256 бит, размер блока – 128 бит); а также каскады алгоритмов, например, AES-Twofish или даже так – AES-Twofish-Serpent. Однако в случае с каскадным шифрованием будет заметно снижена скорость выполнения операций (это можно проверить с помощью все того же теста скорости алгоритмов шифрования TrueCrypt).

Еще одну интересную черту TrueCrypt разработчики назвали Plausible deniability. В переводе на русский звучит как «правдоподобное отрицание». Дело в том, что программа умеет создавать скрытые контейнеры внутри зашифрованных (и даже скрытую операционную систему). Таким образом, после монтирования тома скрытый контейнер остается невидимым. Как это использовать, каждый для себя решит сам. О том же, как создать такой контейнер, пойдет речь дальше. Помимо всего прочего, файлы, созданные при помощи TrueCrypt, не связываются с программой, и определить их происхождение невозможно, так как в заголовке они содержат набор случайных данных.

TrueCrypt никогда не сохраняет промежуточные данные на диск, все хранится в оперативной памяти. Это гарантирует отсутствие доступа к ключам, которые могли храниться во временных файлах. Но, как оказалось, и эта мера не совсем надежна. Примерно год назад группа ученых Принстонского университета показала, как можно получить доступ к данным, хранящимся в оперативной памяти. Желающие могут ознакомиться с материалами на сайте университета [1].

Ну и вдобавок ко всему хочется отметить, что TrueCrypt не восприимчива к атакам «грубой силой», имеется возможность двойной защиты доступа к данным и использования токенов и смарт-карт для размещения ключа.

Установка программы

Этот процесс вряд ли у кого вызовет затруднения. Правда, есть один нюанс, о котором нужно сказать отдельно. Дело в том, что программа может быть установлена в двух разных режимах. В режиме инсталляции вместе с программой в систему устанавливается драйвер TrueCrypt. Это нужно для операции шифрования системного раздела, а также для возможности работы с контейнерами TrueCrypt в контексте пользователя, не имеющего прав администратора (об этом далее). В режиме, который называется traveler mode, программа копирует свои файлы в заданную вами папку. Таким образом, установленный TrueCrypt можно переносить на съемном носителе и использовать на любой системе. Однако в этом случае нет возможности шифрования системного диска.

Для того чтобы русифицировать TrueCrypt, стоит всего лишь скачать файл локализации с сайта разработчика [2] и поместить его в каталог с программой.

Создание зашифрованного контейнера

Для того чтобы вы могли переносить свои файлы в зашифрованном виде и использовать их на разных машинах, вам нужно создать файл-контейнер TrueCrypt. Итак, открываем программу и нажимаем «Создать том». Далее следуем указаниям «Мастера создания томов». Отмечаем, что мы

хотим создать обычный том TrueCrypt, его название и расположение. Вот здесь хотелось бы сделать небольшую ремарку. Дело в том, что TrueCrypt все равно, как вы назовете файл, программа сама определит при попытке смонтировать раздел, ее это детище или нет. Поэтому для большей скрытности вы можете назвать ваш контейнер хоть «Любимое кино моей бабушки.avi». Идем дальше. Выбираем алгоритм шифрования данных и хеш-алгоритм, который используется генератором случайных чисел (RNG, Random Number Generator) TrueCrypt для создания ключей, а также функцией деривации ключа заголовка (header key derivation function). Далее определяем размер контейнера, вводим пароль и, если необходимо, указываем путь к ключевому файлу (keyfile, его первые 1,048,576 бит смешиваются с паролем для повышения криптостойкости). В качестве такого файла можно использовать любой, имеющийся на вашем жестком диске, либо создать произвольный при помощи TrueCrypt. Тут стоит оговориться, потому что вы можете указать даже путь к целой папке, и тогда все файлы в ней будут ключевыми. Однако при утере хотя бы одного ключевого файла доступ к зашифрованному контейнеру будет невозможен. Далее нужно выбрать тип файловой системы для тома TrueCrypt и размер кластера (как правило, остается по умолчанию). Жмем «Разметить» и по истечении некоторого времени создание контейнера завершено. Файл-контейнер будет содержать произвольные данные, которые будут затираться по мере копирования файлов вовнутрь контейнера и вновь появляться, если будет освобождаться место внутри него при операции удаления файлов.

Для доступа внутрь контейнера в окне программы выбираем его, нажав «Файл» и в окне выше из списка доступных букв выбираем необходимую и жмем «Смонтировать». Вводим пароль и указываем путь к ключевым файлам, если они используются. Контейнер монтируется как том Windows, и с данными можно работать, как если бы они находились на обычном логическом разделе.

Чтобы создать скрытый раздел внутри зашифрованного контейнера, нужно также запустить мастер и выбрать «Скрытый том TrueCrypt». Сначала мастер предложит создать обычный том, а затем внутри него скрытый, проведя два раза один и тот же перечень операций по выбору параметров. В качестве файловой системы для внешнего контейнера (обычного тома) будет рекомендовано выбрать FAT из-за особенности размещения служебных данных на томах NTFS.

Для доступа внутрь скрытого контейнера нужно выбрать основной носитель – обычный том. И в окне ввода пароля указать пароль, который был введен при настройке скрытого тома. Тем самым будет смонтирован скрытый том как том Windows.

При работе с контейнером, имеющим внутри скрытый том, есть вероятность перезаписи данных при нехватке места на внешнем томе и повреждения информации внутри скрытого раздела. Чтобы не допустить этого, при монтировании обычного тома TrueCrypt в окне ввода пароля нужно в параметрах указать, что скрытый том нужно защитить, затем ввести пароль доступа к нему и не переживать за сохранность лежащих внутри данных.

Для полной дешифровки файлов, находящихся внутри зашифрованного раздела, необходимо скопировать их в любое свободное место на жестком диске, а контейнер просто удалить.

Важной особенностью при работе с контейнерами TrueCrypt является следующее. Для выполнения операций шифрования/дешифрования нужен специальный драйвер TrueCrypt, использование которого для обычного пользователя невозможно, если только система не установлена на компьютере. Поэтому ни установить, ни использовать TrueCrypt в режиме traveler mode пользователь без привилегий администратора не сможет.

Шифрование разделов

Для начала рассмотрим шифрование несистемного раздела. Делается это при помощи того же мастера. Весь процесс похож на создание файла-контейнера. Только вместо файла указывается раздел, который нужно зашифровать, и далее параметры шифрования. Отмечу, что шифрование раздела с данными без их удаления поддерживается только в Windows Vista. В случае с Windows XP нужно будет предварительно сделать резервную копию файлов целевого тома. Затем зашифровать раздел и скопировать на него файлы.

Рисунок 1. Основное окно управления TrueCrypt

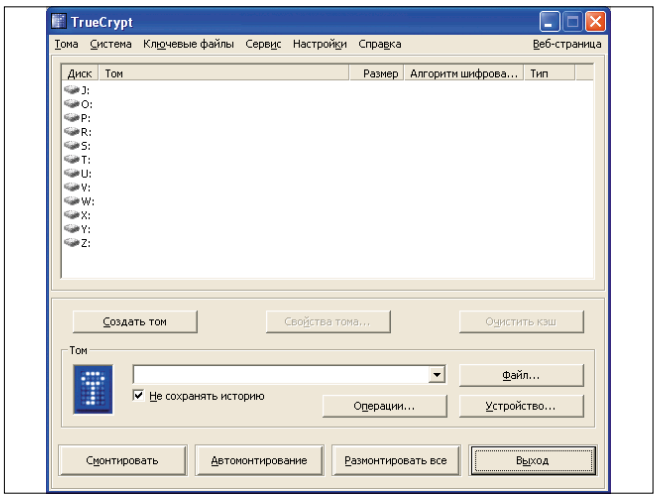
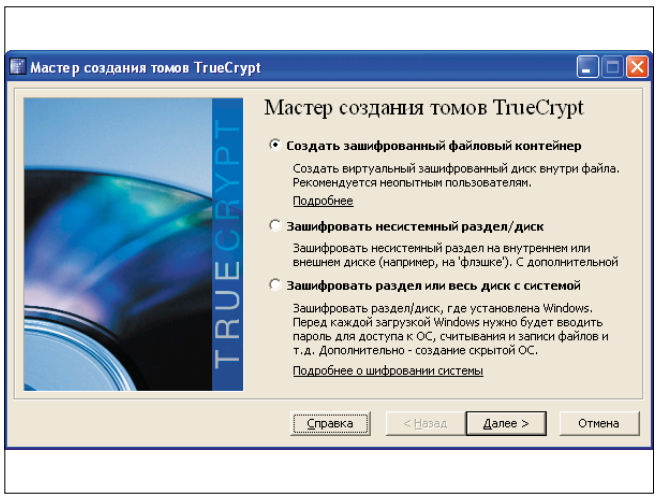


Рисунок 2. Мастер создания томов TrueCrypt



По аналогии с контейнерами внутри такого зашифрованного раздела можно создать скрытый том.

После шифрования раздел по назначенной ему Windows букве диска доступен не будет, более того, для секретности вы можете ее вовсе удалить. Чтобы работать с зашифрованным разделом, нужно в главном окне TrueCrypt выбрать его как устройство, назначить букву и смонтировать.

Что касается шифрования системы, то сделать это можно лишь с ОС семейства Windows, начиная с Windows XP. Можно зашифровать как весь системный диск (жесткий диск, на котором находится системный раздел), так и отдельно раздел, где находится система. Первый вариант возможен только в Windows Vista, и мы оставим его изучение для ее любителей. Единственное замечание нужно сделать вот о чем. Extended-разделы после проведения операции шифрования перестают быть видны в системе, и, чтобы добраться до данных, лежащих на них, необходимо будет перманентно расшифровать системный диск. Не очень удобно. Однако разработчики обещают в скором времени устранить эту неприятную особенность.

Процесс шифрования системного раздела несколько сложнее, чем операции, описанные в предыдущих параграфах. И выполняться он будет в два этапа. Первый – этап подготовки. Пользователь должен будет указать обычный или скрытый раздел, который он хочет создать (именно так TrueCrypt позволяет создать скрытую операционную систему), параметры шифрования, а также количество операционных систем, установленных на вашем компьютере (мы рассмотрим вариант с одной ОС), после чего программа создаст образ диска восстановления. Его необходимо, не прерывая работы мастера, записать на диск. После успешной проверки создания такого диска нужно будет перезагрузить машину и загрузиться с него. Далее вводим пароль, который указали в параметрах шифрования, и, если все прошло удачно, TrueCrypt приступит ко второму этапу – непосредственному шифрованию системы, причем во время этого можно делать что угодно на компьютере. Более того, процесс можно приостановить и продолжить позже или даже после перезагрузки компьютера, система будет оставаться частично зашифрованной. Помимо этого, после загрузки BIOS управление будет передаваться загрузчику TrueCrypt. Приятной возможностью является то, что пользователь сам может указать, что будет выводиться на экран после загрузки BIOS. Можно даже написать что-то вроде «DISK BOOT FAILURE, INSERT SYSTEM DISK AND PRESS ENTER», тем самым имитируя отсутствие системы как таковой. Однако после ввода пользователем валидного пароля система продолжит загрузку.

Вернемся к диску восстановления. Нетрудно догадаться, что он привязан именно к той сессии шифрования, в которую он был создан, и не является универсальным. Он поможет в случае, когда поврежден мастер-ключ либо заголовок тома. С его помощью также можно перманентно расшифровать системный том, если у вас появились проблемы с загрузкой Windows и вы хотите провести операцию восстановления. Однако все это возможно, если вы помните правильный пароль для доступа к зашифрованному системному разделу.

Процесс создания скрытого системного раздела с установленной в нем операционной системой в рамках этой статьи мы рассматривать не будем. Желающие могут ознакомиться с достаточно подробной документацией на сайте разработчика.

Шифрование USB-накопителя

Честно говоря, эта операция мало чем отличается от создания зашифрованного несистемного диска. В списке устройств на этапе настройки нужно найти свою флешку и выполнить ее шифрование. Однако замечу, что более удобным в этом случае является размещение на USB-накопителе TrueCrypt в режиме traveler mode и создание на нем файла-контейнера. Таким образом, мы получим возможность доступа к зашифрованным данным на любой системе, даже где не установлен TrueCrypt.

В заключение, рассмотрев основной функционал программы, ответим на вопрос, поставленный в начале статьи. TrueCrypt шифрует данные, находящиеся на носителях информации. Однако она не может шифровать ICQ-трафик или сообщения электронной почты (хотя ничто не мешает при этом пересылать контейнеры TrueCrypt как вложения), а также не имеет функций для создания ЭЦП (электронно-цифровой подписи).

Недостатки TrueCrypt

Помимо всего прочего, нужно отметить, что программа имеет некоторые недостатки. Во-первых, это ориентированность на Windows-системы – многие функциональные возможности, как было отмечено выше, работают только в ОС Windows (кстати, из-за своей неоднозначной лицензии TrueCrypt была выведена из состава многих Linux-дистрибутивов). Во-вторых, нет возможности изменения размера контейнера, к тому же операция дешифрования несистемного раздела далеко не тривиальна и требует некоторых манипуляций с файлами. В-третьих, программа не имеет встроенного генератора паролей и допускает использование пользователем простых паролей. В-четвертых, при хранении данных в контейнерах TrueCrypt существует вероятность полной потери данных вследствие удаления файла-контейнера. Ну и, в-пятых, отмечу одну особенность, которая кому-то может послужить на пользу, а кому наоборот. Дело в том, что в многопользовательской среде (терминальный режим) смонтированный том TrueCrypt будет виден и доступен для всех пользователей без исключения, избежать доступа к нему можно использованием разрешений NTFS. Та же ситуация повторится при смене пользователя на системах Windows, начиная с версии Windows XP. Кстати говоря, основные проблемы и ограничения программы указаны на сайте разработчика. Этот список корректируется, если выявляются новые недочеты либо устраняются уже известные.

Несмотря на все это, такой инструмент, как TrueCrypt, будет полезен тем, кто хочет защитить свои данные от взлома и не позволить себя скомпрометировать.

Разъяснения многих понятий и терминов криптографии, а также некоторая информация касательно функционала программы (например, использование токенов и смарт-карт) не вошли в статью. Обо всем этом можно почитать в специальной литературе, а также на официальном сайте TrueCrypt. EOF

1. http://citp.princeton.edu/memory.
2. www.truecrypt.org.

Визитка

АНДРЕЙ ЛУКОНЬКИН, ведущий инженер-программист ОАО «НижегородАвтоДор». Занимается автоматизацией производства, бухгалтерского, управленческого и кадрового учета

Управляемое приложение

Первые осторожные шаги

Какие сюрпризы готовят нам разработчики управляемого приложения? На примере небольшой конфигурации попробуем освоить новые возможности платформы.

Изучать новую платформу можно и по демонстрационной конфигурации, но гораздо интереснее и эффективнее сделать что-то своими руками. Для этого я скопировал имеющуюся самописную конфигурацию по учету компьютерной техники (про неё подробно расскажу после окончания работ над функционалом) в отдельный каталог и запустил её в режиме конфигуратора на новой платформе. Для работы базы данных в управляемом приложении требуется конвертация, поэтому на вопрос «Произвести конвертацию информационной базы» отвечаем утвердительно и ждем окончания процесса.

Можно работать с программой в обычном режиме, как и работали раньше на платформе 8.1. Для этого есть соответствующие настройки: в свойствах дерева конфигурации есть параметр «Основной режим запуска» и в прочих настройках пользователя поле «Режим запуска». Для наглядности я создал в базе двух пользователей, отличающихся только режимом запуска – «ОбычноеПриложение» и «УправляемоеПриложение».

Прежде чем продолжить, обратимся к теории. Формы в управляемом приложении не прорисовываются детально, а описываются разработчиком с помощью определения состава, поведения и расположения элементов. И уже на основе этого логического описания система автоматически создаст форму. Структура элементов описывает внешний вид формы, а функциональность описывается в виде реквизитов и выполняемых действий.

Проверить это можно, запустив программу сначала под одним пользователем, затем под другим. При открытии какого-либо справочника (у меня это справочник «Компьютеры») очевидны различия (см. рис. 1). У пользователя «ОбычноеПриложение» справочник выглядит так же, как и раньше, а вот у пользователя «УправляемоеПриложение» форма справочника вытянута по вертикали, все элементы располагаются один под другим, т.е. работу в таком виде продолжать нельзя. Что же делать?

В конфигураторе в справочнике создадим еще одну форму элемента, назовем её УправляемаяФорма, обязательно

Рисунок 1. Управляемая форма, созданная платформой автоматически

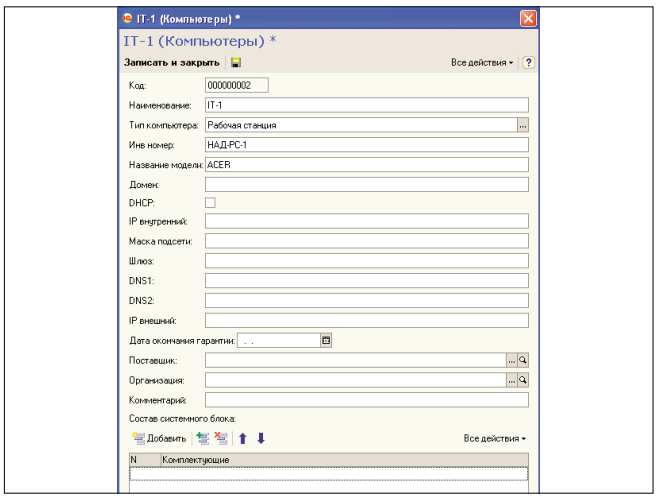
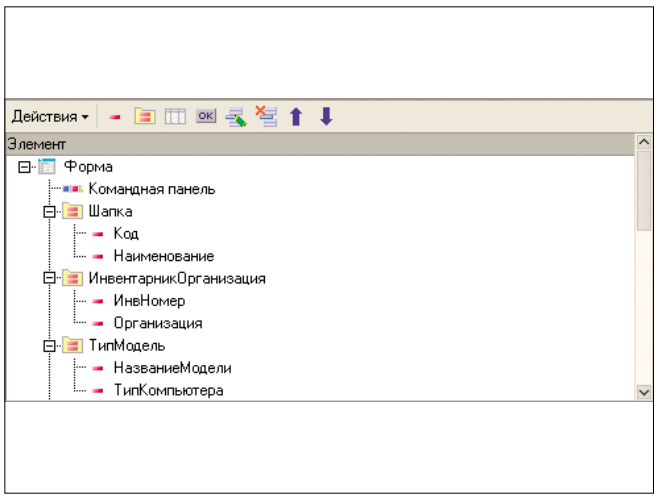
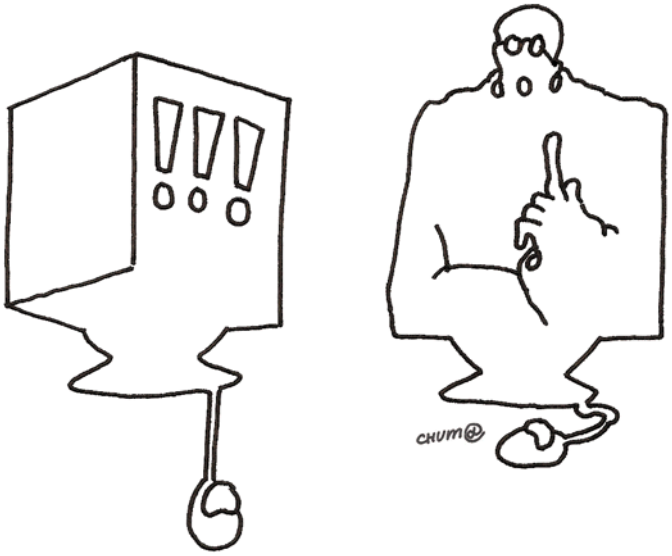


Рисунок 2. Окно управление элементами формы





установив тип формы как управляемая. Пока нас интересует только управление расположением реквизитов, чтобы форма получилась удобочитаемой. Здесь мы можем объединять несколько реквизитов в группу, и для этой группы задавать некоторые параметры.

Например, если мы хотим, чтобы код и наименование находились в одной строке, а не друг под другом, то создадим группу «Шапка» и поместим код и наименование в неё. Затем изменим в свойствах группы значение параметра «Группировка» на «Горизонтальная». В нижнем окне сразу можем видеть результат наших изменений – код и наименование справочника теперь располагаются рядом.

Можно объединить некоторые реквизиты по логическому принципу не только в виртуальную группу, но и выделить их на форме. Для этого используется свойство группы «Отображение». В нашем случае мы объединим сетевые настройки компьютера в рамку (см. рис. 2).

На рис. 1 видно, что все реквизиты одной длины и привязаны к краю формы. Я использовал свойства реквизита «Ширина» и «РастягиватьПоГоризонтали» для более удобного расположения, то есть фактически управление расположением происходит не интерактивно, а описательно, с помощью задания неких параметров.

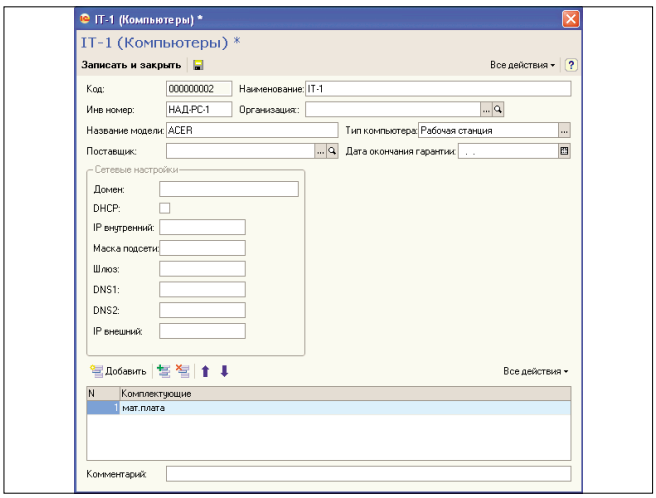
Таким образом, объединяя в группы, расставляя в нужном порядке, задавая размеры и способы привязки по вертикали и горизонтали, мы получаем форму нужного вида, которая будет отображаться для пользователя «УправляемоеПриложение».

Теперь возникает вопрос – какая форма будет основной? Так как пользователям может назначаться один из двух вариантов работы, то соответственно и основные формы задаются для каждого из двух режимов. Для управляемого приложения основные формы задаются в закладке «Основные» (указываем форму элемента «УправляемаяФорма»), для обычного режима работы в закладке «Дополнительные» (указываем форму элемента «ФормаЭлемента»). Теперь при входе в систему пользователя «ОбычноеПриложение» справочник будет выглядеть так же, как и раньше, на платформе 8.1, а при входе пользователя «УправляемоеПриложение» будет такой, какой она показана на рис. 3. Следующим важным шагом будет распределение объектов метаданных по подсистемам. Если раньше это разделение было больше для разработчиков, то в управляемом приложении оно отражается непосредственно на работе пользователей. При этом структура подсистем не обязательно одноуровневая, можно создавать вложенные схемы.

Создание подсистем влияет не только на визуальный интерфейс при работе пользователей, но также этот процесс важен при использовании хранилища конфигурации (лично я сторонник использования хранилища даже в тех случаях, когда с программой работает один программист). Дело в том, что в управляемом приложении реализована возможность захвата в хранилище конфигурации отдельной подсистемы, что повышает удобство работы программиста.

В статье затронута лишь небольшая часть работы с интерфейсом, но именно описанные выше действия необходимы для дальнейшего ознакомления с новыми возможностями системы. EOF

Рисунок 3. Управляемая форма с заданными настройками параметров



Визитка

ИВАН ПАНИН, инженер по технической информационной безопасности.
Сфера интересов: сетевые технологии, защита информации

WebVPN
на базе Cisco IOS

Технология WebVPN организует эффективное VPN-взаимодействие, позволяющее мобильным сотрудникам получить доступ к корпоративным ресурсам.

VPN (Virtual Private Network – виртуальная частная сеть) – логическая сеть, создаваемая поверх другой сети. За счёт шифрования создаются закрытые каналы. Технология совместима с любым обозревателем, поддерживающим SSL. В условиях современного бизнеса VPN является незаменимым решением в плане эффективности мобильного доступа, безопасности и экономической целесообразности.

На рис. 1 представлена схема подключения мобильных сотрудников к корпоративными ресурсам. Для организации безопасного соединения используется Secure Socket Layer (SSL) Protocol и Transport Layer Security (SSL/TLS1). В качестве WebVPN [2] шлюза можно использовать возможности Cisco IOS, Cisco VPN 3000 Concentrator или Cisco ASA. В процессе работы используется сертификат, в отличие от обмена ключами, используемого в IPSec.

Модели удаленного доступа

Существуют три модели удаленного доступа:

- Clientless SSL VPN (WebVPN);
- Thin Client SSL VPN (Port Forwarding);
- SSL VPN Client (SVC-Full Tunnel Mode).

Clientless SSL VPN (WebVPN)

Доступ к преднастроенным URL-ссылкам через портал к внутренним интранет-веб-сайтам компании.

Common Internet File system (CIFS). Позволяет удаленным пользователям обозревать и получать доступ к файлам, расположенным на Windows-based-серверах в корпоративной сети.

Thin Client SSL VPN (Port Forwarding)

Позволяет удаленным пользователям запускать клиентские приложения на их ПК через шифрованное соединение в корпоративной сети.

SSL VPN Client (SVC-Full Tunnel Mode)

Посредством установки клиента WebVPN удаленный компьютер становится частью корпоративной сети.

Cisco Secure Desktop. Дополнительно к SSL VPN (Full Tunnel) устанавливается клиент защищенного рабочего стола Secure Desktop.

Первый этап настройки шлюза WebVPN на базе IOS: подготовка

```
! Задействуем модель контроля доступа AAA
aaa new-model

! Создаем учетную запись пользователя в локальной базе
! данных, также можно использовать внешнюю аутентификацию,
! например, TACACS- или RADIUS-сервер
username user01 privilege 0 secret 0 cisco221

! Задействуем аутентификацию для локальных пользователей
aaa authentication login default local

! DNS-настройки для WebVPN-шлюза: имя хоста, домен
! и сервер имен
hostname router01
ip domain name company.ru
ip name server 192.168.1.3
```

Создание доверительного сертификата

WebVPN основан на SSL, поэтому должен быть создан сертификат X.509: Public Key Infrastructure (PKI). При подключении клиента сертификат будет проверяться политикой безопасности на соответствие имени и IP-адреса WebVPN-шлюза, поэтому самоподписанный сертификат, создаваемый маршрутизатором по умолчанию при «включении» WebVPN, не подойдет. Перед созданием сертификата необходимо проверить время, дату и временную зону на маршрутизаторе.

```
! Обьявляем удостоверяющий центр
! (Certification Authority, CA)
crypto pki trustpoint router01.company.ru
! Подписываем
 enrollment selfsigned
! Общая информация, главное здесь - каноническое имя:
! CN, совпадающее с записью A на DNS-сервере
 subject-name cn=router01.company.ru, ↵
        o=JSCCompany,c=RU,st=AltayTerritory
 rsakeypair router01.company.ru
! Генерируем сертификат
```


```
crypto pki enroll router01.company.ru
```

Теперь сертификат готов, его можно посмотреть при помощи команды:

```
#show crypto pki certificates
```

Создаем пул динамических адресов для WebVPN-клиентов:

```
ip local pool ssl-vpn-client-dynpool 10.10.1.5 10.10.1.20
```

Второй этап: настройка WebVPN

На рис. 2 изображена концепция WebVPN, представляющая собой три базовых блока. Контекст, по сути, является контейнером, содержащим все параметры для подключения клиентов.

Сначала необходимо создать виртуальный шлюз, указать имя, хост, IP-адрес, назначить перенаправление порта с HTTP на HTTPS, если задействован HTTP-сервер. Также здесь указываем использование созданного нами ранее удостоверяющего центра сертификатов.

Шлюз работает подобно proxy, для защиты корпоративных ресурсов.

```
webvpn gateway WebVPNGateway
 hostname router01
 ip address 172.16.1.1 port 443
 http-redirect port 80
 ssl trustpoint router01.company.ru
 ! Определяем алгоритм шифрования для SSL-протокола,
 ! также доступны aes-sha1 и rc4-md5
 ssl encryption 3des-sha1
 ! Ведение журнала ошибок и событий
 logging enable
 ! Задействуем WebVPN-шлюз
 inservice
```

Копируем AnyConnect или SSLClient-клиент и Secure Desktop на маршрутизатор, например, при помощи TFTP-сервера и устанавливаем[1]. Можно установить до 9 клиентов, например, для поддержки разных операционных сис-

Рисунок 1. Топология WebVPN

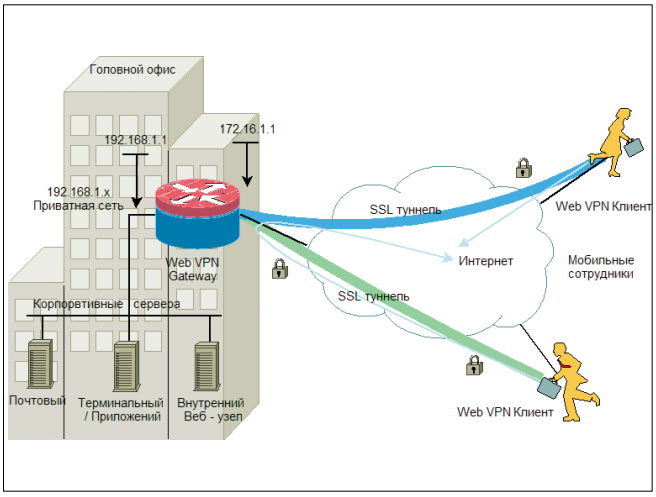
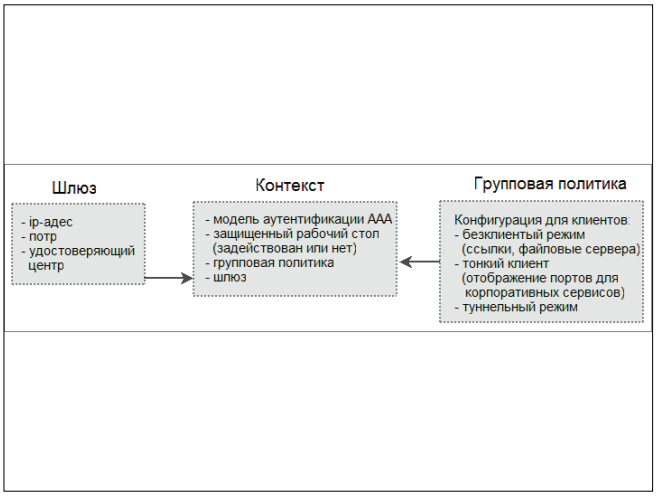


Рисунок 2. Концепция WebVPN



тем. Порядок загрузки определяется параметром sequence <number>.

При подключении клиент выбирается автоматически, в зависимости от типа ОС.

```
webvpn install svc flash:/anyconnect-win-2.x.pkg sequence 1
webvpn install svc flash:/anyconnect-macosx-i386-2.x.pkg ↵
       sequence 2
! Клиент для Windows CE, подходит для Mobile,
! т.к. они основаны на CE
webvpn install svc flash:/anyconnect-wince-ARMv4I-2.x.pkg ↵
       sequence 3
webvpn install svc flash:/anyconnect-linux-2.x-k9.pkg ↵
       sequence 4
webvpn install csd flash:/securedesktop-ios-3.x-k9.pkg

! После в конфигурации появятся строки:
webvpn install svc flash:/webvpn/svc_1.pkg sequence 1
webvpn install svc flash:/webvpn/svc_2.pkg sequence 2
webvpn install svc flash:/webvpn/svc_3.pkg sequence 3
webvpn install svc flash:/webvpn/svc_4.pkg sequence 4
webvpn install csd flash:/webvpn/sdesktop.pkg

! Для быстрой коммутации IP-пакетов необходимо включить
! Cisco Express Forwarding (CEF)
 webvpn cef
```

Далее создается WebVPN-контекст, который необходим для ассоциации шлюза и индивидуальных настроек, т.к. существует возможность для создания множества контекстов с различными уровнями доступа в зависимости от указанного домена.

```
webvpn context SSLVPN
 ! Заголовок и сообщение на странице аутентификации
 ! портала, оформление
 title "Router01 Web-VPN page Welcome!"
 title-color #CCCC66
 secondary-color white
 text-color black
 logo file flash:/company.gif
 login-message "Please enter your credentials.."

 ! Ограничение на число одновременных WebVPN-сессий
 max-users 150

 ! Режим проверки сертификата
 ssl authenticate verify all
 ! Здесь можно задействовать Cisco Security Desktop
 csd enable
```

Создаем список HTTP-ссылок, доступных в портале (если будет разрешен групповой политикой).

```
url-list "Links"
  heading "QuickLinks"
  url-text "WebMail" url-value "mail.company.ru"
  url-text "SharePoint" url-value "wss.company.ru"
  url-text "CRM" url-value "crm.company.ru"
```

Создаем список Windows-based-файловых серверов. Один из серверов должен быть назначен как master, в роли основного локального «браузера домена» обычно выступает контроллер домена, выполняющий регистрацию имён компьютеров в сети и преобразование имен в IP-адреса, т.к. при обращении к сетевым ресурсам будут использоваться NetBIOS-имена, а не полные DNS.

```
 nbns-list "NBNS-Servers"
 nbns-server 192.168.1.4 master
 nbns-server 192.168.1.5 timeout 10 retries 5
```

Создаем список ссылок на сетевые папки:

```
cifs-url-list CIFS-List
heading Share-list
url-text "Public_on_Server01" url-value \\server01\public
url-text "Sales_on_Server01" url-value \\server01\sales
```

Конфигурация тонкого клиента (Port Forwarding)

Список портов для приложений, которые отображаются (mapping) на локальные порты хоста клиента.

```
port-forward "Portlist"
  local-port 30025 remote-server "192.168.1.2" ↵
       remote-port 25 description "SMTP"
  local-port 30143 remote-server "192.168.1.2" ↵
       remote-port 143 description "IMAP"
  local-port 30022 remote-server "192.168.1.3" ↵
       remote-port 3389 description "RDP"
```

Групповая политика настраивается отдельно для каждого экземпляра WebVPN, содержит набор параметров, ассоциированных с контекстом. Здесь определяется, будет ли доступ к файлам по CIFS, задействован «безопасный рабочий стол», режим тонкого клиента и полно-туннельный режим.

Рисунок 3. Аутентификация

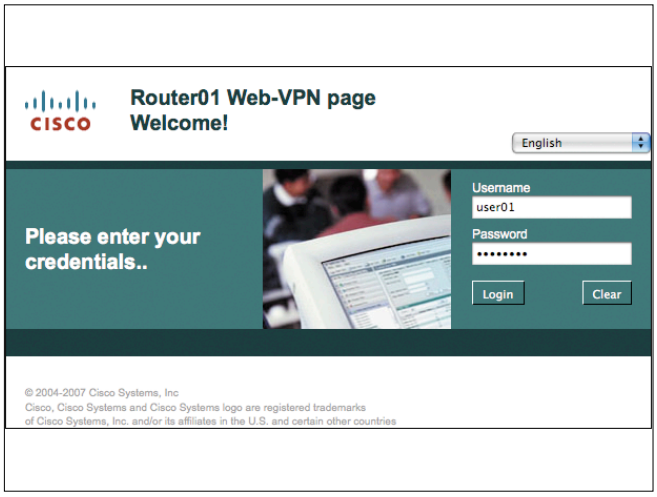
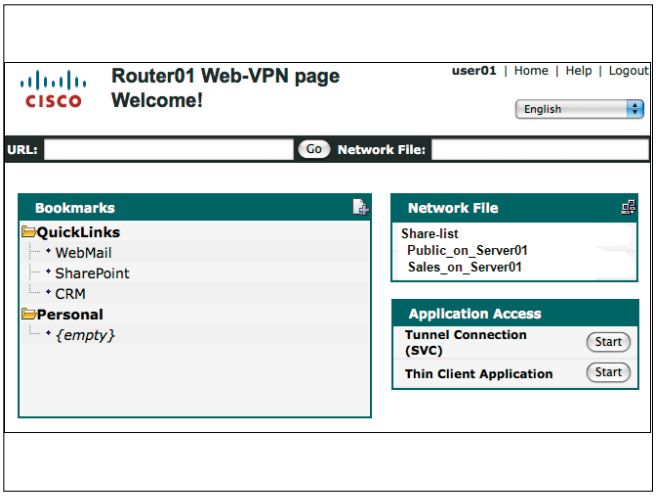


Рисунок 4. Навигация



```
policy group SSL-Policy
  ! Ассоциируем созданный ранее набор ссылок «Links»
  ! с групповой политикой
  url-list "Links"
  ! Кнопка для запуска тонкого клиента (в портале), также
  ! можно настроить автозапуск Java-апплета сразу после
  ! успешной аутентификации путем добавления ключа
  ! auto-download
  port-forward "Portlist"
  ! Разрешаем доступ к списку файловых серверов с указанием
  ! прав доступа
  nbns-list "NBNS-Servers"
  functions file-access
  functions file-browse
  functions file-entry
  ! Ассоциируем созданный ранее набор ссылок сетевых папок
  ! «CIFS-List» с групповой политикой
  cifs-url-lis "CIFS-List"
  ! Кнопка туннеля (в портале)
  functions svc-enabled
  ! Сообщение после успешной аутентификации на портале
  banner "JSC Company, support: <admin@company.ru>"
  ! Простой и продолжительность сессии в секундах
  timeout idle 1800
  timeout session 36000
  ! Сетевые настройки для VPN-клиентов
  svc address-pool "ssl-vpn-client-group-dynpool"
  svc default-domain "company.ru"
  svc dns-server primary 192.168.1.4
  svc wins-server primary 192.168.1.4
  svc default-domain company.ru
  ! Сохраняем установленный SVC-клиент на компьютере
  ! пользователя, в противном случае после завершения
  ! сеанса будет автоматически деинсталлирован
  svc keep-client-installed
```

Ассоциация групповой политики с контекстом

Данная политика будет использоваться по умолчанию до тех пор, пока не будут настроены атрибуты AAA сервера для запроса другой политики.

```
default-group-policy SSL-Policy
! Ассоциация шлюза с контекстом
gateway WebVPNGateway
! Задействуем конфигурацию контекста
inservice
```

Настройка WebVPN закончена. Информацию о контексте и шлюзе можно посмотреть при помощи команд:

```
#sh webvpn context <name>
#sh webvpn gateway <name>
```

Дополнительные параметры настройки контекста, шлюза и групповой политики доступны по адресу [4].

Подключение мобильного пользователя

На рис. 3 представлена заглавная страница портала, на которой необходимо пройти аутентификацию. На рис. 4 представлена домашняя страница: навигация. На которой в соответствии с групповой политикой доступны «быстрые» ссылки к корпоративным ресурсам, доступ к файлам по CIFS (при доступе запрашиваются имя и пароль доменной учетной записи), режим тонкого клиента и полнотуннельный режим.

При выборе туннельного режима будет предложено принять сертификат и загрузить VPN-клиент, после чего установится соединение, значок состояния располагается в трее.

При выборе режима «Тонкий клиент» будет загружен Java-апплет и представлена таблица отображения портов удаленных сервисов на локальный компьютер. На удаленном клиенте должна быть предустановлена Java Runtime Environment (JRE) версии 1.4 или выше. Также хочу отметить, что ни тонкий, ни толстый клиенты не заработали на Windows XP и Vista (установленных с фирменных дисков), пока ОС не были обновлены.

SSLClient или AnyConnect-Client

Выбор клиента осуществляется на этапе {1}. AnyConnect является Next Generation-поколением WebVPN-клиента. Несмотря на поддержку маршрутизаторами, разрабатывается в основном для Cisco Adaptive Appliances (ASA) серии 5500. Перечень маршрутизаторов, поддерживающих описанную технологию, вы найдете по адресу [2].

Вариантом установки может быть как загрузка с портала, так и предустановленный вариант. В отличие от SSLClient, поддерживаются не только ОС Windows, но и Linux, MacOS, мобильные устройства на базе Windows Mobile/CE. Перечень ОС, поддерживаемых AnyConnect, доступен по адресу [3]. Были и совмещенные версии SSL-Client-AnyConnect, но поддержка SSLClient прекратилась в начале 2008 года, поэтому нужно использовать AnyConnect. О режиме защищенного рабочего стола в статье речь не идет, т.к. поддержка также остановлена и развивается только для ASA. После установки на компьютере пользователя остается клиент, который можно запустить без интернет-обозревателя, в то время как SSLClient не может запускаться отдельно.

Особенностью решения по сравнению с альтернативным EasyVPN (описанным в статье [1]) является работа по протоколу HTTPS, который доступен всегда, в отличие от специфичных портов, используемых для подключения EasyVPN. WebVPN позволяет управлять доступом, например, указать URL или сервис, к которым может обращаться пользователь. Тем самым снижается риск доступа к внутренним сетевым ресурсам с незащищенных клиентов или из недоверенных сетей. EOF

1. Панин И. Корпоративные VPN на базе Cisco. //Системный администратор, №6, 2009 г. – С. 78-84.
2. Thin-Client SSL VPN (WebVPN) IOS Configuration – http://www.cisco.com/en/US/products/ps6496/products_configuration_example09186a008072aa61.shtml.
3. Cisco AnyConnect VPN Client – http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect23/release/notes/anyconnect23rn.html.
4. Other Security Features – SSL VPN http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_ssl_vpn.html.

Таблица 1. Сравнительная характеристика режимов работы WebVPN

Clientless Mode	Thin-Client Mode	Tunnel Mode
Поддержка веб-приложений Файловые ресурсы по CIFS	Использование Java-апплета TCP port mapping: Telnet, e-mail, приложения на статических портах	Работает подобно IPsec VPN Загружается через Java или ActiveX Поддерживаются все IP приложения Для установки клиента требуются административные права, перезагрузка компьютера не требуется Защищенный рабочий стол

Понять Билла

Говорят, что понять человека — значит его принять. Когда речь заходит о Билле Гейтсе, на это способен далеко не каждый

Михаил Гаков

Билл Гейтс – не только создатель легендарной компании Microsoft и самого продаваемого продукта на рынке компьютерного софта. Он – еще и самая противоречивая фигура в мире бизнеса, вызывающая у одних приступы почти религиозного экстаза, а у других – столь же иррациональной ярости. Иначе чем объяснить, что огромное число людей, ежедневно пользуясь системой Windows, вдруг восприняли название культового фильма Тарантино «Убить Билла» исключительно по-своему? Понятно, какого Билла.

Трудновоспитуемый вундеркинд

Жизнь главного «везунчика» в мире бизнеса неизбежно окружена мифами, легендами, преувеличениями и откровенными передержками. И сегодня стоит попытаться оценить «сухой остаток»: что успел сотворить за свой «полтинник» хорошего и не очень?

Самый богатый человек в мире (по версии Forbes), входящий в сотню самых влиятельных людей XX века и полусотню представителей киберэлиты (по версии журнала Time), многократный человек года и CEO года, почетный доктор пяти университетов (включая знаменитый Гарвардский), рыцарь-командор Ордена Британской империи, кавалер высших орденов ряда стран и прочая и прочая родился 28 октября 1955 года в Сиэтле (штат Вашингтон). С родословной у Уильям Генри Гейтса III все сложилось, как надо: отец – преуспевающий адвокат, мать – член совета директоров банка, дед – вице-президент Национального банка, прадед – мэр Сиэтла. В своих мечтах родители видели отпрыска тоже адвокатом.

Впрочем, начало его биографии никаких особенных взлетов не сулило, скорее наоборот – обещало одни неприятности. В школе Билл учился неважно, не помогла и семейная система кнута (порка отцовскими подтяжками) и пряника (25 центов за каждую положительную оценку). Родители даже сводили непутевого сына к психотерапевту, но все тщетно – будущий бизнес-гений не желал учиться.

Все изменилось в восьмом классе, когда родительский комитет подарил школе в Лейксайде, где учился Билл, компьютер производства компании General Electric. Тогда еще, разумеется, ни о каких «персоналках» речь не шла – в школе были установлены лишь терминал с телетайпом, соединенные с большой машиной, находившейся в другом месте, плюс выдана некая квота машинного времени. И юный Билл Гейтс вместе с закадычным другом Полом Алленом «запали» на новинку. Они сбегали с уроков, просиживали у терминала ночи напролет и все выходные.

Известно, что в 13 лет Билл Гейтс написал свою первую компьютерную программу на языке BASIC – для игры в крестики-нолики. А когда квота на машинное время истекла, тинейджер вместе с такими же продвинутыми компьютерными фанатами переключился на другие ЭВМ, имевшиеся в городе. Вскоре, правда, Билла с Полом и еще двух «мушкетеров» из Лейксайдской школы от этих машин отключили за то, что смышленые подростки ухитрились добывать халявное время с помощью обнаруженных «дыр» в тогдашних программах! Правда, позже владельцы компьютеров сменили гнев на милость и предложили юным «хакерам», наоборот, выявлять аналогичные попытки несанкционированного доступа к тер-

миналам в обмен на драгоценное машинное время.

В 1970 году корпорация разорилась, но к тому времени молва о талантах великолепной четверки из Лейксайда разошлась далеко. И вскоре еще одна солидная корпорация поручила Биллу и компании написание программ на языке COBOL – за то же машинное время плюс проценты с продаж (роялти). Одной из самых успешных стала программа регулирования уличного движения – она принесла Гейтсу около $20 тыс. А в 17 лет он вместе с Алленом создал компанию Traf-O-Data, главной целью которой была также компьютеризация городского трафика.

Последний год учебы в школе Билл Гейтс откровенно прогулял. Ему уже было не до того – молодой программист зарабатывал в крупной аэрокосмической корпорации TRW $20 тыс. в год. По настоянию родителей, все еще видевших сына адвокатом, Билл поступил в Гарвард, но, как и в школе, рассматривал пребывание в престижном университете исключительно в качестве «средства доступа» все к тем же компьютерам. На втором месте после них стоял покер, за что студент Гейтс заслужил прозвище «покерного наркомана».

Из Гарварда он вынес одно полезное знакомство – однокурсник Стив Балмер в будущем наследует Билла Гейтса на посту CEO Microsoft. И, по крайней мере, одну полезную мысль, почерпнутую на лекциях по математике: оказывается, в мире есть люди поумнее его. С этими ценными приобретениями студент-второкурсник в 1974 году был отчислен за прогулы и академическую неуспеваемость. Самого прогульщика, впрочем, это мало расстроило. Его ждали великие дела на ниве бизнеса.

В начале был софт

В конце того же 1974 года компания MITS выпустила прототип будущих «персоналок» – сравнительно компактный компьютер Altair-8800. В этой машине все было хорошо, не хватало только удобного и доступного широким юзерским массам программного обеспечения. Это ясно понимала и компания-производитель. Поэтому, получив от Билла Гейтса и Пола Аллена предложение купить приспособленный для нового компьютера «софт», президент MITS Эд Робертс тут же назначил «благодетелям» встречу в штаб-квартире компании в Албукерке (штат Нью-Мексико).

Правда, авторы выгодного предложения к тому времени не только не написали чудо-программы, но и самого компьютера Altair 8800 в глаза не видели. Все знакомство Билла Гейтса с новой моделью ограничилось прочитанной статьей в январском номере журнала Popular Electronics за 1975 год. Так закладывался фирменный стиль будущего создателя и владельца Microsoft: главное – ввязаться в сражение, а там будь что будет. В переводе с военного языка на современный маркетинговый это означало следующее. Главное – широко анонсировать новую версию «софта» и любыми средствами протолкнуть ее на рынок, а отладками и доводками заниматься потом. В том числе и за счет пользователей, посылающих по Интернету свои вопросы и замечания в Microsoft.

лет существования новоиспеченной компании все ее сотрудники, включая президента, пахали на ниве программирования. Известно, что Гейтс вникал в каждую строчку только что написанных кодов и собственноручно правил их. Негласным корпоративным принципом Microsoft было: нельзя терпеть начальником того, кто пишет программы хуже тебя самого. Но потом в связи с беспрецедентным ростом компании о подобной черновой работе пришлось забыть. Не дело президента возиться с такой мелочевкой, его сфера – деньги, стратегия развития бизнеса.

С деньгами (еще один миф) на первых порах тоже все обстояло непросто. Первые пять заказчиков молодой компании разорились, не успев расплатиться за выполненные заказы. Несколько поправили дела проданные компании Apple лицензионные программы для ее будущего триумфа – модели Apple II, но все же в 1979-м друзьям пришлось несолоно хлебавши возвращаться в родной Сиэтл, разместив новую штаб-квартиру компании в его пригороде Беллвью.

Автор новой ОС был большим шутником, ибо ее название расшифровывалось как Quick and Dirty Operating System — «Сделанная наспех дрянная операционная система

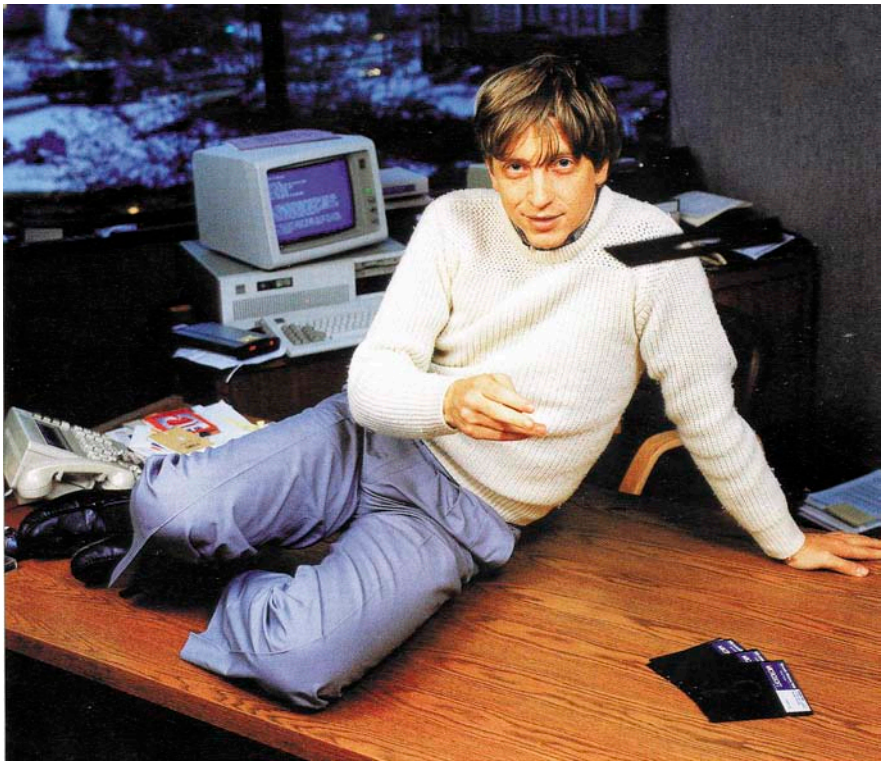
Как бы то ни было, за пару недель Билл с Полом освоили новый компьютер, написали для него программу и выгодно продали права на ее использование MITS. После чего переименовали свою компанию в Micro-Soft, а спустя год, в ноябре 1976-го, зарегистрировали в штате Нью-Мексико торговую марку как Microsoft.

Дальнейшее, как говорится, история. И неизбежная в случае таких компаний-легенд мифология.

В частности, широко распространено заблуждение о том, что Билл Гейтс собственноручно написал знаменитую операционную систему для первой «персоналки» (MS-DOS), а впоследствии и первые версии Windows. Этот миф родился даже не в недрах Microsoft (сам Билл Гейтс никогда не утверждал ничего подобного), а скорее в среде компьютерных фанатов и в СМИ, поначалу молившихся на основателя Microsoft. Действительно, первые пять

И вот там-то их ждал поистине звездный заказ от компании IBM, отчаянно нуждавшейся в ПО для своей революционной новинки – первого в мире персонального компьютера. Вообще-то такие гиганты, как правило, избегают случайных связей с вышедшими на рынок «малолетками». Но у IBM не было иного выхода – компания Digital Research, взявшая подряд на создание софта, срывала все сроки, а время широко разрекламированного старта серийных IBM PC поджимало. Вот и пришлось связываться с фирмочкой со штатом в десяток человек и 20-летним президентом-недоучкой, отчисленным из Гарварда.

Как известно, ни заказчик, ни исполнитель впоследствии не пожалели о скоропалительно заключенном со-



юзе. Спустя пару недель Гейтс представил IBM операционную систему 86-DOS (QDOS), в основе которой лежала система, разработанная Тимом Патерсоном, сотрудником небольшой компании Seattle Computer Products (SCP). Между прочим, автор новой ОС был большим шутником, ибо ее название расшифровывалось как Quick and Dirty Operating System – «Сделанная наспех дрянная операционная система»! А роль самого Гейтса в создании будущей MS-DOS заключалась лишь в покупке эксклюзивных прав на продажи системы и приглашении Патерсона в Microsoft, где ему было поручено довести систему до нужд будущей «персоналки».

Гениальная деловая интуиция не отказала Гейтсу. Он догадался пойти на одноразовую продажу (за $50 тыс.) IBM новой ОС, переименованной в MS-DOS, – но не прав на нее! Уже тогда глава Microsoft разглядел, как в скором времени «айбиэмовские» PC с их открытой архитектурой начнут клонировать все, кому не лень. Так и случилось – и отныне все это «ай-би-эм-писи-совместимое железо» продавалось с предустановленным на нем софтом от Билла Гейтса.

Окна в будущее

К началу «высокотехнологичных восьмидесятых» компания Microsoft превратилась в корпорацию. Президентом и председателем совета директоров стал Билл Гейтс, а исполнительным вице-президентом – Пол Аллен. И среди сотрудников появился новичок – тот самый Стив Балмер.

В разгар бума hi-tech, когда даже президенты государств выделяли миллиардные средства на создание высокотехнологичного оружия для будущих «звездных войн», компания Microsoft осенью 1983 года анонсировала новую ОС Windows 1.0 с графическим интерфейсом, подозрительно напоминавшим операционную систему главного конкурента – компании Apple. Судебные тяжбы двух супертяжеловесов длились более пяти лет и закончились в пользу Билла Гейтса, патологически ненавидящего любые проигрыши. Но пока суд да дело, в 1985 году, когда первые «Окна» поступили в продажу, прибыль Microsoft приблизилась к рубежу $150 млн.

Весной следующего года детище Билла Гейтса вышло на IPO, выручив за первый день торгов более $60 млн. И еще спустя несколько месяцев 31-летний президент Microsoft стал самым молодым миллиардером в истории – принадлежавший ему пакет из более чем десяти миллионов акций, до этого стоивший $390 млн, подорожал до $1,25 млрд. На акциях компании разбогател не только ее глава – сегодня среди сотрудников Microsoft (нынешних и бывших) есть уже четыре миллиардера и около 12 тысяч миллионеров.

После первой версии Windows последовали Windows 3.0 (в 1990 году), количество продаж которой за две первые недели превысило 100 тысяч, Windows NT и так далее вплоть до новейшей Vista и недавно анонсированной Windows 7.

Уже к 1993 году фирменная «оконная» система от Microsoft стала самой распространенной в мире. Параллельно были разработаны не менее успешные продукты – такие, как Microsoft Office. Кроме операционных систем и офисных приложений, компания агрессивно вторгалась и на соседние сегменты рынка. Это собственные сеть кабельного телевидения MSNBC, интернет-портал MSN, мультимедийная энциклопедия Microsoft Encarta, «фирменная» мышь и оригинальные продукты в сфере «домашних развлечений» (Home Entertainment) – такие, как Xbox, Xune и MSN TV. Так обретала логическое завершение негласная стратегия компании, сформулированная еще на заре ее существования: «Компьютер с программным обеспечением от Microsoft – на каждом офисном столе и в каждом доме».

К началу 1990-х сформировался и стиль управления «от Билла Гейтса». В своей внешней политике он жестко и даже яростно защищает свое детище и собственный штат, во внутренней – столь же яростно, а порой беспощадно критикует подчиненных за малейший промах. Как часто бывает с вундеркиндами, Гейтс порой бывает высокомерен, самовлюблен, раздражителен и упрям. Особенно нетерпим он к тем, кого считает тупицами и бездарями. «Я справлюсь с этой задачкой за уик-энд», – любимая присказка главы Microsoft. Вместе с тем он всегда готов признать правоту подчиненного, если тот сможет аргументированно отстоять свою позицию.

Богатые тоже платят

Но все это мелочи на фоне иных грехов Билла Гейтса.

Уже к началу 1990-х годов примерно треть сотрудников Microsoft была выведена за штат, обеспечив дополнительный рост доходов компании – выплаты внештатникам не облагались

налогами, внештатникам не положена была и «социалка», которая в Америке ценима едва ли не больше зарплаты. Даже после того как в 1997 году Microsoft проиграла судебную тяжбу с собственными сотрудниками, требовавшими ввести их обратно в штат, Гейтс со свойственным ему упрямством придумал новую схему эксплуатации человека человеком. На сей раз прием на работу в Microsoft был переложен на плечи так называемых кадровых агентств заемной рабочей силы. Схема состояла в следующем – целые подразделения компании сначала выводились в аутосорсинг, при этом их сотрудники лишались всех льгот и соцпакетов. А затем выведенных сотрудников заново приглашали на работу, но уже в штат подобного агентства.

В результате этой реструктуризации, как выразился вице-президент Microsoft, «наши доходы выросли на 91%, а штат фактически сократился на 19%».

Однако главные обвинения, которыми с завидной регулярностью противники и конкуренты Microsoft осыпают компанию и лично Билла Гейтса на протяжении последней четверти века, сводятся к нечистоплотной конкуренции.

Бизнес-тактику главы Microsoft один из критиков свел к трем латинским E: embrace, extend и extinguish. В переводе на русский это означает: объять (другое значение – воспользоваться), расширить (распространить) и потушить (уничтожить, аннулировать). Иначе говоря, задача компании состоит в том, чтобы воспользоваться чужим продуктом, затем на его базе создать собственную версию, несовместимую с оригиналом, и уж потом задавить конкурента с помощью «нового продукта Microsoft». Эти обвинения не лишены оснований. Как писал другой критик, «история Microsoft богата случаями того, как компания применяла и патентовала изобретения, которые, по мнению многих, основывались на изобретениях других – или просто на заведомо очевидных идеях».

Хотя, с другой стороны, что такое бизнес, как не умение всегда оказываться в нужном месте в нужное время! Купить то, что дешево или вовсе бесплатно, чтобы затем продать это, но уже за большие деньги?

Гейтс всегда был бескомпромиссен, когда дело касалось только бизнеса, чем, разумеется, нажил себе кучу врагов. В том числе и среди бывших партнеров и долговременных клиентов. Глава Microsoft умудрился поссориться даже с Пентагоном! Дело на сей раз касалось еще одной ахиллесовой пяты Microsoft – принципиальной закрытости ее программного обеспечения. Военное ведомство решило, что открытые системы типа конкурирующей Linux лучше послужат задачам национальной безопасности, и Гейтс развернул беспрецедентную пропагандистскую кампанию с целью не допустить ухода Пентагона к конкурентам. Позже, начиная с 2004 года, антимонопольные службы Евросоюза дважды штрафовали Microsoft (почти на полмиллиарда евро) за отказ раскрыть программный код своих операционных систем.

Однако главные судебные баталии развернулись вокруг системы Internet Explorer. После выпуска очередной версии своей ОС – Windows 95 – Билл Гейтс всерьез задумался о собственной разработке интернет-браузера. Так появилась серия Internet Explorer, ныне (версия 8.0) занимающая первое место в мире по числу пользователей (65,5% рыночной доли, по данным на май 2009 года). И все благодаря тому, что Microsoft не продала ни единой копии Internet Explorer, а просто начиная с 1995 года предустанавливала браузер на компьютеры вместе с очередными версиями Windows!

Иначе говоря, вместе с операционной системой пользователю вульгарно навязывают конкретный браузер, лишая возможности выбирать среди конкурирующих продуктов. Это не могло пройти мимо внимания Федеральной антимонопольной комиссии и министерства юстиции. В 1998 году начался судебный марафон «Соединенные Штаты против Microsoft», в котором сторона обвинения выдвинула предложение принудительно раздробить могущественную «империю Билла» на две самостоятельные компании – одна пусть выпускает операционные системы, а другая – интернет-браузеры. В апреле 2000 года суд решил дело в пользу Соединенных Штатов, обвинив Microsoft в злоупотреблении монополизмом, и настоял на разделе компании. Затем, однако, апелляционный суд отвел часть обвинений, в 2001 году было достигнуто некое мировое соглашение с министерством юстиции, но фактически процесс продолжается по сей день.

Последним отголоском затяжной баталии стал иск в Еврокомиссию со стороны европейской софтверной компании Opera Software ASA. Она обвиняет Microsoft в незаконной, по мнению истца, привязке Internet Explorer к Windows.

Трудно быть Биллом

В общем, борьба идет с переменным успехом. Пока во всяком случае Microsoft и не подумала раскрывать свои программные коды, а конкурентную борьбу продолжает вести все так же агрессивно. У Билла Гейтса хватает денег на лучших в стране адвокатов, а в США (вот ужас-то!) государство не имеет иных рычагов давления на «зарвавшегося бизнесмена», кроме законных – судебных…

Может быть, поэтому за последние полтора десятилетия глава Microsoft все чаще обращал внимание на рынки других стран. В Китае, Индии, да и в нашей «суверенной демократии» у Билла Гейтса многое получается лучше, чем на родине. Особенно когда дело касается разного рода «нацпроектов» (вроде тотальной компьютеризации властных структур или школ), в которых появление поставщика-монополиста не вызывает такой болезненной реакции. Правда, деятельность вездесущего Билла в последнее время вызывает раздражение и в Индии, и в Китае, руководство этих стран вслед за американским Пентагоном тоже подумывает о том, чтобы перейти на программное обеспечение с открытым кодом. Да и беспрецедентное пиратство в странах БРИК вряд ли радует главу Microsoft.

Как бы то ни было, в последние годы Билл Гейтс значительно изменил собственный имидж. Теперь он чаще появляется в СМИ не как «Гейтс – великий и ужасный», а как любящий муж и заботливый отец (у четы Гейтсов трое детей). И не просто любящий и заботливый, но и справедливый, что в каноне протестантской этики означает прежде всего бережливый. Сорить деньгами он, действительно, не любит – ну разве что прикупить на аукционе коллекцию рисунков Леонардо за каких-то $30 млн! Обладатель многомиллиардного состояния исправно выплачивал по брачному контракту любимой жене по $10 тыс. за каждого рожденного ребенка, а всем троим отпрыскам в наследство обещал оставить целых $10 млн. Резонно заявив, что это весьма неплохой стартовый капитал – сам Гейтс начинал с куда меньшей суммы…

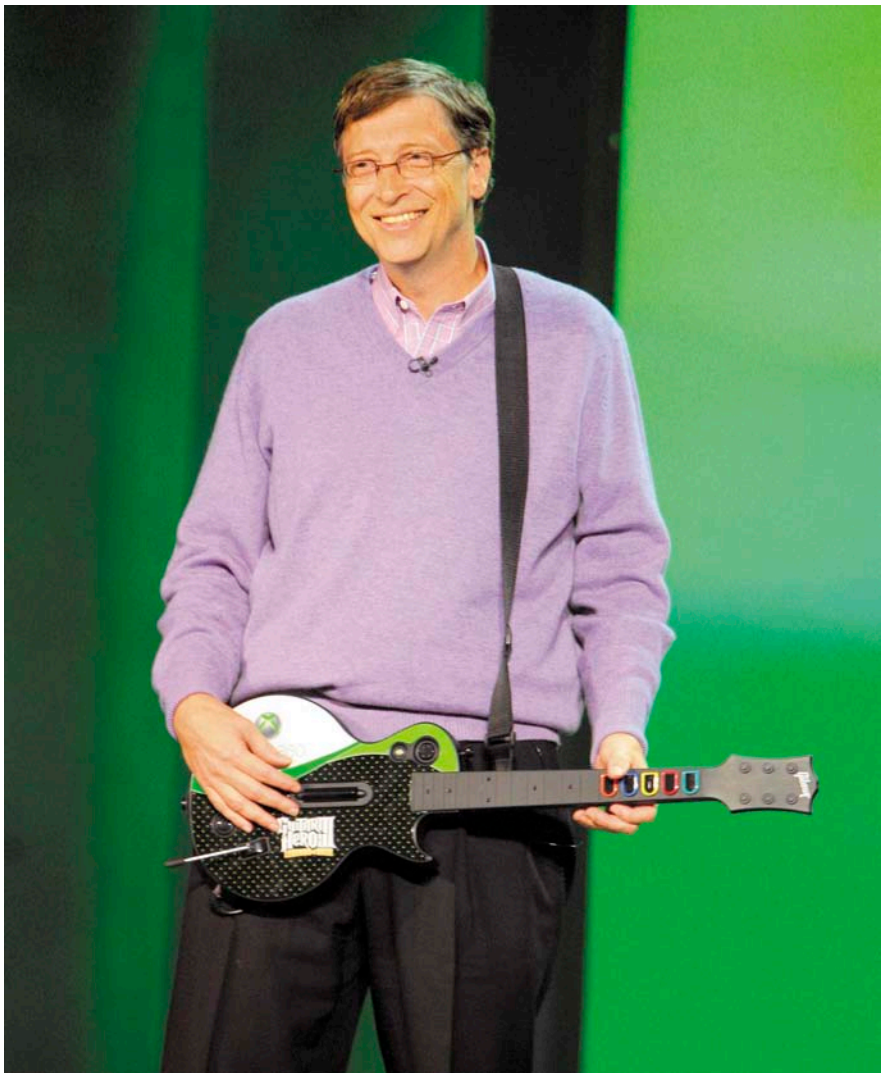
Живут супруги в доме на берегу озера Вашингтон в одноименном штате. Их «дом будущего», вместе с землей тянущий на $125 млн, представляет собой триумф hi-tech, но одновременно и пример энерго- и ресурсосберегающих технологий. Таким образом хозяин дома как бы извиняется за отнюдь не «зеленую» репутацию своей компании, по данным Greenpeace, занимающую вторую строку в рейтинге «18 самых антиэкологичных компаний», уступая только Nintendo.

Главной сферой деятельности Билла Гейтса, первого и пока единственного «стомиллиардера» (в 1993 году его «капитализация» превзошла символический рубеж $101 млрд – сегодня, конечно, гораздо меньше), в последние годы стала благотворительность. В 2000 году он покинул пост CEO компании, передав свои полномочия Стиву Балмеру, а за собой сохранил посты председателя правления и «главного архитектора софта». А в июне прошлого года бессменный глава Microsoft, следуя своей же многолетней практике, вывел за штат себя самого. Хотя и остался крупнейшим индивидуальным акционером компании, владея 8-процентным пакетом акций.

Теперь он, как и его старый друг и главный преследователь по рейтингу Forbes Уоррен Баффет, активно «раздает деньги». Но не всяким благотворительным фондам, а только тем, которые учредил сам вместе с супругой Мелиндой. Главным из них остается Bill & Melinda Gates Foundation – крупнейший в мире из тех, что называют «прозрачными». Любой бенефициар фонда имени супругов Гейтс вправе получить исчерпывающую информацию о том, куда идут деньги. По данным на 2007 год, супруги Гейтс занимали второе место среди филантропов Америки с $28 млрд, потраченными на здравоохранение, образование и научные исследования.

Хотя критики и в этом случае не унимаются. Мол, своей «безвозмездной компьютерной помощью» школам в США и ряде стран экс-глава Microsoft просто готовит рынки к новому вторжению очередных Windows и прочих продуктов компании… Может быть, критики и правы. А может, перефразируя Хармса, Билл Гейтс просто очень любит детей.

А еще он коллекционирует анекдоты о себе самом. Один из самых любимых такой: «В чем разница между Создателем и Биллом Гейтсом? Создатель не считает себя Биллом Гейтсом». EOF



Переполнение буфера в обработке HTTP-ответов в Google Ghrome

Программа: Google Chrome до версии 2.0.172.33.
Опасность: Критическая.
Наличие эксплоита: Нет.
Описание: Переполнение буфера обнаружено при обработке некоторых HTTP-ответов. В результате можно выполнить произвольный код через специально обработанный HTTP-ответ, полученный от злонамеренного HTTP-сервера.
URL производителя: http://www.google.com.
Решение: Установите последнюю версию браузера.

Уязвимость при обработке пустых сообщений в GUPnP

Программа: GUPnP 0.12.7, возможно, другие версии.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Уязвимость существует из-за ошибки при обработке сообщений для подписки и контрольных сообщений, не содержащих данные. Удаленный пользователь может отправить пустое сообщение уязвимому приложению и аварийно завершить его работу.
URL производителя: www.gupnp.org.
Решение: Установите последнюю версию 0.12.8 с сайта производителя.

Уязвимость в обработке JPEG-изображений в php exif_read_data()

Программа: PHP до версии 5.2.10.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Недостаточная проверка данных обнаружена в функции exif_read_data(), что может привести к аварийному завершению работы программы через специально обработанное JPEG-изображение.
URL производителя: http://www.php.net.
Решение: Обновите до версии 5.2.10.

Переполнение буфера при обработке изображений в xcftools

Программа: xcftools 1.0.4.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Переполнение буфера обнаружено в функции flattenIncrementally() в flatten.c. В результате можно выполнить произвольный код при запуске xcf2pnm утилиты с параметрами -C или -O со специально обработанным изображением.
URL производителя: http://henning.makholm.net/xcftools.
Решение: Не используйте подозрительные файлы с xcftools.

DoS-атака в Secure Gateway service в Citrix Secure Gateway

Программа: Citrix Secure Gateway 3.x.
Опасность: Средняя.
Наличие эксплоита: Нет.
Описание: Специально созданный запрос к Secure Gateway service может вызвать чрезмерное использование ресурсов центрального процессора и привести к зависанию системы.
URL производителя: http://www.citrix.com.
Решение: Установите соответствующее исправление.

Удаленное выполнение кода в EDraw PDF Viewer ActiveX-компоненте

Программа: EDraw PDF Viewer ActiveX Control 3.x.
Опасность: Высокая.
Наличие эксплоита: Да.
Описание: Уязвимость связана с небезопасным методом FtpDownloadFile() в PDFVIEWER.PDFViewerCtrl.1 ActiveX-компоненте (pdfviewer.ocx). В результате возможно загрузить произвольный файл в произвольное место на системе целевого пользователя, посетившего специально созданный веб-сайт. Успешная эксплуатация позволяет выполнить произвольный код.
URL производителя: http://www.edrawsoft.com.
Решение: Обновите программу до версии 3.2.0.126.

Уязвимость в обработке кодированных символов в International Components for Unicode (ICU)

Программа: International Components for Unicode (ICU) версии до 4.0.1.
Опасность: Низкая.
Наличие эксплоита: Нет.
Описание: Ошибка преобразования существует, когда ICU обрабатывает некоторые кодированные символы. В результате можно обойти некоторые контент-фильтры, выполнить XSS-нападение и раскрыть чувствительную информацию.
URL производителя: http://icu-project.org.
Решение: Установите последнюю версию – 4.0.1.

Переполнение буфера в потоке JPEG 2000 в Foxit Reader JPEG2000/JBIG Decoder Add-On

Программа: Foxit Reader JPEG2000/JBIG Decoder Add-On до версии 2.0 Build 2009.303.
Опасность: Критическая.
Наличие эксплоита: Нет.
Описание: Переполнение буфера обнаружено в потоке JPEG 2000. В результате можно выполнить произвольный код через специально созданное изображение JPEG 2000.
URL производителя: http://www.foxitsoftware.com.
Решение: Обновите до версии 2.0 Build 2009.616.

Составил Александр Антипов

Визитка

АНТОН ГРИШАН, ведущий программист крупного регистратора доменных имен

Ускоряем загрузку сайта,
минимизируя количество HTTP-запросов

Загрузка результатов работы веб-приложения занимает около 80% от общего времени обработки пользовательского запроса. Почему это так, и как с этим бороться?

Быстрая доставка результатов работы интернет-приложения пользователю (обычно HTML-документ) существенно повышает общую производительность приложения. Один из основных факторов, замедляющих процесс загрузки страницы – избыточное количество HTTP-запросов. Рассмотрим подробнее причины падения скорости загрузки.

Причина №1: Увеличение объёма данных

Для загрузки данных с сервера клиент должен отправить HTTP-запрос и дождаться ответа, содержащего HTTP-заголовок и данные. Таким образом, количество байт, которые необходимо передать по сети для загрузки объекта (изображения, скрипта, таблицы стилей, флеш-ролика), складывается из:

- длины HTTP-запроса в байтах;
- длины HTTP-заголовка ответа;
- длины передаваемых данных.

Необходимость в передаче и приёме HTTP-заголовков ведет к увеличению объёма данных, передаваемых по сети. Не стоит думать, что это незначительное увеличение, которым можно пренебречь. При посылке запроса браузер отправляет серверу:

- тип и версию браузера (User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; ru; rv:1.9.0.10) Gecko/2009042316 Firefox/3.0.10);
- поддерживаемые форматы данных (Accept: text/html, application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8);
- пользовательские предпочтения языков отображения содержимого (Accept-Language: ru,en-us;q=0.7,en;q=0.3);
- поддерживаемые алгоритмы сжатия (Accept-Encoding: gzip,deflate);
- данные о предпочтительной кодировке (Accept-Charset: windows-1251,utf-8;q=0.7,*;q=0.7);
- cookies, объём которых зависит от содержащихся в них данных;
- POST/GET-данные и множество других параметров.

Например, для загрузки моей страницы в социальной сети vkontakte.ru браузер выполнил 40 запросов, суммарный размер переданных и принятых HTTP-заголовков составил 43176 байт (43 Кб), т.е. для загрузки одного объекта потребовалось дополнительно около 1076 байт. Особенно ощутимы накладные расходы при загрузке небольших файлов.

Причина №2: Скорость передачи данных ниже скорости приёма

В последнее время широкой популярностью пользуются технологии доступа к Интернету с асимметричной скоростью передачи данных (например, ADSL). Это означает, что скорость приёма и передачи данных при таком соединении различна, обычно скорость передачи исходящего трафика (посылка запроса) значительно ниже скорости приёма данных (загрузка ответа сервера). Конкретные величины зависят от оборудования пользователя и тарифного плана провайдера, но суть остается прежней. Соотношение скоростей приема/передачи колеблется в диапазоне от 3:1 до 20:1, это означает, что за время, необходимое для передачи одного байта запроса, пользователь может получить от 3 до 20 байт ответа.

Рассмотрим наиболее эффективные способы борьбы с избыточным количеством HTTP-запросов.

Способ №1: объединение объектов

Объединение объектов позволяет сократить количество HTTP-запросов, необходимых для загрузки страницы, за счет уменьшения количества загружаемых объектов. Например, если требуется загрузить несколько JavaScript-сценариев, то их можно объединить в один файл, таким образом, сократится количество загружаемых объектов, а значит, и количество необходимых HTTP-запросов.

Загрузка JavaScript и CSS-кода

Для правильной визуализации документа браузеру необходимо загрузить все таблицы стилей и JavaScript-библиотеки, подключаемые внутри документа. Например, если осуществляется подключение трех таблиц стилей и четырёх сценариев JavaScript, то для загрузки документа браузеру не-

обходимо выполнить восемь запросов – по одному запросу для каждого JS/CSS-файла плюс один запрос для получения HTML-кода.

Сократить количество HTTP-запросов можно, объединив все загружаемые таблицы стилей в один файл, а все библиотеки JavaScript – в другой. Таким образом, в приведенном выше примере для загрузки страницы потребуется не 8, а всего 3 запроса, что значительно лучше.

Сложно объединять файлы вручную, особенно если разные страницы требуют разный набор JS/CSS-файлов. Для решения этой проблемы существует множество утилит, наиболее известные из которых minify (http://code.google.com/p/minify) и Combo Handler Service (http://yuiblog.com/blog/2008/07/16/combohandler). Оба сервиса работают по одинаковому принципу, поэтому здесь и далее примеры будут приводиться для minify.

Minify – приложение, написанное на PHP5, основная функции которого – объединение и минификация JS/CSS-файлов с целью повышения скорости загрузки документа за счет сокращения количества HTTP-запросов и уменьшения размера JS/CSS-кода. Рассмотрим принцип работы на примере подключения одинакового количества JS/CSS-файлов с использованием minify и без оного.

1. Подключение JS/CSS-файлов в теле HTML-документа без minify (7 HTTP-запросов):

```
<link type="text/css" rel="stylesheet" ↵
       href="/css/main.css" />
<link type="text/css" rel="stylesheet" ↵
       href="/css/forms.css" />
<link type="text/css" rel="stylesheet" ↵
       href="/css/menu.css" />
…
<script type="text/javascript" src="/js/main.js"></script>
<script type="text/javascript" src="/js/form.js"></script>
<script type="text/javascript" ↵
       src="/js/calendar.js"></script>
<script type="text/javascript" src="/js/menu.js"></script>
```

2. Подключение JS/CSS-файлов в теле HTML-документа с использованием minify (2 HTTP-запроса):

```
<link type="text/css" rel="stylesheet" ↵
       href="/min/b=css&amp;f=main.css,forms.css, ↵
       menu.css" />
…
<script type="text/javascript" ↵
       src="/min/b=js&amp;f=main.js,form.js, ↵
       calendar.js,menu.js"></script>
```

Во втором случае список подключаемых файлов передаётся скрипту minify, который:

- объединяет JS/CSS-файлы;
- минифицирует объединенный JS/CSS-код (с помощью библиотеки JSMin);
- сжимает полученный результат с помощью gzip (если браузер пользователя поддерживает сжатие).

В результате сокращается количество запросов и уменьшается размер JS/CSS-кода, что заметно повышает скорость загрузки HTML-страницы. Minify поддерживает систему кэширования, позволяющую избежать повторного выполнения работы по минификации одних и тех же файлов.

При объединении нескольких JavaScript-файлов может возникнуть проблема со сценариями, использующими метод document.write для вывода части текста страницы. Данные участки кода придется модифицировать, таким образом, чтобы обойтись без document.write или не объединять данный скрипт с остальными сценариями.

Объединение изображений

Как правило, сайты содержат множество мелких графических элементов, таких как интерфейсные иконки, пиктограммы, фоновые изображения и т.п. Для загрузки каждого изображения требуется отдельный HTTP-запрос, кроме того, иногда запрашиваемый файл меньше размера HTTP-заголовков, что ведет к неэффективному использованию канала передачи данных.

Решить эту проблему можно, объединив графические элементы страницы в один файл (ресурсная картинка), который будет загружен браузером за один запрос. Таблица стилей определяет, где и какие части этого графического файла необходимо использовать. Данная техника известна под названием «CSS-спрайты» (CSS sprites).

В качестве примера использования CSS-спрайтов рассмотрим реализацию кнопки «Удалить» на страницах поисковой выдачи системы Google (см. рис. 1).

Ресурсная картинка, содержащая графические элементы пользовательского интерфейса поисковой системы Google (см. рис. 2), располагается по адресу (на момент написания данного текста) http://www.google.ru/images/nav_logo4.png.

HTML-код, отвечающий за отображение кнопки «удалить», выглядит следующим образом:

```
<button class=w20 title="Remove"></button>
```

Как видно из кода, кнопка реализована в виде button-элемента, использующего для отображения класс w20. С помощью CSS определяется правило отображения элементов класса w20:

```
.w10, .w11, .w20, .w21, .w24, .wci, .wpb {
background:transparent url(/images/nav_logo4.png) ↵
       no-repeat scroll 0 0;
border:0 none;
cursor:pointer;
height:16px;
margin-left:8px;
vertical-align:bottom;
width:16px;
}

.w20, .w21 {
margin-left:3px;
}

.w20 {
background-position:-152px -32px;
}
```

В первом блоке фигурных скобок определяются общие правила отображения элементов, подобных w20. Класс задаёт параметры ширины, высоты, отступов и указывает фоновое изображение (/images/nav_logo4.png). Так как для разных элементов используются разные части ресурсной картинки, конкретные координаты указываются только для класса w20, в последнем блоке фигурных скобок (background-position:-152px -32px;).

Создавать ресурсные картинки вручную – довольно утомительное занятие, поэтому для автоматизации процесса существуют специальные online-сервисы, такие как http://spritegen.website-performance.org.

Техники CSS-спрайтов позволяют существенно увеличить производительность сайта, но прежде чем принимать решение об использовании данной технологии, необходимо ознакомиться со списком достоинств и недостатков:

Достоинства:

Сокращение количества HTTP-запросов. Благодаря ресурсной картинке все графические элементы могут быть загружены за один HTTP-запрос.

Уменьшение объёма файлов. Размер ресурсной картинки меньше (в среднем на 30%) суммарного размера графических файлов, в неё входящих. Этот факт объясняется особенностями графических форматов и алгоритмов сжатия.

Недостатки:

Усложнение процесса разработки. Использование техники CSS-спрайтов требует дополнительных навыков верстки с учетом возможных отличий при отображении в разных браузерах.

Сложность сопровождения и обновления. Добавление, удаление или модификация графического элемента, отображаемого с помощью CSS-спрайтов, требует редактирования объединенного графического файла. Значительно больше проблем возникает, когда модификация графического элемента приводит к изменению его размера, в этом случае придется редактировать таблицы стилей.

Замедленное отображение страницы. Неправильное использование спрайтов может привести к визуальному замедлению загрузки сайта. Дело в том, что объединенный файл, содержащий все графические элементы пользовательского интерфейса, будет загружаться медленнее, чем половина картинок, в него входящих. Браузер может использовать картинку сразу после загрузки, поэтому в случае множества мелких изображений отдельные графические элементы начнут отображаться скорее, хотя полная загрузка сайта займет большее количество времени.

Рисунок 1. Реализация кнопки «Удалить» на страницах поисковой выдачи системы Google

Рисунок 2. Графические элементы пользовательского интерфейса поисковой системы Google

CSS-спрайты не имеют собственного URL, alt и title. Картинка, отображаемая с помощью CSS-спрайтов, не имеет собственного URL-адреса, а также атрибутов alt (альтернативный текст) и title (заголовок). Если пользователь отключит в браузере отображение графических элементов, то на месте изображения, выводимого через спрайты, ничего не будут отображено. То есть не будет ни альтернативного текста, ни пиктограммы, говорящей о том, что здесь должно быть изображение.

Исходя из приведенных выше достоинств и недостатков, а также своего опыта разработки, могу рекомендовать следующие принципы использования спрайтов:

Ресурсная картинка не должна быть большой. Старайтесь создавать ресурсные картинки, размер которых не превосходит 10-15 Кб. При необходимости создайте несколько ресурсных картинок, содержащих различный набор графических элементов.

Объединяйте только совместно используемые изображения. Объединить в одну ресурсную картинку можно все графические элементы сайта, но это не значит, что так стоит поступать. Некоторые картинки используются для отображения на определенных страницах. Если иконка с изображением телефона используется только на странице «Контакты», то её не обязательно загружать на главной странице. Создавайте ресурсные картинки таким образом, чтобы загружались только реально используемые графические элементы.

Использование CSS-спрайтов не всегда оправдано. В случаях, когда для изображения наличие URL, alt- и title-атрибутов важно с точки зрения функциональности и/или поискового продвижения (SEO), не стоит использовать спрайты. В качестве примера можно привести логотип сайта или изображение товара в online-магазине.

Объединение текстовых и графических данных

Обычно графические изображения в HTML/CSS-коде подключаются с помощью указания пути до нужного файла:

```
<img src="icon.png" alt="подключение картинки" />

.test {background:url(icon.png);}
```

В соответствии со схемой data:URL (см. RFC 2397), URL можно использовать не только для указания места нахождения данных, но и для размещения самих данных внутри URL. Формат data:URL предельно прост:

```
data:[<MIME-type>][;charset="<encoding>"][;base64],<data>
```

где:

[<MIME-type>] – тип хранимых данных, например, для картинок в формате PNG данный параметр имеет вид image/png. Если тип данных не указан, то предполагается text/plain.

[;charset="<encoding>"] – кодировка текстовых данных в случае с картинкой не имеет смысла и поэтому не указывается.

[;base64] – метод кодирования данных чаще всего используется base64, но если этот параметр опущен, то данные представляются, с использованием кодировки ASCII в диапазоне безопасных символов URL. Для символов вне этого диапазона применяется стандартное %xx шестнадцатеричное кодирование URL.

Например, так выглядит тег img, содержащий в поле src не путь до картинки, а саму картинку в формате data:URL:

```
<img src=" ↵
        AAABAAAAAQAQMAAAAlPW0iAAAABlBMVEUAAAD///+l2Z/ ↵
        dAAAAM0lEQVR4nGP4/5/h/1+G/58ZDrAz3D/ ↵
        McH8yw83NDDeNGe4Ug9C9zwz3gVLMDA/A6P9/ ↵
        AFGGFyjOXZtQAAAAAElFTkSuQmCC" ↵
        alt="картинка внутри HTML" />
```

Аналогичным образом можно использовать картинки в CSS-классах:

```
.test {
background:url( ↵
        ANSUhEUgAAABAAAAAQAQMAAAAlPW0iAAAABlBMVEUAAAD ↵
        ///+l2Z/dAAAAM0lEQVR4nGP4/5/h/1+G/58ZDrAz3D/ ↵
        McH8yw83NDDeNGe4Ug9C9zwz3gVLMDA/A6P9/ ↵
        AFGGFyjOXZtQAAAAAElFTkSuQmCC);
}
```

Для преобразования графических файлов в формат data:URL существуют прикладные программы и online-сервисы, например, http://www.sveinbjorn.org/dataurlmaker.

Как и любая другая технология, data:URL обладает рядом преимуществ и недостатков, которые необходимо знать для максимально эффективного использования.

Достоинства:

- Для загрузки data:URL-данных не требуются дополнительные HTTP-запросы, что позволяет уменьшить нагрузку на сеть в случаях, когда встроенное содержимое сопоставимо по размеру с заголовком HTTP-запроса/ответа.
- Браузеры имеют ограниченное количество одновременных подключений к серверу (обычно 4, данный параметр зависит от браузера), таким образом, использование data:URL освобождает подключения для загрузки остального содержимого страницы.
- Встроенные изображения позволяют иметь HTML-документ с графическими изображениями в виде одного файла.

Недостатки:

- Встроенные в тело HTML-документа изображения не кэшируются браузером, если сам HTML-документ не кэшируется.
- Не все браузеры поддерживают встроенные изображения, как всегда, проблемы возникают с Internet Explorer, поддержка схемы data:URL появилась только в восьмой версии браузера.
- Размер изображения, закодированного в base64, больше бинарного аналога примерно на 30-40%.
- Максимальная длина URL, которую обязан поддерживать браузер, – 1024 байта (в соответствии со стандартом RFC), поэтому данная техника подходит только для небольших изображений.
- Картинки в формате data:URL, расположенные в CSS/HTML-файлах не могут загружаться в параллельном режиме, так как для загрузки одного CSS/HTML-файла, содержащего внедренные с помощью data:URL изображения, браузер использует одно соединение.
- Размещение в HTML-коде страницы двух одинаковых картинок в формате data:URL, потребует дублирования кода, что приведет к увеличению размера страницы и времени загрузки.

> Для модификации изображения потребуется редактировать все файлы, в которых оно использовано в формате data:URL.

Несмотря на внушительный список недостатков, при правильном использовании данная технология крайне полезна в таблицах стилей для хранения небольших изображений (фоны, пиктограммы, элементы дизайна). В теле HTML-документа встроенные изображения не должны встречаться, единственным исключением может быть иконка страницы (favicon.ico). Пример отображения иконки сайта с использованием data:URL:

```
<?php
function getFaviconHtml($faviconPath = 'favicon.ico') {

  $isBrowserSupportDataUrl = !isset($_SERVER ↵
        ['HTTP_USER_AGENT']) || (strpos($_SERVER ↵
        ['HTTP_USER_AGENT'], 'MSIE') === false);

return '<LINK rel="icon" href="'.( ↵
        $isBrowserSupportDataUrl ? ↵
        convertImgToDataUrlFormat($faviconPath, ↵
        'image/x-icon'): $faviconPath).'" ↵
        type="image/x-icon">';
}

function convertImgToDataUrlFormat($imgFilePath, ↵
        $mimeType)  {
  $contents = file_get_contents($imgFilePath);
  $base64   = base64_encode($contents);
  return ('data:' . $mimeType . ';base64,' . $base64);
}

?>
<html>
<head>
  <?=getFaviconHtml('favicon.ico')?>
        <title>Favicon with data:URL</title>

</head>
<body>
HELLO data:URL
</body>
</html>
```

В приведенном примере HTML-код, содержащий инструкции по отображению иконки сайта (favicon.ico), генерируется с помощью функции getFaviconHtml. Внутри функции осуществляется проверка типа браузера. Для Internet Explorer (т.е. предположительно не поддерживает data:URL) отображается путь до картинки, для остальных изображение преобразуется в формат data:URL.

В данном примере осуществляется очень примитивная проверка браузера, в реальных проектах необходимо учитывать не только тип, но и версию браузера.

Способ №2: загрузка объектов из кэша браузера

Правильное кэширование загружаемых объектов позволяет не только экономить трафик, но и радикально сократить количество HTTP-запросов, необходимых для повторной загрузки страницы, без уменьшения количества загружаемых объектов.

Контроль актуальности данных

Для правильной работы кэша данные, хранящиеся на сервере, должны быть идентичны данным кэша. Если версия файла на стороне сервера и в кэше не совпадает, то для правильной работы требуется загрузить новую версию с сервера.

Каким образом браузер узнает о том, что файл устарел и требуется повторная загрузка? Для этого существуют три методики.

1. Дата последней модификации. При первой загрузке файла сервер отправляет клиенту дату последней модификации файла в поле Last-Modified заголовка HTTP-ответа:

```
HTTP/1.x 200 OK
Date: Thu, 04 Jun 2009 06:41:11 GMT
Server: Apache/2.2.4 (Win32) mod_ssl/2.2.4
OpenSSL/0.9.8d PHP/5.2.4
Last-Modified: Wed, 03 Jun 2009 05:24:27 GMT
Accept-Ranges: bytes
Content-Length: 9973
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: image/png
```

После первой загрузки файл попадает в кэш браузера (иногда и прокси-сервера). При повторном использовании браузер, чтобы убедиться в том, что в кэше хранится последняя версия файла, – повторно отправляет HTTP-запрос на загрузку файла, но в этот раз, указывает дату последней модификации запрашиваемого файла (поле If-Modified-Since):

```
GET /logo.png HTTP/1.1
Host: test.localhost
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; ru;
rv:1.9.0.10) Gecko/2009042316 Firefox/3.0.10
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: ru,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: windows-1251,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://test.localhost/
If-Modified-Since: Wed, 03 Jun 2009 05:24:27 GMT
Cache-Control: max-age=0
```

В случае совпадения даты модификации файла, хранящегося на сервере, с датой, указанной в запросе, сервер отправляет пользователю ответ с кодом 304, означающий, что браузер может использовать имеющийся в кэше файл.

```
HTTP/1.x 304 Not Modified
Date: Thu, 04 Jun 2009 06:46:01 GMT
Server: Apache/2.2.4 (Win32) mod_ssl/2.2.4
OpenSSL/0.9.8d PHP/5.2.4
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
```

Если даты не совпадают, то сервер передает обновленный файл браузеру, который в свою очередь обновляет данные кэша.

2. Идентификатор версии сущности (ETag). ETag – строка, однозначно идентифицирующая версию файла, вычисляется на стороне сервера. Если файл модифицируется, то изменится и значение ETag. Алгоритм построения идентификатора не имеет принципиального значения, например, может быть использована MD5-сумма файла (хотя это и не самый лучший вариант). При загрузке файла, сервер передает соответствующее значение ETag в поле Etag HTTP-заголовка:

```
HTTP/1.x 200 OK
Date: Thu, 04 Jun 2009 06:41:11 GMT
Server: Apache/2.2.4 (Win32) mod_ssl/2.2.4
OpenSSL/0.9.8d PHP/5.2.4
```

```
Etag: "1eb78-170e-de8f95e0"
Accept-Ranges: bytes
Content-Length: 9973
Keep-Alive: timeout=5, max=94
Connection: Keep-Alive
Content-Type: image/png
```

Логика работы данного метода полностью совпадает и с проверкой актуальности данных по дате последней модификации, за исключением той разницы, что вместо даты используется ETag.

3. Декларативный срок актуальности данных. В отличие от двух предыдущих способов, мы сами объявляем дату, после которой необходимо загрузить новую версию файла. При запросе на загрузку объекта дата предполагаемой модификации (т.е. дата из будущего) файла, устанавливается в поле Expires:

```
HTTP/1.x 200 OK
Date: Fri, 05 Jun 2009 06:36:26 GMT
Server: Apache/2.2.4 (Win32) mod_ssl/2.2.4
OpenSSL/0.9.8d PHP/5.2.4
Accept-Ranges: bytes
Content-Length: 11298
Expires: Thu, 15 Apr 2034 20:00:00 GMT
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: image/jpeg
```

Браузер сохраняет в кэше файл и дату, после которой необходимо загрузить новую версию файла. При необходимости повторно воспользоваться данным файлом до указанной даты, браузер не отправляет никаких запросов серверу, а сразу берет файл из кэша, что позволяет избавиться от лишних HTTP-запросов.

Если заголовок Expires не задан, то для проверки актуальности данных используется дата последней модификации и/или ETag (в зависимости от настроек сервера), что приводит к ситуации, при которой загрузка данных из кэша требует выполнения HTTP-запросов.

Наша цель – минимизировать количество HTTP-запросов, поэтому для кэширования статичных данных подходит только третий вариант (декларативный срок актуальности данных).

Кэширование статичных объектов

Большинство загружаемых объектов, таких как изображения, таблицы стилей и JS-код, – статичны. Для статичных объектов наиболее эффективный метод кэширования – декларативный срок актуальности данных.

Предположим, существует сайт www.domain.tld под управлением сервера Apache. Статичные объекты сайта располагаются в папках:

- www.domain.tld/res/img/ – изображения;
- www.domain.tld/res/css/ – таблицы стилей;
- www.domain.tld/res/js/ – JavaScript-библиотеки.

Есть множество способов, позволяющих включить режим декларативного срока актуальности данных. Один из способов – поместить в папку www.domain.tld/res/ файл .htaccess, содержащий следующие инструкции:

```
FileETag None
Header unset Last-Modified
Header set Expires "Thu, 15 Apr 2030 20:00:00 GMT"
```

Первая строка – убирает из HTTP-заголовка ETag, вторая – дату последней модификации, третья добавляет поле Expires. До наступления указанной в Expires даты, файл не будет перезагружен с сервера.

В нашем случае указана дата из далёкого будущего (Thu, 15 Apr 2030 20:00:00 GMT). На практике это означает, что файлы будут загружаться единожды и в дальнейшем всегда использоваться версии, хранящиеся в кэше. Данная мера помогает избавиться от огромного количества HTTP-запросов и существенно повышает скорость повторной загрузки страниц.

Однако в случае обновления файла на сервере до указанной даты браузер все равно будет упорно использовать версию из кэша, что приведет к неправильному функционированию сайта из-за проблемы синхронизации данных на сервере и в кэше.

Хорошие вещи не даются даром, поэтому для существенного ускорения сайта придется самостоятельно заботиться о контроле версий загружаемых объектов. К счастью, существует простой и проверенный способ решения этой проблемы, заключающийся в привязке версии к URL-адресу объекта. Другими словами, изменение адреса объекта является признаком модификации.

Если на сайте существует изображение с адресом www.domain.tld/res01/img/logo.png, то после изменения файла, должен измениться и его URL www.domain.tld/res02/img/logo.png. Здесь версия файла включена в URL-адрес в виде имени подпапки res02, но это не единственный способ, также версию файла можно передавать в виде параметра, например, www.domain.tld/res/img/logo.png?ver=03.

После очередного обновления сайта изменятся URL адреса даже тех объектов, которые в действительности не были модифицированы, что приведет к необходимости загружать все объекты заново, даже если часть из них уже присутствует в кэше.

Решить проблему можно путем присвоения индивидуальной версии каждому объекту. Идентификатор версии объекта должен быть привязан к данным, хранящимся внутри файла. Для вычисления идентификатора версии можно использовать crc32, md5 или дату последней модификации файла в формате UnixTime. Таким образом мы создаем свой аналог ETag, передаваемый посредством URL:

```
www.domain.tld/res/img/logo.png?etag=342345334
www.domain.tld/res/img/map.png?etag=983234521
```

Вычисление индивидуального идентификатора версии объекта позволяет эффективнее использовать систему кэширования. Однако налагает обязательство всякий раз при генерации ссылки на объект вычислять его версию, что даёт дополнительную нагрузку на сервер. Для большинства проектов разумным компромиссом будет использование в виде версии единого значения (определяемого константой) для всех объектов.

Способ вычисления идентификатора версии объекта и внедрения его в URL-адрес не влияет на принцип работы данного метода кэширования.

Для правильной работы сайта необходимо, чтобы все страницы использовали корректные URL-объекты. Редактирование всех мест, где осуществляется подключение таблиц стилей, скриптов и изображений после каждого обнов-

ления сайта, достаточно утомительное и малопродуктивное занятие. Лучшее решение проблемы – создание метода, отвечающего за построение URL-адреса объекта с учетом текущей версии, например, так:

```
<?
class View {
    const resVersion = '04';

    public static function includeImg($fileName)     {
        return '/res'.self::resVersion.'/img/'.$fileName;
    }
}

echo '<img src="'.View::includeImg('logo.png').'">';
?>
```

Результатом работы сценария, будет вывод строки: <img src="/res04/img/logo.png">. Использование метода для подключения изображений, таблиц стилей и JavaScript-библиотек позволяет легко изменить URL всех подключаемых объектов. Также можно включать версию файла в качестве параметра запроса, например, /res/img/logo.png?ver=04.

Проверка теории практикой

Для проверки эффективности данного метода кэширования проведем эксперимент. Создадим простую веб-страницу вида:

```
<html>
<head>
<link rel="stylesheet" href="/res_v1/css/style.css" ↵
       type="text/css">
       <title>Test cache system</title>
</head>
<body>
<h1>Try to load some</h1>
<p>Load some imgs, load some aditional CSS and JS code</p>

<img src="/res_v1/img/1.jpg">
<img src="/res_v1/img/2.jpg">
<img src="/res_v1/img/3.jpg">
<img src="/res_v1/img/4.jpg">
<img src="/res_v1/img/5.jpg">

<script type="text/javascript" src="/res_v1/js/test.js"> ↵
       </script>
</body>
</html>
```

Сконфигурируем веб-сервер таким образом, чтобы для кэширования объектов из папки res_v1 использовалась метка сущности (ETag). С помощью Firebug (расширение для Firefox) измерим скорость повторной загрузки страницы, т.е. в момент загрузки все объекты присутствуют в кэше браузера (см. рис. 3).

Теперь отключим ETag и в качестве алгоритма кэширования воспользуемся датой из далёкого будущего с включением версии объекта в URL строку (см. рис. 4).

Из результатов эксперимента видно, что во втором случаи страница была загружена на 27ms быстрее (т.е. ускорение на 57%).

Достоинства и недостатки

Достоинства:

- Максимальное ускорение повторной загрузки кэшируемых объектов. Снижение нагрузки на сервер.

Недостатки:

- Необходимость контролировать версии файлов и актуальность URL-адресов.
- Кэшируемые подобным образом объекты не должны иметь внешних ссылок. Если потребуется установить ссылку на картинку, содержащую версию сайта http://www.domain.tld/res04/img/logo.png, то после обновления сайта, URL картинки изменится, предыдущая ссылка перестанет работать. Сервер можно настроить таким образом, чтобы ссылки вида http://www.domain.tld/res[любое число]/img/logo.png указывали на существующий файл, но в этом случае пользователь не сможет получать обновления.

Описанная методика кэширования статичных объектов успешно работает во множестве проектов, позволяет добиться наиболее значительного ускорения повторной загрузки страниц.

Способ №3: распределение объектов между серверами

Часть объектов, необходимых для визуализации страницы, браузер может загружать в параллельном режиме, остальные объекты будут ждать своей очереди. Сколько именно объектов может быть загружено в параллельном режиме, зависит от настроек браузера.

Стандарт, описывающий протокол HTTP/1.1, рекомендует не более 2 параллельных соединений. С тех пор, когда был написан стандарт, прошло много времени, средняя скорость доступа к сети возросла, поэтому современные браузеры позволяют осуществлять большее количество соединений (от 4 до 8, в зависимости от типа и версии браузера).

Если браузер пользователя имеет ограничение на количество одновременных загрузок равное 4, то при отображении страницы, требующей подключения 20 различных объектов, параллельная загрузка начнётся для первых 4 ресурсов, остальные 16 будут ожидать появления свободного соединения.

Обойти это ограничение можно. Идея заключается в том, чтобы распределить загружаемые ресурсы между несколькими хостами. Например, для сайта www.domain.tld картинки можно разместить с использованием хостов img1.domain.tld, img2.domain.tld,…, imgN.domain.tld (IP-адреса хостов могут совпадать).

Суммарное количество HTTP-запросов останется прежним, однако они будут распределены между несколькими хостами, что позволит одновременно загружать большее число объектов.

В предыдущем разделе описаны преимущества использования специального метода для подключения изображений, данная техника полезна и для решения задачи распределения ресурсов между хостами. Модифицируем View::includeImg(), таким образом, чтобы осуществлялось равномерное распределение подключаемых изображений между заданным количеством хостов:

```
<?php
class View {
    const resVersion = '02';
    const baseDomain = 'domain.tld';
    const hostAmount = 4;

    public static function includeImg($fileName)     {
        $hostN = abs(crc32($fileName)) % self::hostAmount;
        return http://img'.$hostN.'.'.self::baseDomain.'/ ↵
            res'.self::resVersion.'/img/'.$fileName;
    }
}
```

```
echo '<img src="'.View::includeImg('logo.png').'">';
echo '<img src="'.View::includeImg('logo8.png').'">';
echo '<img src="'.View::includeImg('user.gif').'">';
echo '<img src="'.View::includeImg('foto.png').'">';
?>
```

Результатом работы скрипта будет следующий HTML-код:

```
<img src="http://img0.domain.tld/res02/img/logo.png">
<img src="http://img1.domain.tld/res02/img/logo8.png">
<img src="http://img2.domain.tld/res02/img/user.gif">
<img src="http://img3.domain.tld/res02/img/foto.png">
```

В алгоритме распределения важны два фактора:

- распределение ресурсов между хостами должно быть равномерным;
- имя хоста должно быть жестко привязано к файлу, иначе возникнут проблемы с кэшированием.

Можно сделать так, чтобы каждый файл грузился с отдельного хоста, что позволит загружать файлы одновременно. Однако данная мера приведет к существенному увеличению времени загрузки страницы по следующим причинам:

Чтобы браузер мог загрузить файл с хоста, ему необходимо знать IP-адрес. Определение IP-адреса по имени хоста занимает время, если эту операцию придется выполнять для каждого загружаемого объекта, то это существенно понизит скорость загрузки страницы.

Скорость загрузки объектов ограничена пропускной способностью канала передачи данных. Параллельные загрузки делят имеющийся канал между собой.

Какое количество хостов оптимально для загрузки объектов? Для ответа на этот вопрос специалисты компании Yahoo провели исследование (http://yuiblog.com/blog/2007/04/11/performance-research-part-4). Исследователи пришли к выводу, что нужно использовать минимум два хоста для загрузки объектов, при увеличении числа хостов свыше четырёх наблюдается падение производительности.

С моей точки зрения, разумно остановиться на небольшом числе хостов, зависящем от количества загружаемых объектов, например один хост для 10-15 объектов. Этот параметр индивидуален для каждого проекта и должен подбираться экспериментальным путём.

Подводим итоги

Доведя любую идею до абсолюта, можно получить её противоположность. Объединив все ресурсы, необходимые для визуализации страницы, в один большой HTML-документ можно сократить количество необходимых HTTP-запросов до одного.

Помимо проблем с поисковыми системами и трудностями сопровождения данное решение чревато низкой скоростью загрузки страниц, обусловленной следующими факторами:

- отсутствие кэширования;
- все данные загружаются последовательно, в один поток, что существенно замедляет процесс визуализации страницы.

Важно помнить, что снижение количества HTTP-запросов не конечная цель, а средство повышения скорости загрузки сайта. Секрет высокой производительности – поиск оптимального количества HTTP-запросов, позволяющих максимально эффективно использовать канал передачи данных и систему кэширования. EOF

1. Библиотека для минификации JS/CSS-кода и минимизации HTTP-запросов – http://code.google.com/p/minify и http://yuiblog.com/blog/2008/07/16/combohandler.
2. Передача изображения внутри HTML-документа – http://ru.wikipedia.org/wiki/Data:_URL.
3. Подробное объяснение техники CSS Sprite – http://www.alistapart.com/articles/sprites и http://css-tricks.com/css-sprites.
4. Online-сервис для генерации CSS-спрайтов – http://spritegen.website-performance.org.
5. Online-сервис по преобразованию изображений в data:URL-формат – http://www.sveinbjorn.org/dataurlmaker.
6. Правила, регулирующие количество одновременных соединений для протокола HTTP/1.1: http://www.w3.org/Protocols/rfc2616/rfc2616-sec8.html#sec8.1.4.
7. Использование нескольких доменов для загрузки объектов – http://www.stevesouders.com/blog/2009/05/12/sharding-dominant-domains и http://yuiblog.com/blog/2007/04/11/performance-research-part-4.

Рисунок 3. Результат: 8 HTTP-запросов, 47ms

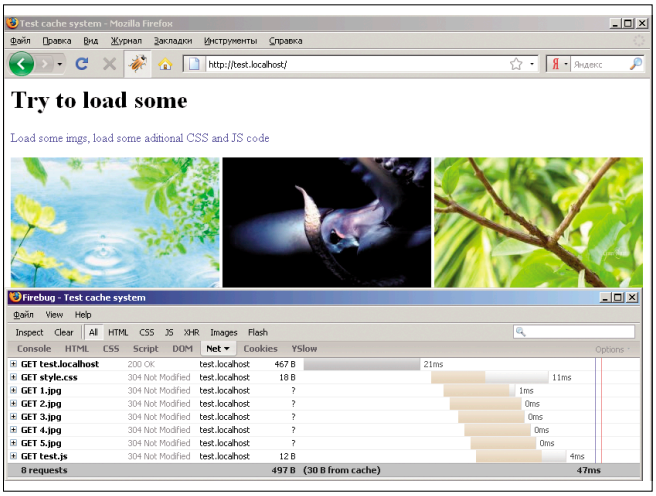
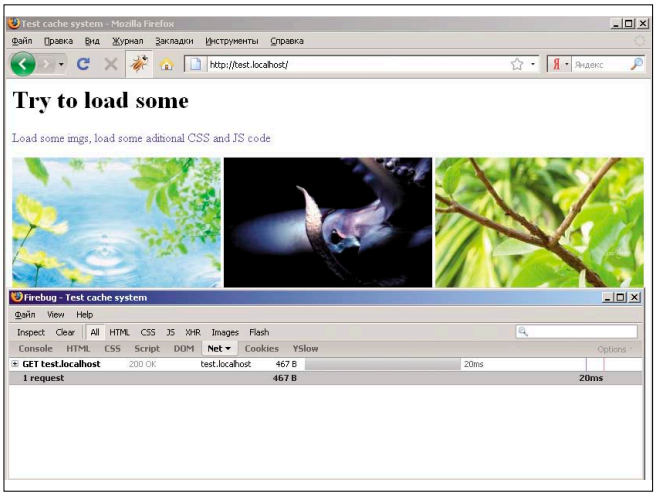


Рисунок 4. Результат: 1 HTTP-запрос, 20ms



Визитка

АНДРЕЙ ШЕТУХИН, руководитель почтовой службы Rambler

Как работает suexec

Безопасность — одна из самых важных задач индустрии веб-хостинга. Вторая, не менее значимая, задача — построить систему, удобную для пользователя. Рассмотрим принцип работы одного из инструментов для построения подобной системы — Apache suexec.

Apache suexec впервые появился в версии 1.2 и с тех пор зарекомендовал себя как стабильный и простой инструмент для безопасного запуска пользовательских скриптов. Тем не менее следует отметить, что неправильная настройка или непонимание принципов работы suexec могут привести к печальным последствиям для всего веб-хостинга. Поэтому детальное знание принципов работы suexec необходимо любому администратору веб-сервиса.

Прежде всего надо понимать, для чего предназначен suexec: для безопасного запуска CGI-сценариев. Поскольку ключевой момент – безопасность, suexec делает множество разнообразнейших проверок, призванных предотвратить возможные попытки взлома системы. Общая схема работы Apache следующая: веб-сервер Apache, как правило[1], запускается от пользователя root, но работает от непривилегированного пользователя, обычно от пользователя www, www-data, apache или nobody (зависит от ОС). Переход от root к непривилегированному пользователю производится системными вызовами setgid и setuid. Вызовы setgid и setuid доступны только пользователю root. Это означает, что никаким образом в рамках одного процесса невозможно из пользователя www стать пользователем username. Будь это не так, ОС UNIX-like были бы дырявы, как решето.

Как же решить задачу исполнения CGI-сценариев от указанного нами в конфигурации Apache пользователя?

Ответ прост: воспользоваться программой suexec.

Suexec – программа, выполняющая CGI-сценарий от указанного владельца. В рамках одного процесса невозможно сменить одного непривилегированного пользователя на другого. Поэтому suexec – отдельная suid-программа, запускающаяся на каждое исполнение CGI-сценария от пользователя root и работающая с правами указанного пользователя. Давайте рассмотрим права доступа к suexec:

```
ls -la /usr/local/sbin/suexec
```

```
-rws--x--x  1 root  wheel  10292 30 май 13:58
/usr/local/sbin/suexec*
```

Символ s в правах доступа означает установленный suid bit. Программа с установленным suid bit независимо от того, кто ее запустил, исполняется от того пользователя, кому принадлежит. Suexec принадлежит root, поэтому, когда Apache его запускает, он работает с правами root.

Далее все просто: suexec делает необходимые проверки и выполняет вызовы setgid и setuid, устанавливая владельца и его группу. Потом запускается требуемый CGI-сценарий. Схематично все описанное выглядит так, как показано на рисунке. Вот, собственно, и весь алгоритм. Дальнейший материал будет посвящен детальному описанию проверок, производимых suexec перед вызовом CGI-сценария.

Конфигурация suexec

Запуск suexec возможен двумя способами:

- С параметром -V. В этом случае печатается набор опций, с которыми была собрана программа.
- С 3 параметрами командной строки: именем пользователя, именем группы и путем к запускаемому сценарию.

Вывод опций может выглядеть примерно так:

```
-D AP_DOC_ROOT="/home"
-D AP_GID_MIN=1000
-D AP_HTTPD_USER="www"
-D AP_LOG_EXEC="/var/log/apache/suexec_log"
-D AP_SAFE_PATH="/usr/local/bin:/usr/bin:/bin"
-D AP_UID_MIN=1000
-D AP_USERDIR_SUFFIX="www
```

Кратко остановимся на каждой:

AP_DOC_ROOT – каталог, в котором возможен запуск CGI-сценариев. В данном случае – /home и все его подкаталоги. Программы, расположенные в других каталогах, например, в /usr, исполняться не будут.

AP_GID_MIN, AP_UID_MIN – минимальный UID и GID владельца, для которого разрешен запуск CGI.

AP_HTTPD_USER – имя пользователя, от которого запущен Apache. Никто, кроме указанного пользователя, использовать по назначению suexec не может. В случае

1. Запуск от пользователя root требуется для работы с TCP-портами меньше 1024-го. Для выполнения команды bind на 80 порт требуются права суперпользователя.

попытки в лог будет записано сообщение: user mismatch (имя_пользователя instead of www).

AP_LOG_EXEC – имя лог-файла suexec.

AP_SAFE_PATH – список путей, признанных безопасными. Здесь перечислены дополнительные каталоги, откуда возможен запуск программ.

AP_USERDIR_SUFFIX – имя каталога, откуда следует запускать программу в случае, если имя пользователя указано в виде '~username.

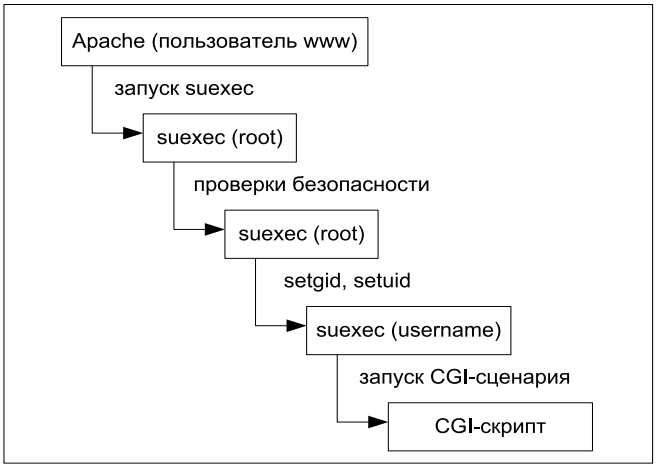
AP_SUEXEC_UMASK – маска прав при создании файлов и каталогов.

Алгоритм работы и проверок suexec

Список с примерами ошибок дан в соответствии с последовательностью проверок в коде suexec.c.

- Очистка переменных окружения. Допустимыми считаются только те переменные, что указаны в списке:
  - HTTP_*
  - SSL_*
  - AUTH_TYPE=
  - CONTENT_LENGTH=
  - CONTENT_TYPE=
  - DATE_GMT=
  - DATE_LOCAL=
  - DOCUMENT_NAME=
  - DOCUMENT_PATH_INFO=
  - DOCUMENT_ROOT=
  - DOCUMENT_URI=
  - GATEWAY_INTERFACE=
  - HTTPS=
  - LAST_MODIFIED=
  - PATH_INFO=
  - PATH_TRANSLATED=
  - QUERY_STRING=
  - QUERY_STRING_UNESCAPED=
  - REMOTE_ADDR=
  - REMOTE_HOST=
  - REMOTE_IDENT=
  - REMOTE_PORT=
  - REMOTE_USER=
  - REDIRECT_HANDLER=
  - REDIRECT_QUERY_STRING=
  - REDIRECT_REMOTE_USER=
  - REDIRECT_STATUS=
  - REDIRECT_URL=
  - REQUEST_METHOD=
  - REQUEST_URI=
  - SCRIPT_FILENAME=
  - SCRIPT_NAME=
  - SCRIPT_URI=
  - SCRIPT_URL=
  - SERVER_ADMIN=
  - SERVER_NAME=
  - SERVER_ADDR=
  - SERVER_PORT=
  - SERVER_PROTOCOL=
  - SERVER_SIGNATURE=
  - SERVER_SOFTWARE=
  - UNIQUE_ID=
  - USER_NAME=
  - TZ=

Схема работы suexec



> Проверка существования учетной записи пользователя, от которого запускается suexec.
> Проверка соответствия имени пользователя, запустившего suexec и AP_HTTPD_USER.

```
root!machine# suexec stellar stellar /bin/ls
[2008-10-31 12:34:14]: user mismatch (root instead
of www)
```

> Проверка пути к запускаемому CGI-скрипту. Путь к запускаемому сценарию не должен начинаться с «/» и «../», а также не должен содержать «/../».

```
www!machine$ suexec stellar stellar /bin/ls
[2008-10-31 12:36:20]: invalid command (/bin/ls)
```

> Проверка существования пользователя (по имени или по ID).

```
www!machine$ suexec stellar nonexistent ./ls
[2008-10-31 15:14:34]: invalid target group name:
(nonexistent)
www!machine$ suexec stellar 88888 ./ls
[2008-10-31 15:10:55]: invalid target group id:
(88888)
```

> Проверка существования группы пользователя (по имени или по ID).

```
www!machine$ suexec nonexistent nonexistent ./ls
[2008-10-31 15:10:47]: invalid target user name:
(nonexistent)
www!machine$ suexec 77777 88888 ./ls
[2008-10-31 15:10:55]: invalid target user id: (77777)
```

> Проверка AP_GID_MIN, AP_UID_MIN – минимальных UID и GID владельца, для которых разрешен запуск CGI.

```
www!machine$ suexec root 0 ./ls
[2008-10-31 15:16:03]: cannot run as forbidden uid
(0/./ls)
www!machine$ suexec stellar 0 ./ls
[2008-10-31 15:16:03]: cannot run as forbidden gid
(0/./ls)
```

> Далее производится вызов setgid и setuid. Если возникла ошибка, выдается сообщение:

```
www!machine$ suexec stellar stellar ./ls
[2008-10-31 15:24:01]: uid: (ashetuhin/ashetuhin) gid:
(ashetuhin/ashetuhin) cmd: ./ls
[2008-10-31 15:24:01]: failed to setgid (1001: ./ls)
[2008-10-31 15:24:01]: failed to setuid (1001: ./ls)
```

Обычно это означает, что неверно выставлены права на программу suexec, а точнее, что не установлен suid bit.

> Проверка на запуск скрипта из userdir. Если имя пользователя задано с тильдой (~), осуществляется переход в домашний каталог пользователя, а затем – в каталог, заданный в AP_USERDIR_SUFFIX. Если имя пользователя задано без тильды, осуществляется проверка на вхождение текущего каталога в AP_DOC_ROOT[2].

```
www!machine$ suexec stellar stellar ./ls
[2008-10-31 15:39:20]: cannot get docroot information
(/usr/local/www/data)
```

> Проверка прав доступа к текущему рабочему каталогу.
> Проверка невозможности записи в рабочий каталог для всех, кроме владельца.
> Проверка прав доступа к запускаемому сценарию.

```
www!machine$ suexec stellar stellar ./ls
[2008-10-31 16:05:39]: cannot stat program:
(./nonexistent)
```

> Проверка невозможности записи в файл CGI-сценария для всех, кроме владельца.

```
www!machine$ suexec stellar stellar ./ls
[2008-10-31 16:08:50]: file is writable by others:
(/usr/local/www/data/stellar/./ls)
```

> Проверка отсутствия установленных на файл CGI-сценария suid- и sugid-флагов.

```
www!machine$ suexec stellar stellar ./ls
[2008-10-31 16:09:34]: file is either setuid or
setgid: (/usr/local/www/data/stellar/./ls)
```

> Проверка совпадения владельца, группы каталога и запускаемого сценария с указанными в параметрах командной строки suexec.

```
www!machine$ suexec stellar stellar ./ls
[2008-10-31 15:43:48]: target uid/gid (1001/1001)
mismatch with directory (80/80) or program (0/0)
```

> Проверка флага execute CGI-сценария.

```
www!machine$ suexec stellar stellar ./ls
[2008-10-31 16:10:20]: file has no execute permission:
(/usr/local/www/data/stellar/./ls)
```

> Установка AP_SUEXEC_UMASK.
> Запуск CGI-сценария.

Итак, мы рассмотрели все аспекты работы suexec. Несмотря на то что технологии CGI и SSI все более вытесняются mod_(phplperllpython) и FastCGI, до сих пор существует большое количество приложений, для безопасной работы которых требуется suexec. Надеюсь, статья поможет в освоении этого полезного инструмента. EOF

2. Получение текущего рабочего каталога, переход в AP_DOC_ROOT, получение имени текущего рабочего каталога (должно получиться AP_DOC_ROOT), переход обратно в каталог, откуда запускалась программа, сравнение полученного каталога и AP_DOC_ROOT. Такая сложная проверка не позволяет подделать путь при помощи символических ссылок.

12 лет

НАША КОМПАНИЯ ПРЕДОСТАВЛЯЕТ ЛИНИИ СВЯЗИ В САМЫХ НЕПРОХОДИМЫХ МЕСТАХ МОСКВЫ

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

ЗВОНИТЕ, ДОГОВОРИМСЯ!

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

Визитка

СТАНИСЛАВ ШПАК, более 5 лет занимается сопровождением Active Directory и Windows-серверов. Имеет сертификаты MCSE по Windows Server 2000/2003

История одного знакомства

Будильник зазвенел пронзительно и настойчиво. Иногда по утрам Игорю казалось, что было ошибкой ставить в качестве мелодии для пробуждения звонок старого классического будильника, но, надо отдать должное, просыпаться это помогало, хоть и не поднимало настроения. А сегодня был к тому же особый случай – у него было жуткое похмелье. Несмотря на то что Игорь не был принципиальным трезвенником, как и большинство админов, он обычно ограничивался пивом. Однако вчера обычная админская посиделка плавно перетекла в празднование какой-то знаменательной даты одного из знакомых и как следствие – с переходом на более крепкие напитки. В результате события вчерашнего дня вспоминались отрывочно. Судя по тому, как ему сейчас было плохо, можно было с уверенностью сказать, что вчера было очень хорошо.

На работу Игорь явился с большим опозданием и бутылкой кисломолочного напитка в руках. К счастью шеф, сочувственно посмотрев, не сказал ничего. Работник из него сегодня был никакой, но худо-бедно получалось справляться хотя бы с текучкой, и после обеда, почувствовав себя несколько лучше, он осилил все-таки залогиниться в аську, чтобы с коллективной помощью восстановить в памяти пропущенные участки вчерашнего дня.

Источник информации искать не пришлось – его уже дожидалось несколько сообщений, присланных ему, пока он был не в Сети, среди которых одно было от Андрея – его друга, который также присутствовал в рядах вчерашней компании. После нескольких дежурных фраз и пары дружеских подначек началась более содержательная беседа:

– А знаешь, ты вчера нас здорово удивил, когда взялся спорить с той девчонкой, – писал Андрей.

– О, замечательно, теперь я узнаю, что там еще была девушка, – и что я с ней делал? Надеюсь ничего такого, за что потом будет стыдно перед админами ютуба?

– Гы, нет друг, ты, как настоящий админ, даже выпив и даже с девушкой, обсуждал сугубо админские темы – мы тобой гордились!

– А что хоть за девушка была? Я ее знаю?

– Теперь знаешь, вы как раз и познакомились на почве сетевых угроз и защиты периметра :-) Кстати, ты помнишь, о чем и на что вы поспорили в конце концов?

– Дружище, некоторые моменты я помню совсем слабо, так что не томи, пролей свет на эту историю!

– Ну так вот, вы заспорили – она говорила, что в любую корпоративную сеть можно проникнуть, если иметь хорошую мотивацию, а ты утверждал, что если сеть будет достаточно маленькая, чтобы управляться одним человеком «с головой и руками», то это будет практически невозможно. В качестве примера ты приводил сетку в несколько десятков компов на твоей работе. Закончилось все тем, что вы поспорили – если она сможет до конца рабочей недели проникнуть в твою сеть, то ты на ней женишься.

Дочитав до конца фразу, Игорь едва не поперхнулся бутылочным айраном.

– Я ЧТО сделаю???

– Женишься, же-нишь-ся, дружище! Я поэтому и сказал, что мы тобой гордимся – поставить всю свою будущую жизнь на карту в каком-то споре, при этом забыв обговорить, что будет в случае, если ты победишь, – это героический поступок!

– Ты шутишь? Я не мог такого сказать!

– Ну спроси у других – еще 4 человека подписались проследить за результатами вашего спора. Так что я ничего не выдумываю!

– И как же будет определяться проникновение?

– Как-как, письменно! Мы пятеро должны получить письмо якобы от тебя, с текстом о том, что ты признаешь свое поражение и готов исполнить свои обещания. Письмо должно иметь служебный заголовок, в котором бы фигурировал внешний IP-адрес твоей работы и внутреннее имя, и айпишник твоего рабочего компьютера. Образец твоего письма для анализа заголовка мы ей предоставили сразу после заключения спора. Так что, друг, береги свою сеть в ближайшую неделю как никогда не берег! А меня вызывает шеф, так что до связи!

– Эй, погоди, она хоть симпатичная? – попытался спросить Игорь, но статус друга уже сменился на Away.

Игорь задумался… Воспоминания о событиях минувшего вечера были настолько рваными, что изложенная история его спора вполне могла оказаться правдой. Да и друг бы врать не стал, одно дело мелкие подколки, а другое – такой жестокий стёб, нет, это вряд ли. Значит, надо исходить из того, что это правда. Голова упорно отказывалась думать. Игорь мысленно перебрал потенциальные, уязвимые снаружи места: файервол, публикация внутренних сервисов наружу, антивирусная защита, установленные заплатки, почтовик… Ага, почтовик. По условиям спора письмо должно в заголовке содержать не только внешний IP, но и связку из внутреннего айпиш-

ника и имени его компьютера. И если второе совсем не проблема, то первое получить не так просто. Для этого ей придется взломать рабочий компьютер Игоря или их корпоративный почтовый сервер. На счет защиты сервера Игорь был спокоен – те серверы, которые обслуживали запросы из Интернета, были на особом контроле. А вот очень внимательно обследовать собственный комп на предмет уязвимостей совсем не помешает. Кроме того, на всякий случай веб-серфинг лучше будет вести из виртуальной машины. Остается еще возможность подделки заголовка письма, но тут знаний Игоря уже не хватало на то, чтобы здраво оценить вероятность такого маневра. Игорь было подумал, не заблокировать ли полностью SMTP-трафик со своего компьютера, но потом решил не впадать в паранойю. Да и к тому же это будет уже жульничество, а значит, можно будет спор аннулировать. Остаток дня Игорь провел, гоняя различные анализаторы уязвимостей и вылизывая защиту собственного компьютера. К вечеру комп можно было считать неприступной крепостью. Но на следующий день ничего экстраординарного не произошло, постепенно работа потекла своим чередом, и Игорь начал забывать о событиях минувших выходных.

До тех пор пока в пятницу утром, когда Игорь ехал на работу, ему не позвонил Андрей.

– Привет, Игорь, ну что, когда свадьба?

– Не понял, какая?

– Ну как, пари помнишь? Мне пришло ночью письмо вроде как от тебя, заголовок верный, в нем написано, что ты проиграл спор.

– Не может быть! – Игорь снова подумал, что это шутка.

– Ну как знаешь, сейчас я тебе это письмо перешлю вложением, сам можешь оценить.

Похоже, Игорь еще никогда не хотел попасть на работу так быстро. Влетев в комнату, он тут же упал за комп под изумленными взглядами коллег. Так, почтовый клиент, вот письмо от друга, так, аттачмент, так, вот оно, посмотреть заголовок и …

В нижней строчке received значилось:

Received: from igor ([192.168.1.12]) by mail.megasupercorp.ru […]

А чуть выше:

Received: from mail.megasupercorp.ru (mail.megasupercorp.ru [216.32.181.22]) by […]

Игорь в растерянности смотрел на заголовок. Имя его компьютера, айпишник его компьютера, внешний айпишник их фирмы – все было правильным. Как во сне, он полез на корпративный почтовый сервер и, сделав поиск отправленных за ночь писем, нашел это письмо. Около 3 часов ночи. С его компьютера. Игорь открыл журнал событий на своем компьютере. Все чисто. Кроме… Вот она – запись о том, что отключался кабель от сетевой платы, а затем вновь был подключен. Та-а-ак. Кто-то физически был тут. И отключал сетевуху, чтобы в сети не было конфликтов IP-адресов. Кто-то отключил его компьютер, включил вместо него какой-нибудь ноут, назначил ему айпишник Игоря, отправил письмо. Но это не честно – спор был о преодолении защиты сети снаружи, а не реальный взлом офиса. Кстати, а что скажет охрана? И Игорь отправился к охранникам.

Скоро все закончилось тем, что Игорю, настаивавшему на том, что кто-то чужой был в офисе ночью, дали посмотреть видеозаписи камер наблюдения, и когда он сам убедился в том, что никто в это время суток в офис не заходил, то стал подозревать чуть ли не общий заговор. На этом месте он сказал себе «Стоп» и решил, что все вопросы он сможет выяснить у этой загадочной девушки, которую он и не помнил, твердо пообещав себе, что выведет ее на чистую воду и что его одинокой холостяцкой жизни пока ничего не угрожает. Игорь снял трубку и позвонил другу.

– Андрей, мне нужны контакты этой девушки.

– Что, признаешь свое поражение?

– Нет пока. Я не спорю, что заголовок верный, но у меня есть сомнения в честности достигнутого результата.

– Ну-ну, ладно. Разбирайтесь. Мы с интересом посмотрим, чем кончится дело – ваша история уже получила некоторую огласку среди ЖЖ-сообщества, так что скоро на тебя можно будет делать ставки. Сейчас я постараюсь выяснить ее номер телефона, напишу тебе тогда.

Не прошло и часа, как Игорь набирал номер той девушки.

– Привет, это Игорь, тот, с которым ты спорила….

– Привет, а меня зовут Инна. Правда, мы уже знакомились, но ходят слухи, что ты не помнишь некоторых деталей того вечера, так что представлюсь еще раз на всякий случай.

– Шутница однако… Но спор выиграла ты нечестно, не было речи о том, чтобы пробираться в офис в реале!

– Вообще-то спор я выиграла честно. И если ты хочешь узнать подробности, а твое желание вполне справедливо, то придумывай, где встретиться, и я удовлетворю твое любопытство по любому вопросу. Не надо голословно обвинять меня в нечестной игре только потому, что ты не смог посмотреть на вопрос шире, – в голосе у нее послышались презрительно-обиженные нотки.

– Ладно, давай завтра после работы, устроит?

– Устроит. Я работаю до 18.30.

– Хорошо, я тебе завтра позвоню, и мы договоримся подробнее о времени и месте встречи.

– Угу, и заодно о том, как ты меня будешь угадывать.

– Эту почетную обязанность я возложу на тебя, во-первых, у тебя есть женская интуиция, а во-вторых, ты-то помнишь, как я выгляжу.

– Ладно, разберемся. До связи.

– До связи.

Нажав «отбой» Игорь вздохнул облегченно. Разговор получился не тягостный, а голос у девушки был приятный. Правда, действительно сильно напрягало то, что он не помнил, как она выглядит. Игорь снова потянулся к телефону, чтобы позвонить друзьям и постараться выяснить ее фамилию, поискать ее фотки в ЖЖ или в социальных сетях, но потом передумал. Во-первых, это пока только слухи ходят, что он не помнит в лицо девушку, с которой спорил, а если он начнет вести расспросы, это станет явным. А во-вторых, черт возьми, сей факт придает некоторую пикантность ситуации. Игорь улыбнулся и позвонил все-таки другу, но только лишь для того, чтобы договориться встретиться сегодня вечерком и выпить по бутылочке пива. Игорь чувствовал, что ему катастрофически нужны свободные уши, в которые можно выговориться.

Около его столика стояло миловидное, но отнюдь не смазливое создание с черными волосами чуть ниже плеч. Стройненькая и одета совсем не так, как представлял себе девушку-админа Игорь…

Встретились они вечером на крыше дома у Андрея. Не так много в городе высоток, на крышу которых можно попасть вполне беспрепятственно, а у друга были ключи от чердака, и лучшего места для разговора под пиво было не найти. Да, это было еще и романтическое место, куда можно было бы привести девушку посмотреть на огни ночного города с высоты птичьего полета, но после того как одна из таких девушек стала женой Андрея, дружеские посиделки на крыше как-то сошли на нет.

– Что ты будешь делать, если все окажется правдой и ты действительно проиграл спор? – спросил Андрей.

– Не знаю. Я вообще ума не приложу, как я мог так опрометчиво спорить. Ты же меня знаешь, я не азартный и не спорщик в принципе. Это все из-за нее, наверное. Глупая бравада перед существом противоположного пола! Тьфу, природные инстинкты! Захотел выпендриться, вот теперь расплачиваюсь!

– Игорь, а вообще ты боишься жениться?

– Как тебе сказать. Я знаю, что рано или поздно это произойдет. Когда начинаешь встречаться с девушкой, первая влюбленность, куча эмоций, думаешь, что вот она, твоя вторая половинка, и даже мысль о свадьбе не так уж и страшна, и кажется, что вот с этим человеком ты готов будешь провести всю жизнь. Но чем больше потом узнаешь человека, тем сильнее оказываются его отличия от нарисованного идеала. Ты начинаешь чувствовать, что кто-то пытается переделать твою жизнь и согнуть тебя по-своему. Возникают ссоры, ревность, упреки и как следствие – расставание.

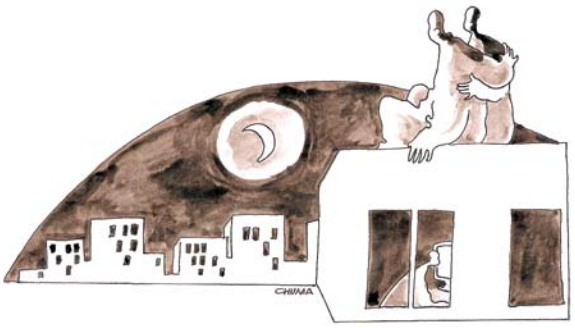
– Игорь, а знаешь, наверное, у каждого мужчины бывают в жизни такие моменты. Ну вот, к примеру, я. Женат уже два года. И ты меня знаешь давно. Все описанное тобой было и у меня. Но если найти в себе силы и не разорвать отношения во время размолвки, то когда вы помиритесь, ты скажешь себе: «Как же клево, что я не сказал того, что вертелось у меня на языке во время ссоры». И я счастлив. Пусть не каждый миг своей жизни, но в целом – счастлив. А тебе, Игорь, может быть, действительно стоит жениться вот так – сразу. Когда над твоими отношениями уже не будет витать «дух страшного загса», может быть, и отношения будут другими?

Они помолчали, потом Игорь задумчиво сказал:

– Знаешь, во многом ты, наверное, прав. И идеалов в природе не существует, конечно. И, наверное, замечательно, когда любишь ты и любят тебя. И ссориться можно хотя бы для того, чтобы потом можно было помириться и почувствовать, как это здорово. Но я тут думал о моей ситуации, и, наверное, не все так плохо. Проще всего было бы, конечно, объявить спор шуткой – никто меня силой под венец не потянет ведь. Может быть, это несколько старомодно, но я привык отвечать за свои слова. К тому же слишком много людей знают о споре, и если я откажусь, то буду объектом шуток еще не знаю сколько времени. Но из-за всего этого можно сделать себе и неплохой пиар! Смотри – админ проигрывает спор, но он честен и поэтому, выполняя все его условия, соглашается жениться. Это будет обмусоливаться в ЖЖ, и я буду почти герой! А свадьба… Ну подумаешь… Существует ведь и развод. В целом это может изрядно встряхнуть мою устоявшуюся жизнь – такое вот своеобразное развлечение.

– Я смотрю, ты уже создал себе своими рассуждениями удобную эмоциональную норку. Мой только тебе совет, Игорек, когда ты рано или поздно женишься, не нацеливайся на развод. Вообще забудь о нем. Пусть эта возможность у тебя будет, но живи так, будто у тебя ее нет. Представь развод, как самоубийство. Ведь ты свои жизненные проблемы не решаешь суицидом, верно? Даже когда плохо и кажется, что это единственный выход, к тому же самый простой. А когда все оказывается позади, ты живешь и радуешься. Вот так и в семейной жизни. Развод – это самоубийство. Ты расписываешься в своем бессилии, малодушности и убиваешь семью. У тебя должен быть очень веский повод для этого. Помни это.

Они еще долго болтали, сидя на крыше. Через какое-то время к ним присоединилась жена Андрея, и втроем они разговаривали о всякой ерунде



и смотрели на постепенно гаснущие огни в окнах окружающих домов.

На следующий день вечером Игорь сидел в небольшом кафе и ждал Инну. Сначала он сел лицом к двери, но спустя 10 минут ему надоело рассматривать всех входящих девушек, вздрагивать, когда кто-то из них направлялся в его сторону, особенно если девушка, мягко говоря, не соответствовала представлениям Игоря о красоте. Поэтому он пересел спиной к двери и сосредоточился на изучении чашечки кофе.

«Привет, Игорь!» – он поднял голову и с трудом подавил вздох облегчения. Около его столика стояло миловидное, но отнюдь не смазливое создание с черными волосами чуть ниже плеч. Стройненькая и одета совсем не так, как представлял себе одежду девушки-админа Игорь – не броско, но со вкусом. Игорь поднялся, поздоровался и предложил ей сесть, попутно отметив, что он все-таки несколько выше ее ростом.

От пустых разговоров о том, будем ли есть или только пить и что именно, как погода за окном и насколько трудным был сегодняшний день на работе, быстро избавились и перешли к тому, что Игоря интересовало больше всего. Он наконец спросил:

– Инна, все-таки расскажи мне детально о том, как появилось то самое письмо?

– OK. Сначала я напомню тебе события дня, когда мы познакомились в первый раз. – Инна улыбнулась.

– Ты тогда обмолвился, что несмотря на то, что все пользователи твоей фирмы имеют выход в Интернет, доступ в социальные сети у вас закрыт. Тем самым ты натолкнул меня на мысль. Я сделала поиск в социальных сетях по названию твоей фирмы. Да, она не очень крупная, но в результате поиска образовалось несколько человек. Из них я выбрала три жертвы – девушки, которые, судя по их анкете, достаточно общительные. Мне пришлось создать три поддельных анкеты симпатичных парней и обратиться к своим друзьям с тем, чтобы они добавили этих выдуманных персонажей в список друзей. Некоторые расписали мне «стену», прокомментировали якобы мои фотографии, в общем, за несколько часов я получила три «живые» анкеты.

Далее я «стала» парнем и познакомилась со всеми тремя девушками. – Инна отхлебнула из своей чашки и лукаво добавила:

– Всегда хотела попробовать завести анкету парня. В рабочее время их в Сети, разумеется, не было, поэтому пришлось убить пару вечеров на то, чтобы втереться в доверие, что, кстати, оказалось несложно. На следующем этапе мне надо было выяснить их корпоративные адреса электронной почты. Это оказалось чуть сложнее, но ненамного. После этого я прислала каждой красивую картинку с цветочками, потом пару приколов, а потом специальную программку, замаскированную под прикол. Программку писала не я, а мой хороший знакомый программист, суть ее в том, что, запускаясь вместе с оболочкой при старте операционной системы, она, перебирая стандартные порты, находила открытый и периодически обращалась к удаленному серверу в ожидании появления там команды или дополнительного программного модуля для скачивания. Команда выполнялась на локальном компьютере, а результат направлялся на тот же самый удаленный сервер. Так как мне не хотелось «светить» свой рабочий статический айпишник, пришлось регистрировать имя на одном из сервисов динамического DNS и цеплять его к своему домашнему интернет-каналу. Да, это не помогло бы скрыть мой IP, но по динамическому IP-адресу из пула провайдера обычному человеку не так уж много удастся выяснить, к тому же я не собиралась совершать никаких деструктивных действий.

Рассказ Инны прервал телефонный звонок на мобильник Игоря, но тот, не раздумывая, отключил звук и жестом предложил продолжить.

– Итак, оформив эту программку под забавную флэш-анимацию, я закинула ее трем своим знакомым. Я тебе потом скажу их фамилии, если хочешь, потому что все три ее запустили. Уже на этом этапе я могла инициировать отправку письма из твоей сети, с именем твоего компьютера в заголовке, который, как ты знаешь, обусловлен всего лишь командой приветствия в SMTP, но мне необходимо было выполнение еще одного условия – наличия в заголовке IP-адреса твоего компьютера. Это показалось мне сначала проблемой. Как бы ты поступил на моем месте? – неожиданно задала вопрос Инна.

Игорь растерялся.

– Ну, если под твоим контролем был компьютер, можно было бы поменять ему айпишник, если ты знаешь на какой. Правда, возник бы конфликт адресов в сети, ведь я очень редко выключаю свой компьютер.

Инна снова улыбнулась. Игорь отметил, что у нее очень красивая улыбка.

– Вот-вот, – продолжила девушка, – надежда на то, что ты выключаешь компьютер перед уходом с работы, разумеется, не оправдалась, поэтому просто сменить айпишник на твой было нельзя. Однако когда я проводила сканирование вашей сети в поисках почтового сервера, мне попался IP-адрес управляемого коммутатора, правда, тогда я не придала этому значения. Но потом, при ближайшем его рассмо-

трении, мне действительно здорово повезло – коммутатор оказался с админским паролем по умолчанию. Игорь, вот это твоя первая оплошность – я понимаю, что рулить коммутаторами приходится нечасто, но это еще не повод оставлять у них стандартный пароль.

Игорь смутился. Да, черт возьми, действительно коммутатор с дефолтным паролем достался ему по наследству от предшественника и так и остался в этом положении.

Отхлебнув еще кофе, Инна продолжила:

– Дальше было несложно – выяснить MAC-адрес сетевой платы твоего компьютера, зная IP-адрес, плевое дело, коммутатор поддерживал telnet, инструкцию к нему я нашла в Интернете и найти и отключить порт, на котором висит данный MAC-адрес, было нетрудно. Сложнее оказалось убедить «носителей» моей программы не выключать на ночь компьютеры. В принципе это не было большой необходимостью, так как я могла бы провернуть все и в рабочее время, пока бы ты разбирался, почему у тебя исчез линк с компьютера. Но красивее было бы сделать это ночью. Как выяснилось, одна из моих подопечных и так не отключала компьютер на ночь, но вот беда – у нее не было прав локального администратора, которые нужны для смены IP-адреса. Эту необходимость я поначалу упустила из виду и уж было хотела опять обращаться к другу-программисту, чтобы он написал что-нибудь, умеющее повышать свои привилегии в системе, но памятуя о том, что ты говорил о развернутом в сети сервере обновлений, думаю, что все заплатки на операционную систему там уже стояли, а изыскания других возможностей или анализ свежих уязвимостей – это заняло бы какое-то время. Однако у двух других девушек, права локального администратора были. Это твое второе упущение, Игорь, если ты говоришь о защищенности сети, то нельзя давать пользователю права локального администратора.

Игорь снова перевел глаза с Инны на свою чашку и стал ее рассматривать так, будто очень хотел запомнить ее форму на всю оставшуюся жизнь. В свое время права локального администратора пришлось давать некоторым пользователям, чтобы заработало подключение к сканеру в МФУ по IP. Игорь тогда еще хотел разобраться, на какие файлы и ветки реестра надо дать права пользователю, чтобы не давать повышенные права в системе в целом, но пользователи проблем не доставляли и права локального администратора у них так и остались.

– Мне продолжать или ты уже и так все понял? – спросила Инна.

– Продолжай, вдруг всплывут еще интересные детали, – бесстрастно сказал Игорь.

– Ну слушай. Как на зло, именно эти две девушки компьютеры на ночь и выключали, поэтому мне надо было только убедить их так не делать. Для этого я сначала издалека поинтересовалась у них, разумеется от имени парня, как долго загружаются их компьютеры по утрам, а потом рассказала, как здорово выключать только монитор, а не компьютер. В общем, мне поверили. Наконец в ночь с четверга на пятницу, когда срок нашего спора уже подходил к концу, я получила на ночь компьютер с запущенной моей программой. Ну, что было дальше ты, наверное, уже представляешь – заблокировать твой порт на коммутаторе, сменить из командной строки IP-адрес компьютера – носителя программы на твой адрес, подождать, пока снова восстановится линк, дальше инициировать SMTP-сессию к вашему корпоративному почтовому серверу, передать нужные SMTP-команды, не забыв в команду HELO прописать имя твоего компьютера, убедиться, что письмо пришло и имеет верный заголовок, после этого вернуть все обратно и дать программе команду на самоуничтожение.

Игорь задумчиво помешивал в чашке остатки кофе. Да, кто бы мог подумать, что все так аукнется! А он, как дурак, сосредоточился на защите своего компьютера!

– Хорошо, Инна. Я согласен – ты выиграла. – Игорь залпом допил остатки кофе. – Я не буду увиливать и юлить и готов выполнить свое обещание. Когда тебе удобно поехать в загс и подать заявление?

– Игорь, ты глупый, – Инна посмотрела на него, как на несмышленого младенца. – Неужели ты думаешь, что я настолько хочу замуж, что готова тащить парня в загс таким способом?! Я не считаю себя уродиной или обделенной по жизни и все-таки хочу создать семью по любви, а не в результате выигранного спора! Ты, наверное, думал о том, как ты, бедняга, пожертвуешь своей свободой и холостяцкой жизнью и совсем не задумывался, что для меня это тоже будет жертва. Но поскольку пари мое и по условиям мы не обговаривали, что я должна принять твое предложение, то я отказываюсь. Я, конечно, ценю то, что ты оказался честным настолько, чтобы соблюсти все условия, и даже сомневалась, сможешь ли ты на такое решиться. Ты – смог. Уважаю. Но на этом все. Ты убедился в моих словах об уязвимостях сетей, я убедилась в том, что есть еще люди, которые верны своему слову, и теперь мы распрощаемся. Можешь когда-нибудь прислать мне поздравительную СМС-ку на 8 Марта.

Инна встала, подхватила сумку и добавив: «Приятно было познакомиться и пообщаться», – пошла к выходу.

Игорь медлил всего минуту. После чего, оставив деньги за кофе на столе, выскочил вслед за Инной. Он догнал ее стоящую на светофоре пешеходного перехода и спросил:

– Инна, этого не было в условиях пари, но, если ты не торопишься домой, может быть, мы немного погуляем?

Она посмотрела на него долгим внимательным взглядом. Светофор переключился на зеленый, а Игорь поймал себя на мысли о том, что он ждет ответа Инны, как мальчишка!

– И куда ты предлагаешь пойти? – спросила Инна.

Игорь быстро перебрал в уме стандартные варианты. В кафе только что сидели, в кино как-то бессмысленно в данном случае, в парке сейчас много людей, а хотелось уединения, и тут Игоря осенило:

– Я знаю одно место. Думаю, тебе там понравится – по крайней мере ты наверняка не часто видела город с такого ракурса.

Инна улыбнулась:

– Игорь, быть загадочным – это удел девушек. Но, как и любая девушка, я люблю сюрпризы, поэтому пойдем, посмотрим на город из этого «секретного» места.

Она взяла его под руку, и они пошли по вечерней улице. По дороге Игорь сделал только один телефонный звонок – он попросил Андрея не уходить пока из дома – ему очень нужен был ключ от выхода на крышу высотки. EOF

Павел Закляков:
«Нужно, чтобы после прочтения человек бежал к компьютеру»

На вопросы «Системного администратора» отвечает наш постоянный читатель и автор, ИТ-специалист Павел Закляков

– Почему вы читаете «Системный администратор»?

– Жизнь надо ценить за её многообразие, а журнал – за наличие в нём статей единомышленников. Привлекает возможность узнать что-то новое. Если кто-то потратил 10 часов на настройку, то он всегда сможет дать совет новичкам. Заочное обучение получается. Технические науки настолько ёмкие, что нельзя быть специалистом везде, вот журнал и позволяет обмениваться опытом и не наступать на грабли повторно.

Думаю, что именно это привлекает читателей и авторов – обмен мнениями. Изначально повелось, что в журнал писали те, кто этого хотел, а редакция лишь отбирала лучшие материалы, не взирая на лица.

Статьи должны заставлять читателей задумываться, разрушать их привычные стереотипы. Это самое главное в журналистике. Нужно, чтобы после прочтения человек бежал к компьютеру – пытался сделать привычное по-новому, торопился высказать своё мнение на форуме…

– Какая изюминка, на ваш взгляд, должна быть у «Системного администратора»?

– Во-первых, эксклюзивное общение с органами власти по вопросам информатизации общества. Можно регулярно (раз в квартал, например) публиковать ответы на вопросы читателей. Технические умы могли бы предлагать решения важных для общества вопросов, а чиновники – критиковать или внедрять их в жизнь. Ведь и чиновники не могут без технических идей, и мы без них не можем ничего внедрить.

Во-вторых, это обучение: понятные тексты и больше ссылок на материалы по конкретным вопросам. Будем писать понятно, интересно и с ссылками на хорошую литературу – число читателей вырастет автоматически.

Жизнь надо ценить за её многообразие, а журнал — за наличие статей единомышленников

Возьмите школьников старших классов, интересующихся информатикой, – это тоже потенциальные подписчики и будущие авторы!

– Какой рубрики не хватает журналу?

– Несомненно, научной. Многие администраторы используют вычислительные сети, хорошо их настраивают, но спросим у них: а как на производительность локальной сети повлияет изменение MTU и меняли ли вы эту настройку у себя? Предвижу, что однозначного ответа от половины читателей мы не получим… Или поставим такую «простенькую» задачку: возможно ли перейти от использования СУБД MSSQL к PostgreSQL, какие принципиальные проблемы есть на пути перехода? Если на эти вопросы отвечать серьёзно, то вполне можно претендовать на то, чтобы договориться и открыть на страницах журнала «ВАКовский» раздел, где публиковать статьи с полноценным рецензированием. Пусть рубрика будет не постоянной, но всё же журнал станет принципиально отличаться от своих собратьев хотя бы тем, что на него будут подписаны большинство технических библиотек.

А начать можно с простого: откройте рубрику «Конкурсные задания по информатике». Пусть в знаниях и сообразительности сразятся школьники и администраторы со стажем. Как вы думаете, кто победит?

– Кто ваши друзья, чем увлекаетесь?

– Друзей мало, но именно их разные взгляды позволяют мне объективно смотреть на мир. Делю друзей, как и всех людей, на креативщиков, анализаторов, копировальщиков и сторонних наблюдателей. Из последних увлечений – фотографирую пейзажи, людей и события в неожиданных ракурсах. Хожу на выставки и в театры, хотя это заслуга моей девушки… EOF

Беседовала Оксана Родионова

Редакционнная подписка
для физических лиц

> Вы можете оформить подписку только на **российский адрес.**
> При заполнении квитанции обязательно **разборчиво укажите фамилию, имя, отчество полностью, почтовый индекс и адрес получателя (область, город, улица, номер дома, номер квартиры), контактный телефон.**
> Журнал высылается почтой заказной бандеролью только после поступления денег на расчетный счет и **копия заполненного и оплаченного бланка, отправленная в редакцию по факсу: (495) 628-8253, (доб. 120) или на emil: subscribe@samag.ru**

ИЗВЕЩЕНИЕ

Кассир

ООО "С 13" Форма № ПД-4
ИНН 7708654814/ КПП 770801001
Р. сч. 40702810300080001868 К. сч. 30101810100000000787
ОАО «УРАЛСИБ» г. Москва БИК 044525787
Коды: по ОКПО 84027582, по ОКОПФ 65

Вид платежа: Редакционная подписка на журнал "Системный администратор" за 2009 г.

01	02	03	04	05	06	07	08	09	10	11	12
X	X	X	X	X	X	X	X	X	X	X	X

Дата_____ Сумма платежа: 2400 руб. 00 коп.

Информация о плательщике:

_____
(Ф. И. О. почтовый индекс, адрес и телефон)

_____

_____

Подпись _____

КВИТАНЦИЯ

Кассир

ООО "С 13" Форма № ПД-4
ИНН 7708654814/ КПП 770801001
Р. сч. 40702810300080001868 К. сч. 30101810100000000787
ОАО «УРАЛСИБ» г. Москва БИК 044525787
Коды: по ОКПО 84027582, по ОКОПФ 65

Вид платежа: Редакционная подписка на журнал "Системный администратор" за 2009 г.

01	02	03	04	05	06	07	08	09	10	11	12
X	X	X	X	X	X	X	X	X	X	X	X

Дата_____ Сумма платежа: 2400 руб. 00 коп.

Информация о плательщике:

_____
(Ф. И. О. почтовый индекс, адрес и телефон)

_____

_____

Подпись _____

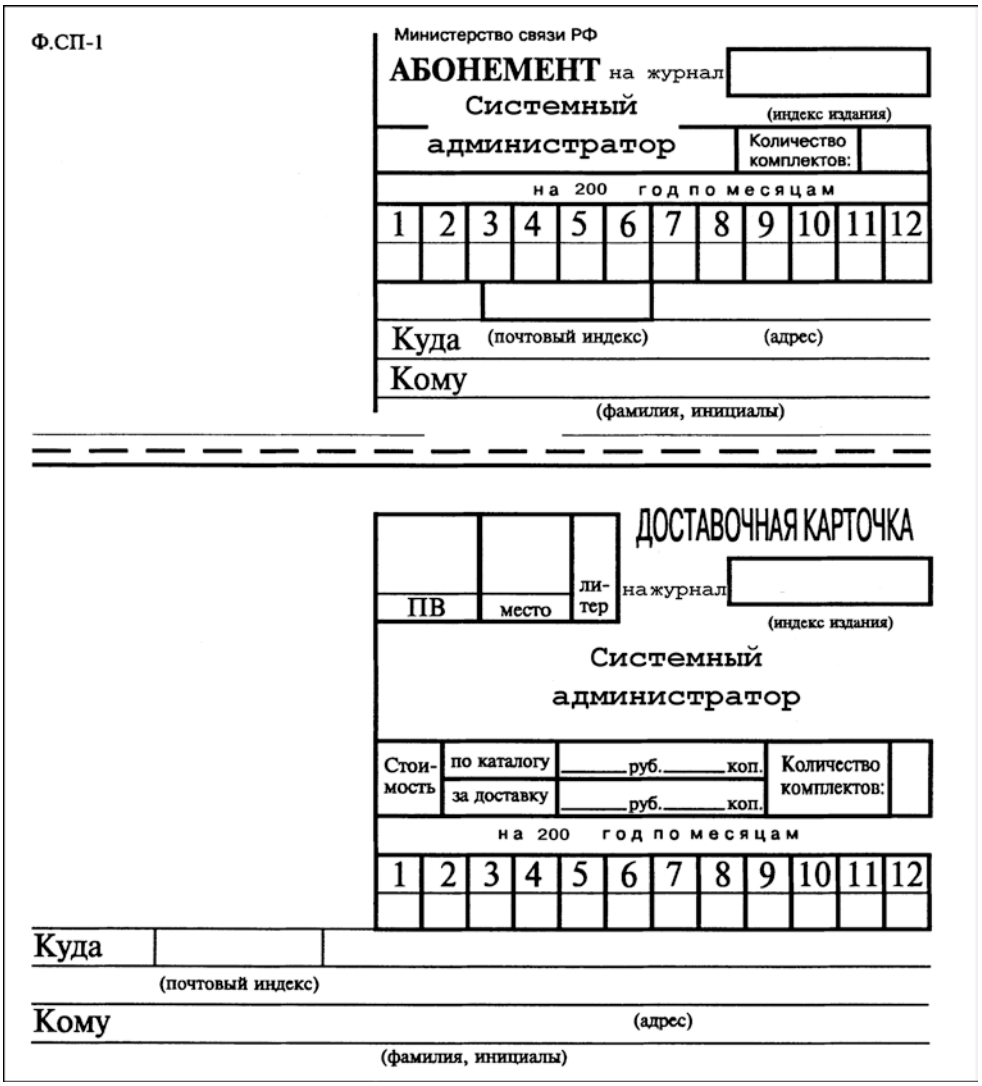
Российская Федерация

> Подписной индекс годовой – **20780**, полугодовой – **81655**
Каталог агенства **«Роспечать»**
> Подписной индекс годовой – **88099**, полугодовой – **87836**
Объединенный каталог **«Пресса России»**
Адресный каталог **«Подписка за рабочим столом»**
Адресный каталог **«Библиотечный каталог»**
> Альтернативная подписка агенства:
«Интер-Почта» (495) 500-00-60, курьерская доставка по Москве
«Вся Пресса» (495) 787-34-47
«Курьер-Прессервис»
«ООО Урал-Пресс» (343) 375-62-74
ЛинуксЦентр www.linuxcenter.ru
> Подписка On-line:
http://www.arzi.ru
http://www.gazety.ru
http://www.presscafe.ru

СНГ

В странах СНГ подписка принимается в почтовых отделениях по национальным каталогам или по списку номенклатуры **«АРЗИ»**:

> **Азербайджан** – по объединенному каталогу российских изданий через предприятие по распространению печати **«Гасид»** (370102, г. Баку, ул. Джавадхана, 21)
> **Казахстан** – по каталогу **«Российская Пресса»** через ОАО **«Казпочта»** и ЗАО **«Евразия пресс»**
> **Беларусь** – по каталогу изданий стран СНГ через РГО **«Белпочта»** (220050, г. Минск, пр-т Ф. Скорины, 10)
> **Узбекистан** – по каталогу российские издания через агентство по распространению печати **«Davriy nashrlar»** (7000029, г. Ташкент, пл. Мустакиллик, 5/3, офис 33)
> **Армения** – по списку номенклатуры **«АРЗИ»** через ГЗАО **«Армпечать»** (375005, г. Ереван, пл. Сасунци Давида, д. 2) и ЗАО **«Контакт-Мамул»** (375002, г. Ереван, ул. Сарьяна, 22)
> **Грузия** – по списку номенклатуры **«АРЗИ»** через АО **«Сакпресса»** (380019, г. Тбилиси, ул. Хошараульская, 29) и АО **«Мацне»** (380060, г. Тбилиси, пр-т Гамсахурдия, 42)
> **Молдавия** – по каталогу через ГП **«Пошта Молдовей»** (МД-2012, г. Кишинев, бул. Штефан чел Маре, 134)
по списку через ГУП **«Почта Приднестровья»** (MD-3300, г. Тирасполь, ул. Ленина, 17)
по прайс-листу через ООО Агентство **«Editil Periodice»** (МД-2012, г. Кишинев, бул. Штефан чел Маре, 134)
> **Украина** – Киевский главпочтамт
Подписное агентство **«KSS»**, тел./факс (044)464-0220



Подписные индексы:

20780*
+ диск с архивом статей 2008 года
81655**
без диска

по каталогу агентства «Роспечать»

88099*
+ диск с архивом статей 2008 года
87836**
без диска

по каталогу агентства «Пресса России»

* Годовой
** Полугодовой
*** Диск вкладывается в февральский номер журнала, распространяется только на территории России

Системный администратор

УЧРЕДИТЕЛИ ИЗДАНИЯ
Частные лица

Генеральный директор
Владимир Положевец
Главный редактор
Галина Положевец
chief@samag.ru
Выпускающий редактор
Наталья Хвостова
sekretar@samag.ru
Выпускающий редактор
Владимир Лукин
Главный редактор электронного приложения «Open Source»
Дмитрий Шурупов
osa@samag.ru
Дизайн-макет
Марина Рязанцева
Дмитрий Бессонов
Иллюстрации
Виктор Чумачев

Над номером работали:
Алексей Барабанов, Александр Емельянов, Кирилл Сухов, Андрей Бешков, Андрей Бирюков, Андрей Луконькин, Рашид Ачилов

Рекламная служба
Дарья Зуморина, reklama@samag.ru,
Евгения Тарабрина, expo@samag.ru,
тел./факс: (495) 628-82-53 (доб.120)

Распространение
Светлана Зобова
(495) 628-82-53 (доб.120)

Адрес редакции
107045, г. Москва, Ананьевский переулок, дом 4/2, стр.1,
тел./факс: (495) 628-82-53 (доб.120)
Сайт журнала: www.samag.ru

Издатель
ООО «С 13»

Отпечатано в типографии
ООО «Периодика»
Тираж 17000 экз.
Тираж электронной версии 62000 экз.